ICSNC 2011

The Sixth International Conference on Systems and Networks Communications

ISBN: 978-1-61208-166-3

October 23-29, 2011

Barcelona, Spain

ICSNC 2011 Editors

Pascal Lorenz, University of Haute Alsace, France

ICSNC 2011

Forward

The Sixth International Conference on Systems and Networks Communications (ICSNC 2011), held on October 23-29, 2011 in Barcelona, Spain, continued a series of events covering a broad spectrum of systems and networks related topics.

As a multi-track event, ICSNC 2011 served as a forum for researchers from the academia and the industry, professionals, standard developers, policy makers and practitioners to exchange ideas. The conference covered fundamentals on wireless, high-speed, mobile and Ad hoc networks, security, policy based systems and education systems. Topics targeted design, implementation, testing, use cases, tools, and lessons learnt for such networks and systems

The conference had the following tracks:

- WINET: Wireless networks
- HSNET: High speed networks
- SENET: Sensor networks
- MHNET: Mobile and Ad hoc networks
- VENET: Vehicular networks
- RFID: Radio-frequency identification systems
- SESYS: Security systems
- MCSYS: Multimedia communications systems
- POSYS: Policy-based systems
- PESYS: Pervasive education system

We welcomed technical papers presenting research and practical results, position papers addressing the pros and cons of specific proposals, such as those being discussed in the standard forums or in industry consortiums, survey papers addressing the key problems and solutions on any of the above topics, short papers on work in progress, and panel proposals.

We take here the opportunity to warmly thank all the members of the ICSNC 2011 technical program committee as well as the numerous reviewers. The creation of such a broad and high quality conference program would not have been possible without their involvement. We also kindly thank all the authors that dedicated much of their time and efforts to contribute to the ICSNC 2011. We truly believe that thanks to all these efforts, the final conference program consists of top quality contributions.

This event could also not have been a reality without the support of many individuals, organizations and sponsors. We also gratefully thank the members of the ICSNC 2011 organizing committee for their help in handling the logistics and for their work that is making this professional meeting a success. We gratefully appreciate to the technical program committee co-chairs that contributed to identify the appropriate groups to submit contributions.

We hope the ICSNC 2011 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress in networking and systems communications research.

We hope Barcelona provided a pleasant environment during the conference and everyone saved some time for exploring this beautiful city.

ICSNC 2011 Chairs

Advisory Chairs
Eugen Borcoci, University Politehnica of Bucarest, Romania
Sathiamoorthy Manoharan, University of Auckland, New Zealand
Reijo Savola, VTT, Finland
Leon Reznik, Rochester Institute of Technology, USA
Masashi Sugano, Osaka Prefecture University, Japan
Zoubir Mammeri, IRIT, France

Research Institute Liaison Chairs
Song Lin, Yahoo! Labs / Yahoo Inc. - Sunnyvale, USA
Habtamu Abie, Norwegian Computing Center - Oslo, Norway

Industry/Research Chairs
Rolf Oppliger, eSECURITY Technologies - Guemligen, Switzerland
Jeffrey Abell, General Motors Corporation, USA
Christopher Nguyen, Intel Corp., USA
Javier Ibanez-Guzman, RENAULT S.A.S. / Technocentre RENAULT - Guyancourt, France

Special Area Chairs

Mobility / vehicular
Maode Ma, Nanyang Technology University, Singapore

Pervasive education
Maiga Chang, Athabasca University, Canada

ICSNC 2011

Committee

ICSNC Advisory Chairs

Eugen Borcoci, University Politehnica of Bucarest, Romania
Sathiamoorthy Manoharan, University of Auckland, New Zealand
Reijo Savola, VTT, Finland
Leon Reznik, Rochester Institute of Technology, USA
Masashi Sugano, Osaka Prefecture University, Japan
Zoubir Mammeri, IRIT, France

ICSNC 2011 Research Institute Liaison Chairs

Song Lin, Yahoo! Labs / Yahoo Inc. - Sunnyvale, USA
Habtamu Abie, Norwegian Computing Center - Oslo, Norway

ICSNC 2011 Industry/Research Chairs

Rolf Oppliger, eSECURITY Technologies - Guemligen, Switzerland
Jeffrey Abell, General Motors Corporation, USA
Christopher Nguyen, Intel Corp., USA
Javier Ibanez-Guzman, RENAULT S.A.S. / Technocentre RENAULT - Guyancourt, France

ICSNC 2011 Special Area Chairs

Mobility / vehicular
Maode Ma, Nanyang Technology University, Singapore

Pervasive education
Maiga Chang, Athabasca University, Canada

ICSNC 2011 Technical Program Committee

Habtamu Abie, Norwegian Computing Center - Oslo, Norway
João Afonso , FCCN - National Foundation for Scientific Computing, Lisbon, Portugal
Mohammad Al Saad, Freie Universität Berlin, Germany
Jose Maria Alcaraz Calero, University of Murcia, Spania
Sultan Aljahdali, Taif University, Saudi Arabia
Juan Antonio Cordero. INRIA Saclay, France
Abdullahi Arabo, Liverpool John Moores University, UK
Shin'ichi Arakawa, Osaka University, Japan
Mladen Berekovic, Technische Universität Carolo-Wilhelmina zu Braunschweig, Germany
David Bernstein, Huawei Technologies, Ltd., USA
Robert Bestak, Czech Technical University in Prague, Czech Republic
Carlo Blundo, Università di Salerno - Fisciano, Italy

Antti Lahtela, University of Eastern Finland, Finland
Wolfgang Leister, Norsk Regnesentral (Norwegian Computing Center), Norway
Tayeb Lemlouma, IRISA / IUT of Lannion (University of Rennes 1), France
Jian Li, IBM Research in Austin, USA
Yan Li, Conviva, Inc. - San Mateo, USA
Yaohang Li, Old Dominion University, USA
Song Lin, Google, Inc., USA
Wei-Ming Lin, University of Texas at San Antonio, USA
Edmo Lopes Filho, Algar Telecom, Brazil
Eugene Lutton, University of Newcastle - Callaghan, Australia
Maode Ma, Nanyang Technology University, Singapore
Christian Maciocco, Intel Corporation, USA
Zoubir Mammeri, IRIT, France
Herwig Mannaert, University of Antwerp, Belgium
Sathiamoorthy Manoharan, University of Auckland, New Zealand
Gregorio Martinez, University of Murcia, Spain
Noriharu Miyaho, Tokyo Denki University, Japan
Karol Molnár, Brno University of Technology, Czech Republic
Mohammad Mostafizur Rahman Mozumdar, Univeristy of California at Berkeley, USA
Christopher Nguyen, Intel Corp., USA
Gabriele Oligeri, ISTI - CNR - Pisa, Italy
Rolf Oppliger, eSECURITY Technologies - Guemligen, Switzerland
Péter Orosz, University of Debrecen, Hungary
Gerard Parr, University of Ulster-Coleraine, Northern Ireland, UK
Ioannis Pefkianakis, University of California Los Angeles (UCLA), USA
Dennis Pfisterer, Universität zu Lübeck, Germany
Przemyslaw Rafal Pochec, University of New Brunswick - Fredericton, Canada
Victor Ramos, UAM-Iztapalapa, Mexico
Nicolas Repp, TU-Darmstadt, Germany
Leon Reznik, Rochester Institute of Technology, USA
Joel Rodrigues, University of Beira Interior, Portugal
Javier Rubio-Loyola, CINVESTAV, Mexico
Carol Savill-Smith, Technology for Learning LSN - London, UK
Reijo Savola, VTT, Finland
Marialisa Scatà, University of Catania, Italy
Gonzalos Seco Granados, Universitat Autònoma de Barcelona, Spain
Valentin Sgarciu, Politechncia University of Bucharest, Romania
Axel Sikora, Baden-Wuerttemberg Cooperative State University - Loerrach, Germany
Adão Silva, University of Aveiro / Institute of Telecommunications, Portugal
Idris Skloul Ibrahim, Heriot-Watt University - Edinburgh, UK
Weilian Su, Naval Postgraduate School - Monterey, USA
Martin Suchara, Princeton University, USA
Masashi Sugano, Osaka Prefecture University, Japan
Jani Suomalainen, VTT Technical Research Centre of Finland, Finland
Ted Szymanski, McMaster University - Hamilton, Canada
Stephanie Teufel, University of Fribourg, Switzerland

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Improving Spectral Efficiency of Spread Spectrum Systems Under Peak Load Network Conditions

Moses E. Ekpenyong
Informatics Forum
University of Edinburgh
EH8 9AB, Edinburgh
e-mail: mosesekpenyong@gmail.com

Joseph Isabona
Department of Basic Sciences
Benson Idahosa University
PMB. 1100, Benin City, Benin, Nigeria
e-mail: josabone@yahoo.com

Abstract— **In this contribution, we study the spectral efficiency performance of spread spectrum networks, where the networks are generalized to consider the frequency reuse factor and arbitrary processing gain resulting from in-cell interference, which adds undue penalties in the form of network cost. We observed that interference cost generates an increase in the received efficiency relative to frequency division multiple access (FDMA), weighted against a reduction in the signal requirement resulting from using the code division multiple access (CDMA) network. In particular, we focus on spectral efficiency optimization by studying realistic FDMA and CDMA networks operating in Nigeria. Performance models for both case studies are also proposed and simulated using observed data means as model predictors. We discovered that bandwidth effects of channel coding, modulation and spread spectrum do have impact on the spectral efficiency and the received power by all users under peak load conditions, thus necessitating the need for efficient coding and modulation and rate adaptation techniques as feasible solutions for improving channel capacity and efficiency of the scarce radio spectrum.**

Keywords-Frequency reuse; interference suppression; coding and modulation; spread spectrum; spectral efficiency.

I. INTRODUCTION

The available radio spectrum for wireless data services and systems is extremely scarce, while the demand for these services is growing at a rapid pace [1]. Spectral efficiency is therefore of primary concern in the design of future wireless data communication systems. This efficiency is partly achieved by cellular systems that exploit power "fall-off" of spatially distributed signals that reuse (or share) the same frequency channel across the propagation environment (i.e., at various distances or locations). However, while frequency reuse provides more efficient use of the limited available spectrum, it also introduces unavoidable co-channel interference [2-7], which ultimately determines the Bit Error rates (BERs) available to each user. Another technique for increasing spectral efficiency is the use of multilevel quadratic amplitude modulation (M-QAM). This technique increases the link spectral efficiency by sending multiple bits per symbol [8]. However, wireless channels are subjected to severe propagation impairment which results in a serious degradation of the link carrier-to-noise ratio (CNR). Even if efficient fading compensation techniques are used, multilevel schemes will require higher power level than binary modulations for a specified BER. Therefore to keep the co-channel interference at an acceptable level, it becomes necessary to increase the frequency-reuse distance (or equivalently the cluster size), which eventually leads to a lower system spectral efficiency.

Previous studies on system spectral efficiency for cellular systems assumed constant and equal data rate for all users, regardless of interference conditions and channel quality [3-9]. Then, spectral efficiency calculation was based on a criterion introduced in [10] and defined as the ratio of the carried traffic per cell (in Erlangs) to the product of the total system bandwidth and area supported by a base station. This criterion is not suitable for data systems, as Erlangs are just a measure of traffic loading rather than throughput intensity. A more pertinent measure of spectral efficiency in cellular data systems is the total throughput. This problem has been addressed in [9]. They show that there exists a tradeoff between the system and the link spectral efficiency, which is also confirmed in [11], who claim that 4-QAM is the optimum multilevel modulation for high-capacity cellular systems, therefore opting for higher modulation level will reduce the system's spectral efficiency. This is essentially due to the fact that fixed modulation systems designed relative to the CNR produces better link and system spectral efficiencies. The basic concept of variable-rate transmission is real-time balancing of the link budget through adaptive variation of the symbol time duration, constellation size, coding rate/scheme, or any combination of these [12-13]. Thus, without wasting much power or increasing co-channel interference and sacrificing BER, this approach provides a much higher average spectral efficiency that takes advantage of the "time-varying" nature of wireless channel and interference conditions. Under favourable interference/channel conditions, the system could transmit at high speeds and respond to an increase in interference and/or channel degradation through a smooth reduction of their data throughput. Since buffering/delay of the input data may be required in this process, adaptive system techniques are required for applications which are to some extent bursty in nature and are therefore best suited for high-speed wireless data transmission.

 ISBN: 978-1-61208-166-3

II. RESEARCH BACKGROUND

Research works on spectral efficiency has progressed steadily over the years. Most of the researches carried out in literature concentrate on analytical approaches. Abrardo, Benelli, Giambene and Sennati [14] consider a power controlled CDMA implemented by varying the transmitted power of mobile units such that an adequate signal-to-interference ratio (SIR) is maintained at the receiver for each transmission. They focus on closed-loop power control, in which the estimates are formed at the base station (BS) receiver, and commands to adjust the transmitted power are sent from the BS to the mobile unit. The effect of closed-loop power control on system performance is considered in [15-17] for receivers that employ rake reception. They focus on a CDMA system with specified chip rate, but they do not address the difference in multipath resolution capability obtained with different chip rates. Bonneau, Debbah and Altman [18], Bonneau, Debbah, Altman and Caire [19] analyze the performance of uplink and downlink CDMA system respectively, with random spreading and multi-cell interference. They provide a useful framework aimed at determining the base station coverage for wireless flat fading channels with very dense networks. Considering three receiver structure, they use asymptotic arguments to obtain analytical expressions of the spectral efficiency with a simple expression that determines the network capacity based on few parameters. A general analytical framework quantifying the area spectral efficiency (ASE) of cellular systems with variable rate transmission is well treated in [20]. They derive expressions for the ASE as a function of the reuse distance for the best and worse case interference configuration and use Monte Carlo simulations to estimate the ASE for average interference conditions for partially and fully loaded cellular systems. Significant amount of work has been done on improving the spectral efficiency of wireless communication systems. The Enhanced Data Rates for GSM and TDMA/136 Evolution (EDGE) technology [21] provides significantly higher user bit rates and spectral efficiency.

Recently, Isabona, et al. [22] have improved on the existing wideband CDMA (WCDMA) user capacity expressions in single and multi cell environments for the uplink, they integrate new parameters that affect the system. They also studied and reported the effect of multi-user detection and adaptive antenna gain on users' capacity in the presence of loading, voice activity, sectorization, power control and bandwidth efficiency.

The current work takes a practical look at second generation (2G) and third generation (3G) systems. For the sake of completeness, a study of the spectral efficiency of these systems is made. A performance model is then derived for the two network categories using a generic methodology, suitable for both systems and verified through computer simulations. The research is advantageous because it will inform network operators on best practices and how to deal with network performance issues as well as enhance collaboration between academics and the industries.

III. MATERIALS AND METHOD

In this research, we identified two classes of networks: the FDMA and CDMA networks, for the purpose of collecting empirical data. These networks were the *Airtel Nigeria* and *Globacomm Nigeria*. For each network case, the Erlang-capacity data were obtained over a period of two weeks and the spectral efficiency computed. The processing gain for each network were acquired from the field and used for the computation. The spectral efficiency methodology implemented in this paper is summarized in Fig. 1.

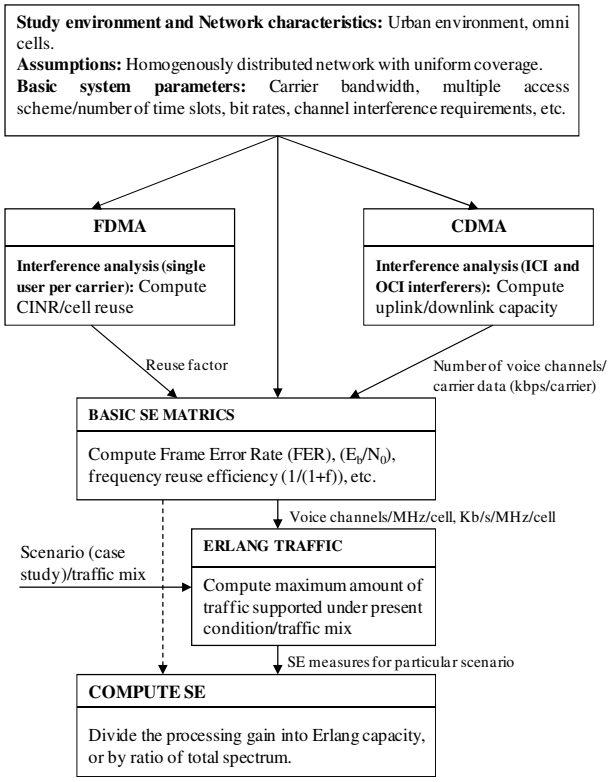


Figure 1. Spectral efficiency methodology

IV. SYSTEM MODEL

The efficient use of the radio frequency (RF) spectrum serves as a fundamental design goal for cellular radio network engineers. The more calls that can be supported by a base station at an acceptable quality, the less base stations that are required to support a given subscriber's demand. Since there is large fixed capital costs associated with base stations deployment, it becomes desirable to maximize the number of subscribers each base station supports. The maximum number of users supported by each base station per CDMA carrier is given as [16]:

 ISBN: 978-1-61208-166-3

$$n = \frac{W_s}{R_b} F\left(\frac{1}{\gamma}\left(1-\frac{1}{r}\right)\right) \quad (1)$$

where

W_s is the RF spread bandwidth

R_b is the data rate

$\gamma = \frac{E_b}{I_0 + N_0}$ represents the signal-to-noise (SNR) per bit

$r = \frac{I_0 + N_0}{N_0}$ is the rise above thermal

$F = \frac{1}{(I+f)}$ is the frequency reuse efficiency

Equation (1) applies to CDMA networks such as IS-95 that are non-cooperative, in the sense that they do not exploit interference through multi-user detection. This equation has historically been associated with CDMA networks when interference rises to a level where users cannot compensate for less than the desired quality of service (QoS), by increasing their transmit power. Such a condition establishes a maximum on the number of users supported for a given QoS objective and in theory, a pole exists in the transmit power required to meet the expected QoS. Equation (1) holds when all users at the various base stations possess the required $E_b/(I_0 + N_0)$ needed to meet a QoS objective such as the mean opinion score (MOS) or a frame error rate (FER). This is a pole condition, since any additional user would create interference that could not be compensated for through further increase in the transmitted power. Various forms of (1) can be derived [16][23][24] by assuming that the number of interfering users in the serving cell that creates the in-cell interference (ICI) power is the same as the number of users in the other base stations that creates the out-of-cell interference (OCI) power. This assumption counts the desired signal as interference, which becomes significant for lower processing gains. Disregarding this assumption, the number of users for arbitrary processing gains and frequency reuse can be established. The following generalization considers the impact of allowing and prohibiting in-cell-interference in cellular systems design.

A. *Speading with In-cell Interference: A CDMA Case*

Let us consider an idealized hexagonal lattice of base stations where the number of users supported by each base station is increased uniformly throughout the network, until the interference-and-noise power is just at a level required to meet a given QoS objective. At this point, the network ideally blocks additional calls due to QoS considerations. Blocking due to resource limitation (a traditional blocking mechanism that applies to any cellular technology) is assumed here to be insignificant. A bit stream after source coding of R_b bits per second, expands in bandwidth due to modulation, with a spectral efficiency of modulation η. A spreading sequence of bandwidth W, increases the bandwidth before spreading B, by a spreading gain of:

$$G = \frac{W}{B} \quad (2)$$

The positive bandwidth of a RF signal is doubled due to spectrum shift. Tradeoffs arising from using different combinations of spreading, modulation, and coding for a fixed bandwidth and spectrum efficiency constitute a decade of research [25-27]. Exploring these tradeoffs necessitate the consideration of not only the required SNR per bit $(E_b/(I_0 + N_0))$ for a given QoS demand, but also the effect that the bandwidth expansion/contraction has on the average received $E_b/(I_0 + N_0)$ when the number of users is held constant. The maximum number of users supported by the network is derived when all of the users are exactly satisfying the requirement, since the addition of users beyond this maximum cannot be accomplished without degrading the received $E_b/(I_0 + N_0)$ and the corresponding QoS.

The total number of users, n_T, given an available spectrum (or bandwidth), each base station can accommodate is:

$$n_T = \frac{W_A}{KW_s} \quad (3)$$

where

W_A is the bandwidth available to the cellular operator.

K is the cluster size

The number of users per carrier can be obtained directly by writing the carrier-to-interference and noise power ratio (CINR) of each user, assuming that the interference realistically spreads and dispreads, as:

$$\Gamma = \frac{Carrier\ Power}{ICI + OCI + Noise} = \frac{C}{\frac{C(n-1)d}{G} + \frac{nfCd}{G} + N} \quad (4)$$

where

C is the received carrier power of each user

$N \equiv (N_0 B)$ is the noise power of the dispread signal bandwidth

f is the total interference from an out-of-cell user (other cells) normalized to the carrier power (loading factor).

G is the spreading gain

d is the interference reduction due to the voice duty cycle (voice activity factor).

The processing gain G, defined as W_s/R_b can differ from the amount of bandwidth increase resulting from direct spread sequence and thus calls for the introduction of a gain term. So, before channel coding and modulation,

 ISBN: 978-1-61208-166-3

$$G = \frac{W}{R_b} \tag{5}$$

After channel coding,

$$G = \frac{WR_c\eta}{R_b} \tag{6}$$

where

R_c is the coding rate

η is the modulation frequency

Solving for *W*, we have,

$$W = \frac{GR_b}{R_c\eta} \tag{7}$$

Substituting *W* in (7) into (2) and solving for B, we arrive at

$$B = \frac{R_b}{R_c\eta} \tag{8}$$

Now, (4) can be represented in the form: $\frac{E_b}{(I_0 + N_0)}$, by utilizing the bandwidth relationship in (7) for $R_b/B = \eta R_c$ (8), thus,

$$\gamma \equiv \frac{E_b}{I_0 + N_0} = \frac{1}{\frac{n-1+nf\eta R_c d}{G} + \frac{N_0}{E_b}} \tag{9}$$

Solving for *n* in (9) and substituting same into (1) results in:

$$n_T = \frac{W_A GF}{\eta R_c K W_s d}\left(\frac{1}{\gamma}\left(1-\frac{1}{r}\right)+\frac{d\eta R_c}{G}\right) \tag{10}$$

but $F = \frac{1}{1+f}$, so, we rewrite equation (10) as:

$$n_T = \frac{W_A\, G}{\eta R_c K W_s d(1+f)}\left(\frac{1}{\gamma}\left(1-\frac{1}{r}\right)+\frac{d\eta R_c}{G}\right) \tag{11}$$

The spectral efficiency (SE) [8][28] of a system is defined as:

SE = network capacity × (processing gain)$^{-1}$ b/s/Hz (12)

so,

$$SE = \frac{n_T}{G} = \frac{\frac{W_A G}{\eta R_c K W_s d(1+f)}\left(\frac{1}{\gamma}\left(1-\frac{1}{r}\right)+\frac{d\eta R_c}{G}\right)}{G}$$

$$= \frac{W_A}{\eta R_c K W_s d(1+f)}\left(\frac{1}{\gamma}\left(1-\frac{1}{r}\right)+\frac{d\eta R_c}{G}\right) \tag{13}$$

B. Spreading Without In-cell Interference: A FDMA Case

The following equation is a lower limit on (3) that considers only a single user per carrier in each base station, i.e.,

$$n_T = \frac{W_A}{KW_s} = \frac{W_A\eta R_c}{2GKR_b} \tag{14}$$

This is a Frequency Division Multiple Access (FDMA) limiting case that does not permit same channel frequency reuse within a base station. When $W_s = 2B$, the spreading gain is unity and the lower limit results in the conventional cellular FDMA, with a frequency reuse factor K. For non-unity spreading gains, $E_b/(I_0 + N_0)$ can be increased at the cost of a reduction in the number of users, supported by increase in the spreading gain. The spreading gain from (2), when n = 1 is

$$G_{FDMA} = \frac{r\gamma R_c\eta d}{(r-1)}\, f > 1 \tag{15}$$

Substituting (15) into (14), gives the total number of users supported when spread spectrum is used with FDMA and a frequency reuse strategy prohibiting ICI, as:

$$n_T = \frac{1}{\gamma}\left(1-\frac{1}{r}\right)\frac{W_A}{2KfdR_b} \tag{16}$$

But

$$R_b = \eta R_c \frac{W_s}{2}$$

Thus,

$$n_T = \frac{1}{\gamma}\left(1-\frac{1}{r}\right)\frac{W_A}{KW_s fd\eta R_c} \tag{17}$$

and

$$SE = \frac{\frac{1}{\gamma}\left(1-\frac{1}{r}\right)\frac{W_A}{KW_s fd\eta R_c}}{G} = \frac{1}{\gamma}\left(1-\frac{1}{r}\right)\frac{W_A}{GKW_s fd\eta R_c} \tag{18}$$

V. ANALYSIS OF REALISTIC CDMA AND FDMA SYSTEMS

It is expected that current telecommunication technologies will give high system performance, i.e., the performance capabilities of CDMA systems should be higher than that of FDMA systems, because they posses the ability to offer high speed data transfers and video/multimedia communications. This also implies that the higher the spectral efficiency, the better the system. As can be seen in Fig. 2, the CDMA system under study has a higher spectral efficiency than the FDMA system, but the spectral efficiency in the CDMA system has an inconsistent trend compared to that of FDMA system, which inconsistent pattern can easily be predicted. We observed that the main reason behind the unstable nature of the system lies in the initial design concept, where more flexibility is emphasized

 ISBN: 978-1-61208-166-3

thus allowing the scheduling scheme to depend largely on the operator's choice.

The observed effect is largely due to the high interference/traffic and inefficient frequency reuse technique (in CDMA) noticed during the study period. To provide a coherent pattern for model prediction, we fit trend line equations to the average spectral efficiency plots in Fig. 3. The computed coefficient of determination (R^2) for both networks show that in the CDMA system under study, spectral efficiency is not significantly influenced by the number of base stations, but on some other factors/parameters that could be optimized at the base stations to service the increased systems capacity. Specifically, optimization should include techniques that mitigate multi-path fading/shadowing, a major contributor to co-channel interference. The number of base stations tends to have diminutive influence on the spectral efficiency in the FDMA system. This is due to the fixed radio spectrum at each base station. The fitted trend line is also useful for the prediction of new empirical results.

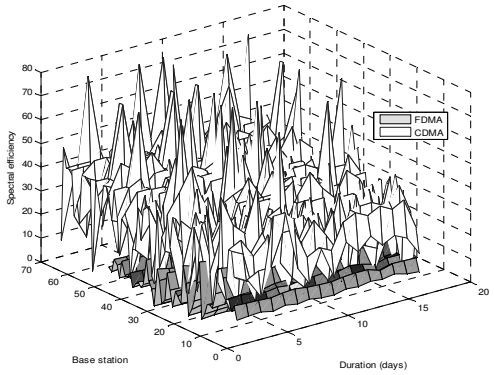


Figure 2. Spectral efficiency analysis for observed FDMA and CDMA systems

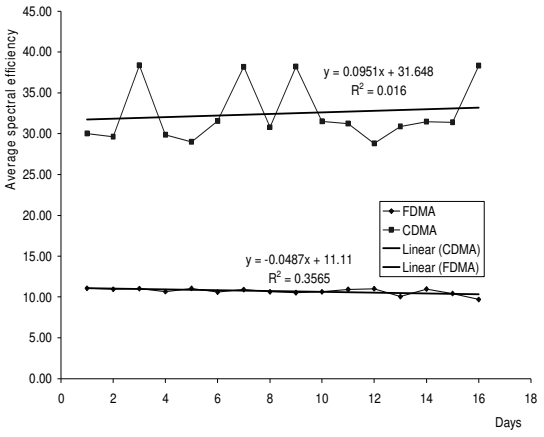


Figure 3. A graph of Spectral efficiency vs. duration for observed FDMA and CDMA systems

Further findings reveal that mobile operators/field engineers have little or no knowledge on performance measures and problem solving techniques. This is largely due to the fact that in Nigeria, most of these operators are updating their services from 2G to 3G technologies and as a result tend to carry the idea of frequency bound technology, which does not suffer much interference into a frequency-reuse technology, which is interference-prone. However, detail interactions show that more interest seems to be placed on profit making and ad-hoc maintenance/services, rather than problem solving and service improvements.

VI. SIMULATION AND DISCUSSION OF RESULTS

Sample data from the field were used to judge the performance of the existing system. Simulation runs were carried out to evaluate the performance of both systems using the proposed system models. The input parameters and their respective values used during the simulation are shown in Table 1. These parameters on the average gave optimum performance and enabled us to report on the systems performance. Sample outputs were generated in the form of graphs using MATrixLABoratory plot commands. The graphs which predict the systems' behaviour and important results obtained from the simulation are discussed.

TABLE I. SIMULATION MODELS PARAMETERS

Parameter	Value
SNR (γ)	1-10dB
Rise above thermal (r)	3
Frequency reuse factor (f)	0.74
Interference reduction due to voice duty cycle (d)	0.58
Radio frequency spread bandwidth ($W_A = W_s$)	FDMA = 11.25, CDMA = 12.28
Processing gain (G)	FDMA = 39, CDMA = 43
Cluster size	FDMA = 1, CDMA = 3
Modulation efficiency	2, 3
Coding rate (R_c)	0.5, 0.75

The interference limited forms for FDMA and CDMA systems are plotted in Fig. 4 and Fig. 6 with joint coding and modulation modeling parameters for system performance improvement. The plots show that increase in the number of users degrades the link reliability, represented by the signal-to-noise ratio (SNR). The results from these plots also reveal that coding and modulation can be jointly modeled to improve the system performance. This technique overcomes the adverse effects of frequency selective fading channels and offers high spectral efficiency. Although the influence of higher order modulation on the spectral efficiency of multi inter-cell systems is similar (in performance) to single cell systems [29], interference

 ISBN: 978-1-61208-166-3

remains a notorious obstacle to attain wide area coverage and high spectral efficiency in cellular systems. In general, interference from adjacent cells significantly reduces the spectral efficiency for discrete modulation efficiency, calling for an increase in the constellation size to obtain a high spectral efficiency for low noise region. As earlier observed, CDMA systems are interference-limited rather than noise-limited. This defect however results in negative consequences such as: (i) inter-channel interference (ICI) and inter-symbol interference (ISI), (ii) BER exceeding the target E_b/N_0, requiring increased signal strength and SINR, reduced traffic-load and/or reduced bit-rate to maintain the network QoS, (iii) increased transmit power due to neighboring users requesting more power to contend with the increased interference. As a result, it is important to maximise the network capacity by ensuring that each user transmits with a required minimum power such that the interference caused by other users within the network is minimised. With this the base station will have the capacity to accommodate more users. This results in a second-order effect where each base station lowers the transmit power for interference cancellation-enabled users, with the aim of mitigating noise on all mutually interfering sectors and leads to further reduction in the network transmit power.

In the uplink, the spectral efficiency of the systems under study decreased with the number of users. This is primarily due to the following reasons: (i) more power is occupied to transmit the uplink pilot signal, (ii) more resource is used to maintain the minimal transmit rate for each user, as a result, each user suffer severe interference. Also, we have observed during simulation that the rise above thermal (r) and its outage rate are two important performance measures that indicate the degree of stability of the system. These matrices could as well be optimised to ensure users satisfaction in practical systems.

Figs. 5 and 7 show the plots of spectral efficiency (SE) versus SNR with coding and modulation as performance improvement parameters for FDMA and CDMA systems respectively. These graphs show that as the user density increases, the radio resources to support them gets exhausted. In general, systems with higher SE provides more data services and support more users at a given grade of service (GoS) before experiencing resource exhaustion. The impact of this on the network performance is that, as the traffic load increases, the total base station transmit power also increases, because users require more transmit power from the base station to maintain stability in dense interference. This effect causes a major decrease in the coverage probability and thus degrades the network performance, resulting in users experiencing a greater number of dropped and blocked calls.

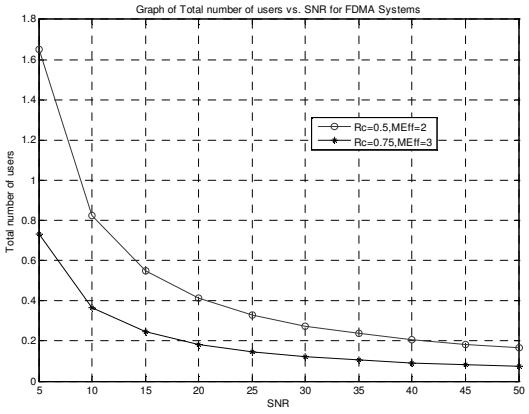


Figure 4. Graph of total number of users vs. SNR for FDMA systems

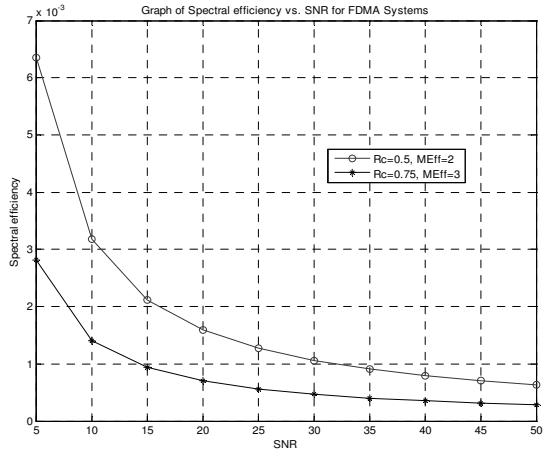


Figure 5. Graph of spectral efficiency vs. SNR for FDMA systems

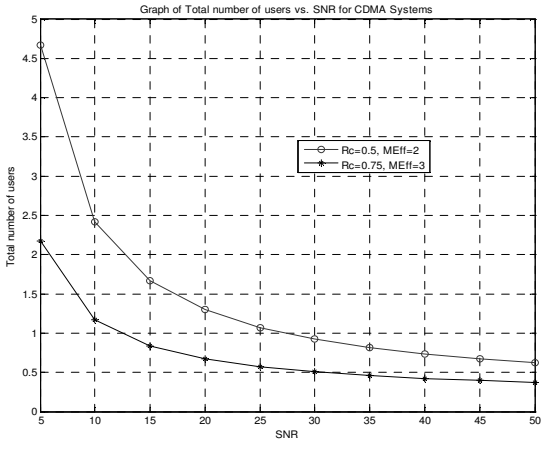


Figure 6. Graph of Total number of users vs. SNR for CDMA systems

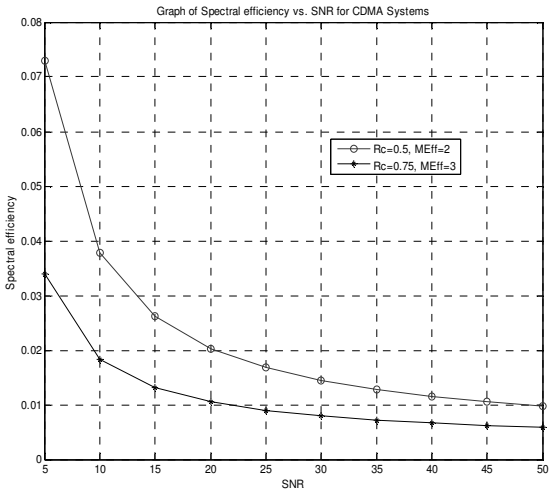


Figure 7. Graph of spectral efficiency vs. SNR for CDMA systems

In addition, high-power transmitters will generally offer reduced capacity and network efficiency to adjacent channel users. This problem of power limitation usually occurs in urban areas, where the spectrum is likely to be more congested, but is much less of a problem in rural areas, that sparsely use the spectrum. To address this problem, transmitted power levels in urban environments should be lowered and increased in rural environments. Power can be reduced through the deployment of low-power transmission networks, such as those currently used in cities by cellular and PCS service providers. With more transmitters, the transmission capacity will increase. Power in rural areas can be increased by permitting even higher power levels. This could enable service to be provided in areas that can't be economically justified at the moment.

VII. CONCLUSION AND FUTURE WORK

Cellular technology is a fascinating and fast growing area of research in the communication world, where more researches will be of enormous benefits, considering the increasing attention it has attracted globally. We have studied the spectral efficiency optimization in spreading spectrum of two different networks, the CDMA and FDMA network respectively. We adopted a practical approach and have provided best practices for network providers. Results obtained show that bandwidth effects of channel coding, modulation and spread spectrum can significantly impact on the spectral efficiency and the received interference of CDMA systems. However, the spectral efficiency of the system drops depending on the interference level. This fact and the much demanding implementation of higher order modulation schemes and interference cancellation techniques [30] should be considered during system design.

We have discovered that in Nigeria for instance, issues of spectral efficiency management and enactment of the right policy to accommodate the growing spectrum demands in both private and public sectors is yet to be effectively addressed. This is due to the unplanned/inefficient deployments of some communication services, congested cities and poor topologies. However, the following are helpful hints a commission/regulatory body can adopt to improve spectral efficiency: (i) access improvement through power, time, frequency, bandwidth, and space; (ii) flexible use of the spectrum (i.e., unhindered users/uses permission); (iii) encouraging efficient spectrum use; (iv) combination of technically-compatible systems; (v) adjusting regulations inline with technological improvements.

To create an enabling environment for future research work and improvements, a holistic survey of the current spectral efficiency performance is important, as this will reveal the level of inefficiency in the existing system and create room for a more structured approach and effective state-of-the-art implementation plan. This we intend to pursue on the acquisition of research funding.

This contribution has enormous potentials as follows:

- It will impact on the telecommunications industry and inform network operators on how to improve on the performance of their system
- It presents a practical approach to spectral efficiency analysis
- It will bootstrap further research and development in this area
- It will establish/strengthen collaboration between the academia and telecom industries
- It will advise network operators who are always afraid to release data to see the need for research partnership in order to improve their services

ACKNOWLEDGMENT

We are grateful to the field engineers of the *Airtel* and *Globacomm* Nigeria for their assistance during the data collection stage of this research.

REFERENCES

[1] K. Pahlavan and A. Lecesque, "Wireless data communications," IEEE Trans. on Commun., Invited Paper, vol. 82 (9), pp. 1398-1430, 1994.

[2] R. Muammar and S. Gupta, "Co-channel interference in high capacity mobile radio systems," IEEE Transactions on Communications, vol. 30(8), pp. 1973-1978, 1982.

[3] Y. Nagata and Y. Akaiwa, "Analysis for spectrum efficiency in single cell trunked and cellular mobile radio," IEEE Transactions on Vehicular Technology, vol. 36(3), pp. 100-113, 2006.

[4] R. Prasad and A. kegel, "Effects of Rician faded and lognormal shadowed signals on spectrum efficiency in microcellular radio," IEEE Transactions on Vehicular Technology, vol. 42(3), pp. 274-280, 2002.

[5] A. Abu-Dayya, "Outage probabilities of cellular mobile radio systems with multiple Nakagami interferers," IEEE Transactions on Vehicular Technology, vol. 40(4), pp. 757-768, 2002.

 ISBN: 978-1-61208-166-3

[6] Y. Yao and A. Sheikh, "Investigations in co-channel interference in microcellular mobile radio systems," IEEE Transactions on Vehicular Technology, vol. 41(2), pp. 114-123, 2002.
[7] R. Prasad and A. Kegel, "Improved assessment of interference limits in cellular radio performance" IEEE Transactions on Vehicular Technology, vol. 40(2), pp. 412-419, 2002.
[8] W. Webb and L. Hanzo, Modern Quadrature Amplitude Modulation, IEEE Press; 1994.
[9] R. Haas and J. Belfiore, "Spectrum efficiency limits in mobile cellular system," IEEE Transactions on Vehicular Technology, vol. 45(1), pp. 33-40, 1996.
[10] D. Hatfield, "Measure of spectral efficiency in land mobile radio," IEEE Transactions on Electromagnetic Compat, vol. EMC(19), pp. 266-268, 1997.
[11] N. Morinaga, M. Yokoyama M and S. Sampei, ". Intelligent radio communication techniques for advanced wireless communication systems," IEICE Transactions on Communication, vol. E79(B), pp. 214-221, 1996.
[12] T. Ue, S. Sampei and N. Morinage, "Symbol rate and modulation level controlled adaptive modulation/ TDMA/TDD for personal communication system," IEEE Transactions on Communication, vol. E78(B), pp. 1117-1124, 1995.
[13] S. Chua and A. Goldsmith, "Variable rate variable-power M-QAM for fading channels," IEEE Transactions on Communications, vol. 45(10), pp. 1218-1230, 1997.
[14] A. Abrardo, G. Benelli, G. Giambene and D. Sennati, "An analytical approach for closed-loop power control error estimations in CDMA cellular systems," Proceedings of IEEE ICC Conference. Jun 18. New Orleans, LA. 2000; 3: 1492-1496.
[15] F. Fahri and D. Astharini. Feedback Delay Effect on the CDMA Closed loop Power Control. Second IEEE International Conference on Advances in Computing, Control and Telecommunication Technologies (ACT), Dec. 2-3. Jakarta. 2010; pp. 64-68.
[16] A. Viterbi and A. Viterbi, "Erlang capacity of a power controlled CDMA system," IEEE Journal on Selected Areas in Communications, vol. 11(6), pp. 892-900, 2002.
[17] S. Ariyavisitakul and I. Chang. Signal and interference statistics of a CDMA system with feedback power control, IEEE Transactions on Communication, vol. 41, pp. 1626-1634, 1993.
[18] N. Bonneau, Debbah M. and E. Altman, "Spectral efficiency of CDMA downlink cellular networks with matched filter," EURASIP Journal on Wireless Communications and Networking, vol. 2006, pp. 1-10, 2006.
[19] N. Bonneau, M. Debbah, E. Altman and G. Caire, "Spectral efficiency of CDMA uplink cellular networks," Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Apr 7; Philadelphia, USA. 2005; vol. 5, pp. 821-824.
[20] M. Alouini and A. Goldsmith, "Area spectral efficiency of cellular systems with Nakagami multipath fading," Proceedings of IEEE International Conference on Communications. Jun. 8-12. Montreal, Que., 1997; 1, pp. 76-80.
[21] A. Furuskar, S. Mazur, F. Muller and H. Olofsson, "EDGE: Enhanced Data Rates for GSM and TDMA/136 Evolution," IEEE Personal Communications, vol. 6(3), pp. 56-66, 1999.
[22] J. Isabona, M. Ekpenyong and S. Azi, "Enhanced spectral utilization of 3G WCDMA-based FDD mode in the uplink transmission," Modern Applied Science, vol. 5(1), pp. 117-132, 2011.
[23] T. Rappaport. Wireless communications principle and practice, Prentice Hall; 1996.
[24] H. Xia. CDMA System design and deployment, in VTC '98 tutorial notes, Ottawa, ON, Canada; 1998.
[25] P. Malm and T. Masieng, "Optimum number of Signal Alternative in Mobile Cellular Systems," Proceedings of 48th IEEE Conference on Vehicular Technology. May 18-21, Ottawa, Ont, Canada. 1998; 2, pp. 944-948.
[26] K. Nikolai, K. Kammeyer and A. Dekorsky, "On the Bit Error Behaviour of Coded DS-DMA with Various Modulation Techniques," Proceedings of IEEE 9th International Symposium on Personal Indoor and Mobile Radio Communications. Sep. 8-9. Boston, MA. 1998; 2, pp. 784-788.
[27] E. Biglieri, G. Caire and G. Taricco, "Coding and modulation under power constraint," IEEE Transactions on Personal Communications, vol. 5(3), pp. 32-39, 1998.
[28] S. Hosham and B. Hussein, "Performance enhancement of GSM cellular phone network using dynamic frequency hopping," Engineering and Technology, vol. 26(3), pp. 365-375, 2008.
[29] L. Milstein and D. Shilling, "The CDMA Overlay Concept," Proceedings of 4th IEEE International Symposium on Spread Spectrum Techniques and Applications, Sep. 22-25. Mainz, Germany. 1996; 2, pp. 476-480.
[30] Y. Gao, X. Zhang, Y. Jiang and J-W. Cho, "System Spectral Efficiency and Stability of 3G Networks: A Comparative Study," Proceedings of IEEE ICC 2009 Conference; Jun. 14-18; Dresden. 2009; pp. 1-6.

 ISBN: 978-1-61208-166-3

Uplink Power Control Based on an Evolutionary Algorithm with Associative Memory

Vladislav Vasilev[1], Vladimir Poulkov[2], Georgi Iliev[3]
Department of Telecommunications
Technical University of Sofia
Sofia, Bulgaria
E-mail: [1]doublevvinged@gmail.com;[2]vkp;[3]gli@tu-sofia.bg

***Abstract*—In the present paper, a new approach for uplink power control is proposed. The developed method is based on dividing the cell into sectors and applying an evolutionary algorithm approach of controlling the transmitted uplink power. Simulation experiments are presented demonstrating the control of transmitted power from the active cell sectors as the overall neighboring cells interference is kept below a predefined threshold. The major advantage of this approach is the random power allocation over active sectors which results in increased throughput and fair resource management.**

Keywords-evolutionary algorithms; long term evolution (LTE); dynamic uplink power control

I. INTRODUCTION

Over the years, Evolutionary Algorithms (EA) have attracted a lot of attention from different research areas because of their ability to solve complex optimization problems by imitating some aspects of natural evolution. In the context of biology, the evolution is considered as the change of one or several individual characteristics which are then transferred to the offspring. EA make use of different biological processes as reproduction, mutation, recombination and selection to find the optimal solution in a particular application. The solution candidates are considered as individuals belonging to a particular population while the environment is defined as a set of constraints to the optimization problem. As a rule, considerable computational resources are needed for EA simulation as the problem solution time is very sensitive to the specific model and its parameters.

Basically, two groups of optimization problems are solved using EA. First one is formed by a variety of Stationary Optimization Problems (SOPs) where the problem is precisely defined in advance and remains fix over the time [1]. The second group is related to the field of dynamic optimization problems (DOPs) which are characterized with ever-changing environment [2]. Usually for SOPs the aim is to find quickly and precisely the optimal solution in the search space. However, for DOPs, where the environment is dynamic, in addition to the above mentioned aims an ability to track and adapt to the changing conditions is crucial and often is in conflict with the requirement for fastness and preciseness.

Following the existing examples of application areas for EA, in the present paper, we propose an EA to solve the problem of uplink power control in Long Term Evolution (LTE) wireless mobile networks. We consider this problem as DOP and utilize the intrinsic ability of EA to solve such kind of problems. At present, several methods for uplink power control are practically considered.

First one is a 3GPP specification and provides slow Open Loop Power Control (OLPC). The method is known as Fractional Power Control (FPC) that allows for full or partial compensation of slow path gain (path loss) and shadowing variations. The performance of FPC has been investigated intensively in [3] and [4]. The basic conclusion is that there is a trade-off between the overall cell throughput (overall spectral efficiency) and the outage cell throughput.

Second method is named Interference Based PC (IBPC) [5] and [6]. It is based on Closed Loop PC (CLPC) to adjust the user equipment (UE) power thus improving the system performance both from the overall and outage cell throughput perspective. The basic idea is that the power should be controlled to compensate for the generated interference to the system rather than the path gain (path loss). The result is that each user generates the same amount of interference. IBPC is very promising but still keeping the average cell throughput of the outage cell gain is less than 30 %.

Other methods are also suggested in the literature based on combining the above ones or applying game theoretical or cognitive approaches [7].

Despite all of the above mentioned approaches, the problem of uplink power control is still open in the context of throughput gain and fair resource allocation for users in the central and outage cell areas. Moreover in most of the cases these methods are analyzed assuming static conditions such as fixed bandwidth, balanced loads, evenly distributed users in the cell, etc. This is the motivation to try the application of EA to solve uplink power control problem considered as a typical DOP.

The reminder of the paper is organized as follows. Section II introduces details about some basic characteristics of EA. Section III presents the proposed EA for uplink power control (EA-UPC). The main results are presented in Section IV, and finally, the conclusions are summarized in Section V.

II. EVOLUTIONARY ALGORITHM WITH ASSOCIATIVE MEMORY

An EA can be divided into three major phases. First phase: a number of individuals exist in the environmental

 ISBN: 978-1-61208-166-3

plane. They interact between each other and with the environment. In the second phase, using a fitness function estimation, the most successful individuals are chosen. Their characteristics are combined, processed and transformed according to specific predefined rules. In the third phase (selected evolved individuals), the most successful individuals are taken back to the environment. This process of evolution is illustrated in Fig. 1.

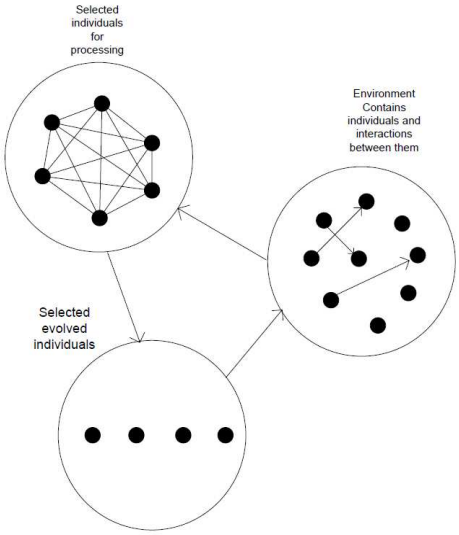


Figure 1. The main phases of an EA.

If we consider the evolutionary process from the perspective of one individual (G) its behavior can be characterized by several specific features:

1. Random behavior in the process of finding solutions and nondeterministic state;
2. Every interaction, even self-interaction, generates reaction which can not always be estimated or measured;
3. Each evolved individual G has found at least one solution as a result of the interaction;
4. There are a finite number of individual states;
5. There are an infinite number of interactions with the environment but their intensiveness is finite.

An example of evolutionary process and solution finding is illustrated in Fig. 2 for one individual (G). In order to prevent information loss for the EA, it is necessary the state "S", which is responsible for solution finding, to have access to the results from each generation "G" on the evolutionary path. In addition to the decision which available tools (filters) to be used, S generates also a set of possible states (T) which can be tested along the path. Therefore the process of solution finding evolves by evolving the states (T).

The following three equations represent the main features of an evolutionary process and solution finding.

$$S = \sum\{G\} + \sum\{T\} \quad (1)$$

$$\deg(S) = |\{G\}| + |\{T\}| \quad (2)$$

where $\deg(S)$ is the degree of vertex S, $|\{G\}|$ is the number of tested generations and $|\{T\}|$ is the number of evolved tools.

$$f(S(T)) = extremum\ (f) \quad (3)$$

Eq. 3 means that using a particular tool T, EA finds a local extremum for the environmental fitness/cost function.

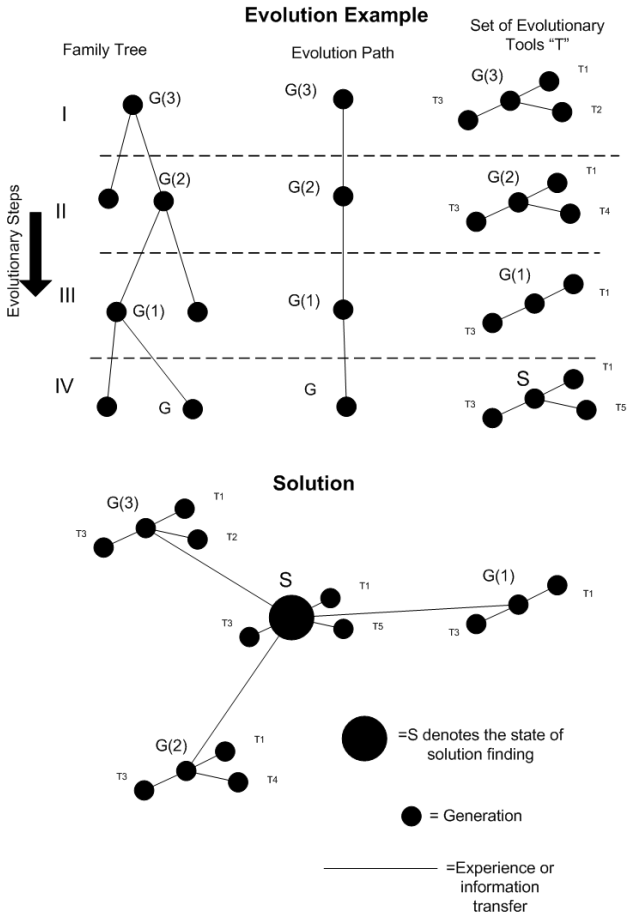


Figure 2. Example of evolutionary process and solution finding.

Usually, during the implementation of an EA, Eqs. 1 and 2 are solved, the current solutions are temporary buffered, and the best are placed in an associative memory. As seen in Fig. 2, state S provides information or attempts to describe the environment using the tools of the individual. The final solution is random and the probability to find a better

 ISBN: 978-1-61208-166-3

individual/generation depends entirely on the ability of state S to deduct information from the previous generations.

III. UPLINK POWER CONTROL USING EA

In order to develop an EA for uplink power control, formulating the optimization problem is necessary first. We consider an example situation as presented in Fig. 3. A LTE cell with base station (BS) "B" is given. The neighboring cells are presented by their BSs – B1, B2, B3, B4, B5, B6. The cell is divided into sectors. The users located in each sector can transmit a signal with a total power of $p(i, j)$ and thus for every neighboring cell a maximum overall level of the interference, measured at its BS, is defined.

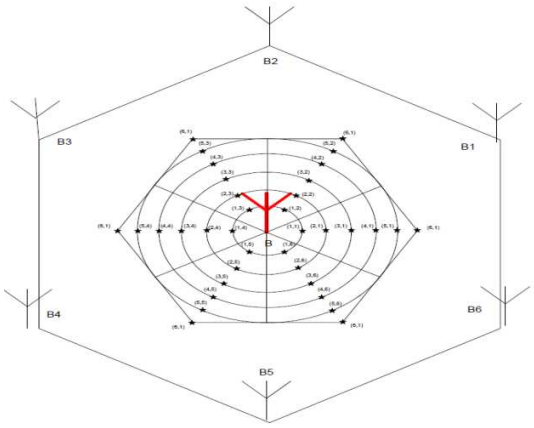


Figure 3. Cell division into sectors.

The interference vector $\vec{V}_{\Sigma}^{k}$ is a sum of the interference caused by each active (transmitting at that time) sector as shown in Fig.4. A sector is considered as active if the transmitted power is above a predefined threshold.

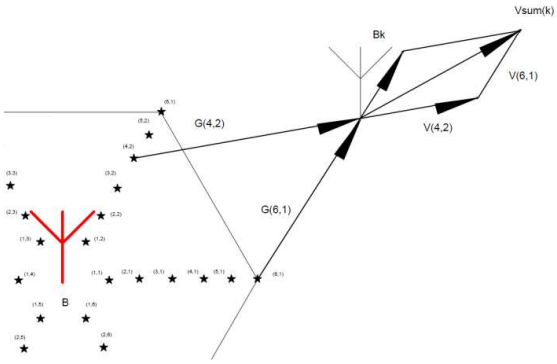


Figure 4. Interference at BS "B_k" caused by active sectors G(4,2) and G(6,1).

Having this arrangement for the cell and the interference vector, we formulate the optimization problem as follows. First, the interference measured at BS "B_k" is represented by $\vec{V}_{\Sigma}^{k}$. Second, $\vec{T}_m=[\vec{X}_m(i,j),\vec{p}_m(i,j))]$ contains the current generation. Third, $\vec{X}_m(i,j)=[\vec{a}_m(i),\vec{b}_m(j)]$ represents the coordinates of the sectors belonging to generation $\vec{T}_m$.

The intensity of the interference can be found using Eq.4.

$$E=\frac{\sqrt{p_m(i,j)}}{|\vec{X}_m-\vec{B}_k|} \tag{4}$$

where $\vec{B}_k$ represents the coordinates of BS "B_k".

The interference vector $\vec{V}_m^k$ for the active sector with coordinates (i, j) transmitting a signal with power $p_m(i,j)$ is defined as

$$\vec{V}_m^k=\frac{\vec{X}_m}{|\vec{X}_m|}E \tag{5}$$

Substituting *E* in Eq. 5 we find

$$\vec{V}_m^k=\frac{\vec{X}_m}{|\vec{X}_m|}\cdot\frac{\sqrt{p_m(i,j)}}{|\vec{X}_m-\vec{B}_k|} \tag{6}$$

Finally, the overall interference vector for BS "B_k" is represented by

$$\vec{V}_{sum}(k)=\vec{V}_{\Sigma}^{k}=\sum_{m=1}^{n}\vec{V}_m^k \tag{7}$$

The objective is maximizing the throughput under the constraint that the interference level is below a given limit. Then, if a set $\{\vec{X}_m\}$ is given, the aim is to find $\{p_m\}$ for which Eq.8 holds, subject to the constrains presented in Eq.9:

$$\max\sum_{k=1}^{6}\left|\vec{V}_{\Sigma}^{k}\right| \tag{8}$$

$$\left|\vec{V}_{\Sigma}^{k}\right|\le P_{\max},\ k=1,2,3,4,5,6 \tag{9}$$

As seen from Eqs. 8 and 9, during the uplink power control optimization process we try to increase the signal power of the active sectors, thus increasing the throughput, while keeping for each neighboring cell the interference below a predefined threshold (P_{max}).

To solve the uplink power control optimization problem we develop an EA implemented in the following steps.

Evolution Step 1: First, let the total number sectors is "J", and the number of active sectors is "N" (N<J). We choose one set consisting of "n" (n<N) active sectors in a random manner. The transmitted signal power for each of these

 ISBN: 978-1-61208-166-3

sectors is allocated randomly. We check if the requirements in Eq. 8, and the constrains in Eq. 9 are fulfilled. If the check is positive, then the solution is considered as suboptimal and the current generation $\bar{T}_m$ is memorized. This is performed for a number of "I" iterations. Then we perform this experiment for another set of active sectors. This is done for all possible sets of n active sectors - R. As a result from step 1 we have memorized a number of suboptimal solutions, including the sets of active sectors with their corresponding allocated transmitted signal power.

Evolution Step 2: The allocated signal power found in step 1 of each of the "R" set of active sectors is transformed as follows. We increase by a random factor the transmitted power for all sectors belonging to the set. This goes for another "I" iterations. Then we check if the constrains in Eq.9 are fulfilled. If the check is positive then the solution is considered as suboptimal and it is memorized.

Evolution Step 3: We again randomize the sector combinations, but this time using (n+1) active sectors. Then we look for combination match in the memory of sector indexes for each permutation of randomized combination. If there is one or more matches we use one of them as base for step 3. We chose randomly one active sector belonging to the set and increase its power with 1 unit. Then we check if the constrains in Eq.9 are fulfilled. If the check is positive then the solution is considered as suboptimal and it is memorized.

The flow chart of the proposed EA for uplink power control (EA-UPC) is presented in Figs. 5, 6, 7 and 8.

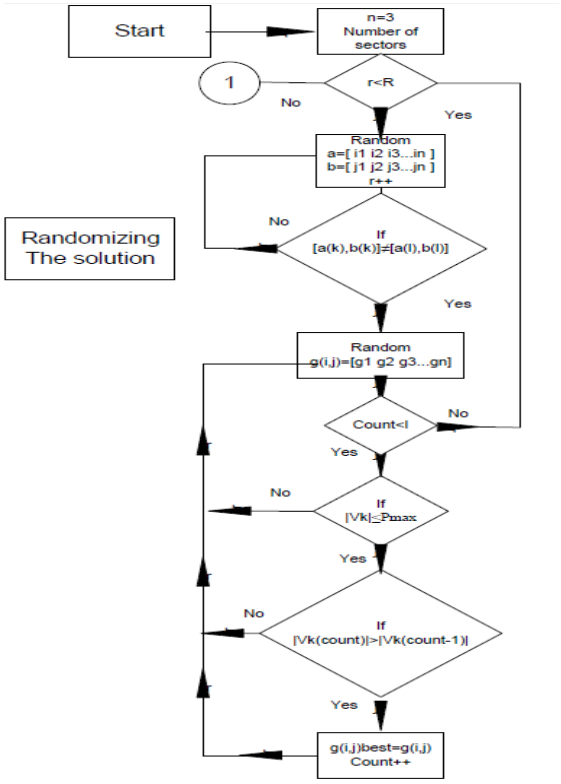


Figure 5. EA-UPC chart diagram (EA step 1).

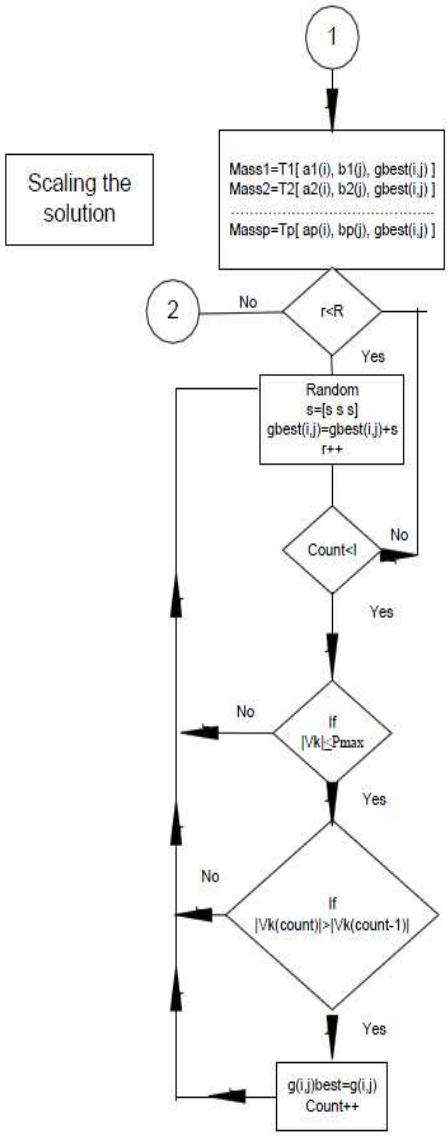


Figure 6. EA-UPC chart diagram (EA step 2).

As a result from EA-UPC we build a look-up table consisting of different combinations of active sectors with their signal power. These combinations represent the suboptimal solutions found in the optimization process.

Evolution Step 4: Each solution is compared to others using the sector coordinates and if the difference vector for two solutions is below a given threshold an associative link is created between them. This process develops an associative memory as shown in Fig. 9. Here, the elements MASS(m,n) represent the combination set of active sectors and STR[(m,n),(p,q)] the associative links between them. During uplink power control if a particular solution comes out not to be appropriate, because of specific sector or cell throughput requirements, or some QoS issues [8], then one of its associates could be used. The STR links could be also used for further evolutionary processing.

 ISBN: 978-1-61208-166-3

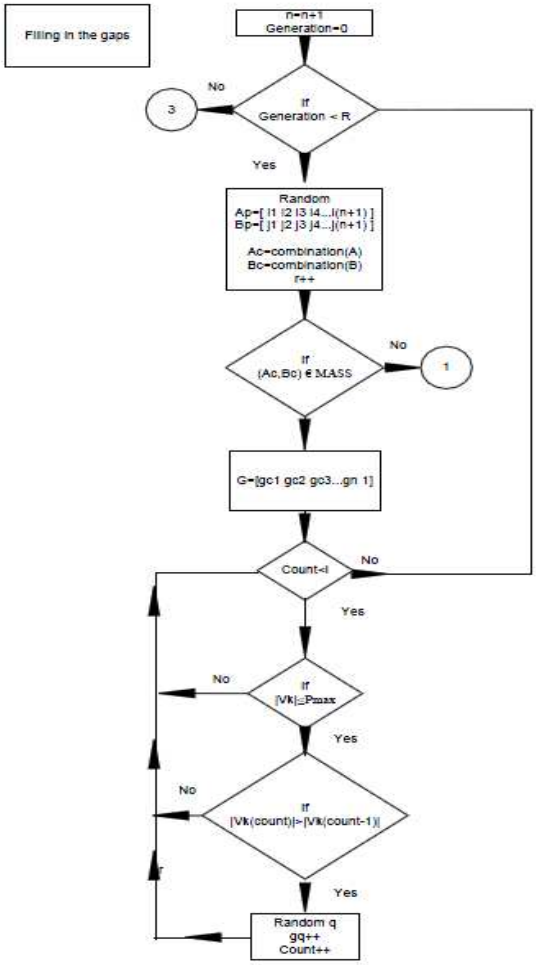


Figure 7. EA-UPC chart diagram (EA step 3).

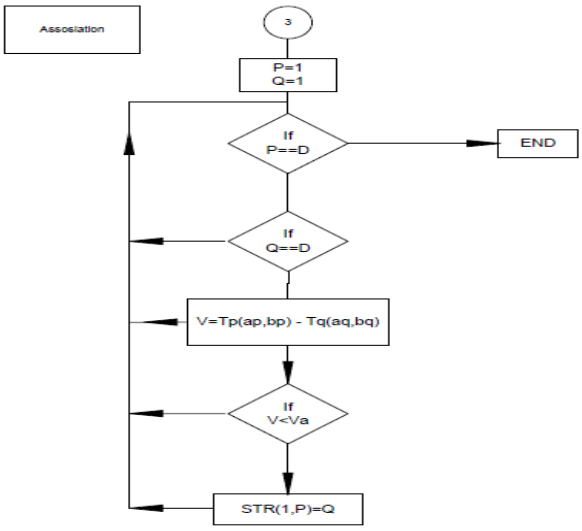


Figure 8. EA-UPC chart diagram (EA step 4).

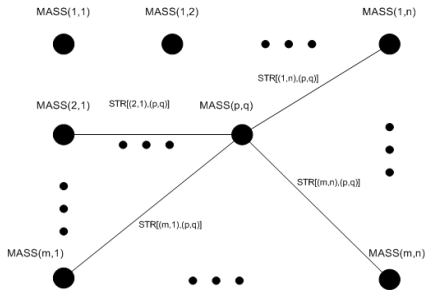


Figure 9. Associative memory.

IV. SIMULATION RESULTS

As a simplified example for EA-UPC we consider the cell presented in Fig. 10, and assume that the number of active sectors is four. The cell is divided into six sectors and in the process of initial set up BS "B", applying the EA a "look-up table" is created in which the suboptimal solutions are memorized. For our case of four active sectors the look up table is illustrated in Table 1. During the operation the BS locates the set of active sectors. Then using the look up table, the BS limits the corresponding uplink signal power level for each one of the active sectors. If some of the sectors needs power above the assigned limit, because of throughput or QoS requirements, then the BS can use one of the associated combinations. The fourth column of Table 1 represents the associative combinations.

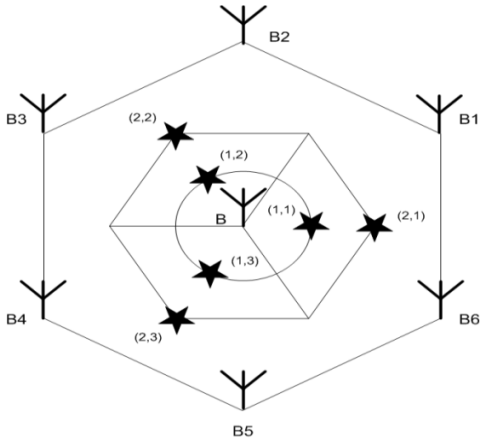


Figure 10. A simplified example for EA-UPC UPC.

To evaluate the performance of EA-UCP we simulate each evolutionary step during the initial set-up procedure of the BS. The results are presented in Fig. 11. During the experiments, the maximum allowed for each neighboring cell interference is set at an absolute value of 20. We run 150 independent simulations of the EA-UCP and each one undertakes 300 iterations. The results for the overall neighboring cells interference are averaged over all 150 simulations. Combinations of different active sectors are investigated to evaluate the influence of the sectors location on the performance of EA-UPC.

 ISBN: 978-1-61208-166-3

TABLE I. LOOK-UP TABLE FOR EA-UPC

Active sector combination MASS (m,n)	Sector coordinates	Corresponding power $p_m(i,j)$ (absolute value)	Associate combinations STR([(..),(..)]
1	(2,3), (1,1), (1,2), (2,2)	1, 6, 6, 1	15, 10
2	(2,2), (2,1), (1,1), (1,2)	5, 2, 5, 1	15, 9
3	(2,3), (1,3), (1,1), (2,1)	1, 8, 4, 1	12, 10, 9
4	(1,3), (2,1), (1,2), (2,2)	9, 6, 1, 1	9, 12
5	(1,2), (1,3), (1,1), (2,3)	2, 2, 1, 1	5, 14
6	(2,1), (2,3), (2,2), (1,3)	10, 9, 2, 1	8
7	(1,1), (1,3), (2,1), (1,2)	8, 1, 3, 1	14
8	(2,1), (2,3), (2,2), (1,2)	10, 9, 2, 1	8, 11, 6
9	(1,3), (2,2), (1,1), (2,1)	5, 2, 2, 1	4, 3, 2
10	(1,3), (2,2), (1,1), (2,3)	5, 2, 2, 1	13, 3, 1
11	(2,2), (2,1), (1,1), (2,3)	5, 2, 5, 1	11, 8
12	(1,3), (2,1), (2,3), (1,2)	8, 8, 7, 1	13, 4, 3
13	(2,2), (2,3), (1,3), (1,2)	2, 3, 5, 1	12, 10
14	(1,3), (1,2), (2,2), (1,1)	7, 8, 3, 1	7, 5
15	(2,3), (1,1), (1,2), (2,1)	1, 6, 6, 1	3, 2, 1

The simulation results demonstrate that in each of the evolutionary steps, the EA-UPC algorithm tends to maximize the overall neighboring cells interference, thus maximizing the overall cell throughput, but at the same time keeping the interference below the predefined allowable threshold. All steps in EA show, as expected, a logarithmic increase in overall neighboring cell interference. While the algorithm goes thought steps 1, 2, and 3, the second derivative decreases and the graphics straighten, as the difference in power allocated between steps differs.

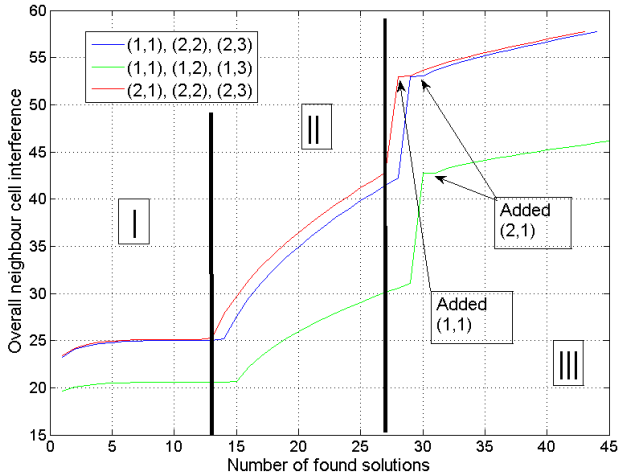


Figure 11. Combined evolutionary steps.

It could also be seen from this simple example, that after the 10th suboptimal solution of the first evolutionary step, most probable is each following suboptimal solution to give very little contribution to the increase of the overall neighboring cells interference and thus to the throughput. This justifies the application of the next step of EA. The simulation results show, that in the third evolution step (Fig.11), the rise of the interference level reaches the maximum allowable limit. For the chosen set of sectors the algorithm stops to evolve, as it has reached the constraints of maximum interference of the absolute value of 20 for one of the neighboring BS stations.

V. CONCLUSIONS

The proposed, in this contribution, evolutionary algorithm can be used effectively for uplink power control in LTE networks. Assuming an interference limited approach to power control, based on the division of the cell into sectors and estimating, via the proposed EA algorithm, the maximum allowable overall interference generated for different combinations of active sectors, a maximum of average cell throughput could be achieved. The EA-UPC demonstrates good performance characteristics for a broad range of active sector combinations. Compared to the now-existing methods for uplink power control the presented approach reveals several major advantages. First, EA-UPC is CLPC method because we keep the interference below a predefined maximum. Second, because of the random manner of power allocation for the active sectors, EA-UPC provides fair resource management independent of the sector location in the cell (central or outage zone). Besides these the look up table could be cell specific depending on the number of sectors in the cells, dimension and type of the area (rural or non-rural) QoS requirements and other cell parameters or conditions.

ACKNOWLEDGMENT

This work was supported by the Bulgarian National Science Fund – Grant No. DDVU 02/131.

REFERENCES

[1] P. Larranaga and J. Lozano, Estimation of Distribution Algorithms: A New Tool for Evolutionary Computation, MA: Kluwer, 2002.

[2] S. Yang and X. Yao, Population-Based Incremental Learning with Associative Memory for Dynamic Environments, IEEE Trans. on Evolutionary Computation, vol.12, Oct. 2008, pp. 542–561.

[3] C. Castellanos, D. Villa, C. Rosa, K. Pedersen, F. Calabrese, P. Michaelsen, and J. Michel, Performance of uplink fractional power control in UTRAN LTE, Proc. VTC Spring 2008, 11-14 May 2008, Singapore, pp. 2517–2521.

[4] D. Astely, E. Dahlman, A. Furuskar, Y. Jading, M. Lindstrom, and S. Parkvall, LTE: the evolution of mobile broadband, IEEE Communications Magazine, Apr. 2009, pp. 44-51.

[5] M. Boussif, N. Quintero, F. Calabrese, C. Rosa, and J. Wigard, Interference based power control performance in LTE uplink, Proc. IEEE International Symposium on Wireless Communication Systems, 21-44 Oct. 2008, Reykjavik, pp. 698–702.

[6] B. Muhammad and A. Mohammed, Performance evaluation of closed loop power control for LTE system, Proc VTC Fall 2009, 20-23 Sept. 2009, Anchorage, pp. 1-5.

[7] H. Gochev, V. Poulkov, and G. Iliev, Improving Cell Edge Throughput for LTE Using Combined Uplink Power Control, Proc. TSP 2010, Vienna, 2010, pp. 465-467.

[8] E. Pencheva and I. Atanasov, book chapter Web Services for Quality of Service Based Charging, in „Developing Advanced Web Services through P2P Computing and Autonomous Agents: Trends and Innovation", IGI Global, 2010, pp. 219-236.

 ISBN: 978-1-61208-166-3

High Spectrum Efficiency Delay Tolerant Scheduling and Resource Allocation of Diverse Traffic in LTE Networks

Tengfei Xing, Xiaoming Tao and Jianhua Lu
State Key Laboratory on Microwave and Digital Communications
Tsinghua National Laboratory for Information Science and Technology
Dept. of Electronic Engineering, Tsinghua University, Beijing 100084, China
Email: {xingtf, taoxm, lujh}@wmc.ee.tsinghua.edu.cn

***Abstract*—In this paper, we propose a multiuser scheduling scheme for traffic with diverse delay constraints in the downlink of 3GPP UMTS/LTE. Traditional scheduling algorithms applied in Long Term Evolution (LTE) do not take much consideration of various delay tolerances of data packets, and most of them are on a slot-to-slot basis, which limits the ability to share spectrum and power resources among time. This would cause the network failing to deliver some packets or declining certain requests with longer delay tolerances, thereby lowering the efficiency of limited spectrum resources. Our proposed scheme schedules packets from multiple users by gathering information including service QoS, channel conditions and available resources in a preset time window, whose length equals the typical delay tolerance of multimedia data packets. The gathering of those information could be aided by channel/traffic estimations and predictions. By doing so, the algorithm achieves notably higher effective throughput than conventional schemes, thereby boosting spectrum efficiency. Simulation results show that our scheduling and resource allocation strategy can achieve 200% to 400% times of spectrum efficiency under typical system parameters.**

***Index Terms*—delay tolerant scheduling, resource allocation, LTE, spectrum efficiency**

I. Introduction

In the next decade, rapid growth of cellular communication service demands are expected to come. Applications with diverse Quality of Service (QoS), including high data rates, different real-time and interactive features, etc., will take up most of the traffic loads in cellular networks. Thereby, scheduling and allocation of radio resources is an area that deserve much attention in cellular systems such as LTE, since it is widely recognized as an element which can greatly affect the performance and spectrum efficiency of the network.

Due to the important role of scheduler in determining the overall system performance, there have been many studies on LTE scheduling in open literatures. The fundamental idea of a scheduler is to allocate each resource block to the user who can best make use of it according to some utility, and the scheduling problem is to determine the allocation of all the resource blocks to a subset of users in order to maximize some objective function, such as network throughput. [1]-[5] proposed different scheduling schemes considering heterogeneous traffic, especially their delay constraints. The delay constraints are often transformed into various instantaneous rate constraints. Moreover, [6] focused on energy efficiency when dealing with delay constrained traffic. However, to the best of the authors' knowledge, the existing studies rarely take delay tolerance of scheduling into consideration when designing algorithms since they are on a slot-to-slot basis. Thereby they are ineffective in dealing with heterogeneity/bursty of services. Our paper gives a possible solution to this problem, trying to make better use of spectrum resource to support various traffic by designing a delay-tolerant scheduling method.

We will first introduce the framework of delay tolerant scheduling, and formulate an optimization problem to represent the scheduler. To efficiently solve the problem, we will provide a two-stage heuristic algorithm consists of packet selection/subchannel allocation and power allocation with low complexity. The scheduler fully exploits the delay tolerance and jointly processes QoS and channel quality information within a certain period to get the optimal scheduling decision. Simulation results will be given to demonstrate the better performance with respect to spectrum efficiency. The advantage is that our algorithm prioritize the transmissions of the right packets, not the early packets, thereby achieves the overall optimal effect and efficiency of resource allocation.

In this paper, we first present the system model and formulate the delay tolerant sum effective rate maximization scheduling and resource allocation problem in Section II. This leads to a nonlinear hybrid-binary integer program. We then use a heuristic method to solve the problem in Section III to solve the resource allocation problem efficiently. Next we give simulation results in Section IV that compare our proposed delay tolerant scheduler with existing ones in terms of throughput. Concluding remarks will be provided in Section V.

II. System Model and Problem Formulation

Fig. 1 illustrates the downlink of an OFDMA single antenna (SISO) multiuser LTE network. A delay tolerant scheduling server (DTSS) is attached to the eNB, and it carries out RB scheduling and power allocation in a centralized manner through information exchange with the eNB. Let N be the

 ISBN: 978-1-61208-166-3

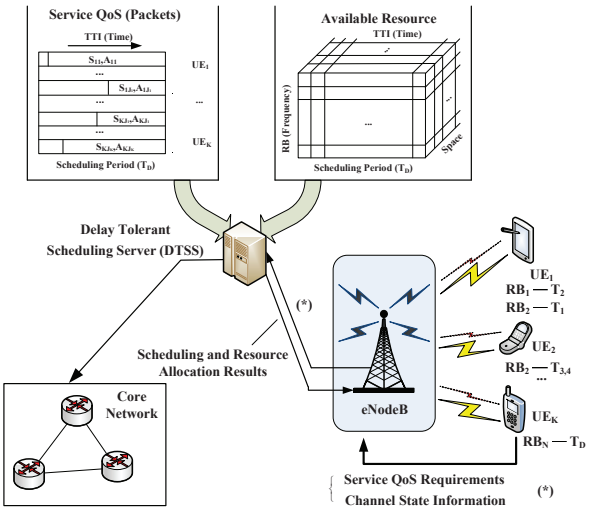


Fig. 1. System Architecture of Delay Tolerant Scheduling in the Downlink of 3GPP LTE

number of RBs and K be the number of UEs in a sector. The CSI is sent back from each UE to the eNB through a delay-free and error-free feedback channel, in order to let the DTSS do adaptive RB/power allocation and select suitable UE to serve. For the sake of analyzing spectrum efficiency, this paper does not involve specific modulation and coding. Suppose that all the users are pedestrians, so the factor of hand-over is not included here since the time scale of scheduling period is hundreds of milliseconds.

Let us consider that each UE generates data traffic in a Poisson manner. The average arrival interval is T_S TTIs. Each TTI is a basic subchannel scheduling block, and its length is configured due to the fast fading property of the propagation channel, commonly 1 ms. However, for the sake of reducing algorithm complexity, we use a larger TTI value. Here we use a non-causal hypothesis, which gathers all the service QoS, CSI and available resources (including RBs and power in all TTIs) information within the scheduling period for the scheduler. Let T_D TTIs (the unit TTI to describe time will be omitted from here on for simplicity) be the delay tolerance (or scheduling period) of the scheduler, which starts from an arbitrary packet transmission request. Thereby, we would get all the packet arrival time, packet sizes, delay tolerances of each packet, CSI, available RBs and total available power in T_D. Then we do RB scheduling and power allocation in the scheduling period T_D.

Suppose the duration of an RB is T_{RB}, and $1TTI = N_{RB} \cdot T_{RB}$. We suppose that all the RBs within a scheduling block is allocated to a single user. This is reasonable since the channel state does not vary much with in a TTI, and it also lowers the complexity of the algorithm. Then we put all the RBs on the same frequency into groups of N_{RB}, and the number of groups is T_D. Denote the number of RBs on the frequency dimension N_F. Thereby, the number of RB scheduling units within a scheduling period is $T_D \cdot N_F$. Let A_{kj} and S_{kj} be the arrival TTI index and size of the j th data packet of the k th UE ($j = 1, \cdots, J_k$) within the scheduling period. Certain distribution among a finite set of values for S_{kj} is used to model dfferent types of traffic. Also, the delay bounds of all packets is set to be the end of the scheduling period, which is the instant at T_D. Then reshape all the A_{kj} and S_{kj} to be a column vector $\hat{A}$ and $\hat{S}$ with elements $\hat{A}_l$ and $\hat{S}_l$ ($l = 1, \cdots, \sum_{k=1}^{K} J_k$), with ascending orders of user first and then data packets. Let B_l be a binary matrix indicating which RB groups are allocated to the l th data packet,

$$B_l(m,n) = 1,\ (m = 1, \cdots, N_F,\ n = 1, \cdots, T_D) \Leftrightarrow \\ RB\ at\ (m,n)\ position\ is\ allocated\ to\ packet\ l \tag{1}$$

with $B_l(m,n)$ denoting to the (m,n) th value of B_l. Reshape B_l into a column vector b_l in a column-by-column manner, i.e. $b_l(mN_F+n) = B_l(m,n)$. In a SISO system, each RB at a certain time can only be allocated to a single UE's single packet, in order to avoid interference. Thereby the RB allocations are not overlapping, meaning that

$$b_s^T \cdot b_t = 0 \quad \forall s \neq t \tag{2}$$

which is not a necessary assumption in a multiuser MIMO system. The power allocated onto RB group m in TTI n is denoted by P_{mn}. We define an effective packet transmission as the packet is successfully transmitted with its full length and without going over its delay limit. The design goal of our scheduling algorithm is to maximize the throughput of effective packet transmissions given the delay tolerance of the scheduler and available system resources.

Let $\alpha(l)$ be the UE index of packet l. The achievable transmission rate of packet l in RB group m and TTI n can be expressed as:

$$r_{mn}^l = B_l(m,n)\left[W_{RB}\log_2\left(1 + \frac{P_{mn}H_{\alpha(l)}(m,n)}{N_0 W_{RB}}\right)\right] \tag{3}$$

where $H_{\alpha(l)}(m,n)$ denotes the channel gain for user α_l in RB group m and TTI n, W_{RB} denotes the bandwidth of an RB and N_0 denotes the power spectrum density of noise.

Finally, the delay tolerant scheduler can be formulated as an sum rate maximization problem:

$$\max_{b_l, P_{mn}} \left\{ \sum_{l=1}^{L} C_l \right\} \\ where\ \ C_l = \begin{cases} \hat{S}_l,\ if\ \left(\sum_{m,n} r_{mn}^l\right) \cdot TTI \geq \hat{S}_l \\ 0,\ else \end{cases} \tag{4}$$

$$s.t. \quad b_l(n) \in \{0,1\} \quad \forall l,n \tag{5}$$

$$b_l(mN_F + n) = 0 \quad \forall n = 1, \cdots, \hat{A}_l - 1,\ m \tag{6}$$

$$b_s^T \cdot b_t = 0 \quad \forall s \neq t \tag{7}$$

$$\sum_{m,n} P_{mn} \leq P_{\max} \cdot T_D \tag{8}$$

where $P_{\max}$ is the total transmit power limit of the eNB. (6) means that no RBs is allowed to be allocated to a packet before its arrival. Clearly this is a highly non-linear hybrid-binary integer program, for which no efficient solution exists.

 ISBN: 978-1-61208-166-3

As an NP-hard problem, exhaustive searching algorithm with high complexity can solve the problem. In the next section, a low-complexity allocation scheme based on heuristic methods is proposed.

It is worth mentioning that the heterogeneity and bursty of services is embodied through the above modeling of packet arrival and QoS (size and delay tolerance). Specifically, with independent arrivals, the possibility of bursty packet arrivals is increased with the number of users. Also with different arrival and same deadline, various levels of delay tolerance is presented for each packet. Moreover, the difference in packet sizes represents heterogeneity of services.

III. Maximum Effective Rate Scheduler and Resource Allocation

We propose a heuristic scheme that achieves sub-optimal solution to the proposed delay tolerant scheduling problem. The scheme is divided into iterations of the following two stages. In the first stage, the algorithm selects a packet to serve, and the RBs are assigned to this packet under the assumption that the eNB's total transmission power left (initially $P_{\max}$) is equally distributed among every RB left in both frequency and time dimensions, i.e. $P_{mn} = \frac{P_{\max} \cdot T_D}{N_F \cdot T_D}$ initially. This stage only implements RB selection and allocation. In the second stage, power are allocated to the RBs assigned in the first step in order to save as much transmission power as possible and potentially lowers the number of RBs required. The allocated RBs and power are excluded from the resource left for the next iteration. The exit condition of the iterations is that none of the packets can be served with the RBs and power left. The step-by-step iterations to determine the packets to serve and the separation of subchannel allocation and power allocation enable a suboptimal algorithm; however, it makes the complexity significantly lower than the exhaustive search.

A. Throughput-oriented Packet Selection and RB Allocation

Due to the target of maximizing the sum rate of effective packet transmissions and our assumption that each packet have different arrival time and the same deadline, it is reasonable to use the following criteria to select which packets should be scheduled with a higher priority:

1) For packets with the same sizes, the one with a longer delay tolerance should be scheduled first.
2) For packets with the same delay tolerances, the one with a smaller size should be scheduled first.
3) For any packets, the one with a smaller average rate requirement (its size divided by its delay tolerance) should be scheduled first.

The main idea behind these criteria is to consume as few resources (including RBs and power) per unit of data as possible, in order to serve more packets with the same total resources. Firstly, due to the principle of diversity, the possibility to have an RB with good channel quality within a longer period of time is higher. Therefore, the packet with a longer delay tolerance may consume less resources, making it a favorable choice. Also, within the same period, the packet with a larger size generally requires more RBs or power. However, the possibility to have more RBs with better channel quality is less for a fixed user. This also leads to a smaller efficiency of resource utilization. Hence, the packet with a smaller size is favorable among the ones with the same delay tolerance. Last but not least, the third criterion is a combination of the first two.

TABLE I
Packet Selection/RB Allocation of Delay Tolerant Scheduler

0. Preliminary Process (only execute once at the beginning of a scheduling period):
Calculate the average rate requirements for every packet, $R_l = \frac{\hat{S}_l}{T_D-(\hat{A}_l-1)}$.
Set $b_l(mN_F+n) = 0 \quad \forall m,n,l.\ P_0 = P_{\max} \cdot T_D$.
Create an empty queues Q_1, storing the indexes of packets selected to serve.
1. Initialization:
a) Let Φ be the set of the index of packets left un-selected, Θ_{RB} be the set of the index of RBs left un-allocated, and P_0 the power left un-allocated.
b) Do a sorting of $R_l\,(l \in \Phi)$ in ascending order, and store the index of the results in a queue Q.
c) Set $P_{mn} = \frac{P_0}{\|\Theta_{RB}\|}$. $\hat{C}_l = \hat{S}_l\,(l \in \Phi)$.
2. Packet Selection and RB allocation:
a) Select a packet l_1 with the smallest R_l from Q. Exclude l_1 from Q. Create an empty queue Q_S to store the indexes of RBs that will be allocated to packet l_1.
b) Do a sorting of $H_{\alpha(l_1)}(m,n)$ $\left(u = mN_F + n \in \Theta_{RB}, n \geq \hat{A}_{l_1}\right)$ in descending order, and store the index of the results u in a queue Q_H.
c) Select an RB whose index is $u_0 = m_0N_F + n_0$ with the largest $H_{\alpha(l_1)}(m,n)$ value. This is equivalent to finding $u = \arg\max_{u \in \Theta_{RB}} r^{l_1}_{mn}$ $\left(n \geq \hat{A}_{l_1}\right)$. Exclude u_0 from Θ_{RB}. Add u_0 to Q_S.
d) Allocate RB u_0 to packet l_1, and calculate the unserved data size, $\hat{C}_{l_1} = \hat{C}_{l_1} - r^{l_1}_{m_0n_0} \cdot TTI$.
e) If $\hat{C}_{l_1} \leq 0$, exclude packet l_1 from Φ and add it to Q_1, exclude all elements in Q_S from Θ_{RB}, mark the corresponding elements of b_{l_1} to 1, and finish allocation. Go to power allocation.
f) If $\hat{C}_{l_1} > 0$ and Q_H is not empty, go to step c).
g) If $\hat{C}_{l_1} > 0$ and Q_H is empty, which means that this packet cannot be served with the resource left, exclude packet l_1 from Φ, and go to step a).

We propose a throughput-oriented packet selection and RB allocation scheme in Table I, based on the criteria above. First, we calculate the average rate requirements of all the packets. Then we select the packet with the lowest rate requirements, l_1, as a candidate to be scheduled in this scheduling period. Among all the RBs that are valid to be allocated to l_1 (meaning that they are not allocated to other packets, and their time index has to be larger or the same as $\hat{A}_{l_1}$), the ones with better channel quality regarding UE $\alpha(l_1)$ are allocated to l_1 one by one. Once the total data size provided by the allocated RBs exceed $\hat{C}_{l_1}$, l_1 is successfully scheduled, and the algorithm goes to the next stage of power allocation. The elements of the indicator vector b_{l_1} are also marked to 1 correspondingly, and the allocated RBs from the set of available RBs are excluded for further scheduling. If all the RBs are allocated to l_1 and the total data size still cannot exceed $\hat{C}_{l_1}$, then l_1 cannot be

 ISBN: 978-1-61208-166-3

served. This will lead to another packet selection with the next lowest rate requirements.

B. Resource Efficient-oriented Power Allocation

After packet l_1 is selected in the first stage, we can further optimize the consumption of transmit power and number of RBs. In the RB allocation process, equal power allocation is assumed. Now we use an inverse-waterfilling (IWF) method to minimizing power subject to a rate constraint (meaning that the packet needs to be delivered at its full size), which is a dual problem of conventional waterfilling [6].

Suppose the indexes in Q_S is $u_i = m_i N_F + n_i \, (i = 1, \cdots, d)$, where d is the number of allocated RBs. The IWF method can be formulated as an convex optimization problem:

$$\min_{r_{u_1}^{l_1}, \cdots, r_{u_d}^{l_1}} \sum_{i=1}^{d} P_{u_i} \quad \text{where } P_{u_i} = N_0 W_{RB} \cdot \frac{2^{\left(r_{u_i}^{l_1} / W_{RB}\right)} - 1}{H_{\alpha(l_1)}(m_i, n_i)} \tag{9}$$

$$s.t. \quad \left(\sum_{i=1}^{d} r_{u_i}^{l_1} \right) \cdot TTI = \hat{S}_{l_1} \tag{10}$$

$$r_{u_i}^{l_1} \geq 0 \quad \forall i = 1, \cdots, d \tag{11}$$

where $r_{u_i}^{l_1} = r_{m_i n_i}^{l_1}$ is the achievable rate on RB u and P_{u_i} is the power allocated on RB u. After the optimal r_{u_i} is solved, P_{u_i} can be simply calculated. This problem can be easily solved using the Lagrangian method:

$$r_{u_i}^{l_1} = W_{RB} \cdot \left\langle \log_2 \left(\frac{H_{\alpha(l_1)}(m_i, n_i)}{H_{th}} \right) \right\rangle_0^{\infty} \tag{12}$$

where H_{th} is the water level and the solution to

$$\sum_{i=1}^{d} \left\langle \log_2 \left(\frac{H_{\alpha(l_1)}(m_i, n_i)}{H_{th}} \right) \right\rangle_0^{\infty} = \frac{\hat{S}_{l_1}}{W_{RB} \cdot TTI} \tag{13}$$

We can see that an RB is utilized only if a positive energy is scheduled on it, i.e., $r_{u_i}^{l_1} \geq 0$ or equivalently $H_{\alpha(l_1)}(m_i, n_i) > H_{th}$. Then we calculate the total energy consumed, and subtract it from P_0, the total energy left for the other un-scheduled packets. For all u_i that $r_{u_i} \leq 0$, meaning that these RBs are not needed for transmitting packet l_1 and thereby can be re-allocated to other packets, add them back to Θ_{RB}. It is obvious that this power allocation step not only optimizes the power consumption for the packet transmission, but also potentially saves some spectrum resource blocks for further scheduling of more packets.

C. Brief Summary and Performance Metric of Delay Tolerant Scheduling

Combing the above two stages, we summarize the solution to the delay tolerant scheduling problem in Table II. After the scheduling is done for as many packets as possible, the maximized sum data size served is $\sum_{l \in Q_1} \hat{S}_{l_1}$. It is easy to see that the complexity of the above method is much lower than exhaustive search.

TABLE II
SOLUTION TO DELAY TOLERANT SCHEDULING

While Φ is not empty, where Φ is the set of the index of packets left un-selected:

1) Follow the process in Table I, select a packet l_1 to serve, and allocates RBs in Q_S to l_1.

2) Do power allocation among RBs in Q_S by solving the convex optimization problem in (9); go back to step 1).

IV. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

In order to compare the proposed scheduling scheme with existing ones, we use a standard compliant LTE system level simulator [7] that is publicly available, based on which necessary modules are further developed.

The simulation parameters are summarized in Table III. We use a microscale fading channel model with channel gain constant during a 20ms TTI and independent among all TTIs. Due to the delay-free and error-free CSI feedback assumption, the DTSS gets the CSI information before transmissions. The packets have sizes and delay properties as typical multimedia traffic (including audio, video streaming, etc.), and the scheduling period is set to be 10 or 20 TTIs. The delay tolerance of packets span from 1 TTI (20ms) to 20 TTIs (400ms), which corresponds to the QoS demands of most typical services. All the packets can be viewed as non-realtime (NRT) service requests, which have average rate constraints within their own valid periods. Thereby, the heterogeneity of services are embodied through the difference of packet sizes and delay tolerances.

First, we consider the case with a fixed number of five users and compare the performance of different schedulers. Fig. 2 shows the sum throughput of all the users versus their average signal-to-noise ratio (SNR) when applying different schedulers. Our proposed DTS with scheduling period (delay tolerance) of 10 and 20 TTIs are shown with three typical scheduling algorithms, including Round Robin (RR), MaxMin (MM) and Proportional Fair (PF) scheduling. A best effort (BE) upper bound, which is the capacity limit of five users with all full buffer Best Effort (BE) traffic without considering packet arrivals and delay constraints, is simulated and shown for comparison.

It is shown that DTS can achieve up to 2 to 4 times of throughput than existing schedulers at normally used common SNR region (0 to 10 dB). The throughput gain is larger for lower SNR values and diminishes gradually as the SNR increases. This gain is achieved since under low SNR, existing schedulers may not successfully serve packets at its full size or accept certain requests, due to both the tighter constraints of frequency and power resources within a shorter period and lack of utilization of QoS and CSI to make proper scheduling decisions. On the other hand, DTS is able to jointly utilize the resources within a longer period and optimize the scheduling decisions, by collecting the QoS and CSI information within the delay tolerance, thereby achieving more successful transmissions of packets and higher throughput. Other than

 ISBN: 978-1-61208-166-3

TABLE III
SIMULATION PARAMETERS

Parameter	Value
System Bandwidth	1.4MHz
Number of subcarriers	72
Number of RBs N	12
Number of user K	5 per sector
Packet Arrival Interval (Poisson)	1 TTI
Channel Model	ITU-T PedB [10]
eNodeB Settings	distance 500m, tx power 20W
Large-Scale Fading	3GPP TS25.814
Shadowing	R9-Claussen, 10dB variance

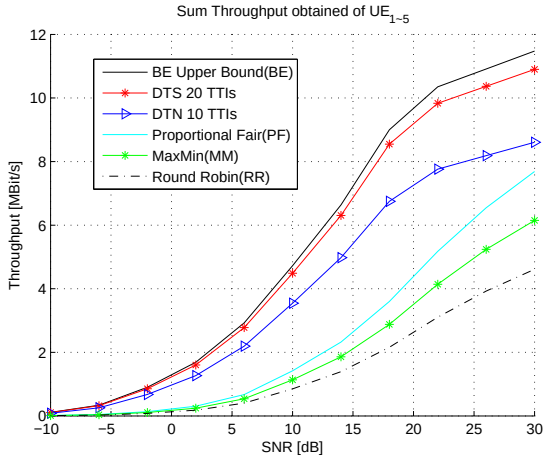


Fig. 2. Sum Throughput versus SNR with different schedulers

a first-in-first-out manner, DTS prioritize the transmissions of the right packets, not simply the early packets. With a higher throughput, the spectrum efficiency is also times higher. Moreover, by increasing delay tolerance, the throughput of DTS is further boosted and thereby the gap between it and the BE upper bound decreases.

Then, we show the benefits of multiuser diversity in the scheduling process. Fig. 3 shows the sum throughput of different schedulers versus different number of users under a fixed average SNR of 10dB. It is shown that as the number of users increases in the same cell, the throughput gradually increases. This is due to the effect of multiuser diversity. Similar application of this concept can be found in [8]. Also, we can observe that the increasing rate of throughput of DTS is larger than the ones of other schedulers. The reason is that our algorithm can better collaborate multiuser diversity with frequency and time diversity of channel fading.

V. CONCLUSIONS

In this paper, we proposed a delay tolerant scheduling scheme for real-time traffic of multiple users in an OFDMA-based LTE downlink network. We introduced the framework of delay tolerant scheduling, and formulate the target of maximizing spectrum utilization in supporting heterogenous traffic as an optimization problem. To efficiently solve the

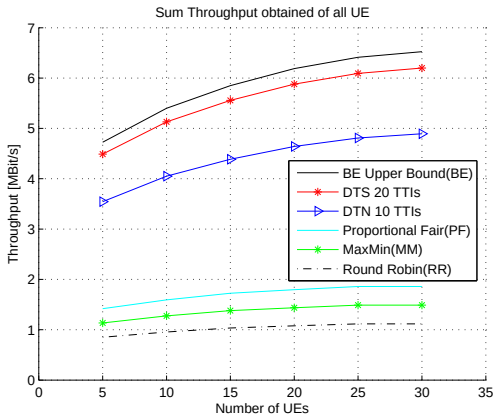


Fig. 3. Sum Throughput versus number of UEs with different schedulers

problem, a two-stage heuristic algorithm consists of packet selection/subchannel allocation and power allocation with fair complexity is given. This algorithm embodies the essence of DTS, which is to utilize all the spectrum and power resources onto the most proper packets. This is done by exploiting the delay tolerance of the scheduler and jointly processing QoS and channel state information within a longer period to get the optimal scheduling decision. Simulation results show that our scheduler outperforms existing algorithms with respect to system throughput and spectrum efficiency.

ACKNOWLEDGMENT

This research work was supported by National Basic Research Program of China (No. 2007CB310601) and NSFC (No. 60972021).

REFERENCES

[1] M. Tao, Y. Liang, and F. Zhang, Resource Allocation for Delay Differentiated Traffic in Multiuser OFDM Systems, ;IEEE Transactions on Wireless Coomunications, ;vol. 7, no. 6, pp. 2190 - 2201, Jun. 2008.
[2] R. Zhang, Optimal Dynamic Resource Allocation for Multi-Antenna Broadcasting With Heterogeneous Delay-Constrained Traffic, IEEE Jou. on Sel in Sig. Proc, ;vol. 2, no. 2, pp. 243 - 255, Apr. 2008.
[3] R. Zhang, Optimized Multi-Antenna Broadcasting for Heterogeneous Delay-Constrained Traffic, ;IEEE ICC 2008, May. 2008.
[4] T. Girici, and A. Epl, Practical Resource Allocation Algorithms for QoS in OFDMA-based Wireless Systems, ;IEEE CCNC 2008, Jan. 2008.
[5] T. Girici, and A. Epl, A channel-aware queue-aware resource allocation algorithm for OFDMA system with heterogenous delay requirements, ;ICPCSPA 2010, Jul. 2010.
[6] J. Lee, and N. Jindal, Energy-efficient Scheduling of Delay Constrained Traffic over Fading Channels; IEEE Transactions on Wireless Coomunications, ;vol. 8, no. 4, pp. 1866-1875, Apr. 2009.
[7] [Online]. Long Term Evolution (LTE) System Level simulator. Available: http://www.nt.tuwien.ac.at/ltesimulator/
[8] B. Niu, O. Simeone, O. Somekh and A. M. Haimovich, Ergodic and Outage Sum-Rate of Fading Broadcast Channels with 1-Bit Feedback, ;IEEE Transactions on Vehicular Technology, ;vol. 59, no. 3, pp. 1282 - 1293, Mar. 2010.

 ISBN: 978-1-61208-166-3

Self-Adaptive TCP Protocol Combined with Network Coding Scheme

Sicong Song[1], Hui Li[1*], Kai Pan[1], Ji Liu[1], Shuo-Yen Robert Li[2]
1. Shenzhen Key Lab of Cloud Computing Technology & Application, Shenzhen Graduate School, Peking University, Shenzhen, China, 518055
2. Dept. of Information Engineering, The Chinese University of Hong Kong, China
E-mail: songsc0707@yahoo.com.cn, lih64@pkusz.edu.cn, pankai0905@gmail.com, jliu@pkusz.edu.cn bobli@ie.cuhk.edu.hk

***Abstract*—A Self-Adaptive Network Coding TCP protocol is proposed for dynamical adaptation of the redundancy factor in the network, including the case of a wireless network. It trims packet loss effectively via redundant packets of network coding. It also adapts certain traffic information, to be stored in the header of TCP or ACK packets, thus enables the sender to dynamically adjust the redundancy factor of the network. Simulation of traffic fluctuation in the real network shows better utilization of communication channels and better throughput by the proposed protocol than TCP-Vegas as well as NC-TCP.**

Keywords-network coding; packet loss; TCP

I. INTRODUCTION

Network coding is a technique where, instead of simply forwarding the packets the nodes receive, they will combine several packets together for transmission in order to be used for attain the maximum possible information flow in a network. It has emerged as an important potential approach to the operation of communication network, including the case of a wireless network where network coding can trim losses effectively. The major advantage of network coding is masking packet loss by mixing data across time and across flows [1-3]. In lossy networks, network coding can mask the packet loss via redundant packets, thus decrease the delay caused by the timeout and to raise the utilization of the channels. However, we still seem far from seeing widespread implementation of network coding across network. Since network coding can bring benefits in terms of throughput and robustness [4,5], how to put it into practice in real communication network is the main problem that needs to be solved. To do so, firstly, we need to plant network coding into TCP properly with minor changes to the protocol stack, thereby allowing incremental development. We therefore see a need to find a sliding-window approach as similar as possible to TCP for network coding that makes use of acknowledgments for flow and congestion control [6]. Such an approach would necessarily differ from the generation-based approach more commonly considered for network coding [7, 8]. Secondly, we need to solve the delay of encoding and decoding caused by network coding, which can do harm to the performance of networks.

TCP-NC protocol was presented in 2008 [9] which successfully implemented the network coding into TCP with minor changes to the protocol stack. The key idea was adding a network coding layer between transport layer and IP layer to masks packet losses from congestion algorithm. In fact, masking losses from TCP was considered earlier by using link layer retransmission [10]. Yet it has been noted in [11] and [12] that the interaction between link layer retransmission and TCP retransmission is complicated and the performance may suffer due to independent retransmission protocols at different layers. TCP-NC modifies the ACK echo system, and brings in a new notion "see packets". The biggest difference compared to the original mechanism is that under network coding the receiver does not obtain original packets of the message, but linear combinations that are then decoded to get the original message once enough such combinations have arrived. The "see packets" notion can perfectly adapt to these changes, and before explain the notion, they introduce a definition that will be useful throughout the paper [3]. In NC-TCP, packets are treated as vectors over a finite field F_q of size q. All the discussion here is with respect to a single source that generates a stream of packets. The k^{th} packet that the source generates is said to have an index k and is denoted as $\mathbf{p_k}$. As a result, a node is said to have seen a packet $\mathbf{p_k}$ if it has enough information to compute a linear combination of the form ($\mathbf{p_k} + \mathbf{q}$), where $\mathbf{q} = \sum_{l>k} \alpha_l \mathbf{p}_l$, with $\alpha_l \in F_q$ for all $l > k$. Thus, $\mathbf{q}$ is a linear combination involving packets with indices larger than k. To conclude, there are two main differences in our scheme. First, whenever the source is allowed to transmit, it sends a random linear combination of all packets in the congestion window. Second, the receiver acknowledges every sequence number of seen packet. Additionally it brings in a redundancy factor R, which is used for masking the packet loss. For example, if the loss rate is about 10%, then the optimal R equals to 1/ (1-10%) ≈ 1.11, this means the sender will send one more redundant packet every ten packets NC-TCP achieves a goal,

 ISBN: 978-1-61208-166-3

that is, planting network coding into TCP properly. In some communication networks, where the loss rate is roughly constant, via setting the redundancy factor *R* to an optimal number, a better throughput can got compared to the original TCP.

TCP-DNC protocol is presented in 2009 [13], which focuses on reducing the decoding delay and redundancy by adding some information in packet's header. It inherits the coding approach and "see packets" notion presented by the NC-TCP scheme [9]. In the receiver, the TCP-DNC brings in a new factor "loss", which indicates how many combinations the sender needs to retransmit enable the receiver decode all the combinations it has received. The "loss" factor will be sent back to the sender, and the sender uses this factor to decide how many redundant packets should be sent and how many original packets should be coded. By doing this, this new scheme can avoid the retransmission of the useless redundant packets, and due to sending redundancy packets coded by the appropriate number of original packets, it significantly reduces the decoding delay and improves the performance of the networks.

We propose a new scheme named SANC-TCP protocol, which mainly optimizes the scheme based on NC-TCP. To be concrete, in NC-TCP, the redundancy factor *R* is constant, we need to know the loss rate of the network circumstance, and set *R* to the optimal number. However, when the system is under lossy networks, especially wireless network where the loss rate is not constant, the constant redundancy factor *R* may cause problems, either sending bunches of useless redundancy packets or being not able to mask the packets loss. Both will impair the performance of the network. As a result, we need to find a scheme to adjust *R* adaptively to the real system, aiming to better the utility of the networks and decrease the retransmission of the useless redundant packets. Our new scheme, SANC-TCP, adds some feedback information in the ACK header, to indicate the current network state, thus enable the sender to dynamically change the *R* according to the real system.

In Section I, we get an overview of the NC-TCP scheme, and describe the basic theory for background; In Section Ⅱ, we introduce the arithmetic of the Active-R NC-TCP Protocol; In Section Ⅲ, we prove the fairness of our new scheme compared to the old one; In Section Ⅳ, we demonstrate the effectiveness of the new protocol, and show its advantage over the old others. Finally, in Section Ⅴ, we make a succinct conclusion of the whole article.

II. SELF-ADAPTIVE NC-TCP PROTOCOL

In this section, we will describe the basic ideas of the SANC-TCP protocol and the arithmetic for dynamically adjusting the redundancy factor *R*.

The SANC-TCP aims to better the utilization of channels by dynamically adjusting the redundancy factor *R* in unknown lossy networks. To fulfill this target, we make some minor changes to the original protocol stack via adding two variables to the ACK header, i.e., *loss* and *echo_pktID*. At the receiver, the difference which is indicated by *loss* between the largest packet index in the coefficient vector and the number of seen packets implies the number of packets the sender needs to retransmit. Another variable *echo_pktID* indicates the packet ID of which packet generates this ACK. At the sender, once it receives a new ACK, it checks the *echo_pktID*. When *echo_pktID* = 10 or *echo_pktID* > 10 for the first time, it starts to adjust the *R*. First, the sender picks up the variable *loss* from the header of ACK, then figures out the value of *diff_loss_new*, that is, *diff_loss_new* = *loss* – *loss_old*, where diff_loss_new indicates the effect of the redundant packets that sended in the latest turn. The new *R* = 1 + (*diff_loss_new*/10)*2 + *diff_loss_old*/10 , and the original *diff_loss_old* = 0. The current variables *echo_pktID*, *diff_loss_new*, *loss* and *R*, that is *W* = *echo_pktID*, *diff_loss_old* = *diff_loss_new*, *loss_old* = *loss*, *R_old* = *R* is also recorded; For example, if the sender receives a new ACK, and the *echo_pktID* in the ACK equals to 10, then the sender decides to adjust the *R*. Suppose one packet lose among the first ten packets, then the *loss_new* = 1. Meanwhile, the *loss_old* = 0 originally. So, the new redundancy factor *R* = 1 + (1/10)*2 + 0 = 1 + 0.1*2 + 0 = 1.2. After this, the sender keeps checking *echo_pktID* from every new ACK. When *echo_pktID* = *W* + 10**R*, or *echo_pktID* > *W* + 10**R* for the first time, adjust the *R*. At this time, *R* = *R_old* + (*diff_loss_new*/10)*2 + *diff_loss_old*/10. Record the current variables *echo_pktID*, *diff_loss_new*, *loss* and *R*, that is *W* = e *echo_pktID*, *diff_loss_old* = *diff_loss_new*, *loss_old* = *loss*, *R_old* = *R*. If the result of *R* is smaller than 1, set the *R* to 1. For example, if the previous *echo_pktID* = 200, *R* = 1.1, and the sender did not receive ACK which contain *echo_pktID* = 211 or *echo_pktID* = 212. Then, when it receives the ACK whose *echo_pktID* = 213, the sender starts to adjust the *R*. At the receiver when this ACK is generated, if l*oss_new* = 20, *loss_old* = 19, then *diff_loss* = 20 – 19 = 1; This time, at the sender, if *diff_loss_old* = 1, then *R* = 1.1 + (1/10)*2 + 1/10 = 1.4.

To make it clear, we independently describe the actions which are taken on the sender and receiver side. Provided we have introduced a network coding layer between the transport layer and the IP layer.

(1) Receiver side: The receiver side algorithm has to respond to two types of events – the arrival of a packet from the sender, and the arrival of ACKs from the TCP sink.

1. Wait state: If any of the following events occurs, respond as follows; else wait.
2. ACK arrives from TCP sink: If the ACK is a control packet for connection management, deliver it to the IP layer and return to the wait state; else, ignore the ACK.
3. Packet arrives from the sender side:
   a) Remove the network coding header and retrieve the coding vector.
   b) Add the coding vector as a new row to the existing coding coefficient matrix, and perform Gaussian elimination to update the set of seen packets.

 ISBN: 978-1-61208-166-3

c) Add the payload to the decoding buffer. Perform the operations corresponding to the Gaussian elimination, on the buffer contents. If any packet gets decoded in the process, deliver it to the TCP sink and remove it from the buffer.

d) Count the variable *loss* which equals to the difference between the largest packet index in the coefficient vector and the number of seen packets; Pick up the value of *pktID* from the received packet's header, record it to *echo_pktID*.

e) Generate a new ACK with sequence number equals to that of the oldest unseen packets and add two variables loss and echo_pktID to the ACK header.

(2) Sender side: On the sender side, the algorithm again has to respond to two types of events – the arrival of a packet from the sender TCP, and the arrival of an ACK from the receiver via IP.

1. Set NUM to 0;

2. Wait state: If any of the following events occurs, respond as follows; else wait.

3. Packet arrives from TCP sender:

a) If the packet is a control packet used for connection management, deliver it to the IP layer and return to wait state.

b) If packet is not already in the coding window, add it to the coding window.

c) Set NUM = NUM + *R*. (*R* = redundancy factor)

d) Repeat the following ⌊NUM⌋NUM] times:

i) Generate a random linear combination of the packets in the coding window.

ii) Add the network coding header specifying the set of packets in the coding window and the coefficients used for the random linear combination. Add the variable *pktID* to the network coding header.

iii) Deliver the packet to the IP layer.

e) Set NUM:= fraction part of NUM.

f) Return to the wait state.

4. ACK arrives from receiver:

a) Pick up the variable *echo_pktID*, to judge if it is time to adjust the value of *R*.

i) If echo_pktID = W + 10**R*_old or echo_pktID > W + 10**R*_old for the first time, start to reset the value of *R*.

Ⅰ) Extravagate the value of *loss* from the ACK header, *diff_loss_new* = *loss* – *loss_old*;

Ⅱ) Then *R_new* = *R_old* + 2*(*diff_loss_new*/10) + *diff_loss_old*/10.

Ⅲ) Record variables, such as, *R_old* = *R_new*; *diff_loss_old* = *diff_loss_new*; *loss_old* = *loss*; *W* = *W* + 10**R_new*.

ii) else doing nothing and move to state b).

b) Remove the ACKed packet from the coding buffer and hand over the ACK to the TCP sender.

Following the approach above, the sender adjusts the redundancy factor *R* from time to time, thus to dynamically change the R according to the real system. The algorithm to adjust the redundancy factor *R* in the sender is showed in Figure 1.

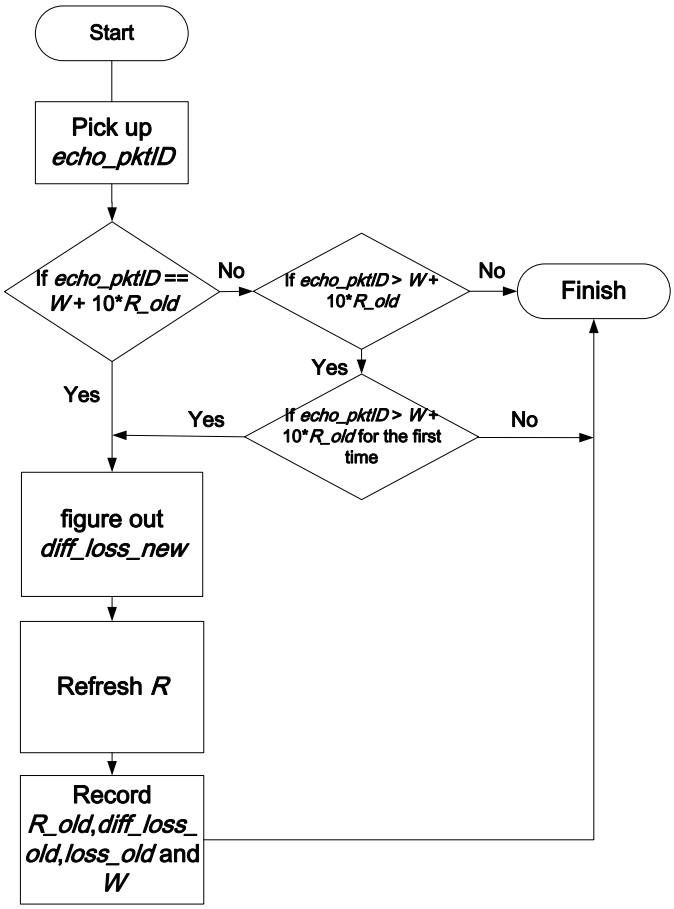


Figure 1. The algorithm to adjust the redundancy factor *R* in the sender

III. FAIRNESS OF THE NEW PROTOCOL

We use the network simulator-2 [14] to access the performance of different protocols in network. The topology for all the simulations is a tandem network consisting of 8 hops (hence 9 nodes), shown in Figure 2.

In this system, there are two flows generated by two FTP applications. One is from node 0 to node 7, and the other is from node 1 to node 8. They will compete for the intermediate channels and nodes. All the channels have a bandwidth of 1 Mbps, and a propagation delay of 10ms. The buffer size on the channel is set to 200. The TCP receive window size is set to 40

 ISBN: 978-1-61208-166-3

packets, and the packet size is 1000 bytes. The Vegas parameters are chosen to be α =28, β = 30, γ =2.

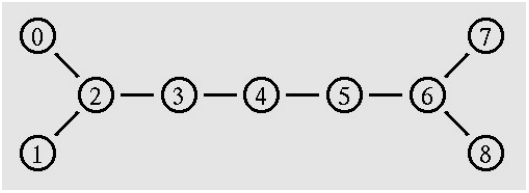


Figure 2. A tandem network consisting of 8 hops

By fairness, we mean that if two or more similar flows compete for the same channel, they must receive an approximately equal share of the channel bandwidth. In addition, this must not depend on the order in which the flows join in the network. It is well known that depending on the value chosen for α and β, TCP-Vegas could be unfair to an existing connection when a new connection enters the bottleneck link. In our simulation, we first choose a certain value of α and β (in this case, α =28, β =30) that allows fair sharing of bandwidth when two TCP-Vegas flows without our modification. Then, we choose the same value of α and β, and figure out the fairness characteristic under three different situations:

Situation 1: a TCP-Vegas flow competes with an SANC-TCP flow.

Situation 2: an SANC-TCP flow competes with another SANC-TCP flow.

Situation 3: five SANC-TCP flows compete with each other.

In Situation 1, the loss rate is set to 0%, and the SANC-TCP flow starts at 0.5s while TCP-Vegas flow is 200s later. The SANC-TCP flow ends at 800.5s, while TCP-Vegas flow ends at 1000.5s. The system is simulated for 1100s. The current throughput is calculated at intervals of 2.5s. The evolution of the two flows' throughput over time is shown in Figure 3 which indicates, when TCP-Vegas flow joins in the channel, it quickly shares an equal amount of bandwidth of the channel with the previous SANC-TCP flows, thus proving the fairness of new SANC-TCP.

In Situation 2, the loss rate is set to 0%, and one of the SANC-TCP flows start at 0.5s while the other one is 300s later, and they both end at 1000.5s. The system is simulated for 1100s. The current throughput is calculated at intervals of 2.5s. The evolution of the two flows' throughput over time is shown in Figure 4 which is similar to Figure 3. The latter flow quickly shares an equal amount of bandwidth of the channel with the former one after it joins in the system. This also demonstrates that the fairness of SANC-TCP.

In Situation 3, five different SANC-TCP flows start independently at 0.5s, 100.5s, 200.5s, 300.5s, 400.5s. According to the result showed in Figure 5, when each flow comes into the channel, they quickly share equal amount of the channel's bandwidth compared to others, and thus, it proves that the SANC-TCP is strictly fair.

IV. EFFECTIVENESS OF THE NEW PROTOCOL

Backed-up by the simulation, we now try to prove that our new protocol SANC-TCP has a better throughput rate and utilization of the channels under unknown lossy channels, compared to NC-TCP. In part A, we compare the throughput rate and the utility of three different protocols TCP-Vegas, NC-TCP, SANC-TCP under the same lossy channels, with different loss rate every measured time. For the NC-TCP, we set the redundancy factor at the optimum value corresponding to each loss rate. In part B, we set the redundancy factor to a constant number 1.11. The loss rate of the channels is varied from 10% to 45%. We will compare the throughput rate and the utilization of the channels between NC-TCP flow and SANC-TCP flow. Finally, in part C, we consider a situation called bursty loss situation, where there will be a sudden large loss rate for a short time in the system. We compare the performance of three different protocol flows under bursty loss situation.

Fairness

The topology setup is identical to that used in the fairness simulation, except that now we only use one FTP flow, which is from node 0 to node 7. We set the same loss rate on the channels between node 2 and node 6. For example, if we set loss rate to 0.1 on every channels between node 2 and node 6, we get the total loss rate $1-(1-0.1)^4 = 0.3439$. When simulation starts, the FTP0 flow starts at 0.5s, and the intermediate channels start to lose packet in a certain rate at 0.6s. The simulation time is set to 1000s.

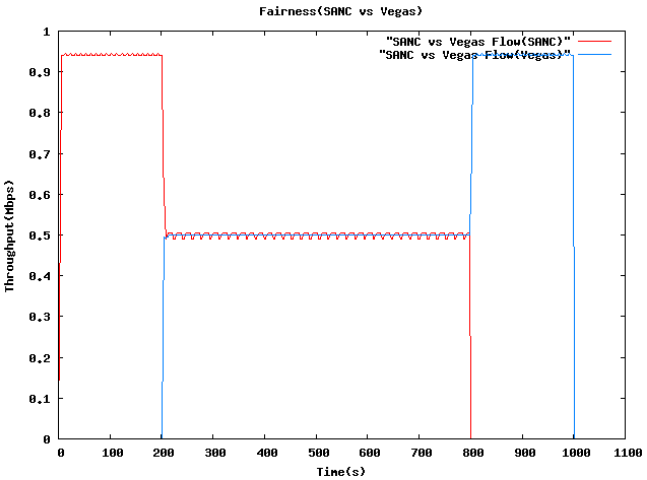


Figure 3. A TCP-Vegas flow compete with an SANC-TCP flow

 ISBN: 978-1-61208-166-3

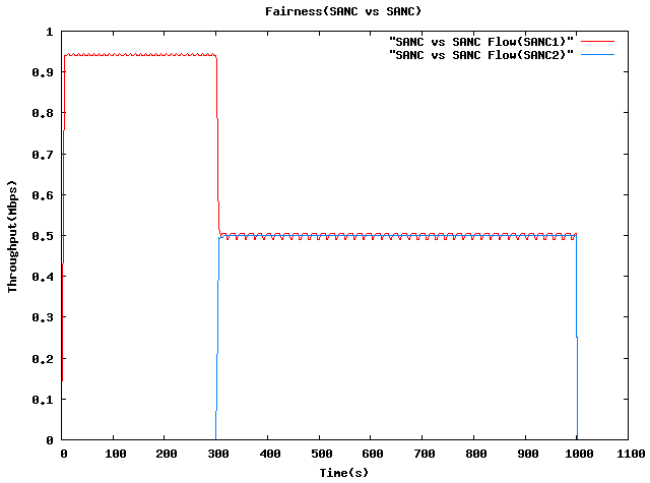


Figure 4. an SANC-TCP flow compete with another SANC-TCP flow

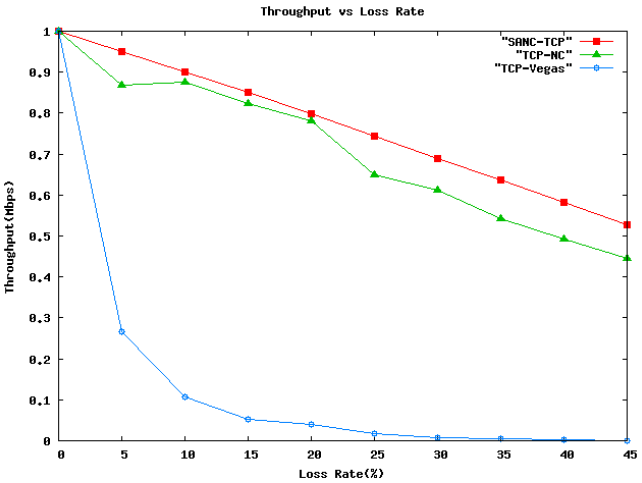


Figure 6. The throughputs of three different flows

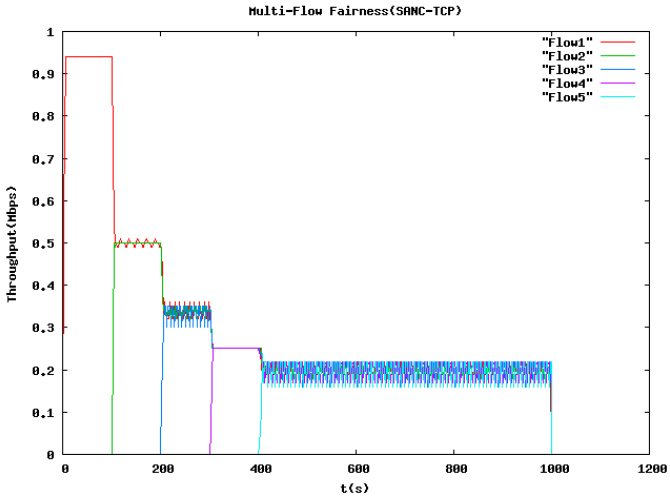


Figure 5. Five SANC-TCP flows compete with each other

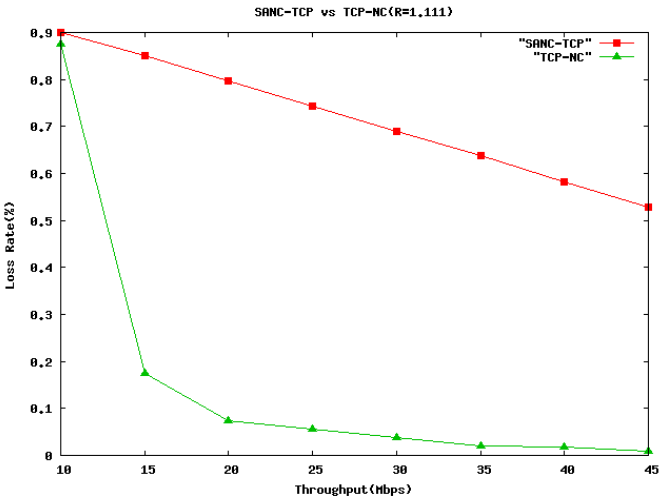


Figure 7. The throughputs of TCP-NC flow and SANC-TCP flow

Simulation results are shown in Figure 6. The X-axis represents the various loss rate, and the Y-axis represents the throughput rate corresponding to different loss rate. As we set the link capacity to 1 Mbps, the Y-axis can also represents the utilization of the channels. The blue line is referred to TCP-Vegas, the green line is referred to NC-TCP and the red is to SANC-TCP. To emphasize, under every different loss rate, the redundancy factor *R* is set to the optimal value. For example, if the loss rate is 20%, then the *R* is set to be 1 / (1-0.2) = 1.25. Figure 5 shows that, when the loss rate is 0%, the throughput of all three protocols almost reaches the optimal value 1Mbps. However, as the loss rate becomes larger, the throughput of TCP-Vegas descends drastically, while both NC-TCP and SANC-TCP are close to the theoretical value of maximum utilization of channels. For example, theoretical value of maximum utility of channels is 1Mbps * (1 – 20%) = 0.8Mbps when loss rate is set to 20%, as we can see NC-TCP and SANC-TCP are both close to it from Figure 6.

Effectiveness

In order to compare the throughput and utilization of the channel between NC-TCP flow and SANC-TCP flow under various loss rate, we set the R to 1.11 in NC-TCP flow case, while the other parameters of simulation environment are totally the same.

As is shown in Figure 7, The X-axis represents the different loss rate which is varied from 10% to 45%, and the Y-axis represents the throughput rate corresponding to different loss rate which can also be understood as utilization of the channel. The green line is referred to NC-TCP flow and the red one is to SANC-TCP flow. When the loss rate is 10%, NC-TCP flow requires high throughput with R equals to 1.11 as the optimal value and approximates SANC-TCP flow. However, as the loss rate becomes larger, the throughput of NC-TCP case descends drastically because it cannot mask the packet loss with the *R* value sticking to 1.11. Adversely, the throughput of SANC-TCP flow is close to theoretical value under every loss rate. For example, the theoretical value of maximum utility of the channel is 1Mbps * (1 – 30%) =

 ISBN: 978-1-61208-166-3

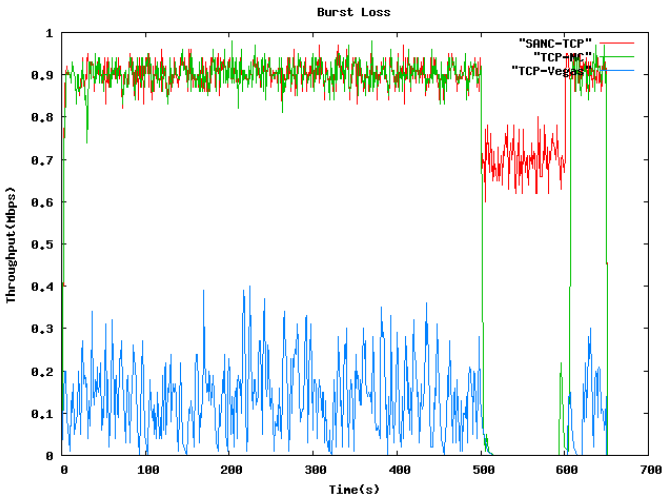


Figure 8. Bursty loss situations

0.7Mbps when loss rate is set to 30%, and the SANC-TCP flow is close to it. In addition, given *R* equals to 1.11, lots of packets will be sent unnecessarily which leads to low performance if there are more than one flow in the network when the loss rate is smaller than 10%. SANC-TCP adjusts *R* to the practical condition and maintains it at the optimal state which avoids wasting bandwidth.

Bursty

In real wireless networks, the loss rate is affected by various reasons. Sudden large loss, we call it bursty loss, is one of the phenomena that occur in the system. To evaluate the performance of the three different protocol flows under bursty loss situation, we set a circumstance where the loss rate of the system is kept as 10%, except for the time from 500s to 600s, the loss rate is changed to 30%. We use the same topology as Part A and Part B.

As is shown in Figure 8, the X-axis represents the simulation time, and the Y-axis represents the throughput or the utilization of the channel. The blue line is referred to TCP-Vegas flow, the green line is referred to NC-TCP flow whose redundant factor R is set to the optimal value of 1.11 and the red line is referred to SANC-TCP flow. During the time when the loss rate is kept in 10%, the NC-TCP flow and SANC-TCP flow can both nearly reach the theoretical value of the throughput. However, when the time comes to 500s, the loss rate is suddenly changed to 30% until 600s. According to Figure 8, NC-TCP flow suffers a lot during the time from 500s to 600s, the throughput is almost drop to 0. Comparably, the SANC-TCP shows its robustness to the bursty loss, and maintains the theoretical value of throughput during 500s to 600s.

V. CONCLUSION AND FUTURE WORKS

Network coding is an effective tool to fight against non-congestion losses. However, due to the different loss rate in different period of time in wireless networks, the NC-TCP with constant redundancy factor *R* cannot effectively solve the non-congestion losses problem by retransmitting redundant packets. In this work, we propose a new approach to dynamically adjust *R* to the real networks. As the redundancy factor *R* is no longer constant, we can change it according to the real current circumstance, thus better the performance under lossy networks where the loss rate is not constant.

For future work, we plan to focus on the encoding and decoding delay problem which stands in the way for the network coding technology to implement in the real system.

VI. ACKNOWLEDGEMENT

This work has been supported by 973 Program 2012CB315904; NSFC 60872010; SZJC201005260234A; SZZD201006110044A; GDNSF No.9150 6420 1000 031.

REFERENCES

[15]

[1] R. Ahlswede, N. Cai, S. Y. Li, and R. W. Yeung, "Network Information Flow," IEEE Trans. On Information Theory, vol. 46, pp. 1204-1216, 2000.

[2] T. Ho, "Networking from a network coding perspective," phD Thesis, Massachusetts Institute of Technology, Dept. of EECS, May 2004.

[3] J. K. Sundararajan, D. Shah, and M. Medard, "ARQ for network coding," in IEEE ISIT 2008, Toronto, Canada, Jul, 2008.

[4] S. Katti, H. Rahul, W. Hu, Databi, M. Mcdard, and J. Crowcrofg, "XORs in the Air: Practical Wireless Network Coding," in IEEE/ACM Transactions on Networking, 16(3): 497-510, June 2008.

[5] C. Fragouli, J.-Y. Le Boudec, and J. Widmer, "Network coding Aninstant primer," ACM Computer Communication Review, Jan. 2006.

[6] C. Fragouli, D. S. Lun, M. Medard, and P. Pakzad, "On feedback for network coding," in Proc. of 2007 Conference on Information Sciences and Systems (CISS 2007).

[7] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," in Proc. of Allerton Conference on Communication, Control, and Computing, 2003.

[8] S. Chachulski, M. ennings, S. Katti, and D. Katabi, "Trading structure for randomness in wireless opportunistic routing," in Proc. of ACM SIGCOMM 2007, August 2007.

[9] J. K. Sundararajan, D. Shah, M. Medard, M. Mitzenmacher, and J. Barros, "Network Coding Meets TCP," in IEEE INFOCOM, Apr 2009.

[10] S. Paul, E. Ayanoglu, T. F. L. Porta, K.-W. H. Chen, K. E. Sabnani, and R. D. Gitlin, "An asymmetric protocol for digital cellular communications," in Proceedings of INFOCOM, 1995.

[11] A. DeSimone, M. C. Chuah, and O.-C. Yue, "Throughput performance of transport-layer protocols over wireless LANs," IEEE Global Telecommunications Conference (GLOBECOM '93), pp. 542-549 Vol.1, 1993.

[12] H. Balakrishnan, S. Seshan, and R. H. Katz, "Improving reliable transport and handoff performance in cellular wireless networks," ACM Wireless Networks, vol. 1, no. 4, pp. 469-481, December 1995.

[13] J. Chen, W. Tan, and L. X. Liu, "Towards zero loss for TCP in wireless networks," in Performance Computing and Communications Conference(IPCCC), 2009 IEEE 28th international.

[14] "ns-2 Network Simulator," http://www.isi.edu/nsnam/ (Sep 20th, 2011)

 ISBN: 978-1-61208-166-3

Content Management Systems using Quality Transition Mode in Video Content Utilization Services

Mei KODAMA[*,**]
[*]Graduate School of Integrated Arts and Sciences,
Hiroshima University
[**] Information Media Center,
Hiroshima University
1-7-1-C112 Kagamiyama Higashi-Hiroshima, 739-8521 JAPAN
mei@hiroshima-u. ac. jp

Abstract—**Thanks to the recent improvements in speed and capacity of data networks, we observe a proliferation of network video content services. From the user's perspective more video requires more memory. To address this problem, we propose a new content management that uses cached delivery and scalable content. Our approach uses a data transition process of scalable structure, and is based on elapsed time and content usage parameters. We present the analysis of the efficiency of the new model.**

Keywords-Content Management Method; On-Demand Services; Video Data Structure; Data Transition; Video Quality.

I. INTRODUCTION

In recent years, video content delivery services by Video On-Demand: VoD are beginning to spread by the popularization of network and improvement of the speed. Moreover, the environment to play videos always is ready without accumulating in user terminals for these services, considering copyright. Generally speaking, in every aspect of content services, there some issues to enhance the efficiency of network management and content management. For examples, the way to solve the delay caused by collisions and retransmitting for large number of contents, the data management schemes and the prioritized transmission for multi-quality contents in heterogeneous environment to play them. There are some content provider sites, such as NicoNico-Douga [1] and YouTube [2]. Users, who are interested in the new content service using the network and streaming services by on-demand, are driving force of a service popularization. However, to solve the problems of the compatibility and the cooperation among some service systems is still insufficient, and there are some problems when they use their service in different systems. Considering the continuity of content services, an information management is one of the important tasks of communication technologies for their services. When the number of used contents exceeds a predetermined level, they have any problem because of the limitation of disk capacity. For example, it becomes very difficult to grasp the whole situation if the time passed, after they moved the content data to the external device. In other words, as they manipulate the information, which is beyond the ability of our memory because of the spread of the digital environment to make our communities more livable, we can say that there is a limit in the information management.

To increase the satisfaction of users for their services, the reduction of content providing costs and the service time is required. Thus, the problem of pricing method and the high efficiency of contents distributed systems based on the priority orders had been studied [3][4]. On the other hand, we had studied about the cache delivery method considering the priority for each content [5] and content management system using scalable architecture [6]. In this paper, we paid attention to the contents management method in contents services of multiple qualities, and present the method using scalable structure and distribution systems supported quality. In this study, we propose video content management methods for multiple qualities. The overview of proposed schemes and the utilization models are explained. Finally, the efficiency is considered.

II. PROPOSED MANAGEMENT METHOD

When the opportunity to use the content service increases, the management method is one of the important problems in video content distributed systems. In order to be able to play contents of multiple qualities quickly and browse them for heterogeneous terminals for video resolutions, it is needed that users keep them in user terminals themselves. Here, the number of layered structure is set to two. First, information data of proposed system is defined. In this system, we use content data and index information. Data structure is scalable, and index data has IDs, qualities, usage time and so on.

A. Data transition process

We explain the data transition method which is used in management systems. Generally, they use the reduction method for disused contents to save their contents in local hard disk of users' terminals, which have limited storage capacity. If the system does not have the functionality of the auto reduction, we cannot record our video clips, or the scheduled program does not work well. From the viewpoint of the user terminal, the condition of this system is considered. Users want to keep as many contents as possible themselves after purchase, because they watch some contents at any time and they would like to play some contents again. They think that the convenience of service is important. Moreover, they require the model that the lack of information can be acquired quickly by on-demand services. The re-use contents' data should be reduced temporally, or moved to the other device.

 ISBN: 978-1-61208-166-3

For these issues, in this study, the whole data of the content is not reduced, but the part data of its content only is done by scalable structure. We use scalable video coding architecture, such as, spatial scalability, SNR scalability and temporal scalability, etc. in international coding standard MEPG-2, MPEG-4 [7][8][9]. The gradual data by data transition process consists of layered coding architecture and the procedure of data transition is proposed and adapted to the content management system.

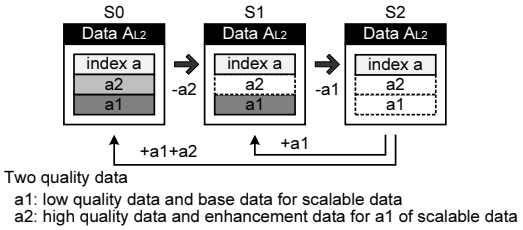


Figure 1. Data transition of scalable structure

Fig. 1 shows the data transition process and their status. The status S0 shows the data structure of high quality, H and I. H is two layered data, and it has base layer of low quality (a1) and enhancement layer of high quality (a2). L is only a1 for low quality. I information is index information. The data structure is lower quality progressively from left to right. The right status has only index information. In addition, there are the number of layer for content quality, current status of data and content data itself, as management information. According to the order of contents' priority, we reduce the data quality and its data structure is changed from the original data structure of used data to right data. On the other hand, if users access to high quality, the status is moved to the left side. Here, scalable structure can adapt to the different quality representation for heterogeneous terminals.

B. Procedure of data transition

The procedure of data transition is explained. The determination process of data transition uses the value function and the status of local disk space. The order calculated by the value function also decides the reduction scheme in the management method. The definition of basic priority function based on data transition of scalable data structure according to elapsed time is shown by Fig. 2.

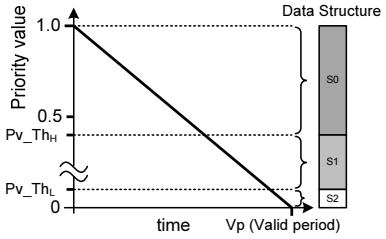


Figure 2. The priority function based on the elapsed time and the status of data structure

We simply show that the figure indicates monotonic decrease. It also shows that the value is related to the elapsed time. The longer the elapsed time from the access time is, the lower its value is. When they use the high quality content, the data status becomes S0. Meanwhile, when low quality, it becomes S1. When they do not use them periodically, it is S2. It is the model when the number of use increases, the value is high.

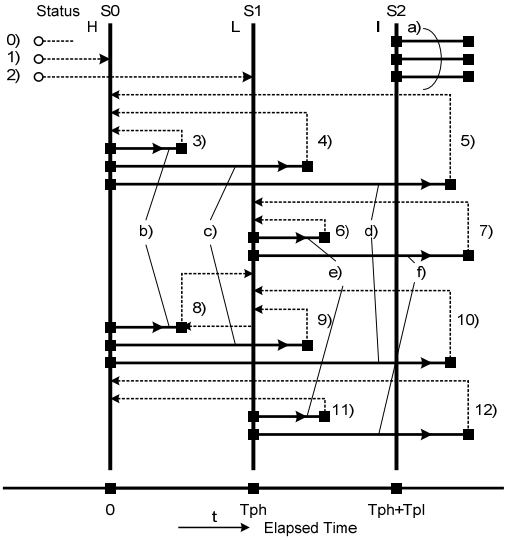


Figure 3. Updating process of used elapsed time for some quality contents and transition state

Final data transition is determined by the judgment of the priority calculated by the value function, some thresholds, and the utilization condition of local disk in user terminal. According to the space of local disk, it is decided whether the action actually is performed or not. The content status transits from high level to low level, S0, S1, S2 in turn, based on the order of the priority. Actually, the reduced target content is calculated by usage history of contents and the frequency of use. At this time, the utilization time table is used, and the priority order becomes low for long term of elapsed time. The high level transition is based on the usage of high quality. Fig. 3 shows the relationship of updating process of elapsed time from used time for some quality and transition state. The horizontal axis shows an elapsed time, and repeated use is important to keep the data status in local device. The upper data level is decided by use of the high quality. In this figure, a)-f) show the transition status after use, and 0)-12) show the updating status of quality selection. The group of a) shows S2 of initialized data. b): S0, c): S1, d): S2, e): S1, f): S2, g): S1. On the other hand, 0): No use, 1): High quality use, 2): Low quality use. 3) 4) 5) 11) 12) show that stored data return to the S0 structure after data transition, respectively. 6)-10) also show that stored data return to the S1. For instance, in 3), when they use H, the status is S0 and t=0 is set.

C. Procedure of data management method

Next, the content management procedure in local disk of user terminal is shown by Fig. 4. We simply explain the flow.

In a periodical time, we check the number of the contents and the disk space in local disk. However, in the case where the content does not exist in local device and in the case where the data space is sufficient, the data transition process is suspended. The order of the content priority is calculated by some information, such as, usage history, frequency, quality, and the value function using elapsed time. We treat the current

 ISBN: 978-1-61208-166-3

time and the used time of contents, and manage the time information and disk space for stored contents. The target number of reducing is calculated by disk space, and the data transition process is repeated until the disk space of new contents satisfies a threshold value. Finally, the content management method based on data transition is useful. You can see that the old contents, which are not available, are reduced in local disk. Here, these processes are treated as the first process at stated intervals. Some samples of the parameters of target contents are shown. Content data size: D_p[bit], Quality: H:*a1+a2*, L:*a1*, *a1=a2*, the disk capacity in user terminal: S[bit]. For x[week], N_u: the summation of the number of usage, y:limited number, C_{ux}: the number of usage in one interval. The check functions of the number are defined by countH, countL, countI for high, low data and index information respectively. In this study, we put the frequency ahead of the elapsed time and the priority function is used for renewal period. If the renewal period is long, the frequency information is important. Meanwhile, if it is short, the time data is considered. The detail setting of the function is the further study.

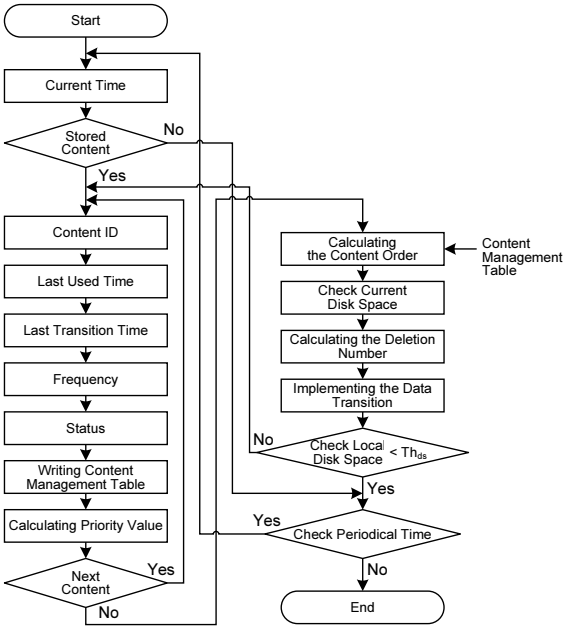


Figure 4. The procedure of content manage method

$$\begin{cases} Pc(x) = countH(x-1) + g\ countL(x-1) \\ \quad -y + k \cdot N_u\ (x-1)/(x-1) \\ N_u(x-1) = \sum_{n=1}^{x-1} Cu_n \end{cases} \quad (1)$$

The calculating function of the target transition number: Pc(x) is defined by equation (1). Here, g = a2/(a1+a2)=1/2. In this function, when *Pc(x)>0*, the data transition process is performed according to the rank of the priority. Otherwise, the process is suspended.

III. CONTENT USAGE MODEL

The content utilization services and the usage models are described.

A. Service model

We think two hierarchical qualities as the content services. In high quality video, users watch home-TV in large-sized monitor, and they use mobile-TV in low quality video. In addition, when they also browse video contents, low quality data is used. They become a member of either-or content service of the quality, or both. Here, when they download the content, which is required, after the data is temporally stored in home server, it moves to user terminal, such as, home TV terminal and mobile TV terminal. That is to say, the home server relays their contents to user terminals.

We can consider that there are three utilization forms, UT_m, UT_n and UT_o for two qualities as services models. In this figure, the gray color means no members. Moreover, once users store the contents in local disk of user terminals, they play them. The service model is shown by Fig. 5.

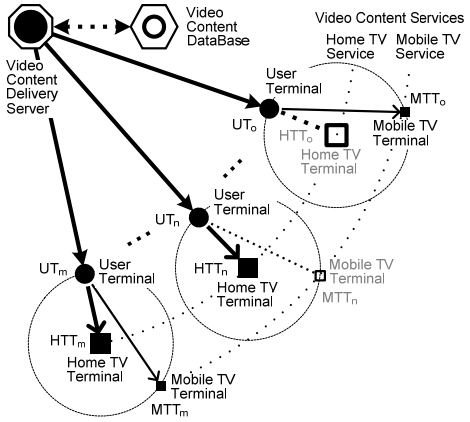


Figure 5. Service model

B. Utilization model

In this service, the simple access model for multi-quality selection is defined by Fig. 6. Users start utilization services, and browse the content list. After that, they actually browse some contents shortly. If you need the contents to browse them, the contents in local disk are retrieved. However, if not, the contents are downloaded from the server. They select the content number, and the quality in the determination processes. If they can find that in local terminal, they proceed to the play process. If they cannot, they proceed to the next process. They check the status of contents and the quality in local terminals. After the content search, calculating process of the different data and data transmission in turn, they update the status and index information for the content management. In the data exchange between the server and clients, once they execute login procedures, they access to the server. After they retrieve the contents by download process, they play them at any time. If they repeat to select, they return to browse. Otherwise, they finish the service. Moreover, we suppose that this system has two information management processors in both the server and user terminals. They can exactly know the current status of the contents, the frequency and the elapsed time from the access time for every user. Therefore, the status by scalable structure is changed according to the elapsed time and the utilization of the quality.

 ISBN: 978-1-61208-166-3

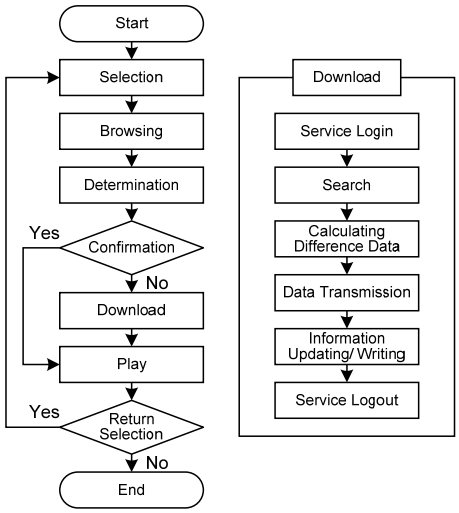


Figure 6. Access model

IV. CONSIDERATION

Firstly, we define the utilization condition in proposed method. Next, the efficiency of this system is considered.

A. Conditions

Suppose that this system transmits the contents to each Terminal (HTT, MTT in Fig.5) for each quality. One of users plays the required content according to the above statement. We assume that he uses them in quantities of C_u units of average times per an interval, and the quantity of servers' contents is enough to use. However, we do not treat the user tastes of the contents in this study. The number of browsing the contents is z units, before selecting. The number of z is depended on usage history and the status of storage. Moreover, he uses the low quality data each to browse them, which are stored in local disk. When the data is not stored in the local disk, the part of content data corresponding to only browsing is transmitted from the server to the user terminal. The amount of content information is D_p[bit], the play time is D_a[s] and the browsing time is D_b[s]. The speed of transmission for users is W[bps].

$$\begin{cases} T_{service} = T_{selection} + T_{browsing} + T_{Determination} \\ \qquad\qquad + T_{confirmation} + T_{Download} \\ T_{download} = T_{search} + T_{datatransmission} + T_{updating} \end{cases} \quad (2)$$

Next, the required time of retrieving service is defined bellow. It does not have the play time, and he plays the content, after the download process. As the required times which everyone cannot ignore, there are browsing time and data transmission time. The browsing time of T_p is shown by $D_b \cdot z$. The transmission time to play one content is D_p/W, the transmission time to browse it, T_b is shown by $T_b \leq z \cdot D_b/D_a \cdot D_p/W$ and $T_{browsing} = T_b + T_p$. Therefore, the summation shows the whole service time. It is the point that the rate of retrieving the low quality of stored content and the hit ratio are intimately related to the service time. The other processing times are ignored. The service times are described by equation (3).

$$\begin{cases} T_{service}1 = z \cdot D_b + \left(z\dfrac{D_b}{D_a}D_p + D_p\right)/W \\ T_{service}2 = z \cdot D_b + \left\{(z - z_h - 1)\dfrac{D_b}{D_a}D_p + D_p\right\}/W \\ T_{service}3 = z \cdot D_b + \left\{(z - z_h)\dfrac{D_b}{D_a}D_p + D_d\right\}/W \\ D_d = \begin{cases} 0 & (D_p \in S0) \\ g\,D_p & (D_p \in S1) \\ D_p & (D_p \in S2) \end{cases} \end{cases} \quad (3)$$

The service time 1 shows the case of no hit of use history. The second is shown that the content of use does not match the download content, but it hits the browsing contents. The third is shown that it matches the browsing contents without the download content. You can know that D_d of amount of the transmission data is changed by the status. z_h is the number of hit contents. If the service time is long, the cost is high. When we consider the situations, we divide into two main cases, the case of utilization of single quality, and the case of utilization of multiple qualities both. In this study, theoretical approach is explained, but the experimental approach is future tasks.

B. Single quality use

This case is applied to the situation of UT_n, UT_o defined by the service system. In single quality use, L has two transition statuses and H has three transition statuses. The former boils down to the problem whether the contents are cached or not. On the other hand, the latter is related to the solution whether it is efficient or not when the part data of the contents is cached.

At first, we consider the first problem to simplify the problem. It is indicated that the management method using the frequency of use is generally useful by reference [5]. Meanwhile, it is the point whether the efficiency of caching method partly can be expected. Here, data size of a1 is the same as a2.

Here, for example, we consider the model in a uniform access model as content services. In this case, the every probability of the content is the same. Therefore, if the status of H moves to the a1, the rate of occupation in the used contents is reduced by half.

We consider the uniform model in detail here. The frequency function of content hit ratio is uniform and the smaller the amount of transmission data is gradually, the larger the probability is. The summation of the transmission for no hit content is defined by next equation.

$$g(p) = D_{Tra}(0,N)(1-p) = A(1-p) \quad (4)$$
$$A = D_{Tra}(0,N)$$

$$h(p) = (1-p)D_{Tra}(0,N) + pD_{Tra}(1, \quad N) \quad (5)$$
$$= A(1-p) + Bp$$
$$A = D_{Tra}(0,N), \quad B = D_{Tra}(1,N)$$

The equation of the ratio of hierarchal data is shown.

$$f(p) = (1-q)g(p) + qh(p) \quad (6)$$

Therefore, when we use Px, Py, the function are described.

$$f(P_x, Q_x) = (1-Q_x)\,g(P_x) + Q_x h(P_x) \quad (7)$$
$$f(P_y, \quad Q_y) = (1-Q_y)\,g(P_y) + Q_y h(P_y) \quad (8)$$

The difference function r(P) between h() and g() shows next equation.

$$r(P_x) = h(P_x) - g(P_x) \quad (9)$$
$$= A(1-P_x) + BP_x - A(1-P_x) = BP_x$$

We arrange the conditions for above mentioned situation. The hit ratio of cached content by structure G is constant.

$$r(P_x)(1-Q_x) = r(P_y)(1-Q_y) \quad (10)$$
$$BP_x(1-Q_x) = BP_y(1-Q_y)$$
$$\therefore\ P_x = \frac{1-Q_y}{1-Q_x}P_y, \quad P_y = \frac{1-Q_x}{1-Q_y}P_x$$
$$Q_y = 1 - \frac{1-Q_x}{P_y}P_x, \quad Q_x = 1 - \frac{1-Q_y}{P_x}P_y$$

Here, the amount of content itself is defined by $D_G = D_{SS}$.

$$D_{SS} = D_L + D_H \quad (11)$$

The summation of the transmission used hierarchical hit ratio P_{ss} for the number of n is described.

$$D_{Tra}(0,N) = \sum_{n=1}^{N} D_G(n) = ND_G \quad (12)$$
$$D_{Tra}(1,N) = \sum_{n=1}^{N} D_H(n) = ND_H$$
$$A = ND_G, \quad B = ND_H$$
$$\therefore\ A = \frac{D_G}{D_H}B$$

There are the similarity relationship between the gained number of hit ratio and the rate.

$$r(P_x)Q_x \times P_xQ_x\frac{D_H + D_L}{D_L} = r(P_y)Q_y \times P_xQ_x \quad (13)$$
$$\therefore\ P_y = \frac{Q_x(D_H+D_L)}{Q_yD_L}P_x$$

By equation (10)(13),

$$P_y = \frac{1-Q_x}{1-Q_y}P_x, \quad P_y = \frac{Q_x(D_H+D_L)}{Q_yD_L}P_x \quad (14)$$
$$\therefore\ Q_y = \frac{Q_x(D_H+D_L)}{D_HQ_x + D_L}$$

The condition of advantage of hierarchical allocation method is $g(P_x) \geq f(P_y, Q_y)$. This means that the transmission data after moving is able to be reduced. The summation D_{Tra} of the transmission in each content is defined by the function f() for the change of structure allocation.

$$g(P_x) - f(P_y, Q_y) = A(P_y - P_x) - BQ_yP_y \quad (15)$$

If equation (13)(14) are used,

$$= A\left(\frac{Q_x(D_H+D_L)}{Q_yD_L}P_x - P_x\right) - BQ_y \times \frac{Q_x(D_H+D_L)}{Q_yD_L}P_x \quad (16)$$
$$= P_x\left\{A\left(\frac{Q_x(D_H+D_L)}{Q_yD_L} - 1\right) - B\frac{D_H+D_L}{D_L}Q_x\right\}$$
$$= P_x\left\{A\left(\frac{Q_x(D_H+D_L)}{\frac{Q_x(D_H+D_L)}{D_HQ_x+D_L}D_L} - 1\right) - B\frac{D_H+D_L}{D_L}Q_x\right\}$$
$$= P_x\left\{A\left(\frac{D_HQ_x+D_L}{D_L} - 1\right) - B\frac{D_H+D_L}{D_L}Q_x\right\}$$
$$= \frac{P_xQ_x}{D_L}\{AD_H - B(D_L+D_H)\} \quad \geq 0$$
$$\therefore\ A \geq \frac{D_H+D_L}{D_H}B$$

Thus, $D_G \geq D_L + D_H$ by equation (12)(16). You can know that the equality only meets conditions. We consider this condition is not available for hierarchical data. Figure 7 shows the relationship between transmission data and the probability of hit contents for cached contents. In this figure, the larger the ratio of hierarchical allocation is, the larger the summation of the transmission data by the probability of access. On the other hand, the smaller the ratio of hierarchical allocation, the lower the vertical value is. The higher the transmission data is for vertical axis, the larger the probability of hit is. In the other word, if q is bigger, there is the space of disk for cached contents, and the number of stored contents is larger. Therefore, the status is moved to right point. Meanwhile, the lower the transmission data is, the smaller the hit rate is because of decreasing scalable data. Since the movement by decreasing is occurred according to the slope of g(t), the gradient is high and the rate of increasing the summation is also high. However, you can understand that there is no transition of scalable data structure for the condition.

This case is the uniform access model of used contents. Thus, the equal access for each content if you use the limited capacity of cached disk, full cached data structure is good. That is to say, it is better when non scalable structure is used.

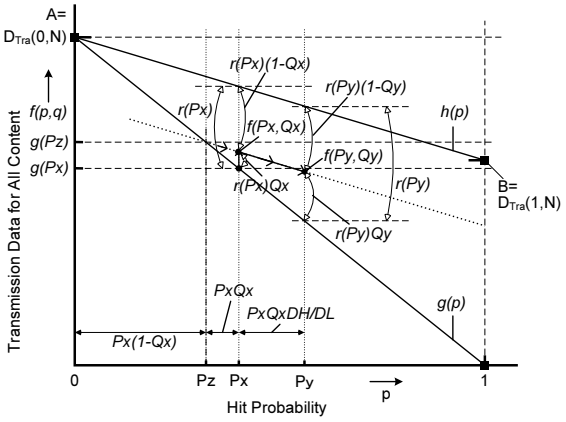


Figure 7. Relationship between transmission data and the probability of hit contents for cached contents

Consequently, to have an advantage, the processes only have to double the hit ratio. However, the ratio is not more than twice in theory. Thus, there is no case when the efficiency of the transmission is improved. Next, we take up the model that the popularity of content access centers on some contents. In the same way, even if the number of stored contents is increased, the efficiency is not more useful. However, you can know that the browsing time is shorter by these processes. As mentioned above, for the purpose of reduction of data transmission, this system is insignificant.

C. Multiple qualities use

This case is applied to the situation of UT_m defined by the service system. We do not treat the situation of single quality for services.

By Fig. 3, there are two cases that they use the low quality after high quality: 8) 9) 10), and that they use the high quality after low quality: 11) 12). When the status S1 is changed to S0, it is the same as previous study [6]. It showed that the transmission of the difference data is efficient in content

distribution systems. Moreover, the statuses of the actual transition are 10)11)12). T_e is defined as the elapsed time from the request of the content in 10). Considering the transition time, $T_e \geq T_{ph} + T_{pl}$.

The way we can meet the conditions in 11) 12) is to set that T_{pl} is larger. We can say that it is available, if they reuse and browse the contents while the elapsed time is less than T_{pl}. Consequently, if we define that T_{pl} is larger than $T_{ph,}$ the probability of contents' hit is higher and this system has an advantage of data transition. In this way, considering the worth of time domain, if this system manages the content and the information for the quality, it is better than previous study, which uses the independent data for some multiple qualities. We can summarize that the efficiency of the data management is not expected by data transition process for only a member of Home TV. It is the same way in Mobile TV. On the other hand, if both qualities are used, when the number of the used content is hit for valid period of the status, or when the used content is matched to the browsing one, this system is more available by proposed methods. Since we can use that stored data to browse the content, the cost of service is lower.

V. CONCLUSIONS

In this paper, we proposed the content management method using data transition for multiple qualities in video content distributed system. Users freely use the content for multiple qualities, and the elapsed time is used to reduce the unnecessary data in proposed methods. We explain the procedure of data transition, and consider the cases of the improvement of convenience and the low cost.

In prospective conditions of the number of low quality used contents, when they use the content of multiple qualities, if the transition time is set to be long, proposed method is efficient. In addition, when they do not use the multiple qualities, it cannot be expected to reduce the transmission data. However, there is some advantage of browsing.

As the further studies, we continue to consider the detail models for multi-quality video, and evaluate the proposed system using access models in some experiments.

REFERENCES

[1] NicoNicoDouga : ” http://www. nicovideo. jp/” .

[2] YouTube: ”http://www. youtube. com/”.

[3] T. Kamae, H. Numata, N. Sonehara:”Pricing and Disclosing Scheme of Digital Contents for Sale”, Trans. on IEICE D, Vol. J91-D, No. 1, pp. 12- 22 (Jan, 2008).

[4] E. Takahashi, N. Yagi, K. Yamori and Y. Tanaka:”Content Delivery System by Using Market-Based Priority Control”, Trans. on IEICE B, Vol. J88-B, No. 6, pp. 1047-1057 (Jun, 2005).

[5] M. Kodama:"Video Content Mangement Methods using Time Value Function", IIEEJ , Vol. 40, No. 2, pp. 345-354 (Mar, 2011).

[6] M. Kodama and S. Suzuki:"Video Contents Cache and Delivery Method with Scalability Architecture for Selecting Multi-Quality Video", ITE, Vol. 59, No. 7, pp. 1020-1032 (Jul, 2005).

[7] ISO/IEC 13818-2, Information technology – Generic coding of moving pictures and associated audio information: Video, Recommendation H. 262 (1995).

[8] ISO/IEC 14496-2, Information technology - Coding of audio-visual objects - Part 2 (1999).

[9] ISO/IEC 14496-10, Information technology - Coding of audio-visual objects - Part 10: Advanced Video Coding (2006).

 ISBN: 978-1-61208-166-3

A Practical Implementation of Fountain Codes over WiMAX Networks with an Optimised Probabilistic Degree Distribution

Jaco du Toit and Riaan Wolhuter
Department of Electrical and Electronic Engineering
Stellenbosch University
Stellenbosch, South Africa
e-mail: 14409607@sun.ac.za, wolhuter@sun.ac.za

***Abstract*—Recently, rateless codes have attracted much attention in the communications research community. The most well known being Luby transform codes, were the first practical realisation of record-breaking sparse-graph codes for binary erasure channels. These codes have the advantage of not requiring a priori knowledge of specific channel conditions and lends itself to application in nondeterministic wireless networks. This paper revisits the Luby transform fountain code, predecessor of the well known Raptor codes, and proposes a novel parameterised probabilistic degree distribution, which is used in the encoding process, along with the belief propagation decoding algorithm. By combining piecewise-defined convex functions and running a non-symmetric Kullback-Leibler divergence measure between the expected and actual degree distributions, we optimise our degree distribution and substantiate a significant reduction in reception overhead and symbol operations. This will support such forward error correction codes in efficient multimedia communication systems. Our proposition was implemented over a WiMAX network and the practical results obtained indicate that a few conditions are sufficient to define an optimal encoding process.**

Keywords-Rateless Codes; Universal Codes; Belief Propagation; Parameterised Degree Distribution.

I. INTRODUCTION

Binary linear rateless coding is an encoding method that can generate potentially infinite parity check bits for any given fixed-length binary sequence as they do not have a fixed rate as the case for conventional codes. Fountain codes constitute a class of rateless codes, which were first discovered in by Luby. [1] Luby Transform (LT) codes are linear rateless codes that transform k information symbols into infinite coded symbols. Regardless of the statistics of the erasure events on the channel, we can send as many encoded packets as needed in order for full recovery of the source data. Typically $N = k(1 + \varepsilon)$ packets are needed to successfully decode the original input message with a certain degree of probability where ε is the overhead. Each encoded symbol is generated independently and randomly, where the randomness is governed by the so-called Robust Soliton distribution. Luby's main theorem proved that there exists bounds around the belief propagation decoding failure probability as a function of reception overhead, that for a value c given N received packets, the decoding algorithm will recover the k source packets with probability $1 - \delta$. [1] [8] For large k (thousands), the Robust Soliton distributions have shown good performance. For smaller k Markov chain approaches have been implemented, which also showed good results. One conclusion to this study was that in a well-chosen parametric form of the degree distribution, just a few parameters need to be tuned in order to get maximal performance. [3] Given the work already done, optimal forms of parameterised degree distributions for different message lengths continue to provide an interesting problem. In this paper we will investigate a new parameterised degree distribution shaped by convex functions and test its performance on a WiMAX network in real world scenarios, where random channel noise introduce packet loss.

The rest of this paper is organised as follows: In Section 2, we review the theory of rateless encoding and believe propagation (BP) decoding, in particular the LT process and probabilistic degree distributions (PDD). In Section 3, we present our proposed optimised degree distribution, utilising a set of piecewise convex functions shaping the ideal degree distribution to an improved solution as presented in literature, after reviewing related performance enhancing methods. We analyse the computational cost, and performance of our proposition in Section 4 and show results of emulation and practical implementation of our suggested solution. We finally state our conclusion and future work in Section 5.

II. PRELIMINARIES

A. LT codes

LT codes proposed by Luby in 1998 are the first codes fully realising the digital fountain concept. [1][4] They are rateless, i.e., the number of generated encoded packets are potentially limitless, and encoded symbols are generated on the fly. [8]

1) Encoding of LT code: Randomly choose the degree $\boldsymbol{d}$ of the packet from a key element in the process, the so-called *degree distribution*. The encoded symbol is then generated by choosing $\boldsymbol{d_n}$ blocks from the original file uniformly at random. The value of the encoded symbol is the bitwise exclusive-or of the $\boldsymbol{d_n}$ neighbours. The encoding operation defines a irregular sparse graph connecting encoded symbols to source symbols.

2) Decoding of LT codes: Decoding is done iteratively by using the Belief Propagation decoding algorithm. First we *release* a encoded symbol of degree-one, with *complete certainty*, and subtract the connected symbols from each received packet by taking an exclusive-or between the packet and the known symbols. This procedure removes all edges connected to the source packets and is repeated until all source symbols are recovered. The set of covered input symbols that have not yet been processed is called the ripple. This process is well illustrated in most fountain code

 ISBN: 978-1-61208-166-3

literature. [5][6][8] Algorithm 1 and 2 demonstrates the encoding and decoding procedures respectively.

Algorithm 1: LT Encoding

1: **repeat**
2: choose a degree d from degree distribution *p(d)*
3: choose uniformly at random d input symbols $n(i_1)$,.,$n(i_d)$.
4: calculate value $n(i_1)$ xor $n(i_2)$ xor ... xor $n(i_d)$
5: **until** stop bit received

Algorithm 2: LT Decoding

1: **repeat**
2: **if** d = 1 packet in buffer
3: n(j) ← recover j
4: **for all** n(j) in buffer : v includes n(j) **do**
5: d ← d - 1 (reduce degree)
6: v ← v xor n(j) (update value)
7: **end for**
8: **until** all input symbols recovered

The complexity of BP, prominent in the decoding of LT codes, is essentially the same as the complexity of the encoding algorithm [1] i.e., there is exactly one symbol operation performed for each edge in the bipartite graph between the source symbols and the encoded symbols during both encoding and decoding. Therefore, the computational complexity of this algorithm is linear in the average degree of the degree distribution multiplied by the size of the source block. [6] BP will, however, fail when output nodes of degree-one exhaust and various algorithms i.e., Gaussian Elimination (GE) have been suggested [5][8][11] to counter this failure. However, this adds undesirable running time where fast decoding is required, especially for large matrices. For small code block lengths GE could be used efficiently, since BP requires a larger overhead for small block sizes. For this reason it is extremely important to find a degree distribution to effectively reduce reception overhead and the number of symbol operation for any block size.

B. Degree Distributions

The LT process described in [1] helps explain the design and analysis of a good degree distribution for the LT codes by comparing the process to the well known balls in bins problem, where encoded symbols are analogous to balls and input symbols are analogous to bins. The analysis of this problem shows that $\mathbf{N = k\ln(k/\delta)}$ balls are needed on average to ensure that each of the $\boldsymbol{k}$ bins is covered by at least one ball, with probability at least $\mathbf{1-\delta}$. This classic process can be viewed as a special case of the LT process, where all encoded symbols have degree-one and released simultaneously. It is shown in [1] that the Ideal Soliton distribution in (1), ensures that just over $\boldsymbol{k}$ encoding symbols with the sum of their degrees being $\boldsymbol{O(k\ln(k/d))}$ will suffice to cover all $\boldsymbol{k}$ input symbols and produces the least number of symbol operations.

Luby further explained that the goal of the degree distribution design is to slowly release encoding symbols as the process evolves and to keep the ripple size small to prevent redundant coverage. The ripple should also be large enough to prevent it from disappearing prematurely. An ideal property required by a good distribution is that input symbols are added to the ripple at the same rate as they are processed. The Ideal Soliton in Fig. 1 displays this desired behaviour.

$$\rho(d) = \begin{cases} \frac{1}{k}, & d = 1 \\ \frac{1}{d(d-1)}, & d = 2,3,\ldots,k \end{cases} \quad (1)$$

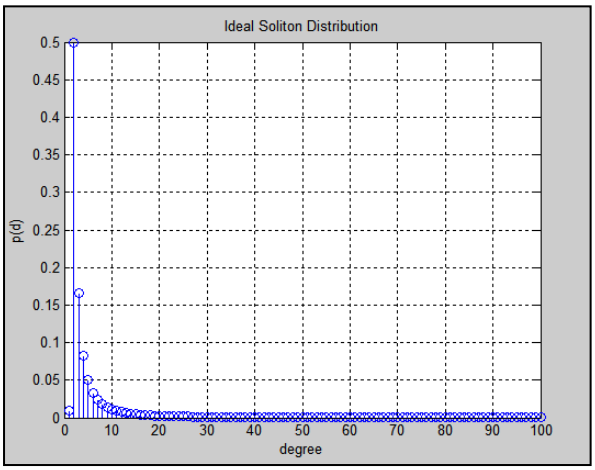


Figure 1: Ideal Soliton degree distribution for k = 100 input symbols.

The expected degree of an encoding symbol for this distribution is the harmonic sum up to $\boldsymbol{k}$:

$$\sum_{d=1}^{k} \rho(d) \approx \ln(k) \quad (2)$$

This means that in order to cover all the input symbols the degrees of all the encoding symbols needs to be around $\boldsymbol{k\ln(k)}$ and the Ideal Soliton compresses this into the least number of encoding symbols possible. This distribution, however ideal in theory, turned out to be quite fragile in practice, since the slightest variation in its expected behaviour can cause the ripple to disappear prematurely.

The Robust Soliton distribution from [1] ensures the ripple size stays large enough at each decoding step so that it never disappears completely and that few released encoding symbols are redundantly covered by input symbols already in the ripple. The Robust Soliton distribution (3) was designed so that the expected ripple size is roughly $\mathbf{\ln(\frac{k}{\delta})\sqrt{k}}$ throughout this process. Let $\mathbf{R = c\sqrt{k}\ln(\frac{k}{\delta})}$, where $\boldsymbol{c}$ is some suitable constant of order one.

$$\tau(d) = \begin{cases} \frac{R}{dk}, d = 1,\ldots,\frac{k}{R} - 1 \\ \left(\frac{R}{k}\right) ln\left(\frac{R}{\delta}\right), d = k/R \\ 0, \quad d = \frac{k}{R} + 1,\ldots,k \end{cases} \quad (3)$$

The small-$\boldsymbol{d}$ end of $\boldsymbol{\tau}$ ensures that the decoding process starts with a reasonable ripple size and the larger spike at $\mathbf{d = k/R}$ ensures all source packets are connected, keeping the ripple large enough. The expected number of encoded

 ISBN: 978-1-61208-166-3

packets required at the receiver to ensure that the decoding can run to completion, with probability 1 - **δ** has now increased to **N = *k*Z**. Where the normalising factor becomes $\mathbf{Z} = \sum_{\mathbf{d}} \mathbf{p(d)} + \boldsymbol{\tau}\mathbf{(d)}$. The Robust Soliton distribution is shown in Fig. 2.

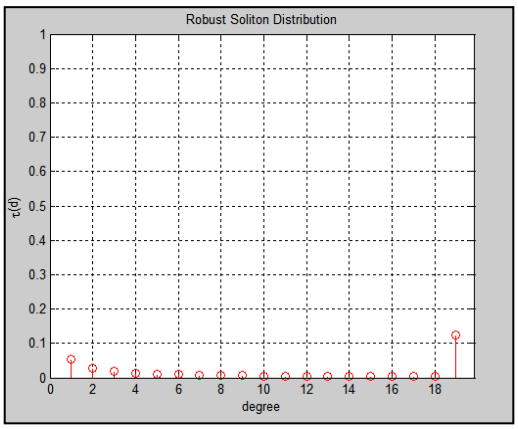


Figure 2: Robust Soliton degree distribution for k = 100, c = 0.1 and δ = 0.5.

Theoretical analysis of the properties of the Robust Soliton distribution is given in [1] where pessimistic estimates was used to prove the amount of encoding symbols necessary for full recovery of an input message. This was simplified to be $\mathbf{N = k + } \boldsymbol{O}(\sqrt{\mathbf{k}}\,\mathbf{ln}\,(\frac{\mathbf{k}}{\boldsymbol{\delta}})^{\mathbf{2}})$ and the average degree of an encoding symbol was shown to be $\mathbf{D} = \boldsymbol{O}(\mathbf{ln}(\frac{\mathbf{k}}{\boldsymbol{\delta}}))$. A typical Robust Soliton distribution, normalised using (4), is illustrated below in Fig. 3.

$$\mu(d) = \frac{(\rho(d)+\tau(d))}{Z} \qquad (4)$$

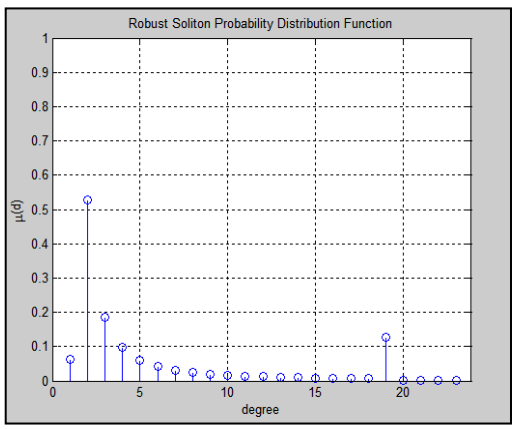


Figure 3: Robust Soliton degree distribution for k = 100, c = 0.1 and δ = 0.5.

A lot of previous work studying the various performance aspects of LT codes and their applications [7][9][10] have implicitly accepted the Robust Soliton degree distribution as sufficient and optimal. This is a sound assumption from the theoretical proofs presented in [1]. However, many of these studies present limited effort in deriving a optimal parameterised form of the degree distribution or even an practical implementation of a general LT code over an actual network. Our work is centred around the potential use of LT codes as an AL-FEC for media distribution, we have chosen not to test ***k*** values larger than 1000. Too much latency is introduced while waiting for the large amounts of encoded symbols, and in various other works we have seen that very small values introduce high reception overhead. Therefore, we have chosen to test both ***k*** = 100 and ***k*** = 1000 block sizes. The analysis of the Robust Soliton distribution based on probability and statistics is sound only if ***k*** is infinite. In practice however, the behaviour of the LT code will not match the mathematical analysis exactly, especially for small ***k***. Typical results for the Robust Soliton degree distribution is illustrated below in Table I. The constant ***c*** = 0.1 were chosen as it produced an acceptably low standard deviation and overhead mean.

TABLE I. TYPICAL RESULTS FOR THE ROBUST SOLITON DEGREE DISTRIBUTION

Input Symbols (k)	δ	Z	Mean	Std	Mean	Std
			N		Symbol Operations	
100	0.01	1.89	172.49	17.64	1007	166
	0.1	1.51	149.26	14.41	858	153
	0.9	1.24	135.69	13.21	704	139
1000	0.01	1.43	1373.65	39.92	14364	1232
	0.1	1.28	1256.70	33.37	12521	1113
	0.9	1.16	1171.99	33.11	10488	1128

Interestingly enough we see that by increasing **δ** beyond 1 the efficiency increases even more. In the original case where it is used to predict failure of decoding, this parameter becomes more accurate only when a linear congruential generator is used for random number generation. [10]

The focus of our work is on finding a more efficient parameterised degree distribution to reduce the number of symbol operations and amount of overhead with small deviation.

III. PROPOSED OPTIMISED DEGREE DISTRIBUTION

By combining convex functions and the expected ripple size $\mathbf{R} = \mathbf{c}\sqrt{\mathbf{k}}\mathbf{ln}(\frac{\mathbf{k}}{\boldsymbol{\delta}})$ from the Luby transform a new set of equations can be derived to shape the Ideal Soliton distribution to optimise the amount of symbol operations and overhead ***N***. The expected ripple size determining the position of the spike somewhere on ***d***, ensures that all unprocessed input symbols are covered. [1] However, instead of keeping the weight at d = k/R a constant, (6) and (7) distributes the expected area exponentially over k, which maintains a good ripple size throughout the decoding steps by ensuring ample symbol connections. If Z is close to 1, (where Z ≥ 1) we expect the optimal amount of symbol operations. Parameters $\boldsymbol{c_1}$, $\boldsymbol{c_2}$ and $\boldsymbol{c_3}$ determine the curvature and area supplementary to the Ideal Soliton PDD, which is proportional to the average degree of an encoded symbol. Tweaking these parameters leads to an optimal solution if

 ISBN: 978-1-61208-166-3

the correct distributed area is added to the correct location on the degree distribution.

A. Piecewise functions used to shape the PDD

Fig. 4 illustrates the shape of each exponential function given by (5), (6) and (7). The parameters c_1, c_2 and c_3 are used to alter the amplitudes and curvatures of each set. By changing these parameters, the total area under the graph (affecting Z) can be modified to reduce N by keeping $\mathbf{D} \geq O(\ln(k))$.

$$y_1(d) = \left(\frac{c_1}{\sqrt{k}}\right)(c_2)^{-d} \quad , d = 1, \dots, k \qquad (5)$$

$$y_2(d) = \left(\frac{c_1}{\sqrt{k}}\right)(4c_2)^{-d+\frac{k}{R}-1} , d = \frac{k}{R}+1, \dots, k \qquad (6)$$

$$y_3(d) = \left(\frac{c_3}{k}\right)(3)^{d-\frac{K}{R}} \quad , d = 1, \dots, \frac{k}{R} \qquad (7)$$

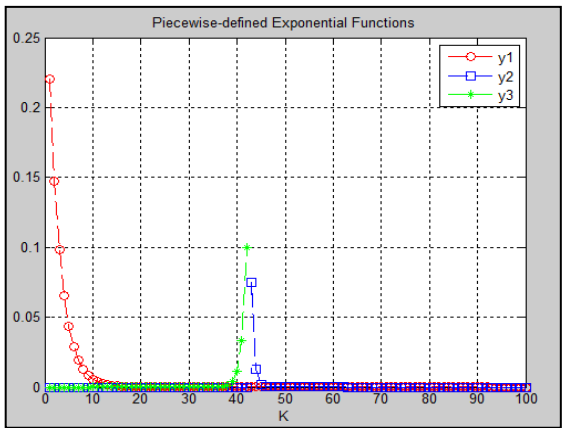


Figure 4: Scaled illustration of piecewise-defined Exponential functions used to shape the new PDD

B. Discrete Kullback-Leibler optimisation approach

The Kullback Leibler distance in (8) can be interpreted as a natural distance function from a "true" probability distribution p to a "target" probability distribution q. In each set of decoded samples of N, the average of the best degree distributions becomes our target degree distribution. The PDD is shaped accordingly and the process continues recursively until the Kullback Leibler distance converges to zero.

$$D(P \parallel Q) = \sum_i p_i \log_2 \frac{p_i}{q_i} \qquad (8)$$

C. Practical Implementation over WiMAX

Our test setup consisted of a WiMAX micro base station and Si indoor CPE 2.5. Consecutive tests were run to determine the effect of SNR and packet loss on the LT code as an application layer implementation. The simple network management protocol (SNMP) was used to retrieve channel information from the base station's client burst profiles. The WiMAX system slots in this receiver to transmitter feedback for adaptive physical layer modulation purposes. The WiMAX network setup and AL-FEC screenshots are illustrated in Figs. 5 - 7.

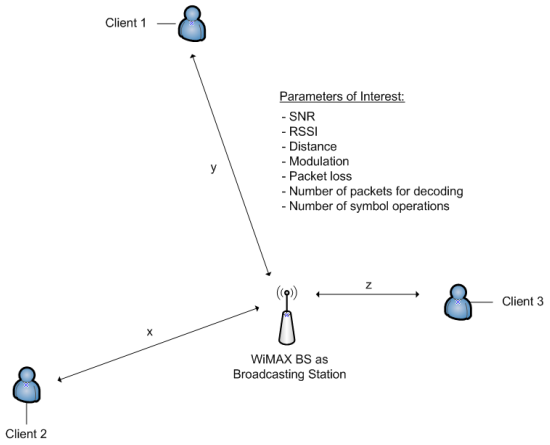


Figure 5:Illustration of the WiMAX Test Setup

In almost all deployed IPTV linear media broadcasting services, audio and video streams are multiplexed into some codec transport stream. Our AL-FEC was implemented over the UDP stream shown in Figs. 6 - 7.

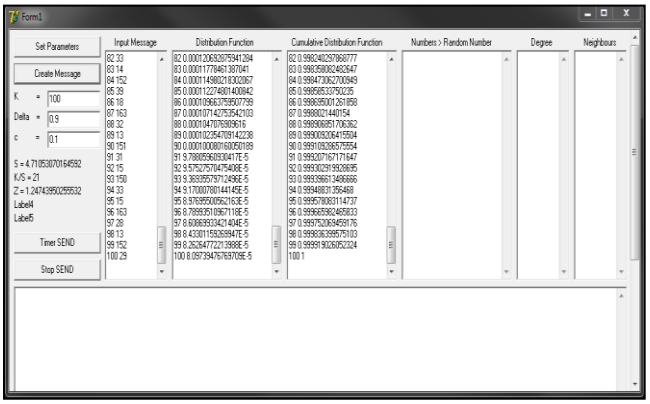


Figure 6: Application Layer UDP encapsulated LT Fountain Encoder

Figure 7: Application Layer UDP encapsulated LT Fountain BP Decoder

The radio link is a quickly varying link, often suffering from great interference. Physical channel conditions such as pathloss, fading and shadowing etc. place constraints on wireless signal transmissions. WiMAX inherently utilises advance FEC techniques such as the concatenated Reed-Solomon Convolutional codes to overcome such destructive effects. For the purpose of our tests the application layer

 ISBN: 978-1-61208-166-3

measured packet loss is an indication of the system suffering from packet loss after the inherent FEC layers built in WiMAX.

IV. RESULTS

Figs. 8 - 12 and Figs. 19 - 23 shows simulated and practical results of the improved degree distribution ***y(d)*** for ***k*** = 100 and ***k*** = 1000. Figs. 11 - 18 and Figs. 22 - 23 illustrates practical results over the WiMAX network.

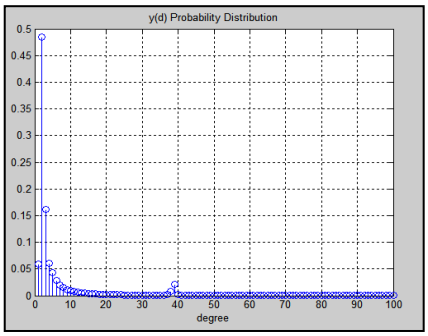


Figure 8: k=100, c_1=1.08, c_2=2.316, c_3=1, δ=4, c=0.08, Z=1.12

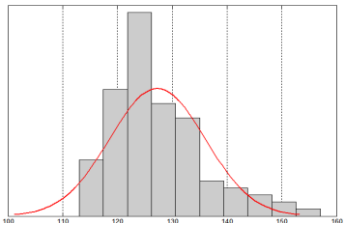


Figure 9: Simulated number of packets N (mean=127.2, std=8.6)

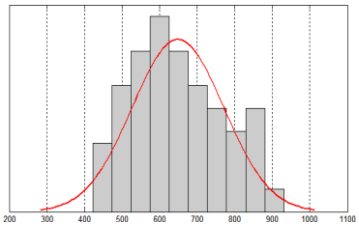


Figure 10: Simulated number of symbol operations (mean=648, std=121.8)

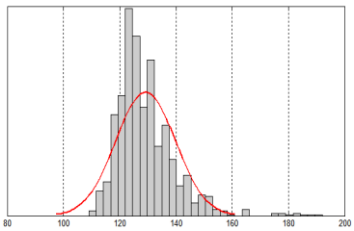


Figure 11: Number of packets N (mean=129.2, std=10.6)

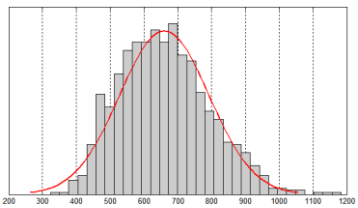


Figure 12: Number of symbol operations (mean=660, std=132.1)

Figs. 13 - 18 indicate practical result obtained over WiMAX (CPE 800m from BS) for ***k*** = 1000, ***c*** = 0.1 and **δ** = 0.9, using the Robust Soliton degree distribution. From these measurements it is clear that the fountain code did not suffer significantly when introduced to a drastic reduction in SNR.

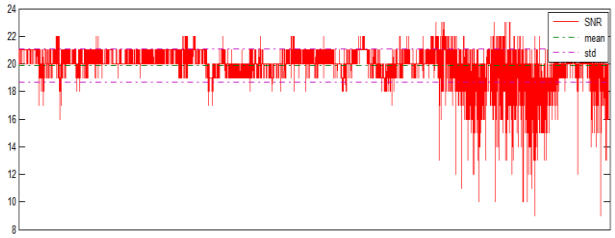


Figure 13: DL Signal to Noise Ratio

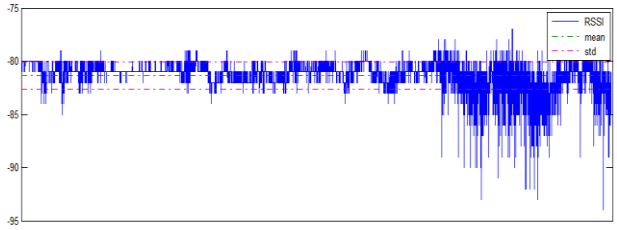


Figure 14: DL Received Signal Strength Indication

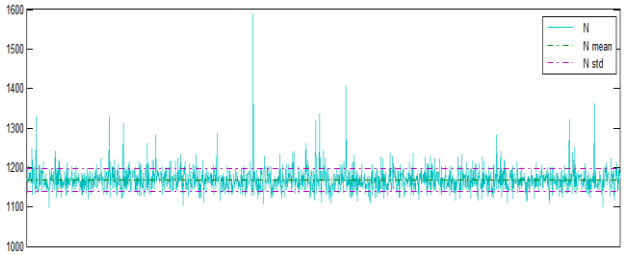


Figure 15: Number of Packets N

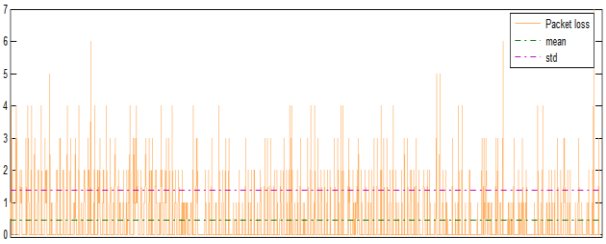


Figure 16: Packet loss

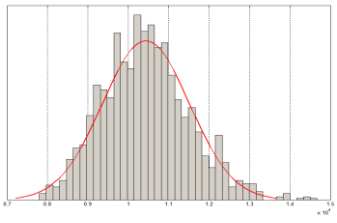


Figure 17: Number of symbol operations (mean=10434 , std=1076)

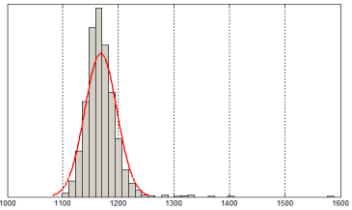


Figure 18: Number of packets N (mean=1168 , std=28.8)

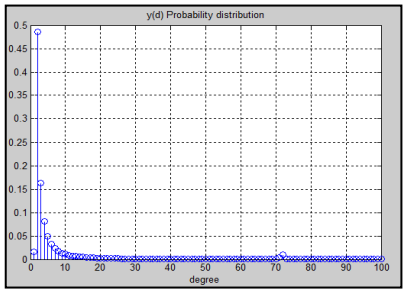


Figure 19: k=1000, c_1=1, c_2=2, c_3=9.5, δ=4, c=0.08, Z=1.04

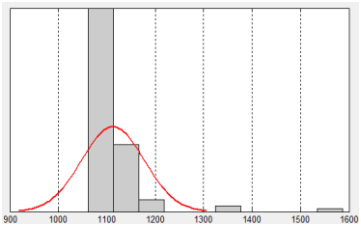


Figure 20: Simulated number of packets N (mean=1112.7, std=64.6)

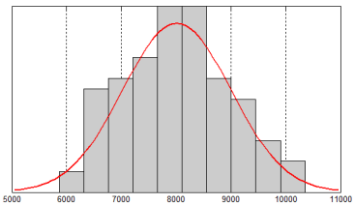


Figure 21: Simulated number of symbol operations (mean=8012.5, std=987.2)

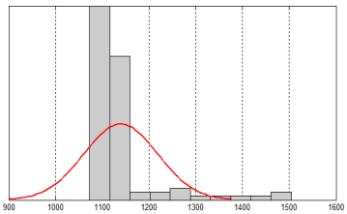


Figure 22: Number of packets N (mean=1139, std=76)

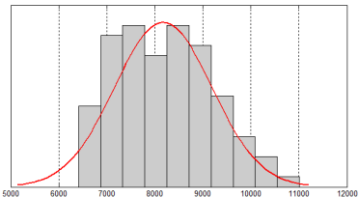


Figure 23: Number of symbol operations (mean=8174, std=1011)

TABLE II. COMPARISON BETWEEN ROBUST SOLITON AND OPTIMISED PDD

Input Symbols (k)	PDD	Mean	Std	Mean	Std
		N		Symbol Operations	
100	y(d)	127.20	8.60	648	121
	μ(d)	135.69	13.21	704	139
1000	y(d)	1112.70	64.60	8012	987
	μ(d)	1373.65	39.92	14364	1232

V. CONCLUSION AND FUTURE WORKS

In this paper, we presented an improved degree distribution by shaping the theoretically optimal distribution with convex functions until optimal results were obtained. Only five parameters were sufficient to define an optimal encoding process to reduce decoding cost and overhead. The practical and simulated results shown is a significant improvement over LT codes using the popular Robust Soliton as degree distribution. To the best of our knowledge we also introduced the first practical implementation of fountain codes over a WiMAX network, and presented useful data regarding the transmission thereof. Regarding LT codes, it turns out that BP alone is not efficient enough to get very tight bounds on decoding failure probability as a function of reception overhead. This was the rationale behind the Raptor codes [6], which combines a weak LT code with a traditional block code and decodes with both GE and BP. Future investigations include the analysis of Raptor codes and the design of alternative degree distributions with desirable properties in terms of both overhead and decoding complexity.

VI. REFERENCES

[1] M. Luby, “LT Codes,” in Proceedings of The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002, pp. 271–282, doi: 10.1109/ICICIC.2008.250.

[2] M. Rossi, G. Zanca, L. Stabellini, R. Crepaldi, A. F. Harris, and M. Zorzi, "SYNAPSE: A Network Reprogramming Protocol for Wireless Sensor Networks using Fountain Codes, July 2008, doi: 10.1109/SAHCN.2008.32.

[3] E. Hyytia, T. Tirronen, and J. Virtamo, "Optimal Degree Distribution for LT Codes with Small Message Length", in IEEE INFOCOM mini-symposium, pp. 2576-2580, doi: 10.1109/INFCOM.2007.324.

[4] J. W. Byers, M. Luby, and M. Mitzenmacher, “A Digital Fountain Approach to Asynchronous Reliable Multicast” in IEEE Journal 2002, doi: 10.1109/JSAC.2002.803996.

[5] D.J.C. MacKay, "Capacity Approaching Codes Design and Implementation", Fountain Codes, IEE Proc-Commun, Vol. 152. No. 6, December 2005, doi: 10.1049/ip-com:20050237.

[6] A. Shokrollahi, "Raptor Codes", Foundation and Trends in Communications and Information Theory, IEEE Information Theory Society, doi: 10.1109/TIT.2006.874390.

[7] H. Tarus, J. Bush, J. Irvine, and J. Dunlop, "Exploiting Redundancies to Improve Performance of LT Decoding", 2008 IEEE, doi: 10.1109/CNSR.2008.81.

[8] D.J.C. MacKay, "Information Theory, Inference, and Learning Algorithms", Cambridge University Press 2003, August 2004.

[9] D. H. Wang, “Hardware Designs for LT Coding”, Masters Dissertation, Delft University of Technology, 2006.

[10] C. Harrelson, L. Ip, and W. Wang, “Limited Randomness LT Codes,” Proceedings of the 41st Annual Allerton Conference on Communication Control and Computing, 2003.

[11] V. Bioglio, M. Grangetto, R. Gaeta, and M. Sereno, "On the fly Gaussian Elimination for LT Codes", doi: 10.1109/LCOMM.2009.12.091824.

 ISBN: 978-1-61208-166-3

The Adaptive Content and Contrast-aware Technique for Visible Watermarking*

Min-Jen Tsai and Jung Liu
Institute of Information Management
National Chiao Tung University, R.O.C.
mjtsai@cc.nctu.edu.tw
rongrong211@gmail.com

Ching-Hua Chuang
Department of Information Management, Tahwa
Institute of Technology, R.O.C.
chuang@thit.edu.tw

***Abstract*—The efficiency of a digital image watermarking technique depends on the preservation of visually significant information. This is attained by embedding the watermark transparently with the maximum possible strength. This paper presents an Adaptive approach for still image in which the watermark embedding process employs the wavelet transform and incorporates Human Visual System (HVS) characteristics. The sensitivity of a human observer to contrast with respect to spatial frequency is described by the Contrast Sensitivity Function (CSF). The strength of the watermark within the decomposition sub-bands is adjusted according to this sensitivity. Moreover, the watermark embedding process is carried over the sub-band coefficients by the analysis of Noise Visibility Function (NVF) in which the distortions are less noticeable. Such unique design is novel and the experimental evaluation of the proposed method shows excellent results in terms of robustness and transparency.**

Keywords- Image Watermarking; HVS; CSF; wavelet.

I. INTRODUCTION

Due to the advancement of digital technologies and rapid communication network deployment, digital images are now widely distributed on the Internet or via other digital devices. Digital image allows an unlimited number of copies from an "original", people can acquire or distribute the images without any reduction in quality through both authorized and unauthorized distribution channels. With the ease of editing and reproduction, protection of the intellectual property right and authentication of digital multimedia becomes an important issue.

In recent years, digital watermarking has been extensively studied and regarded as a potentially effective means for protecting copyright ownership of digital media content [1], since it makes possible the embedding of secret information in the digital content to identify the copyright owner. Many researchers have invented various visible watermarking schemes to protect copyrights. From the literature survey, Chen [2] proposed a visible watermarking mechanism to embed a watermark by a statistic approach. They divided the image into equal-sized blocks and calculated the standard deviation of those pixels in block. They later calculated the embedding ratio of watermark into the corresponding pixels for watermarking. Chen et al. [3] describe an approach for adaptive visible watermarking based on the analysis of the threshold value of the image using Otsu's threshold to select the best embedding strength of the watermark at a particular position. Huang and Tang [4] presented a contrast sensitive visible watermarking scheme with the assistance of human visual system (HVS). They computed the contrast sensitive function (CSF) mask from discrete wavelet transform domain and used a square function to determine the mask weights for each sub-band. At last, they adjusted the embedding weights based on the block classification with the texture sensitivity of HVS. Tsai [5] incorporated the collaboration of CSF and noise visible function (NVF) for HVS models and proposed a new visible watermarking technique where the intensity of the watermark in different regions of the image depends on the underlying content of the image and humans' sensitivity to spatial frequencies. However, the previous works extended the following issues:

1. Since the applications of visible watermarking are often limited to content browsing or previewing, content viewers are annoyed at degraded visual quality. Therefore, the embedded patterns should be unobtrusive. However, the robustness of watermarking and quality of the digital content are generally conflicted with each other.
2. The embedding factors for watermarking emphasize different weights in various frequency domains. Subsequently, certain thresholds should be examined carefully during the design of watermarking schemes.

The goal of this paper is to present an adaptive visible watermarking algorithm (ACOCOA) with a novel contrast sensitivity function masking for wavelet based watermarking method which considers the characteristics in different frequency domain. The main contribution of this paper is to leverage the knowledge of Contrast Sensitivity Function and Noise Visibility Function to embed low energy in the area where the sensitivity of CSF is high and vice versa. The experimental results demonstrate that the proposed technique improves the watermarked image quality, translucence and robustness of the watermarking.

The rest of this paper is organized as follows. In Section 2, we will give the detailed description of the proposed theoretical approach for watermarking technical. In Section 3, numerical results and discussion are illustrated to justify the proposed approach. Finally, the conclusion is drawn in Section 4.

 ISBN: 978-1-61208-166-3

II. THE ACOCOA WATERMARKING ALGORITHM

The most important requirements in the visible watermarking scheme are the robustness and translucence, but unfortunately they are in confliction with each other. If we increase the energy of watermark to improve its robustness, the problem we get is perceptual translucence decreasing with less image fidelity and vice versa. We find the critical factor "HVS" in providing the good translucence of the watermarked image and a better robustness [4]. HVS research offers the mathematical models about how humans see the world. Hemanmi [6] applied uniform quantization noise to measure the psychovisual sensitivity in wavelet sub-bands within an image and showed the results that human vision has different sensitivity from various spatial frequencies (frequency sub-bands). The HVS by using the contrast sensitive function (CSF) and noise visibility function (NVF) is integrated in this study and will be explained in brief as following:

A. CSF (Contrast Sensitive Function)

Mannos and Sakrison [7] originally presented a model of the CSF for luminance (or grayscale) images is given as follows:

$$H(f) = 2.6 \times (0.0192 + 0.114 \times f) \times e^{-(0.114 \times f)^{1.1}} \quad (1)$$

where $f = \sqrt{f_x^2 + f_y^2}$ is the spatial frequency in cycles/degree of visual angle (f_x and f_y are the spatial frequencies in the horizontal and vertical directions, respectively). The HVS is most sensitive to normalized spatial frequencies between 0.025 and 0.125 and less sensitive to low and high frequencies.

CSF masking [8], [9] is one way to apply the CSF in the discrete wavelet domain. CSF masking refers to the method of weighting the wavelet coefficients relative to their perceptual importance. In [9], the DWT CSF mask utilizes the information in all of the approximation sub-bands as well as all of the detail sub-bands to yield 11 unique weights in the mask. All of the weights are normalized so that the lowest weight is equal to one. The 11 weights of DWT CSF mask are shown in Figure 1 after 5-level wavelet pyramidal DWT decomposition and the HVS is most sensitive to the distortion in mid-frequency regions (level 3) and sensitivity falls off as the frequency value drifts on both sides (level 1, 2, 4 and 5). The square function in [4] is applied to approximate the effect of CSF masking. The adequate modulation rate β^{λ} for each sub-band is determined by:

$$\beta^{\lambda} = 0.01 + \frac{(7.20 - r^{\lambda})^2}{7.20^2} \quad (2)$$

where r^{λ} represents the wavelet coefficient CSF of the perceptual importance weight for each sub-band where λ denotes the decomposition level.

B. NVF (Noise Visibility Function)

Alexander et al. [10] presented a stochastic approach based on the computation of a NVF (Noise Visibility Function) that characterizes the local image properties and identifies texture and edge regions. This allows us to determine the optimal watermark locations and strength for the watermark embedding stage. The adaptive scheme based on NVF calculated from stationary GG model is superior to other schemes, which is defined as follows:

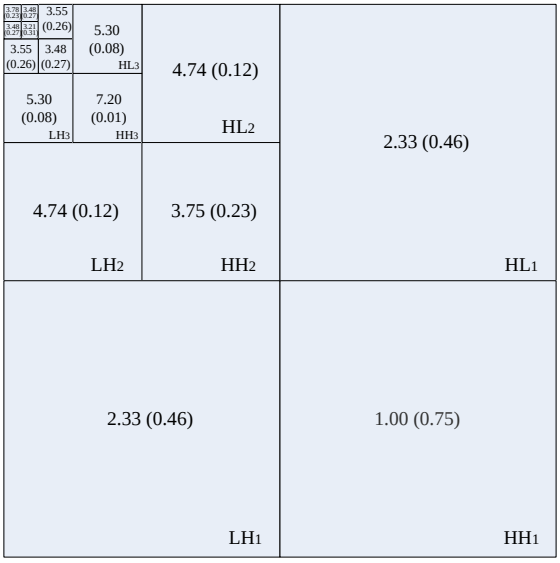


Figure 1. A five-level wavelet pyramidal decomposition. $r^{\lambda}(\beta_{\lambda,\theta})$ values for each level λ are indicated at the center of each band.

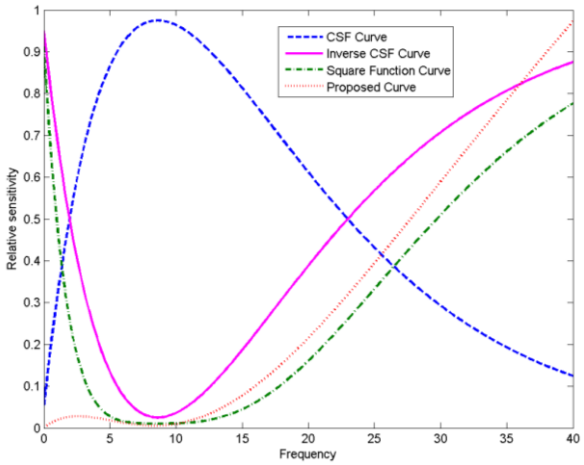


Figure 2. The sensitivity curve of CSF, inverse CSF, square function and proposed cruve.

TABLE I. ADAPTIVE CSF MASKING FOR A FIVE-LEVEL DWT

Orien-tation	Level				
	1	2	3	4	5
LL					0.000001
HL/ LH	0.599316	0.211279	0.031660	0.032198	0.031905
HH	1.000000	0.341371	0.005418	0.031905	0.030574

$$NVF_{x,y} = \frac{w_{x,y}}{w_{x,y} + \sigma_I^2} \quad (3)$$

where $w_{x,y} = \gamma[\eta(\gamma)]^{\gamma} / \left\| r_{x,y} \right\|^{2-\gamma}$ and σ_I^2 is the global variance of the original image. $\eta(\gamma) = \sqrt{\Gamma(3/\gamma)/\Gamma(1/\gamma)}$, $\Gamma(s) = \int_0^{\infty} e^{-u} u^{s-1} du$ (gamma function) and $r_{x,y} = \frac{I_{x,y} - \bar{I}_{x,y}}{\sigma_I}$, γ is the shape parameter and $r_{x,y}$ is determined by the local mean and the local variance. For most of real images, the shape parameter is in the range $0.3 \le \gamma \le 1$. In our scheme, the estimated shape parameter for $\gamma = 0.65$, and width of window is 1.

C. Adaptive CSF masking

The property of CSF is a measure of fundamental spatiochromatic of the HVS, and people are more sensitive in mid-frequency regions. Therefore, we need embed low intensity of visible watermarking in high sensitivity regions and vice versa. According to such observation, we can draw the inverse CSF as shown in Figure 2, which represents the embedding intensity allowed based on the study of HVS. Therefore, a good visible watermarking should embed low energy in mid-frequency regions from the plot of inverse CSF to avoid obtrusiveness and affect the visual quality. Consequently, the square function applied in [4-5] dose not match the perfect inverse CSF curve as shown in Figure 2 so they need to set certain thresholds to avoid adding too much energy in the low DWT frequency domains. In order to solve the problems and obtain the better watermarked image for HVS that contains the characteristics of robustness and translucence, we use the interpolation method to construct the Adaptive CSF masking to improve the HVS model for better image quality. From above discussion, we have proposed an Adaptive CSF masking, which is defined in formula (4) and tabulated the corresponding coefficients of the associated sub-bands in Table 1:

$$\text{Adaptive CSF masking} = (1 - H(f)) \times f \quad (4)$$

Since LL band is very critical during the reconstruction of the image, a small value of parameter is derived in order to preserve the quality of watermarked image. According to such observation, we also draw the proposed curve as shown in Figure 2, which can help us to compare the different watermark weighting curve.

D. ACOCOA Visible Watermarking Algorithm

ACOCOA algorithm leverages the study of [5] and modifies the controlling parameters of watermark embedding based on the consideration of the image quality. The watermark embedding procedures are briefly described as following steps and the flow chart is shown in Figure 3:

Step 1. The original color image is converted in the color space domain from RGB to YCrCb.

Step 2. By using Bi9/7 filter from [11], compute the 5-level 2-D wavelet coefficients of Y component from original color image and grayscale logo watermark image.

Step 3. Modify the DWT coefficients of the host image by

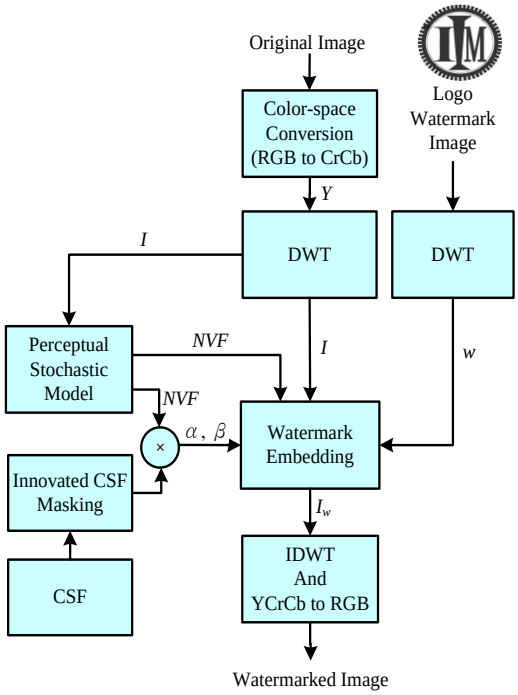


Figure 3. The flow chart of ACOCOA visible watermarking.

TABLE II. PSNR (DB) SUMMARY OF WATERMARKED COLOR IMAGES

Method / Image	Method of [4]	Method of [5]	I-COCOA
Lena	26.78	32.67	36.21
Lake	26.03	31.66	33.95
Peppers	26.83	32.48	35.29
F16	27.96	32.43	34.87
Tiffany	27.57	32.92	34.64
Splash	25.68	32.37	36.78

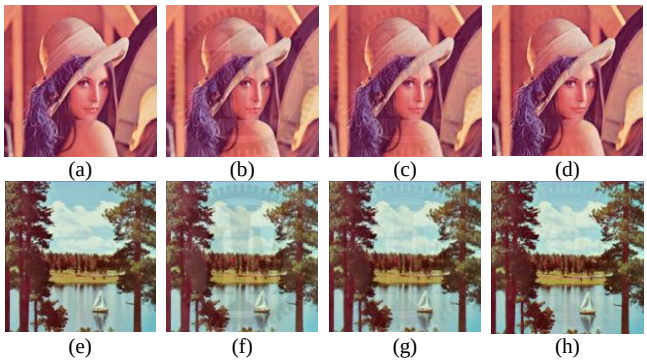


Figure 4. The visual quality comparison of original and watermarked images. (a), (e) are original Lena, Lake images respectively. (b), (f) are watermarked images by the method of [4]. (c), (g) are watermarked images by the method of [5]. (d), (h) are watermarked images by the ACOCOA method.

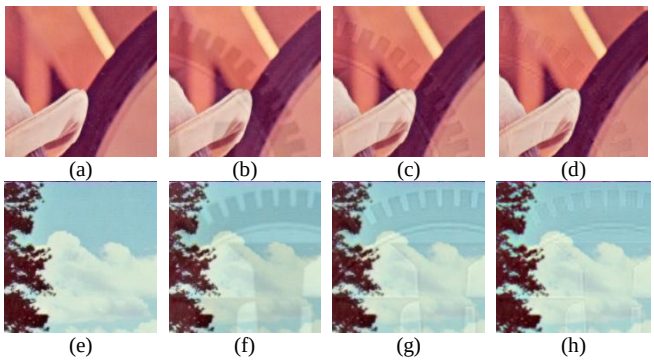


Figure 5. The visual quality comparison of close-ups for images in Figure 4 (a),(e) are original Lena, Lake images. (b),(f) are watermarked images by the method of [4]. (c),(g) are watermarked images by the method of [5]. (d),(h) are watermarked images by the ACOCOA method.

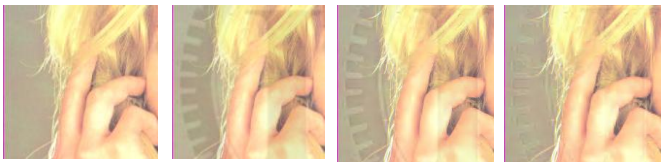


Figure 6. The visual quality comparison of close-ups for Tiffany image after JPEG 2000 compression. (a) original image, (b) watermarked image by the method of [4], (c) watermarked image by the method of [5], (d) watermarked images by the ACOCOA method.

TABLE III. PSNR (DB) SUMMARY OF WATERMARKED COLOR IMAGES BEFORE AND AFTER JPEG 2000 COMPRESSION.

Method / Image	Method of [4]			Method of [5]			I-COCOA Approach		
	(1)	(2)	(3)	(1)	(2)	(3)	(1)	(2)	(3)
Lena	26.78	24.40	28.41	32.67	27.06	28.52	36.21	27.92	28.69
Lake	26.03	23.02	26.30	31.66	25.06	26.61	33.95	25.72	27.04
Peppers	26.83	24.44	28.42	32.48	27.03	28.50	35.29	27.83	28.75
F16	27.96	24.94	28.00	32.43	26.71	28.13	34.87	27.37	28.38
Tiffany	27.57	25.09	28.60	32.92	27.36	28.71	34.64	27.86	28.93
Splash	25.68	24.01	29.30	32.37	27.53	29.31	36.78	28.70	29.34

Note:
(1) means the PSNR values before the JPEG 2000 compression.
(2) means the PSNR values after the JPEG 2000 compression.
(3) means the PSNR values are compared between the compressed watermarked image and the watermarked image.

using the following equation:

$$I^{w}_{x,y} = \alpha_{\lambda,\theta} \times I_{x,y} + (\beta_{\lambda,\theta} + NVF_{x,y}) \times w_{x,y} \quad (5)$$

Note: (x,y) indicates the spatial location. I and w are the decomposed wavelet coefficients of the original image and the logo watermark image. $\alpha_{\lambda,\theta}$ and $\beta_{\lambda,\theta}$ are scaling and embedding factors which are defined as below. $NVF_{x,y}$ is defined in formula (3).

$$\beta_{\lambda,\theta} = (1 - NVF_{x,y}) \times (1 - H(f)) \times f \quad (6)$$

$$\alpha_{\lambda,\theta} = 1 - 0.7\beta_{\lambda,\theta} \quad (7)$$

Step 4. Inverse transform the DWT coefficients of the original image to obtain the watermarked image.

III. EXPERIMENTAL RESULTS

The proposed visible watermarking algorithm has been implemented and intensively tested by using the widely available color images from USC image database [12] and the performance of 512×512 experimental images are tabulated in Table 2 for comparison purpose. The grayscale watermark of logo image adopted in the experiments is a department logo and shown in Figure 3.

In order to make a fair comparison with the method from [4], [5], it is better to embed the same watermark for the same cover image. However the watermark used in [4] is not available currently, we embed the logo watermark from Figure 3 to make the best effort for performance comparison. The performance analysis can be categorized as follows:

A. *PSNR (peak signal-to-noise ratios)*

The tabulated results from Table 2 disclose that our watermarking scheme can achieve higher PSNR values than the method in [4] and [5] where the PSNRs are generally below 33dB for different images. The low PSNRs have positive correlation with the degradation in image quality. This denotes the fidelity of images from our method is better than the traditions CSF based method.

B. *Visual Quality*

Figure 4 (a) and 4(e) illustrate the original cover images of Lena and Lake from [12], the results of watermarked images from [4] and [5] are compared with the proposed approach and the results are in Figure 4 (b)(c)(d) and (f)(g)(h).

From Figure 4 (b)(c)(d) and (f)(g)(h) image pairs, the proposed method has the closest luminance maintenance compared with the original ones which are shown clearly and unobtrusive from the photos. The watermarked images by using [4] and [5] have more bright effect in the unmarked areas. To further compare the details from the watermarked images, Figure 5 (a)(e) are the close-ups of original images. Figure 5 (b)(f) are the close-ups of Figure 4 (b)(f) by using [4]'s method. Figure 5 (c)(g) are the close-ups of Figure 4 (c)(g) by using [5]'s method. Figure 5 (d)(h) are the close-ups of Figure 4 (d)(h) by using our proposed method. It is very clear that the watermark's edges and thin lines are blurred and obtrusive in those images by using the method of [4] and [5] but the watermark patterns in our method still has sharp edge and the logo watermark is evidently embedded.

C. *JPEG 2000 Compression*

The robustness of the proposed visible watermark technique should be tested for compression attack. For JPEG

 ISBN: 978-1-61208-166-3

2000 compression, software from [13] is adopted as the compression tool. Figure 6 (d) is the close-up of watermarked image after JPEG 2000 compression by the proposed method. It is apparent that the logo pattern is still evidently existed and recognized. The PSNR values before and after the JPEG 2000 compression are tabulated in Table 3. The compression ratio is 100:3 between the uncompressed image and compressed image.

Other attacks from [14] are also preformed and the experimental results are consistent with the above findings which indicate our visible watermarking scheme has better visual effect and high PSNR values than other schemes like [4] and [5]. In summary, an intensive comparison for proposed ACOCOA technique has been illustrated above. Therefore, we can conclude that the proposed method is more robust with better image quality than the algorithm in [4] and [5].

IV. CONCLUSION AND FUTURE WORKS

In this study, we have proposed a novel watermarking technique I-COCOA where the intensity of the watermark in different regions of the image depends on the underlying content of the image and HVS to spatial frequencies for copyright protection. The Adaptive CSF masking is fine tuned for watermark embedding which results significant improvement in terms of the image quality, translucence and robustness of the watermarking. The experimental results demonstrate the proposed ACOCOA visible watermarking scheme has achieved high PSNR values with better visual fidelity and robustness to attacks than other schemes.

ACKNOWLEDGMENT

This work was partially supported by the National Science Council in Taiwan, Republic of China, under Grant NSC99-2410-H-009-053-MY2.

REFERENCES

[1] I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions On Image Processing*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[2] P.M. Chen, "A visible watermarking mechanism using a statistic approach," *5th International Conference on Signal Processing Proceedings*, vol. 2, pp. 910–913, 2000.

[3] J.J. Chen, T.M. Ng, A. Lakshminarayanan and H.K.Garg, "Adaptive visible watermarking using Otsu's Thresholding," International Conference on Computational Intelligence and Software Engineering, pp. 1–4, Dec. 2009.

[4] B.B. Huang and S.X. Tang, "A contrast-sensitive visible watermarking scheme," *IEEE Multimedia*, vol. 13, no.2, pp. 60–66, Apr.-Jun. 2006.

[5] M.J. Tsai, "A Visible Watermarking Algorithm Based on the Content and Contrast Aware (COCOA) Technique," *Journal of Visual Communication and Image Representation*, vol. 20, issue 5, pp. 323–338, July 2009.

[6] S.S. Hemami, "Visual Sensitivity Considerations for Subband Coding," Proceedings of Thirty-first Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, vol. 1, pp. 652-656, Nov. 1997.

[7] J.L. Mannos and D.J. Sakrison, "The effects of a visual fidelity criterion on the encoding of image," *IEEE Transactions on Information Theory*, vol. 20, no. 4, pp. 525–536, July 1974.

[8] D. Levický and P. Foriˇs, "Human Visual System Models in Digital Image Watermarking," *RADIOENGINEERING*, vol.13, no. 4, pp. 38–43, Dec. 2004.

[9] A.P. Beegan, L.R. Iyer, and A.E. Bell, "Design and Evaluation of Perceptual Masks for Wavelet Image Compression," *IEEE Digital Signal Processing Workshop*, IEEE CS Press, pp. 88–93, Oct. 2002.

[10] S. V. Alexander, Z. A. Herrigel and N. Baumgaertner, "A stochastic approach to content adaptive digital image watermarking," *in Proc. 3rd Int. Workshop Information Hiding*, Dresden, Germany, pp. 211–236, Sep. 1999.

[11] A.B. Watson, G.Y. Yang, J.A. Solomon and J. Villasenor, "Visibility of wavelet quantization noise," *IEEE Transactions On Image Processing*, vol. 6, no. 8, pp. 1164–1175, Aug. 1997.

[12] USC SIPI – The USC-SIPI Image Database., Retrieved Aug. 18, 2011, from http://sipi.usc.edu/database/

[13] JPEG 2000 compression, Retrieved Aug. 18, 2011, from http://www.ece.uvic.ca/ ~mdadams/jasper/

[14] StirMark, Retrieved Aug. 18, 2011, from http://www.petitcolas.net/fabien/ software/StirMarkBenchmark_4_0_129.zip

 ISBN: 978-1-61208-166-3

Mobile broadband everywhere : the satellite a solution for a rapid and large 3,9G deployment

Caroline BES and Christelle BOUSTIE
CNES (French Space Agency)
Toulouse, France
caroline.bes@cnes.fr, christelle.boustie@cnes.fr

Ari HULKKONEN, Juha YLITALO*,*
Ulla.ELSILA and Pekka PIRINEN*[+]
* Elektrobit Wireless Communications
[+]University of Oulu, Centre for Wireless Communications
Oulu, Finland
Ari.Hulkkonen@elektrobit.com ;
Juha.Ylitalo@elektrobit.com;
Ulla.Elsila@elektrobit.com ; pekkap@ee.oulu.fi

***Abstract*— The aim of this paper is to demonstrate the feasibility of the concept of a complementary Satellite Component to the LTE (3GPP Long-Term Evolution, also known as 3,9G) and/or WiMAX (Worldwide Inter-operability for Microwave Access) terrestrial network that mobile network operators intend to deploy to support a mass market offer of "Internet connectivity while on the move" and to show its benefit in ensuring truly global coverage.**

In this paper, we show that the cohabitation of the terrestrial network and the satellite at the same frequency on the same global coverage is possible.

I. INTRODUCTION

Hybrid integrated system (associating satellite and terrestrial transmitters) is an opportunity for this sector to complete the coverage of current commercial mass market and to answer to governmental user needs.

"Integrated system" refers to a system composed of a LTE and/or WiMAX terrestrial network and a multibeam satellite component that re-uses the same frequency band than the terrestrial's one. This integrated system improves the spectral efficiency of the overall system and spatially optimize the use of the frequency bands.

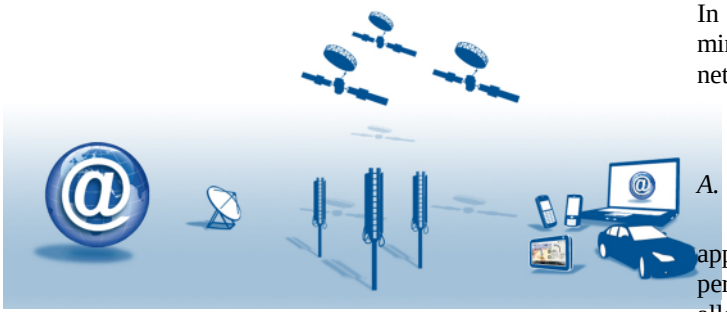


Figure 1. Hybrid integrated network

The main mission of this concept is then to offer a hybrid satellite and terrestrial variation of pure terrestrial technologies for commercial deployment of mobile broadband, with nomadic terminal (Ultra Mobile PC - UMPC) as main target. This axis appears promising since it provides a solution to commercial operators enabling them to cover rapidly a large chunk of the territory and not only 15 to 20% of the surface as it is foreseen for real mobile broadband (approximately 2 Mbps per user on a UMPC like terminal within a few years) deployment based on sole terrestrial components of LTE and/or WiMAX. It then gives the operators a real opportunity to make use of their spectrum beyond the first 15-20% of the territory (e.g.: spectrum usage of UMTS in the first 5 years).

Indeed, deploying more sites in rural areas would be so expensive for the parts of lowest density of population that another solution is now considered: CNES is working on a next-generation mobile satellite system quickly deployable, tightly integrated with terrestrial networks, and behaving as "terrestrial cells in the sky". The terrestrial component will cover high density built-up areas and the satellite component will bring services to the rest of the coverage area.

The sharing of the terrestrial frequency bands with satellite component allows a better spectrum management mostly on rural zone. However, frequency reuse between terrestrial and satellite components may imply co-channel interferences between them.

In this paper, we show that the satellite component has a minimum impact in term of interference on terrestrial network and we present a solution of integrated system.

II. SATELLITE AND TERRESTRIAL SUB-SYSTEM

A. Satellite sub-system

Mobile satellite next generation system becomes an appropriate solution for rural coverage in terms of capacity performance thanks to the use of a large deployable antenna allowing (around 24 m of diameter) a large number of thin beams with between 100-160 km of diameter on ground. The beam densification is in favor of a better frequency reuse and of an increase of the capacity density.

 ISBN: 978-1-61208-166-3

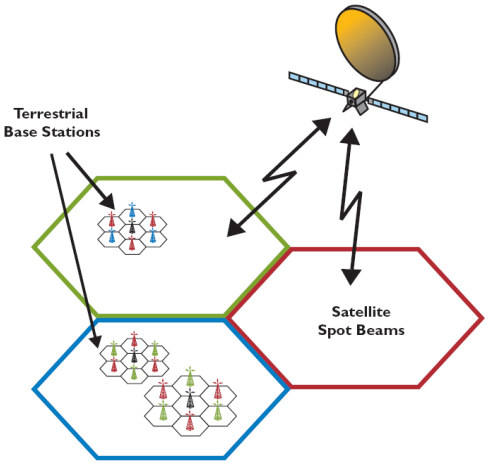


Figure 2. Example of hybrid integrated system deployment on earth

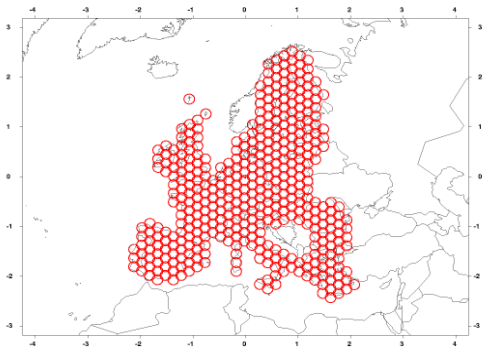


Figure 3. Example of satellite European coverage (around 400 beams)

At our latitude, geostationary orbits are seen at low elevation angle (between 30° and 40°) and require high shadowing margin to have a good availability of the service. The choice of Highly inclined Earth Orbit (HEO) for next-generation mobile satellite system allows a high geographical availability at our latitude even in suburban zone thanks to the fact that the satellite elevation is better than 60° everywhere on the satellite coverage zone. This better propagation condition (less shadowing margin) promotes the use of better spectral efficiency modulations and improves the global capacity.

B. *Terrestrial sub-system*

The integration of the satellite component and the terrestrial component of the radio network is performed at the physical layer. Therefore, the physical layer of the satellite component is following either the LTE or the WiMAX standard. Some modifications may be required, though.

1) *Cellular standards*

a) *LTE*

The 3rd Generation Partnership project (3GPP) has standardized LTE (3GPP Long Term Evolution) to meet the demand of rapidly growing mobile user data traffic. LTE applies in downlink the orthogonal frequency division multiple access (OFDMA) technique to enable efficient time-frequency radio resource allocation for improved system performance. OFDMA is a multiple access technique based on orthogonal frequency division multiplexing (OFDM), a digital multi-carrier modulation scheme that is widely used in wireless systems but relatively new to cellular.

b) *WiMAX*

WiMAX is also an OFDMA based broadband technology especially for high-speed internet data access. It applies OFDM modulation both in downlink and uplink. From the physical layer point of view, the mobile WiMAX (IEEE802.16e) applies the adaptive radio link techniques in a similar manner as LTE.

c) *Fractional Frequency reuse*

However, OFDM does have some disadvantages. The subcarriers are closely spaced making OFDM sensitive to frequency errors and phase noise. For the same reason, OFDM is also sensitive to Doppler shift, which causes interference between the subcarriers. It is known that OFDM will be more difficult to operate than CDMA at the edge of cells. Therefore, some form of frequency planning at the cell edges will be required as shown in the Figure 4.

Different bandwidths can be allocated to cell edges and to cell centers and the band division can be either hard or soft. Several subbands can be reused at the cell edges to avoid inter-cell interference and, moreover, the powers for cell edges and cell centers can be controlled to guarantee users QoS requirement and further reduce the inter-cell interference (Figure 4).

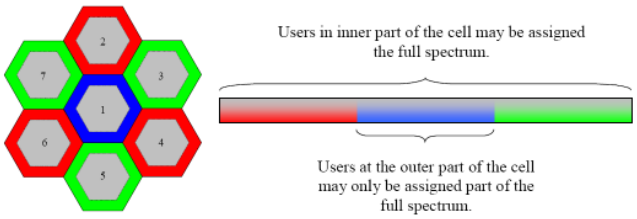


Figure 4. Frequency planning in OFDM

LTE and WiMAX are aimed at frequency reuse 1 scheme. This target is facilitated by several link and system level features, which introduce techniques for mitigating and coordinating intra- and inter-cell interference.

2) *Interference mitigation in the terrestrial system*

These next generations of cellular network aim to provide an increase of their capacity by maximising the use of the frequency spectrum. This implies the use of sophisticated interference mitigation techniques.

 ISBN: 978-1-61208-166-3

These techniques are classified into three major categories such as interference cancellation through receiver processing, interference randomization by frequency hopping, and interference avoidance achieved by restrictions imposed in resource usage in terms of resource partitioning and power allocation. The benefits of these techniques are mutually exclusive, and hence, a combination of these approaches is likely to be employed in the system.

In traditional interference avoidance, inter-cell interference is handled by the classical clustering technique. However, while this technique reduces interference for the cell edge user terminals, it compromises system throughput due to resource partitioning.

As stated before, LTE and WiMAX networks have been designed for a reuse factor of 1 and downlink transmissions are based on OFDM. In addition to data allocation in both time and frequency domains, it creates new possibilities to utilize the available spectrum by flexible and intelligent subcarriers allocation, which is based on both frequency and time domain utilization. In case of a single frequency network this would be one of the ways to avoid interference from the satellite spot beams operating on the same frequency sub-band.

III. RESULTS

A. *Influence of the satellite in term of power*

The power flux density (PFD) emitted by the satellite is considered as constant upon all the coverage of the Satellite system: -104 dBW/m2/MHz. This PFD is considered as interference from the terrestrial point of view and causes a decrease of the LTE/WiMAX cell size.

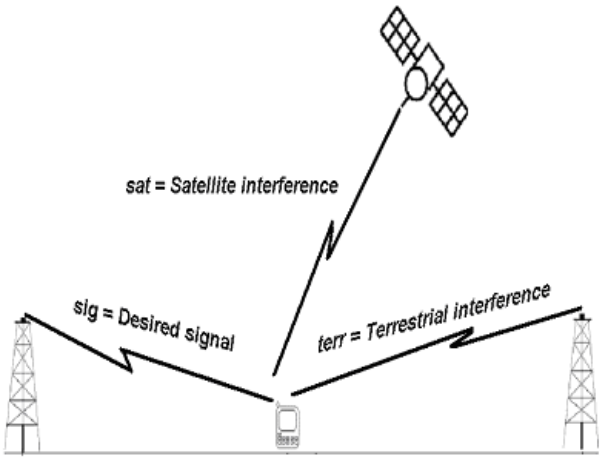


Figure 5. System topology for LTE simulation

Figure 5 presents the system configuration and Figure 6 shows different diameters of a single cell with a given emitted power of the base station 1. Diameter for the cell alone (without interference) 2. Diameter with the influence of a neighbour cell 3. Diameter with the influence of a neighbour terrestrial cell and the satellite spot beam.

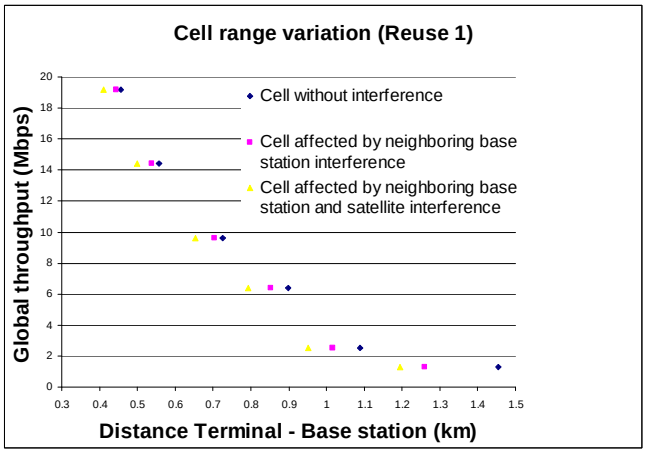


Figure 6

B. *STUDY OF THE INFLUENCE OF THE SATELLITE*

1) *Influence of the satellite on LTE/WiMAX network*

Tolerating the high interference levels that occur in reuse 1 networks is based on both adaptive 2-dimensional scheduling, which can utilize the radio channel characteristics in an optimum way. In addition, interference cancellation is improved with multiantenna receivers. Considering all this, it seemed possible that LTE would provide acceptable performance with satellite overlay scenario without major design or network level changes.

The downlink of both LTE and WiMAX systems is based on multicarrier modulation and it occupies relatively wide bandwidth. The terrestrial radio channel, on the other hand, introduces quite strong frequency selective fading, which means that an advanced multi-dimensional scheduling can allocate dynamically the best slot in both time and frequency domain to each user. Therefore, the HSDPA time domain scheduling principles are valid also in LTE [1]. As the radio channels between an individual mobile user, base stations and the satellite are non-correlating, a good slot can almost certainly be found for each user.

This study also investigated the affect of optimal scheduling. This gave an upper bound on the throughput performance at the cell edge of an LTE link. As a lower bound, the full band average signal to interference plus noise ratio (SINR) was also calculated. Three scenarios are compared: 1) no interference, 2) terrestrial interference only, and 3) terrestrial and satellite overlay interference.

2) *Simulation methodology*

The simulation aim is to investigate the affect of interference on the LTE throughput (the effect on a WiMAX system would be very similar).

 ISBN: 978-1-61208-166-3

In short, the mobile user is spread in a region that includes both sides of the cell edge. The transmit power is set to 20 W on a 5 MHz bandwidth and the antenna gain is 15 dBi. The carrier frequency is 3.45 GHz and the terminal noise -107.5 dBm. The spread is repeated for a number of channel impulse response (IR) realizations generated by the IMT-A [2] channel model generator. Each channel snapshot corresponds to a random snapshot of the defined scenario's propagation conditions. Thus, with a sufficient number of snapshots (or drops) we obtain a statistically stable average of the channel conditions.

For each channel snapshot, the IR is converted to a frequency response from which the SINR is calculated, both across the entire bandwidth and for each LTE resource block individually. LTE resource scheduling is emulated by choosing the resource block (RB) that produces the highest SINR as the scheduled RB. This should give a good upper-bound on the performance enhancement from scheduling. As a lower bound, the full band SINR, which is the average SINR of the RB, is considered.

On Figure 7, the minimum throughput is plotted for the "scheduled" resource blocks as a function of the mobile user location. This analysis takes into account the pilot overhead and the discrete coding and modulation schemes in the LTE downlink. The modulation and coding schemes and their respective SINR requirements are taken from [3].

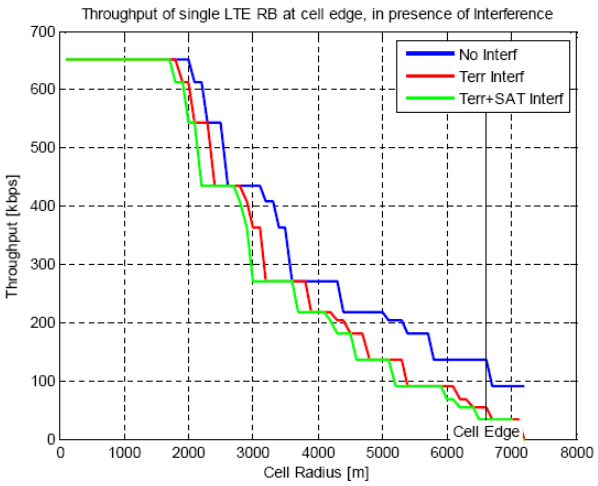


Figure 7 Single Ressource Block throughput in presence of interference

To calculate the cell capacity in terms of throughput, 25 users were placed randomly from 0.1km up to 6km from the eNodeB and a single resource block was allocated for each user.

The cell centre capacity for 5 MHz bandwidth was then obtained for the users at a distance of 0-3km from the eNodeB from the throughput simulation values shown in Figure 7. Correspondingly, the cell edge capacity was obtained from the throughput values for users at 3-6km from the eNodeB. 10000 simulation rounds with 25 different random UE positions in each round were performed for achieving average throughput values. Results are presented on Table 1.

	5 MHz throughput in cell (Mbps)		
Interference scenario	Cell	Cell centre	Cell edge
No interference	10.7	15.12	6.43
Intercell interferences	9.63	14.69	4.74
Intercell + satellite interf.	9.36	14.44	4.46

Table 1 Average throughput values in an LTE cell (5MHz bandwidth)

The simulation results show that it is the inter-cell interference which dominates the throughput loss while the satellite interference plays a minor role. In fact, the loss due to the satellite interference is only at about 2.8%, 1.7%, and 5.9% levels at entire cell, cell centre, and cell edge, respectively. Thus the impact is at largest at cell edge, as expected.

IV. CONCLUSIONS

Based on the simulations it seems that introducing a satellite overlay network on top of a terrestrial LTE or WiMAX network will not introduce a significant interference issue in the case sophisticated interference compensation techniques are used. LTE has been designed to handle reuse 1 scenario, which means the entire network is using the same operating frequency band. This creates a high intercell interference level, which must be handled anyway. Adaptive mechanisms are supported by LTE and also WiMAX thus enabling efficient interference avoidance and compensation. The satellite overlay component does not increase the total interference level significantly and it was estimated that the capacity loss in a cell is only less than 1% and even at the cell edges the performance criteria will be met. The study clearly shows that a satellite overlay component can be introduced and integrated to LTE or WiMAX terrestrial network.

ACKNOWLEDGMENT

Caroline Bès and Christelle Boustie thank warmly Athéna Ibrahim for her help.

REFERENCES

[1] H. Holma and A. Toskala, Eds., WCDMA for UMTS, HSPA Evolution and LTE. Wiley 2007

[2] ITU-R M.2135-1, *Guidelines for evaluation of radio interface technologies for IMT-Advanced.*12/2009. Internet: http://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2135-1-2009-PDF-E.pdf, retrieved 02.02.2011.

[3] Sesia, Stefania, Issam Toufik, and Matthew Baker, "LTE-the UMTS long term evolution: from theory to practice". West Sussex: John Wiley & Sons, 2009.

 ISBN: 978-1-61208-166-3

A New Classification of Backbone Formation Algorithms for Wireless Sensor Networks

Razieh Asgarnezhad
Department of Computer Engineering
Arak Branch, Islamic Azad University
Arak, Iran
raziehasgarnezhad@yahoo.com

Javad Akbari Torkestani
Department of Computer Engineering
Arak Branch, Islamic Azad University
Arak, Iran
j-akbari@iau-arak.ac.ir

***Abstract*—In Wireless Sensor Networks, the most important of challenges is the bandwidth and energy limitations, network topology changes, and the lack of the fixed infrastructures. There is no fixed backbone infrastructure in these networks. Flooding is a kind of broadcasting in sensor networks. But it raises energy consumption because packet retransmission is needed when interference occurs. Also, it will has broadcast storm problem. To solve these circumstances, virtual backbone can be used. A backbone is a subset of active nodes while the rest of the sensors are sleeping. It is able to perform especial tasks and serve nodes which are not in the backbone. For instance, backbone nodes in networks can perform efficient routing and broadcasting. A backbone reduces the communication overhead, increases the bandwidth efficiency, decreases the overall energy consumption, and, at last, increases network effective lifetime in a Wireless Sensor Network. This paper classifies different backbone formation algorithms. We compare performance of these with each other.**

Keywords- backbone formation; clustering; connected dominating set; maximal independent set; wireless sensor network.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have attracted recent research attention due to wide range of applications they support. These networks consists a number of wireless nodes so that all nodes are energy constrained. Sensors are equipped with data processing and communication capabilities. Each sensor can be used to send the collected data to interested parties. The WSNs can be divided into three parts: data collection, based-station and data management center. In WSN, there is no fixed or predefined infrastructure. Flooding is a kind of broadcasting in sensor networks, where each node retransmits the broadcasting message that it receives. But it raises energy consumption because packet retransmission is needed when interference occurs. Also, it will has broadcast storm problem. [2][15]

The extensive research performed in the past of decades in WSNs. Among the topics that clustering formation and interconnection (referred as *backbone formation*) have received especially attention. Backbone will remove unnecessary transmission links through shutting down some of redundant nodes. Although backbone will still guarantee network connectivity in order to deliver data efficiently in a WSN. [5]

A backbone is a subset of active nodes while the rest of the sensors are sleeping. Backbones are able to perform especial tasks and serve nodes which are not in backbone. Therefore, the backbone construction depends on the task to be carried. The backbone of a network is normally required to be connected. For example, connected backbone node in ad hoc networks can perform efficient routing and broadcasting. The most use of backbones is improving of the routing procedure. A backbone reduces the communication overhead, increases the bandwidth efficiency, decreases the overall energy consumption and at last increases network effective lifetime in a WSN. [20]

There are typically three well known methods to constructed backbones: (1) *grid partitioning-based* (2) *clustering-based,* (3) *connected dominating set* (*CDS*)*-based*. In first method, the area of network is divided into grids and one node in each grid is selected as a backbone node. The size of grid should be carefully determined to guarantee that the backbone is connected. In second method, nodes are grouped into clusters. A node is elected as the *cluster-head* (CH) in each cluster. Any node in the network is either a CH or a neighbor of a CH. Rest nodes are required to be included to make the CHs connected. In third method, routing is easier and can adapt quickly to network topology changes. To reduce the traffic during communication, it is desirable to was constructed a Minimum Connected Dominating Set (MCDS). [7][8][14][17][18][20][24][26]

We try to classify different backbone formation algorithms in these networks and compare performance of these with each other. Based on these methods, we have proposed new hybrid methods in this paper. In Section 2, we exhibited these methods and some examples compared in Section 3. In Section 4, we concluded the paper.

II. CLASSIFICATION OF BACKBONE FORMATION ALGORITHMS

From varied aspects, backbone formation algorithms can be classified into different types. Keeping some classifications in view, we present a few instances of these classifications and we propose new hybrid methods.

A. Grid Partitioning-Based Backbone

In this method, the area of the network is divided into grids and one node in each grid is selected as a backbone

 ISBN: 978-1-61208-166-3

node. The size of grid should be carefully determined to guarantee that the backbone is connected.

Geographical adaptive fidelity (GAF) is a grid partitioning algorithm for backbone construction. In this algorithm, each GAF node uses location information itself. The algorithm divides the network into virtual grids so that nodes are distributed into small virtual grids. Any node in one grid can directly communicate with any node in the other grid. This is why that all nodes in the same grid are *equivalent*. Thus, one node from each grid is enough to construct a connected backbone. According to virtual grid, any node in adjacent grid can communicate with each other. The communication range is supposed deterministic. Assume r is the size of the virtual grid, and also R is the transmission range. Because any two nodes in adjacent grids can be communicate with each other, this equation can be used for grids: [26]

$$r^2 + (2r)^2 \leq R^2 \rightarrow r \leq R / \sqrt{5} \quad (1)$$

B. Clustering-Based Backbone

Clustering is method for partitioning nodes of the network into groups. CHs are used to dominate the other nodes within the clusters. Clustering can provide a hierarchical architecture for efficient routing. At most existing solutions for clustering usually consists of two phases: construction and maintenance. In the first phase, nodes are chosen to act such as coordinators of the clusters. Then, clustering maintenance is required to reorganize the clusters due to mobility and failure of nodes. [7][14][18][24]

Low-energy adaptive clustering hierarchy (LEACH) is a protocol. According to this protocol randomly decide whether or not to become CHs. The parameter used in decision making is the percentage of desired CHs in the network. In this protocol, sensors that decide to become CHs broadcast their decision. Each node reports to the CH with the highest signal strength. Selection of CHs is periodically repeated to balance energy consumption of nodes. The structure of the clusters constructed through LEACH is inefficient because the sink may be very far from many CHs. [14]

A clustering algorithm proved that only clustering schemes that position their resultant clusters within the isoclusters of the monitored phenomenon are guaranteed to reduce the nodes' energy consumption and extend the network lifetime. This was the first clustering algorithm; it employs the similarity of the nodes' readings as the main criterion in cluster formation. [24]

Another algorithm [18] proposed a mechanism as no two CHs could be direct neighbors and any other node should be adjacent to at least one CH. Each node has a unique node *key* and also knows the *key*s of its one hop neighbors. The basic idea behind the CH algorithm is to use the node *key* as a priority indicator when selecting CH in each cluster. Each node compares its *key* with the *key*s of its neighbors. At first, all nodes are undecided. If a undecided node has the lowest *key* among its undecided neighbors, the node decides to create its own cluster and broadcasts the decision and its *key* as the cluster *key*. Upon receiving a message from a neighbor so that announces itself to be a CH, each undecided node will declare itself as a non-CH node and also will inform its neighbors through transmitting a message. [18]

Distributed mobility-adaptive clustering (DMAC) is a distributed clustering algorithm. It uses a mechanism similar to the algorithm in Lin and Gerla [18] to construct clusters. But, it uses the weight (the rest energy in the cluster or the capacity of the nodes) of the nodes instead of node ids as keys. This algorithm is followed with such weight instead of the original lowest id used in Lin and Gerla [18]. The basis behind the DMAC is a protocol for the topology control of large WSNs that Basagni et al. [8] proposed and called S-DMAC. This protocol is used to select a subset of nodes to build a connected backbone and let all other nodes switch to an energy conserving *sleep mode*. A connected backbone includes of backbone nodes and gateway nodes so that interconnect the backbone nodes. Backbone nodes are the CHs computed by DMAC. S-DMAC optimized the overhead at both stages consist of construction and maintenance through limiting the use of *hello* messages. The backbone is reorganized only in two times. First, introducing a new batch of nodes with much higher energy than the current nodes, second backbone nodes deplete their energy. A non-backbone node will join a newly inserted backbone node when the residual energy of the new backbone node exceeds the original one's energy through a predefined threshold. [7]

Virtual Backbone for Energy Saving (ViBES) is a backbone algorithm. It uses the energy efficient construction. The idea behind ViBES was a subset of the sensor nodes that formed a connected backbone (the selected nodes via intermediate nodes and links). A small part of the nodes are selected to be the backbone, and the actual backbone is created through connecting the selected nodes via intermediate nodes and links. ViBES construction included of two important phases: (1) selection of primary ViBES nodes (2) their interconnection to form a connected backbone.The selection of the ViBES nodes is performed at each node according to the algorithm proposed in [8]. Every node has a unique id, a generic weight and also knows about the id and the weight of its one hop neighbors. Nodes that have the biggest weight among their neighbors become primary ViBES nodes. The other nodes decide to be primary ViBES nodes or ordinary nodes corresponding with the decision of all the neighbors with a bigger weight. At last, the process terminated when all sensor nodes be partitioned into primary ViBES nodes and ordinary nodes. A backbone is constructed through connecting the primary ViBES nodes via some ordinary nodes. Keeping this algorithm in view, primary ViBES nodes that are two or three hops away, select interconnection nodes until be part of the backbone. Thus, the backbone paths formed guarantee that the final backbone is connected. Figure 1 illustrates the process of selection of ViBES nodes. [6]

 ISBN: 978-1-61208-166-3

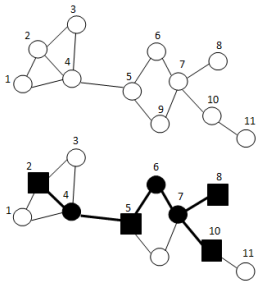


Figure 1. illustrates the process of selection of ViBES nodes. [6] Rectangles and black circles construct the final backbone.

C. Connected Dominating Set (CDS)-Based Backbone

From varii aspects, CDS construction algorithms can be classified into different types. Keeping some classifications in view, we exhibited a few instance of these classifications.

1) UDG and DGB

The CDS construction algorithms can classified into two types: *Unit Disk Graph* (UDG) based algorithms and *Disk Graphs with Bidirectional* (DGB) links. In UDG and DGB, the link between any pair of nodes is bidirectional. The nodes transmission ranges in UDG are the same but in DGB are different. The MCDS in UDG and DGB has been shown to be NP-hard. [2][19][20][21]

2) MIS based and Non-MIS based

Independent set (IS) of a graph G is a subset of vertices so that no two vertices are adjacent in the subset. *Maximal Independent set* (MIS) is an IS, so that it is not a subset of any other IS. Note that in an undirected graph, a MIS is also a *Dominating Set* (DS). The MIS based algorithms have two kinds of realization. The optimal node selection is based on some criteria such as node degree, rest energy of node, and node id. [12][20][22][23]

3) Centralized algorithm and Decentralized algorithm

Algorithms that construct a CDS can be divided into two types: centralized and decentralized. The centralized algorithms in general result in a smaller CDS with a better performance ratio than that of decentralized algorithm. The decentralized algorithms also can be divided into two types: distributed and localized. In distributed algorithms, the decision process is decentralized. But in the localized algorithm, the decision process is not only distributed also requires only a constant number of communication rounds. Most of the distributed algorithms find a MIS and connect this set. [3][13][20][22][23]

Two CDS construction approaches were proposed. The first algorithm begins through marking all vertices white. It selects the node with the maximal number of white neighbors. The selected vertex is marked black and also its neighbors are marked gray. The algorithm iteratively seeks the gray nodes and their white neighbors and selects the gray node or the pair of nodes, whichever has the maximal number of white neighbors. The selected node or the selected pair of nodes is marked black, and also their white neighbors marked gray. Finally, the algorithm terminates, when all of the vertices are marked gray or black. All the black nodes form a CDS. This algorithm results in a CDS of size at most $2(1+H(\Delta)).|OPT|$, where H is the harmonic function and OPT refers to an MCDS. [13]

The second algorithm also begins through coloring all nodes white. A *piece* is defined to be either a connected black component or a white node. The algorithm includes two phases. The first phase iteratively selects a node that yield the maximum reduction of the number of pieces. A node is marked black and its white neighbors are marked gray when it is selected. The first phase terminates when no white node left. There exists at most $|OPT|$ number of connected black components. The second phase constructs a Steiner Tree until connects all the black nodes through coloring chains of two gray and black nodes. The size of the resulting CDS formed via all black nodes is at most $(3+ln(\Delta)).|OPT|$. [13]

A greedy algorithm was proposed for MCDS in UDGs. At first, all nodes are colored white. The construction of a CDS includes four phases. The first phase is computing an MIS and coloring all its members red. In the second phase, a node selects that it can decrease the maximum number of pieces. This node is colored black and all its non-black neighbors are colored gray. After the second phase, we still have some white nodes left. The third phase will compute a spanning tree for each connected component in the sub graph reduced through all white nodes. All non-leaf tree nodes are colored black but leaf nodes are colored gray. The last phase will scan chains of two gray nodes to connect disjoint black components. [11]

The pruning-based heuristic was proposed. The S' CDS is initialized to the vertex set of graph $G(V, E)$. Then each node will be examined to determine whether it should be removed or remained. At first, all nodes in S are colored white. The *effective degree* of a node defined to be its white neighbors in S. With considering a white node $x \in S$ with minimum effective degree if removing x from S makes the resulted graph of S disconnected, then retain x and color it black. Otherwise, remove x from S. If x does not have a black neighbor in S, color its neighbor with maximum effective degree in S black. With repeating this procedure no white node left in S. At first, the algorithm starts from the node with minimum degree, which can be found through modified leader election algorithms in [16]. Let u be the node that we consider at the current step. If removing u causes the CDS disconnected, we color u black. Then, it selects its non-black neighbor with minimum effective degree for consideration in next step. If it is OK to remove u and if u does not have a black neighbor for next step, then u will select a neighbor with minimum effective degree. If u does have a black neighbor v, therefore v will choose its neighbor with minimum effective degree for next step. This procedure will be terminated when all nodes have been examined. This algorithm has time complexity $O(n \log^3(n))$

 ISBN: 978-1-61208-166-3

But, its distributed implementation has higher message complexity. [9]

The distributed implementations of the two greedy algorithms had been proposed. The first algorithm grows one node with maximum degree to be form a CDS. Thus, a node must know the degree of all nodes in the graph. This algorithm produces a CDS with approximation ratio of $2H(\Delta)$ in $O(|C|(\Delta+|C|))$ time, using the $O(n|C|)$ messages, where the harmonic function, n is the total number of vertices, and C represents the final CDS. [12]

In the second algorithm, compute a DS and then selects additional nodes to connect the set. Then, an unmarked node compares its effective degree, with the effective degrees of all its neighbors in two-hop neighborhood. The greedy algorithm adds the node with maximum effective degree to the DS. When a DS is achieved, the first stage terminates. The second stage connects the components via a distributed minimum spanning tree algorithm. This is why that each edge is assigned a weight equal to the number of endpoints not in the DS. Finally, the nodes in the resulting spanning tree compose a CDS. This algorithm has time complexity of $O((n+|C|)\Delta)$, and message complexity of $O(n|C|+m+n.\log(n))$. It have the MCDS with a ratio of $2H(\Delta)+1$, where m is the cardinality of the edge set. [12]

Two versions of an algorithm were provided to construct the DS. In these algorithms, they employ the distributed leader election algorithm [16] to construct a rooted spanning tree. Then, a labeling strategy is used to divide the nodes in the tree to be either black or gray according to their ranks (pair of its level and its id). The labeling process begins from the root node and finishes at the leaves. At first, the node with the lowest rank marks itself black and broadcasts a DOMINATOR message. According to the following rules, the marking process continues:

- "If the first message that a node receives is a DOMINATOR message, it marks itself gray and broadcasts a DOMINATEE message."[3]
- "If a node received DOMINATEE messages from all its lower rank neighbors, it marks itself black and sends a dominator message."[3]

When it reaches the leaf nodes, the marking process finishes. Just now, the set of black nodes form an MIS. In the final phase, the nodes connect in the MIS to form a CDS through INVITE and JOIN messages. Figure 2 illustrates the operation of these algorithms. Node 0 is the root of the spanning tree so that it is constructed through using the leader election algorithm. This algorithm has time complexity of $O(n)$ and message complexity of $O(n.\log(n))$. [3]

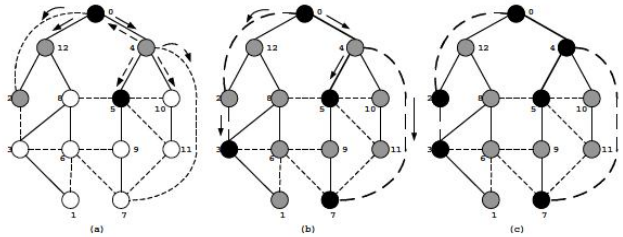


Figure 2. An example of Alzoubi and Wan's algorithm [3]

A completely localized algorithm was proposed to construct CDS in general graphs. At first, all vertices are unmarked. They exchange their open neighborhood information with their one-hop neighbors. Each node knows all of its two-hop neighbors. The marking process applies the following simple rule: any vertex having two unconnected neighbors so that they were marked as a dominator. At last, the set of marked vertices form a CDS, but it has a lot of redundant nodes. There are two pruning principles so that they are provided to post-process the DS. This pruning idea was expressed to the following general rule [10]. According to this rule, if it exist k connected neighbors with higher ids in S so that it can cover all u's neighbors then, a node u can be removed from S. [23]

Connected Dominating Set-Hierarchical Graph (CDS-HG) is a novel distributed MCDS approximation algorithm. This algorithm generates smaller CDS sizes compared with the existing algorithms. Algorithm includes of two phases. In the first phase, rule1 (Essential Node Determination) is used. According to this rule, a set of dominators select for each hierarchical level so that all nodes in the next level are dominated by these dominators. A greedy strategy is used to select the dominators for creating a small initial DS. In the second phase, rule2 is used to remove the redundant dominators. This process repeated from the lowest level to the highest level of the hierarchical graph. According to The greedy strategy that created CDS is connected. The size of generated CDS is at most $(\log n|opt|)$, where n is the number of nodes in the network and opt is the cardinality of a minimum DS. The computation complexity of their algorithm is $O(n^2)$. [25]

Because a centralized CDS algorithm is impractical for WSNs, they implemented a distributed algorithm based on competition. It includes three phases: creating the initial CDS through competition and reducing the CDS size through applying rule2 on all dominators. Respectively, the computation and message complexities of their algorithm are $O(\theta^2)$ and $O(\theta)$, where θ is the maximum number of child nodes in graph. [25]

Another algorithm is proposed for finding MCDS by using DS. DSs are connected via Steiner tree. The approximation algorithm includes of three stages. In the first stage, the DS is determined through identifying the maximum degree nodes to discover the highest cover nodes. In the second stage, connects the nodes in the DS through a Steiner tree. In third stage, this tree prunes to form the MCDS. To local repair, rule k [17] is used to find the nodes

 ISBN: 978-1-61208-166-3

so that can maintain the MCDS. Eventually in the pruning phase, redundant nodes are deleted from the CDS to obtain the MCDS. They proposed a local repair algorithm to take care of node's deletion. [20]

Approximation Two Independent Sets based Algorithm (ATISA) is a new method for constructing CDS. The ATISA has three stages: (1) constructing a connected set (CS), (2) constructing a CDS, and (3) pruning the redundant dominators of CDS. ATISA constructs the CDS with the smallest size compared with some famous CDS construction algorithms. The message complexity of this algorithm is $O(n)$.

The ATISA has two kinds of implementations: centralized implementation and distributed implementation. The centralized algorithm consists of three stages, which are CS construction stage, CDS construction stage, and pruning stage. In the centralized algorithm, the initial node is selected randomly and then, the algorithm executed several rounds. When the first stage is ended, there are no black nodes generated in the network. The generated black node set is formed a connected set. If a white node has black neighbors, then it will select the black neighbor with the minimum id as its dominator, and also change its state into gray. If a white node only has the gray neighbors; then, it will send an invite message to the gray neighbor with the minimum id and also change its state into gray. Finally, in the second stage, constructs a CDS and all the nodes are either black or gray. At last, there is no white node left in the network. According to the third stage, if a black node with no children and also if the neighbors of the black node are all adjacent to at least two black nodes, then the black node is put into connected set. [19]

But, in the distributed implementation, all the nodes exchange their positions information with their neighbors. At first, all nodes are initialized white. After the first stage, there are white nodes, gray nodes, and black nodes. Then, in the second stage, there are black nodes, gray nodes and sometimes white nodes. According to the first stage, white nodes can change their states into gray and also gray nodes can change their states into black. At last, in the third stage, the redundant black nodes are deleted. [13]

Energy-Aware Virtual Backbone Tree (EVBT) is a distributed algorithm for constructing a backbone in WSN. It chooses only nodes with enough energy levels as the member of the virtual backbone. Also, it introduced a concept of threshold energy level for members of virtual backbone. Only nodes with energy levels above a predefined threshold are included in the EVBT. The EVBT can be dynamically reconstructed with changing energy levels and also changing state (on/off) of nodes. Data packet can be delivered along another EVBT, when an EVBT breaks down due depletion of energy of one or more members. All sensor nodes are fixed but, the SN is static. They used a simple graph G(V, E) to represent a WSN, where V and E represents set of all sensor node and all edges, respectively. The graph will be an undirected graph. Hence, sensor node that does not belong to the backbone is termed as *leaf node*. Every node in the network has an EVBT node. They term this EVBT node as the dominator of the corresponding leaf node. They presumed each node v knows its N (v). They check two types of vertices. A tree node is a *fixed vertex* so that it cannot be removed from the EVBT. It means that this vertex will be a part of the final solution. If energy level of *Non-fixed* vertices is not above threshold energy level or its removal does not disjoin the resulting sub graph, then *Non-fixed* vertices will be removed. Therefore, at each step of the algorithm, at least one vertex is either fixed, or removed. It is presumed that at first, all the nodes in the network form the EVBT. At last, these non-removed and fixed vertices form the EVBT. They presumed, the sink node is leader to starts execution of algorithm.

At first, the leader will check its degree. If the degree is greater than one, then it verifies whether removing itself from the graph would disjoin the sub graph. Keeping this in view, criteria for being a member of EVBT are the node must have energy level greater than the threshold energy level, and also highest degree among all the neighbors of the node. When the algorithm terminated that result of iteration is an empty set of each node. At the first iteration, this list is empty. The EVBT computed at the end of all iterations. It at once updates its list of dominators, ever when a node chooses any node as its dominator. In this algorithm, every node in the network has one virtual backbone node, which it selects as its dominator. This dominator will be parent node for that node. Any node in the network will forward its packet to its dominator. In this way the packet eventually reaches the sink node. [1]

A CDS-based backbone was constructed to support the operation of an energy efficient network. That focused on three key ideas in their design: (1) a realistic weight matrix, (2) an asymmetric communication link between pairs of nodes, and (3) a role switching technique to prolong the lifetime of the CDS backbone. This algorithm is distributed in nature. It is deterministic.

Corresponding with the weight comparison among neighbors, some suitable nodes get selected as dominators. The set of dominators is a MIS. Those selected dominators are in conjunction with some Connector nodes (dominator2 nodes), then they form the dominating set of the network. Nodes that are not part of the dominating set remain as dominates and use neighboring dominators as next hops for data communication. This algorithm presumed that all nodes know two hops away neighborhood information and they have equal transmission range. Therefore, the weight matrix used in r-CDS algorithm is: $W_i(r_i, deg_i, id_i)$. Node i is more suitable to be a dominator than neighboring node j, if any of the following is true: [15]

$deg(u)$- The effective node degree of node u

$r(u)$- The number of 2-hop away neighbors

- $r(i) < r(j)$
- $r(i) = r(j)$ and $deg(i) > deg(j)$

- *r(i) = r(j) and deg(i) = deg(j) and id (i) < id (j)*

According to this algorithm, sensor nodes in the r-CDS algorithm can have three different colors: white, gray and black. At first, all nodes are white. In continue, all nodes change their color to either black or gray. Black nodes form network backbone, but gray nodes remain as dominatees. In their algorithm, nodes can broadcast the following messages: BLACK, GRAY and d(u) messages. After each node knows about its two hop away neighborhood, all nodes broadcast their r values. A node u can become dominator1, if it wins in the weight comparison. Then, node u turns black and broadcasts a BLACK message in the neighborhood. If a white node v receives BLACK message from its neighbor u, so v becomes gray and broadcasts GRAY message. This GRAY message includes the pair (v' s id, u' s id). If a black node w receives GRAY message from a gray node v and also the id of another black node u, and if w and u are not connected yet, then v becomes dominator2 node to connect u and w. In that case, after receiving a BLACK message from a node w, if a gray node u has already received a notification so that there is a two hop away black neighbor v sent through a neighbor x and v has not been connected to w yet, then both u and x become dominator2 nodes to connect node v and node w. [15]

An intelligent backbone formation algorithm was proposed according to distributed learning automata. The worst case running time and message complexity of the backbone formation algorithm has a $1/(1-\varepsilon)$ optimal size backbone. This was why that it was shown that through a proper choice of the learning rate of the algorithm, a trade-off between the running time and message complexity of algorithm with the backbone size can be made. [2]

At its implementation, a network of the learning automata isomorphic to the UDG was used. It is formed through equipping each host to a learning automaton. At each stage of this approach, the learning automata randomly choose one of their actions so that a solution can be found in the CDS problem. The created CDS is evaluated via the random environment and also the action probability vectors of the learning automata are updated depending on the response received from the their environment. At last, in an iterative process, the learning automata converge to a common policy so that it constructs a minimum size virtual backbone for us. The network graph is presumed to be undirected. Each host has a unique id and also requires that know its neighbors' id. With comparing the results of proposed algorithm with the other of the best known CDS-based backbone formation algorithms, the results show that their algorithm always outperforms the others in terms of the backbone size and also its message overhead is only a few more than the least cost algorithm. [2]

D. Hybrid Algorithms

Several backbone formation algorithms have been created so that they used from two or more categories such as clustering and CDS. We call their as *Hybrid* Algorithms. At first, these algorithms use clustering and then CDS. In blew some of algorithms have been shown.

One algorithm was proposed for constructing virtual backbone in Wireless Ad-hoc Sensor Networks. According to this algorithm, the sensor network is divided into clusters. This algorithm includes of two phases: (1) clustering nodes, (2) the CDS algorithm for intra clusters. It assumes all vertices are unmarked. Then, exchange their open neighborhood information with their one-hop neighbors. With using two pruning rules are provided to post-process the DS. If there exists a node v with higher id so that the closed neighbor set of u is a subset of the closed neighbor set of v, node u can be taken out from the CDS. [4]

Clique Clustering (CC) is the definition of a protocol for building and maintaining a connected backbone in WSN. In this protocol, the network is partitioned into clusters that are cliques. Thus, removing a node does not disjoin a cluster, and adding one needs simple operations for checking node acceptance to the cluster. The protocol includes three phases: (1) partitioning the network into clusters as *cliques,* (2) connection Clusters to form a backbone, (3) maintains the backbone connected. The cluster formation phase of the CC protocol produces a clustering that includes the following properties: (1) every non-cluster-head node has at least a cluster-head (2) every node in a cluster can communicate directly with every other node in the cluster, and (3) every non-cluster-head node affiliates to the cluster of the first cluster-head inviting it. In their opinion, every node knew its own unique id, its own weight and also the id and weight of each of its neighbors. [5]

The protocol is started through nodes that have the biggest weight among all their neighbors. These nodes send a message so that they will be cluster-heads. Upon receiving this message from one of its heavier neighbors, a node exchanges with the sender information. According to the received information, a cluster-head selects all smaller neighbors that can be affiliated to its own cluster so that maintaining the clique property and invites them to join it. A node decides to be a cluster-head itself, when whose heavier neighbors have joined other clusters or have finished inviting nodes and also that has not been invited to be part of any cluster. When the protocol terminates that every node belongs to a cluster being either a cluster-head or an ordinary node and also knows the role and cluster-head of all its neighbors. At last, to build these cluster connections, each cluster-head needs to know all its *neighboring cluster-heads*. With terminating the cluster formation phase, every node knows the id and weight of each neighbor and also the id and the weight of the cluster-head to which each neighbor is affiliated. Then, each node sending this information to its own cluster-head to select paths for a connected backbone. Figure 3 illustrates the final connected backbone. [5]

 ISBN: 978-1-61208-166-3

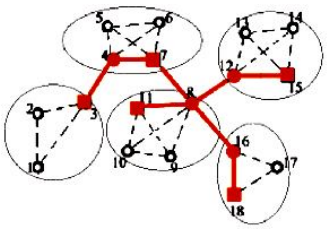


Figure 3. A WSN, the CC-induced clustering and a backbone connecting the cluster [5]

III. COMPARISON OF SOME ALGORITHMS

We have surveyed some well-known backbone formation algorithms in term of time and message complexity. Performance comparison of some algorithms is shown in the table below. We can see that proposed algorithms in [3], [11], [20], [22] have the less time and proposed algorithms in [11], [19], [20], [25] have the less message complexity among other algorithms in this table.

Also, time complexity of proposed algorithms in [13], [25], and message complexity of proposed algorithms in [3], [22] are equal. According to the table below, time and message complexity [2] is only slightly more than the least cost algorithm.

TABLE I. PERFORMANCE COMPARISON

Ref.	Performance comparison		
	Approximation factor	*Time complexity*	*Message complexity*
[2]	-	$O(\Delta)$	$O(n\Delta^2)$
[3]	$8opt+1$	$O(n)$	$O(n \log (n))$
[9]	-	$O(n \log^3 (n))$	$O(n^2 \log^3 (n))$
[11]	$147opt+33$	$O(n)$	$O(n)$
[12]-I	$2H(\Delta)+1$	$O((n+\lvert C\rvert)\Delta)$	$O((n \lvert C\rvert + m + n \log(n))$
[12]-II	$2H(\Delta)$	$O(\lvert C\rvert (\Delta+\lvert C\rvert))$	$O(n \lvert C\rvert)$
[13]	$O(n \log(n))$	$O(n^2)$	$O(n^2)$
[19]	-	-	$O(n)$
[20]	$O(n)$	$O(n)$	$O(n)$
[22]	$8opt$	$O(n)$	$O(n \log (n))$
[23]	$O(n)$	$O(\Delta^3)$	$\Theta(m)$
[25]	-	$O(n^2)$	$O(n)$

(n and m are the number of vertices and edges respectively, opt is the size of MCDS, Δ is the maximum degree, $\lvert C\rvert$ is the size of the computed CDS, H is the harmonic function.)

IV. CONCLUSIONS AND FUTURE WORKS

The backbone has proven to be an effective construct within which to solve a variety of problems that arise in WSNs. In this paper, we classified backbone formation algorithms and a few instances of these classifications and proposed hybrid approaches of these classifications. Also, we have surveyed some famous backbone formation algorithms in term of time and message complexity. Significant attention has been paid to backbone formation algorithms yielding a large number of publications. Backbone construction depends on the task to be carried. A backbone reduces the communication overhead, increases the bandwidth efficiency, decreases the overall energy consumption and at last increases network effective lifetime in a WSN. The important issue that we can be reached is selection algorithm according to our use.

ACKNOWLEDGEMENT

We would like to thank the reviewers who helped us to improve the quality of the current paper.

REFERENCES

[1] T. Acharya, S. Chattopadhyay, and R. Roy, "Energy-Aware Virtual Backbone Tree for Efficient Routing in Wireless Sensor Networks," in Proc. of Int. Conf. on Networking and Services, (ICNS '07), IEEE, pp. 96-102, Athens, Greece, June 19, 2007.

[2] J. Akbari Torkestani, M. R. Meybodi, "An intelligent backbone formation algorithm for wireless ad networks based on distributed learning automata," Computer Networks 54, pp. 826–843, 2010.

[3] K. M. Alzoubi, P. J. Wan, and O. Frieder, "New Distributed Algorithm Connected Dominating Set in Wireless Ad hoc Networks," Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Vol. 9, pp. 297-304, 7 January 2002.

[4] R. Azarderakhsh, A. H. Jahangir, and M. Keshtgary, "A New Virtual Backbone for Wireless Ad-hoc Sensor Network with Connected Dominating Set," Third Annual Conference on Wireless On-demand Network Systems and Services (WONS), pp. 191-195, 2006.

[5] S. Basagni, R. Petroccia, and Ch. Petrioli, "Efficiently reconfigurable backbones for wireless sensor networks," Computer Communications, Vol. 31, Issue 4, pp. 668-698, 5 March 2008.

[6] S. Basagni, M. Elia, and R. Ghosh, "ViBES: virtual backbone for energy saving in wireless sensor networks," Military Communications Conference (MILCOM), IEEE Press, Vol. 3, pp. 1240–1246, 31 October, , 2004.

[7] S. Basagni, "Distributed clustering for ad hoc networks, " Proceedings.IEEE, Fourth International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN '99), pp. 310 -315 , Australia, 23 Jun 1999.

[8] S. Basagni, A. Carosi, and Ch. Petrioli, "Sensor-DMAC: Dynamic Topology Control for Wireless Sensor Networks," In Proceedings of IEEE VTC 2004 Fall, Vol. 4, pp. 2930-2935, Los Angeles, CA, 26 September 2004.

[9] S. Butenko, X. Cheng, and Carlos A. S Oliveira, and P. M. Pardalos, "A New Heuristic For The Minimum Connected Dominating Set Problem On Ad Hoc Wireless Networks," Recent Developments in Cooperative Control and Optimization, pp. 61-73, Kluwer Academic Publishers, 2004.

[10] I. Cidon, O. Mokryn, "Propagation and Leader Election in Multihop Broadcast Environment," Proc. 12th Int. symp. Disrt. Computing, pp. 104–119, Greece, September 1998.

[11] X. Cheng, M. Ding, and D. Chen, "An approximation algorithm for connected dominating set in ad hoc networks," Proc. of International Workshop on Theoretical Aspects of Wireless Ad Hoc, Sensor, and Peer-to-Peer Networks (TAWN), 2004.

[12] B. Das, V. Bharghavan, "Routing in Ad-Hoc Networks Using Minimum Connected Dominating Sets *International Conference on Communications*. IEEE Int. Conf. Communications (ICC 97), Vol. 1, pp. 376-380, Montreal, Canada , June 1997.

[13] S. Guha and S. Khuller, "Approximation algorithms for connected dominating sets," Algorithmica, 20(4), pp. 374-387, April 1998.

 ISBN: 978-1-61208-166-3

[14] W. R. Heinzelman, A. Chandrakasan, and H. BalakrishnanD, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS), Vol. 8, pp. 10-20, January 2000.

[15] S. Hussain, M. I. Shafique, and L. T. Yang, "Constructing a CDS-Based Network Backbone for Energy Efficiency in Industrial Wireless Sensor Network," In Proceedings of HPCC, pp. 322-328, 2010.

[16] K. Islam, S. G. Akl, and H. Meiher, "A constant Factor Localized Algorithm for Computing Connected Dominating Sets in Wireless Sensor Networks," Proc of 14th IEEE International Conference on Parallel and Distributed Systems, (ICPADS), pp. 559-566, Melbourne, VIC, December 2008.

[17] B. Jeremy, D. Min, and T. Andrew and C. Xiuzhen, "Connected Dominating Set in Sensor Networks and MANETs," Handbook of Combinatorial Optimization, Springer, US, 2004.

[18] C.R. Lin, M. Gerla, "Adaptive clustering for mobile wireless network, " IEEE J Sel Areas Commun, Vol. 15, Issue 7, pp. 1265–1275, September 1997.

[19] Z. Liu, B. Wang, and Q. Tang, "Approximation Two Independent Sets Based Connected Dominating Set Construction Algorithm for Wireless Sensor Networks," Inform. Technol. J., Vol. 9, Issue 5, pp. 864-876, 2010.

[20] M. Rai, Sh. Verma, and Sh. Tapaswi, "A Power Aware Minimum Connected Dominating Set for Wireless Sensor Networks," Journal of networks, Vol. 4, no. 6, August 2009.

[21] M.T. Thai, W. Feng, and L. Dan, and Z. Shiwei and D. Ding-Zhu, "Connected dominating sets in wireless networks with different transmission ranges," IEEE Trans. Mobile Comput. , Vol. 6, pp. 721-730, 2007.

[22] P.J. Wan, K.M. Alzoubi and O. Frieder, "Distributed construction of connected dominating set in wireless ad hoc networks," Proc. of IEEE Conf. Computer and Communications Societies, pp. 1597-1604, New York, June 23-27, 2002.

[23] J. Wu, H. Li, "On calculating connected dominating set for efficient routing in ad hoc wireless networks," Proc. of ACMDIALM'1999, pp. 7–14, August 1999.

[24] D. Xia, N. Vlajic, "Near-Optimal Node Clustering in Wireless Sensor Networks for Environment Monitoring," In Proceedings of CCECE, pp.1825 – 1829, 2006 .

[25] R. Xie, D. Qi1, and Y. Li, and J. Z. Wang, "A novel distributed MCDS approximation algorithm for wireless sensor networks," Mobile & Wireless Communications, Vol. 9, Issue 3, pp. 427–437, March 2009.

[26] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed Energy Conservation for Ad Hoc routing ," In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom), pp. 70-84, Rome, Italy, July 16-21, 2001.

 ISBN: 978-1-61208-166-3

A Distributed Cluster-Based Localization Method for Wireless Sensor Networks

Carlos Moreno-Escobar*, Ricardo Marcelín-Jiménez†, Enrique Rodríguez-Colina‡ and Michael Pascoe-Chalke§
Department of Electrical Engineering
Universidad Autónoma Metropolitana
Mexico City, Mexico
*cbi208382775@xanum.uam.mx
†calu@xanum.uam.mx
‡erod@xanum.uam.mx
§mpascoe@xanum.uam.mx

***Abstract*—Node localization is a fundamental capability for several applications of Wireless Sensor Networks (WSN), such as security surveillance, fire detection, animal behavior monitoring, among others. Over the last decade, node localization in wireless sensor networks has evolved from centralized to distributed solutions. Therefore, more demanding conditions have arisen for new applications. These conditions come from massive node deployment and irregular topologies, requiring further analysis. In this paper, we present a method to reduce the signaling overhead due to a distributed localization procedure. This method consists of four stages: Based on the Awerbuch's γ synchronizer, the proposal divides the network into clusters. The cluster size is restricted by a growing factor defined by a cluster-head, i.e., a *leader*. Based on connectivity information, the distance between each pair of nodes, belonging to the same cluster, is calculated by the corresponding leader. Next, each leader solves locally a particular instance of the MultiDimensional Scaling (MDS) problem. Finally, a minimum set of beacons is selected on each cluster. This is in order to assemble each region into a global localization solution within a single system of reference. In our method, we turn the initial settlement into several smaller instances of the original problem which can be solved simultaneously and based on local resources. Simulation results show that this approach produces important savings on the required message exchange.**

Keywords-Localization; Partitioning; Synchronizer; Multidimensional Scaling.

I. I

Wireless Sensor Networks (WSN) is an emerging technology offering a wide spectrum of potential applications, and also a source of challenging problems to be solved [1]. Sensor node localization is a fundamental capability supporting most of these applications. A monitoring system, for instance, is able to determine the source of a critical event only if sensor nodes have accurate localization capabilities. Position awareness can also be used to enhance routing decisions because the nodes can send packets to their final destination based only on the position of nearby nodes, i.e., knowing the position of their neighbors. These routing strategies foster local work and, as a consequence, reduce the resource consumption [7], [11], [17].

For a small set of nodes, their individual positions can be programmed manually. In other cases, a Global Positioning System (GPS) may provide a convenient starting point. Nevertheless, the utilization of a GPS is limited due to budget constraints. Alternatively, a mobile node that is aware of its own position may perform a comprehensive tour across the underlying network. This mobile "coordinator" informs to each node about its corresponding position. It is important to recall that GPS is not recommended for indoor deployments, because satellite signal reception could be poor. When neither a GPS-based procedure, nor a manual programming are feasible, an automatic localization procedure is required.

Over the last years, an important number of proposals addressing self-configurable localization procedures have been published. Most of these proposals imply specialized solutions that perform well, merely under particular circumstances. Only a few of them have proved to be useful for general applications. However, even these general methods may show a poor performance under massive node deployment. In the meantime, technology trends show that WSN have permeated in different sector of our lives, as a consequence the number of deployed nodes is growing abruptly. In this context, scalability seems to be a new borderline in localization.

Despite of the fact that there is a well-known set of localization techniques offering general solutions [9], [10], [14], there are pending issues on the subject to be addressed. Scalability is one of these requirements to be fulfilled. The required methods developed to solve localization cannot be directly applied on a massive node deployment, due to their inherent message complexity, which limits the sensors energy budget. Apparently, the implicit agreement among scientists suggests that partitioning is a promising direction to address the scalability issue [18], [19]. From this approach, the underlying network is split up into regions or clusters. Each of the resulting clusters solves a reduced version of the localization problem. Finally, the local solutions are

 ISBN: 978-1-61208-166-3

assembled between each other, like the pieces of a puzzle, in order to build the global solution.

The partition methods so far developed to address scalability, start selecting a set of nodes; each of these appointed nodes is in charge to build a cluster. A cluster grows inviting its neighbor nodes to join the graph under construction. Nevertheless, to our best knowledge, these procedures do not control neither the cluster growth rate, nor the initial number of appointed nodes. In Shang [16], for instance, each node in the graph is regarded to be a cluster by itself, provided that it is not assimilated by a bigger one. Therefore, the partition message complexity may turn out to be excessive. In addition, the simultaneous construction of clusters may produce an unnecessary condition where neighbor clusters compete for nodes which still are unassigned and, having an impact again, on the number of exchanged messages. In contrast, our proposal provides a control on the number of nodes which are initially appointed to start the graph partitioning. It also offers a parameter k, that allows to "modulate" the growth rate and, indirectly, the order of the resulting clusters, which has a deep impact on the message exchange and time complexity.

In this work, we have addressed the localization problem for a wireless sensor network with arbitrary topology, where the nodes are deployed at fixed but unknown positions. It is also assumed that the nodes do not have implemented a complementary device to estimate either, power range or distance. The method that we introduce consists of four consecutive stages: in the first stage, the underlying graph associated with the network is partitioned with our modified method. In the second stage, for each of the resulting clusters, the appointed starting node calculates the distance in terms of hops, between every couple of nodes belonging to the same cluster. In the third stage, each leader solves locally a particular instance of the multidimensional scaling problem. Finally, in the last stage, a minimum set of three beacons is deployed on each cluster, to assemble each region into a global solution within a single system of reference.

The rest of this document includes the following parts: In Section II, we formally define the problem and introduce the related work. In Section III, we describe the stages of our method and present a collection of performance assessments. In Section IV, we present the analysis of the results. Finally, we present our final remarks in Section V.

II. D R W

From the point of view of graph theory , a network is modeled by a graph $G = (V, E)$, with an edge between any two nodes that can communicate directly with each other. In most of the cases, the multi-hop radio network is modeled as a Unit Disk Graph (UDG). In a UDG $G = (V, E)$, there is an edge $u, v \in E$ if and only if the Euclidean distance between u and v is less than or equal to 1.

An embedding of a graph $G = (V, E)$ in the Euclidean plane is a mapping $f : V \to \mathbb{R}^2$, i.e., each vertex v_j, $j = 1, 2, \ldots, n$ is identified by a point $x_j \in \mathbb{R}^2$ in the plane. A realization of a unit disk graph $G = (V, E)$, in the Euclidean plane is an embedding of G such that $u, v \in E \leftrightarrow d(f(v), f(u)) \leq 1$, where d is the Euclidean distance between two points. Therefore, localization consists of the realization of a unit disk graph in the Euclidean plane.

Localization is also considered as an optimization problem because given a set of measured distances between nodes that build a network, it is necessary to estimate the position of each node on a plane, up to rotations and translations. This is, while the error between the measured distances and the resulting distances from the estimated positions should be minimized. Practitioners introduce nodes with fixed and known locations, called *beacons* or *anchors*, in order to help the system to settle the reference coordinates.

In a sensor network in $\mathbb{R}^2$ there are two types of nodes: common sensors and anchors. A common sensor j is a node which position has to be estimated and, it is denoted by $x_j \in \mathbb{R}^2$, $j = 1, 2, \ldots, n$. In contrast, each anchor k, has a well known position $a_k \in \mathbb{R}^2$, $k = 1, 2, \ldots, m$. Let d_{ij} be the Euclidean distance between a pair of common nodes i and j, and let d_{jk} the Euclidean distance between a common node j and an anchor k.

There are unknown pairs of distances for some cases, so the pairs of nodes, for which mutual distances are known, are denoted as $(i, j) \in N_x$ distance between sensor and sensor and $(j, a) \in N_a$ between sensor and anchor pair, respectively. The localization problem in $\mathbb{R}^2$ can be stated as: given m anchor locations $a_k \in \mathbb{R}^2$, $k = 1, 2, \ldots, m$ and some distance measurements $d_{ij}, (i, j) \in N_x$, $d_{jk}, (j, k) \in N_a$, find the locations of common sensors, such that (ideally)

$$|x_i - x_j|^2 = d_{ij}^2, \quad \forall (i, j) \in N_x \tag{1}$$

$$|x_j - x_k|^2 = d_{jk}^2, \quad \forall (j, k) \in N_a \tag{2}$$

In many instances of the problem, noisy measurements introduce uncertainty on the calculations. Under such conditions, the problem can be reformulated as follows,

$$\min \{|x_i - x_j|^2 - d_{ij}^2\} \tag{3}$$

$$\min \{|x_j - x_k|^2 - d_{jk}^2\} \tag{4}$$

Notice that, anchors provide to the system with a fixed and absolute reference. Otherwise, when there are not anchors at all, the solution shows only relative positions. In other words, the "drawing" of the solution of the original network can be rotated, reflected or translated.

Different techniques have been proposed to *measure the distances* that make up the input set of the localization

 ISBN: 978-1-61208-166-3

problem. These techniques can be classified into two main categories: *range-based* and *connectivity-based* (also called range free). The former depends on a physical signal exchanged between two points which value is a function of the length, or relative position, of the line of sight from transmitter to receiver. e.g., Angle of Arrival (AoA), Time of Arrival (ToA), and Received Signal Strength (RSS).

The downside of range-based techniques is that they require additional hardware that may impact on the price of individual nodes. Besides, they can be very sensitive to environmental conditions. In contrast, *connectivity-based techniques* depend on the number of hops separating any pair of nodes. In this case, it is assumed that two nodes sharing an edge are separated, at most, by one distance unit. For both categories, indirect measurements may be propagated to other nodes in the network using a distributed procedure, such as the Distance-Vector algorithm (DV), where each node successively sends all the distances and the paths to reach the destinations that it already knows.

Research on localization methods has produced reasonable methods that offer excellent performance when the deployed sensors make up a dense and globally uniform network. Among the most relevant proposals, we found that Shang et al. [15] demonstrated the use of a data analysis technique called "MultiDimensional Scaling" (MDS) in estimating positions of unknown nodes. First, using basic connectivity or distance information, a rough estimate of relative node distances is made. Then, classical MDS (which basically involves using eigenvector decomposition) is used to obtain relative maps of the node positions. Finally, an absolute map is obtained by using the known node positions. This technique works well with few anchors and reasonably high connectivity. For instance, for a connectivity level of 12 and 2% anchors, the error is about half of the radio range.

Suppose we could count on the matrix $\mathbf{X}$, where each of its rows codes the position of a point on an Euclidean space. It is possible to calculate the square of the distances between any pair of points in this collection, according to the following expression

$$\mathbf{D(X)}^2 = \mathbf{c1}^T + \mathbf{1c}^T - 2\mathbf{XX}^T = \mathbf{c1}^T + \mathbf{1c}^T - 2\mathbf{B} \qquad (5)$$

where c is a vector made up with the elements from the diagonal of $\mathbf{XX}^T$. Then, we left and right multiply by a centering matrix and by the factor $-1/2$ to obtain

$$\begin{aligned} -\frac{1}{2}\mathbf{HD(X)}^2\mathbf{H} &= -\frac{1}{2}\mathbf{H}(\mathbf{c1}^T + \mathbf{1c}^T - 2\mathbf{XX}^T)\mathbf{H} \\ &= -\frac{1}{2}\mathbf{Hc1}^T\mathbf{H} - \frac{1}{2}\mathbf{H1c}^T\mathbf{H} + \frac{1}{2}\mathbf{H}(2\mathbf{B})\mathbf{H} \\ &= -\frac{1}{2}\mathbf{Hc0}^T - \frac{1}{2}\mathbf{H0c}^T + \mathbf{HBH} = \mathbf{B} \end{aligned} \qquad (6)$$

The first two parts of the equation are canceled since centering a vector made up with 1's produces a vector made up with 0's only ($\mathbf{1}^T\mathbf{H}=\mathbf{0}$). In turn, as we assume that the columns in $\mathbf{X}$ have a mean equal to 0, the centering matrices around $\mathbf{B}$ can be dismissed. Now we can see that if were able to factorize $\mathbf{B}$, according to an eigendecomposition, it will turn out that $\mathbf{Q}\Lambda\mathbf{Q}^T = (\mathbf{Q}\Lambda^{1/2})(\mathbf{Q}\Lambda^{1/2})^T = \mathbf{XX}^T$. There exist a tool that carries out this decomposition: the so-called power method, which is an iterative algorithm of complexity $O(n^3)$, where n is the number of unknown positions. We also tested an optimization approach, called the majorization method, which also is an iterative algorithm of complexity $O(n^2)$, but it is not based on eigendecomposition [3], [8].

III. M

A synchronizer is a set of techniques that enables an asynchronous system to emulate a synchronous behavior. To support this emulation, each node should be able to proceed with the next step of the given algorithm, only when it is granted that all the participants have accomplished the preceding step [13]. A node under these condition is said to be "safe".

Awerbuch [2] introduced three types of synchronizers: the α type, where each node exchanges messages with all its neighbors to let them know that it is safe. The β type, where a spanning tree is previously built. Here, a node sends a message to the root when the current step has finished. Once the root has collected these messages from each node, it broadcasts back a new message to the nodes on the tree, in order to notify the overall safety.

Finally, in the γ synchronizer the underlying graph is partitioned into a forest. Each of the resulting trees, also called cluster, runs a local version of the β synchronizer. However, when the nodes of a given cluster have finished the current step, the root exchanges messages with its neighbor trees to let them know of its local condition. When a root recognizes this condition on each of its neighbor subgraphs, it broadcasts back a new message to the nodes of its cluster to notify the overall safety.

The γ synchronizer requires an initialization procedure to split up the underlying graph in a set of disjoint clusters. The construction of a cluster starts when a given node, still unexplored, is appointed as a leader. The new leader begins aggregating layers to the cluster under construction. It is expected that a new layer that joins the cluster should contain, at least, as many nodes as, k times the total number of nodes already in the cluster. When this condition is not met, the cluster construction stops. Then, a new leader is found and the procedure starts again. Here, there is a special link, called "preferred", between the former tree and the new one about to be settled. This link fixes a relationship between the "ancestor" cluster and its "successor". When the cluster stops growing and a new node cannot be appointed, the leader in charge turns the control back to its ancestor tree.

 ISBN: 978-1-61208-166-3

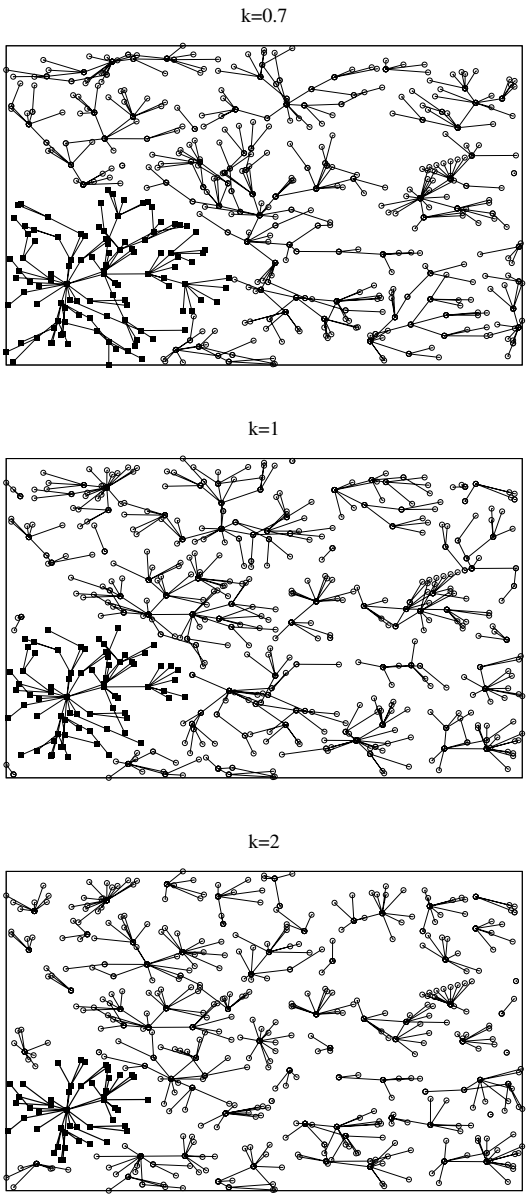


Figure 1. Building clusters with different values of k.

In due time, the receiving leader looks for a node to start a new successor tree, otherwise it also turns the control back to its own ancestor tree. According to this rule, the initial leader is able to recognize the moment when the partition is finished. The graph has been exhaustively explored and each node has been incorporated to a given tree. Our partitioning technique is based on a cluster growth parameter k. While the original work does not consider the values of $k < 1$, our implementation supports any value of $k > 0$. Nevertheless, when the partition process works under these "suboptimal" growth rate, each cluster grows with a very slow pace and the average cluster order increases.

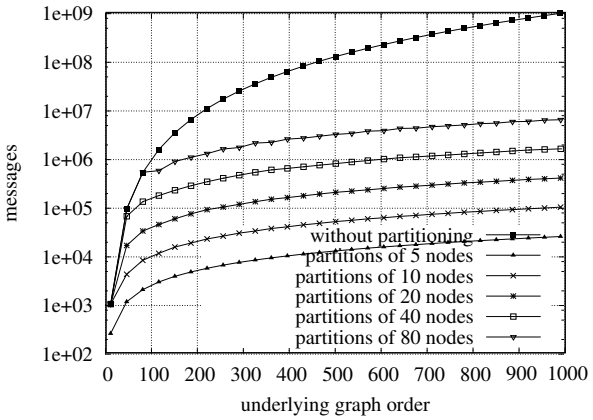


Figure 2. The benefits of partitioning

Besides this original partition procedure, herein called the "serial" partitioning, in this work we propose a new approach called the "concurrent" partitioning which once a cluster stops growing, each node in the border of the cluster selects a neighbor not yet assigned. Each of the newly selected nodes concurrently receives a signal permission to build a new cluster and as a result, preferred links between clusters are implicitly defined. In contrast to the original procedure, a given cluster, does not turn back the control to its ancestor when there is not any further place to explore. This feature does not preclude the further start of the next stage of our global localization method.

Figure 1 shows the behavior of the proposed partitioning algorithm for three values of k: 0.7, 1 and 2, respectively.

Our partitioning approach shows similarities with the work presented in [4], [12]. In contrast, our method does not have as many cluster construction rules as they do. Potential conflicts on the nodes' assignation are solved with a very simple rule: a free node, i.e., a node not yet assigned to a cluster, decides to be part of the first cluster that accepts it. Otherwise it will eventually turn into a new cluster leader on its own.

We developed a first assessment assuming that the system runs the localization procedure without a previous partitioning, then it is run by choosing a partitioning with different orders, i.e., the number of nodes on the resulting clusters. Figure 2 shows the overall message complexity associated to each test. Results show that partitioning saves expenses by several orders of magnitude.

In a second evaluation, we decided to compare the serial and the concurrent partitioning stages, for a value of $k = 1$. We test both over 50,000 different networks with 600 nodes each, which have been generated randomly. Our results provide a 95% confidence.

In the second stage of our localization procedure, a local instance of the Bellman-Ford [6] algorithm is executed on each of the resulting clusters to calculate the shortest

 ISBN: 978-1-61208-166-3

Table I

R

Variables	Serial	concurrent
Finalization Time[a]	809.25	213.01
Messages Transmitted[b]	28146.73	25445.32
Transmitted Messages per Node[c]	49.77	45.81
Leader's Transmitted Messages[b]	1920.82	2091.70
Leader's Transmitted Messages[c]	111.79	83.07
Avg. Number of Resulting Clusters	4.37	11.98
Avg. Cluster Size	19.336	11.11

[a] assuming that a message is transmitted using a time unit
[b] average total number of messages
[c] average individual number of messages

path between every couple of nodes belonging to the same cluster. The length of each path is considered a substitute for the Euclidean distance between nodes, which is required in the following stage. The routing algorithm requires the whole set of links that make part of the induced subgraph. In the original work, each node exchanges messages with all its neighbors, to calculate the shortest path between any couple of nodes. This approach produces a message complexity $O(|V|^3)$, where $|V|$ is the order of the underlying graph, i.e., the total number of nodes that make part of the graph. However, in wireless sensor networks, message transmission is an event that has a major impact on the nodes' energy supply. For this reason, we developed an alternative approach: using the tree that spans its cluster, each node sends to the root its neighbors list. The leader which is appointed as the root, collects this information to build a model of the underlying graph and then it runs a centralized version of the routing algorithm. This method has a complexity $O(|V|)$ on the number of exchanged messages.

When a leader has estimated the distances between any couple of nodes belonging to its cluster, it starts the third stage of our procedure: it solves a local instance of the MultiDimensional Scaling problem (MDS) i.e., it transforms a distance matrix into a list of vectors coding the positions where nodes can be preliminary located. We evaluated three alternatives, see Figure 3: a) the classical eigendecomposition, b) a second iterative procedure called the majorization method, i.e., Scaling by Majorizing a Complicated Function (SMACOF), and c) the combination of both. In this last procedure, we build a preliminary solution using method a) which is further supplied as a new input to method b). As it could be expected, this combined approach offers the best results. Nevertheless, the second alternative offers nearly the same quality under a lower price. Let us recall that eigendecomposition has a complexity order equal to $O(n^3)$, where n is the number of unknown positions. In contrast, majorization's complexity is $O(n^2)$.

To the authors' best knowledge, all the preceding work based on range free distance estimation assume a fixed hop

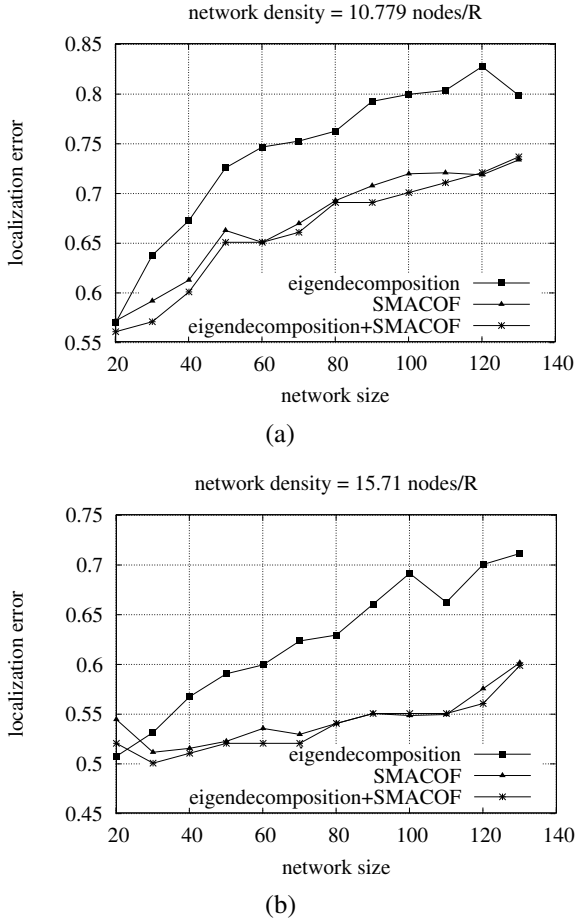


Figure 3. Localization error for two network densities.

length equal to one. Our contribution in this stage also consists on a test varying the hop length between 0 and 1. We found that, depending on the density of the underlying graph there is a hop value that optimizes the outputs of the MDS decomposition. These results are shown in Figure 4. We plotted the reconstruction error for ten different hop values and for three network average densities: 4, 8 and 12 $Nodes/Range$. In each case exists a hop value that minimizes the MDS reconstruction error. Also, note that the mean error decreases due to the network density increment.

When each leader has solved the local instance of the MDS, the geometric center of the cluster is considered at the position $(0, 0)$, or $(0, 0, 0)$, whether the nodes deployment are in 2D or 3D, respectively. This means that all clusters are logically overlapped. In the last stage of our procedure, we install a minimal set of beacons on each cluster in order to perform an isometric transformation that fixes the final coordinates of each region. And thus, a global and coherent picture of the system has been built.

Figure 5 shows the results of localization without and with partitioning, respectively. It is worth mentioning that

 ISBN: 978-1-61208-166-3

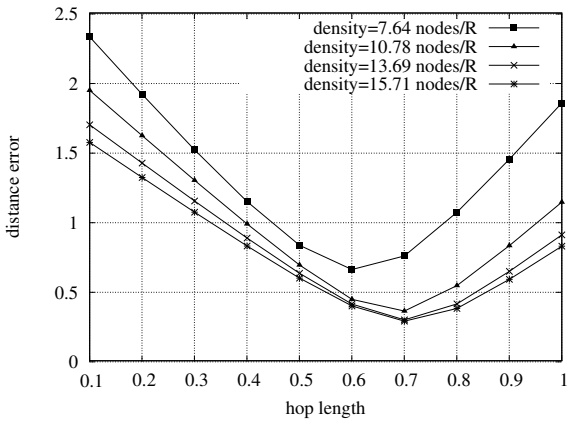


Figure 4. Reconstruction error varying the hop length in normalized units

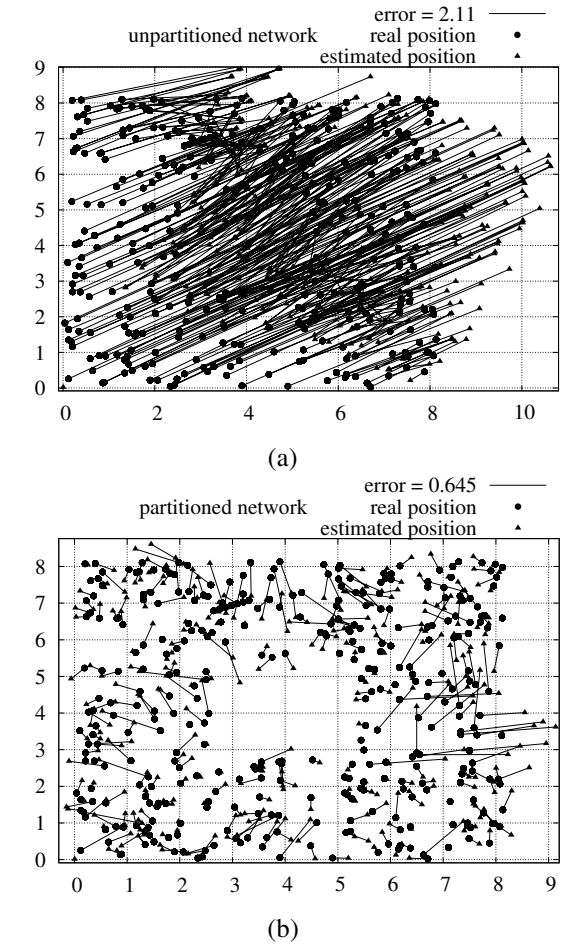


Figure 5. A network reconstruction. Fig. (a) reconstruction without partitioning. Fig. (b) reconstruction with partitioning.

compared to the proposal of Shang, our method achieves similar results. Nevertheless, from Shang's point of view in [15], each node starts working considering itself a cluster on its own and therefore, exchanging an excess of messages. We bound this message complexity by growing clusters during the first stage of our method. The underlying tree that spans the nodes of each cluster provides an efficient message exchange.

IV. A

We introduced a localization procedure which consists of four consecutive stages: in the first stage, the underlying graph is partitioned. In the second stage, each appointed starting node calculates the distance in hops, between every couple of nodes belonging to its cluster. In the third stage, each leader solves a local instance of the multidimensional scaling problem. Finally, in the last stage, we introduce a set of beacons on each cluster, in order to assemble each region into a coherent solution within a single system of reference.

Our partitioning technique is based on a cluster growth parameter k. We realized that a value of $k > 1$ offers better solutions in terms of: i) time to solve stage one, ii) it dramatically reduces the amount of resources involved on the overall procedure, iii) the reduced overall expenses are shared among a bigger number of participants, and iv) it produces more accurate solutions.

In the downside, we consider that the last stage limits the applicability of our method, but we have also identified that in order to overcome this limitation it is necessary to review the connection step between neighbor clusters, during partitioning. It is known that the rigidity of a graph is a desired property that facilitates its realization in an Euclidean space. Therefore, the more connections there are between neighbor clusters, the more rigid is the resulting combined graph [5]. If the number of links between clusters is maximized, then it is possible to use a minimal number of beacons to fix a global coordinated system.

The partitioning method works on any network, independently from its topology and size. We found, in fact, that this partitioning stage can cope with irregularities and obstacles and, it is a necessary step to scale up any localization algorithm. This is a well-known approach called "divide and conquer". The initial settlement turns in several local instances of the original localization problem, where it is assumed that these local instances are easier to solve than the initial settlement and can be solved simultaneously. In addition, this approach enforces the organization based on local resources and being also possible to achieve coordination in a global context.

The coordination is a key capability whose complexity depends on partitioning. If each node of the network were a cluster by itself, it would require to exchange messages with its immediate neighbors to achieve a coordinated action as it is proposed in the α synchronizer. Although it is a very fast strategy for the coordination, it can be very expensive in terms of the overall number of messages sent on each link of the underlying graph. In contrast, the β synchronizer can be used where a single spanning tree could be previously

 ISBN: 978-1-61208-166-3

built on the graph. And as a result, it would be necessary a minimal number of messages to coordinate the whole system. Whereas, the time required to achieve coordination may be as much as the necessary to travel the tree's longest path.

The γ synchronizer and the concurrent version proposed in this work find a trade-off between the number of messages and the time complexity in a coordination procedure, including the localization process.

V. C

The method that we introduce consists of four consecutive stages.

In the first stage, our solution comprises partitioning the underlying communications graph as proposed in [16], [18], [19]. However our method has a significant improvement in reducing computational resources, since we control the cluster grow rate, as well as the number of simultaneous clusters under construction. Indeed, our approach shares many ideas with the work of [4], [12].

In the second stage, for each of the resulting clusters, there exists an appointed starting node called leader, that calculates the distance in hop units between every couple of nodes belonging to its cluster. This operation can be solved using the distance-vector protocol. Nevertheless, this method requires a message exchange that has a major impact on the energy supply. Therefore, we developed an alternative method which reduces the message complexity from $O(|V|^3)$ to $O(|V|)$.

In the third stage, each leader solves locally a particular instance of the multidimensional scaling problem. An estimation of the distances between any couple of nodes lying on the same cluster is required as the input for this stage. In many cases the distance in hop units is regarded as a good alternative. Most of the authors, cited in the references, fixed the hop length to one. We found that the density of the underlying graph determines the optimum hop length for the MultiDimensional Scaling (MDS) decomposition method. Therefore, for each case there is a hop length that minimizes the MDS reconstruction error and for the examples shown here, the optimum hop length is around 0.7 instead of one.

Finally, in the last stage, a minimum set of three beacons is deployed on each cluster. Beacons provide a global reference that supports an isometric transformation of the cluster position. This means that the cluster can be rotated or translated to its final position within a single system of reference.

From our point of view, the saving achieved with our distributed method comes from different sources; evidently, the most important is that the method works simultaneously on the construction of several clusters. In addition and, in contrast with our method, the γ synchronizer spends more time on both, the selection of the next leader and appointing the preferred links.

The proposal presented in this work shows simple but significant contributions in each stage of the localization method. The results show that our solution significantly reduces the number of messages exchanged, which is indeed an important operation condition for wireless sensor networks.

For future work we are planning the implementation of our method on a real massive node deployment.

R

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 12, no. 2, pp. 291–301, June 1991.

[2] B. Awerbuch, "Complexity of network synchronization," *Journal of the ACM (JACM)*, vol. 32, no. 4, pp. 745–770, October 1985.

[3] T. Cox and M. Cox, *Monographs on Statistics and Applied Probability 59: Multidimensional Scaling*. London: Chapman and Hall, 1994.

[4] B. Derbel and M. Mosbah., "A fully distributed linear time algorithm for cluster network decomposition." in *16th IASTED International Conference on Parallel and Distributed Computing and Systems (PDCS04)*, 2004, pp. 548–553.

[5] T. Eren, D. K. Goldenberg, W. Whiteley, Y. R. Yang, A. S. Morse, B. D. O. Anderson, and P. N. Belhumeur, "Rigidity, computation, and randomization in network localization," in *In Proceedings of IEEE INFOCOM '04, Hong Kong*, 2004, pp. 2673–2684.

[6] L. R. Ford and D. Fulkerson, *Flows in Networks*. Princeton University Press, 1962.

[7] C. Georgiou, E. Kranakis, R. Marcelín-Jiménez, S. Rajsbaum, and J. Urrutia, "Distributed Dynamic Storage in Wireless Networks," *International Journal of Distributed Sensor Networks*, vol. 1, no. 3, pp. 355–371, 2005. [Online]. Available: http://dx.doi.org/10.1080/15501320500330695

[8] P. Groenen and I. Borg, *Modern Multidimensional Scaling, Theory and Applications*. New York: Springer-Verlag, 1997.

[9] G. Mao and B. Fidan, *Localization Algorithms and Strategies for Wireless Sensor Networks*. New York: Information Science Reference, 2009.

[10] R. Marcelin-Jimenez, M. Ruiz-Sanchez, M. Lopez-Villasenor, V. Ramos-Ramos, C. Moreno-Escobar, and M. Ruiz-Sandoval, *Emerging Technologies in Wireless Ad Hoc networks: Applications and Future Development*. IGI Global, 2010, ch. A survey on Localization in Wireless Sensor Networks.

[11] R. Marcelín-Jiménez, "Locally-constructed trees for ad-hoc routing," *Telecommunication Systems*, vol. 36, no. 1-3, pp. 39–48, January 2007.

 ISBN: 978-1-61208-166-3

[12] M. Mosbah, B. Derbel, and A. Zemmari, “Fast distributed graph partition and application.” in *In 20th IEEE International Parallel & Distributed Processing Symposium (IPDPS06). IEEE Computer Society Press*, April 2006.

[13] D. Peleg, *Distributed Computing. A Locality-Sensitive Approach*. Philadelphia: Society for Industrial and Applied Mathematics, 2000.

[14] L. M. Pestanao de Brito and L. M. Rodriguez Peralta, “Collaborative localization in wireless sensor networks,” in *Proceedings of the 2007 International Conference on Sensor Technologies and Applications*. IEEE Computer Society, 2007, pp. 94–100.

[15] Y. Shang and W. Ruml, “Improved MDS-based localization,” in *In proceedings of IEEE INFOCOM ’04, Hong Kong*, 2004, pp. 2640–2651.

[16] Y. Shang, W. Ruml, and Y. Zhang, “Localization from mere connectivity,” in *International Symposium on Mobile Ad Hoc Networking and Computing*. ACM, March 2003, pp. 201–212.

[17] J. Urrutia, *Routing with guaranteed delivery in geometric and wireless networks*. New York, NY, USA: John Wiley & Sons, Inc., 2002, pp. 393–406. [Online]. Available: http://portal.acm.org/citation.cfm?id=512321.512339

[18] L. Wang and Q. Xu, “GPS-free localization algorithm for wireless sensor networks,” *Sensors*, vol. 10, no. 6, pp. 5899–5926, 2010. [Online]. Available: http://www.mdpi.com/1424-8220/10/6/5899/

[19] C.-Y. Wen, Y.-C. Hsiao, and F.-K. Chan, “Cooperative anchor-free position estimation for hierarchical wireless sensor networks,” *Sensors*, vol. 10, no. 2, pp. 1176–1215, 2010. [Online]. Available: http://www.mdpi.com/1424-8220/10/2/1176/

 ISBN: 978-1-61208-166-3

Experiences in Ensemble-based Decision Systems for Wireless Sensor Networks

Madalin Plastoi, Ovidiu Banias, Constantin Volosencu and Daniel-Ioan Curiac
Automation and Applied Informatics Department
"Politehnica" University of Timisoara
Timisoara, Romania
{madalin.plastoi, ovidiu.banias, constantin.volosencu, daniel.curiac}@aut.upt.ro

Abstract— **Wireless sensor networks are often used to monitor and measure physical characteristics from remote or hostile environments. In these conditions, data accuracy is a very important aspect for the way these applications complete their objectives. In this paper, we introduce a new approach for detecting wireless sensors anomalies. Our methodology relies on an ensemble-based system, composed of multiple binary classifiers adequately selected to implement a complex decisional system on network base station.**

Keywords- wireless sensor networks, ensemble-based systems, sensors anomalies, data accuracy.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are collections of small hardware devices responsible for monitoring and detecting different kinds of events, in almost any types of environments. Very often, the correctness of the measured values provided by each sensor node is a critical factor for the evolution of the investigated environments. Therefore, for a WSN application it is very important to have robust and fail safe sensors that expose correct measurements and, respectively, to receive and work with correct sets of data. There are situations when one or several network sensors measurements are affected by a deliberate or an accidental anomaly, anomaly that can cause erroneous data, compromising the objectives of the entire network. These behaviors are usually caused by sensor hardware related problems or by security attacks, especially, intrusion attacks for compromising node and network data.

Previous relevant researches in the field of anomaly detection are developed around single binary classifiers that decide if the wireless sensor network activity is normal or abnormal by comparing the actual state of the WSN nodes with an intricate model of "correct behavior". This stratagem was implemented in different forms using intelligent algorithms.

In [1], Bhuse and Gupta enforce the idea of reusing the already available system information that is generated by different protocols, at various layers of the network. Their method incurs very little additional cost and thus is ideally suited for resource constrained WSNs.

The research described in [2] proposes a novel scheme to detect anomalies based on the localization of sensor nodes, called LAD – Localization Anomaly Detection. The scheme takes advantage of the deployment knowledge that is available in many sensor network applications and is implemented in a distributed way at the sensor node level.

Another interesting anomaly detection scheme is depicted in [3]. The proposed approach is able to detect anomalies accurately by employing only significant features of in-network data signals. For this, the authors used a mixture between the Discrete Wavelet Transform (DWT) and a competitive learning neural network called Self-Organizing Map (SOM).

In [4], a cooperative monitoring scheme to detect the displacements of sensor nodes by the cooperation of implicated nodes is described. The methodology is mainly based on the feasible Received Signal Strength Indicator (RSSI) values to collect the data of anomalous actions in WSNs.

In our paper, we propose a new approach for tackling these kinds of issues by implementing a powerful anomaly detection mechanism using an Ensemble-Based System (EBS). This ensemble-based system consists of multiple binary classifiers, each classifying every network node functioning as being accurate or erroneous. In our view, when dealing with dynamic and complex WSN's environments, we can model this proper functioning state based on past measurements recorded by the investigated node and respectively, on measurements recorded by all adjacent nodes.

Numerous research studies have exposed that EBS can outperform the single classifier approach [5]-[7]. The motivation behind this result is that by combining diverse and accurate models, we may improve the ensemble decision over each single classifier decision. The keystone of every EBS is represented by the notion of diversity between base classifiers which plays a crucial role in the success of ensemble learning techniques [8]. Intuitively classifiers are diverse if they make different errors.

The rest of the paper is organized as follows: Section 2 describes the proposed methodology. Section 3 presents the implementation and a case study. Finally, conclusions and future works are offered in Section 4.

II. METHODOLOGY FOR ENSEMBLE-BASED ANOMALY DETECTION

Generally, sensor anomalies are handled by dedicated rule-based decisional systems. For taking node behavior related decisions, it makes more sense to "ask" more than one decision making entities, because this practice assures undoubtedly a better, more informed, and trustable final decision.

 ISBN: 978-1-61208-166-3

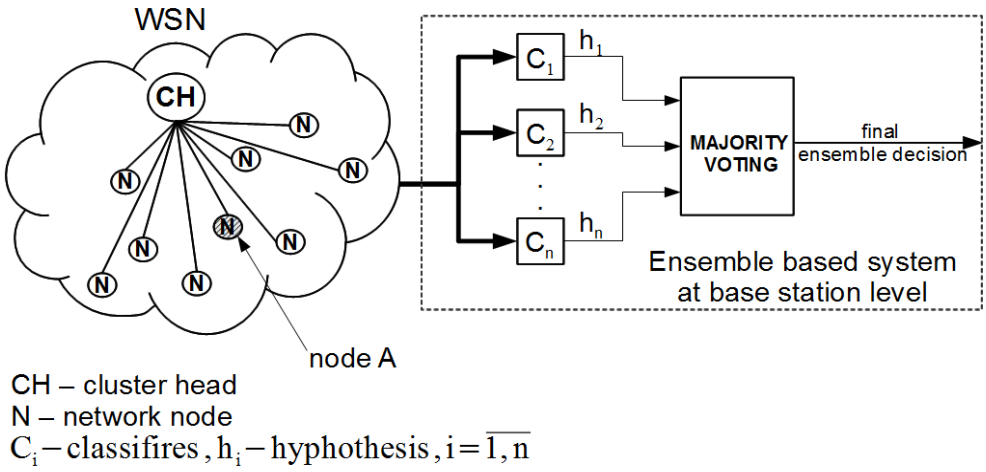


Figure 1. WSN with ensemble-based system at base station level

We name these decisional instances as classifiers or experts, and their collection an ensemble-based system [8][9].

Assuming that all the transmitted data within the network is confidential, the network may be a target for security attacks. In this paper, we address only those security attacks that try to prevent the network from the correct functioning by injecting erroneous sensor measurements. Worst, the network could experience hardware failures for one or more attached sensors that also mean erroneous sensor measurements. We developed and used an ensemble-based system to periodically investigate and detect each and every sensor node's anomaly. As presented in Fig. 1, this ensemble contains several binary classifiers that separately classify the state of each sensor as "reliable" or "unreliable". All the classifier outputs will be aggregated and the final ensemble decision will be generated, using a specific combination pattern [10]. The final ensemble decision will be further used by the base station to take all the required actions for the unreliable nodes.

The proposed methodology describes how the ensemble-based system is designed and used, and consists in the following set of steps:

- **Step 1.** First step in building the EBS is to choose both, the network data that needs to be classified, and the classification results set. Data for classification represents the measurements gathered by a specific node A, at a specific moment in time . Regarding the classification results, all possible results of a classification are called classes and form a set like:

$$\{\omega_1, ..., \omega_C\}, \quad (1)$$

where each ω_i represents a label or property associated with the classified data, and C represents the cardinal or the results set. In the case of anomaly detection, binary classification is used, meaning that we deal with only two possible classes: ω_1 - accurate data, labeled as "0" and ω_2 - erroneous data, labeled as "1".

- ***Step 2.*** In the second phase, the number of classifiers and their input data boundary are decided. In the case of a WSN cluster the EBS input data are represented by past measurements gathered by the node A and respectively, past and present measurements gathered by each of the node A neighbors $x_k(t)$, where k represents one of the neighbor nodes.

- ***Step 3.*** In the third phase, we design and train all classifiers. For EBS, when it comes to designing classifiers, there are several approaches that can be used, depending on the type of data and the real application [11]. All the designed classifiers need to be trained with real or sampled data accordingly to each classification class ω_i . Structurally, each classifier may contain prediction based algorithms, decisional trees and other artificial intelligence algorithms. As presented in (2), each classifier makes a hypothesis $h_j(t)$, indicating the class which better suits the classified data.

$$h_j(t) \in \{\omega_1, ..., \omega_C\} \quad (2)$$

- ***Step 4.*** The obtained classifiers form the EBS residing at base station level. Through a data acquisition interface, every measurement provided by a node A is classified by the ensemble-based system within the base station. This happens for a

fixed period of time and always ends by issuing $h_j(t)$ hypothesis.

- ***Step 5.*** All the classifiers results, $h_j(t)$, are then combined using a voting schema for taking the final ensemble decision. In this context, there are several approaches for combining classifiers results, some of them requiring additional trained classifiers, while others requiring only the $h_j(t)$ hypothesis [12]. The class ω_i that obtains the greatest number of votes $V_i(t)$ is established as the final ensemble decision. A simple vote $v_{ij}(t)$ indicates that hypothesis $h_j(t)$ selected the class ω_i, in other words, the classifier with *j* index, selected the class with *i* index. As presented in (3) and (4) the total number of votes V_i for the class ω_i counts all simple votes for that class.

$$V_i(t) = \sum_{j=1}^{C} v_{ij}(t) \tag{3}$$

$$v_{ij}(t) = \begin{cases} 1, & \text{if } h_j = \omega_i \\ 0, & \text{if } h_j \neq \omega_i \end{cases} \tag{4}$$

The ω_i class is chosen as final ensemble decision if it was chosen by at least one more than half the number of the classifiers; e.g: when having an ensemble of three classifiers, a decision is taken when at least two of three classifiers pass the same vote.

- ***Step 6.*** After the ensemble final decision has been taken, if the investigated node is found as having sensor anomalies, the network base station acts in consequence and excludes node's sensor from network functioning sensors sets for a limited period of time. As an example, this can be achieved based on the following rule: if the EBS indicated at least three times that the node A suffers from a sensor anomaly, the base station decides to inactivate the sensor. The base station could later reuse the sensor after repeating the EBS investigation for testing if new readings became appropriate.

III. IMPLEMENTATION AND CASE STUDY

For demonstrating the above concept and methodology we performed a case study that assumes the existence of a clustered WSN responsible for the temperature measurements into an unsupervised environment. Using an experimental network composed of nine Crossbow-Imote2 nodes equipped with ITS400 sensors boards, we developed an ensemble-based system that detects sensor measurements anomalies.

The experimental network measures the temperature in nine locations $\theta(t)$ and reports all measurements to a base station machine, through a gateway. This process is repeated for a fixed period of time. The measured temperature has values from 21°C to 21.6 °C. We simulate erroneous measurements gathered by a certain node of the network (node A), by artificially increasing the node A measured temperature using a heat lamp placed in the vicinity of node A at three distinct moments in the supervised period *T*. We designed and used three binary classifiers:

1. C_1 - an average based classifier that receives all present measurements of each of the node's A neighbors and computes an average measurement value as presented in (5).

$$x_{A(AV)}(t) = \sum_{i=1}^{k} x_i(t) / k \tag{5}$$

where *k* represents the number of neighbors. The classifier C_1 consists of an average computing block that provides a value that will be subtracted from the current measurement value of the sensor A. If the absolute value of the result exceeds a given threshold ε_{C_1} then the measurement provided by the node A is classified as abnormal.

2. C_2 - an autoregressive predictor based classifier that receives all past measurements of the node A and predicts its current measurement as shown in (6):

$$x_{A(AR)}(t) = a_1(t) \cdot x_A(t-1) + \ldots + a_n(t) \cdot x_A(t-n) + \xi(t) \tag{6}$$

where a_i are the autoregression coefficients, *n* is the order of the autoregression and ξ is assumed to be the Gaussian white noise. This classifier consists of a 3rd order autoregressive predictor that provides an estimated measurement for the sensor A that will be subtracted from the current measurement value of sensor A. If the absolute value of the result exceeds a given threshold ε_{C_2} then the measurement provided by the node A is classified as abnormal. The autoregressive predictor is designed and used similar as in [13].

3. C_3 - a neural prediction based classifier that receives all past and present measurements values

 ISBN: 978-1-61208-166-3

of each of the node's A neighbor nodes and predicts the present measurement of the node A using a transformation function similar with equation (7):

$$f(x) = K(\sum_i \nu_i g_i(x)) \quad (7)$$

where K is a composition function, ν_i are the network weights, and g_i is a vector containing neurons inputs $g = (g_1, g_2, ..., g_n)$. This classifier consists of a 3rd order feed forward neural network with two hidden layers of neurons, trained to provide a value that will be subtracted from the current measured value of sensor A. If the absolute value of the result exceeds a given threshold ε_{C_3} then the measurement provided by the node A is classified as abnormal.

In order to illustrate how our methodology works, we gathered temperature values from a group of nine sensor nodes placed in an indoor environment. The measurements provided by the sensor under investigation (sensor A) were intentionally perturbed using a heat lamp at three instants in time (t=15, t=20 and t=27 seconds). The temperature time series for sensor A and two of its neighbors are presented in Fig.2.

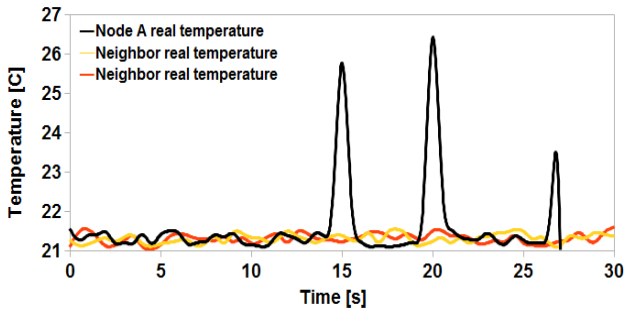
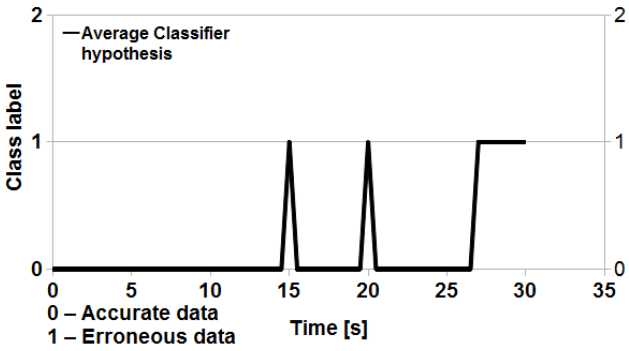


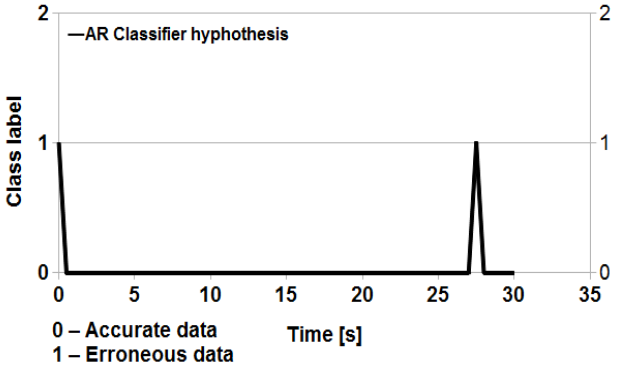
Figure 2. Measured temperatures for the node A and two of its neighbors

Each individual classifier uses an internal threshold value $\varepsilon_{C_i} = 2°C$, the order of autoregression for AR classifier was chosen to be n=3 and the neural network included in the NN classifier was trained using Levenberg-Marquardt algorithm.

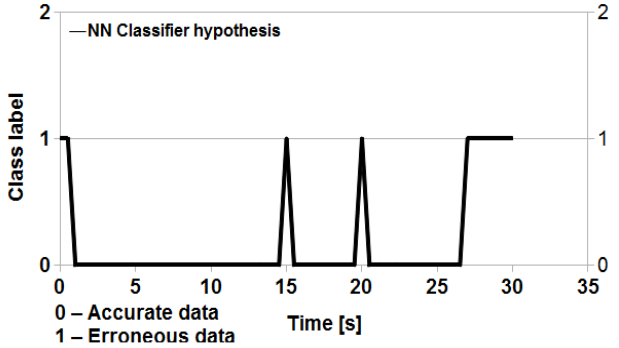
The required heterogeneity of the three binary classifiers included in ensemble plays its role, resulting different classifier hypothesis (Figs. 3a, 3b and 3c). Even if none of the classifiers works accurately in every situation, the ensemble decision obtained through the voting procedure is correct proving the power of ensemble (Fig. 3d).



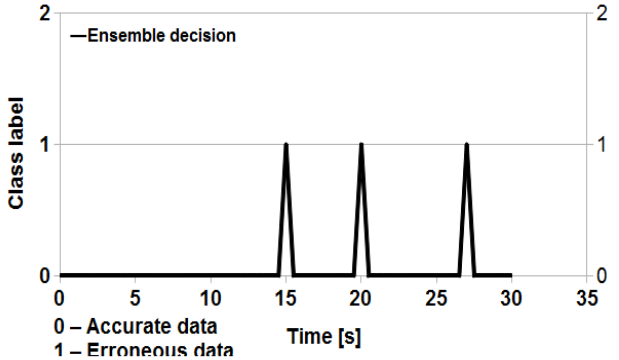
a) Average classifier hypothesis



b) AR classifier hypothesis



c) NN classifier hypothesis



d) Ensemble decision

Figure 3. The outputs of the three classifiers and of the EBS

 ISBN: 978-1-61208-166-3

IV. CONCLUSIONS AND FUTURE WORKS

Whenever we take a decision we want to have confidence in what we have decided. This is also applicable for all technical systems in general and wireless sensor network applications in particular. Being exposed to numerous risks, WSN often implement and use complex decisional systems for controlling their lifecycle, processed data and external threats [14]. In this paper we proposed an anomaly detection solution for WSN sensors using an ensemble-based system. The main advantage brought by this solution is that the final decision is taken based on the interrogation of multiple and different systems.

To fully assess the expected benefits, we continue to go further by improving the ensemble with new binary classifiers based on Adaptive Neuro-Fuzzy Inference Systems (ANFIS) or Support Vector Machine (SVM) and by automating the training and tuning processes of individual classifiers base on pair-wise diversity metrics.

ACKNOWLEDGMENT

This work was developed in the frame of PNII-IDEI-PCE-ID923-2009 CNCSIS - UEFISCSU grant and was partially supported by the strategic grant POSDRU 6/1.5/S/13-2008 of the Ministry of Labor, Family and Social Protection, Romania, co-financed by the European Social Fund – Investing in People.

REFERENCES

[1] Bhuse, V., and Gupta, A.: Anomaly intrusion detection in wireless sensor networks. In Journal of High Speed Networks, vol. 15, no. 1, pp. 33–51, 2006.

[2] Du, W., Fang, L., and Ning, P.: LAD: localization anomaly detection for wireless sensor networks. In Journal of Parallel and Distributed Computing, Volume 66, Issue 7, pp. 874-886, July 2006.

[3] Siripanadorn, S., Hattagam, W., and Teaumroong, N.: Anomaly Detection in Wireless Sensor Networks using Self-Organizing Map and Wavelets. In International Journal of Communications, Issue 3, Volume 4, pp. 74-83, 2010.

[4] Tang, J. and Fan, P.: A RSSI-based cooperative anomaly detection scheme for wireless sensor networks. International Conference on Wireless Communications, Networking and Mobile Computing, IEEE WiCom 2007, pp. 2783 – 2786 Shanghai, China, September 21-25, 2007.

[5] Giacinto G., Roli F., and Didaci L.: Fusion of multiple classifiers for intrusion detection in computer networks, Pattern Recognition Letters Journal, Volume 24, Issue 12, pp. 346-355, 2003.

[6] Giacinto, G., Roli, F.: Dynamic classifier selection. In MCS '00, Proceedings of the 1st International Workshop on Multiple Classifier Systems, pp. 177–189, 2000.

[7] Duin, R., Tax. D.: Experiments with classifier combining rules. In MCS'00, Proceedings of the 1st International Workshop on Multiple Classifier Systems, pp. 16–29, 2000.

[8] Polikar, R.: Ensemble Based Systems in Decision Making. IEEE Circuits and Systems Magazine, vol. 6, no. 3, pp. 21-45, 2006.

[9] Zhang C., Jiang J., and Kamel M.: Intrusion detection using hierarchical neural networks, Pattern Recognition Letters Journal, Volume 26, Issue 6, pp. 779-791, 2005.

[10] Ho, T.K., Hull, J.J., and Srihari, S.N.: Decision combination in multiple classifier systems. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 16, no. 1, pp. 66–75., 1994.

[11] Dietterich, T.G.: Experimental comparison of three methods for constructing ensembles of decision trees: bagging, boosting, and randomization. Machine Learning, vol. 40, no. 2, pp. 139–157, 2000

[12] Kittler, J., Hatef, M., Duin, R.P.W, and Matas, J.: On combining classifiers. In: IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 3, pp. 226-239, 1998.

[13] Curiac, D. I., Plastoi, M., Banias, O., Volosencu, C., Tudoroiu, R., and Doboli, A.: Combined Malicious Node Discovery and Self-Destruction Technique for Wireless Sensor Networks. In: Third International Conference on Sensor Technologies and Applications, SENSORCOMM '09, pp. 436 – 441, Athens, 2009.

[14] Plastoi, M., Curiac, D. I., and Banias, O.: Experiences in complex software development for wireless sensor networks. In: IEEE International Conference on Automation, Quality and Testing, Robotics, AQTR, vol. 3, pp. 1-6. Cluj Napoca, Romania, 2010.

 ISBN: 978-1-61208-166-3

Dust Monitoring Systems

Mokhloss I. Khadem, Valentin Sgarciu
Faculty of Automatic Control and Computer Science
"Politehnica" University of Bucharest
Bucharest, Romania
sml_ka@yahoo.com, vsgarciu@aii.pub.ro

Abstract— **In order to monitor dust in a city or on a large plant, we have designed a distributed network of nodes, which consists of smart sensors that detect dust. Such a network design must be scalable, to allow additional nodes to be added at any time. Each node should operate as a Plug-and-Play device, in order to provide minimal downtime for the network. With the help of microcontrollers embedded in each node it is possible for each sensor to upload measurement results directly to a server within the network. In order to keep a high compatibility of the sensor network and the associated network protocol requirements, an IEEE 1451 standard should be used, to provide a generic interface between a sensor and the outer network, regardless the network protocols. We have obtained new practical results, which we show as comparison between different dust measurement methods.**

Keywords- dust monitoring system; smart sensor; wireless network sensors

I. INTRODUCTION

Dust measurement has considerable significance and applications in modern life, depending on each field of application. Dust has impact on the environment, climate control, aviation, and health. We need to monitor the presence of dust in these fields and trigger an alarm system based on the specific levels of dust, in order to prevent accidents or malfunctions. Dust from outer space has a big effect on the climate of the planet. Ambient radiation heats dust and re-emits radiation into the microwave band, which may distort the cosmic microwave background power spectrum. In industrial applications for various plants and factories, where combustible dust or dust containing goods are produced, processed or stored, dust explosions may be expected if dust is not put under control.

To monitor dust in a city in particular or in any area in general, we have designed a distributed network of nodes, which consists of smart sensors that detect dust. Such a network design has to be scalable to allow additional nodes to be included at any time. Each node should operate as a Plug-and-Play device used to provide minimal downtime for the network. Through microcontrollers embedded in each node, each sensor can upload measurement results directly to a server within the network. In order to keep high compatibility between the sensor network and the associated network protocol requirements, an IEEE 1451 family of standards [4] should be used to provide a generic interface between a sensor and the outer network, regardless of the network protocols.

By networking and deploying an array of sensors, we obtain several benefits such as area coverage and connectivity. A distributed network incorporating sparse network properties will enable the sensor network to span a greater geographical area without adverse impact on the overall network cost. We will use wireless sensor networks and connect them together at sink nodes. The clustering of networks enables each individual network to focus on specific areas and shares only relevant information with other networks, enhancing the overall knowledge base through distributed sensing and information processing.

All the nodes shall transmit information through the network to the main server to process and record into a database the monitoring information. Based on the configured dust acceptance levels on the server, an alarm can be triggered from the server and sent back through the network to the corresponding devices.

The rest of the paper is structured as follows: Section 2 presents the state of the art in dust measurement, Section 3 describes the architecture of the system we propose, Section 4 analyses some experimental results, and Section 5 draws the conclusions of this work.

II. STATE OF THE ART IN DUST MEASUREMENT

Several measurement principles for dust detection are used, among which we can mention: the Gravimetric measurement [1], Triboelectric measurement [2] and Optical measurement [10]. Each of these enumerated measurement principles is suitable for a specific application based on the intensity of dust pollution, water vapor proportion and dimensions of the measurement zones [1, 2].

The gravimetric principle describes a set of methods in analytical chemistry for the quantitative determination of an analysis based on the mass of a solid. A simple example is the measurement of solids suspended in a water sample: A known volume of water is filtered, and the collected solids are weighed [2, 9].

The triboelectric effect (also known as triboelectric charging) is a type of contact electrification in which certain materials become electrically charged after they come into contact with another different material and are then separated (such as through rubbing). The polarity and strength of the charges produced differ according to the materials, surface roughness, temperature, strain, and other properties. We can use this effect to measure the quantity of dust [2, 9].

 ISBN: 978-1-61208-166-3

The optical measurement of dust implies measuring the light transmission using optoelectronic techniques. The measuring principle is based on the attenuation of the intensity of a light beam, penetrating a cloud with solid particles, by absorption and dispersion. The ratio between the resulting and the initial intensity is defined as transmission [1, 8, 9].

There are several applications implying the measurement of dust in liquids, and the most suitable method to be used is the gravimetric principle. The triboelectric dust measurement devices can be used for bag, ceramic and cartridge filters or cyclones where indicative monitoring is required. Dust detectors using the optical measurement principle are usually used for continuous measurement of medium and high dust concentration on industrial plants as well as for monitoring limited values, as required by the applicable directives and regulations. The optical principle is also used to measure the concentration of dust in saturated gas downstream of desulfurization plants, downstream of wet scrubbing plants and wet exhaust gas. This last method of dust measurement is used in the development of the wireless monitoring system described in this paper. Figure 3 shows the advantage of using this system compliant sensors and devices to communicate wirelessly, eliminating the monetary and time costs of installing cables to acquisition points. This document explains not only how to setup system, but also how to compare the dust sensor according application and dust type. Also the user of this system can make configuration threshold according to the specific application for which the dust detection sensor network is used.

III. SYSTEM ARCHITECTURE

To measure and monitor the dust level in a city or on a plant, we propose the distribution of several nodes, from N_1 to N_n. Each node is a smart sensor operating in a Plug-and-Play mode and each node communicates to a server, over a wireless network by using the IEEE 1451.5-802.11 standard [4].

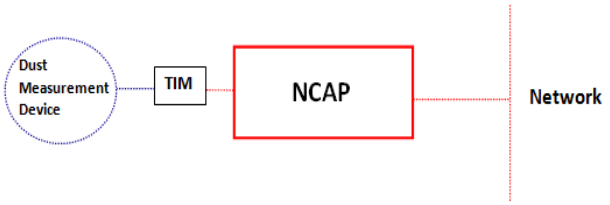


Figure 1. Dust Smart Sensor.

This standard will enable 1451 compliant sensors and devices to communicate wirelessly, eliminating the monetary and time costs of installing cables to acquisition points. IEEE is currently working on three different standards, 802.11, Bluetooth and Zigbee [4].

The server acquires the monitoring information from the distributed network of smart sensors and processes this data via specialized software. Based on the user configured thresholds, the server will either take no action, but to record the data for statistic purposes, or send a signal to other devices for specific tasks, such as air trap shutdown or activating air recirculation systems, in case the configured thresholds have been surpassed to a critical level. This depends on the specific application for which the dust detection sensor network is used.

Each node connects with a smart sensor, namely: a dust detection device, transducer interface model (TIM) and Network Capable Application processor (NCAP) as shown in Figure 1.

A TIM (Transducer Interface Module) is a module that contains the interface, signal conditioning, Analog-to-Digital and/or Digital-to-Analog conversion and in many cases, it also contains the transducer. A TIM can range in complexity from a single sensor or actuator to a module containing many transducers including both sensors and actuators.

An NCAP is the hardware and software that provides the gateway function between the TIMs and the user network or host processor (the transducer channel). The IEEE 1451 standard defines the communications interface between an NCAP or host processor and one or more TIMs. An NCAP or a host processor controls a TIM by means of a dedicated digital interface medium. The NCAP mediates between the TIM and a higher-level digital network. The NCAP may also provide local intelligence.

Figure 2 shows the implementation of a Wireless Sensor Network (WSN) based on IEEE 1451.0 and 1451.5-802.11, using IEEE 1451.2 sensors. This WSN consists of one NCAP node and one WTIM node. An IEEE 1451.2 sensor is connected to the WTIM via a serial port.

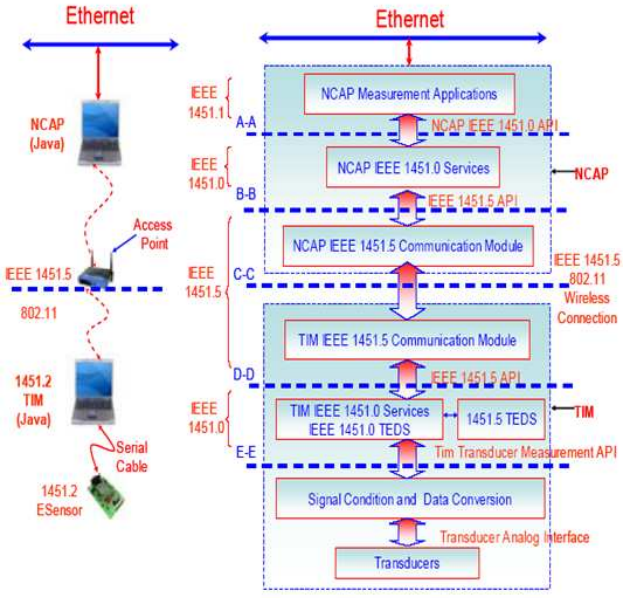


Figure 2. WSN based on IEEE 1451.0 and 1451.5-802.11.

The NCAP can communicate wirelessly with WTIM through IEEE 1451.0 and 1451.5 protocols using the client-server and publisher-subscriber communication models. The client-server and publisher-subscriber communications between the two nodes can be implemented using

 ISBN: 978-1-61208-166-3

Transmission Control Protocol / Internet Protocol (TCP/IP) and Transmission Control Protocol / User Datagram Protocol (TCP/UDP), respectively.

We can integrate a dust smart sensor node into a network of smart sensors, as shown in Figure 3, from Node 1 to Node N, according to the application requirements and the number of sensors needed.

The Server monitoring software can be implemented with the Java programming language, for full flexibility and compatibility.

By using Java, we will also have the advantage of portability, having standardized libraries that provide a generic way to access host-specific features such as threading, network access and automatic memory management.

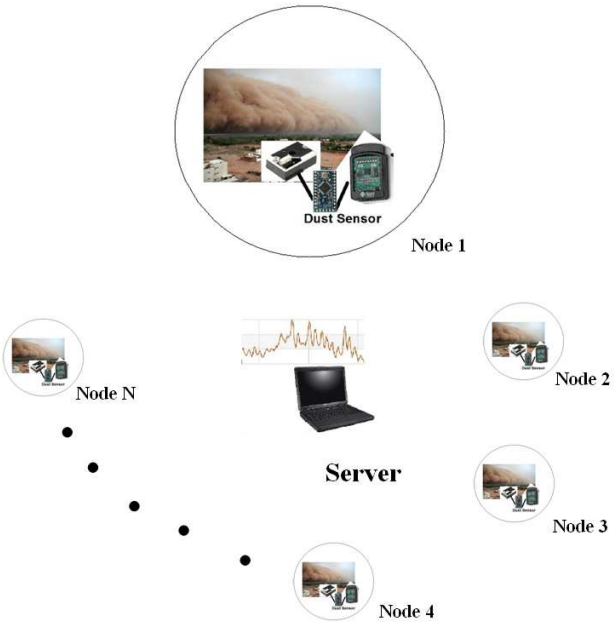


Figure 3. Dust monitoring network.

IV. EXPERIMENTAL RESULTS

Each node was implemented using a Sharp GP2Y1010AU0F dust sensor that is based on the optical principle [8]. The sensor was tied to a Sun SPOT (Sun Small Programmable Object Technology) device, which is an open source wireless sensor network (WSN) mote developed by Sun Microsystems. The device is built upon the IEEE 802.15.4 standard and on the Squawk Java Virtual machine [7]. This allowed us to use the Java programming language to control the data acquisition from the Sharp sensor. The connection from the Sun Spot to the server was assured by a standard wireless connection.

The following lines of code were used to acquire data from the Sharp dust sensor:

```
"byte[] buffer = new byte[64];
try {
  demoBoard.readUART(buffer, 0, buffer.length); returnString = returnString +
  new String(buffer, "US-ASCII").trim();
  dustLevel = Integer.parseInt(returnString);
  }
```

The first line of code in the try clock reads the serial port of the dust sensor and returns the value as an array of bytes. .

The results are sent to the server through the following simple lines of code:

```
 "System.out.print(dustLevel);
  System.out.println(", " +String.valueOf(dustLevel));
leds.getLED(0).setOff();"
```

The experimental results were obtained by using several types of dust: sand dust with high granularity, plaster dust and smoking ash. Another dust detector has been used as a reference, based on the gravimetric principle "D-RC80 Automatic sampling device for Gravimetric Dust measurements", used as reference measuring system. The output of the sensor is sent through the Sun Spot to the server, where we used the LiveGraph program to plot the results. During the experimental phase, modern test methods were taken in to account, such as they are described in the dedicated literature [5, 6].

For the smoking ash, we obtained a fluctuation in the results, as shown in Figure 4, but with a solid average, which was within the values obtained by using the dust detector with gravimetric principle.

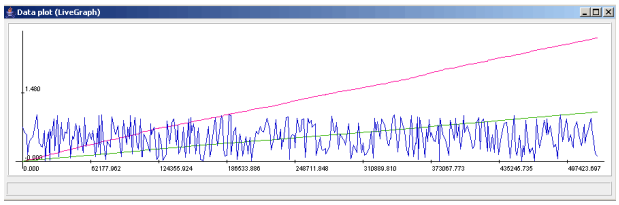


Figure 4. Live Graph plot of smoking ash measurement.

TABLE I. MEAN EXPERIMENTAL RESULTS

Type of dust	Mean measurement with our setup	Gravimetric measurement
Sand	3.2 mg/s	3.6 mg/s
Plaster	2.4 mg/s	4 mg/s
Smoking Ash	1.23 mg/s	1 mg/s

The experimental results depicted in Table 1 are encouraging regarding the accuracy of the optical measurement, compared to the ones made with a gravimetric device. The mean values were calculated based on 20 measurements.

We also conducted tests with two sensors sending data simultaneously to the server and we obtained satisfactory

 ISBN: 978-1-61208-166-3

results. The server was configured with a service, programmed in Java, which allowed multi threaded communication. Our tests were made only at a distance of maximum 30 meters, between the node and the server, due to the wireless technology limitations, but this could be easily improved for higher distances by using a signal repeater.

V. CONCLUSIONS AND FUTURE WORKS

By using a smart sensor network we can monitor and measure the dust in any environment: urban or industrial. The area coverage of a dust monitoring network can be expanded depending on the needs, without any adverse impact to the overall network cost.

Each dust sensing device can focus on a specific area and by managed as a single entity or in turn it can be used as only one point of presence in an area, contributing to the overall accuracy of the measurement. The more nodes we will use for a dust monitoring network, the greater the accuracy of the gathered information will be.

The human interaction will be greatly reduced by using such a network. Also, compared to human observation, the introduction of a smart sensor network is more flexible when it comes to dangerous and hostile environments where humans can't penetrate, allowing access to information previously unavailable from such close proximity.

Sensor scheduling can be obtained by enabling the sensor nodes to modify communication requirements in response to network conditions and events detected.

The optical sensor that we used can easily become a node in a multi node network, and connect to a server over a wireless network.

From the experience of already existing devices, we can expect that in the coming decade a large number of monitoring systems for all physical phenomena will emerge, with great application in the human health sector, industrial sector and the environment. The monitoring system gives excellent opportunities to design and configure many types of sensors to monitor and control all physical phenomena for many applications based on people demands. Like example use similar systems to compare the accuracy and application by use tripoelectric device and compare with optical sensor and gravimetric sensor. Due to the large dust in Iraq, there is an intention to set up a system for monitoring the dust in Baghdad and I am now on the agreement with the relevant authorities.

REFERENCES

[1] Jacob Fraden, "Handbook of modern sensors physics , designs and applications", Springer, Third edition, 2004.

[2] Grard C.M. Meijer, "Smart sensor systems", Delf University of Technology, 1st Edition, 2008, Netherlands.

[3] Occupational safety and health administration (OSHA), the Massachusetts Office of the State Fire Marshall and the Springfield Arson and Bomb Squad, "Joint Foundry Explosion Investigation Team Report.", Springfield, MA, Safety and Health Information Bulletin, 31.07.2005.

[4] IEEE Instrumentation and Measurement Society "IEEE 1451.5, Standard for a Smart Transducer Interface for Sensors and Actuators– Wireless Communication and Transducer Electronic Data Sheet (TEDS) Formats", TC-9, The Institute of Electrical and Electronics Engineers, Inc., New York, N.Y. 10016.

[5] Richard Bono, Mike Dillon, Kevin Gatzwiller and David Brown, "New developments in multichannel test systems, sound and vibration magazine", August 1999.

[6] Pan Fu, A.D. Hope and G.A.King, "An intelligent tool condition monitoring system", The 52nd meeting of the society for machinery failure prevention technology, pp.397-406 (1998).

[7] Sun SPOT Programmer's Manual rel. 6.0, Sun Labs, November 2010.

[8] Sheet No.: E4-A01501EN GP2Y1010AU0F Compact Optical Dust Sensor, SHARP Corporation, 2006.

[9] Jong-Won Kwon; Yong-Man Park; Sang-Jun Koo; Hiesik Kim, "Design of Air Pollution Monitoring System Using ZigBee Networks for Ubiquitous-City", Convergence Information Technology, 2007. International Conference on , vol., no., pp.1024-1031, 21-23 Nov. 2007.

[10] John Webster (editor-in-chief), "The Measurement, instrumentation, and Sensors Handbook", CRC Press, 1999.

 ISBN: 978-1-61208-166-3

Evaluation of Adaptive Interference Cancellation in Chirp Spread Spectrum-based Communication Systems

Martin Brandl, Karlheinz Kellner
Center for Biomedical Technology
Danube University Krems
Krems, Austria
Martin.brandl@donau-uni.ac.at, Karlheinz.Kellner@donau-uni.ac.at

***Abstract*—For data transmission in heavily distorted indoor environments, chirp-based spread spectrum systems operating in the 2.45 GHz ISM band are well applicable. The robustness of spread spectrum systems against narrow band jammers is given by their compression gain, which is defined by the time-bandwidth product of the spreading signal. Using chirp matched filter systems, jammers can pass through the receiver filter and are only weighted by its transfer function. Dividing the receiver chirp filter into time (equivalent to frequency) intervals, a jammer can be suppressed by switching off the corresponding frequency interval, leading to an increased jamming robustness. Due to its simplicity, this is suitable even for low cost systems. Theoretical and experimental results prove the capability of the method.**

Keywords—spread spectrum, chirp, matched filter, FPGA design

I. INTRODUCTION

Nowadays, wireless communication systems employ digital modulation and advanced signal processing capabilities. Wireless transmission systems for short range applications are a fast growing topic in communication engineering. There are many fields of applications, from the transmission of speech and video in cordless telephone sets to high data rate communication in local area networks, for example.

Low power devices (LPDs) for license free operation in the so-called industrial, scientific, and medical frequency bands/ISM (ISM bands are defined by the International Telecommunication Union—Radio Communication Sector /ITU-R in 5.138, 5.150, and 5.280) have been placed on the market. In particular, communication systems for wireless local area networks (WLANs) are targeted for applications in large indoor areas, offices with wiring difficulties, branch offices, and temporary indoor networks. WLANs are appropriate for unwired small business offices such as real-estate agencies, where only a few terminals are needed and where there may be frequent relocations of equipment to accommodate reconfiguration or redecoration of the office space. Therefore, for wireless operation in local area networks, systems have been introduced especially for systems of micro- and picocells within buildings, including the option of roaming. Since an indoor environment with a dominant multipath propagation scenario [1] and unlicensed operation are difficult to beat using narrow band systems, spread spectrum sets have been introduced [2]. They operate with direct sequence modulation with a spreading factor of approximately 10 or in frequency hopping mode with a limited number of channels. Such WLAN systems have succeeded in operation and number, respectively. The WLAN modulation, transmitted spectral distribution, media access control, interoperability, and so on are standardized in IEEE 802.11.

For indoor environments, the coherence bandwidth is typically 2 to 5 MHz for the 2.45 GHz ISM band [3]. Therefore, the bandwidth of the transmission system should be at least two times the channel coherence bandwidth, resulting in narrow band communication systems which are difficult to operate in industrial environments. To overcome this problem, available spread spectrum systems for WLANs use approximately 20 MHz of the 83.5 MHz bandwidth allowed in the ISM band at 2.45 GHz. For indoor data communication, a broad band chirp spread spectrum system has been developed.

II. CHIRP-BASED SPREAD SPECTRUM SYSTEMS

Due to the large bandwidth covered in chirp spread spectrum systems, they show good resistance against selective fading due to multipath propagation. Increasing attenuation on the propagation path because of shadowing results in a decrease in received energy and raises the bit error rate. The influence of Rayleigh fading has been observed to be mostly insignificant for broad band spread spectrum systems. If strong jammers occur, most conventional systems are disturbed heavily. In spread spectrum systems, the signal to interference ratio (SIR) at the detector is increased due to the correlative signal processing gain. The "capability" of jammer suppression by impulse compression on a signal matched filter (MF) is given by the time-bandwidth product (T·B) of the spreading signal [2]. The upper limit for the total jammer power (in dB) within the signal spreading bandwidth is the SIR at the detector required for the minimum error probability minus the MF compression gain (T·B product) in dB. It must be considered that in the case of weighted chirps, which are typically used in communication systems to get a higher peak to side lobe ratio, the effective T·B product becomes smaller than without weighting, resulting in a reduced jamming resistance.

 ISBN: 978-1-61208-166-3

The developed chirp spread spectrum data transmission system utilizes linear chirps for spread spectrum generation. A linear chirp is characterized by linear frequency modulation and can be divided into up-chirps where the angular frequency is increasing over time and down-chirps where the angular frequency is decreasing over time. Chirp signals are characterized by their start and stop frequencies which define the chirp bandwidth B_c and the time duration of the chirp signal T_c. The matched filter compression gain G_c of a chirp spread spectrum signal is therefore given by its time-bandwidth product $G_c = B_c T_c$.

In our system, the effective T·B product was approximately 13.6 dB instead of the theoretical maximum of 19 dB (T_c = 2µs, B_c = 39 MHz, where f_{chirp_start} = 1 MHz and f_{chirp_stop} = 40 MHz; 10*log(T_cB_c) = 19 dB). The chirp signals are Hamming weighted, which reduces the compression gain by 5.35 dB in comparison to non-weighted signals [4]. Signal weighting raises the side lobe suppression by about 30 dB, which is necessary for a reliable intersymbol interference (ISI) reduction [4].

Our chirp-based data transmission system is based on binary orthogonal shift keying (BOK) where the data symbols are coded with up- and down-chirps [5]. In Figure 1 the principle of chirp BOK data transmission is illustrated. In the transmitter, a logical data symbol "1" is coded with an up-chirp signal and a logical data symbol "0" is coded with a down-chirp signal. Both chirp signals are orthogonal, which means that the cross-correlation function is approximately zero. The receiver consists of two matched filters corresponding to the transmitted chirp signals. In the case of a transmitted up-chirp, the up-chirp MF delivers the chirp autocorrelation function at the output with a compression gain G_c. At the same time point, the down-chirp MF delivers the chirp cross-correlation function, which is approximately zero. The reconstruction of the transmitted data symbols is done by a comparator circuit which compares the MF output amplitudes at each symbol interval.

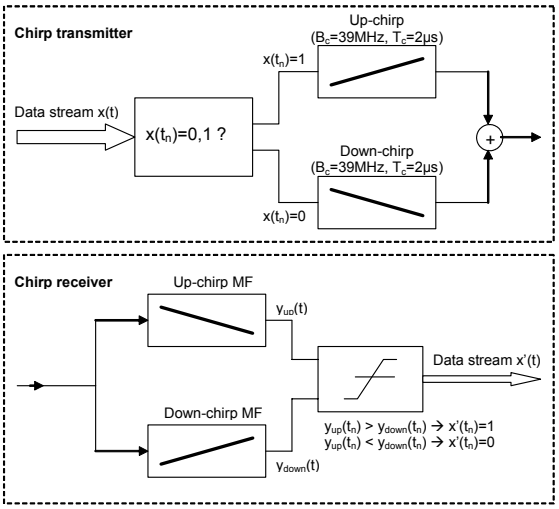


Figure 1. Principle of chirp-based data transmission.

As discussed before, spread spectrum communication systems are robust against fading and jamming but there are clear limits given by the spreading bandwidth and the MF compression gain. To improve the robustness of chirp spread spectrum systems against jamming, which is mainly caused by microwave ovens and other communication systems operating in the same ISM band, we used gated chirps where the jammed chirp subband can be turned off. For linear chirp signals, in the time domain a certain signal interval of the chirp signal corresponds to a certain frequency interval in the frequency domain (Figure 2). In contrast to [5], where an analog implementation of gated chirps based on tapped SAW chip filters is presented, this paper deals with a fully digital chirp filter implementation. This offers several advantages especially in the fully flexible number of chip subbands as well as on the design of the implemented filter transfer function.

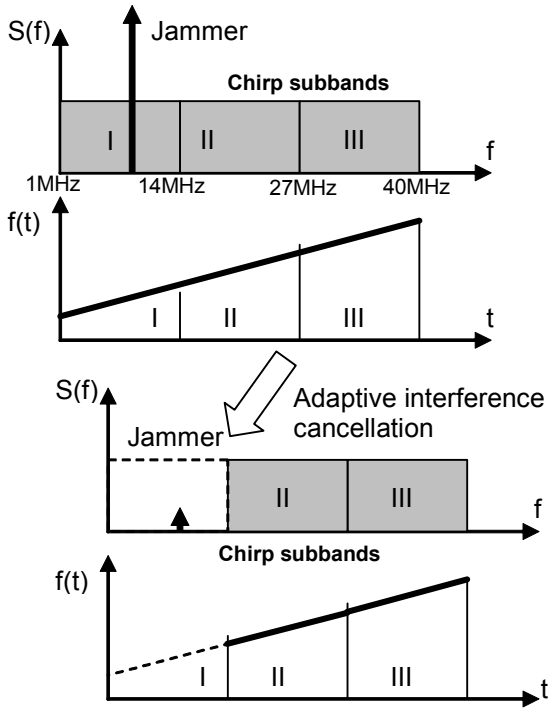


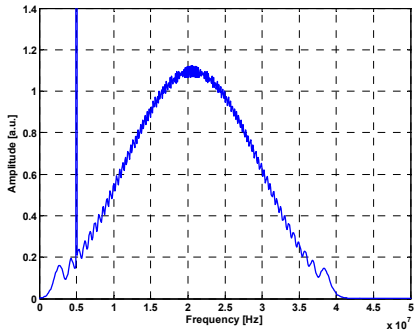
Figure 2. Principle of adaptive interference cancellation by modification of the chirp MF.

The chirp MFs are implemented by digital finite impulse response (FIR) filters. By changing the filter coefficients of the chirp MF the transfer characteristics in the corresponding frequency band can be modified (turned off). In Figure 2 an example is given where the chirp MF impulse response is divided into three subbands. The narrow band jammer is located in subband *I* and can be substantially suppressed by turning subband *I* off. By modification of the chirp MF for adaptive interference suppression (the MF bandwidth is reduced by 1/3), the MF compression gain is reduced in the given example by 3.4 dB.

System simulations where the SIR on the transmission channel is adjusted to 0 dB, which means that the power of

the jammer is equal to the power of the transmitted chirp signal, are shown in Figure 3. The frequency of the jammer is set to 5 MHz and therefore interferes with the chirp subband *I*. By gating off the corrupted frequency band, the jammer can be substantially suppressed as shown in Figure 3.

a)



b)

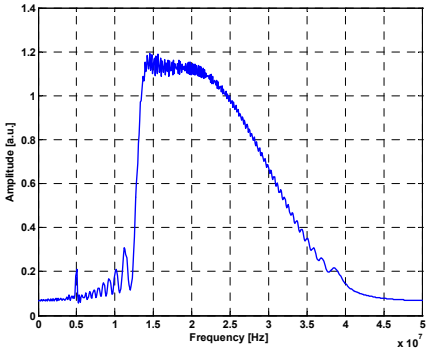


Figure 3. Suppression of a narrow band jammer at 5 MHz by adaptive interference cancellation (SIR = 0 dB).

III. FULLY DIGITAL IMPLEMENTATION OF A CHIRP SPREAD SPECTRUM SYSTEM WITH ADAPTIVE INTERFERENCE CANCELLATION

The chirp BOK system was implemented on an Altera DSP development kit (DSP-DEVKIT-2S60, Altera Corporation, USA) based on an Altera Stratix II FPGA. The complete hardware design is shown in Figure 4. The chirp generation is done by a numerically controlled oscillator (NCO). After subsequent digital to analog conversion and low pass filtering (f_g = 50 MHz) the chirp signals are fed into a 50 ohm coaxial transmission line. The generated chirp signals have a start frequency of 1 MHz, a stop frequency of 40 MHz (B_c = 39 MHz), and a time duration of 2 µs. To compensate the power loss of the combiner circuit, a monolithic RF amplifier (ERA-4, Mini Circuits, USA) is used in the transmission link.

A sinusoidal jammer is generated by a function generator (33250A, Agilent, USA) and is fed into the transmission channel by a power combiner (ZFRSC-42-S+, Mini Circuits, USA). The chirp receiver consists of an analog to digital conversion section with a sampling rate of 100 MSamples/s and two chirp MFs with adaptive switchable filter coefficients for interference suppression. Envelope detection is done by a square law demodulator and an FIR low pass filter.

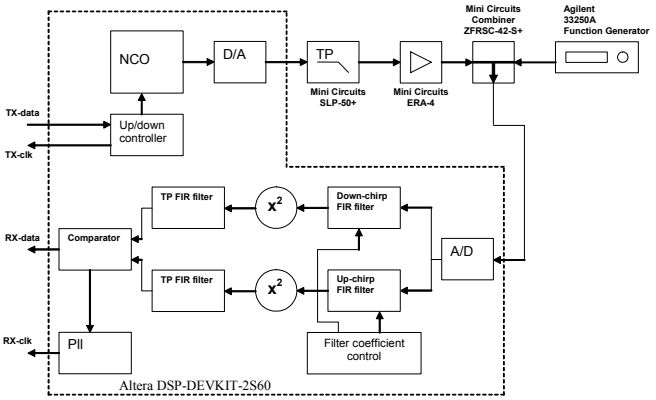


Figure 4. Principle of the chirp BOK data transmission system.

A comparator circuit compares the amplitudes of the demodulated MF output signals and reconstructs the transmitted data stream. For data clock reconstruction a Pll circuit triggered by the reconstructed data symbols is used. Figure 5 shows the measured matched filter output signals after demodulation and filtering. Figure 5 depicts the MF autocorrelation function (compressed chirp signal) without (Figure 5a) and with (Figure 5b) adaptive interference cancellation. The pictures show three compressed chirp signals (MF autocorrelation function) followed by two cross-correlation output signals in equidistant symbol time intervals of 2 µs.

a) **b)**

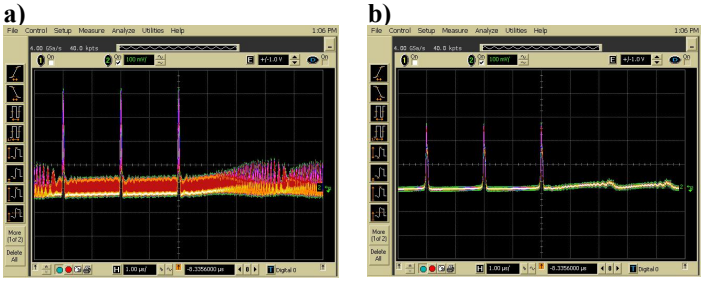


Figure 5. Matched filter output signals after demodulation: **a)** without chirp gating, **b)** with adaptive interference cancellation (f_{jammer} = 5 MHz, SIR = –6dB).

The performance of the chirp data transmission system is evaluated by its bit error rate (BER) in different jamming situations (Figure 6). BER measurement was done by a self-designed BER tester based on the IC DS2172 (Dallas Semiconductor, USA). In general, the chirp BOK data transmission system yields a high jamming robustness. A remarkable BER was firstly measured for an SIR on the transmission channel below –2 dB. For lower SIR values, a

 ISBN: 978-1-61208-166-3

steep increase in the BER to 10e-2 was found, mainly based on wrong decisions at the comparator circuit resulting in lost data bits and high jitter at the clock recovery circuit. Using adaptive interference cancellation by switching off corrupted chirp subbands, the system performance can be increased in SIR robustness by at least 4 dB (Figure 6).

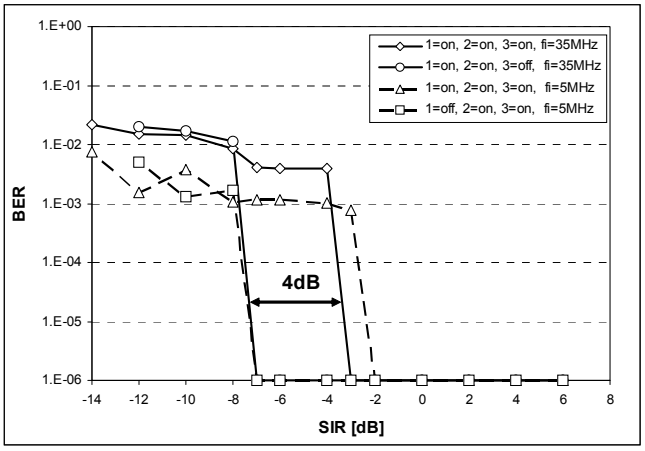


Figure 6. Measured bit error rate in dependency on the SIR at the transmission channel with and without adaptive interference cancellation.

IV. CONCLUSIONS

A chirp spread spectrum BOK data transmission system with adaptive interference cancellation was built. The whole design was fully implemented onto an Altera FPGA board. For selective jammer suppression, an adaptive interference cancellation principle based on gated chirps was shown. By switching off jammed chirp subbands the robustness against narrow band interference can be increased by at least 4dB.

ACKNOWLEDGMENTS

The authors would like to thank the government of Lower Austria and the European Regional Development Fund (EFRE) for their financial support of the project (Project ID: WST3-T-91/004-2006).

REFERENCES

[1] G. Prorakis, Digital Communications, 3rd ed. McGraw-Hill, 1995.

[2] G.R. Cooper, C.D. McGillem, Modern Communications and Spread Spectrum, McGraw-Hill, 1986.

[3] I. Paez, S. Loredo, L. Valle, R.P. Torres, “Measuring broadband radio channel parameters using a simple experimental set-up”, The 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, vol. 1, pp. 473 – 477, 2002.

[4] C.E. Cook., M. Bernfeld, Radar Signals, Artech House, 1993.

[5] M. Brandl, A. Pohl, F. Seifert, L. Reindl, “Fast adaptive interference cancellation in chirp spread spectrum systems “, IEEE Global Telecommunications Conference, 1999; Proceedings Vol. 4, Pages 2218 -2222

 ISBN: 978-1-61208-166-3

The Relationship Analysis of RFID Adoption and Organizational Performance

Yong-Jae Park
Technology Strategy Research Division
Electronics and Telecommunications Research Institute
Daejeon, Korea
pyjeje@etri.re.kr

Myung-Hwan Rim
Technology Strategy Research Division
Electronics and Telecommunications Research Institute
Daejeon, Korea
mhrim@etri.re.kr

Abstract—**The goal of this study is to determine factors influencing the adoption of RFID and its effects on organizational performance. In the research model used in this study, factors influencing the adoption of RFID were examined under a TOE (Technology, Organization, Environment) framework, with a series of hypotheses set up accordingly, and organizational performance was measured using a BSC (Balanced Scorecard). The data were collected from organizations currently using RFID, and the research model and hypotheses were tested through structural equation modeling. The analysis showed that technology competence, technology compatibility, top management support, RFID related cost, competitive pressure, and government support had an influence on the adoption of RFID, and the adoption of it impacted on organizational performance. And policy implications were derived from the results and strategies for stimulating demand for RFID.**

Keywords-RFID; RFID adoption; Balanced scorecard; Organizational performance; Structural equation modeling.

I. INTRODUCTION

Counted among the top 10 technologies of the 21st century [1], RFID is a highly promising technology used in a wide-ranging area, from distribution and logistics to manufacturing, transportation and defense. RFID is a non-contact sensor technology using RF signals. A RFID system is composed of a tag with an integrated chip and antenna and a reader for the processing and transmission of stored data [2]. The global RFID market, estimated at US$ 5.6 billion in 2010, is expected to grow to US$ 24.1 billion in 2021. By region, the RFID market is predicted to reach the largest size in East Asia, in part on the back of a lively growth in the Chinese market [3].

RFID is one of the technology policy focuses in major countries around the world where it is perceived as a next-generation engine for future economic growth, and related R&D is actively underway. In the US, R&D activities in RFID are led by the NITRD (Networking and Information Technology R&D) program. The diffusion of RFID is steadily widening, thanks, in part, to the rule making its use mandatory in key government agencies, including the Department of Defense, FDA and the Department of Homeland Security. In Europe, the use of RFID is actively encouraged as part of the effort to build an intelligent society. RFID is currently piloted in various fields, in Europe, including distribution and logistics, and manufacturing. In Japan, its Ministry of Economy, Trade and Industry started a RFID project, called the "5-yen Tag" project, in 2006. The Japanese Ministry of Internal Affairs and Communications, meanwhile, is carrying out projects to build infrastructure necessary for the broad use of RFID tags. In China, RFID has been selected as one of the key technology tasks for the 11th 5-year plan by its government, and the government is providing extensive support for fostering this industry. Efforts are also underway in China, to establish RFID-related standards [4]. In Korea, RFID has been included in 'new IT,' one of the six fields selected as the next-generation engines for economic growth (which otherwise include energy/environmental technology, IT-based new converged industries, bio-industry, transportation systems and knowledge services) [4].

RFID is increasingly receiving attention from the research community as well, in recent years, with research being actively conducted especially on adoption behavior. However, most studies remain attempts to identifying factors influencing the adoption of RFID by certain organizations, and not its massive take-up or the industry-wide level of adoption. Creating a large enough demand is, needless to say, a vital requirement for the viable growth of the RFID industry. Meanwhile, it is also important to understand, for the long-term prospect of the RFID industry, whether and to what extent the adoption of RFID directly influences organizational performance. This study distinguishes itself from previous research on the adoption of RFID in that it is an empirical attempt to comprehensively investigate whether its adoption has a direct impact on organizational performance. The goal of this study is, therefore, to determine factors influencing the adoption of RFID by organizations and how its adoption influences organizational performance so as to develop strategies for stimulating demand for this technology.

This paper is organized as follows. First, in introduction, background, necessity, and objectives were described. Secondly, in literature review, the factors influencing the adoption of RFID were examined through existing literatures by means of a TOE framework. In addition, BSC methodology was considered to measure organizational performance. Thirdly, on the basis of existing literatures, research model and hypotheses were set up. Fourthly,

 ISBN: 978-1-61208-166-3

research model and hypotheses were tested with structural equation modeling. Finally, implications were derived from the analysis, and significance and research direction in the future were presented.

II. LITERATURE REVIEW

A. TOE Framework

In this study, we explore factors influencing the adoption of RFID using the well-known TOE (Technology, Organization, Environment) framework. The TOE framework has been widely used to determine factors influencing the adoption of a new technology or system from a technological, organization and environmental perspective. Noteworthy studies conducted using the TOE framework include Kuan & Chau [5], investigating influence factors for the adoption of electronic data interchange (EDI), and Xu et al. [6] and Zhu et al. [7]-[9], determining factors influencing the adoption of e-business. Joo & Kim [10] used the TOE framework to discover influence factors for the adoption of e-marketplace, and Soares-Aguiar & Palma-dos-Reis [11], to discover determinants of the adoption of e-procurement systems. Finally Wang et al. [12] explored determinants of the adoption of RFID, utilizing the TOE framework.

B. Balanced Scorecard(BSC)

The Balanced Scorecard (BSC), proposed by Kaplan & Norton [13]-[15], is a technique for measuring organizational performance. Under this technique, the performance of an organization is not just measured through financial indicators, but is comprehensively evaluated by looking also at non-financial aspects; hence, a balanced measurement method. Aside from general organizational performance, The BSC is also frequently utilized to measure the effects of the introduction of a new system or information technology on organizational performance. The BSC considers four perspectives, namely, financial, internal business process, learning and growth, and customer that are derived from an organization's vision and strategy.

Examples of studies using the BSC for measuring organizational performance are numerous and are from widely-varying research fields. Papalexandris et al. [16], for instance, measured performance among Greek software companies, using the four perspectives from the original BSC proposed by Kaplan & Norton, unmodified. As for Michalska [17], he used the BSC in this measurement of corporate performance in the Polish metallurgic industry, but replaced the learning and growth perspective, one of the original four perspectives, with the development perspective, and derived appropriate performance indicators for the readapted perspectives. Gumbus & Lyons [18] measured the performance of Philips, employing a BSC comprising the financial, process, customer and the capacity perspective.

Olson and Slater [19], in their measurement of performance among service and manufacturing companies, used a BSC framework consisting in the customer, internal business process, innovation and growth, and the financial perspective. Chand et al. [20], meanwhile, analyzed the effects of the introduction of an ERP system on organizational performance, employing a BSC framework consisting of a process, customer, financial, and a learning and innovation perspective. Bhagwat & Sharma [21] investigated the impact of supply chain management on organizational performance, using a BSC framework comprising a financial, customer, internal business and an innovation and learning perspective. As for Fang & Lin [22], they used a financial, customer, internal, and an innovation and learning perspective to analyze how the introduction of an ERP system affected organizational performance.

III. RESEARCH MODEL AND HYPOTHESES

The research model for determining factors influencing the adoption of RFID under the TOE framework and measuring the effects of the adoption of RFID on organizational performance was designed, as shown in (Figure 1). In this study, we assumed that technology factors such as technology competence, technology compatibility and technology complexity; organizational factors such as support from company leadership, the size of organization and the cost of implementing a RFID system; and environmental factors such as competitive pressure and government support influence the adoption of RFID. We, further, assumed that the adoption of RFID will have an influence on organizational performance.

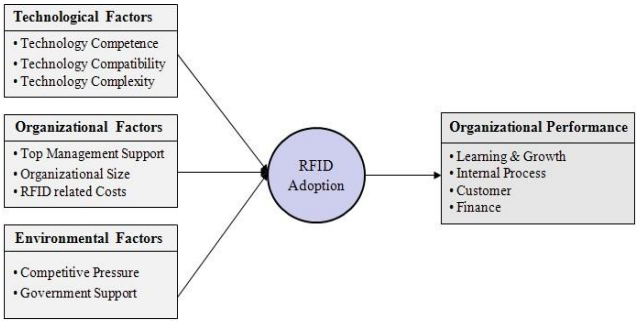


Figure 1. Research model

Concerning technology factors influencing the adoption of a new technology by organizations, quite an important number of previous studies suggested that technological competence, technological compatibility and technological complexity were among the key factors. Kuan & Chau [5] empirically confirmed the impact of technological competence on the adoption of EDI (Electronic Data Interchange), and Xu et al. [6] and Zhu et al. [7] reported that technological competence was a critical influence factor for the adoption of e-business. Kim & Garrison [23] found that technological knowledge was positively associated with the adoption of RFID for supply chain management. Ramamutrthy et al. [24], meanwhile, reported that the adoption of EDI was positively influenced by technological compatibility. Chang et al. [25] and Tsai et al. [26] confirmed through empirical data that technological

 ISBN: 978-1-61208-166-3

complexity was a major influence factor which inhibited the adoption of RFID. Brown & Russell [27] and Wang et al. [12] found that both technological compatibility and complexity importantly influenced the adoption of RFID. Drawing on findings from these previous studies, we set up the following three hypotheses on the relationship between technology factors and the adoption of RFID:

H1. The technology competence has a positive effect on RFID adoption
H2. The technology compatibility has a positive effect on RFID adoption
H3. The technology complexity has a negative effect on RFID adoption

Several studies have reported that organizational factors such as support from company leadership, the size of organization and the cost of implementation were critical factors influencing the adoption of a new technology. Huang et al. [28], in an empirical study on internet-based EDI, found that the adoption of EDI was positively associated with support from company leadership. Joo & Kim [29] stated that the size of an organization was a major influence factor on the adoption of e-marketplace, while AL-Qirim [30] found a positive association between the size of an organization and the adoption of e-commerce. Wang et al. [12] reported, in their empirical study, that the size of an organization had a positive influence on the adoption of RFID. Wymer & Regan [31] suggested that costs played an important role in the adoption of e-commerce. This view was corroborated by Kim & Garrison [23] who also found that financial resources had a measurable influence on the adoption of e-commerce. Brown & Russell [27] reported that the attitude of the management and the size of an organization had a positive impact on the adoption of RFID, and the cost of implementation, a negative impact. Drawing on the existing literature, discussed above, we formulated the following two hypotheses on the relationship between organizational factors and the adoption of RFID:

H4. The top management support has a positive effect on RFID adoption
H5. The organizational size has a positive effect on RFID adoption
H6. The RFID related costs have a negative effect on RFID adoption

A large number of previous studies showed that environmental factors such as competitive pressure and government support had an influence on the adoption of a new technology. Huang et al. [28] suggested that competitive pressure had a positive impact on the adoption of EDI, and Zhu et al. [7] found that it was positively associated with the adoption of e-business. Wang et al. [12] and Brown & Russell [27] stated that competitive pressure was a critical influence factor for the adoption of RFID. Xu et al. [6], meanwhile, advanced that government support in the form of incentive or legal and regulatory support positively influenced companies' adoption of e-business. According to Chang et al. [32], government support would also have an important influence on the adoption of electronic sign-off. In this study, we, therefore, set up the following two hypotheses on the relationship between government support and the adoption of RFID:

H7. The competitive pressure has a positive effect on RFID adoption
H8. The government support has a positive effect on RFID adoption

That organizational performance is positively affected by the adoption of new technologies is a well-known fact. Fang [33] and Fang et al. [34] empirically established that corporate performance is influenced by the adoption of e-business. Chang & Wong [35], meanwhile, showed how the adoption of e-procurement and e-marketplace had an impact on corporate performance. In this study, the influence of the adoption of RFID on organizational performance is measured using a BSC framework, as has been said earlier. Improvements in organization performance under the effect of the adoption of RFID will be, therefore, measured from four perspectives, including learning and growth, internal process, customer and financial. We, therefore, set up the following four hypotheses on the relationship between the adoption of RFID and each of the four BSC perspectives:

H9. The RFID adoption has a positive effect on performance of learning and growth
H10. RFID adoption has a positive effect on performance of internal process
H11. The RFID adoption has a positive effect on performance of customer
H12. The RFID adoption has a positive effect on performance of finance

IV. METHODOLOGY

C. Factors and Data Collection

To identify factors influencing the adoption of RFID and understand whether and to what extend the use of RFID affects organizational performance, we developed a series of measurement items, drawing on the existing literature, as shown in Table 1. All items were measured using a 7-point likert scale.

The data were collected through direct interview of companies currently using RFID by contacting them by phone or through email. Of 130 total responses returned, 103 were retained for analysis, after discarding random or otherwise invalid responses. The demographics of the sample were as follows (see Table 2). An overwhelming majority of 82.5% of respondents were men, and people in their 30s represented 50.5%.

 ISBN: 978-1-61208-166-3

TABLE 1. FACTORS AND MEASUREMENT ITEMS

Factor		Measurement Item	
Technological Factors	Technology Competence (A)	A1	Amount of IT infrastructure related to the deployment of RFID
		A2	Familiarity with RFID technology
		A3	Level of employees' knowledge about RFID
	Technology Compatibility (B)	B1	Compatibility between RFID and existing equipment and facilities
		B2	Compatibility of RFID with routine tasks performed in the company
		B3	Appropriateness of RFID to organizational goals, values, beliefs or strategies
	Technology Complexity (C)	C1	RFID is perceived as complicated to use in our organization.
		C2	Developing RFID is considered a complicated process in our organization.
		C3	Implementing and using a RFID is considered a process requiring a great deal of efforts in our organization.
Organizational Factors	Support from Management (D)	D1	The degree to which the management considers RFID important and supports its use.
		D2	The degree to which the management considers the deployment of RFID as an important issue.
		D3	The extent to which the management will be willing to communicate with staff and participate in the process.
	Size of Organization (E)	E1	Our company's capital is larger than most companies' in the same business sector.
		E2	Our company's profit is higher than most companies' in the same business sector.
		E3	The number of employees in our company is larger than that in most companies in the same business sector.
	RFID-related Costs (F)	F1	The cost of implementing the RFID system is high.
		F2	The cost of providing education and training on RFID is high.
		F3	The cost of using and servicing the RFID system is high.
Environmental Factors	Competitive Pressure (G)	G1	Commensurate with the number of competitors having a RFID system
		G2	Commensurate with the number of companies in the same sector having a RFID system
		G3	Commensurate with the number of companies in the same sector, successfully using a RFID system
	Government Support (H)	H1	Whether the government provides incentives for the introduction of RFID
		H2	The extent to which the government supplies information related to the implementation of RFID
		H3	The extent to which the government makes efforts toward the improvement of laws related to RFID
Adoption of RFID(I)		I1	The extent to which the implementation of RFID
Organizational Performance	Learning & Growth (J)	J1	Enhancement of employees' work satisfaction attributable to RFID
		J2	Increase in the stock of knowledge about RFID
		J3	Improvement in employees' RFID–related skills and proficiency
	Internal Process (K)	K1	Increase in the rate of timely delivery of products and services attributable to RFID
		K2	Increase in the efficiency of inventory management attributable to RFID
		K3	Shortening of work processes and task handling time attributable to RFID
	Customer (L)	L1	Enhancement in customer satisfaction attributable to RFID
		L2	Enhancement of the company image attributable to RFID
		L3	Enhancement in customer loyalty attributable to RFID
	Finance (M)	M1	Cost reduction attributable to RFID
		M2	Sales increase attributable to RFID
		M3	Increase in return on investment attributable to RFID

In terms of education level, college graduates accounted for the largest share of 65.0%. In terms of number of years in service, less than 10 years represented 50.5% of total respondents. Meanwhile, in terms of organizational characteristics, as shown in Table 3, most were manufacturing and ICT companies, representing respectively 30.1% and 20.4% of total respondents. In terms of number of employees, 1,000 or more accounted for the largest share of 41.8%. As for three-year average sales, the greatest number of companies declined to answer this question, but among those providing an answer, 100 billion won to 500 billion won represented the largest share of 23.3%.

D. Structural Equation Modeling

In this study, the research model is tested against the data using structural equation modeling. Structural equation modeling is a technique widely used for evaluating causal relationships between constructs. For the purpose of this study, we used PLS (Partial Least Squares) based structural equation modeling, which helps minimize endogenous variable errors and provides a greater level of explanatory power.

The reliability of constructs, when using PLS analytical tools, is determined by the value of internal consistency (IC) between the constructs. As a general rule, a value of 0.7 or greater indicates the existence of reliability [36][37]:

The validity of constructs is judged based on the value of their AVE (Average Variance Extracted. When the AVE is 0.5 or greater, this is considered an indication of the existence of convergent validity. Meanwhile, when the square root of the AVE is larger than the correlation coefficient between each of the factors, this is considered to indicate the existence of discriminatory validity [36][38].

 ISBN: 978-1-61208-166-3

TABLE 2. DEMOGRAPHIC PROFILE

Demographic Profile		Frequency	%
Gender	Male	85	82.5
	Female	18	17.5
Age(years)	20-29	11	10.7
	30-39	52	50.5
	40-49	33	32.0
	Over 50	7	6.8
Education level	College graduates	67	65.0
	Master/Doctor	36	35.0
Years in current position	Less than 5 years	24	23.3
	5 to 9 years	28	27.2
	10 to 14 years	23	22.3
	15 to 19 years	15	14.6
	20 years or more	13	12.6
Total		103	100.0

TABLE 3. ORGANIZATIONAL CHARACTERISTICS

Organizational Characteristics		Frequency	%
Industry Sector	Manufacturing	31	30.1
	Information & communications	21	20.4
	Financial and insurance	10	9.7
	Distribution/ logistics	11	10.7
	Service	13	12.6
	Construction	11	10.7
	Other	6	5.8
Number of employees	Less than 100	18	17.5
	100 to 499	26	25.2
	500 to 999	16	15.5
	1,000 or more	43	41.8
Sales (3 year average)	Less than KRW 10 billion	14	13.6
	10 billion to - KRW 100 billion	9	8.7
	100 billion - KRW 500 billion	24	23.3
	KRW 500 billion or more	18	17.5
	No answer	38	36.9
Total		103	100.0

V. RESULTS

The reliability analysis performed on the factors used in this study revealed that the IC value was greater than the threshold of 0.7 for all factors, suggesting a good level of reliability. The AVE also proved to exceed the threshold value of 0.5 for all factors, attesting to their convergent validity. All factors were tested satisfactorily for discriminant validity as well.

When the research model was tested using the structural equation modeling technique, all hypotheses, except H3, H5 and H12, were accepted (see Figure 2). Among the technology factors, technology competence and technology compatibility proved to have a strong influence on the adoption of RFID. Technology complexity, on the other hand, showed no significant influence on the adoption of RFID. What these results point to is the importance of organizational capacities such as knowledge about RFID and infrastructure necessary for the deployment of RFID for an organization's adoption of RFID. The results also confirm that whether RFID is compatible with an organization's strategy or the situation it is currently facing and whether it is compatible with tasks routinely carried out in an organization are important determinants of its adoption.

Among organizational factors, analysis revealed that the adoption of RFID was measurably influenced by support from company leadership and the cost of implanting and using RFID. The results indicated, meanwhile, that the size of an organization had no real influence on the adoption of RFID. These results, therefore, attest to the importance of interest and awareness at the level of leadership within a company for its adoption of RFID. Also, the higher the cost of implementing RFID, the lower the probability of an organization's adoption of RFID proved to be. Hence, to broaden the adoption of RFID, it is necessary to find ways of reducing the cost of introducing RFID.

Among environmental factors, the results confirmed that the adoption of RFID was affected by competitive pressure and government support. What this says is that the higher the level of adoption of RFID among competitors in the same business sector, the more willing a company is to adopt RFID in its turn. Equally important is government support, in the form of a tax break or legal and regulatory improvement to incline a company toward the adoption of RFID.

The results of analyzing causal relationships between the adoption of RFID and organizational performance showed that learning and growth, internal process and customer performance were strongly affected by the adoption of RFID. Meanwhile, the adoption of RFID did not appear to influence the financial performance of a company. The results, therefore, point to important contributions by RFID to corporate performance, in terms of learning and growth, internal process and customer performance. But, the use of RFID is yet to produce an impact on the financial performance of companies. The detailed results of hypothesis testing are given in Table 4.

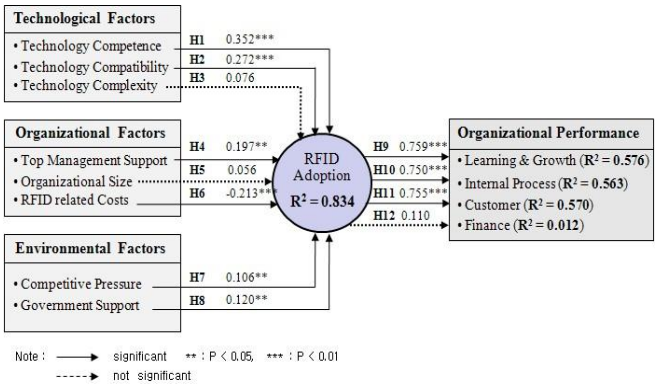


Figure 2. Results of Structural Equation Model Testing

TABLE 4. RESULTS OF RESEARCH HYPOTHESIS (H1-H12) TESTING

Path	Hypothesis	Estimate	S.E.	t value.	Results
Technology competence→ RFID adoption	H1	0.352***	0.095	3.8062	Accept
Technology compatibility→ RFID adoption	H2	0.272***	0.0982	2.7695	Accept
Technology complexity→ RFID adoption	H3	0.076	0.0486	1.5627	Reject
Top management support→ RFID adoption	H4	0.197**	0.0843	2.3370	Accept
Organizational size→ RFID adoption	H5	0.056	0.0437	1.2823	Reject
RFID related costs→ RFID adoption	H6	-0.213***	0.0598	3.5634	Accept
Competitive pressure→ RFID adoption	H7	0.106**	0.0532	1.9925	Accept
Government support→ RFID adoption	H8	0.120**	0.0486	2.4700	Accept
RFID adoption→ Learning and growth	H9	0.759***	0.0518	14.6640	Accept
RFID adoption→ Internal process	H10	0.750***	0.0547	13.7082	Accept
RFID adoption→ Customer	H11	0.755***	0.0574	13.1616	Accept
RFID adoption→ Finance	H12	0.110	0.1096	1.0040	Reject

VI. CONCLUSION AND IMPLICATIONS

This study has been an empirical attempt to understand technology, organizational and environmental factors influencing the adoption of RFID and measure its effects on organizational performance of companies. From the results obtained in this study, we derived the following policy and practical implications for stimulating demand for RFID and accelerating its diffusion:

First, there is a need for policy-level support for the technology factors that were found to influence the adoption of RFID. For example, education and training programs to help companies improve their understanding of, and proficiency with, RFID could be very useful. Also useful would be an onsite technical consulting program to assist companies in determining whether RFID is compatible with their existing systems and tasks they carry out routinely.

Second, this study found that support from company leadership positively influences the adoption of RFID. Therefore, programs to kindle interest in RFID among corporate executives could effectively help promote its adoption. Programs for sharing cases of successful implementation and use of RFID and concrete examples of benefits resulting from the use of RFID with CEOs would be particularly useful for raising interest in this technology and encouraging companies to adopt it.

Third, as emerged from this study, the high cost of setting up a RFID system is a factor making companies hesitant about its adoption. Hence, financial support from the government to assist with initial costs associated with setting up a RFID system could help toward an early adoption of this technology by companies. SMEs in strong need of RFID, but hesitant about actually introducing it due to financial burden could particularly benefit from such support.

Fourth, our study found that external environmental factors such as competitive pressure from within their own business sector and government support played a critical role in their decision to adopt RFID. It may, therefore, be useful to publicize sector-specific cases of successful implementation and use of RFID and details of benefits gained from RFID to kindle interest in this technology. Tax breaks and other forms of incentive for companies introducing RFID will be also effective means for encouraging its adoption, along with legislative and regulatory improvement to facilitate the process.

Fifth, concerning the effects of the adoption of RFID on organizational performance, its influence proved particularly strong on learning and growth, internal process and customer performance. These are positive findings about the beneficial effects of RFID on organizational performance. However, we found no concrete effect of RFID on financial performance. This, therefore, points to a need for further efforts to improve the performance-effects of this technology so that its use can also enhance the financial performance of companies.

This study is significant in that it proposes strategies for promoting and accelerating the adoption of RFID by companies, based on the analysis of influence factors for its adoption and the effects of its use on organizational performance. Future research can improve on this study by developing an objective model for directly evaluating the performance-enhancing effects of RFID and by presenting strategies for promoting its adoption based on concrete performance data. This study found that the use of RFID is yet to produce a measurable effect on the financial performance of companies. Future research, therefore, also needs to investigate factors that can directly influence financial performance.

REFERENCES

[1] C. C. Chao, J. M Yang, and W. Y. Jen, "Determining Technology Trends and Forecast of RFID by a Historical Review and Bibliometric Analysis from 1991 to 2005," Technovation, vol. 27, no. 5, 2007, pp. 268-279.

[2] N. C. Wu, M. A. Nyystrom, T. R. Lin, and H. C. Yu, "Challenges to Global RFID Adoption," *Technovation*, vol. 26, 2006, pp. 1317-1323.

 ISBN: 978-1-61208-166-3

[3] R. Das and D. P. Harrop, RFID Forecasts, Players and Opportunities 2011-2021, IDTechEX, 2010.

[4] M. S. Kang, "2010 R&D Promotion Direction and Technology Road-map of RFID/USN ," *ICT Forum KOREA 2010*, 2010, pp.77-81.

[5] K. K. Y. Kuan and P. Y. K. Chau, "A Perception-based Model for EDI Adoption in Small Businesses using a Technology-Organization-Environment Framework," *Information & Management*, vol. 38, no. 8, 2001, pp. 507-521.

[6] S. Xu, K. Zhu, and J. Gibbs, "Global Technology, Local Adoption: A Cross-Country Investigation of Internet Adoption by Companies in the United States and China," *Electronic Markets*, vol. 14, no. 1, 2004, pp. 13-24.

[7] K. Zhu, K. Kraemer, and Xu, S. "Electronic Business Adoption by European Firms: A Cross-Country Assessment of the Facilitators and Inhibitors," *European Journal of Information Systems*, vol. 12, No. 4, 2003, pp. 251-268.

[8] K. Zhu, K. L. Kraemer, and S. Xu, "The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on E-Business," *Management Science*, vol. 52, no. 10, 2006, pp. 1557-1576.

[9] K. Zhu, S. Dong, S. X. Xu, and K. L. Kraemer, "Innovation diffusion in Global Contexts: Determinants of Post-Adoption Digital Transformation of European companies," *European Journal of Information Systems*, vol. 15, no. 6, 2006, pp. 601-616.

[10] Y. B. Joo and Y. G. Kim, "Determinants of Corporate Adoption of e-Marketplace: An Innovation Theory Perspective," *Journal of Purchasing & Supply Management*, Vol. 10, no. 2, 2004, pp. 89-101.

[11] A. Soares-Aguiar and A. Palma-dos-Reis, "Why Do firms Adopt E-Procurement System? Using Logistic Regression to Empirically Test a Conceptual Model," *IEEE Transactions on Engineering Management*, vol. 55, no. 1, 2008, pp. 120-133.

[12] Y. M. Wang, Y. S. Wang, and Y. F. Yang "Understanding the Determinants of RFID Adoption in the Manufacturing Industry," *Technology Forecasting & Social Change*, vol. 77, 2010, pp. 803-815.

[13] R. S. Kaplan and D. P. Norton, "The Balanced Scorecard-Measures That Drive Performance," *Harvard Business Review*, vol. 70, no.1, 1992, pp.71-79.

[14] R. S. Kaplan and D. P. Norton, "Putting the Balanced Scorecard to Work," *Harvard Business Review*, vol. 71, no.5, 1993, pp.134-142.

[15] R. S. Kaplan and D. P. Norton, "Using the Balanced Scorecard as a Strategic Management System," *Harvard Business Review*, vol.74, no.1, 1996, pp.75-85 [16] A. Papalexandris, G. Loannou, and G. P. Prastacos, "Implementing the Balanced Scorecard in Greece: A Software Firm's Experience," Long Range Planning, vol. 37, 2004, pp. 351-366.

[17] J. Michalska, "The Usage of the Balanced Scorecard for the Estimation of the Enterprise's Effectiveness," *Journal of Materials Processing Technology*, vol.162-163, 2005, pp.751-758.

[18] A. Gumbus and B. Lyons, "The Balanced Scorecard at PHILIPS Electronics," *Strategic Finance*, 2002.

[19] E. M. Olson and S. F. Slater, "The Balanced Scorecard, competitive Strategy, and Peformance," Business Horizons, vol. 45, no. 3, 2002, pp. 11-16.

[20] D. Chand, G. Hachey, J. Hunton, V. Owhoso, and S. Vasudevan, "A Balanced Scorecard- based Framework for Assessing the Strategic Impacts of ERP Systems," Computers in Industry, vol. 56, 2005, pp. 558-572.

[21] R. Bhagwat and M. K. Sharma, "Performance Measurement of Supply Chain Management: A Balanced Scorecard Approach," *Computers & Industrial Engineering*, vol. 53, 2007, pp.43-62.

[22] M. Y. Fang and F. Lin, "Measuring the Performance of ERP System-from the Balanced Scorecard Perspectives," *The Journal of American Academy of Business*, vol. 10, no.1, 2006, pp.256-263.

[23] S. Kim and G. Garrison, "Understanding User's Behaviors Regarding Supply Chain Technology: Determinants Impacting the Adoption and Implementation of RFID Technology in South Korea," *International Journal of Information Management*, vol. 30, no. 5, 2010, pp. 388-398.

[24] K. Ramamurthy, G. Premkumar, and M. R. Crum, "Organizational and Interorganizational Determinants of EDI Diffusion and Organizational Performance: A Causal Model," Journal of Organizational computing and Electronic Commerce, vol. 9, no. 4, 1999, pp. 253-285.

[25] S. I. Chang, S. Y. Hung, D. C. Yen and Y. J. Chen, "The Determinants of RFID Adoption in the Logistics Industry-A Supply Chain Management Perspective," *Communications of the Association for Information systems*, vol. 23, no. 12, 2008, pp. 197-218.

[26] M. C. Tsai, W. Lee, and H. C. Wu, "Determinants of RFID Adoption Intention: Evidence from Taiwanese Retail Chains," *Information & Management*, vol. 47, no. 5-6, 2010, pp. 255-261.

[27] I. Brown and J. Russell "Radio Frequency Identification Technology: An Exploratory Study on Adoption in the South African Retail Sector," *International Journal of Information Management*, vol. 27, no. 4, 2007, pp. 250-265.

[28] Z Huang, B. D. Janz, and M. N. Frolick "A comprehensive Examination of Internet - EDI Adoption," *Information Systems Management*, vol. 25, no. 3, 2008, pp. 273-286.

[29] Y. B. Joo and Y. G. Kim, "Determinants of Corporate Adoption of e-Marketplace: An Innovation Theory Perspective," *Journal of Purchasing & Supply Management*, vol. 10, no. 2, 2004, pp. 89-101.

[30] N. AL-Qirim, "An Empirical Investigation of an E-Commerce Adoption-gapability Model in Small Businesses in New Zealand," *Electronic Markets*, vol. 15, no. 4, 2005, pp. 418-437.

[31] S. Wymer and E. Regan, "Factors Influencing E-Commerce Adoption and Use by Small and Medium Businesses," *Electronic Markets*, vol. 15, no. 4, 2005, pp. 438-453.

[32] I. C. Chang, H. G. Hwang, M. C. Hung, M. H. Lin, and D. C. Yen, "Factors Affecting the Adoption of Electronic Signature: Executives' Perspective of Hospital Information Department," *Decision Support Systems*, vol. 77, 2007, pp. 350-359.

[33] W. Fang, Bringing 'E' to Corporate America: The Drivers of E-Business Adoption and its Impact on Firm Performance, Ph. D. Dissertation, University of Texas at Austin, 2001.

[34] W. Fang, V. Majan, and S. Balasubramanian, "An Analysis of E-Business Adoption and Its Impact on Business Performance," *Journal of the Academy of Marketing Science*, vol. 31, no. 4, 2003, pp. 425-447.

[35] H. H. Chang and K. H. Wong, "Adoption of E-Procurement and Participation of E-Marketplace on Firm Performance: Trust as a Moderator," *Information & Management*, vol. 47, no. 5-6, 2010, pp. 262-270.

[36] Fornell, C.; Larcker, D. F. 1981.Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, *Journal of Marketing Research* 18(1): 39-50.

[37] Chin, W. W. 1998. The Partial Least Squares Approach to Structural Equation Modeling, G. A. Marcoulides(ed.), Modern Methods for Business Research, Lawrence Erlbaum Associates, Mahwah, NJ, 295-336.

[38] Gefen, D.; Straub, D. A. 2005. Practical Guide to Factorial Validity Using PLS -GRAPH: Tutorial and Annotated Example, Communications of the Association for Information Systems, 1: 91-109.

 ISBN: 978-1-61208-166-3

Providing QoS to Secondary Users Employing VoIP Applications in Cognitive Radio Networks

Esra Hatice Demirtaş
Computer Engineering Department
Istanbul Technical University
Istanbul, Turkey
demirtas@itu.edu.tr

Sema F. Oktuğ
Computer Engineering Department
Istanbul Technical University
Istanbul, Turkey
oktug@itu.edu.tr

***Abstract*— Quality of Service in Cognitive Radio is an open area for researches. Previous works on this item are classified as either *Quality of Service of Primary User* or *Quality of Service of Secondary User*. The work described in this paper is related to the latter. We worked on a popular application which is Voice over IP. The aim is to provide a sufficient Quality of Service to Secondary Users employing Voice over IP. For that purpose; calls over a real Application Server with different codecs, and different voice packet size were established; voice packets were collected through a network protocol analyzer, which is *wireshark*; packets were analyzed; and an application layer algorithm has been proposed. Then, a Secondary User with a Voice over IP connection employing the proposed algorithm was simulated considering various arrival patterns of Primary User using the network simulator, *ns-2*. The results obtained confirmed the success of the proposed technique. It is shown that, the cognitive radio applications employing the introduced technique achieve an acceptable Quality of Service level for Voice over IP connections. To the best of our knowledge, this is the first work providing Quality of Service to Secondary Users of Cognitive Radio Networks at application layer.**

Keywords-component; Cognitive Radio; QoS; VoIP

I. INTRODUCTION

There is an increasing spectrum demand because of the uptrend in new bandwidth required technologies. However, users could not be always served since the lack of empty spectrum resource in their location. In the meantime, some portions of the spectrum may be underutilized [1]. Since spectrum is assigned statically in current wireless networks, users can not move to another spectrum although there is an available resource on there. Cognitive Radio Networks (CRN) use dynamic spectrum access. Secondary Users (SUs) sense the spectrum, and they are allowed to use a licensed spectrum if they do not affect the Primary Users (PUs) [2-3].

Works related to Quality of Service (QoS) in CRN are very important for the success of CRN. There are two different QoS research area in CRN:

- QoS of Primary User (PU): Aims to show that in CRN, SUs do not affect the QoS of PU.
- QoS of Secondary User (SU): Providing QoS to SUs in CRN.

The main objective of this study is to provide QoS to SUs of CRN. For this purpose, a widely used application, Voice over IP (VoIP), is chosen. Then, a QoS satisfying VoIP application is aimed in order to provide voice communication to SU in CRN. In this work, an application layer solution is proposed.

The rest of the paper is organized as follows: In Section II, the related works are summarized. VoIP Basics are described in Section III. The technique proposed is presented in Section IV. The simulation environment and the simulation results are given in Section V, followed by conclusion and future works in Section VI.

II. RELATED WORK

Recent researches in QoS of SUs in CRN have been focused on power controls, resource management algorithms and Media Access Control (MAC) designs.

In [4] authors identified every user as selfish and each one tries to achieve its target QoS using least power consumption. They had optimized the problem as non-cooperative game, and analyzed Nash Equilibrium (N.E.). In system model, each user announces its interference regulation price and QoS provisioning price. Then, all of users run the proposed multi-channel power allocation algorithm [4].

In [5], authors worked on resource management algorithms. They proposed a hybrid model named C2net which consists of Integrated Services (IntServ) for high priority flows such as voice, video, and Differentiated Services (DiffServ) for other flows. In [6], a scheduling algorithm is proposed for statistical QoS guarantee over CRN. Cooperative relay node and admission control mechanisms are proposed. In [7], authors investigate a CRN which consists of cluster heads (CHs), and regular sensors. Constant Bit Rate (CBR) and Best Effort (BE) traffic is considered and two different priority algorithms are proposed to provide QoS. In [8], authors analyzed the VoIP capacity and proposed a new method for finding the minimum detection and false-alarm probabilities to ensure the QoS requirement of VoIP users in CRN. They modeled the VoIP traffic as Markov-Modulated Poisson Process (MMPP); channel as two state Markov chain.

 ISBN: 978-1-61208-166-3

In [9] two MAC schemes are proposed for SU accessing the wireless channel. Then, an analytical model is proposed to derive the voice-service capacity for two MAC schemes.

III. VOIP BASICS

VoIP is the growing technology that allows voice conversations to be carried over the Internet Network [10]. VoIP uses Session Initiation Protocol (SIP) [11] or H323 protocol [12] for signaling. Voice conversations have a "sender" and "receiver" roles. Sender and receiver change the roles in different portions of conversation.

A. Working Principle of VoIP

Sender creates an analogue signal on the conversation. These analogue signals are digitized by the use of an encoder [13]. At receiver, incoming packets are placed into a playback buffer to overcome problems caused by late received or non-received packets. These packets decoded using identical decoder. The digital bit stream converted back into an analogue signal and send to the receiver.

B. VoIP Session Initialization via SIP

Calling and called party get an agreement on which codec is going to be used, and what will be the packet rate, and packet sizes, in each new call. These are agreed at session initialization. Session initialization is done with either SIP or H323 messages. Here, we investigated SIP. There is a Session Description Protocol (SDP**)** [14] portion in SIP messages. It contains all information that needs to be shared with the other side to negotiate. Supported codecs are given in rtpmap attribute of SIP message. This attribute maps the Real-time Transport Protocol (RTP) payload type number defined in "m=" line to an encoding name, clock rate and encoding parameters. RTP payloads are defined by The Internet Assigned Numbers Authority (IANA) and then standardized by The Internet Engineering Task Force (IETF) [15-16]. Voice packet size is carried in *ptime* attribute.

After session is established, calling or called party can change the negotiated codec or *ptime*. This is done by in-session requests with INVITE or UPDATE messages.

C. VoIP Packet and Codec Relations

A VoIP packet consists of 20 bytes Internet Protocol (IP) header, 8 bytes User Datagram Protocol (UDP) header, 12 bytes RTP header and a variable size payload according to used codec as illustrated in Fig. 1 [17].

Popular codecs in VoIP have been identified and their packet size, packet interval have been calculated using (1), (2), (3).

$$\text{CodecBitRate} = \text{CodecSampleSize} / \text{CodecSampleInterval} \quad (1)$$

$$\text{PacketsPerSecond} = \text{CodecBitRate} / (\text{VoicePayloadSizeInBit}) \quad (2)$$

$$\text{TotalPacketSize} = (\text{Layer2Header}) + (\text{IP/UDP/RTP\_header}) + (\text{VoicePayloadSize}) \quad (3)$$

Calculated codec packet size and interval according to *ptime* value is provided in Table I.

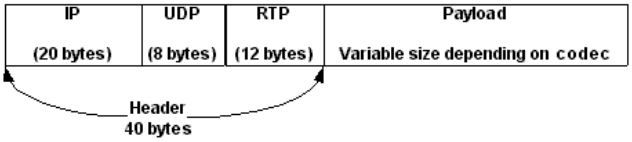


Figure 1. VoIP Packet

D. QoS Evaluation in VoIP

IP Networks were built for non-real time applications such as file transfer, email. That is why delay or available bandwidth was not the big concern. Later, IP Networks are started to be used for real time applications and real time applications are relative to delay [18]. In VoIP, packets are created at real time, encoded, packetized, sent over the network, decoded, and listened by other party. Delay, jitter, available bandwidth, as a result QoS, becomes a major concern in real time applications.

The quality of voice is subjective. Users express the quality of a call as "good", "bad", "quite good", or "very bad". In QoS tests of VoIP, a conversation is listened to users and wanted to quantify the service quality from 1 to 5, 1 being the worst and 5 is the best. The numerical method of expressing voice and video quality is defined as Mean Opinion Score (MOS) [19].

Instead of subjective tests, MOS can be calculated by voice quality effecting factors such as bandwidth, delay, jitter, packet loss, echo or noisy background.

TABLE I. CODEC PROPERTIES

Codec (Defined in rtpmap attribute)	*Voice Payload Size (ms- Defined in ptime attribute)*	*Total packet Size (byte)*
G711	10	126
G711	20	206
G711	30	286
G729	10	56
G729	20	66
G729	30	76
G729	40	86
G729	50	96
G729	60	106
G 723.1	30	70
G 723.1	60	94
G726-32	20	126
G726-32	30	166
G726-32	40	206
G726 -24	20	106
G726 -24	30	136

 ISBN: 978-1-61208-166-3

The ITU-T E-Model [20] defines an analytic model of voice quality between two connections known as "Voice Transmission Quality from Mouth to Ear" with equipment impairment factor method, and previous transmission rating models. E-model calculates the Rating Factor (R). R value is calculated using the formula below:

$$R = R_o - I_s - I_d - I_{e-eff} + A \quad (4)$$

where *Ro* is basic signal-to-noise ratio, including noise sources such as circuit noise and room noise, *Is* is a combination of all impairments which occur more or less simultaneously with the voice signal, *Id* is the impairments caused by delay and the effective equipment impairment factor, $I_{e\text{-}eff}$ is the impairments caused by low bit-rate codecs and impairment due to packet-losses of random distribution, *A* is the advantage factor.

MOS value is calculated through R value as below:

$$MOS = \begin{cases} R <= 6.5: & 1 \\ 6.5 < R <= 100: & 1 - \frac{7}{100}R + \frac{7}{6250}R^2 - \frac{7}{1000000}R^3 \\ R <= 100: & 4.5 \end{cases} \quad (5)$$

See Table II for the relation between, R value and MOS.

IV. PROPOSED SOLUTION

After investigation VoIP working principle, and VoIP signaling details, VoIP packets obtained from one of VoIP service provider, Genband Application Server [21] in IP network of Netaş [22] were collected and analyzed. It was noticed that VoIP packet size was constant and these packets were generated periodically. According to SIP Request for Comments (RFC), experimental data shows that packet sizes are relevant to negotiated codec which is given in *rtpmap* attribute in SIP message at session initialization. Packet receive interval is related to *ptime* attribute in SIP message. So, it is obvious that we can model VoIP traffic as CBR traffic.

As stated in Section II, QoS of VoIP is calculated through MOS value. In our proposal, MOS is calculated periodically. The algorithm remembers the previous MOS value. Then, it is compared with the current MOS value.

- If the difference is 0, it means MOS remains the same
- If difference is less than 0, it means MOS decreases
  - If it is -1, then ptime value should be changed.
  - If the change is greater than 1, then codec value is changed
- If difference is greater than 0, it means MOS increases

When difference is 1, ptime value is increased. In this way, packet rate is decreased. Each packet carries more voice packet. But this supplies SU to wait more time for non-received packets.

If difference is more than 1, then codec value is changed to a lower codec. Total packet size is decreased.

TABLE II. RELATION BETWEEN R VALUE AND MOS [28]

R Value (lower limit)	*MOS_{CQE} (lower limit)*	*User Satisfaction*
90	4.34	Very Satisfied
80	4.03	Satisfied
70	3.60	Some users dissatisfied
60	3.10	Many users dissatisfied
50	2.58	Nearly all users dissatisfied

V. RESULTS OBTAINED

The test bed is created as 500X500-grid area in ns-2 [24] which simulates 500 m X 500 m square area. There is 1 SU in simulation and it is simulated with mobile node functionality of ns-2. PU traffic is thought as aggregated traffic, so there is not a number for PU. Existence of PUs is modeled by moving the Secondary User to a place longer than antenna's range. When PU has gone, SU moved back to original place.

In this paper, Cognitive Radio's Spectrum Sensing is out of scope. It is assumed that Spectrum Sensing is done and available channels and slots are specified.

Simulation has been run for 10s. Primary user traffic is modeled as deterministic. The simulation is run under 3 different PU traffic models as listed below:

- ON Period = OFF Period
- ON Period > OFF Period
- ON Period < OFF Period

In our simulations R value is calculated according to delay, jitter and packet loss as in Table III [23].

TABLE III. R VALUE CALCULATION

```
1  EffectiveLatency = (AverageLatency + Jitter * 2 + 10)
2  # Take the average latency, add jitter, but double the impact
   to latency then add 10 for protocol latencies
3  if (EffectiveLatency < 160)
4     R = 93.2 - (EffectiveLatency / 40)
5  Else
6     R = 93.2 - (EffectiveLatency -120/ 10)
7  Endif
8  # Deduct 2.5 R values per percentage of packet loss
9  R = R - (PacketLoss * 2.5)
```

A. ON Period = OFF Period

First the technique is tested when PU ON and OFF periods are equal. ON period and OFF period are taken as 2 s. Fig. 2(a) illustrates PU traffic model. PU arrives to system and transmits data between 2–4 s and 6-8 s.

Fig. 2(b) shows the change in the MOS value of the SU VoIP application when PU traffic is as given in Fig.2(a).

 ISBN: 978-1-61208-166-3

MOS starts to decrease at time 2.0, which is the PU arrival time. Since our algorithm notices a small decrease in MOS, it increases ptime. That's why MOS increases in the next MOS calculation. Similar behavior occurs at time 2.8. When there is a bigger decrease than 1, like at time 7.0, the algorithm changes codec and in the next period MOS increases.

B. *ON Period > OFF Period*

We also tested the traffic model where ON period of PU is bigger than OFF period. PU traffic model is illustrated in Fig. 3(a). PU arrives to system and transmits data between 2–5 s and 7-10 s. This is risky for the SU, since PU remains in the system longer. ON periods are 3 s; while OFF periods are 2 s.

SU MOS changes are given in Fig. 3(b). MOS changes start to decrease after time 2.0, which is the PU arrival time. Since our algorithm notice a small decrease in MOS, it increases ptime. That's why; MOS increased in next MOS calculation period. Same thing occurs in 2.8. When there is a greater decrease, the algorithm changes codec and in next period MOS increased.

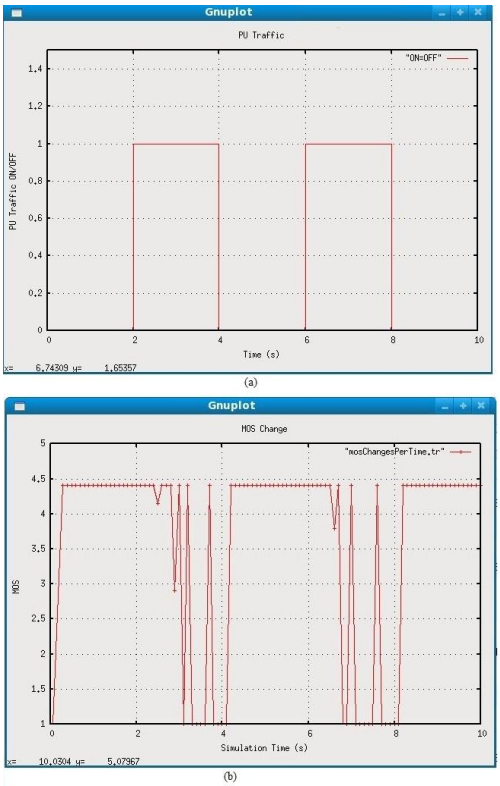


Figure 2. ON Period = OFF Period a) PU traffic b) MOS change on SU

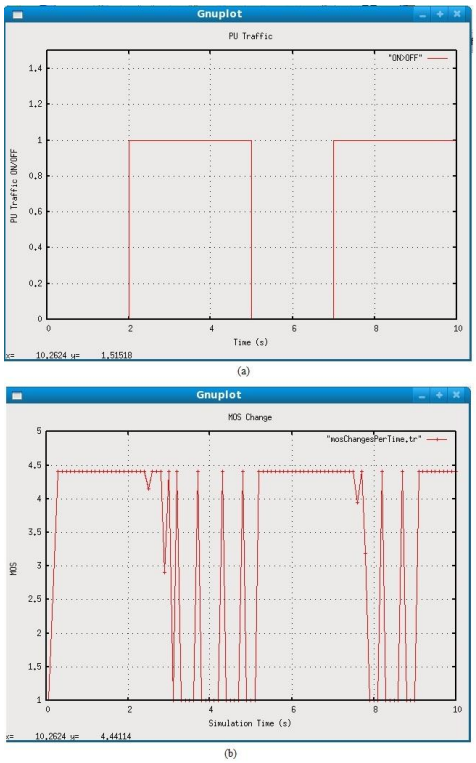


Figure 3. ON Period > OFF Period a) PU traffic b) MOS change on SU

C. *ON Period < OFF Period*

Lately, traffic model of ON period of PU is less than OFF period is tested. Fig. 4(a) illustrates PU traffic model. PU arrives to system and transmits data between 3–5 s and 8-10 s. ON periods are 2 s, while OFF periods are 3 s.

Fig. 4(b) shows the MOS changes in SU according to the behavior of the PU. Changes in MOS start to decrease at time 3.0, which is the PU arrival time. Since our algorithm notice a small decrease in MOS, it increases ptime. That's why; MOS increased in next MOS calculation. Same thing occurs in time 2.8 s. When there is a greater decrease like at time 7.0 s, algorithm changes codec and in the next period MOS increases.

VI. CONCLUSION

This study focuses on the Quality of Service enhancement for the Secondary Users with VoIP connections in Cognitive Radio Networks. One of the most popular applications, Voice over IP is chosen and tried to achieve a satisfying QoS level to the corresponding SUs. For this purpose, first, real VoIP packets are collected from Genband Application Server, and analyzed. After analyzing VoIP packets and VoIP signaling, a solution in application layer is proposed to provide better QoS to SU VoIP applications. Then, we simulate the technique proposed using ns-2. The technique is an application layer approach where the MOS value for the VoIP connection is measured periodically and by chancing the ptime parameter or the codec type according the QoS of the connection is enhanced.

 ISBN: 978-1-61208-166-3

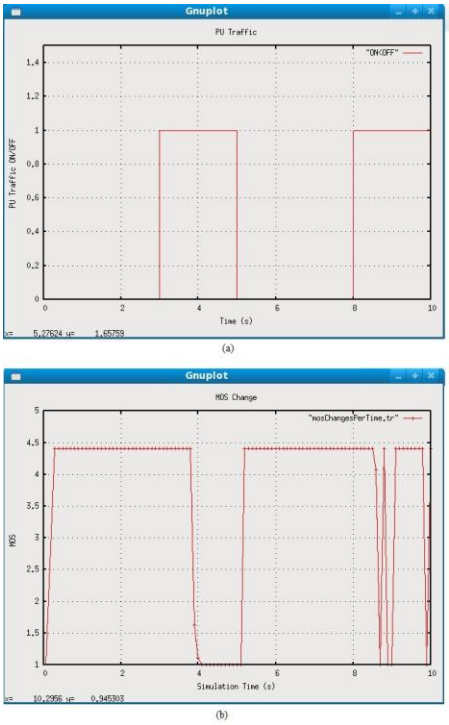


Figure 4. ON Period < OFF Period a) PU traffic b) MOS change on SU.

It is shown that the proposed technique gives promising results for Cognitive Radio Networks by the simulations done in ns-2.

The performance of this algorithm can be further enhanced by not only observing MOS decreases but also observing MOS increases, and changing the codec type or ptime parameter to appropriate values when there is no PU around.

For future work, PUs with different behaviors are going to be employed.

ACKNOWLEDGMENT

Authors would like to thank NETAS for their support.

REFERENCES

[1] Waze, V. L., "Spectrum access and the promise of cognitive radio technology", Cognitive Radio Workshop Presentations, Washington, DC, May 2003

[2] Wang, B., and Liu, K. J. R., "Advances in cognitive radio networks: a survey", IEEE J. Sel. Topics Signal Process, vol.5, no. 1, pp 5-23, 2011

[3] Akyildiz, I. F., Lee, W. Y., Vuran, M. C., and Mohanty, S., "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey", Computer Networks, vol. 50(13), pp 2127–2159, 2006

[4] Wu, Y., Tsang, D. H. K.," Distributed power allocation algorithm for spectrum sharing cognitive radio networks with QoS guarantee", IEEE INFOCOM, Rio de Janeiro, Brazil, April 2009

[5] Yau, A. K. L., Komisarczuk, P., and Teal., P. D., "C2net: a cross-layer Quality of Service (QoS) architecture for cognitive wireless ad hoc networks", ATNAC, Adelaide, SA, December 2008

[6] Lien, S. Y., Prasad, N. R., Chen, K. C., and Su, C. W., "Providing statistical Quality-of-Service guarantees in cognitive radio networks with cooperation", IEEE CogART, Aalborg, Denmark, May 2009

[7] Liang, Z., Zhao, D., "Quality of Service performance of a cognitive radio sensor network", IEEE ICC, Cape Town, South Africa, May 2010.

[8] Lee, H., and Cho, D., "Capacity improvement and analysis of VoIP service in a cognitive radio system", IEEE Trans. Veh.. Technol., vol. 59, no. 4, pp. 1646-1651, 2010

[9] Wang, P., Niyato, D., and Jiang, H., "Voice-Service capacity analysis for cognitive radio networks", IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1779-1790, 2010

[10] Lakas, A., and Boulmalf, M., "Experimental analysis of VoIP over wireless local area networks", Journal of Communications, vol. 2, no. 4, pp. 3-9, 2007

[11] RFC3261, SIP: Session initiation protocol, Internet Engineering Task Force, 2002

[12] H.323, ITU-T Recommendation, 2006

[13] Cruz, H. T., and Torres-Román, D., "Traffic analysis for IP telephony", 2nd International Conference on Electrical and Electronics Engineering (ICEEE) and XI Conference on Electrical Engineering, Amsterdam, the Netherlands, June 8-12, 2005

[14] RFC 4566, Session Description Protocol, Internet Engineering Task Force, 2006

[15] Real-Time Transport Protocol (RTP) Parameters, IANA, <http://www.iana.org/assignments/rtp-parameters>, accessed at 05.06.2011

[16] Schulzrinne, H., Casner, S., RTP profile for audio and video conferences with minimal control, 2003

[17] CISCO, 2005: "Voice Over IP - per call bandwidth consumption", unpublished

[18] Pracht, S., Hardman, D., "Voice quality in converging telephony and IP networks", unpublished

[19] Unuth, N., Mean Opinion Score (MOS) - A Measure Of Voice Quality, http://voip.about.com/od/voipbasics/a/MOS.htm, accessed at 05.06.2011

[20] ITU-T Recommendation G-107, "The E-model, a computational model for use in transmission planning", 2005

[21] Genband Application Serverö <http://www.genband.com/Home/Products/Applications/A2-Business-Applications.aspx>, accessed at 05.06.2011

[22] Netaş, <http://www.netas.com.tr/ >, accessed at 05.05.2011

[23] How is MOS calculated in PingPlotter Pro, <http://www.nessoft.com/kb/50>, accessed at 05.05.2011

[24] NS-2, < http://www.isi.edu/nsnam/ns/>, accessed at 05.06.2011

 ISBN: 978-1-61208-166-3

Overcoming EPC Class 1 Gen 2 RFID limitations with p-persistent CSMA

Leonardo D. Sánchez M. and Víctor M. Ramos R.
Universidad Autónoma Metropolitana
Networking and Telecommunications Research Team
Iztapalapa, Mexico City
{cbi209382362,vicman}@xanum.uam.mx

***Abstract*—Nowadays, Radio Frequency IDentification (RFID) is a widely spread technology used in a diverse set of applications. One of the main problems faced by RFID networks is tag collision. This occurs when two or more tags respond simultaneously to the RFID reader, causing errors and bringing retransmissions in the wireless channel, increasing the delay required to identify the whole set of tags in the coverage range of the reader. There are two standards for RFID tag identification: ISO 18000-7 and EPC Class 1 Gen 2. We propose in this paper a p-persistent CSMA mechanism for RFID tag identification; we also compare our mechanism with the EPC Class 1 Gen 2 as well as with a non-persistent CSMA approach that has been proposed in the literature. We show that the mechanism we propose provides a lower identification delay than the two other mechanisms. Furthermore, our mechanism uses less identification cycles than its non-persistent CSMA counterpart.**

Keywords– RFID, EPC Class 1 Gen 2, p-persistent CSMA.

I. INTRODUCTION

Nowadays, Radio Frequency IDentification (RFID) is a technology used on a wide set of applications. According to [1], 1.3 billion of RFID tags have been built in 2005, and by the end of the last year the amount of tags grew up to 33 billion [1]. Some examples of RFID applications are: public transportation, access control, asset tracking, item identification, counting tasks and automated inventory management.

One of the main advantages of RFID compared to barcodes is its ability of identifying objects in a wireless fashion with no contact or a direct sight line among the communicating devices. Since RFID is now widely used, the identification process must be done in a faster and efficient way. To that end, it is crucial to find better collision resolution mechanisms for RFID networks. This way, the identification process as well as power consumption are improved.

There are two standards for RFID tag identification: ISO 18000-7 and EPC Class 1 Gen 2. We propose in this paper a p-persistent CSMA mechanism for RFID tag identification; we also compare our mechanism with the EPC Class 1 Gen 2 (EPC-Gen 2 from now on) as well as with a non-persistent CSMA approach that has been proposed in the literature. In Section II, we present a review of the state of the art in RFID as well as the problem of tag collisions. In Section III, we depict the related work about collision resolution of RFID tags. We propose finally in Section IV our p-persistent CSMA protocol for RFID; we also compare numerically our mechanism with the EPC-Gen 2 standard as well as with a non-persistent CSMA approach that has been proposed in [2]. The results described in Section V show that our protocol overperforms the other two proposals in terms of identification delay as well as in the average number of identification cycles. We execute simulations for a wide number of tags in the coverage range of the reader. We finally conclude our paper in Section VI and describe our future work.

II. RFID AND TAG COLLISIONS

An RFID network is composed of two sets of devices that communicate through radio-frequency (RF) waves: a set of *tags* joined to objects that need to be identified, and one or more *readers*. A reader has storage and processing abilities, it sends read commands within a given coverage range in order to identify the whole set of tags inside such range. Tags are devices having a unique identifier; they store information about the object they are attached to. RFID tags may be classified as:

- *Active tags*: They account with high processing and storage abilities. They include a power source for data transmission and are also responsible of sensing the channel and detect collisions.
- *Passive tags*: They have limited processing, storage and data transmission characteristics. They have no power source; instead they get power through the energy induced by electromagnetic waves sent by the reader. Besides, they have no sensing capabilities **nor-or** sensing functions.
- *Semi-passive tags*: They use internal batteries to power their circuits and rely on the reader to supply its power for broadcasting.

Based on the type of application, a given type of RFID tag is chosen. Passive tags are frequently used due to their low cost. However, semi-passive and active tags are rapidly gaining an important place in the RFID market.

A. The tag identification problem

A tag identification process consists of a broadcast message sent by the reader to request tags their IDs and/or their stored data. By receiving such broadcast message, the tags send their response to the reader. If just one tag responds, the

 ISBN: 978-1-61208-166-3

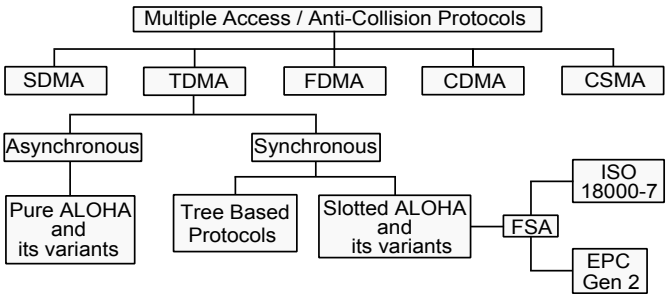


Fig. 1. RFID collision resolution protocols' taxonomy

reader will receive only one message. If several tags respond simultaneously, there will be collisions in the RF channel. Such problem is known as *tag collision* and is one of the main research problems on RFID networks. The time taken to identify the whole set of tags within the range of the reader is known as the *identification delay*; this is one of the most important performance measures in this kind of networks.

Besides tag collisions, there are also reader-reader collisions and reader-tag collisions. The former occurs when there is interference between the signals of two or more readers. The latter occurs when two or more readers want to communicate with the same tag [3].

Currently, the tag collision problem is solved by implementing a collision resolution protocol specified either by the EPC-Gen 2 standard or by the ISO 18000-7 standard. The former being used for passive as well as for active RFID environments, and the latter for active RFID environments. In a recent work [4], we have presented a comparison between our p-persistent CSMA protocol and the ISO 18000-7 standard. In this paper, we restrict ourselves to comparing our work with the EPC-Gen 2 standard and the non-persistent CSMA approach we cited before.

III. Related work

The wireless nature of RFID networks implies the use of a collision resolution protocol at the MAC level of the network stack. Thus, the aim of a collision resolution protocol for an RFID network is to coordinate the access to the transmission medium. We present in Fig. 1 a taxonomy of collision resolution protocols on the basis of medium access and then on the type of protocol used.

A. ALOHA-based protocols

ALOHA-based protocols are probabilistic protocols exhibiting low values on the identification delay. However, such protocols have the problem of *tag starvation* due to their aleatority; such problem happens when a tag has not been identified in a long period of time.

The most widely used protocols in this class are Pure ALOHA (PA), Slotted ALOHA (SA), and Framed-Slotted ALOHA (FSA). These protocols impact directly the performance of RFID networks. The two standards used for RFID networks are based on a modified version of Framed-Slotted ALOHA.

1) Framed Slotted Aloha (FSA): The FSA protocol is based on the SA protocol which assumes that time is slotted and grouped into frames. A slot is a time interval where tags are allowed to transmit their ID [5]. FSA executes several identification cycles (IC) in order to identify the whole set of tags within the coverage range of the reader. Every identification cycle consists of one frame. A frame is a time interval elapsed between reader requests; it is formed of a given number of slots [5]. FSA improves PA and SA by limiting tags to transmit once per frame in order to avoid frequent tag-to-tag collisions.

FSA starts with the reader broadcasting the frame size, N. Once tags know N, every tag generates a random number uniformly distributed between $[0 \ldots$N-1$]$. The generated number corresponds to the slot of time where tags transmit their ID. When two or more tags transmit in the same slot, there is a collision; this event generates a new identification cycle. Such identification cycle is particularly intended for the tags that generated such collision. Furthermore, if there is only one transmission during a slot, the corresponding tag is correctly identified by sending an ACK message; this avoids including the same tag in the next identification cycle.

2) The EPC-Gen 2 standard: The EPCGlobal organization has proposed the EPC-Gen 2 standard for RFID networks. In [6], the "Gen 2" collision resolution protocol is independent of the type of RFID device in which it is implemented, being either passive or active.

Similar to the ISO 18000-7 standard, the EPC-Gen 2 standard proposes to use FSA as a collision resolution protocol for RFID networks. However, EPC-Gen 2 suggests a specific algorithm for adapting the frame size. EPC-Gen 2 works on an environment of 1 reader and N tags. The identification process starts when the reader sends a startup command; then every tag responds to such command causing a collision. When the reader detects the collision, it starts a new identification cycle. An identification cycle starts with the broadcast of a `Query` packet by the reader including the value of $Q \in [0, \ldots, 15]$, this is useful to indicate that the size of the current frame is 2^Q slots. From this point, the tags choose a time slot r in the interval $[0, 2^Q - 1]$; this selection process is randomly done according to a uniform distribution. The value of r represents the frame slot in which every tag transmits its ID. The start of every slot into a frame is controlled by the reader with the transmission of a `QueryRep` packet, with the exception of the first slot which starts after the `Query` command. Thus, the tags use r as a counter which decrements its value after receiving every `QueryRep` packet. When the r value of a tag reaches zero, the tag sends its ID; such event generates three possible cases:

- If two or more slots choose the same time slot, there will be a collision. On one side, the reader detects the collision and sends a `QueryRep` packet. On the other side, the involved tags update r according to $r = 2^Q - 1$.
- If there is only one reply in a given slot, there will be a successful identification. Thus, the reader responds with an `ACK` packet. Even if all the tags receive such packet,

 ISBN: 978-1-61208-166-3

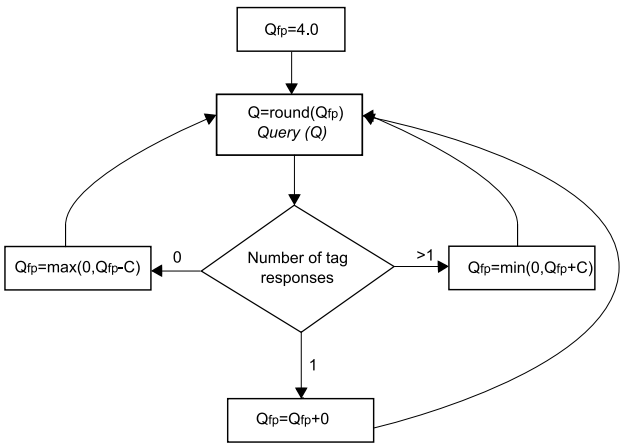


Fig. 2. Frame adapting mechanism for Q.

only the "winner" tag will respond with a `Data` packet. Afterwards, once the reader receives the `Data` packet it responds with a `QueryRep` packet.

- If there is no response before the reader finishes reading the time slot, the reader assumes an empty slot and starts a new one by sending a `QueryRep` command.

This process continues slot after slot until the end of the identification cycle, i.e., until the end of the frame. At the end of each frame, the reader adjusts Q based on the number of empty slots, the number of slots with only one response, the number of slots with multiple responses, and consequently the size of the subsequent frame. The identification process finishes when the whole set of tags has been identified, i.e., when all the slots of the frame have been flushed.

Fig. 2 depicts the EPC-Gen 2's frame adapting mechanism. As we can see, such mechanism increments Q for every slot in which there was a collision, and decrements it for every empty slot in the current frame. The standard proposes the use of $C \in [0.1, \ldots, 0.5]$ to control the frame adapting mechanism in a slot-by-slot fashion. However, it does not specify how to choose C, it only recommends using high values of C for low values of Q and vice-versa.

B. Non-persistent CSMA

In [2], the authors propose the use of non-persistent CSMA for RFID. They extend such protocol to work on an environment of one reader with several tags. The work presented by the authors is based on a contention window for the identification process; this is equivalent to an FSA frame in the context of ALOHA-based protocols. They implement a distribution function that is used also in [7] so as every tag randomly chooses a micro-slot in a contention window to transmit its ID.

The *Sift* distribution (1) associates the probability p_r to the micro-slot r as a function of its location in the contention window and the maximum number of tags. In this way, the probability of choosing the first micro-slots is low while selecting the last micro-slots turns to be high. So, p_r is given by:

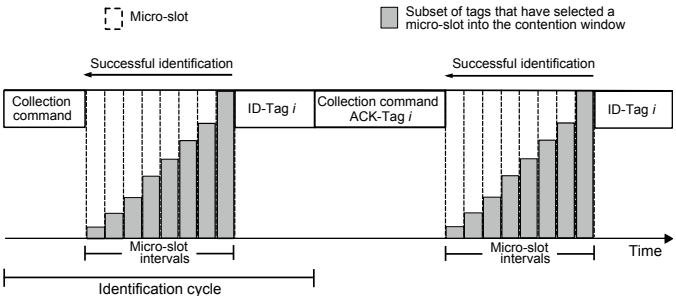


Fig. 3. Non-persistent CSMA with Sift distribution for active RFID environments.

$$p_r = \frac{\alpha^r (1-\alpha)^k}{1-\alpha^k} \tag{1}$$

with $r \in [1, \ldots, K]$ and $\alpha = M^{-1/(K-1)}$. K is the size of the contention window, and M represents the maximum number of contenders.

We now describe how this protocol works: the reader broadcasts an ID-request including the size of the contention window and the maximum number of contenders, which is a priori unknown. After receiving this message, the tags choose a micro-slot in the contention window according to (1) so as to transmit their ID in the chosen micro-slot. Afterwards, every tag sense the channel until the value of the micro-slot chosen and then they transmit if and only if the medium remained free. In other case, a tag leaves until the transmission of the next command by the reader. If there is no collision, the reader sends an `ACK-Collection` command which indicates that the tag has been already identified, and thus requesting more IDs. The same process is repeated for the tags that remain unidentified. Fig. 3 depicts the non-persistent CSMA protocol with Sift distribution.

Under this mechanism, the contention window size remains constant during all the identification process and only one tag is identified per identification cycle. The results shown in [2] show that non-persistent CSMA with Sift distribution overperforms the EPC-Gen 2 standard with respect to the identification delay.

IV. p-PERSISTENT CSMA FOR ACTIVE RFID ENVIRONMENTS

p-persistent CSMA is a slotted scheme where a station that wishes to transmit senses firstly the channel. If the channel is idle, the station transmits with probability p and delays its transmission until the next slot with probability $q = 1 - p$. If the next slot is free, a transmission occurs or it is delayed with probabilities p and q, respectively. This process is repeated until the end of the contention window, or until the beginning of a new transmission by another station. In this last case, the protocol behaves as if a collision had occurred. If at the beginning of a transmission a station detects a busy channel,

 ISBN: 978-1-61208-166-3

it waits until the next time slot and then follows the algorithm just described.

In order to extend the behavior of p-persistent CSMA for RFID, we have that there are N tags in the coverage range of a reader which we need to identify in an ordered fashion by using a congestion window of a fixed size. The reader broadcasts a command of data collection along with the size of the contention window. Following the reception of this command, every tag chooses a time slot in the contention window according to a Sift distribution. Then, every tag computes the transmission probability corresponding to the selected time slot. If it decides to transmit, then it senses the channel during a time equal to a given number of micro-slots according to a Sift distribution, and transmits if and only if the channel remains idle after such period of time. Otherwise, it withdraws until the next collection command; i.e., until a new identification cycle. If there is no collision, the reader sends an `ACK` to tell a tag that it has already been identified and asks for more IDs. In this way, the transmission probability not only reduces the number of participants within a contention micro-slot, but it also allows for tag save energy. This is the key difference between the non-persistent CSMA protocol and our p-persistent approach.

By observing the results reported in [2], we observe that an increase in the number of tags is proportional to the number of collisions, even if the probability of choosing the first micro-slots is very low. In that sense, we see that we require that the transmission probability of each tag is a function of the time micro-slot chosen. Thus, by following the Sift distribution, once a tag has selected one of the first micro-slots to transmit, the probability that this tag does not transmit is close to zero.

In order to assign different transmission probabilities to time micro-slots in a contention window, we use in our proposal (2) so that every tag computes the transmission probability, p_t, based on the contention window size and the time micro-slot chosen in the contention window as well. Once p_t is computed, every tag decides its transmission based on this probability and a random number.

$$p_t = \frac{K - r}{K}, \tag{2}$$

where K is the total number of time micro-slots in the contention window and $r \in [1 \dots K]$ is the time micro-slot chosen for transmission.

The Sift distribution in our scheme offers the advantage that when a tag chooses one of the first time micro-slots, the probability of a decision change is practically zero.

One difficulty faced by our scheme is to decide when there are no more tags to identify, since using the transmission probability does not allow us to be sure of this fact. In order to solve this problem, when the first identification cycle is empty, we make the transmission probability equal to one. This way, we are sure that all the tags in the coverage range of a reader are actually identified.

We can see in Fig. 4 the building blocks of our p-persistent CSMA mechanism with Sift distribution.

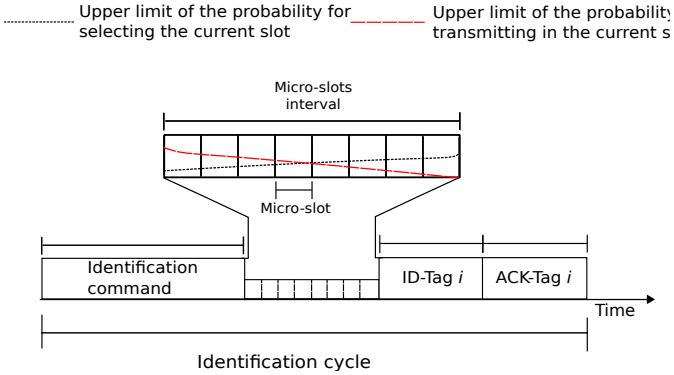


Fig. 4. p-persistent CSMA with Sift distribution for active RFID environments

.

A. Performance parameters

We focus on the identification delay as a performance parameter for comparing our proposal with the non-persistent CSMA protocol as well as with the EPC-Gen 2 standard. The identification delay is the time needed to identify the whole set of tags in the coverage range of the reader. Since the time taken by an identification cycle is a function of the number of slots and the number of messages between the reader and the tags, we transform the identification cycles to absolute time. The parameters we consider are the same as in [2].

When working with EPC-Gen 2, the empty slots and the slots with collision are shorter than the slots that have a correct ID. So, if for example the channel capacity is 40 kbps, a slot with a correct ID lasts for 2.505 ms and the empty slots as well as slots with collision last for 0.575 ms.

For non-persistent CSMA and p-persistent CSMA, we consider that one identification cycle lasts the sum of the following times:

- The time taken by a data recollection command (0.55 ms).
- The time taken by an ID packet (1.4 ms).
- A micro-slot time (0.1 ms), and
- The time duration of an `ACK` packet, in case of a successful identification (1.4 ms).

We assume that tags have a coherent CCA (Clear Channel Assessment), i.e., that the channel is busy when a packet's preamble is detected. We also consider that the network is free of the *capture effect*. The capture effect on RFID refers to the event when two or more tags try to transmit simultaneously to a reader, and one of the tags achieves its transmission because it is under better physical conditions like a higher transmission power or because it is closer to the reader.

We implement EPC-Gen 2 with the mechanism specified in [6], non-persistent CSMA and our p-persistent CSMA with a contention window size equal to 8 micro-slots and M equal to 64. We execute 300,000 simulations for each protocol and we obtain confidence intervals of 95% with a precision less to 1 ms. We also vary the number of tags from 10 to 100. Furthermore, since we are simulating a widely used standard

 ISBN: 978-1-61208-166-3

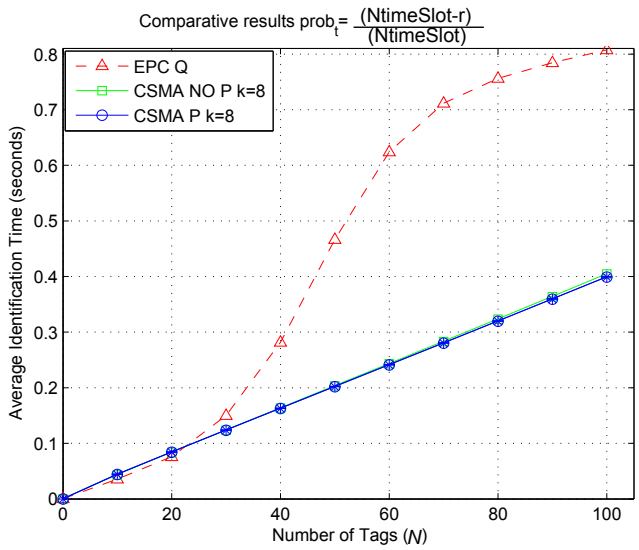


Fig. 5. Identification delay of EPC-Gen 2, non-persistent CSMA and p-persistent CSMA.

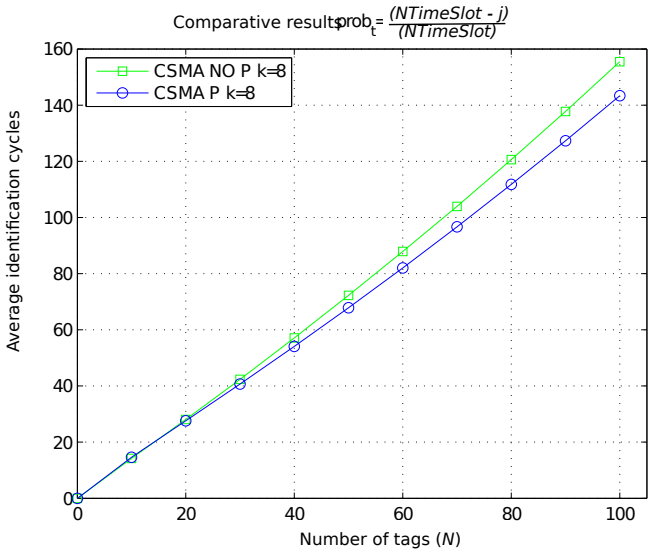


Fig. 6. Identification cycles used by non-persistent and p-persistent CSMA.

for RFID systems, our results are valid for any type of active RFID tag.

V. Results

We present in Fig. 5 the performance comparison between the three protocols we are evaluating. At the beginning of the plot, our protocol exhibits a small degradation on performance compared to the non-persistent CSMA approach, but as the number of tags increases our protocol clearly improves its performance.

In general, the results we get show that our proposal improves the performance of non-persistent CSMA and the EPC-Gen 2 standard. This is because our proposal uses less identification cycles than the non-persistent CSMA approach since the identification delay is directly proportional to the number of identification cycles, even if our proposal uses a bit more micro-slots than non-persistent CSMA. Due to the timescale in Fig. 5, it might seem that the improvement obtained with p-persistent CSMA is little; however, if the time taken by an identification cycle is increased then the improvement is clearer.

Fig. 6 shows a plot that compares the number of identification cycles between non-persistent and p-persistent CSMA.

VI. Conclusions

We have presented in this work a proposal of p-persistent CSMA with Sift distribution for its use on active RFID environments. We compared our protocol with a non-persistent CSMA approach previously proposed in the literature as well as with the widely known EPC-Gen 2 standard. Our results show an improvement of up to 2% in terms of identification time compared to non-persistent CSMA.

We observed that the time taken by an identification cycle directly impacts the performance of every protocol, because a bigger amount of messages is exchanged between the reader and the tags. So, by reducing the number of identification cycles the performance is improved. Finally, the improvement we got with p-persistent CSMA is clearer when the time spent during the identification cycles increases.

Our future work will focus on finding the value of p that optimizes the identification process; i.e., jointly maximizing the throughput while minimizing the loss rate. Furthermore, even if additional performance parameters (e.g., bandwidth, loss rate) are directly related with the identification delay, we will also explore the behavior of our approach with respect those parameters as well. We believe that future versions of RFID standards (i.e., ISO 18000-7 and EPCGen-2) for collision resolution may consider CSMA variants in their proposals.

References

[1] S. A. Ahson and M. Ilyas, *RFID Handbook: Applications, Technology, Security, and Privacy*. CRC Press, 2008.

[2] J. Vales-Alonso, F. J. González-Castaño, E. Egea-López, M. V. Bueno-Delgado, A. Martínez-Sala, and J. G. Haro, "Evaluación de CSMA no persistente como protocolo anticolisión en sistemas RFID activos," in *Primeras Jornadas Científicas sobre RFID*, 2007, pp. 313–320.

[3] G. Maselli, C. Petrioli, and C. Vicari, "Dynamic tag estimation for optimizing tree slotted ALOHA in RFID networks," in *Proceedings of the 11th International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM)*, 2008, pp. 315–322.

[4] L. Sánchez and V. Ramos, "p-persistent CSMA as a collision resolution protocol for active RFID environments," in *Proceedings of the IEEE/IFIP WOCN*, May 2011.

[5] M. A. Bonuccelli, F. Lonetti, and F. Martelli, "Instant collision resolution for tag identification in RFID networks," *Ad Hoc Networks*, vol. 5, no. 8, pp. 1220–1232, 2007, recent Research Directions in Wireless Ad Hoc Networking.

[6] EPCGlobal, "Class 1 Generation-2 UHF RFID Air Interface Protocol Standard Specifications," 2004.

[7] K. Jamieson, H. Balakrishnan, and Y. C. Tay, "Sift: A MAC protocol for event-driven wireless sensor networks," *Wireless Sensor Networks*, 2006.

 ISBN: 978-1-61208-166-3

Incorporating Radio Frequency Identification into The Production Line for Work Flow Improvement

Andrew Mc Clintock[2], Charles Young[1], Kevin Curran[2], Dennis McKeag[2] and Gavin Killeen[1]

[1] NuPrint Ltd, Springtown, Derry, Northern Ireland
[2] University of Ulster, Northern Ireland

***Abstract* - Radio Frequency Identification (RFID) technology can be used in many different applications. There are numerous instances of RFID being used in everyday life. For instance, anyone who works in a secure office, goes to university, drives a car with an immobiliser or parks in a secure car park. Other scenarios include the tracking of animals in the farming industry when cattle and sheep need to be identified by the farmer. Another instance where RFID can be used is in the manufacturing industry. Tags can be attached to items that are moving through the factory on conveyer belts or being moved around by staff on trucks or forklifts. This paper documents a "real life" manufacturing facility, assess its current work flow process, evaluate them against industries best practices and seek to integrate RFID to help stream line work flow. After assessment, the RFID solution will be implemented to tackle the highlighted areas. This will be achieved by understanding the client's current situation, industrial best practices and how RFID technology can be implemented now and modified in the future to continue to maximize efficiency. The expected outcome of the research is that RFID can contribute to modern work flow systems, however all systems will be inevitably based on a software database, and it will be how the RFID technology is used to create additional database entries and manipulate or link existing data that will see its true value.**

Keywords – RFID; Lean manufacturing; Location Determination; RFID tracking.

I. INTRODUCTION

It is often said in the automation industry that to control, you must first measure. RFID is a non contact, long distance, water proof, high temperature resistant, data storage, automatic identification system. These attributes make RFID the ideal solution for tracking and measuring the flow of physical items throughout a plant. The RFID system comprises of an integrated collection of components, the tag, the reader, the reader antenna, a controller, a sensor, actuator and annunciator (optional), host and software system and communication infrastructure [1]. These qualities allow RFID to play an important role in allowing the physical flow of equipment throughout a plant to be linked to, or create an information flow that is real-time. This type of information used in the correct way can allow for a transparent plant wide view of how the plant runs, enabling users to see and predict bottlenecks and backlogs. In acquiring this data, the plant is then in a position to allow for data interrogation in order to optimize plant or process activities. Lean Manufacturing is a process of data interrogation in order to eliminate any Non Value Adding Tasks (NVAT) thus improving efficiency [2].

All manufacturing facilities must possess and adhere to their own manufacturing systems. These systems are the foundation on which any industrial accreditations are built, they define the work flow process and are therefore critical to all aspects of how the company operates. The tools the systems are built on usually refer to electronic tools, such as software packages and written documents manually created, maintained and archived. A vast majority of these systems operating today have been developed onsite by skilled employees knowing their own responsibility and therefore produced a tool that delivers what his or her department needs to. These tools have been developed in a similar fashion, as quality controls or accreditation standards increase or the business changes. It is therefore accepted that a vast majority of these tools certainly serve their purpose, but are not as efficient or as transparent as they could be.

In today's global manufacturing environment the western world is at a disadvantage because of , high labour costs, high land rates, stringent environmental rules and regulations. These factors make it difficult for manufacturing facilities to compete with its neighbouring Asian counterpart. It is no surprise then that our manufacturing industry is in a consolidation period and looking to maximizing efficiency by increasing utilization of their current assets. This is clearly reflected in industrial management buzzwords. These buzz words are encapsulated by two ideas, Lean manufacturing and Total Cost of Ownership. Lean Manufacturing was a system originally developed by Toyota and defines wastefulness as any activity that is non value adding. It was claimed by implementing lean manufacturing, you can use less of everything compared to mass production- half the human effort in the factory, half the manufacturing space, half the investment in tools, and half the engineering hours to develop a new product. In addition, it requires keeping less

 ISBN: 978-1-61208-166-3

than half of the needed inventory on site, results in a lot fewer defects, and produces a greater and ever-growing variety of products. In short, it is called lean because it uses less, or the minimum of everything required to produce a product or perform a service [1].

All this can be achieved by reducing NVAT's at every stage in the system. Total cost of ownership analysis then looks at the total cost of the system for its life time. These costs include but are not limited to, cost of installation, preventative maintenance, corrective maintenance, operational costs, repair costs and end of life costs and expand the buyer's thought process beyond the initial purchase cost [3]. For manufacturing facilities to address the problem areas they must first find them. The solution requires gathering more data, gathering the data quicker, making the data more transparent and easy to access, increase communication ability and increase tractability. In comparing RFID technology to the traditional barcode system to provide the technology for the solution it has many advantages including but not limited to, short scan times, anti pollution and durable, flexible data, penetrability through other materials, usable user data and better security [4]. Given these advantages it is easy to see why the technology has been adopted in a wide range of industries such as logistic, Health care, toll systems, retail, security and identification to name a few. This project will look to integrating RFID into the current manufacturing work flow system to expose these advantages thus reducing waste and the TCO.

The "real life" facility is NuPrint Technologies LTD, a local manufacturing company who manufacture labels. NuPrint management have highlighted that there is an opportunity to reduce waste in two key production stages. These stages are known as Pre-prep and Production. Pre-prep, as the name suggests prepares the equipment before use in production, and maintains it after the job is complete. The equipment is in the form of plates and rollers. The plates must be wrapped around the roller and aligned. Production fit the plates to automated printing machines and produces the required label. The pre-prep process is not as straight forward as it may seem. This is due to a multiple of variables including, damaged or weakened plates, plates being difficult to align, prioritisation of batch jobs, sourcing and reserving common plates to multiple jobs as well as keeping in touch with Operation control and Production to continually evaluate the job status. The aim of this project was to integrate an RFID solution into a Manufacturing Execution System (MES). It is hoped that the RFID solution will allow the MES to view the process in greater detail in terms of job and equipment location in real time. The real time MES will provide a transparent view of the process to Pre-prep, Production and Operation Control. This electronic view will allow each department to have up to date process information with no need to ask the other department, thus greatly reducing the requirement for personnel interaction. Personnel interaction is a major fluctuating unknown, which can be very wasteful. The real time view will also build a history database of the information gathered, as well as having the ability to hold any additional notes the operators may want to add.

II. RELATED WORK

The Department of Industrial Engineering, Tsinghua University, Beijing, set up a micro plant as to best simulate a real plant situation. RFID technology was used to support the MES to automate the tracking of materials, Work in Progress (WIP), fixed and mobile resources. They designed and implemented the solution to target three key areas. These were Data Collection and Document Control, Labor Management and Production Control and Performance Analysis. Data Collection and Documentation Control is a continuous task throughout the manufacturing process, but are of particular advantage in the job scheduling and inventory control. The best example of this advantage comes at the beginning of the manufacturing system, after a customer places an order, an operator scans the RFID labeled inventory stock, this real time scan, allows the MES to decide if the required inventory is available to complete the customer request. If it is, the job is sent to the sorting centre for packaging before being sent to the assembly line. However, if the required inventory is not available the MES system automatically generates a Purchase Order (PO) and produces it for review before emailing it to the supplier.

Labor Management and Production Control in this solution were encapsulated by visibility. Two billboards where utilised, one for the assembly line operator which updated them on the current job information and segment procedure. After the job is completed the operator interfaced with the MES system and indicated if it was finished or scrapped, triggering a job status change. The second billboard allowed management visibility of the production schedule being completed, including the current status of jobs. Performance Analysis is achieved as a byproduct of the previous two implementations. The system now is data rich, and is used to target Key Performance Indicator (KPI) matrices such as work station load and production efficiency. Any target change made can now be evaluated on tangible numeric data that is non intrusive [5].

RFID MES system can be flexible and responsive to continuous, changing customer requirements [6]. Huang et al. [6] outlines an RFID MES implementation in JAC, an automotive production company based in china. JAC manufacture a full line of brand vehicles including trucks, Special Reconnaissance Vehicle's (SRV's) and

 ISBN: 978-1-61208-166-3

Mechanically Propelled Vehicle's (MPV's). JAC already had an MES system using traditional data acquisition methods such as manual input and barcodes. However, they believed the gap between physical flow of product and information flow in the MES was too great to properly monitor and manage the production system. The additional data acquisition obtained by attaching RFID tags to tools, materials, personnel and equipment ensured the MES turned into a Real Time MES (RT-MES). The enhanced RT-MES decreased SRV cycle time from 5 days to 4 days, increased production efficiency by 20% and increased the MES data accuracy rate to 99.9%. It is important to look at what the technology has in store for the future. One key area for future development is combined logistical tracking with RFID & GPS [7]. The advantage here is the ability to link both business process info and geographical locations, this specifically targets the time consumed for sales, customer service, operation and warehouse staff to locate specific cargo in transit and provide the customer with the most accurate data in a time frame that is acceptable [8]. This data could also be shared between manufacturers, logistics and purchasers on the web so that better planning and scheduling can be done for incoming inventory.

III. RFID System Design

The design of this solution is to implement RFID in a manufacturing environment, to aid in the stream lining of production work flow. The incorporation of RFID itself may not achieve this, but using RFID as a data gathering tool to enrich databases with real-time information can target important areas to the business. The RFID system used was a Promag PCR-340 Dual-Frequency Stationary tag reader. The tags used were a combination of Gen2 Class1 Labels. These areas of the business include real time information which will highlight work flow bottlenecks. Monitoring this information during and after an operational fix has been implemented to reduce the bottleneck which will allow management to evaluate the fix and continue to improve it or move on to the next high priority bottleneck. In addition, operational procedures are stream lined whereby operatives must complete the previous task before moving on to the next stage.

Management Information System Integration

During the design of this solution, the client (Nuprint) bought an "off the shelf" Manufacturing Information System (MIS) called Tharsten [9][1]. Tharsten's MIS was implemented to control the production area and gathers a lot of critical information via user interfaces regarding the running of the printing presses. It was clear that if we could extract already gathered information from the Tharsten system we could greatly improve the richness of data in the Access database and therefore achieve better results. In light of this, Figure 1 shows a more detailed architectural overview of how data is gathered and shared between both systems. Data transfer is broken down into two types, same system communications and sub system communication. Same system communications is the server interacting with its own type of client to enable database entries, this takes place on both the Access side and the Tharsten side and is inherent in the systems and therefore relatively straight forward. What is not as usual is the passing of data between the systems, i.e. sub system communications. The Tharsten system is an SQL based server and after some research and testing it was decided that the sub system communications could be reliably delivered via an Open Database Connectivity (ODBC) link, note during discussions with Tharsten technical engineers it was clear that to maintain the Tharsten system integrity and support we could only read data from their system with no function of writing data to their system.

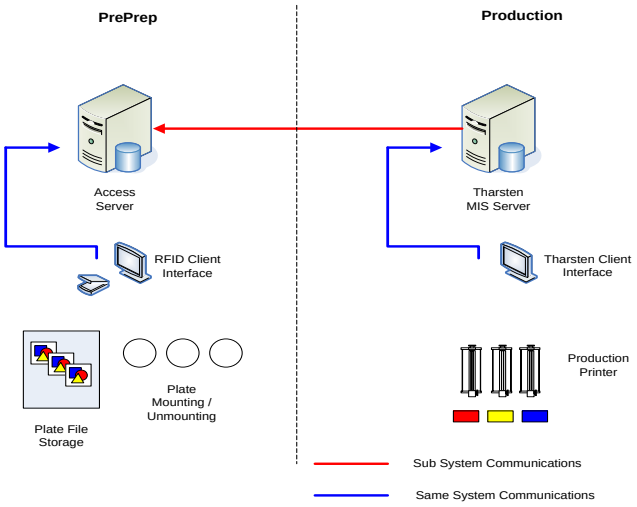


Figure 1 : System Communications

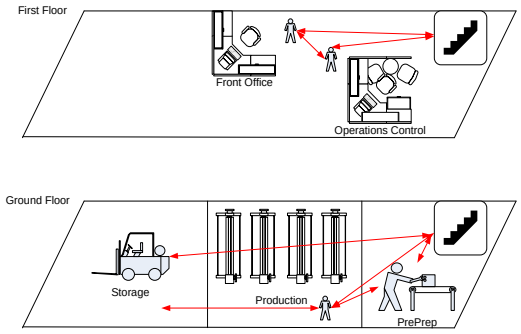


Figure 2 : Nuprint Facility Layout

[1] http://www.tharstern.com

Figure 2 shows how the facility is laid out and the typical personnel movement required to get a label batch produced from start to finish. After initial analysis, it was clear from the personnel movement that there are areas of concern i.e. the work flow is not fluid and there is a lot of required points of contact for each department to allow them to complete their individual tasks. This gives ground for a detailed analysis of both physical and data flow for a complete label batch production. It is clear that the area of greatest concern in the system is the communications between pre-prep and the production area. Given financial waste outlined earlier, it is clear there is an opportunity to introduce a system that will aim to tackle this area of high waste. It was decided that the specification is to incorporate an RFID system to operate as follows:

- Scan in Pre-prep to locate plate file and log time and confirm job is mounted ready for production and log time
- Scan at Production to identify and acknowledge receipt thus logging time beginning job production and indicate job completion and log time
- Scan in Pre-Prep to confirm receipt of plates and log time and to confirm plates have been cleaned, restored and log time

The incorporation of RFID should enable production control to establish the overall job status. These include the time taken to mount job, time spent in transit/waiting from pre-prep to the press, time spent on press and backlog of plates to be cleaned by pre-prep. The system should increase communication between production and pre-prep i.e. it should enable pre-prep to see the press status i.e. when the previous job has been scanned in by the printer to anticipate when a new job should be prepared. It should also allow pre-prep to see when the printing has finished and when the used plates/cylinders should be collected and production to check on the status of their next job. The system will provide traceability and accountability. It will enable JIT production with pre-prep preparing the next job only when the previous one has been scanned / received by the press. This will prevent wasted time caused by pre-prep mounting jobs too early in advance and potentially having to dismount them for an urgent job.

System Operation

After consultation with Nuprint and considering the new benefits the Tharsten system would have on the RFID system, the system operation was designed and a clear vision of how the final solution should interact with the operations team. It was clear that they required two main interfaces, one, to maintain their plate file database allowing the RFID labels to take over the old labelling system of Plate File numbers.

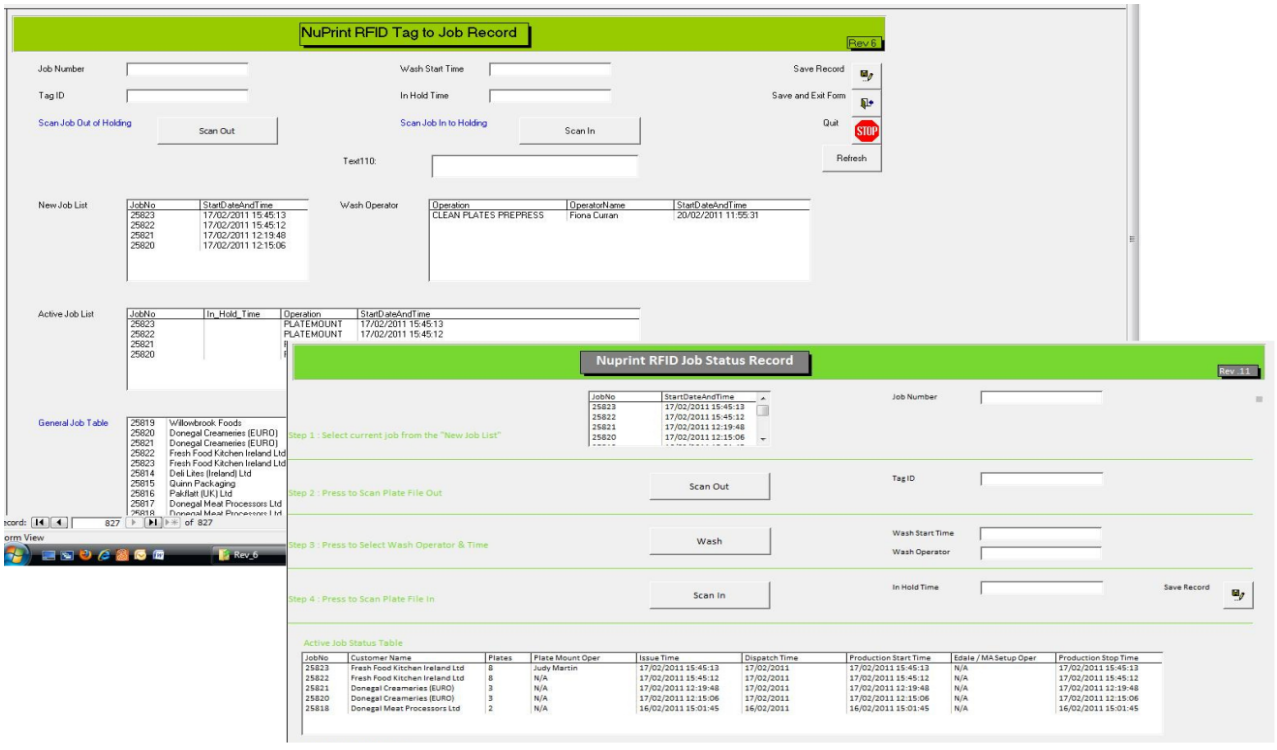


Figure 3 : User Friendly form design

The second interface is to allow production information to be inputted for the beginning and end of a job cycle in the Preprep area. These interfaces must be unambiguous, and simple to use. They must not increase the work load of operations and whether gathering information from Tharsten, RFID or Access appears to be one coherent system. The Nuprint RFID Plate File Record section is available to operations to associate RFID labels with the Plate File details. These details include, number of plates, Customer, supplier reference, number of colours, die size and product code.

The interface allows all relevant information to be shown with a simple scan button to associate a label with the plate file details. This interface will be used heavily on system implementation as Nuprint has approximately 350 current plate files, after this initial use the interface will only be used when a new job has been created for a customer or the RFID tag needs updating for an existing plate file. The Nuprint RFID Plate File Record section is the main operative interface. The interface is broken down into three main sections. Section one shows the operative interactions broken down into four main steps. Step one is for the operative to select an appropriate job, the choice available must only be jobs dispatched from Tharsten not yet picked up by Access, i.e. new jobs. Step two is to scan the plate file out of holding, there should be logical checks done in the background that ensures the correct plate file has been removed from holding by the operative, if the wrong one has been removed the operative should be prompted and not allowed to continue. Step three is to associate a plate cleaning operative and time with the plates after production has taken place. Step four is the scanning of the plate file back into hold and thus completing the job cycle. All steps must be clear and concise as to the operative actions. Figure 3 shows how the form was developed from early revisions to ensure user friendliness and additional work was kept to a minimum. This is the main form and subform which allows the worker in charge of preparing the plates to associate plates with tags and to also start a new job. Here a worker in the preprint area will locate a folder and select the scan out button. This will now start the clock for the time the folder is out of the preprint area. Once a job is finished and the cleaning down process begins, the worker will select the 'wash' button. This will now start the timer for the time taken to wash. This time will be complete when the worker selects the 'scan in' button which will allow them to replace the folder in the cabinet. This completes the process but most importantly, will time each of the stages allowing reports to be generated in real-time. The solution required multiple queries to provide operations and management with quality data to help improve work flow. The outputs of which provide dispatched jobs not yet picked up by operations, active jobs currently being manufactured, number of plates required per job, dates and times of specific actions, operator responsible for specific actions and the accumulative meters a plate has produced and sub divided into the specific jobs.

IV. RFID SYSTEM EVALUATION

It is important to evaluate how this project actually delivers on the key target areas outlined at the start. Analysis during the baseline showed the area of greatest waste in the communications between areas, take place between the Preprep and Production. The time now spent on overall communications is reduced from 37.1 min to 10.22 a reduction in 26.88 minutes per job, which represents a 72.4% reduction This data must now be equated to financial savings. The dispersion of the total saving 26.88 minutes is broken down into 19.03min for Production and 7.85 min for Preprep. Assuming that Nuprint run 1.5 batches a day these times increase to 28.6 min for production and 11.8 for Preprep. Taking a Preprep operative value at £30.00 per hour, the waste can be calculated as:

Financial Waste = (Saved Time (min) / 60) x 30
= (11.80 / 60) x 30 **= £ 5.90 per day**

Taking a Production operative value at £120.00 per hour, the waste can be calculated as:

Financial Waste = (Saved Time (min) / 60) x 120
= (28.60 / 60) x 120 **= £ 57.20 per day**

This equates to a total of **£ 63.10** of financial saving per day. As well as the everyday savings there is also non regular occurrences highlighted during base lining that the system tackles these types of individual issues are as follows:

Individual Issues: A typical example of an individual issue was, during a period when the pre-prep operator was off ill the pre-prep operators duties fell on the production operators. However, the process of washing the plates is an undesired task coupled with the limited time the production operator had, it was decided the plates would be left unwashed in a pile and not cleaned or filed away. The consequence of this was that when an urgent job came through, a delay was incurred in locating the plates. When the plates were located a further delay was incurred because they had to be washed and mounted. Once the plates were placed on the machine and the job ‘setup’ ready for ‘signoff’, it transpired that two were damaged as they had been situated at the bottom of the pile and were subsequently compressed. This necessitated the re-purchase of two £70 plates at a £10 delivery cost. The operations control was also faced with the dilemma of cleaning down

 ISBN: 978-1-61208-166-3

the machine to run a job while the replacement plates were being manufactured and delivered or to hold off on the wash-up / setup and run the job the next day. This expense was in addition to delaying delivery of the labels. The result of this bad relationship was an escapade wasting £100's and damaged reputation with a customer. After site consultation this likelihood and financial waste was evaluated at £250 per month, i.e. approximately **£12.5 per day**.

To summarize, the system is saving approximately £63.10 + £12.50 = **£75.60 per day**. This saving is substantial when equated to yearly savings of **£18,144.00** calculated at 5 day week, 4 weeks per month and 12 months per year. Not only is the saving justification enough but throughout this project it has become clear that Nuprint's ability to introduce and work with RFID technology is of utmost importance. RFID is becoming a technology that more and more label purchasers are requesting to fulfill their own manufacturing processes. Having this technology already in Nuprint's portfolio allows them to be proactive in selling the technology in the market place and not be driven to it by customers who could go elsewhere in this competitive market space.

V. CONCLUSION AND FUTURE WORKS

This project initially assessed a manufacturing plants work flow processes and evaluated them against industry best practices. RFID was identified as a technology which could help stream line the flow of work on the factory floor. It was clear initially that there were NVAT in NuPrint's system. However obvious this waste is to anyone that analyses the system, it was of utmost importance to numerically evaluate this waste. This numerical evaluation base line, in terms of finance and time, will firstly keep focus on the project aims throughout the period of the project, and secondly allow for proper evaluation and justification for the end install. Ultimately, the system provides a mass amount of information to the system and allows proper analysis of how the system operates and how it can be modified to enhance KPI's. This information input not only provides great transparency between departments but allows management to oversee the complete process, and answer questions such as whether any jobs that went for production are not returned to storage, the length it normally takes for job A to be completed, and whether areas such as pre-prep hold up production or vice-versa? The main aim was to provide a solution that reduces waste in NuPrint. The key here was not just the RFID technology but rather the data manipulation in the MES which must be capable of providing transparent accurate, easy to access data to all departments. It was found that this system will save approximately £63.10 + £12.50 = **£75.60 per day**. This saving is substantial when equated to yearly savings of **£18,144.00** calculated at 5 day week, 4 weeks per month and 12 months per year. Throughout this project it became clear that Nuprint's ability to introduce and work with RFID technology is of utmost importance. RFID is becoming a technology that more and more label purchasers are requesting to fulfill their own manufacturing processes. Having this technology already in Nuprint's portfolio allows them to be proactive in selling the technology in the market place and not be driven to it by customers who could go elsewhere in this competitive market space.

The next step in the system is to incorporate live twitter alerts and emails to customers once labels are finished. This allows Nuprint's customers to be more informed of each relevant job on the factory floor.

REFERENCES

[1] Wong, Y., Wong, K.W., & and Ali, A. (2009) Key Practice Areas of Lean Manufacturing, International Association of Computer Science and Information Technology - Spring Conference, 2009. IACSITSC '09.

[2] Lahiri, S. (2005) - "RFID System" in RFID Sourcebook

[3] Ritsma, R.J., Tuyl, A., and & Snijders, B. (2009), Buying the lowest Total Cost of Ownership (TCO), PCIC Europe, 2009. pp: 12-18, PCIC EUROPE '09.

[4] Bellis, M. (2007) Ernst Alexanderson 1878 - 1975, About.com, Available: http://inventors.about.com/library/inventors/blalexanderson.htm

[5] Chen, X., Xie, Z.X., and & Zheng, L. (2009), RFID-based manufacturing execution system for intelligent operations", Industrial Engineering and Engineering Management, 2009. IE&EM '09. 16th International Conference on, pp: 36-46

[6] Huang, G. Yuan, G., and & Li, J. (2010), Developing real-time manufacturing execution system for automobile assembly factory, Intelligent Control and Information Processing (ICICIP), pp: 72-84

[7] He, W., Tan, E., Lee, E., and & Li, T. (2009), A solution for integrated track and trace in supply chain based on RFID & GPS, IEEE ETFA 2009 Conference on Emerging Technologies & Factory Automation, 2009. pp: 1-6

[8] Willhite, J. (2004), Implementing the principles of lean manufacturing at Semicon Associates Samarium Cobalt Magnet Facility, IVEC 200 - Fifth IEEE International on Vacuum Electronics Conference, 2004, pp: 104-105

[9] Tharstern. http://www.tharstern.com Accessed 19/9/2011.

 ISBN: 978-1-61208-166-3

Cross-Layer Analysis and Performance Evaluation of Cognitive Radio Networks

Yakim Y. Mihov
Dept. of Telecommunications Networks
Technical University of Sofia
Sofia, Bulgaria
e-mail: yakim_mihov@abv.bg

Abstract—**This paper investigates the traffic capacity and the quality of service provisioning in cognitive radio networks used as secondary networks for dynamic spectrum access in accordance with the hierarchical spectrum overlay approach. An analytical model for cross-layer performance analysis of secondary cognitive radio networks is developed. New performance measures for the interference experienced by the primary and the secondary users are proposed. A novel approach for evaluation of the call dropping probability of the secondary users is suggested.**

Keywords-cognitive radio; cross-layer analysis; dynamic spectrum access; quality of service; traffic capacity

I. INTRODUCTION

Cognitive radio (CR) is the key enabling technology for dynamic spectrum access (DSA) [1]. DSA is a new paradigm for spectrum regulation which is expected to solve the problem with the inefficient spectrum use caused by the current static command-and-control approach for spectrum regulation (see [2] and the references therein). Radio spectrum is a scarce and precious resource and the spectrum demands grow increasingly due to newly emerging wireless services and applications. Therefore, efficient spectrum utilization becomes a matter of great importance.

Hierarchical spectrum overlay is an approach for DSA where secondary (unlicensed or cognitive) users (SUs) are allowed to use opportunistically and on a non-interference basis spectrum resources which have been assigned to primary (licensed or incumbent) users (PUs) but are not currently being used (by any PU). The SUs transmit on momentarily unoccupied spectrum segments without causing harmful interference to the PUs. Because of the dynamic nature of the spectrum available to the SUs, the capacity evaluation and the quality of service (QoS) provisioning for the SUs is a challenging and demanding task.

There are many publications on CR used for DSA in the literature. Issues related to spectrum sensing are investigated in [3]-[9]. Spectrum handover is studied in [10]-[13]. QoS-related issues in CR networks (CRNs) are investigated in [14]-[19]. The capacity of CRNs is considered in [20]-[22].

Due to the nature of CR, cross-layer analysis has to be applied for a comprehensive and exhaustive performance evaluation. There are numerous publications related to cross-layer issues in CRNs (see [23]-[30]). An overview of the general methodology for cross-layer design and some cross-layer optimization schemes and algorithms are presented in [23]. Unified cognitive cross-layer architecture for the next-generation IP-based mobile tactical networks is proposed in [24]. The resource allocation problem in a multiuser orthogonal frequency division multiplexing (OFDM) based CR system concerning the QoS provisioning for both real-time and non-real-time applications is investigated in [26]. Although the papers mentioned above provide important results, they do not present a thorough CRN performance evaluation encompassing jointly the capacity, the QoS provisioning, and some specific CR mechanisms, such as spectrum sensing and spectrum handover.

In this paper, a general and comprehensive cross-layer analytical model for thorough performance evaluation of CRNs is developed. It jointly considers the CR throughput and capacity, the CR QoS provisioning, namely the SU call dropping probability and the maximum tolerable transmission delay in the CRN, and the spectrum sensing and spectrum handover mechanisms. To the best knowledge of the author, the present paper is the first in the literature to propose and apply such a model.

The rest of the paper is organized as follows. The novel cross-layer model is presented in Section II, followed by numerical results in Section III. Section IV concludes this paper.

II. THE ANALYTICAL CROSS-LAYER MODEL

In the model, each SU is assumed to use one and the same transceiver for spectrum sensing and for transmission or reception. Spectrum sensing is performed periodically in compliance with predetermined quiet periods (QPs) during which all SUs stop transmitting to sense PU channels.

In general, physical layer spectrum sensing for PU transmitter detection can be based on energy detection, matched filter detection, and cyclostationary feature detection [3], [4]. The latter two approaches outperform the energy-based detection but require some prior knowledge about the PU signals which may not always be readily available. In order to preserve the generality and the wide applicability of the proposed model, energy-based spectrum sensing is considered and assumed to be applied.

Spectrum sensing may be cooperative or non-cooperative [4], [5]. In general, the former outperforms the latter. Cooperative spectrum sensing has already been exhaustively investigated (see [4], [5], [7] and [8]) and its advantages over non-cooperative spectrum sensing will not be discussed herein. Since under certain conditions (e.g., if only one SU operates on a given frequency band) cooperative spectrum sensing may not be possible, non-cooperative spectrum

 ISBN: 978-1-61208-166-3

sensing is assumed in order to develop a general and widely applicable framework for cross-layer analysis.

Energy-based spectrum sensing is assumed to be performed with the optimal sensing threshold, i.e. the probability for misdetection is equal to the probability for false alarm:

$$1 - p_d = p_f = p_e, \tag{1}$$

where p_d is the probability for detection, p_f is the probability for false alarm, and p_e is the probability for detection error.

Under these conditions, the probability for detection error can be expressed in terms of the Q-function [3]:

$$p_e = \mathrm{Q}\left(\sqrt{N_B}\,\frac{SNR}{1+\sqrt{(\alpha-1)SNR^2+SNR+1}}\right), \tag{2}$$

where SNR is signal-to-noise ratio (SNR) of the PU signal, α is an intrinsic PU signal parameter that relates to its randomness ($1 \le \alpha \le 2$; $\alpha=1$ for constant amplitude signals, e.g. BPSK, QPSK, and $\alpha=2$ for complex Gaussian signals), and N_B is the buffer size expressed as a number of samples.

According to the Nyquist-Shannon sampling theorem, we have:

$$N_B = 2BW\tau, \tag{3}$$

where τ is the spectrum sensing duration for one PU channel and BW is the bandwidth of a PU channel.

Substituting (3) into (2), τ can be obtained for given p_e, SNR, BW, and α.

Let us denote with T_{ss} the total duration of the spectrum sensing procedure for a SU during one QP and with r the number of observed (sensed) PU channels. Then, we have:

$$T_{ss} = \sum_{i=1}^{r} \tau_i, \tag{4}$$

where τ_i is the duration of the spectrum sensing for the i^{th} observed PU channel.

It should be noted that if the number of PU channels n in the system is relatively large, it is unreasonable for a SU to sense all the PU channels. Therefore, it can be assumed that the following relation holds true:

$$r << n. \tag{5}$$

Let us denote with T_p the duration of the spectrum sensing period. For simplicity, T_{ss} is assumed to be equal to the duration of the QPs. Consequently, the nominal SU transmission time t within one spectrum sensing period is:

$$t = T_p - T_{ss}. \tag{6}$$

It should be noted that due to misdetections, false detections, and the PU activity, the mean effective SU transmission time T_{eff} within one spectrum sensing period is actually less than the nominal transmission time t.

Let us denote with T_{int} the mean interference duration within one spectrum sensing period due to simultaneous PU and SU transmissions on the same PU channel. The cognitive medium access control (MAC) protocol of the CRN is assumed to provide perfect spectrum sharing among SUs, so that no interference occurs due to overlapping SU transmissions.

The proposed approach for evaluation of T_{int} and T_{eff} is similar to that in [4] but unlike the method used in [4] where a single-channel primary system is considered, the derivation of T_{int} and T_{eff} presented in this paper is generalized in order to be applicable to a multichannel primary system.

The PU call arrival and service processes are modeled by Poisson random processes with rates λ_p and μ_p, respectively. Hence, the offered PU traffic is:

$$A_p = \frac{\lambda_p}{\mu_p}, \tag{7}$$

and the PU call blocking probability B_p can be evaluated according to the Erlang loss formula:

$$B_p = E_n(A_p) = \frac{\dfrac{A_p^n}{n!}}{\displaystyle\sum_{i=0}^{n}\frac{A_p^i}{i!}}. \tag{8}$$

The carried PU traffic per one PU channel, i.e. the mean PU channel utilization, is:

$$\eta = \frac{A_p\left(1-B_p\right)}{n}. \tag{9}$$

The mean number of available (unoccupied by PU transmissions) channels to the CRN is:

$$a = floor\left[n - A_p\left(1-B_p\right)\right], \tag{10}$$

where *floor* is a function that rounds its argument to the nearest integer towards minus infinity. It should be noted that when $n > 1$ (a multichannel primary network is considered) and the PU network is not overloaded with PU traffic, the relation $a > 0$ always holds true; otherwise, if the PU network is overloaded or congested by PU calls, the use of CR for DSA is obviously unreasonable.

Taking into account the negative exponential distributions of the inter-arrival time and the service time of PU calls, η, a, t, and the possibilities for misdetection and false detection, T_{int} and T_{eff} can be derived as follows:

 ISBN: 978-1-61208-166-3

$$T_{int} = \eta(1-p_d)\left[te^{-\mu_p t} + \eta t\left(1-e^{-\mu_p t}\right)\right] + \\ +(1-\eta)(1-p_f)\frac{\left(1-e^{-\lambda_p t}\right)}{a}\eta t, \quad (11)$$

where the first addend in (11) refers to the case in which a SU misdetects an occupied PU channel, starts transmitting on that channel and the PU call does not end until the next spectrum sensing period or ends before the next spectrum sensing period; the second addend in (11) refers to the case in which a SU starts transmitting on an available channel and later a new PU call arrives and occupies that channel;

and

$$T_{eff} = (1-\eta)(1-p_f)\left[\begin{array}{l} te^{-\lambda_p t} + \left(1-e^{-\lambda_p t}\right)\left(1-\frac{1}{a}\right)t + \\ +\frac{\left(1-e^{-\lambda_p t}\right)}{a}(1-\eta)t \end{array}\right] + \\ +\eta(1-p_d)\left(1-e^{-\mu_p t}\right)(1-\eta)t, \quad (12)$$

where the first addend in (12) refers to the case in which a SU starts transmitting on an available channel and no PU calls arrive until the next spectrum sensing period or a new PU call arrives before the next spectrum sensing period but occupies another available channel or occupies the same channel; the second addend in (12) refers to the case in which a SU misdetects an occupied PU channel, starts transmitting on that channel and the PU call ends before the next spectrum sensing period.

In (11) and (12), ηt is assumed to be the mean interference duration when a SU starts transmitting on an available channel and a new PU call occupies that channel before the beginning of the next QP or when a SU misdetects and starts transmitting on an occupied channel and the ongoing PU call ends before the next QP.

Now the CRN throughput and capacity can easily be derived. The normalized mean effective transmission time ρ of a SU is:

$$\rho = \frac{T_{eff}}{T_p}. \quad (13)$$

The CR is assumed to use non-contiguous OFDM (NC-OFDM) waveform. NC-OFDM allows the CR to deactivate (null) the subcarriers overlapping with any PU transmission and thus to adjust the spectrum of its signal to fit into the available frequency gaps [17]. Furthermore, CR with NC-OFDM can be deployed in any primary network irrespective of its channelization scheme and even if fixed channelization is not supported, which facilitates the wide applicability of the model developed in this paper. It has already been assumed that perfect spectrum sharing is provided by the cognitive MAC protocol. Based on the above-mentioned assumptions, the mean throughput of the CRN C (bit/s) can be obtained:

$$C = n\varepsilon BW\rho, \quad (14)$$

where ε is the mean spectral efficiency (bit/s/Hz) of the SUs.

The CRN can be considered as a serving system with m channels:

$$m = floor\left[\frac{C}{c}\right], \quad (15)$$

where c (bit/s) is the necessary mean rate for a SU call to be served.

The traffic capacity of the CRN can be determined according to the Erlang loss formula:

$$B_s = E_m(A_s) = \frac{\frac{A_s^m}{m!}}{\sum_{i=0}^{m}\frac{A_s^i}{i!}}, \quad (16)$$

where A_s is the offered SU traffic and B_s is the SU call blocking probability.

In order to evaluate the interference experienced by the PUs and to guarantee that the CRN will not degrade the performance of the primary network, the following constraints have to be satisfied:

$$t \le T_{int}^{max}, \quad (17)$$

and

$$\gamma = \frac{T_{int}}{T_p} \le \gamma_{max}, \quad (18)$$

where T_{int}^{max} is the maximum tolerable interference duration in the PU network and γ_{max} is the maximum tolerable normalized mean interference duration. In (18), γ is introduced as a new precise performance measure for the interference experienced by the PUs.

In order to evaluate the interference experienced by the SUs, another new performance measure δ is proposed which is implicitly relevant to the CR QoS provisioning:

$$\delta = \frac{T_{int}}{T_{eff} + T_{int}}. \quad (19)$$

Next, the SU QoS provisioning is analyzed. A novel approach for evaluation of the SU call dropping probability which incorporates the maximum tolerable transmission delay in the CRN is proposed. It is particularly applicable to the system model considered in this paper.

 ISBN: 978-1-61208-166-3

It can be assumed without loss of generality that SU call dropping occurs only if SU connection failure occurs. SU connection failure occurs when a SU is unable to transmit during several consecutive spectrum sensing periods and the maximum tolerable transmission delay D in the CRN is exceeded. It should be noted that D is a QoS-dependent parameter and may vary according to the type of application.

Let us denote with q the minimum number of consecutive spectrum sensing periods for which SU connection failure occurs if a SU does not have a successful transmission during all of these periods. Therefore, we have:

$$q = floor\left[\frac{D}{T_p}\right] + 1. \quad (20)$$

A SU is unable to transmit during a spectrum sensing period either due to misdetection and continuous interference during the nominal transmission time t, or due to detections of PU transmissions or false alarms on all of the observed channels. No transmission opportunities are missed due to unsuccessful spectrum handovers since the cognitive MAC protocol is assumed to provide perfect spectrum handover procedure. Consequently, taking into account the above considerations and (5), the SU connection failure probability p_{cf} is obtained:

$$p_{cf} = \sum_{i=0}^{q} \binom{q}{i} \left[\eta\left(1-p_d\right)e^{-\mu_p t}\right]^i \left[\eta p_d + \left(1-\eta\right)p_f\right]^{r(q-i)}. \quad (21)$$

III. NUMERICAL RESULTS

In this section, some numerical results (Fig. 1 – Fig. 6) obtained using the analytical model described above are presented and analyzed. For simplicity, but without loss of generality, it has been assumed that the SNR of the PU signals is equal on all of the n PU channels and that the duration of the QPs is equal to the duration of the spectrum sensing procedure T_{ss}.

Fig. 1 - Fig. 3 show the SU transmission efficiency ρ, the interference experienced by the PUs γ and by the SUs δ, and the SU call dropping probability, i.e. the SU connection failure probability p_{cf}, as a function of the spectrum sensing period T_p for different number of observed channels r. When T_p increases, ρ, γ, δ, and p_{cf} also increase. As r increases, ρ, and p_{cf} decrease but the change in γ and δ is negligible. Moreover, when $T_p >> \tau$ and r is relatively small (as it has already been assumed in (5)), a change in r slightly affects ρ. Therefore, in this case, T_p has a dominant effect on both the CR throughput and on the interference, whereas r has a dominant effect only on the SU call dropping probability and affects the CR throughput to a significantly lesser extent in comparison with T_p.

New performance measures γ and δ for evaluation of the interference experienced by the PUs and by the SUs have been proposed. In order to guarantee that the CRN operates on a non-interference basis both (17) and (18) have to be satisfied. When ρ is high and δ is relatively low, the CR operates efficiently under low interference. If δ is relatively high, the CR operates in a high interference environment either because of improper configuration of the spectrum sensing mechanism or because of unfavorable conditions for DSA, e.g. very high PU traffic load.

Fig. 1 and Fig. 3 also show that if r increases, ρ and p_{cf} both decrease, and vice versa. Consequently, by increasing r, it is possible to achieve more reliable communications in the CRN at the price of reduced throughput and capacity.

Fig. 4 illustrates that the SU call dropping probability, i.e. the SU connection failure probability p_{cf}, decreases if the maximum tolerable transmission delay D in the CRN increases. As r increases, p_{cf} also decreases. Since D depends on the QoS requirements of the provided service, it can be concluded that the CR is particularly suitable for delivering of non-real-time delay-tolerant services.

Fig. 5 shows the CR traffic capacity A_s as a function of the signal-to-noise ratio SNR of the PU signals. As SNR increases, the time required for spectrum sensing decreases. Therefore, the nominal transmission time t, and thus A_s, both increase. However, in order to satisfy the interference constraints (17) and (18), it may be necessary to reduce t by decreasing T_p. Due to the strong dependence of A_s on SNR, PU channels with higher SNR should be preferred for spectrum sensing.

Fig. 6 shows the CR traffic capacity A_s as a function of the offered PU traffic A_p. As A_p increases, spectrum sensing has to be performed more frequently in order to satisfy the interference constraints imposed by the primary network, which means that T_p, and thus ρ and A_s, both decrease. The interplay of PU traffic and SU traffic should always be carefully considered. The deployment of CRNs for DSA is reasonable only if the primary network is sufficiently underutilized.

The presented numerical results in this section lead to the general conclusion that many cross-layer interdependencies, such as those analyzed herein, should be considered in order to achieve optimal CRN performance.

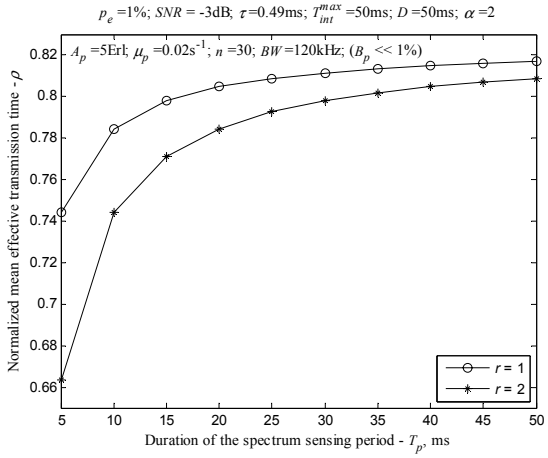


Figure 1. Transmission efficiency versus the spectrum sensing period for different number of observed channels.

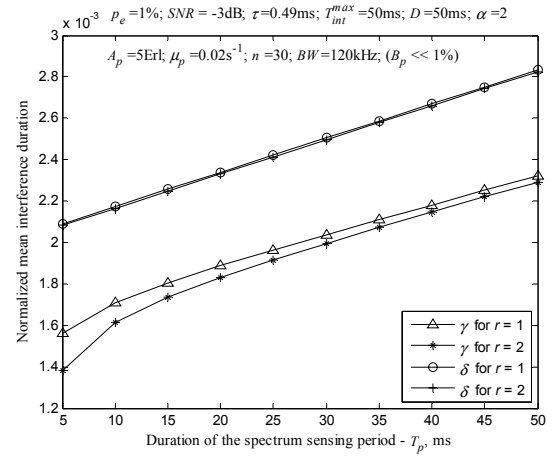


Figure 2. Interference experienced by the PUs (γ) and by the SUs (δ) versus the spectrum sensing period for different number of observed channels.

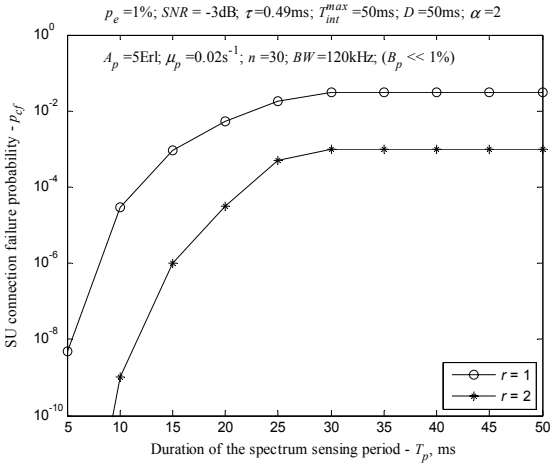


Figure 3. SU call dropping probability versus the spectrum sensing period for different number of observed channels.

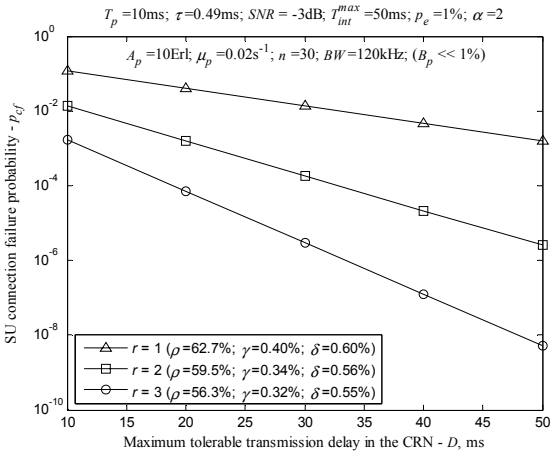


Figure 4. SU call dropping probability versus the maximum allowable transmission delay in the CRN for different number of observed channels.

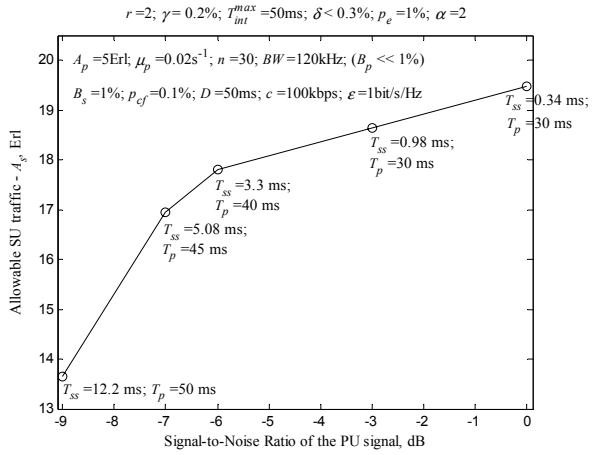


Figure 5. Cognitive traffic capacity for given QoS constraints versus the SNR of the PU signals.

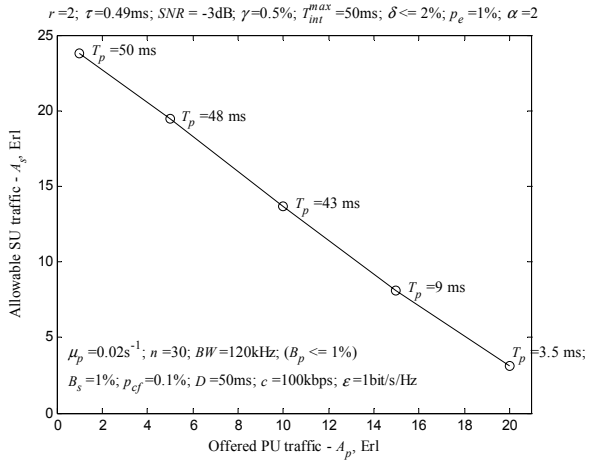


Figure 6. Cognitive traffic capacity for given QoS constraints versus the offered PU traffic.

IV. CONCLUSION AND FUTURE WORK

In this paper, an analytical model for cross-layer analysis and performance evaluation of CRNs is developed. New performance measures, namely γ and δ, for evaluation of the interference experienced by the PUs and by the SUs are suggested. A novel approach for evaluation of the SU call dropping probability is proposed. Various cross-layer interdependencies are investigated and analyzed.

The model is generic and comprehensive, which determines its wide applicability and theoretical significance. It can be applied to both infrastructure and ad hoc CRNs. Moreover, it can be used as a general cross-layer design framework which could be elaborated, modified, or adapted to meet specific design characteristics of a particular CRN.

The analytical model presented in this paper could further be extended to consider cooperative spectrum sensing, imperfect spectrum handover, and imperfect spectrum sharing. The spectrum sensing method could also be modified and matched filter detection or cyclostationary feature detection could be considered.

 ISBN: 978-1-61208-166-3

For future research work, the author plans to extend the cross-layer model developed herein in order to investigate various cross-layer optimization issues and the application of machine learning for enhancing the overall CR performance.

ACKNOWLEDGMENT

This research was financially supported by the author.

REFERENCES

[1] IEEE Std. 1900.1-2008, "IEEE standard definitions and concepts for dynamic spectrum access: Terminology relating to emerging wireless networks, system functionality, and spectrum management," pp. c1-48, September 2008.

[2] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," IEEE Signal Processing Magazine, vol. 24, no. 3, pp. 79-89, May 2007.

[3] H. Tang, "Some physical layer issues of wide-band cognitive radio systems," 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pp. 151-159, Baltimore, MD, USA, 8-11 Nov. 2005.

[4] W.-Y. Lee and I. F. Akyildiz, "Optimal spectrum sensing framework for cognitive radio networks," IEEE Transactions on Wireless Communications, vol. 7, no.10, pp. 3845-3857, 28 October 2008.

[5] A. A. El-Saleh, M. Ismail and M. A. M. Ali, "Optimizing spectrum sensing parameters for local and cooperative cognitive radios," 11th International Conference on Advanced Communication Technology (ICACT), pp. 1810-1815, Gangwon-Do, South Korea, 15-18 Feb. 2009.

[6] T. Yucek and H. Arslan, "Spectrum characterization for opportunistic cognitive radio systems," IEEE Military Communications Conference (MILCOM), pp. 1-6, Washington DC, USA, 23-25 October 2006.

[7] S. Xie, Y. Liu, Y. Zhang and R. Yu, "A parallel cooperative spectrum sensing in cognitive radio networks," IEEE Trans. on Vehicular Techn., vol. 59, no. 8, pp. 4079-4092, Oct. 2010.

[8] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), pp. 131-136, Baltimore, MD, USA, 8-11 Nov. 2005.

[9] D.-J. Lee and M.-S. Jang, "Optimal spectrum sensing time considering spectrum handoff due to false alarms in cognitive radio networks," IEEE Communications Letters, vol. 13, no. 2, pp. 899-901, Dec. 2009.

[10] L.-C. Wang and C. Anderson, "On the performance of spectrum handoff for link maintenance in cognitive radio," 3rd International Symposium on Wireless Pervasive Computing (ISWPC), pp. 670-674, Santorini, Greece, May 2008.

[11] O. Jo and D.-H. Cho, "Seamless spectrum handover considering differential path-loss in cognitive radio systems," IEEE Communications Letters, vol. 13, no. 3, pp. 190-192, March 2009.

[12] O. Jo, H. H. Choi and D.-H. Cho, "Seamless spectrum handover improving cell outage in cognitive radio systems," 4th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), pp. 1-6, Hannover, Germany, June 2009.

[13] D. Lu, X. Huang, C. Liu and J. Fan, "Adaptive power control based spectrum handover for cognitive radio networks," IEEE Wireless Communications and Networking Conference (WCNC), pp. 1618-1622, Sydney, 18-21 April 2010.

[14] B. Canberk, I. F. Akyildiz and S. Oktug, "A QoS-aware framework for available spectrum characterization and decision in cognitive radio networks," IEEE 21st International Symposium on Personal Indoor and Mobile Radio Commun. (PIMRC), pp. 1533-1538, Istanbul, Sept. 2010.

[15] Q. Xin and J. Xiang, "Joint QoS-aware admission control, channel assignment, and power allocation for cognitive radio cellular networks," IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (MASS), pp. 294-303, Macau, 12-15 Oct. 2009.

[16] T. Wysocki and A. Jamalipour, "Mean-variance based QoS management in cognitive radio," IEEE Trans. on Wireless Commun., vol. 9, no. 10, pp. 3281-3289, October 2010.

[17] J. W. Mwangoka, K. B. Letaief and Z. Cao, "Robust end-to-end QoS maintenance in non-contiguous OFDM based cognitive radios," IEEE International Conference on Communications (ICC), pp. 2905-2909, Beijing, May 2008.

[18] S.-W. Liu, S.-L. Wu and J.-L. Chen, "Adaptive cross-layer QoS mechanism for cognitive network applications," 12th International Conference on Advanced Commun. Techn. (ICACT), pp. 1389-1393, Gangwon-Do, Korea, Feb. 2010.

[19] A. Alshamrani, X. S. Shen and L.-L. Xie, "QoS provisioning for heterogeneous services in cooperative cognitive radio networks," IEEE Journal on Selected Areas in Communications, vol. 29, no. 4, pp. 819-830, April 2011.

[20] H. Cho and J. Andrews, "Upper bound on the capacity of cognitive radio without cooperation," IEEE Transactions on Wireless Commun., vol. 8, no. 9, pp. 4380-4385, Sept. 2009.

[21] Z. Rezki and M.-S. Alouini, "On the capacity of cognitive radio under limited channel state information," 7th International Symp. on Wireless Communication Systems (ISWCS), pp. 1066-1070, York, UK, 19-22 Sept. 2010.

[22] Y. Kim and G. de Veciana, "Joint network capacity region for cognitive networks heterogeneous environments and RF-environment awareness," IEEE Journal on Selected Areas in Communications, vol. 29, no. 2, pp. 407-420, February 2011.

[23] Y. Liu and Q. Zhou, "State of the art in cross-layer design for cognitive radio wireless networks," International Symposium on Intelligent Ubiquitous Computing and Education, pp. 366-369, Chengdu, China, May 2009.

[24] S. Ci and J. Sonnenberg, "A cognitive cross-layer architecture for next-generation tactical networks," IEEE Military Communications Conference (MILCOM), pp. 1-6, Orlando, FL, USA, 29-31 Oct. 2007.

[25] Y. Peng, J. Peng, X. Zheng, Z. Liu and H. Long, "A cross-layer architecture for OFDM-based cognitive radio network," pp. 129-133, World Congress on Software Engineering (WCSE), Xiamen, China, 19-21 May 2009.

[26] Y. Zhang and C. Leung, "Cross-layer resource allocation for mixed services in multiuser OFDM-based cognitive radio systems," IEEE Trans. on Vehicular Technology, vol. 58, no. 8, pp. 4605-4619, October 2009.

[27] H. Su and X. Zhang, "Cross-layer based opportunistic MAC protocols for QoS provisioning over cognitive radio wireless networks," IEEE Journal on Selected Areas in Communications, vol. 26, no. 1, pp. 118-129, January 2008.

[28] S. Ali and F. R. Yu, "Cross-layer QoS provisioning for multimedia transmissions in cognitive radio networks," IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-5, Budapest, 5-8 April 2009.

[29] N. Baldo and M. Zorzi, "Fuzzy logic for cross-layer optimization in cognitive radio networks," 4th IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, Jan. 2007.

[30] H. Peng and T. Fujii, "Joint cross-layer resource allocation and interference avoidance with QoS support for multiuser cognitive radio systems," 7th International Symposium on Wireless Communication Systems (ISWCS), pp. 626-630, York, UK, 19-22 September 2010.

 ISBN: 978-1-61208-166-3

Performance Analysis of Coordinated Base Stations in Multi-Cellular Network Using Multistream Transmission and Different Size Cells

Tetsuki Taniguchi
Department of Communication Engineering and Informatics

Yoshio Karasawa
Department of Communication Engineering and Informatics

Nobuo Nakajima
Department of Informatics

Advanced Wireless Communication research Center (AWCC)
The University of Electro-Communications (UEC), Chofu, Tokyo 182-8585, Japan
{taniguch,karasawa}@ee.uec.ac.jp,n.nakajima@hc.uec.ac.jp

***Abstract*—As a promising approach to mitigate the performance degradation of multi-cellular network in cell-edge region, Base Station Cooperation (BSC) is collecting attentions. This paper investigates "how much" BSC using practical algorithm could improves the performance of the system, when the shape and size of cells are flexibly changed based on BS location and inter BS-UT channel condition. Here, we consider multistream transmission assuming that BSs and User Terminals (UTs) are all equipped with multiantenna. In multistream case, interferences arriving from surrounding cells consist of larger number of data sequences than single stream case, hence first, we investigate the nature of inter-cell interference. Next, the performance gain of BSC is evaluated using five types of algorithms with and without BSC through computer simulations. The results show that BSC achieves about three times larger capacity compared to cooperation less scheme.**

***Keywords*-Coordinated Multi-Point (CoMP) transmission, Multiple Input Multiple Output (MIMO), cellular network, spatial multiplexing.**

I. INTRODUCTION

It is well known that the performance of multi-cellular network is degraded in the cell-edge, because the desired signal from the target Base Station (BS) is weakened due to the relatively large attenuation, while the interferences from adjacent cells become stronger. As a mitigation strategy of this problem, Base Station Cooperation (BSC) is collecting attentions (overview of BSC is found, for example, in [1], [2]) (cooperation is considered also in uplink [3], [4]). By sharing information among multiple BS, increment of throughput in the region other than cell edge could be also anticipated. There are many works presenting transmission schemes and resource allocations for BSC, but conventional works mainly focused on the cases of regular cell geometry, and the performance improvement by BSC has not been quantitatively evaluated under practical communication strategy.

This paper investigates the effect of BSC under multistream transmission assuming that BSs and User Terminals (UTs) are all equipped with multiantenna, and the shape and size of cells are flexibly changed based on BS location and inter BS-UT channel condition. In case of multistream transmission, the interferences contains more number of data sequences compared single stream schemes. Therefore, to investigate the behavior of interferences and to find adequate cluster size (number of cooperative BSs), first, the interference analysis is carried out. Then, we move onto the main topic of this study, namely, evaluate "how much" the performance is improved by BSC based on five typical algorithms with and without BSC through computer simulations. Those results are useful to know how the effect of BSC changes if the multistream scheme is used utilizing spatial multiplexing ability of Multiple Input Multiple Output (MIMO) system.

The organization of the rest of this paper is as follows: after Section II presenting state of art, namely, past works and the novelty of this paper, Section III describes the system model considered in this study and design algorithms. In Section IV, the effectiveness of BSC under given situation is verified through computer simulations. Section V gives conclusion and future works of this study.

II. PAST WORKS AND NOVELTY OF THIS STUDY

BSC problems contain design of transmission scheme, resource allocation [5], system design (e.g., clustering strategy [6]), and analysis from propagation aspect [7], [8]. But those works mainly considering "how to" achieve BSC, and it has not well been investigated "how much" performance improvement is anticipated by practical BSC algorithms (information theoretic analysis based on the capacity is considered using 3-cell model in [9], but it is for a single antenna case).

Hence, in this paper, authors focus on performance analysis of BSC using linear processing (For multiuser MIMO including multi-cellular network, nonlinear methods represented by Dirty Paper Coding (DPC) are also known (e.g., [10]). But those methods are accompanied by demand of complicated power control problem, so here we limit our interest in linear processing approaches.) based on MIMO communication. In addition, majority of previous works have premised on fixed cell geometry, the most typical is the hexagonal one. But BSs might not be located in the cell

 ISBN: 978-1-61208-166-3

center because of physical (there's not adequate space for BS setting) or social (BS setting is not permitted) reason, and in this case, the regular cell shape does not fit in with the reality.

In authors' previous work [11], we carried out BSC assessment in the codition of irregular cell geometry derived from Voronoi diagram which changes the cell shape and size based on BS location, but there, only the single stream transmission has been considered. This paper extends assessment to multistream transmission fully utilizing the fact that BSs and UTs are all equipped with multiantenna, and to the case where the shape and size of cells are flexibly determined based on not only BS location but also inter-BS-UT channel condition.

III. System Model and Design Algorithms

In this section, the model of cellular system and its design algorithms are shortly described.

A. System Model

In the cellular system considered here (imagine cell geometry like Fig. 1), one BS exists in each cell, and it communicates one active user chosen from UTs (both sides are equipped with multiantenna). If different frequency band is used in all the cells, no interference occurs among cells, but frequency efficiency becomes quite low. Hence members of a group consisting of some cells use common frequency, and it brings the problem of inter-cell interference. The interference cancellation is possible utilizing the multiantenna processing, but if BS are connected through backhaul link, they can share information (e.g., channel and data), which enables BSC to derive a higher total performance. This effect is larger in the cell edge where the target signal is attenuated and interferences become relatively strong. The rest of this subsection provides a model suitable for the analysis of BSC under practical conditions.

In this study, BS location is nonuniformly allocated, and their location is expressed by the displacement from the conventional hexagonal center. The conventional cells are shown by green dashed line in Fig. 1: they are numbered anti-clockwise from the inside to the outside (Cell n corresponds to User n). Actual BS location is moved onto a circle with radius r_b and rotation angle θ from the hexagon center, and then cell borders are given as Voronoi diagram as shown by solid line in Fig. 1. This geometry means the domain where the maximum mean power connection is derived against the BS inside of the same cell, and used as a guideline for giving the concept of cell edge. The cell layers are defined as in Table I, where Cell 0 (= Layer 0) is surrounded by 6 cells, and they are further embraced by 12 cells, and outer layers are given in a similar manner. The cell edge is defined as in Fig. 2 ($r_c = 1 - d'_{m,n}/d_{m,n}$ means cell edge ratio, which is the width of shaded region against inter BS distance $d_{m,n}$, and for the simplicity, cell edge is defined

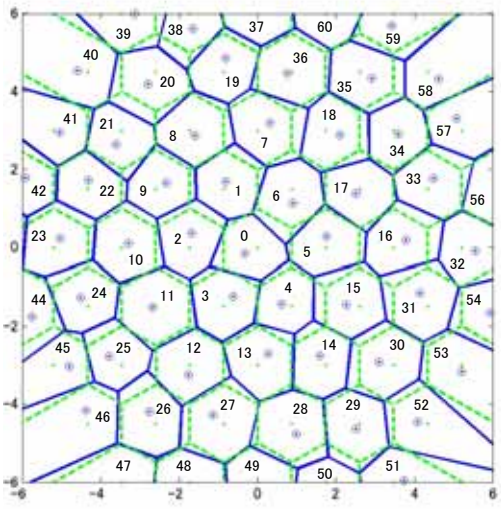


Figure 1. Example of multi-cell geometry.

TABLE I
Layer Construction

	Cell Numbers
Layer 0	0
Layer 1	1, 2, $\cdots$, 6
Layer 2	7, 8, $\cdots$, 18
Layer 3	19, 20, $\cdots$, 36
Layer 4	37, 38, $\cdots$, 60

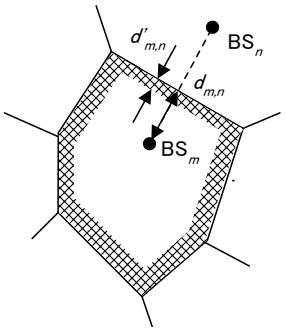


Figure 2. Definition of cell edge.

even if $d_{m,n}$ is small, namely, the UT is located relatively near the target BS), and one active UT can exist in this area for each cell. All the BSs and UTs are equipped with N_b and N_u antennas respectively, and BS of User m (BS$_m$) transmits L data streams $\{s_{m,\ell};\ \ell = 0,\ \cdots,\ L-1\}$ using weight set $\{\boldsymbol{w}_{b,m,\ell};\ \ell = 0,\ \cdots,\ L-1\}$ to the corresponding UT (UT$_m$), and UT$_m$ produces the output signals by using weight set $\{\boldsymbol{w}_{u,m,\ell};\ \ell = 0,\ \cdots,\ L-1\}$ (By choosing adequate weights in UTs, the amplitude and phase of the signal after passing the channel is adjusted so that the power of the desired component is maximized against those of noise plus interferences through the work as a spatial filter. A similar effect could be anticipated also by weights in BS side.). The MIMO channel between BS$_m$ and UT$_n$ is given by $N_u \times N_b$ matrix $H_{n,m}$.

B. Design Algorithms

For the performance comparison, following five algorithms are considered (they are not novel approaches, but remark that our aim in this paper is not to develop new algorithms, but the measurement of BSC effect). The definition

 ISBN: 978-1-61208-166-3

of BSC in this paper is cooperative transmission utilizing share of Channel State Information (CSI) $\mathcal{H} = \{H_{n,m}\}$ and/or data signal $\{s_{m,\ell}\}$ among all BSs, and in this sense, among Case $1 \sim 5$, Case 4 and Case 5 are included in BSC method. The algorithms are briefly described below.

Case 1 and Case 2 (w/o interference cancellation)

Transmit and receive weights of User m are designed by Singular Value Decomposition (SVD) of channel matrix $H_{m,m}$ (utilization of left and right singular value vectors corresponding the first L largest singular values) [12] not considering interference cancellation. In Case 1, interferences from other cell are ignored in the simulation as if M parallel MIMO system exist, which is unrealizable scenario but used as an upper bound in case without BSC. On the contrary, Case 2 is fully exposed to interferences from $M-1$ users, and its capacity is used as a lower bound.

Case 3 (with interference cancellation, w/o BSC)

Transmit weights are designed by SVD as Case 1 and Case 2. But receiver weights are designed to achieve interference cancellation by beamforming using Minimum Mean Square Error (MMSE) criterion. Here, for the m-th user, the ratio of $|\boldsymbol{w}_{u,m,\ell}^H H_{m,m} \boldsymbol{w}_{b,m,\ell}|^2 P_{S,m}$ is maximized against $\sum_{(n,k)\in\mathcal{I}(m,\ell)} \boldsymbol{w}_{u,m,k}^H H_{m,n} \boldsymbol{w}_{b,n,k} \boldsymbol{w}_{b,n,k}^H H_{m,n} \boldsymbol{w}_{u,m,k} P_{S,n}$, where $\mathcal{I}(m,\ell) = \{(n,k);\ n \neq m\} \cup \{(m,k);\ k \neq \ell\}$. The solution is derived by conventional way of MMSE solution [13].

Case 4 (BSC with CSI sharing) [11]

The receiver weights are first designed by SVD as Case 1 and Case 2. Then utilizing the share of CSI, namely, set $\{H_{n,m}\}$ consisting of $|\mathcal{H}| = M^2$ matrices, transmit weights for the ℓ-th stream of User m are designed to eliminate the interferences $\{H_{n,m}\boldsymbol{w}_{u,n,k};\ (n,k) \in \mathcal{I}(m,\ell)\}$ to other cells and other streams using Zero Forcing (ZF) method. By designing receiver weights first, degrees of freedom required for ZF become $LM - 1$.

Case 5 (BSC with CSI and data sharing)

In this case, utilizing the share of data among all users, a virtual array with MN_b antenna elements could be configurated. Transmit and receive weights are designed by Block Diagonalization (BD) [14]. While large performance improvement by the increment of degrees of freedom could be anticipated, the traffic in backhaul is significantly increased from Case 4 for the data sharing.

The energy is allocated to each stream by water filling [13], and in this process, some streams with negative energy are excluded (in this case, streams less than the rank of channel matrix are used).

Other than those algorithms, various design criterion and conditions are presented and we can derive the exact/approximated solution for some of them, but here we adopted practical well known method which is suitable to implement in actual systems. Case 1, 2, 4, and 5 correspond to the optimal solution under certain zero forcing conditions, and Case 3 achieves MMSE optimality in the receiver.

IV. Performance Analysis

In this section, computer simulation are carried out to assess how the effectiveness of BSC changes (or does not change) by adopting multistream transmission. Default simulation conditions are given in Table II.

The evaluation measure of the output signal of total users is sum capacity which is approximated by $C = \sum_m \log_2(1+\Gamma_m)$ using Signal to Interference plus Noise Ratio (SINR) defined by $\Gamma_m = \frac{|\rho_m|^2}{1-|\rho_m|^2}$ for the m-th user, where $\rho_m = \frac{E[\hat{s}_m(k) s_m^*(k)]}{\sqrt{E[|\hat{s}_m(k)|^2] E[|s_m(k)|^2]}}$. On the contrary, noise condition is expressed by Signal to Noise Ratio (SNR) given by $\gamma_m = P_{S,m}/P_{N,m}$ using noise power $P_{N,m}$ of the m-th user. Here, $P_{S,m} = 1$ for all m, and noise power is adjusted so that the SNR at the vertex of original hexagonal cell becomes $\gamma_m = 10 \sim 30$dB (remark that the hexagon vertex is normalized to one since the actual length (order of kilo meter) changes depending on the situation, and in this case, inter-BS distance is $\sqrt{3}$). The (sample) mean SINR and capacity are evaluated by randomly changing the pattern of BS displacement ($r_b \sim U[0, 0.4]$ and $\theta \sim U[0, 2\pi)$) using total 4,000 samples (20 BS positions $\times$ 20 UT positions $\times$ 10 channels).

First, to derive the guideline of system design, the power of interference arriving from outer cells is investigated.

Figure 3 depicts the layer number versus total energy of interferences arriving from the corresponding layer received using the weight corresponding to the first stream (which is the singular vectors belonging to the largest singular value). In each cell, BS ($N_b = 7$) transmits L streams to UT ($N_u = 3$) without interference cancellation (it corresponds to Case 2), where streams $\ell = 1$ and $\ell = 2$ become interferences. The energy in layer zero means that of thermal noise. From this figure, it can be seen that the amount of interference coming from each layer is not so much different between single and multiple stream transmission schemes, since the energy of BS transmission is kept to a constant even though the number of stream is inctreased. The total strength of interference decreases in outer cell though the number of the cell increases, but they are still stronger than that of the thermal noise, which means the importance of the interference cancellation.

As the energy of interferences become large, larger amount of their influence could be reduced by BSC, and in Case 5 they are utilized as sources of the desired signal. The results of interference assessment show the outer 6 cells occupies the significant part of energy, which means even if more than 7 cell have cooperation, its effect is very small

 ISBN: 978-1-61208-166-3

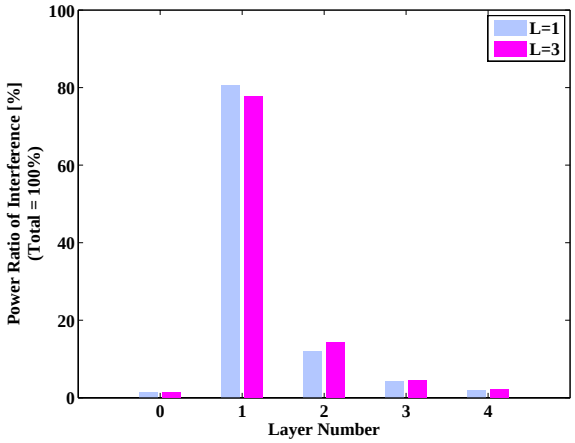
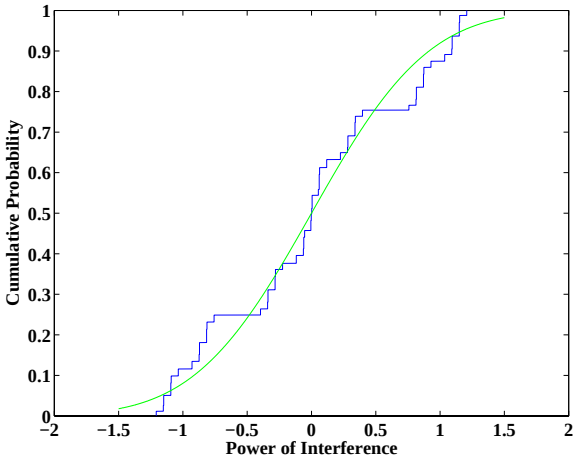


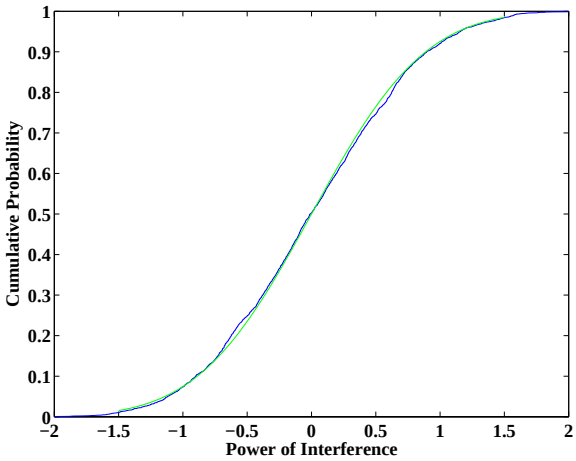
Figure 3. Energy of interferences arriving at Cell 0 from outer cells.

Table II
DEFAULT SIMULATION CONDITIONS.

Number of Cells	$M = 19$ or 61
Number of Cooperation BSs	$M = 7$
Cell Shape	Voronoi Diagram
Size of Henxagon	$d = 1$
BS Position	on a circle with radius r_b
UT Position	Uniform Distribution in Cell Edge
Cell edge ratio	$r_c = 0.8$
BS Displacement	$r_b \in U[0, 0.4]$
(BS,UT) Antenna Number $(N_{b,m}, N_{u,m})$	$(7, 3)$ interference analysis $(14, 2)$ performance comparison
SNR	$\gamma_m = 10 \sim 30$ dB (default : 20dB)
Path Loss Exponent	$\alpha = 3.5$
Shadowing	Log Normal Distribution Standard Deviation $\sigma = 6$
Fading	i.i.d. Quasistatic Rayleigh



(a) BPSK.



(b) QPSK.

Figure 4. Examples of distribution functions of interference in Layer 1 (real part) ($L = 3$).

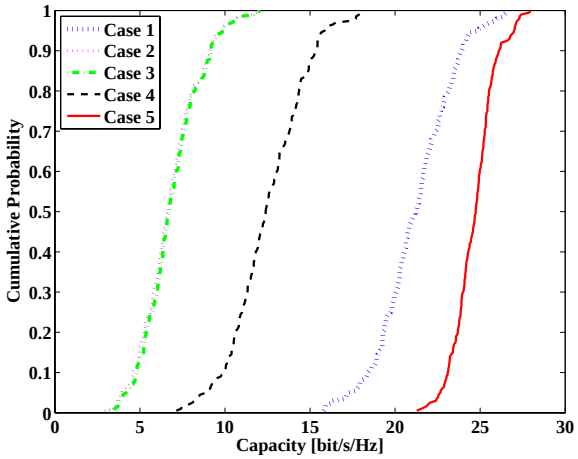
since there's small amount of component which could be utilized for the enhancement of the desired signal. On the other hand, increment of cooperative BS results in larger cost of implementation (backhaul connection) and computation cost, and more than 7 cell cooperation is impractical. So here we consider 7 cell cooperation, namely, those cells use the same frequency band, and the outer cells use different frequency.

Figure 4 plots examples of distribution function of interference when the channel matrix is fixed. In most cases, the distribution could be approximated by normal distribution, though exceptions exist (particularly, for BPSK modulation, we should remark that the Gaussian approximation could not be applied in Layer 1 even in multistream case).

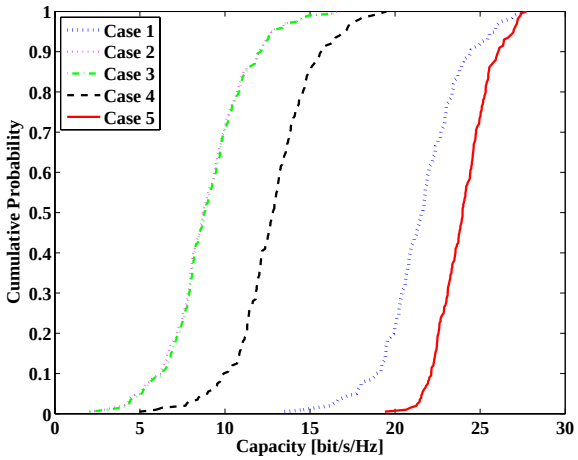
Next, the performance comparison of algorithms (evaluation of BSC effect) is carried out for 7-cell cooperation. If L streams are not realizable for User m in ZF schemes as a result of water filling, the maximum possible number less than L is adopted. Here, two-stream transmission is considered because, to pass L streams for each user, UTs (Case 3) or BSs (Case 4) should have $LM - 1$ antennas, and equipment of array elements which enables more than two stream is impractical (usually, UTs do not have space more than two antennas, hence in our simulation, we assume practical two-antenna UT system). The UT is connected to the BS with the best channel condition (here, the largest channel matrix norm), and if plural UT choose on BS, the one with the largest norm is selected. In the next round, UTs which could not find the pair BS in the first round try again to find their target BS which has the largest channel norm from BSs without pair UT, and repeat this operation until all the UTs find their partner (this procedure defines flexible cell geometry).

Figure 5 depicts the distribution functions of sum capacity of two streams ($L = 2$) for Cell 0 and Cell 6 for (the curves of Case 2 and Case 3 alomost overlap). In both figures, though the BSC only sharing CSI has a limited capacity

 ISBN: 978-1-61208-166-3



(a) User 0.



(b) User 6.

Figure 5. Distribution functions of capacity.

improvement, BSC with data sharing achieves about three times larger capacity than that of Case 3 without BSC, and in addition, its curve has a steeper gradient which means better outage characteristics. The amount of the improvement in Cell 0 surrounded by 6 cells is larger than in border cell (Cell 6), since the origins of interferences change to the sources of the desired signal.

The relation between input SNR and sum capacity is depicted in Fig. 6. While Case 3 without BSC cannot improve the performance because of the residual interference (degrees of freedom in UT are not enough), methods with BSC (Case 4 and Case 5) steadily increase the capacity as SNR becomes higher.

From those results, we can see that BSC is still effective in multistream transmission.

V. Conclusion

This paper has investigated the effect of BSC under multistream transmission assuming that BSs and UTs are all

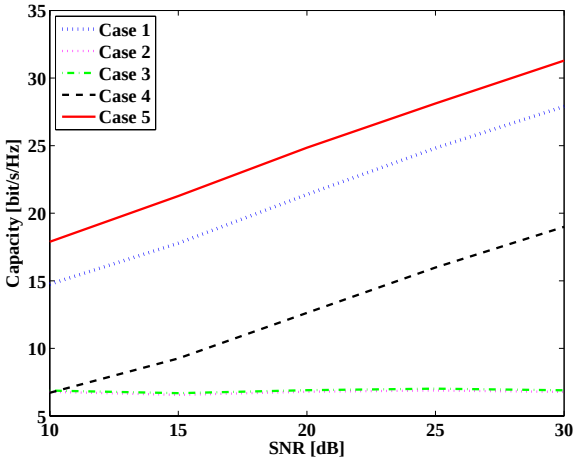


Figure 6. Input SNR versus capacity (User 0).

equipped with multiantenna, and the shape and size of cells are flexibly determined based on BS location and inter BS-UT channel condition. First, the nature of interferences from outer cells has been assessed. Then, the performance gain of BSC has been evaluated using five types of algorithms with and without BSC through computer simulations. The results show that BSC achieves about three times larger capacity compared to cooperation less scheme.

The future work is the investigation of BSC effect under the imperfect CSI. The extension of this work to relay aided BSC is also an attractive and important subject of study.

Acknowledgment

The authors would like to thank Dr. T. Fujii, Soft Bank Telecom, Japan, for his helpful suggestions about this study. This work was performed under research contract on cooperative base station system for the Ministry of Internal Affairs and Communications (MIC) of Japan.

References

[1] H. Zhang and H. Dai, “Cochannel interference mitigation and cooperative processing in downlink multicell multiuser MIMO networks,” EURASIP J. Wireless Commun. Networks, vol.2004, no.2, pp. 222-235, 2004.

[2] D. Gesbert, S. Hanly, H. Huang, S. Shamai, O. Simeone, and W. Yu, “Multi-cell MIMO cooperative networks: a new look at interference,” IEEE. J. Selec. Areas. Commun., vol.28, no.9, pp. 1380-1408, Dec. 2010.

[3] R. Irmer, H. Droste, P. Marsch, M. Grieger, G. Fettweis, S. Brueck, H.-P. Mayer, L. Thiele, and V. Jungnickel, “ Coordinated multipoint: Concepts, performance, and field trial results,” *IEEE Commun. Mag.*, vol.49, no.2, pp. 102-111, Feb. 2011.

[4] H. Lima, A. Moco, A. Silva, and A. Gameiro, “Performance assessment of single and multiple antenna relays for the uplink OFDM systems,” *4th Int. Conf. Syst. Networks Commun. (ICSNC’09)*, pp. 76-81, Porto, Portugal. Sept. 2009.

 ISBN: 978-1-61208-166-3

[5] A. Ahmad and M. Assaad, “Joint resource optimization and relay selection in cooperative cellular networks with imperfect channel knowledge,” *Proc. 2010 IEEE 11th Int. Workshop Sig. Process. Advances Wireless Commun. (SPAWC2010)*, Marrakech, Morocco, June 2010.

[6] A. Papadogiannis, D. Gesbert, and E. Hardouin, “A dynamic clustering approach in wireless networks with multi-cell cooperative processing, *Proc. IEEE Int. Conf. Commun. (ICC’08)*, pp. 4033-4037, Beijing, May 2008.

[7] Y. Akaiwa, “An adaptive base station cooperated cellular system and its theoretical performance analysis,” *Proc. 2011 IEEE 73rd Veh. Technol. Conf. (VTC2011-Spring)*, Budapest, Hungary, May 2011.

[8] R. Fritzsche, J. Voigt, C. Jandura, and G. Fettweis, “Comparing ray tracing based MU-CoMP-MIMO channel predictions with channel sounding measurements,” *Proc. 2010 4th European Conf. Antennas Propagat. (EuCAP2010)*, Barcelona, Spain, Apr. 2010.

[9] S. Shamai and A. D. Wyner, “Information-theoretic considerations for symmetric, cellular, multiple-access fading channels -Part II,” IEEE Trans. Inf. Theory, vol.43, no.6, pp. 1895-1911, Nov. 1997.

[10] G. R. Mohammad-Khani, S. Lasaulce, and J. Dumont, “About the performance of practical dirty paper coding schemes in Gaussian MIMO broadcast channels, *IEEE 7th Workshop Sig. Process. Advances Wireless Commun. 2006 (SPAWC ’06)*, Cannes, France, July 2006.

[11] T. Taniguchi, Y. Karasawa, and N. Nakajima, “MIMO cellular systems with irregular cell geometry based on base station cooperation,” *Proc. 2011 IEEE 73rd Veh. Technol. Conf. (VTC2011-Spring)*, Budapest, Hungary, May 2011.

[12] N. Jankiraman, *Space-Time Codes and MIMO Systems*, Artech House, Norwood, MA, 2004.

[13] J. Proakis, *Digital Communications*, 4th ed., McGraw-Hill, New York, NY, 2000.

[14] Q. H. Spencer, C. B. Peel, A. L. Swindlehurst, and M. Haardt, “An introduction to the multi-user MIMO downlink,” *IEEE Commun. Mag.*, vol.42, pp. 60-67, Oct. 2004.

 ISBN: 978-1-61208-166-3

Design Framework for Heterogeneous Hardware and Software in Wireless Sensor Networks

David Navarro, Fabien Mieyeville, Wan Du, Mihai Galos, Nanhao Zhu, Ian O'Connor
Université de Lyon, Institut des Nanotechnologies de Lyon (INL), UMR5270 - CNRS, Ecole Centrale de Lyon, Ecully, F-69134, France
david.navarro@ec-lyon.fr, fabien.mieyeville@ec-lyon.fr, wan.du@ec-lyon.fr, mihai.galos@ec-lyon.fr, nanhao.zhu@ec-lyon.fr, ian.oconnor@ec-lyon.fr

***Abstract*- Wireless Sensor Networks are composed of many autonomous resource-constrained sensor nodes. Constrains are low energy, memory and processing speed. Nowadays, several limitations exist for heterogeneous Wireless Sensor Networks: various hardware and software are hardly supported at design and simulation levels. Meanwhile, to optimize a self-organized network, it is essential to be able to update it with new nodes, to ensure interoperability, and to be able to exchange not only data but functionalities between nodes. Moreover, it is difficult to make design space exploration, as accurate hardware-level models and network-level simulations have very different (opposite) levels. We propose a simulator –based on SystemC language- that allows such design space explorations. It is composed of a library of hardware and software blocks. More and more sophisticated software support is implemented in our simulator. As trend is to deploy heterogeneous nodes, various software levels have to be considered. Our simulator is also thought to support many levels: from machine code to high level languages.**

Keywords-wireless sensor network; WSN; simulation; model; systemC

I. INTRODUCTION

Many applications use communicating and distributed sensory systems, such as for example environmental data collection, security monitoring, logistics or health [1]. These radiofrequency-based communicating systems are called Wireless Sensor Networks (WSN). Wireless Sensor Networks are large-scale networks of resource-constrained sensor nodes (electronic systems). Limited resources are of different kinds: energy, memory, processing and data-rate. Indeed, these autonomous systems have to ensure a so long autonomy that processing architecture and communications data-rate have to be very low. Sensor nodes cooperatively monitor and transmit data, such as temperature, vibration, pressure etc. They are typically composed of one or more sensors, a 8-bit or 16-bit microcontroller, a few Kbytes non-volatile memory, a low data-rate (often 250 Kbits/s) radiofrequency transceiver and a light battery. Fig. 1 shows a typical sensor node architecture.

A lot of hardware platforms exist (for example Crossbow, Ember, Meshnetics, Zolertia) and several devices are widely used: ATMEL, Texas Instruments or Microchip for microcontrollers, Texas Instruments, ATMEL, Freescale, or ST-Microelectronics for radiofrequency transceivers. Linux systems composed of 32-bit RISC processors exist – like the well known Crossbow's Stargate platform - but prohibitive energy consumption relegates these products to the border of the Wireless Sensor Networks field.

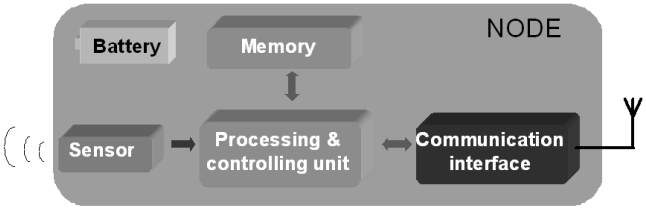


Figure 1. Wireless sensor node hardware architecture

We do not consider such systems, and we do focus on long autonomy systems. Low power constraint and large number of existing devices oblige us to think about dedicated (heterogeneous support) accurate simulator and programming tools.

Wireless Sensor Networks interconnect (topologies and network hierarchy) is inspired from wireless telecommunication and computer networks. We only focus on the often used IEEE 802.15.4 standard [2] that is widespread in Wireless Sensor Network commercial or custom platforms. Although complex topologies exist, such networks are dedicated to low power and low data rate applications, mainly for physical and environmental remote measurements. Most used topologies are also star or mesh networks [3].

Wireless Sensor Networks design is a difficult task, because the system designer has to develop a network with low level (at sensor node) hardware and software constraints. Computer-Aided-Design (CAD) tools would also be required to make system-level simulations, taking low-level parameters into account.

As presented in [4], many simulators have been developed over the last few years [5-9], but most of them are restricted to specific hardware or precisely focus on either network level or node level. They can be broadly divided into two categories: network simulators enhanced with node models (e.g., NS-2 [7] and OMNeT++ [8]), and node simulators enhanced with network models (e.g., Avrora [9], or SCNSL [10]). In the first category, simulators are not sensor platform specific and they are too high level for

 ISBN: 978-1-61208-166-3

hardware considerations. Precision problems are recurrent. In the second category, simulators are better suited for electronic system designers, requiring precise low level models for top-down (network to node) approach, but they suffer from too low-level aspects. Scalability and simulation time are problematic. Instruction Set Simulators have the same drawbacks. We propose a fast simulator of the last category.

Heterogeneous support means at first to be able to program several devices with a single compiler (C-level programming is nowadays the most used for Wireless Sensor Networks [11]), and to allow not only data but functionality exchange between nodes. As wireless sensor nodes are not often accessible, they have to be able to compile by themselves. Dynamic reconfiguration is also required. Many solutions exist nowadays; they require Operating Systems or Virtual Machines. The most known Operating Systems are TinyOS [11], Contiki [12], SOS [13], but they don't support heterogeneous firmware update. Indeed, they all use monolithic binary updates, which are architecture-specific. The most popular Virtual Machines for Wireless Sensor Networks are Maté [14], Darjeeling [15], VMStar [16], and ContikiVM [17]. They interpret a bytecode that is higher level than machine code. The drawback of these solutions is that big energy overhead is required to interpret and execute each bytecode instructions. It is well known that most of the power consumption in these systems is due to radiofrequency devices. So, a dedicated solution would be to consider in-situ compilation that minimizes code size transmission, in order to match the Sensor Networks constraints.

In this paper, we present a hIerarchical DEsign plAtform for sensOr Networks Exploration called IDEA1. It is characterized with SystemC simulation kernel, and a graphical interface to make it easier to use. Section II details its architecture, particularly in terms of hardware, software and network models. Section III details simulator user interface and results.

II. MODELS DETAILS

Our simulator is inspired from the SCNSL library [10], a networked embedded systems simulator. It is written in SystemC and C++. SystemC is widely used in electronics community; it is part of the classical design flow. SystemC based on an event-driven simulator kernel, and this language permits to model hardware and software at same time, in the so-called co-simulation. As Fig. 2 shows, three main models exist: nodes (in SystemC), node-proxy (in SystemC) and network (in C++). C++ is used to model the network in terms of connectivity and communication characteristics; and proxies that make input/output interfaces between nodes and network. Simulation occurs in two steps: a gcc compilation creates the network, that is also static, and then the SystemC kernel runs the simulated time. It would be possible to simulate a dynamic (moving) network, but simulation time would be largely affected.

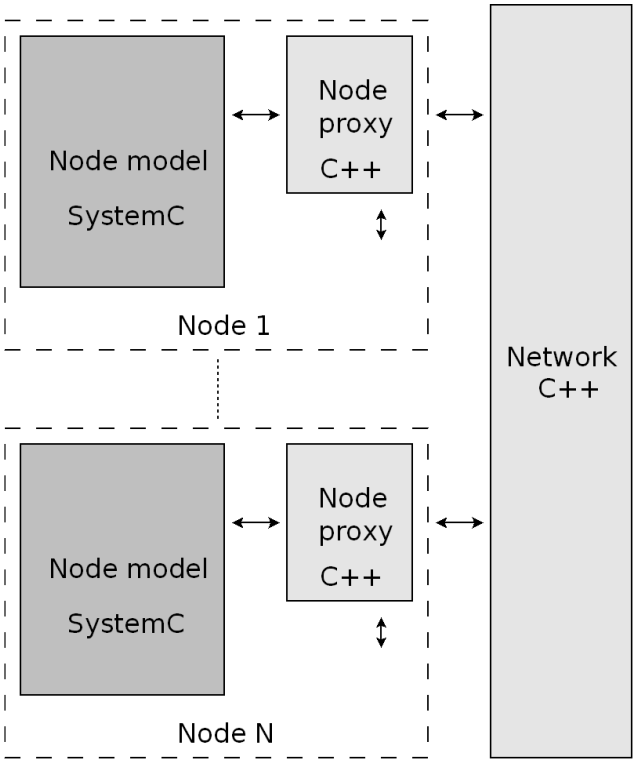


Figure 2. Wireless sensor network model

Node model is detailed in Fig. 3. It is composed of hardware and software parts. This physical layer is also detailed below for hardware and software parts.

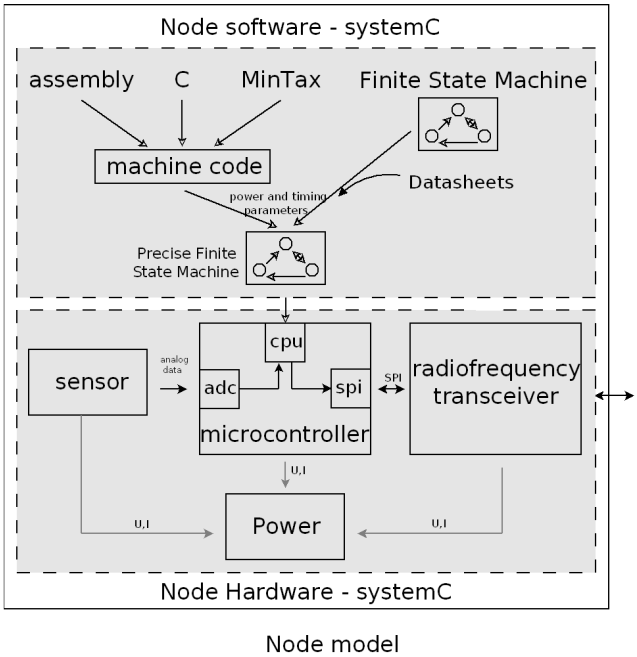


Figure 3. Wireless sensor node architecture model

A. Hardware model

Hardware part embeds classical wireless sensor nodes devices: a sensor, a microcontroller, a radiofrequency transceiver and a battery. Hardware devices models are detailed with electrical and timing parameters.

As battery discharge is based on chemical non linear reactions, we prefer - for the moment - to define a simpler power module that monitors instantaneous and average power and energy. A generic battery life time can be computed.

Sensor is modeled with its transfer function that gives sensor output voltage versus physical input. This transfer function can be composed of integrations during time, or error deviations.

Microcontroller is the processing and controlling unit. Depending on application, an external flash memory is sometimes used, its usage really impacts power consumption. Sensor data is captured by an Analog to Digital Converter (ADC) that is typically a 10-bit successive approximation converter. It gives the best balance between speed and accuracy. Concerning communication interface that enables dataflow output, it is done by a classical serial communication, hardware supported by means of a serial peripheral interface (SPI) block. The processing part of the microcontroller is a simple 8-bit or 16-bit datapath organized around a light arithmetic and logic unit (ALU). In power-aware Wireless Sensor Nodes, processing power of that element is at maximum a few tens of MIPS, coupled with specific low power architectures.

Next, data are output from the node by a radiofrequency transceiver. This complex device allows generating a high frequency carrier in order to propagate data over the air. The carrier depends on country norms, the most typical free frequencies that are used are 433MHz, 868MHz, 916MHz, 2.4GHz. Due to market explosion concerning embedded products, and to small size of antenna, 2.4GHz radiofrequency transceivers are nowadays mostly used in embedded systems. Data have to be organized in packets. These packets allow to route data towards the right node, to ensure data integrity, while respecting a given communication protocol. The radiofrequency transceiver model contains different working states (receive, transmit, idle, sleep), and several operating modes.

At the whole, several hardware devices have been modeled (Table I). These hardware devices are interchangeable in order to model different existing or novel hardware platforms. Simulator enables user to test an application on several hardware devices to find the solution that best fits requirements, such as data-rate and energy. ATMEL ATMega128 and Microchip PIC16LF88 are well known low power microcontrollers. Texas Instruments CC2420 and Microchip 24J40 are the most used transceivers, as their carrier is 2.4GHz, and they support the IEEE 802.15.4 standard and the ZigBee stack. Sensors are often used ones. The first is a light sensor of the Crossbow Mica platform, the other one is a widespread temperature sensor.

TABLE I. LIST OF MODELEDHARDWARE DEVICES

Microcontrollers		ATMEL ATMega128 Microchip 16LF88
Radiofrequency transceivers		Texas Instruments CC2420 Texas Instruments CC1000 Microchip MRF24J40 Nordic nRF24L01
Sensors	**Temperature**	National Semiconductor LM35DZ
	Light	Clairex CL9P4L

B. Software model

Software has to be considered on two different aspects:

- Portability: executable (machine) code is specific to each precise hardware architecture.
- Level: many different languages exist, thus enabling different levels of coding, from assembly to high level languages.

For these two reasons, we have decided to support heterogeneous multiple software levels. As Fig. 3 shows, the software input can be at state machine level or at programming language level.

1) State Machine level

The software running on microcontroller is divided into different tasks (states), such as data processing, analog to digital conversion (ADC) and communication (SPI). The execution time of each task is calculated according to its datasheet typical values. For example, the time taken by PIC16LF88 to configure and launch ADC is taken into account (hardware delays such as the 11.974µs minimum required acquisition time [18]).

When data are transferred from microcontroller to radiofrequency transceiver, a trigger command enables transmission. At the right time (depending on network policy), the radiofrequency transceiver will transmit data to another node. Microcontroller that drives radiofrequency transceiver has different working states, detailed in Fig. 4 for a simple example.

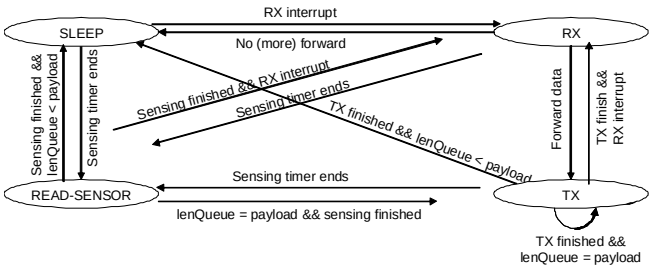


Figure 4. Simple capture and send program in microcontroller

This finite state machine has been implemented with realistic (from datasheet and measurement validated) parameters in terms of delays and power consumption. Actual hardware library with finite state machine models is detailed in table I. In our model, the microcontroller can configure some parameters of physical (PHY) and MAC layers in the radiofrequency transceiver registers (IEEE 802.15.4 - compliant).

Both IEEE 802.15.4 non-beacon and beacon modes are supported in our simulator. Non-beacon mode is based on a channel free access and packet-based philosophy. When a node wants to send data, it senses the channel, then sends them if the channel is free. If the channel is busy, it waits a random time (called back-off time) and then checks for free channel again. This method is called CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance). Beacon mode is a synchronized mode: the network coordinator (network head) sends synchronization packets to inform nodes when they can communicate. In this case, the mode is also channel-based, inspired from the well known TDMA (Time Division Multiple Access) method.

Time is organized according to a superframe that is defined by the network coordinator. Two beacon-mode algorithms exist: slotted CSMA-CA, and GTS communication non-predictive GTS and predictive GTS [2]. Slotted CSMA-CA is a CSMA-CA based communication, within a given slot time. In GTS algorithm, nodes that want to communicate send a GTS request to the coordinator during a first time slot (the Contention Access Period). Then, nodes are allowed to communicate during a following time slot (the Contention Free Period).

A power module has been implemented. It computes and monitors electrical power and energy consumed by sensor, microcontroller and radiofrequency transceiver. Different energy-saving (sleep) modes, data flow and global behavior can also be co-designed according to power constraints.

2) Language level

If user selects language input instead of finite state machine, several solutions are available. This step is currently being implemented in our framework. Input language can be in assembly, in C language, or in a high level language we have developed (MinTax). Software support of ATMEL ATMega128 is currently realized, we plan to support Texas Instruments MSP430 and Microchip PIC16LF88 later. The commercial platforms we are using for testcase and measurements are ATMEL AVRraven and Zolertia Z1, comprising for Texas Instruments MSP430 and ATMEL ATMega128 microcontrollers.

In order to meet the energy constraints in a Wireless Sensor Network, the processing and controlling unit is nearly all the time a microcontroller. Such devices often consume less than 5 mW. Meanwhile, they often have 8-bit or 16-bit datapaths that process less than 20 MIPS, and they embed less than 128 Kbytes of program memory (FLASH ROM), and less than 16 Kbytes of data memory (RAM). Such light architectures require specific lightweight solutions.

If assembly language is used, the code is analyzed in order to estimate process timing of microcontroller, and its associated power consumption.

If C language is selected, compilers are used to generate low level assembly and machine code. IAR Systems compiler is used for Texas Instruments MSP430, AVR-gcc is used for ATMEL ATMega128. C language compilation generates assembly code that is treated in the same way as direct assembly input. More precisely, lss output files from compilers are treated.

As a test-case, we have demonstrated that our simulator is moreover able to consider new languages that could better suit Wireless Sensor Network specificities. To prove this, the simulator supports a high level dedicated language we have developed, with an energy-aware syntax that allows to compactly write microcontroller tasks. That minimal syntax (MinTax, detailed in [19]), based on C language, has the advantage to require fewer characters, and also shorter radiofrequency communications for program exchanges. A MinTax and C comparison example is given in table II. We can clearly see that MinTax reduces the number of characters to code the example (pin toggle program). Data to send are also reduced by a 3 factor.

TABLE II. MINTAX – C COMPARIZON.

MinTax	**C**

f{
WT
$b%2
#
};
	void f()
	{
	while(true)
	{
	PORTB ^= (1<<2);
	}
	}

11 bytes	37 bytes

As in C language, this high level syntax permits designer to have hardware abstraction, and also to consider a single language on heterogeneous platforms. A functionality exchange in a heterogeneous network has been implemented as testcase. ATMEL AVRraven and Zolertia Z1 platforms were used, and functionality written in MinTax has been send from ATMEL ATMega to T.I. MSP430 through ATMEL AT86RF230 and T.I. CC2420 transceivers (IEEE 802.15.4 standard).

The compiler that is related to this language is based on classical compiler structure, as shown in Fig. 5. As it is embedded (compilation is done in-situ with low processing unit), all of its parts have been optimized for compactness. Two stages exist: an analysis stage then a synthesis stage. The analysis stage reads the high-level language, splits it into tokens and orders them. It recognizes for example variables names and functions calls. The synthesis stage generates the executable code (binary machine code). More information about classical compiler structure is detailed in [20].

 ISBN: 978-1-61208-166-3

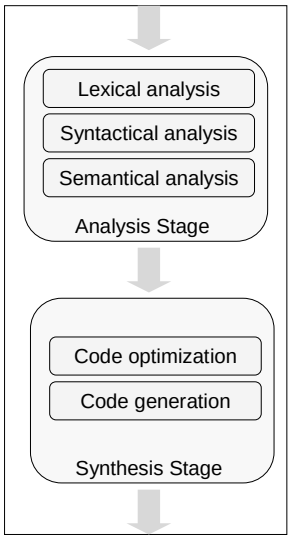


Figure 5. Classical compiler structure

Several variants of the compiler exist: it has been cross - developed on x86 personal computer and on several microcontroller architectures. The PC variant allows easier debugging because of its human-machine interface. It permits to deploy the code on the nodes by serial programming machine code (output files such as .hex). The microcontroller variant has been developed on several hardware architectures to prove the heterogeneity support. Software support, from low level (assembly) to novel high level specific languages (MinTax) has also been proved.

III. SIMULATOR INTERFACE AND RESULTS

User interface is shown in Fig. 6. It is composed of different sub-windows. The information appears graphically in the right window, to clearly display the network topology. Each node and coordinator is characterized by a spatial position. Lines between nodes represent possible communications routes according to position, transmit power and receive sensitivity. When parameters are changed, the graphical viewer refreshes the possible communications (lines). For this early version, free space communications are considered. Focus is set on communication capabilities and data rate, not on mechanical or electromagnetic environments. Hardware parameters of microcontrollers and radiofrequency devices are set. At higher level, many parameters of the IEEE 802.15.4 can be set. Sensors sampling rate and packets payload can also be changed.

By clicking on the launch button in the graphical interface, a SystemC simulation is launched in background. The simulation log is displayed in the bottom window of graphical interface, and a timing trace (VCD) viewer is opened. Output log files are also generated. From these results, we can explore design space in order to find the best-suited design solution.

As a test example, we simulated an 8 nodes network. We chose Microchip PIC16LF88 and MRF24J40 as target test hardware. As IEEE 802.15.4 data-rate is low (250 Kb/s), a systematic trade-off between payload (number of sent data bytes per packet), sampling rate (of ADC) and packet delivery rate has to be explored.

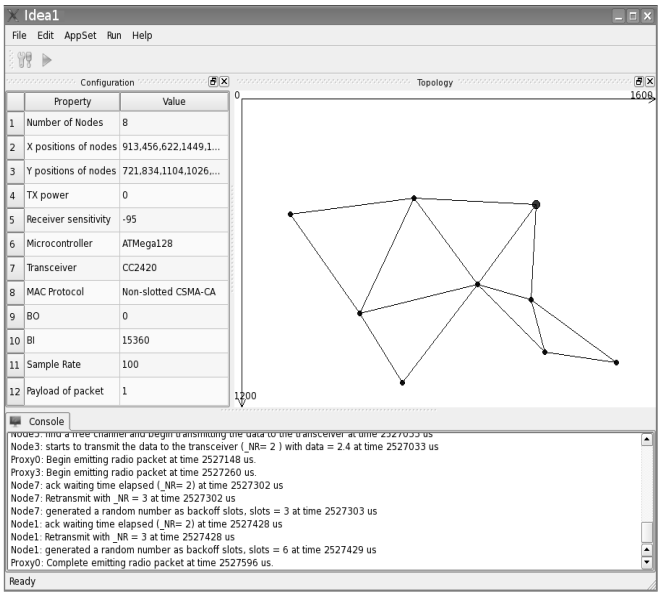


Figure 6. Simulator graphical interface

Simulator can output a transient VCD trace and text log. Log permits to process data in order to evaluate Packet Delivery Rate (PDR), Packet Latency (PL), Energy Per Packet (EPP), and average power consumption. Packet delivery rate is the ratio of number of successful packets over the total number of sent packets is measured. Packet latency is the time needed by a packet to go from one node to another one. Energy per packet is related to the product of sent packets by the sample period. Average power consumption is the one consumed by electronic devices. Global power consumption of hardware devices level is available; this result was shown in [21].

Moreover, it is now possible to detail the power consumption of each hardware part in microcontroller. Fig. 7 shows decomposition of power consumption in microcontroller according to analog to digital converter (ADC), serial communication (SPI), processing of CPU, and sleep state. This analysis is done for various frequencies of data sampling. Power consumption is high when sample rate is high, because nodes are always busy in these two cases. Moreover, as almost maximal usage is reached from 100Hz, power consumption difference is small for 100 and 1000 Hz. Most power consuming states are CPU processing and inter-chip communications. It clearly shows the impact of hardware support of radiofrequency device on power consumption of microcontroller: depending if IEEE 802.15.4 is hardware supported in radiofrequency device or not, power consumption distribution changes. Indeed, the bigger part of physical and MAC layers to be managed by the microcontroller, the more power consumption will be observed for this device. At the same time, radiofrequency

 ISBN: 978-1-61208-166-3

transceiver will have different idle and sleep timings according to this eventual IEEE 802.15.4 hardware support, so different power consumption is impacted too.

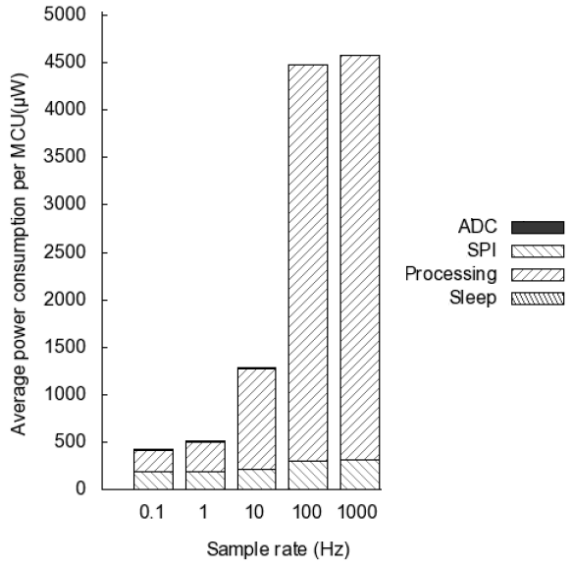


Figure 7. Microcontroller unit (MCU) detailed power consumption

IV. CONCLUSION

A Wireless Sensor Network design framework, based on SystemC, has been presented. It permits design space exploration, considering hardware and software details. Hardware is modeled as a finite state machine, characterized by timings and power consumption of each state. Software can be modeled as finite state machine in the same way. Current work is done in order to take real program inputs at different levels: assembly, C language using existing compilers, or high level minimalist language (MinTax) associated to its in-situ compiler we already have developed. This language permits to exchange functionalities between non-compatible (heterogeneous) processing units, with a small energy cost. A graphical user interface permits to easily simulate and compare several IEEE 802.15.4 configurations and programs on many interchangeable (and parameterized) hardware devices.

REFERENCES

[1] M. Horton and J. Suh, “A vision for wireless sensor networks”, IEEE Microwave Symposium Digest, USA, June 2005, pp. 361-364.

[2] IEEE 802.15 WPAN Task Grup 4, “IEEE 802.15 part 15.4-2006 wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs), http://www.ieee802.org/15/pub/TG4.html, last access date: July 2011.

[3] A. Salhieh, J. Weinmann, M. Kochhal, and L. Schwiebert, “Power efficient topologies for wireless sensor networks”, International Conference on Parallel Processing, Spain, Sept. 2001, pp. 256-163.

[4] W. Du, D. Navarro, F. Mieyeville, and F. Gaffiot, “Towards a taxonomy of simulation tools for wireless sensor networks” International Conference on Simulation Tools and Techniques, Spain, March 2010, pp. 1-7.

[5] P. Levis, N. Lee, M. Welsh, and D. Culler, “Tossim: accurate and scalable simulation of entire tinyos applications”, International Conference on Embedded Networked Sensor Systems, USA, Nov. 2003, pp. 126-137.

[6] M. Varshney, D. Xu, M. Srivastava, and R. Bagrodia, “sQualNet: an accurate and scalable evaluation framework for sensor networks”, International Symposium on Information Processing in Sensor Networks, USA, April 2007, pp. 196-205.

[7] S. McCanne and S. Floyd, “Network simulator NS-2”, http://www.isi.edu/nsnam/ns, last access date: July 2011.

[8] A. Varga, “The OMNeT++ discrete event simulation system”, European Simulation and Modeling Conferences, Czech Republic, June 2001, pp. 319-324.

[9] B. Titzer, D. Lee, and J. Palsberg, “Avrora: scalable sensor network simulation with precise timing”, Information Processing in Sensor Networks, USA, April 2005, pp. 477-482.

[10] F. Fummi, D. Quaglia, and F. Stefanni, “A systemC-based framework for modeling and simulation of networked embedded systems”, Forum on Specification and Design Languages, Germany, Sept. 2008, pp. 49-54.

[11] L. Mottola and G.P. Picco, “Programming wireless sensor networks: fundamental concepts and state of the art”, ACM Computing Surveys. Volume 43, Issue 4, Dec. 2010, pp. 1-19.

[12] A. Dunkels, B. Gronvall, and T. Voigt, “Contiki - a lightweight and flexible operating system for tiny networked sensors”, IEEE International Conference on Local Computer Networks., USA, Nov. 2004, pp. 455-462.

[13] C.-C. Han, R. Kumar, R. Shea, E. Kohler, and M. Srivastava, “A dynamic operating system for sensor nodes”, International Conference on Mobile systems Applications and Services, USA, June 2005, pp. 163-176.

[14] P. Levis and D. Culler, “Mate: a tiny virtual machine for sensor networks”, International Conference on Architectural Support for Programming Languages and Operating Systems, USA, Oct. 2002, pp. 85-95.

[15] N. Brouwers, K. Langendoen, and P. Corke, “Darjeeling, a feature-rich VM for the resource poor”, ACM Conference on Embedded Networked Sensor Systems, USA, Nov.2009, pp. 169-182.

[16] J. Koshy and R. Pandey, “VMSTAR: synthesizing scalable runtime environments for sensor networks,” International Conference on Embedded Networked Sensor Systems, USA, Nov. 2005, pp. 243-254.

[17] A. Dunkels, “Programming Memory-Constrained Embedded Systems”, PhD Thesis, Swedish Institute of Computer Science, 2007.

[18] Microchip Inc., “PIC16F87/88 Enhanced Flash Microcontrollers with nanoWatt Technology Datasheet”, http://www.microchip.com, last access date: July 2011.

[19] M. Galos, F. Mieyeville and D. Navarro, “Dynamic reconfiguration in wireless sensor networks”, International Conference on Electronics Circuits and Systems, Greece, Dec. 2010, pp. 918-921.

[20] R. Mak, “Writing compilers and interpreters”, Ed Wiley Computer Publishing, ISBN 471-11353-0.

[21] W. Du, F. Mieyeville and D. Navarro, “Modeling energy consumption of wireless sensor networks by systemC”, International Conference on Systems and Networks Communications, France, Aug. 2010, pp. 94-98.

 ISBN: 978-1-61208-166-3

A Fair and Efficient Spectrum Assignment for WiFi/WiMAX Integrated Networks

† Kazuhiko Kinoshita, † Masashi Nakagawa, ‡ Keita Kawano, † Koso Murakami
† Department of Information Networking,
Graduate School of Information Science and Technology, Osaka University
1-5 Yamadaoka, Suita, Osaka 565–0871, JAPAN
‡ Center for Information Technology and Management, Okayama University
3-1-1 Tsushimanaka, Okayama, Okayama 700–8531, JAPAN
E-mail: † {kazuhiko, nakagawa.masashi, murakami}@ist.osaka-u.ac.jp
‡ keita@cc.okayama-u.ac.jp

***Abstract*—In recent years, integrated wireless networks and spectrum sharing in such networks have been researched actively. We have also proposed a spectrum assignment method for improving the average throughput of the whole network. In this method, however, WiFi users would obtain higher throughput at the expense of WiMAX users. This would be unfair in WiFi/WiMAX integrated networks. To overcome this problem, this paper proposes a fair and efficient spectrum assignment method for such networks. Finally, simulation experiments show the excellent performance of the proposed method.**

Keywords*-*spectrum assignment; spectrum sharing; dynamic spectrum access; WiFi; WiMAX.

I. INTRODUCTION

With advances in communication technologies, network services available via the Internet have become widely diversified. People can use such services not only via wired networks but also via wireless networks. With the demand for multimedia services via wireless networks growing, just as for wired networks, the bandwidth of cellular networks is growing and the number of wireless LAN access points (APs) is increasing greatly.

There are already several wireless systems being used in practice, including Cellular [1], WiFi [2], and WiMAX [3], [4]. Each system uses its own spectrum as prescribed by law to avoid interference.

However, these wireless communication systems operate independently, because the mechanisms of these systems are fundamentally different. Therefore, switching between systems must be performed manually by users. To avoid this inconvenience, an integrated network [5], [6], within which these systems can interwork, has been designed as a next-generation wireless communication system. In such an integrated network, mobile users can have seamless, continuous communication via the best available wireless communication system, according to the application or the local conditions of the wireless systems. Therefore, it will be possible to provide better communications for mobile users.

However, the available spectrum resources are finite, and so other approaches that use radio resources more effectively are being considered. As mentioned above, although the amount of available radio spectrum for a particular form of wireless communication is decreasing because of the increasing diversity of wireless networks, the traffic demand for wireless networks is increasing with the increasing variety of broadband applications. To address this dilemma, "cognitive radio" [7], [8] is receiving much attention.

Cognitive radio technologies can be classified as either multimode systems or dynamic spectrum access (DSA) systems [9], [10]. Multimode systems select between a number of independent wireless systems according to the communication environment of the user and the condition of each wireless system. Conversely, a DSA-based wireless system can make secondary use of the radio frequency spectrum that other wireless systems are using. The frequency spectrum is used more efficiently in DSA systems than in multimode systems.

We have proposed a spectrum assignment method for improving the average throughput of the whole network [11]. However, because this method focuses only on the overall improvement of the average throughput in the network, WiFi users would obtain higher throughput at the expense of WiMAX users. This would be unfair in WiFi/WiMAX integrated networks.

To overcome this problem, this paper proposes a fair and efficient spectrum assignment method for such networks.

In the rest of this paper, Section II introduces related work and points out the problematic issues. Section III proposes the fair and efficient spectrum assignment method. It is evaluated in Section IV and V. Finally, Section VI makes some conclusions and indicates future works.

II. RELATED WORK

A. Integrated Wireless Network

Although several wireless systems, such as Cellular, WiFi, and WiMAX, have developed independently, they should be integrated for seamless access by users. Therefore, in recent years, Cellular/WiFi integrated networks [12], [13] and WiFi/WiMAX integrated networks [14], [15] have been researched actively. In particular, a WiMAX/WiFi integrated

 ISBN: 978-1-61208-166-3

network can achieve high-quality communications by using WiMAX and WiFi as complementary access resources. This integrated network enables load balancing between WiMAX and WiFi by using each system selectively in response to the demands of users and the condition of each system.

However, this integrated network assumes that each wireless system uses the spectrum band prescribed by law, so that, even if the WiMAX system has unused spectrum temporarily, it cannot be used by WiFi systems. As a possible solution to this problem, cognitive radio is receiving much attention.

B. DSA

According to [10], DSA strategies can be categorized in terms of three models, namely, the Dynamic Exclusive Use Model, the Open Sharing Model, and the Hierarchical Access Model, which are described below.

1) Dynamic Exclusive Use Model: This model protects the current spectrum regulation policy, in which spectrum bands are licensed to services for exclusive use. The main idea is to introduce flexibility to improve spectrum efficiency. Two approaches have been proposed under this model, namely, spectrum property rights and dynamic spectrum assignment. The former approach allows licensees to sell and trade spectrum and to choose freely between technologies. The economy and the market will therefore play major roles in driving towards the most profitable use of this limited resource. On the other hand, the latter approach aims to improve spectrum efficiency through dynamic spectrum assignment by exploiting the spatial and temporal traffic statistics of the various services.

2) Open Sharing Model: This model employs open sharing among peer users as the basis for managing a spectral region. Advocates of this model draw support from the phenomenal success of wireless services operating in the unlicensed Industrial, Scientific, and Medical radio band.

3) Hierarchical Access Model: This model adopts a hierarchical access structure with primary users (licensees) and secondary users. The key idea is to open licensed spectrum to secondary users while limiting the interference perceived by primary users. Two approaches to spectrum sharing between primary and secondary users have been considered, namely, spectrum underlay and spectrum overlay. The former approach imposes severe constraints on the transmission power of secondary users so that they operate below the noise floor of primary users. By spreading transmitted signals over a wide frequency band (i.e., using an Ultra-Wideband system), secondary users can potentially achieve short-range high data rates with extremely low transmission power. Alternatively, the latter approach does not necessarily impose severe restrictions on the transmission power of secondary users, but rather on when and where they may transmit. It directly targets spatial and temporal white space in the spectrum by allowing secondary users to identify and exploit local and instantaneous spectrum availability in a nonintrusive manner.

C. The Existing Method for WiFi/WiMAX Integrated Networks and Problematic Issues

A spectrum-sharing method whereby several WiFi APs temporarily use an unused WiMAX band in a WiFi/WiMAX integrated network has been proposed. It is based on the spectrum overlay described above. In this proposal, as shown in Fig. 1, a central control server called the spectrum manager (SM) manages the spectrum assignment and necessary information for assignment in a WiMAX base station (BS) and the WiFi APs inside the WiMAX service area of the BS. In this paper, we abbreviate “WiMAX service area” to “area” and call the hexagonal area accessed by the WiFi AP the “cell”.

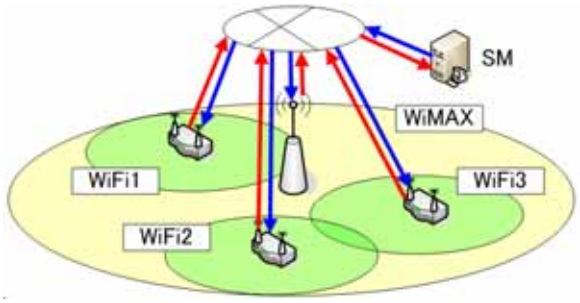


Fig. 1. Network Model

The coverage area of the WiMAX BS, a few kilometers in radius, is so large that it will include some WiFi APs. Therefore, the same spectrum can be used repeatedly by assigning unused WiMAX spectrum to WiFi APs without causing interference between the adjacent WiFi APs. If two or more WiFi APs use some WiMAX BS spectrum, the spectrum utilization efficiency can be enhanced for the whole network.

In [11], a spectrum assignment method to improve the overall average throughput for the network was proposed. In this method, the WiFi APs best suited to receive an additional channel from the WiMAX system are decided by using a genetic algorithm (GA). The sum of the number of users who connect to assigned target WiFi AP is defined as its *fitness value*. As a *constraint*, the method does not assign a certain channel to adjacent WiFi APs simultaneously. In this paper, we call this method the “existing method”.

It was confirmed that the existing method improved the overall average throughput in the network compared with a method without spectrum sharing, as shown in Fig. 2. In this graph, the horizontal and vertical axes show the arrival rate for the entire network and the average download time, respectively.

However, because the existing method focuses only on improvements in the average throughput of the entire network, the individual throughput obtained by WiFi or WiMAX is unfairly distributed, as shown in Fig. 3. That is, WiFi users obtain their higher throughput at the expense of WiMAX users. This would be manifestly unfair in a WiFi/WiMAX integrated network.

 ISBN: 978-1-61208-166-3

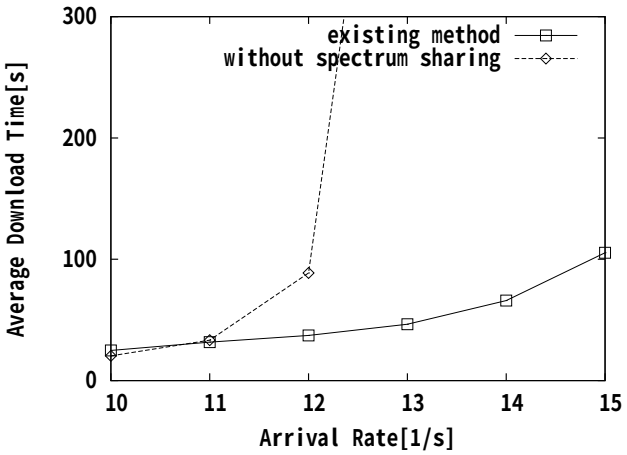


Fig. 2. Throughput Improvement via the Existing Method

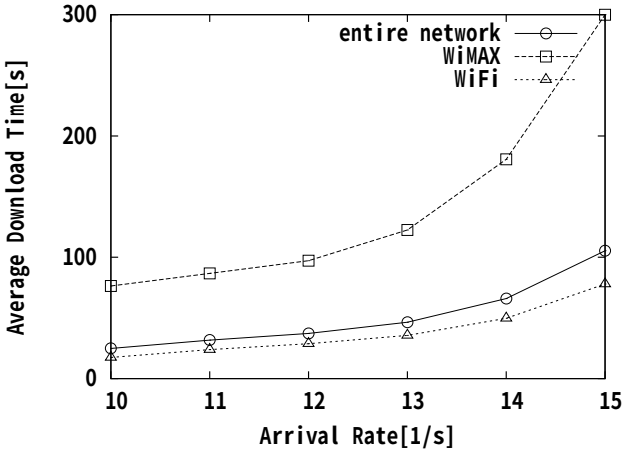


Fig. 3. Performance Characteristics of Existing Method

III. Proposed Method

To overcome the problem described above, we propose a spectrum-sharing method that improves fairness in addition to providing higher throughput. The proposed method aims not only to improve total throughput but also to minimize the difference in throughput between WiFi users and WiMAX users. To achieve this, we introduce an *index* to indicate the effectiveness of the spectrum assignment. Here, a smaller value for the index means a better spectrum assignment.

The procedure for the proposed method is shown in Fig. 4. First, the number of users who connect to each system is acquired. Next, the index is calculated for the instant of time of the assignment. In addition, suppose that one channel is assigned from the WiMAX spectrum, and the APs of the assignment target are decided. After the assignment is conducted, the capacity of each system will be changed. Therefore, the capacity of each system is renewed and the index is recalculated.

The index is then calculated for the case of a second additional channel being assigned from WiMAX in the same manner. Finally, the number of assignment channels that minimizes the index is decided.

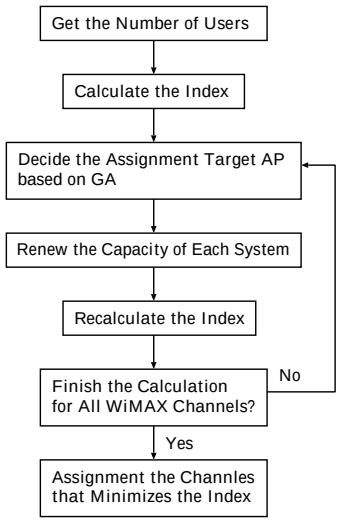


Fig. 4. Flowchart of the Proposed Method

As mentioned above, after the assignment is carried out, the capacity of both WiFi and WiMAX will be changed. In what follows, "capacity" means the capacity after increasing or decreasing the number of channels.

The average throughput for WiFi users is calculated by Eq. (1).

$$\frac{\sum_{i=1}^{n} p_i u_i}{\sum_{i=1}^{n} \frac{1}{\frac{c_i}{u_i}} \times p_i u_i}, \tag{1}$$

where n, c_i, and u_i are the number of areas, the capacity of the WiFi AP, and the number of connected users, respectively. p_i is an indication function, with $p_i = 1$ indicating that area i contains a WiFi AP, and $p_i = 0$ indicating otherwise.

In the same way, the average throughput of WiMAX users is calculated by Eq. (2).

$$\frac{C}{U}, \tag{2}$$

where C and U refer to the capacity of the WiMAX system and the number of connected WiMAX users, respectively.

The index of the proposed method is defined in Eq. (3) and the proposed method assigns additional channel(s) from WiMAX to WiFi based on the number of channels that minimizes the value of this index.

$$\left| \frac{\sum_{i=1}^{n} \frac{1}{\frac{c_i}{u_i}} \times p_i u_i}{\sum_{i=1}^{n} p_i u_i} - \frac{U}{C} \right| \tag{3}$$

IV. Performance Evaluation

A. Simulation Model

In this section, we evaluate the performance of the proposed method by simulation experiments.

Fig. 5 shows the network model assumed in this simulation. One WiMAX BS and $10 \times 10 = 100$ small areas are allocated to the access area of the WiMAX system. The WiFi APs are allocated to the small areas according to the *distribution rate*. For example, if the distribution rate is 0.75, $100 \times 0.75 = 75$ small areas are selected at random and each has a WiFi AP.

The spectrum of the WiMAX BS is divided into several channels of 20[MHz] each. The WiMAX system is assumed to provide 40 Mbps per channel in accordance with [18] and the WiFi systems are assumed to provide 17.5 Mbps per channel according to our preliminary experiments that used ns2 [19]. In addition, the spectrum utilization, the load status of each system, the control of the spectrum assignment, and the implementation of GA are managed by the SM, as shown in Fig. 5.

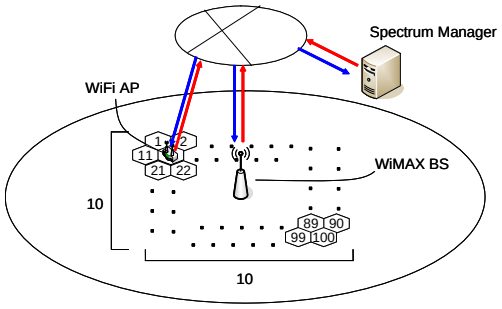


Fig. 5. Simulation Model

In this paper, we focus on best-effort traffic such as data downloading or web browsing. Users are assumed to be downloading a 10[MByte] file. When a new mobile user joins the integrated network, the user connects to a wireless system selected by the spectrum manager and starts downloading data at the allocated throughput. When the downloading is complete, the mobile user disconnects from the wireless system.

If a new user arrives in an area with a WiFi AP, the WiFi connection is used. Otherwise, the WiMAX BS is used. In addition, users stay in the arrival area until the end of their downloading. Calls occur according to a Poisson arrival process, and the arrival rate depends on the existence of the WiFi AP. Because WiFi APs tend to be set up in places where people gather, such as cafes, offices, and rail stations, the call arrival rate in an area with a WiFi AP is assumed to be x times higher than that in an area without a WiFi AP.

We define the arrival rate for the entire network in the case of $x = 1$ as λ_{sys}. To keep λ_{sys} independent of the distribution rate r and the arrival rate ratio x, arrival rates of λ_a (with WiFi AP) and λ_b (without WiFi AP) were selected to satisfy the following equations.

$$\lambda_a = \lambda_{sys} \times \frac{x}{(1-r) \times 1 + r \times x} \quad (4)$$

$$\lambda_b = \lambda_{sys} \times \frac{1}{(1-r) \times 1 + r \times x}. \quad (5)$$

To measure performance, we observe the average time to finish downloading (*download time*) and its coefficient of variance.

Other parameter settings are as shown in Table I.

TABLE I
DEFAULT SIMULATION PARAMETERS

Distribution rate for WiFi APs r	0.5
Spectrum bandwidth for WiMAX	100 MHz
Arrival rate ratio x	5
Interval time T for spectrum assignment	300 seconds

V. SIMULATION RESULTS

Fig. 6 shows the average download time as a function of the call arrival rate. It indicates that the average throughput of the proposed method is almost equal to that of the existing method.

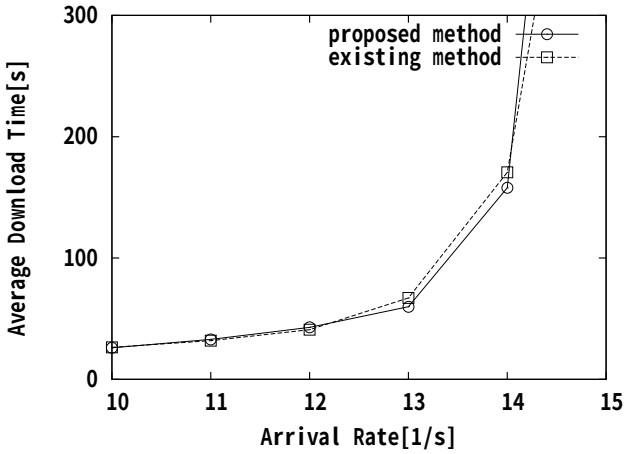


Fig. 6. Mean Dowload Time

Fig. 7 shows the coefficient of variance as a function of the call arrival rate. From this figure, the proposed method is shown to have a lower coefficient of variance than the existing method for heavy-load situations.

Figs. 8 and 9 show the average download time and its coefficient of variance as a function of the arrival rate ratio x, respectively. The call arrival rate was set to 12[1/s].

These results indicate that the proposed method is robust against the arrival rate ratio.

VI. CONCLUSION AND FUTURE WORKS

In this paper, we have described a spectrum-sharing method that improves the average throughput in a WiFi/WiMAX integrated network and we have shown that there was still room for improvement in the fairness of individual-user throughput. We have therefore enhanced the method to consider fairness in addition to providing higher throughput.

In future work, it will be necessary to propose a spectrum-sharing method that considers QoS issues for network traffic.

 ISBN: 978-1-61208-166-3

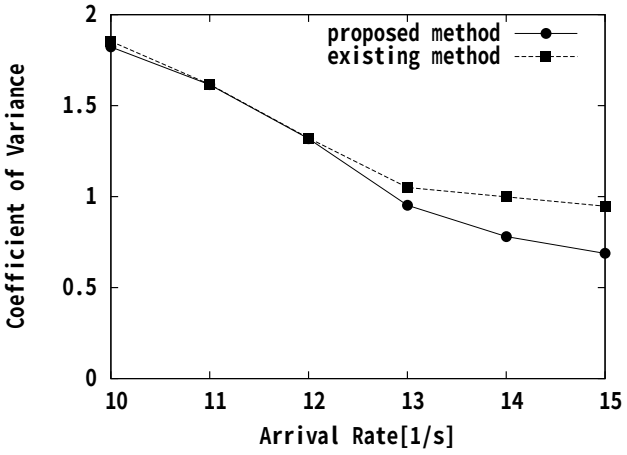


Fig. 7. Coefficient of Variance

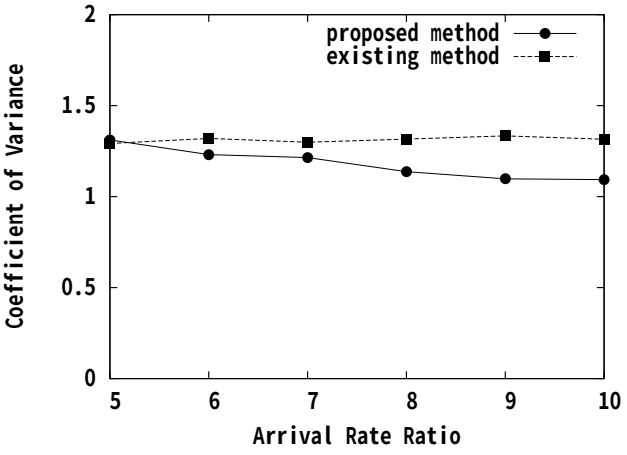


Fig. 9. Coefficient of Variance (variable arrival rate ratio)

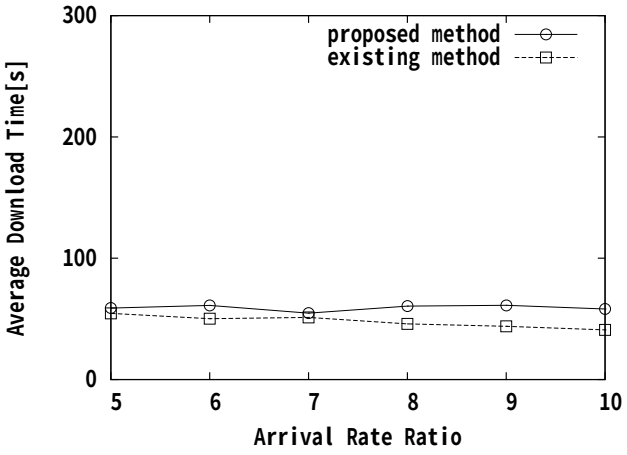


Fig. 8. Mean Download Time (variable arrival rate ratio)

REFERENCES

[1] 3GPP, http://www.3gpp.org/.

[2] WiFi Forum, http://www.wifi-forum.com/wf/.

[3] "Air Interface for Fixed Broadband Wireless Access Systems," *IEEE STD 802.16–2004.*, (Oct. 2004).

[4] "Air Interface for Fixed and Mobile Broadband Wireless Access Systems," *IEEE P802.16e/D12.*, (Feb. 2005).

[5] S. Ohmori, Y. Yamao and N. Nakajima, "The Future Generations of Mobile Communications Based on Broadband Access Technologies," *IEEE Communications Magazine*, vol. 38, no. 12, pp. 134–142, (Dec. 2000).

[6] M. Buddhikot, G. Chandranmenon, S. Han, Y.W. Lee, S. Miller and L. Salgarelli, "Integration of 802.11 and Third-Generation Wireless Data Networks," *IEEE INFOCOM'03*, vol. 1, pp. 503–512, (Apr. 2003).

[7] J. Mitola III and G. Q. Maguire, "Cognitive Radio: Making Software Radios More Personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–14, (Aug. 1999).

[8] I.F. Akyildiz, et al., "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks Journal*, vol. 50, pp. 2127–2159, (Sept. 2006).

[9] Q. Zhao and B.M. Sadler, "A Survey of Dynamic Spectrum Access," *IEEE Signal Processing Magazine*, vol. 24, no. 3, pp. 79–89, (May 2007).

[10] M. Nekovee, "Dynamic spectrum access - concepts and future architectures," *BT Technology Journal*, vol.24, no.2, pp. 111–116, (Apr. 2006).

[11] M. Nakagawa, K. Kawano, K. Kazuhiko and K. Murakami, "A Spectrum Assignment Method based on Genetic Algorithm in WiMAX/WiFi Integrated Network," *Proceedings of the 5th ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT2009)*, (Dec. 2009).

[12] W. Song and W. Zhuang, "Resource Allocation for Conversational, Streaming, and Interactive Services in Cellular/WLAN Interworking," *IEEE GLOBECOM '07*, pp. 4785–4789, (Nov. 2007).

[13] W. Song, W. Zhuang, and Y. Cheng, "Load Balancing for Cellular/WLAN Integrated Networks," *IEEE Network*, vol. 21, no. 1, pp. 27–33, (Jan.-Feb. 2007).

[14] L. Berlemann, C. Hoymann, G. R. Hiertz, S. Mangold, "Coexistence and Interworking of IEEE 802.16 and IEEE 802.11(e)," *Vehicular Technology Conference*, vol. 1, pp. 27–31, (May 2006).

[15] D. Niyato, E. Hossain, "Intergration of WiMAX and WiFi: Optimal Princing for Bandwidth Sharing," *IEEE Communications Magazine*, vol. 45, no. 5, pp. 140–146, (May 2007).

[16] O. lleri and N.B. Mandayam, "Dynamic Spectrum Access Models: Toward an Engineering Perspective in the Spectrum Debate," *IEEE Communications Magazine*, vol. 46, no. 1, pp. 153–160, (Jan. 2008).

[17] S. Hanaoka, J. Yamamoto and M. Yano, "Platform for Load Balancing and Throughput Enhancement with Cognitive Radio," *IEICE Transactions on Communications*, vol. E91–B, no. 8, pp. 2501–2508, (Aug. 2008).

[18] WiMAX Forum, "Mobile WiMAX - Part I: A Technical Overview and Performance Evaluation," http://www.wimax forum.org/technology/downloads/Mobile_WiMAX_Part1_Overview_and_Performance.pdf, (2006).

[19] ns-2, http://www.ise.edu/nsnam/ns/.

 ISBN: 978-1-61208-166-3

Research on Indoor Visible-Light Communications System with Carrier Interferometry OFDM

Xiaoming TAO
Dept. of Elec. Engr.,
Tsinghua University,
Beijing, 100084, P.R.China
taoxm@tsinghua.edu.cn

Zhengyuan XU
Dept. of Elec. Engr.,
Tsinghua University,
Beijing, 100084, P.R.China
xuzy@tsinghua.edu.cn

Jianhua LU
Dept. of Elec. Engr.,
Tsinghua University,
Beijing, 100084, P.R.China
lhh-dee@tsinghua.edu.cn

***Abstract*—In order to enhance the overall performance of the visible light communications system and to achieve the efficient use of spectrum resources, by leveraging the characteristic of channel frequency selection, we propose a novel visible light communications system based on Carrier Interferometry Orthogonal Frequency Division Multiplexing (CI-OFDM) transmission scheme. Through the frequency domain diversity, the system performance can be efficiently improved. At the same time, with a meticulous designed CI codes, the system Peak-Average Power Ratio (PAPR) can be effectively reduced. Analysis and simulation results demonstrate that, under the same Signal to Noise Ratio (SNR) condition, the proposed CI-OFDM scheme performs significantly better in BER than the traditional OFDM system, and greatly reduces the PAPR of the transmitted signal.**

***Index Terms*—Visible light communication; CI-OFDM; PAPR.**

I. INTRODUCTION

Wireless communication has become not only a pillar of the world high-tech industry, but also an essential part for global development of informationization. However, it still faces the problem of system capacity expansion under the existent technology, which contradicts with the explosive growth of the growing business demand [1]. Visible light communications will provide an effective way to address the above problem. The high-speed flashes of light and dark signals issued by the light-emitting diode, which transmit information, cannot be perceived by the naked eye but can be captured by the photoelectric detector device. Therefore, the data transmission can be supplied simultaneously with regular illumination. Furthermore, the visible light communication is immune from complicated electromagnetic interference to provide a very rich spectrum of resources (extra wide spectral band of approximately 375THz, 1THz = 1000GHz) for high-capacity communications services [2].

However, in the visible light communication system, in order to achieve better communication and illumination effects, and to prevent the ”shadow” being produced, it is common to arrange multiple Light Emitting Diode (LED) lights. Thus, the light pulses of signal can be overlapped in time and received by detectors through different transmission paths, resulting in the occurrence of Inter Symbol Interference (ISI), which requires an in-depth study of signal processing methods to overcome it. Multi-carrier Orthogonal Frequency Division Multiplexing (OFDM) technology modulates the high-speed serial data in parallel onto multiple orthogonal subcarriers to reduce the code rate and the impact of ISI. At the same time, a protection interval is inserted between each OFDM symbol to further eliminate the residual ISI [3]. However, the visible light OFDM system has its own inherent shortcomings. For example, without frequency diversity, the bit error rate is severely affected by the zero channel spectrum, and the Peak to Average Power Ratio (PAPR) is so large that the amplifier nonlinear problem is launched [4][5].

To further enhance the overall performance of visible light communication system, this paper introduces the Carrier Interferometry OFDM (CI-OFDM) modulation technology into the visible light communication systems. Different from the visible light OFDM scheme, in the CI-OFDM transmission, the data after the constellation mapping and the serial to parallel conversion is not just for their respective sub-carrier modulation, but is simultaneously transmitted on all sub-carriers. In order to enable the receiver to separate the different simultaneous transmitted data, all the data are multiplied by mutually orthogonal CI code during modulation. Research shows that, through the frequency domain diversity, the above transmission technology can on one hand effectively improve the visible light transmission quality, on the other hand, the CI code allows each data modulation is evenly staggered in the time-domain waveform, instead of as a random sum of multiple sinusoidal signals in the OFDM, which can effectively reduce the OFDM transmission signal PAPR. Therefore, CI-OFDM can be potentially applied as a multi-carrier transmission scheme in visible light communication system.

The rest of the paper is organized as follows: The system structure and principle are presented in Section 2. In Section 3, the performance analysis is performed. The simulation results of our system are showed in Section 4. Finally, the conclusion is drawn in Section 5.

II. SYSTEM STRUCTURE AND PRINCIPLE

A. CI Code and CI-OFDM

The concept of CI code was firstly proposed by Nassar, et al. in 1999 [6]. It was then regarded as a new multiple access technique and applied in the multi-carrier systems. The

 ISBN: 978-1-61208-166-3

CI code that is formulated by the row vectors of the Fourier matrix is given as

$$\mathbf{C}_N = [W_{i,k}]_{N\times N}, \tag{1}$$

where $W_{i,k} = \exp\left(\frac{2\pi\sqrt{-1}}{N}ik\right), 0 \le i,k \le N-1$, and each vectors of $\mathbf{C}_N$ is orthogonal with the others. The ith CI code word $\mathbf{c}_i (0 \le i \le N-1)$ is the ith row vector of $\mathbf{C}_N$, denoted as

$$\begin{aligned}\mathbf{c}_i &= \left(c_i^0, c_i^1, \cdots, c_i^{N-1}\right) \\ &= \left(W_{i,0}, W_{i,1}, \cdots, W_{i,N-1}\right).\end{aligned} \tag{2}$$

The basic idea of CI-OFDM is demonstrated in Fig.1. The transmitted symbol is firstly converted into N symbols in parallel. Each symbol is then extended onto a CI code sequence with the length of N, which is then modulated by N subcarriers. The CI code for each symbol is unique, and is orthogonal with all the others CI-codes. At the receiver, the orthogonality of the CI codes is utilized to demodulate each symbol.

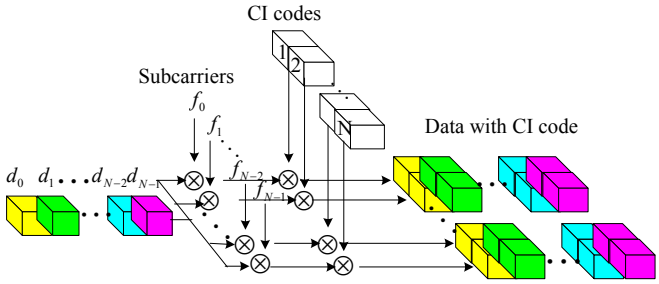


Fig. 1. Basic Idea of CI-OFDM

B. Visible-Light CI-OFDM Communication System

The baseband model of visible-light CI-OFDMA communication system is given in Fig.2. At the transceiver, the input bits are mapped into the constellation, which forms the data stream $d_1, d_2, \cdots$. Then the serial data stream is converted into parallel form, and data d_i is modulated by the Nth subcarrier. At the receiver, in order to separate N data transmitted simultaneously , each data d_i times the corresponding $\mathbf{c}_i$ during the modulation period and the complete CI-OFDM symbol is presented as $\sum_{i=0}^{N-1} d_i\mathbf{c}_i$. To mitigate the ISI caused by multi-path effect, the cyclic prefix(CP) is added and the CP should be longer than the delay spread of the multi-path channel. Finally, the discrete CI-OFDM symbol $s(n)$ is achieved by the serial-parallel conversion. During IM/DD visible-light transmission, proper direct component is usually needed to warrant a positive signal.

After transmitted in the optical channel $h(n)$, the CI-OFDM symbol received is given as

$$r(n) = \Re s(n) \otimes h(n) + w(n). \tag{3}$$

$w(n)$ is the additive white Gaussian noise(AWGN), $\Re$ is the efficiency of photoelectric detection, and $\otimes$ means convolution.

At the receiver of the system, PD receives the light signals transmitted by the white-light LED and converts it into electrical signals. After the serial-parallel conversion, the CP is eliminated. Each subcarrier is then compensated for the channel and the phase offsets, and finally all the estimation values are combined. In Fig.2, ω_k denotes the weight of the kth subcarrier, and it is determined by the combination scheme. For the MMSE combination, for instance,

$$\omega_k = \frac{A\alpha_k}{{\alpha_k}^2 + \sigma^2}, \tag{4}$$

where A is a constant representing the normalized energy per bit; α_k is the amplitude of the channel for subcarrier k; and σ^2 is the variance of the noise.

III. Performance Analysis

A. Bit Error Rate (BER) Analysis

The CI code of data d_i is expressed as equation (2), and then the received signals for the visible-light CI-OFDM system in the frequency selective fading scenario is formulated as

$$\begin{aligned}r(t) = \mathrm{Re}\Bigg[\sum_{l=0}^{N-1}\sum_{k=0}^{N-1} E_b \cdot \alpha_k(t) \cdot d_l \cdot c_l^k \cdot p(t) \cdot \\ e^{j(2\pi f_k t + \theta_k(t))}\Bigg] + n(t).\end{aligned} \tag{5}$$

The constant E_b is the normalized energy per bit. The frequency f_k is defined as $f_k = f_c + k/T_s$, where T_s is the period per symbol. $p(t)$ is a rectangular pulse during $[0, T_s]$. α_k and θ_k are the altitude and phase of the channel response for the kth subcarrier respectively. $n(t)$ is the AWGN with a mean of zero and a power spectrum density of $N_0/2$.

When the demodulation and combination are completed at the receiver of the visible-light CI-OFDM system, the obtained variable to be determined for d_i is

$$\begin{aligned}\xi_i &= \sum_{m=0}^{N-1}\sum_{l=0}^{N-1}\sum_{k=0}^{N-1} \omega_m E_b d_l c_l^k \left(c_l^k\right)^* \rho_{k,m} + \sum_{m=0}^{N-1}\omega_m \cdot n_m \\ &= S + I_{OS} + I_{SO} + I_{ICI} + \eta,\end{aligned} \tag{6}$$

where

$$\rho_{k,m} = \frac{1}{T_s}\int_0^{T_s} \alpha_k \cos\left[2\pi\left(f_k - f_m - \varepsilon\right)t + \theta_k - \widehat{\theta}_m\right] dt. \tag{7}$$

In (7), ε is a constant and it stands for the frequency offset. $\widehat{\theta}$ is the estimation of the phase. In (6), the weight for combination of the mth subcarrier is ω_m, and it is determined by the combination scheme. $\eta = \sum_{m=0}^{N-1}\omega_m \cdot n_m$ denotes noise, while S is the desired signal. The interferences I_{OS}, I_{SO}, and I_{ICI} are the interference from other users on the same subcarrier, the interference brought about by other subcarriers, and the interference caused by different data transmitted on different subcarriers respectively.

When $l = i$ and $k = m$, S is given as

$$S = Ad_i \cdot \frac{\sin(\pi N\overline{\varepsilon})}{\pi N\overline{\varepsilon}} \sum_{m=0}^{N-1}\omega_m\alpha_m, \tag{8}$$

 ISBN: 978-1-61208-166-3

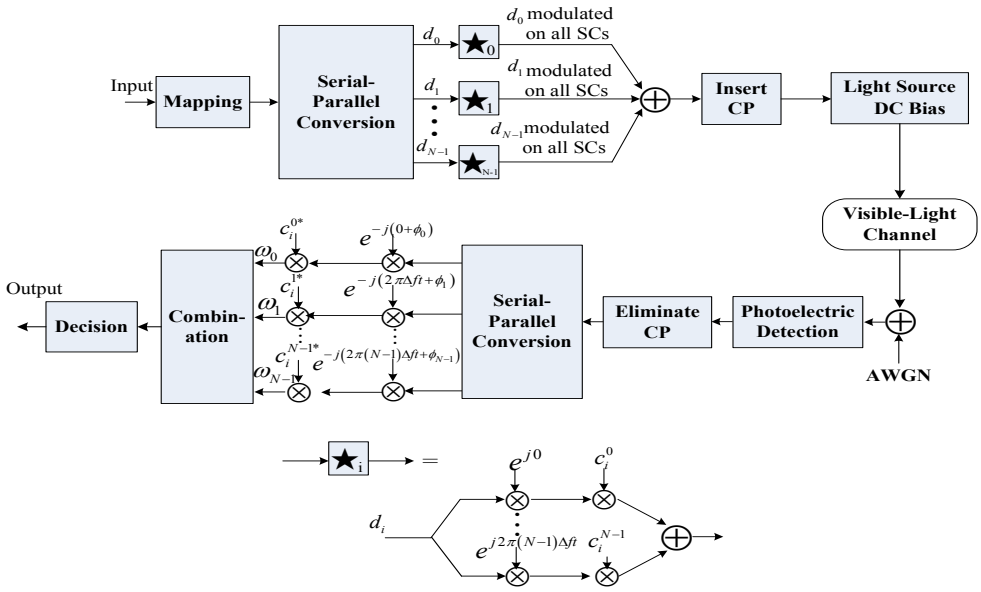


Fig. 2. The baseband model of visible-light CI-OFDM communication system

where $\overline{\varepsilon}$ is the normalized frequency offset throughout the whole band and the estimation of the phase is got by $\widehat{\theta_k} = -\pi N\overline{\varepsilon} + \theta_k \bmod 2\pi$.

When $l \neq i$ and $k = m$, I_{OS} is given as

$$I_{OS} = E_b \frac{\sin(\pi N\overline{\varepsilon})}{\pi N\overline{\varepsilon}} \sum_{l=0,l\neq i}^{N-1} \sum_{m=0}^{N-1} d_l \omega_m \alpha_m c_l^m (c_l^m)^*. \quad (9)$$

When $l = i$ and $k \neq m$, I_{SO} is given as

$$I_{SO} = E_b d_i \cdot \sum_{m=0}^{N-1} \sum_{k=0,k\neq m}^{N-1} \omega_m \alpha_k c_l^m (c_l^m)^* \zeta_{m,k}. \quad (10)$$

where

$$\zeta_{m,k} = \frac{\sin(\pi N\overline{\varepsilon})}{\pi(m-k+N\overline{\varepsilon})} \cos(\theta_m - \theta_k). \quad (11)$$

When $l \neq i$ and $k \neq m$, I_{ICI} is given as

$$I_{ICI} = E_b \sum_{l=0,l\neq i}^{N-1} d_l \sum_{m=0}^{N-1} \sum_{k=0,k\neq m}^{N-1} \omega_m \alpha_k c_l^m (c_l^m)^* \zeta_{m,k}. \quad (12)$$

Afterward, the signal to interference and noise ratio (SINR) is given as

$$SINR = \frac{P_S}{P_{OS} + P_{SO} + P_{ICI} + P_\eta}. \quad (13)$$

Here P_S, P_{OS}, P_{SO}, P_{ICI} and P_η are power for S, I_{OS}, I_{SO}, I_{ICI} and the noise η. According to the Gaussian approximation, the BER is readily given as

$$Pe = \int_0^\infty Q\left(\sqrt{SINR}\right) p(SINR)\, d(SINR). \quad (14)$$

B. Peak-to-Average Power Ratio (PAPR) Analysis

In this section, the PAPR of visible-light CI-OFDM system is analyzed. Without loss of generality, let $E_b = \frac{1}{\sqrt{N}}$, and the equivalent baseband form for the transmitted signals in one OFDM symbol period is achieved by

$$s(t) = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \sum_{k=0}^{N-1} d_l \cdot c_l^k \cdot e^{j2\pi kt/T_s}. \quad (15)$$

According to **[?]**, the average power of $S(t)$ is N, which means $\mathbf{E}\left[|s(t)|^2\right] = \mathrm{N}$ (**E** means the mathematical expectation), and the instantaneous power of $s(t)$ can be expressed as

$$|s(t)|^2 = N + \frac{2}{N}\mathrm{Re}\left\{ \sum_{k=1}^{N-1} \left(\sum_{l=0}^{N-1} R_l[k] + \sum_{l=0}^{N-1} \sum_{l'=0,l'\neq l}^{N-1} d_l (d_{l'})^* Z_{l,l'}[k] \right) e^{j2\pi kt/T_s} \right\}, \quad (16)$$

where

$$R_l[k] = \sum_{m=0}^{N-k-1} c_l^m \left(c_l^{m+k}\right)^*, \quad (17)$$

$$Z_{l,l'}[k] = \sum_{m=0}^{N-k-1} c_l^m \left(c_{l'}^{m+k}\right)^*. \quad (18)$$

$R_l[k]$ is defined as the partial autocorrelation function of the lth CI code, while $Z_{l,l'}[k]$ is the partial cross-correlation function for the lth and the l'th spread spectrum code.

As for (16), the envelop of the CI-OFDM transmitted signal is determined by $R_l[k]$, $Z_{l,l'}[k]$ and information sequence d_l. According to the definition of PAPR, we use P to stands for

 ISBN: 978-1-61208-166-3

the PAPR, and it is given as

$$P = \frac{\max\limits_{0\le t\le T_s}|s(t)|^2}{\mathrm{E}\left[|s(t)|^2\right]} = \frac{\max\limits_{0\le t\le T_s}|s(t)|^2}{N} = \max_{0\le t\le T_s}\left[1+\frac{2}{N^2}\mathrm{Re}\left\{\sum_{k=1}^{N-1}\left(\sum_{l=0}^{N-1}R_l\left[k\right]+\sum_{l=0}^{N-1}\sum_{l'=0,l'\neq l}^{N-1}d_l(d_{l'})^*Z_{l,l'}\left[k\right]\right)e^{j2\pi kt/T_s}\right\}\right] \tag{19}$$

Due to the orthogonality among different CI codes, we have

$$\sum_{l=0}^{N-1}R_l\left[k\right] = \sum_{l=0}^{N-1}\sum_{m=0}^{N-k-1}c_l^m\left(c_l^{m+k}\right)^* = \sum_{m=0}^{N-k-1}\sum_{l=0}^{N-1}c_l^m\left(c_l^{m+k}\right)^* = 0 \tag{20}$$

which means the PAPR of CI-OFDMA is determined only by the partial cross-correlation function and the information sequence. With BPSK being utilized, $d_l \in \{-1, 1\}$, and the upper bound of PAPR is further given as

$$\begin{aligned} P &= 1+\frac{2}{N^2}\max_{0\le t\le T_s}\mathrm{Re}\left\{\sum_{k=1}^{N-1}\sum_{l=0}^{N-1}\sum_{l'=0,l'\neq l}^{N-1}d_l(d_{l'})^*\cdot Z_{l,l'}\left[k\right]e^{j2\pi kt/T_s}\right\} \\ &\le 1+\frac{2}{N^2}\max_{0\le t\le T_s}\left|\sum_{k=1}^{N-1}\sum_{l=0}^{N-1}\sum_{l'=0,l'\neq l}^{N-1}d_l(d_{l'})^*Z_{l,l'}\left[k\right]e^{j2\pi kt/T_s}\right| \\ &\le 1+\frac{2}{N^2}\max_{0\le t\le T_s}\sum_{k=1}^{N-1}\left|\sum_{l=0}^{N-1}\sum_{l'=0,l'\neq l}^{N-1}d_l(d_{l'})^*Z_{l,l'}\left[k\right]\right| \\ &\le 1+\frac{2}{N^2}\max_{0\le t\le T_s}\sum_{k=1}^{N-1}\sum_{l=0}^{N-1}\sum_{l'=0,l'\neq l}^{N-1}\left|Z_{l,l'}\left[k\right]\right| = Q \end{aligned} \tag{21}$$

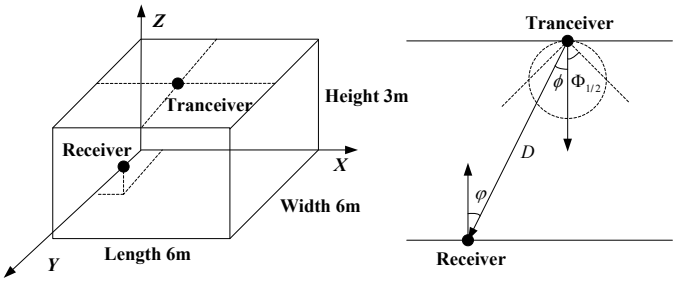
On the basis of the partial cross-correlation function, the equation (21) gives out the upper bound Q for the PAPR using BPSK modulation.

IV. Simulation Results

The visible-light communication is a new type of wireless communication approach, and hence measuring and modeling its channel model is still under investigation. Therefore, there is no such multi-path wireless channel model that is universally acknowledged internationally. On the consideration that the modeling of the channel is not the key point of this paper, we adopt the channel model used in [7]. In such a model, the simulation is carried out in a room with the length of 6m, width of 6m and height of 3m. The coordinators of the transceiver and the receiver are (3,3,3) and (1,3,1) respectively. This scenario is given in Fig.3.

As for this scenario, [7] achieved the impulse response for the multi-path channel via the combination of computer simulation and physical concepts. The impulse response is given as

$$h\left(t\right) = 5.8H\left(0\right)\left(\frac{11.0561\tau_{rms}}{t+11.0561\tau_{rms}}\right)^6 u\left(t\right)\cdot \tag{22}$$



a) Simulation Scenario b) Channel Model for Transmission

Fig. 3. Simulation scenario and optical channel model for transmission

$H\left(0\right)$ is a DC gain for the line-of-sight(LOS) link, and it is calculated as

$$H\left(0\right) = \begin{cases} \frac{(m+1)A}{2\pi D^2}\cos^m\left(\phi\right)T_s\left(\varphi\right)g\left(\varphi\right)\cos\left(\varphi\right), & 0\le\varphi\le\psi_c \\ 0, & \varphi>\psi_c \end{cases} \tag{23}$$

where A is the receiving area for the photoelectric detector. D is the distance between the transceiver and the receiver. ϕ is the emission angle, while φ is the incidence angle. $T_s\left(\varphi\right)$ is the gain for the optical filter and $g\left(\varphi\right)$ is the gain for optical concentrator. ψ_c is the FOV of the receiver. $m = -\frac{\ln 2}{\ln\cos\Phi_{1/2}}$ is the radiation mode of the light source, and $\Phi_{1/2}$ is named the half-angle of the transmission power. The simulation parameters is given in table 1.

TABLE I
System Parameters for Simulation

Parameters	Values
Central lightening power of LED	30mW
FOV of the receiver)	60°
Half-angle of the transmission power	60°
Area of the photoelectric detector	$1\mathrm{cm}^2$
Refractive index of the optical concentrator	1.5
Efficiency of the photoelectric detector	0.5(A/W)
Reflection index of the reflection plane	0.8
Room size (length×width×height)	6m×6m×3m
Transceiver coordinator	(3,3,3)
Receiver coordinator	(1,3,1)
Number of subcarriers	128

Fig.4 gives the comparison of the BER between visible-light CI-OFDM and visible-light OFDM using MMSE combination and BPSK modulation. Simulation results show that, the performance of CI-OFDM outperforms OFDM obviously. For instance, for the required BER of 10^{-3}, visible-light CI-OFDM has a gain of 1dB concerning SNR.

In the CI-OFDM system, CI-codes make the peaks of signal waves staggered from each other in time domain. This is quite different from OFDM whose symbol is the sum of many stochastic sine waves and solve the PAPR problem in OFDM systems. Fig.5 plots the PAPR distribution of the white-light signal for both OFDM and CI-OFDM systems. From the

 ISBN: 978-1-61208-166-3

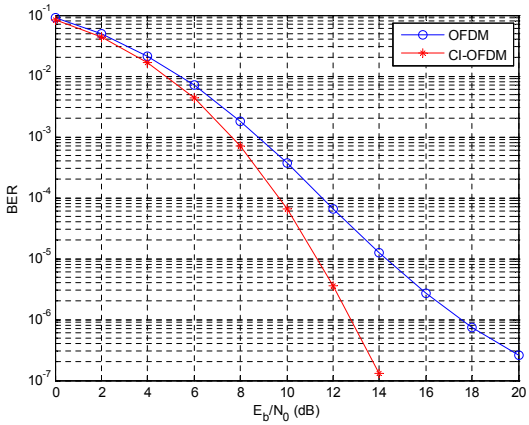
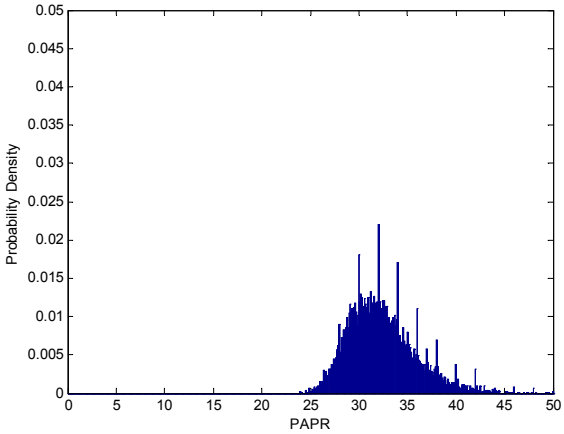
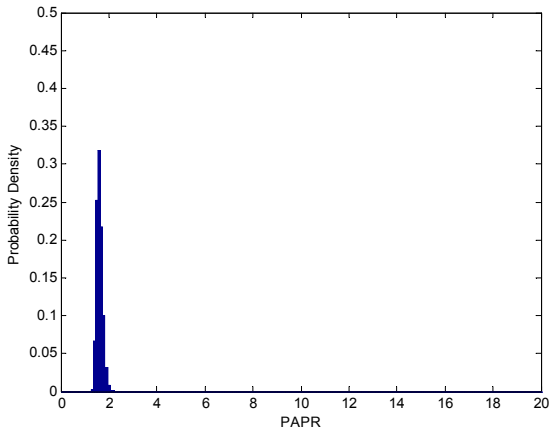


Fig. 4. BER performance of visible-light CI-OFDM and OFDM systems

results, it can be seen that the visible-light CI-OFDM can obviously reduce the PAPR of OFDM systems.



(a) PAPR distraibution of the white-light signal in OFDM system



(b) PAPR distraibution of the white-light signal in CI-OFDM system

Fig. 5. PAPR performance of visible-light CI-OFDM and OFDM systems

V. Conclusion

In this paper, we propose a visible-light communication system and corresponding transmission scheme based on CI-OFDM, which can function as an effective technique enhancing the performance of visible-light communication system. Simulation results show that for a required BER of 10^{-3} in the frequency selective channel, the visible-light CI-OFDM can yield 1dB gain of SNR. Simultaneously, this method can effectively reduce PAPR with the help of CI codes.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (No. 61101071) and China Post-doctoral Science Foundation (No. 20100470332).

References

[1] A. Goldsmith, S. A. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of MIMO channels," IEEE Journal on Selected Areas in Communications, Vol. 21(5), pp. 684-702, 2003.

[2] G. Pang, Ka-Lim Ho, T. Kwan, and E. Yang, "Visible light communication for audio systems," IEEE Transactions on Consumer Electronics, Vol. 45(4), pp. 1112-1118, 1999.

[3] Geoffrey Li and Gordon L. Stber, Orthogonal Frequency Division Multiplexing for Wireless Communication. School of Electrical and Computer Engineering, USA, 2006, pp. 18-21.

[4] Y. Wang, X. F. Tao, P. Zhang, J. Xu, X. Q. Wang, and T. Suzuki, "MIMO-OFDM PAPR Reduction by Combining Shifting and Inversion with Matrix Transform," IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, 2007, pp. 1-5.

[5] D. A. Wiegandt, C. R. Nassar, and Zhiqiang Wu, "Overcoming peak-to-average power ratio issues in OFDM via carrier-interferometry codes," IEEE VTS 54th Vehicular Technology Conference, 2001. VTC 2001 Fall, pp. 660-663.

[6] C. R. Nassar, B. Natarajan, and S. Shattil, "Introduction of carrier interference to spread spectrum multiple access," Wireless Communications and Systems, 2000. 1999 Emerging Technologies Symposium, pp. 41-45.

[7] L. Jiang, Research on Indoor Visible-Light Communication Based on Adaptive OFDM [D], Changchun University of Science and Technology, 2010.

 ISBN: 978-1-61208-166-3

A Distributed Group Rekeying Scheme for Wireless Sensor Networks

Seyed Hossein Nikounia, Amir Hossein Jahangir
Department of Computer Engineering
Sharif University of Technology
Tehran, Iran
nikoonia@ce.sharif.ir, jahangir@sharif.ir

Vanesa Daza
Department of Information and Communication Technologies
Pompeu Fabra University
Barcelona, Spain
vanesa.daza@upf.edu

***Abstract*—In applications that require group communication and clustering, there is usually a single key for all members of the group. This key should be updated in order to support dynamic nature of the groups and also to handle possible node compromise attack. In this paper, we propose a new distributed group rekeying scheme with t-revocation capability that is based on local collaboration of group members. Our proposed scheme provides t-wise backward and forward secrecy. It can be used with any key size. This scheme, in contrast to centralized schemes, does not require a centralized rekeying server, so the rekeying process is handled locally in the group itself and the communication overhead is reduced. The security of this scheme is analyzed. We have also implemented our proposal for TinyOS and have used Avrora to simulate the compiled binary for MICA2 motes. Simulation results show that compared to the only published distributed scheme, our scheme consumes less energy and has lower communication overhead.**

Keywords-Security; Key Management; Group Rekeying; Wireless Sensor Networks.

I. INTRODUCTION

Wireless sensor networks consist of many small low-cost and low-power nodes that sense their environment, process data, and communicate through wireless links [1]. These networks are often deployed in adverse or even hostile environments. Nodes are resource-constrained and they are often deployed in unattended manner. Due to cost limitations, it is not practical to use tamper-proof hardware for all nodes. Hence, an adversary can mount a physical attack on a node and read, probably secret, data from its memory. These issues make providing security services a challenging task.

Grouping is a technique to do localized computation and to reduce communication overhead in wireless sensor networks. The most common grouping technique is clustering. Cluster head usually do coordination and some aggregation to send the results back to the sink.

There is usually a group-wide key, called the *group key*, shared between group members. When a node become compromised, we remove the compromised node by not revealing the new group key to that node. The process of renewing the group key is called *group rekeying*. This is also referred to as *group key revocation* in some literature.

In this paper, we review the existing schemes for group rekeying. We propose a new group rekeying scheme which is not based on a centralized rekeying server. We have compared our proposed scheme with other group rekeying schemes using various performance parameters including communication and computation overhead.

The rest of this paper is organized as follows. Section I-A presents preliminaries including notations and definitions as well as description of Shamir's secret sharing scheme. Section II reviews existing techniques for group rekeying in sensor networks. In Section III, we describe our proposed scheme. Sections IV and V presents simulation results and performance analysis, respectively. We compare our proposed scheme with a distributed scheme in Section VI. Finally, this paper ends with conclusions in Section VII.

A. Goals

The general goal is to develop an efficient and unconditionally secure rekeying scheme for wireless sensor networks. This scheme should be able to tolerate node compromise.

Due to hardware constraints of sensor nodes, the harsh environments in which sensor networks are often deployed and also security requirements, a suitable rekeying scheme should provide:

- t-revocation capability (See Definition 1).
- t-wise forward secrecy (See Definition 2).
- t-wise backward secrecy (See Definition 2).
- On-demand rekeying: a suitable scheme should provide a mechanism for revoking a compromised node from the group on-demand.
- and also low communication, computation and low storage overhead.

In this section, we define some notations and definitions for our proposed scheme. We also describe Shamir's Secret Sharing scheme. The idea of Shamir's secret sharing scheme is usually used in group rekeying schemes.

B. Notations and Definitions

We assume a group of n sensor nodes, deployed closely to each other within a large scale sensor network. A group consists of $n-1$ group members and one group controller.

 ISBN: 978-1-61208-166-3

The group controller is responsible for the management of the group. Each group member has an ID $i > 0$, and a secret key shared with the group controller. There is a group key K shared with all group members. They use this key to get confidentiality and/or integrity of their communication.

When needed, the group controller uses a rekeying scheme to update K. Let us call the j-th group key (group key of session j) K_j. Each node stores a personal secret. Node i, stores S_i as its personal secret. S_i is used in the rekeying process. This secret is known only by the node itself.

The group controller renew the current group key when, for example, a node become compromised. Hence, the rekeying mechanism should have the ability not to reveal the new group key to the compromised nodes.

In a rekeying event, there might be w nodes that should be revoked (i.e., the new group key should not be revealed to these nodes). After the rekeying process, those nodes are no more members of the group.

There are mainly three pieces of information that are used in the rekeying process:

- The personal secrets, S_i, that every sensor hold.
- Rekeying materials that should not be revealed and are used by the group controller (or the rekeying server) to compute a broadcast message.
- The broadcast message. Group members use this message plus S_i to compute the new group key.

There are three types of actors:

- Group controller which acts like a coordinator in a rekeying event.
- Group members $\mathcal{U} = \{U_1, \ldots, U_n\}$, which are the group of sensonr nodes. When a member is not accepted to be part of the group anymore, it is called revoked.
- Network manager is a person who initialize the nodes offline (i.e., before deployment)

Please note that we are assuming an adversary that can do the node compromise attack and the network IDS is capable of detecting it. The attacker can also eavesdrop the wireless communications. To further clarify our goals, we give the following definitions.

To further clarify our goals, we give the following definitions.

Definition 1. *(Group rekeying with revocation capability) Let $t, i \in \{1, \ldots, n\}$ and p be a prime number. In a group rekeying Ξ, the group controller seeks to establish a new $K \in \mathbb{F}_p$ with each group member U_i through a broadcast message and some personal information S_i it owns. In detail:*

1) *Ξ is a group rekeying scheme if*
   a) *For any group member U_i, K is determined by S_i and B.*
   b) *For any set $M \subset \mathcal{U}$, $|M| \leq t$, and any $U_i \notin M$, the members in M are not able to learn anything about S_i.*
   c) *No information is leaked from either the broadcast message or the S_i alone.*
2) *Ξ has t-revocation capability if given any set of revoked group members $R \subset \mathcal{U}$ such that $|R| \leq t$, the group controller can generate a broadcast message B such that $U_i \notin R$, U_i can recover K but the revoked group members cannot recover K.*

Definition 2. *(t-wise backward and forward secrecy) Let $t, i \in \{1, ..., n\}$, $j \in \{1, ..., m\}$ and $K_j \in \mathbb{F}_p$ be the group key of session j.*

1) *A rekeying scheme guarantees t-wise forward secrecy if for any set $R \subseteq \{U_1, ..., U_n\}$, where $|R| \leq t$ and all $U_i \in R$ are revoked before session j, the members in R together cannot get any information about K_j, even with the knowledge of group keys before session j.*
2) *A rekeying scheme guarantees t-wise backward secrecy if for any set $R \subseteq \{U_1, ..., U_n\}$, where $|R| \leq t$ and all $U_i \in R$ joined after session j, the members in R together cannot get any information about K_j, even with the knowledge of group keys after session j.*

Similar definitions are also used in [2].

C. Shamir's Secret Sharing Scheme

The idea of Shamir's secret sharing scheme is usually used in group rekeying schemes. It is used in our scheme as well. The goal is to share a secret S between n people so that $t + 1$ (or more) of them can recover S. For this purpose, a random t-degree polynomial in which $S = P(0)$ is generated. This polynomial is evaluated over $\mathbb{F}_p$, where p greater than n. $P(i)$ is given to person $i > 0$ as his/her share. Now, $t + 1$ (or more) person can recover the original polynomial, and hence S. But having less than $t + 1$ shares do not give any information about S. See Theorem 1.

Theorem 1. *Suppose the opponent knows t shares of this polynomial. For each candidate value $S' \in [0, p-1]$ he can construct one and only one polynomial $P'(x)$ of degree t such that it satisfies conditions of shares and also $P'(0) = S'$.*

By construction, these p possible polynomials are equally likely, and thus there is absolutely nothing the opponent can deduce about the real value of S.

Proof: Refer to [3] for the proof. ■

II. Related Work

Mainly, there are two categories of schemes for group rekeying in sensor networks: there are some distributed schemes which do not rely on a rekeying server and there are some centralized schemes which require a rekeying server

to construct the broadcast message. It is assumed that the rekeying server is secured and could not be compromised. Here we review both distributed and centralized schemes, but before that let us review some basic methods of sharing a secret to only legitimate members that are used in some of the schemes described later.

A. Underlying Methods

In this section, we review some general solutions to the problem of revealing a secret to non-revoked group members. These solutions are underlying method for most of the group rekeying schemes for wireless sensor networks.

1) Method 0 (Naive): Every group member should have a secret key shared with the group controller. The group controller can encrypt K_j with this secret key for each member and send the message to the appropriate member. The communication overhead of this scheme is $O(n)$ where n is the number of group members.

2) Method 1: In this scheme, each member has an ID $i > 0$. A t-degree random polynomial $P(x)$ which is evaluated over $\mathbb{F}_p$ (p is prime) is constructed and shares of it (i.e., $P(i)$) are pre-distributed to group members. The secret to be revealed is $K = P(0)$.

Suppose that $w = t$. The group controller reveals shares of revoked members. At this point, every non-revoked group members have $t + 1$ shares and can recover the original polynomial so non-revoked group members can evaluate $K = P(0)$.

This scheme has been proposed in [4]. It can also be used for $w < t$ if the group controller reveals shares of w revoked-members plus shares of arbitrarily selected $w - t$ dummy members.

3) Method 2: In [2], the group controller randomly picks a $2t$-degree masking polynomial $h(x) = h_0 + h_1x + ... + h_{2t}x^{2t}$ over a finite field $\mathbb{F}_p$ where p is prime. Each group member i gets its personal secret $S_i = h(i)$ from the group controller.

Given a set of revoked group members $R = \{r_1, r_2, ..., r_w\}, w \leq t$, the group controller randomly picks a t-degree polynomial $p(x)$ and constructs $q(x) = K - p(x)$. Then the controller distributes the shares of the t-degree polynomials $p(x)$ and $q(x)$ to non-revoked sensors using the following broadcast message:

$$\begin{aligned} B = \{R\} \\ \cup\{P(x) = g(x)p(x) + h(x)\} \\ \cup\{Q(x) = g(x)q(x) + h(x)\} \end{aligned}$$

where $g(x) = (x - r_1)(x - r_2)...(x - r_w)$. If any non-revoked group member i receives such a broadcast message, it evaluates polynomials $P(x)$ and $Q(x)$ at point i. and gets $P(i) = g(i)p(i) + h(i)$ and $Q(i) = g(i)q(i) + h(i)$.

Because member i knows $h(i)$ and $g(i) \neq 0$, it can compute $p(i) = \frac{P(i)-h(i)}{g(i)}$ and $q(i) = \frac{Q(i)-h(i)}{g(i)}$. Member i can then compute the new group key $K = p(i) + q(i)$. The revoked members (which are not member of the group anymore) cannot compute K because $g(i) = 0, \forall i$ revoked.

As it is proved in [2], this schemes is unconditionally secure rekeying scheme with t-revocation capability. It also provides t-wise backward and forward secrecy.

B. Distributed Schemes

In [5], a group rekeying protocol has been proposed. In this protocol, rekeying materials are preloaded into each node. Each member distributes encrypted shares of its rekeying materials to other nodes which will be returned back to the node in a rekeying event. There is also some improvements to their basic protocol, B-PCGR, which improves its security. To the best of our knowledge, this is the only published distributed group rekeying scheme for sensor networks.

C. Centralized Schemes

In [6], Danio and Savio have proposed a group key revocation protocol for wireless sensor networks that has communication overhead of $O(\log n)$, instead of $O(n)$ in naive scheme (see Subsection II-A1). This protocol also provides a lightweight key authentication using one-way hash chains. In this protocol, each node has a symmetric key shared with the keying server. They have proposed to use a (binary) tree of hash chains. Leaves are assigned to group members and each group member has the current key in the hash chain of the nodes which are in the path between this leaf and the root.

Authors have shown that using this structure, the number of messages are reduced to $O(\log n)$ but some of the messages should be sent to more than one member. But the drawback of this scheme is that it does not provide backward secrecy and that is due to the use of hash chains of keys.

In [7], a self-healing group key revocation has been proposed. In this protocol, lifetime of the group is divided into some intervals and nodes can authenticate the new group key using a dual hash chain. There is no communication overhead for revocation and it can tolerate rekeying message loss (the self-healing property of this scheme).

But there are some drawbacks. The revocation could not be done on-demand, network manager should plan for the revocation time in advance. And also there is an implicit assumption that the adversary is not able to compromise group nodes and hence, could not read the keying materials in their memory.

Another protocol for updating group key has been proposed in [8]. They adapt the secret-sharing revocation scheme that is explained in Subsection II-A2 for sensor networks by reducing the computation overhead. A centralized group rekeying scheme has been proposed in [9]. The underlying rekeying scheme is very similar to Method 2 (see Subsection II-A3) that is also used in [10].

 ISBN: 978-1-61208-166-3

D. Motivation

While centralized schemes require a secured rekeying server and also a secure connection between the group controller and the rekeying server, the only published distributed scheme [5] has a large communication overhead.

A secured rekeying server might not be applicable for some applications in which the network is being deployed in adverse environments. In addition to computation and communication overhead of the aforementioned distributed scheme, it has another drawback. In order to provide t-revocation capability, the underlying IDS should provide each group member with the information of compromised nodes.

We propose to distribute shares of required materials for a rekeying event (which are stored in the rekeying server in centralized solutions) between group members using a method inspired by [5]. The group controller uses these shares and constructs a broadcast message similar to [2] (see Subsection II-A3). In this scheme, a rekeying server is not required and as we show in the following sections, the energy consumption of the proposed scheme is less than [5].

III. A New Group Rekeying Scheme

In this section, we describe our proposed group rekeying scheme for wireless sensor networks. The goal is to build a distributed group rekeying scheme with t-wise backward and forward secrecy without the need of a secured rekeying server. A group consists of $n-1$ group members and one group controller. Let $R = \{r_1, r_2, ..., r_w\}$ be the set of group members to be revoked in rekeying event j.

In this scheme, shares of required rekeying materials are pre-distributed between group nodes. In a rekeying event, they deliver their shares to the group controller and the group controller uses these shares to compute the broadcast message. Group members renew the group key using this message. Note that all polynomials are evaluated over $\mathbb{F}_p$ where p is prime. In this scheme, $t < n$, $1 \leq \lambda \leq 2t$ and $\mu \geq t$ are system parameters. $\mu \leq n$ is assumed. We'll discus how to choose these parameters later.

A. Details

The initialization process is as follows. These operations are done offline by the network manager:

1) Generate the random polynomial $h(x, y)$. The degree of x and y are $2t$ and λ, respectively.
2) Generate the random polynomial $e(x, y, u)$. The degree of x, y and u are $2t$, λ and μ, respectively and $t \leq \mu \leq 2t$.
3) Let $h'(x, y)$ be a polynomial defined as $h'(x, y) = h(x, y) + e(x, y, 0)$;
4) Then $h(i, y)$ and $e(x, y, i)$ are predistributed (or sent by the sink) to group member i. Actually, $\lambda+1$ group members should have $e(x, y, i)$, but for the sake of fault tolerance, we may distribute to more than $\lambda + 1$ members. Note that $h(i, y)$ and $e(x, y, i)$ are one and two variate polynomials, respectively. They are the result of evaluation of polynomials h and e for each group member i.
5) $h'(x, y)$ is kept by the group controller.

The j-th rekeying process (revealing j-th group key, K_j) is as follows:

1) The group controller sends a request to $\mu + 1$ group members for sending their shares of e. Note that we've assumed $\mu \leq n$.
2) They send back $e(x, j, i)$ to the group controller, where i is the ID of the member. To prevent eavesdropping, encryption might be used in this step. Shares can be encrypted with a pairwise key between group member i and the group controller. In this case, any encryption scheme might be used. Based on the used encryption algorithm and key length, group members and the group controller consume energy for this process.
3) As the group controller receives shares, it follows the steps:
   - The group controller constructs $e(x, j, u)$ by solving $\mu+1$ $(\mu+1)$-variable linear equations. It then computes $h(x, j) = h'(x, j) - e(x, j, 0)$.
   - Let $g(x) = (x - r_1)(x - r_2)...(x - r_w)$; Generate a t-degree random polynomial $p(x)$;
   - Let $q(x) = K_j - p(x)$. Broadcast the following message to the group members:

$$\begin{aligned} B = \{R\} \\ \cup\{P(x) = g(x)p(x) + h(x, j)\} \\ \cup\{Q(x) = g(x)q(x) + h(x, j)\} \end{aligned}$$

4) Non-revoked group member i could evaluate polynomials $P(x)$ and $Q(x)$ at point i, and gets $P(i) = g(i)p(i) + h(i, j)$ and $Q(i) = g(i)q(i) + h(i, j)$. Since for non-revoked group members $g(i) \neq 0$, they can compute $p(i) = \frac{P(i)-h(i,j)}{g(i)}$ and $q(i) = \frac{Q(i)-h(i,j)}{g(i)}$. The new group key is $K_j = p(i) + q(i)$.

B. Example

Here's a simple example of our proposed scheme with four group members and one group controller. We assumed $t = \lambda = \mu = 2$. Figure 1 shows their location. From the initialization process (See Figure 2), group member i has $h(i, y)$ and $e(x, y, i)$ and the group controller has $h'(x, y)$. Assume that in $7th$ rekeing member 4 is the one to be removed; That is $R = \{4\}$. Group controller asks non-revoked members to send their shares. Member i sends back $e(x, 7, i)$ (See Figure 3). As in Figure 4 Group controller computes the broadcast message B and broadcast it to all members (See Figure 5). Non-revoked members (i.e.,

member 1, 2 and 3) can get the new group key K_7 while revoked member 4 cannot (See Figure 6).

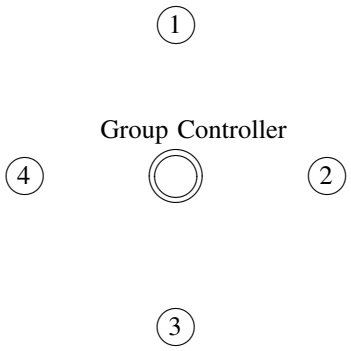


Figure 1. Location of a group controller and 4 group members

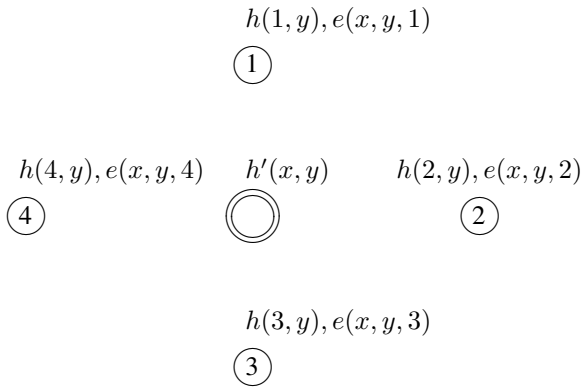


Figure 2. After initialization process; group member i has $h(i,y)$ and $e(x,y,i)$ and the group controller has $h'(x,y)$.

C. How to Choose System Parameters

This scheme can handle up to t revocations in one rekeying event. In order to compromise the whole group, an adversary should compromise the group controller plus $\mu+1$ (or more) group members. In order to guarantee t-wise backward and forward secrecy, $t \leq \mu$ should be considered.

Having larger μ does not straighten backward and forward secrecy. However it makes it harder for the adversary to compromise e polynomial. The adversary should capture $\mu+1$ group members in addition to the group controller.

Group members do not reveal their original share to the group controller. Instead, they send a *session share* for that specific session. Although they send it encrypted, in order to enhance the security of this scheme, we put a constrain

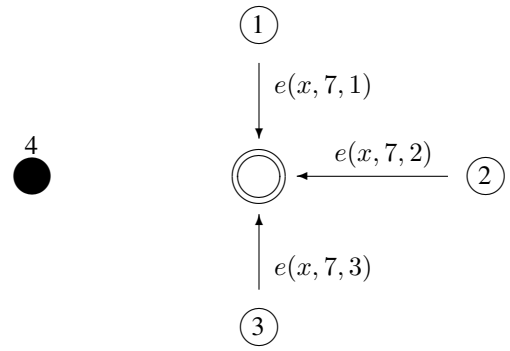


Figure 3. 7th rekeying: Group members sending their shares to the group controller; Member 4 to be revoked; In other word $R = \{4\}$

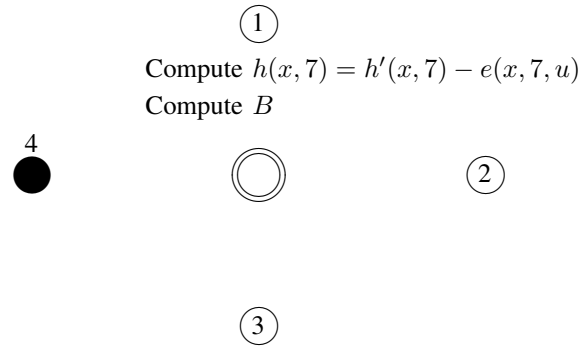


Figure 4. 7th rekeying: Group controller receives shares and compute $h(x,7)$ and the broadcast message B.

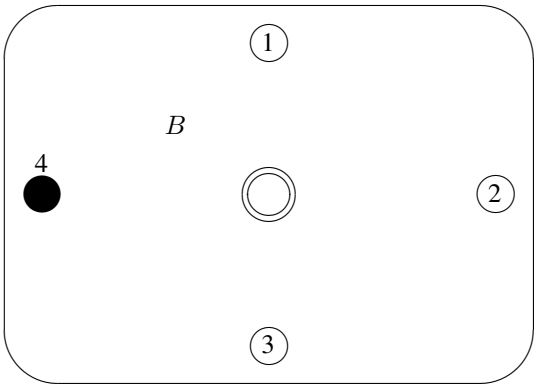


Figure 5. 7th rekeying: Group controller broadcast B; Anyone can receive B.

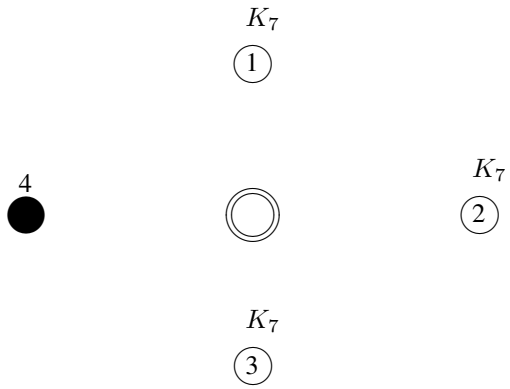


Figure 6. 7th rekeying: Group members (members 1,2 and 3) can compute the new group key but revoked member(s) (member 4) cannot get the new group key since $g(4) = 0$.

that knowing less than $\lambda + 1$ session share of a node do not provide any information about the original stored share. Based on the cryptographic algorithm that is used for sending the shares, $1 \leq \lambda \leq 2t$ should be chosen.

D. Fault Tolerance

In the proposed scheme, like other schemes where the group controller is responsible for sending the broadcast message, the group controller is a single point of failure. In order to tolerate k failures in the group controller, it could be possible to have k group controllers (only one of them is active at a time). But group nodes should be able to trust k group controllers instead of one.

If h becomes compromised, the whole rekeying mechanism is compromised. In order to tolerate k compromises of h polynomial, it is possible to have k distinct instances of the scheme with k group controllers. So each group member has k personal secrets.

E. Security Analysis

According to Theorem 4, this scheme has t-revocation capability. It also provides t-wise backward and forward secrecy.

Theorem 2. *$h(x, y)$ is compromised if and only if*

1) *$\mu + 1$ (or more) shares of e are compromised and $h'(x, y)$ is also compromised.*
2) *or $2t + 1$ of group members become compromised.*

Proof: Having $\mu + 1$ (or more) shares of e, one can find the original $e(x, y, u)$ by solving $\mu+1$ $(\mu+1)$-variable linear equations. Knowing less than $\mu + 1$ share, $e(x, y, u)$ could not be constructed. It is clear that $h(x, y)$ could be constructed if and only if $e(x, y, u)$, and $h'(x, y)$ are also available.

Table I
MAXIMUM AND MINIMUM AMOUNT OF MEMORY CONSUMPTION IN THE GROUP CONTROLLER (BYTES). $\mu = \lambda = t$

$t = 2$	$t = 3$	$t = 4$	$t = 5$	$t = 6$	
400	812	1440	2332	3536	Minimum
656	1200	1976	3032	4416	Maximum

Table II
MAXIMUM AND MINIMUM AMOUNT OF MEMORY CONSUMPTION IN THE GROUP MEMBER (BYTES). $\mu = \lambda = t$

$t = 2$	$t = 3$	$t = 4$	$t = 5$	$t = 6$	
112	184	272	376	496	Minimum
164	256	364	488	628	Maximum

If $2t + 1$ group members become compromised, actually $2t+1$ of $h(i, y)$ are compromised which are enough material to reconstruct h polynomial. ■

Theorem 3. *This scheme has t-revocation capability. It also provides t-wise backward and forward secrecy.*

Proof: The proof is similar to the proof of Theorem 2. Note that we have assumed $t \leq \mu$. ■

IV. IMPLEMENTATION AND SIMULATION

We have implemented our proposed scheme for TinyOS-2.1.0 [11]. We installed TinyOS on Ubuntu Linux with 2.6.24-16-server kernel. We have used Avrora (Beta 1.7.10) [12] to simulate the implemented code. Simulation results are give bellow.

In our implementation, we have used dynamic memory allocation for storing polynomials coefficients. Although this code has been tested on a real MICAz mote [13], we are not claiming that it is perfectly optimized. Since the largest integer data type in TinyOS is `uint64_t`, we used `uint32_t` for coefficients in polynomials[1]. So the key length is 32 bits. We have also implemented the basic version of the only published distributed scheme, B-PCGR [5], using the same computation engine as ours.

A. Memory Usage

To have a better understanding of memory usage of our implementation, we logged the amount of memory allocated (`malloc()`) and freed (`free()`) for each phase of the rekeying procedure.

The initially allocated memory (minimum) and the maximum amount of allocated memory during execution of rekeying process in the group controller and a group member are shown in Table I and II, respectively.

Note that these figures are only the amount of dynamically allocated memories and does not contain memory usage of function codes, local variables, etc.

[1]to be able to have multiplication of two 32-bit integers

 ISBN: 978-1-61208-166-3

Table III
ENERGY CONSUMPTION OF COMPUTATION IN EACH PHASE OF THE PROPOSED SCHEME ON A MICA2 MOTE. THE GROUP CONTROLLER DOES STEP 3 ONCE. $\mu + 1$ GROUP MEMBERS DO STEP 2. ALL GROUP MEMBERS DO STEP 4

Step 3	Step 2	Step 4	
491.85 μJ	56.6 μJ	129.83 μJ	$t = \lambda = \mu = 2$
861.73 μJ	104.59 μJ	146.63 μJ	$t = \lambda = \mu = 3$
1334.56 μJ	167.32 μJ	163.39 μJ	$t = \lambda = \mu = 4$
1946.38 μJ	244.75 μJ	191.38 μJ	$t = \lambda = \mu = 5$

Table IV
ENERGY CONSUMPTION OF COMPUTATION IN EACH PHASE OF B-PCGR ON A MICA2 MOTE. COMPUTING SHARES IS DONE IN EACH GROUP MEMBER $\mu + 1$ TIMES. EACH GROUP MEMBER COMPUTES K ONCE

Computing the group key	Computing shares	
272.9 μJ	0.5 μJ	$t = \mu = 2$
644.71 μJ	0.62 μJ	$t = \mu = 3$
1178.03 μJ	0.79 μJ	$t = \mu = 4$
1944.11 μJ	0.99 μJ	$t = \mu = 5$

B. Energy Consumption

Although radio communications consume most of the motes' energy, energy consumption of computations should also be considered. We have used Avrora to measure the energy consumption of computations of each phase of the rekeying procedure for our proposed scheme as well as B-PCGR [5] in MICA2 motes.

For this purpose, codes of each phase of the rekeying process have been run in a `for` loop for 100 times. The energy consumption has been measured with and without running loop and the difference divided by 100 is reported for the energy consumption of that phase.

Table III and IV demonstrate the measured figures for our proposed scheme and B-PCGR, respectively. As it is clear, the most power hungry part of our scheme runs in the group controller. While each phase of B-PCGR consumes an small mount of energy, these phases should be run several times.

Figure 7 shows total energy consumption of computations of our scheme with $\mu = \lambda = t$ and B-PCGR with $\mu = t$ for $n = 10$. Our scheme consumes less energy compared to B-PCGR, and the difference becomes more significant for larger ts.

Figure 8 demonstrates how growth of n affects the total energy consumption of computations in our scheme with $\mu = \lambda = t = 3$ and B-PCGR with $\mu = t = 3$.

C. Computation Time

We have measured computation time of our scheme using Avrora simulator for MICA2 motes. Table V presents the results.

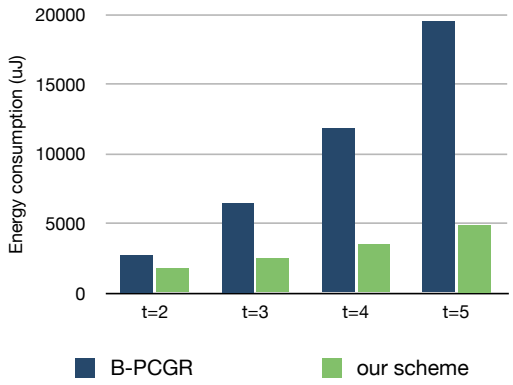


Figure 7. Total energy consumption (μJ) of our proposed scheme and B-PCGR for $n = 10$

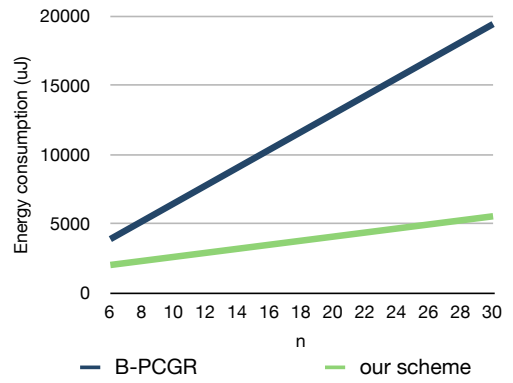


Figure 8. Total energy consumption (μJ) of our proposed scheme with $\mu = \lambda = t = 3$ and B-PCGR with $\mu = t = 3$

D. Communication Overhead

Table VI and VII shows total size of the payloads that should be sent in our scheme and B-PCGR, respectively for $n = 10$. Figure 9 compares total payload size of the sent packets in our scheme and B-PCGR for different values of n.

Table V
COMPUTATION TIME OF OUR IMPLEMENTATION ON A MICA2 MOTE. THE GROUP CONTROLLER DOES STEP 3 ONCE. $\mu + 1$ GROUP MEMBERS DO STEP 2. ALL GROUP MEMBERS DO STEP 4

Step 3	Step 2	Step 4	
22.22 ms	2.68 ms	6.39 ms	$t = \lambda = \mu = 2$
39.06 ms	5 ms	7.77 ms	$t = \lambda = \mu = 3$
60.68 ms	8.09 ms	9.48 ms	$t = \lambda = \mu = 4$
88.74 ms	11.98 ms	12.11 ms	$t = \lambda = \mu = 5$

Table VI
TOTAL PAYLOAD SIZE IN OUR SCHEME

total size	share request packet	no.	share packet	no.	broadcast message	no.	
120 Byte	= 12 Byte	×1	+20 Byte	×3	+48 Byte	×1	$t = \lambda = \mu = 2$
196 Byte	= 16 Byte	×1	+28 Byte	×4	+68 Byte	×1	$t = \lambda = \mu = 3$
288 Byte	= 20 Byte	×1	+36 Byte	×5	+88 Byte	×1	$t = \lambda = \mu = 4$
396 Byte	= 24 Byte	×1	+44 Byte	×6	+108Byte	×1	$t = \lambda = \mu = 5$

Table VII
TOTAL PAYLOAD SIZE IN B-PCGR FOR $n = 10$

total size	share request packet	no.	share packet	no.	
240 Byte	= 12 Byte	×10	+4 Byte	×30	$t = \mu = 2$
320 Byte	= 16 Byte	×10	+4 Byte	×40	$t = \mu = 3$
400 Byte	= 20 Byte	×10	+4 Byte	×50	$t = \mu = 4$
480 Byte	= 24 Byte	×10	+4 Byte	×60	$t = \mu = 5$

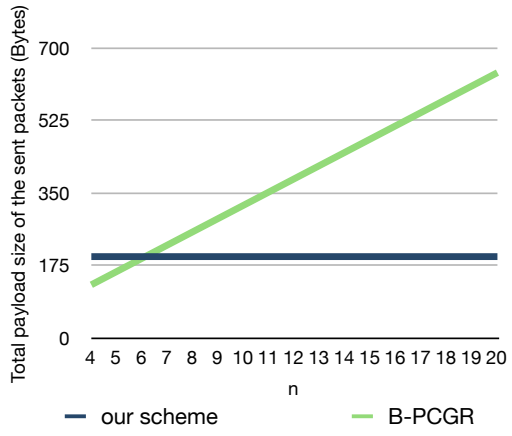


Figure 9. Comparison of total payload size of sent packets in our scheme and B-PCGR

E. Source Code

The source code is available in `http://ce.sharif.edu/~nikoonia`

V. PERFORMANCE ANALYSIS

In this section, we analytically evaluate the performance of the proposed scheme. We compare the performance of our scheme and the only published distributed scheme in Section VI. In the next sub-sections, we assume a group of n sensor nodes that do their key management computations in $\mathbb{F}_p$. Hence, the key size is $\lceil \log q \rceil$.

A. Communication Cost

In a rekeying event, $\mu+1$ nodes should send their session share of size $(2t+1) \times \lceil \log q \rceil$ bit to the group controller; The group controller computes a broadcast message of size $(w + 2 \times (2t+1)) \times \lceil \log q \rceil$ bits[2]. In the worst case, $w = t$. So in the worst case, the broadcast message size is $(5t + 2) \times \lceil \log q \rceil$ bits

B. Computation Overhead

In a rekeying event, $\mu + 1$ nodes must evaluate e polynomial at an specific point (i.e., j) which has a computation overhead of $O(t\lambda)$ modular arithmetic operation.

The group controller has to rebuild e polynomial and evaluate it for $u = 0$ from $\mu + 1$ shares using Gaussian elimination which together requires $O(\mu^2)$ arithmetic operation. Computing $P(x)$ and $Q(x)$ for the broadcast message requires $O(t^2)$ modular arithmetic operation.

Finally, group members need to do $O(t)$ modular arithmetic operation to recover K.

So the computation overhead of a rekeying operation for the group controller is $O(t^2 + \mu^3)$ and the average computation overhead for each group member is $O(t) + \frac{\mu+1}{n} O(t\lambda)$.

C. Storage Requirements

The group controller stores $h'(x, y)$ which is $(2t + 1) \times (\lambda + 1) \times \lceil \log q \rceil$ bits. Group member i should store $h(i, y)$ and $e(x, y, i)$ which needs $(\lambda + 1) \times \lceil \log q \rceil$ and $(2t + 1) \times (\lambda + 1) \times \lceil \log q \rceil$ bits, respectively.

VI. COMPARISON

In this section, we conclude our comparison between our proposal and the only published distributed scheme. Table VIII provides a comparison between our proposed scheme and B-PCGR [5]. Note that by the *communication overhead*, we mean the number of bits that should be sent and not the traffics that are forwarded by the nodes due to the routing process. Both schemes provide t-wise backward and forward secrecy. They also provide on-demand rekeying.

[2]We assume $\lceil \log q \rceil$ bit IDs

Table VIII
COMPARISON OF GROUP REKEYING SCHEMES. $L = \lceil \log q \rceil$ IS THE KEY SIZE.

	Our Scheme	B-PCGR [5]
Attacker Model	Active	Active
On-demand rekeying	Yes	Yes
t-wise forward secrecy	Yes	Yes (for $\mu > t$)
t-wise backward secrecy	Yes	Yes (for $\mu > t$)
System Model	Distributed	Distributed
Total point-to-point communication overhead (bits)	$(\mu+1) \times (2t+1) \times L$	$n \times (\mu+1) \times L$
Broadcast communication overhead (bits)	$(5t+2) \times L$	none
Computation overhead for each nodes	$O(t^2) + \frac{\mu+1}{n} O(\lambda^2)$ Modular arithmetic operation	$O(\mu^3 + (n+1) \times t^2)$ modular arithmetic operation
Computation overhead for the group controller	$O(\mu^3 + t^2)$ Modular arithmetic	none
Storage overhead for each node (bits)	$(2t+1) \times (\lambda+1) \times L$	$(n+1)(t+1) \times L$

In order to provide these features, B-PCGR needs to have an underlying IDS with the capability to inform all group members about the compromised nodes which costs more complexity of the IDS and more communication overhead. While in our proposal, only the group controller needs to have such information.

Our scheme consumes less energy in its computations (see Section IV-B). It also have lower communication overhead (see Section IV-D).

VII. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a new distributed group rekeying scheme which does not require a secure rekeying server and is based on local collaboration of group members. We have evaluated analytically the performance and the security of this scheme.

We have also implemented our proposal for TinyOS and used Avrora to simulate the compiled binary for MICA2 motes. Energy consumption, memory usage and communication overhead have been reported. Simulation results show that comparing to the only published distributed scheme, our scheme consumes less energy in its computations and has lower communication overhead.

Most of the group rekeying schemes, including our proposed scheme, rely on one group controller. A failure in the group controller could damage the whole group. This problem is not addressed in the literature. Our future work includes the study of the impact of multiple group controllers. Choosing the optimum key size in order to minimize energy consumption of the encryption, decryption and rekeying processes is another issue that we will study in our future work.

ACKNOWLEDGMENT

The work of the third author was partially supported by the Spanish Ministry of Education and Science under Projects TEC2009-13000 and CONSOLIDER CSD2007-00004 (ARES).

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[2] D. Liu, P. Ning, and K. Sun, "Efficient self-healing group key distribution with revocation capability," in *Proceedings of the 10th ACM conference on Computer and communications security (CCS '03)*, 2003, pp. 231–240.

[3] A. Shamir, "How to share a secret," *CACM*, vol. 22, no. 11, pp. 612 – 613, 1979.

[4] M. Naor and B. Pinkas, "Efficient trace and revoke schemes," in *LNCS, Vol. 1962*, 2001, pp. 1–20.

[5] W. Zhang and G. Cao, "Group rekeying for filtering false data in sensor networks: a predistribution and local collaboration-based approach," in *Proc. of INFOCOM*, 2005, pp. 503–514.

[6] G. Danio and I. M. Savino, "An efficient key revocation protocol for wireless sensor networks," in *Proceedings of WOWMOM'06*, 2006, pp. 450–452.

[7] Y. Jiang, C. Lin, M. Shi, and X. S. Shen, "Self-healing group key distribution with time-limited node revocation for wireless sensor networks," *Ad-Hoc Networks*, vol. 5, no. 1, pp. 14–23, 2007.

[8] F. I. Khan, H. Jameel, S. M. K. Raazi, A. M. Khan, and E. N. Huh, "An efficient re-keying scheme for cluster based wireless sensor networks," in *LNCS No. 4706*, 2007, pp. 1028–1037.

[9] Y. Wang and B. Ramamurthy, "Group rekeying schemes for secure group communication in wireless sensor networks," in *Proc. of ICC'07*, 2007, pp. 3419–3424.

[10] Y. Wang, B. Ramamurthy, and X. Zou, "Keyrev: An efficient key revocation scheme for wireless sensor networks," in *IEEE International Conference on Communications (ICC '07)*, 2007, pp. 1260–1265.

[11] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, D. Gay, J. Hill, M. Welsh, E. Brewer, and D. Culler, "Tinyos: An operating system for sensor networks," *Ambient Intelligence*, pp. 115–148, 2005.

[12] B. L. Titzer, D. K. Lee, and J. Palsberg, "Avrora: scalable sensor network simulation with precise timing," in *Proceedings IPSN '05*, 2005, pp. 67–71.

[13] Crossbow. http://xbow.com, accessed on aug. 31, 2011.

 ISBN: 978-1-61208-166-3

GEMOM Middleware Self-healing and Fault-tolerance: a Highway Tolling Case Study

Federica Paganelli, Gianluca Vannuccini, David Parlanti,
National Interuniversity Consortium for Telecommunications
Firenze, Italy
Federica.paganelli@unifi.it

Dino Giuli[1], Paolo Cianchi[2]
[1]Dept. of Electronics and Telecommunications
Via S. Marta 3, Firenze, Italy
dino.giuli@unifi.it
[2] Negentis srl, Firenze, Italy
pcianchi@negentis.com

***Abstract*—Application of message-oriented communication in business critical systems has to cope with requirements for end-to-end intelligence, security, scalability, self-adaptation and fault-tolerance. To this extent, the Genetic Message-Oriented Middleware (GEMOM) European Research Project focused on the design and development of a fast-forwarding message oriented middleware, endowed with robustness, resilience, self-adaptability, and scalability capabilities. This paper reports on the design, development and testing results of a case study for the GEMOM middleware on highway toll data management and collection. The case study has a twofold objective: first, it offers a reference scenario that poses requirements challenging a specific set of self-healing and fault-tolerance GEMOM features and thus providing an application scenario suitable for features validation; second, it aims at representing a real-world application scenario and consequently at providing valuable insights on GEMOM exploitability in a specific market sector.**

Keywords-message-oriented middleware; self-healing; fault tolerance; toll data management.

I. INTRODUCTION

Message-Oriented Middleware (MOM) systems are considered as promising assets for supporting current challenges in the enterprise computing landscape [1]. These challenges are: the need for increasing support of sense-and-respond applications (i.e., applications endowed with massive sensing, analytics and control capabilities); the growing interconnection of enterprise systems over geographically distributed wide areas; the need to differentiate message traffic according to QoS-aware policies. Such challenges stress requirements for end-to-end intelligence, security, scalability, self-adaptation and fault-tolerance.

One of the most widely adopted approaches to support scalability and resilience in messaging infrastructures is based on hot standby brokers with instant switch over and no data loss. However, once switch-over is performed, usually these systems have no means to compensate for the reliability loss by automatically finding another source of redundancy. Also, they are relatively prone to the incidence of feed failures as they often do not take redundant feeds into account. It is often said that the existing state-of-the-art achieves arbitrary resilience by a brute-force approach. The state of the art is often outside of the reach of Small Medium Enterprises) (SMEs) and even of large companies. Moreover, self-healing is either rudimentary or non-existent, and when it is available, it requires high-level skills to be configured and managed [2].

The European Project for a Genetic Message Oriented Middleware (GEMOM [3]) was aimed at addressing the above issues, by researching, developing and deploying a prototype of a messaging platform endowed with robustness, resilience, self-adaptability and scalability capabilities.

According to their experience in messaging-systems and business areas of interest, the GEMOM partners were involved in the development of five case studies, with a twofold objective: first, each case study offers a reference scenario that poses requirements challenging a specific set of GEMOM features and thus providing an application scenario suitable for GEMOM key features validation; second, each case study represents a real-world application scenario and consequently provides valuable insights on GEMOM exploitability across a wide set of market sectors.

This paper reports on preliminary results in the design, development and testing of a GEMOM case study on a highway toll data management and collection scenario. The proposed case study aims at validating GEMOM capability in guaranteeing reliable message exchange across highway infrastructure nodes against different fault simulation scenarios.

The paper is structured as follows: Section II outlines the GEMOM middleware requirements definition, the corresponding GEMOM key features and system architecture. Section III describes the GEMOM experimentation in a toll collection management case study. Finally, Section IV sums up conclusions and future research directions.

II. THE GEMOM MIDDLEWARE

This section briefly introduces the GEMOM middleware by first presenting the adopted risk analysis methodology and design requirements, and then by describing main characteristics of the GEMOM architecture.

A. Risk Analysis and Requirement Definition

Risk analysis for the GEMOM infrastructure was derived by taking into account the assets of a MOM, the threats that may hang over such assets, the vulnerabilities that may be

 ISBN: 978-1-61208-166-3

exploited by the attacker and, finally, the impact of a specific attack on each asset.

The main assets under consideration were: end user (using an application that exploits the middleware), agent (such as applications, probes, effectors), agents acting as message publisher and/or subscriber, message sender and receiver, brokers, links (primary and backup), paths composed of multiple links and, finally, messages and message topics defined in the MOM. Such assets were assigned a risk level depending on the specific case study under consideration within the GEMOM project.

Other assets were considered as extremely relevant and highly-risky for the GEMOM system, being them the management layer (hereafter named "Managerial Nodes") of the overall GEMOM infrastructure.

Afterwards, the threats that could affect those assets were assessed. The value of a threat was estimated by considering how often an attacker could perform its attack, or how easily it could access the asset.

Examples of threats that were considered for the GEMOM project are message flooding or publishing from non-existent or un-authorised brokers, agent nodes registration/deregistration via spoofing, and replay attacks from malicious nodes. Also threats related to confidentiality and integrity corruption in the messaging path were considered. Examples of specific threats, that might be more relevant for the highway tolling messaging system, could be toll-gate power-supply interruptions (due, for instance, to flooding or other natural phenomena), as they are likely to affect the capability to exchange messages with the central toll collection station. Other threats, even if less likely to happen, being the network a totally dedicated infrastructure, could be related to tolling message tampering and sniffing.

Vulnerability analysis in the GEMOM infrastructure was conceived as a continuous run-time assessment process, addressed with a specific tool that can be activated in the GEMOM messaging layer. Vulnerability detection and the consequent adaptive security policies are out of the scope of this paper (details may be found in [2]). Nevertheless, common vulnerabilities derived from the OWASP [4] and SANS [5] top lists were considered as a first step.

Once the main assets, threats and vulnerabilities were considered for the GEMOM infrastructure, a further step was done in order to extend the concept of security risk, including also performance and QoS degradation that, as much as a security attack, affect the overall system performance and, as a consequence, the final quality of the delivered service. This wide-sense approach is conceptualised in GEMOM in the extended notion of "fault".

A fault may be seen as a status-change of a GEMOM asset between two different security risk-levels, and/or between two different SLAs. For instance, if a message, belonging to a guaranteed class-of-service, encounters a path with compromised QoS capabilities, which will only offer unreliable class-of-service, a corresponding fault may be triggered.

The capability of the GEMOM system to react to (and to prevent) these faults is referred to as Fault Tolerance.

Fault tolerance requirements specify the prevention actions that GEMOM should perform in order to avoid the fault, as well as the actions that the GEMOM infrastructure should launch in order to mitigate the impact of the occurred fault, and to establish a new reliable and performing steady state.

The GEMOM requirements gathering process was driven also by case study analysis. Table I shows a resume of the requirements that were selected for the Highway Tolling Data Collection and Management case study with the help of the highway operator representatives and their corresponding priority level for validation.

B. Gemom Key Features

According to the above-mentioned risk analysis and requirements definition, the GEMOM infrastructure was

TABLE I. GEMOM REQUIREMENTS FOR THE TARGET CASE STUDY

Requirement	Detailed description	Priority
1. Tolerance to Connectivity failures	GEMOM shall use traffic engineering techniques at networking layer to be tolerant to links failures. In case of detection of compromised connectivity to consumers, GEMOM routing algorithm shall select another alternate path (or more, for redundancy and load sharing) to message consumers.	LOW
2. Tolerance to hardware/software faults in nodes	GEMOM shall keep an updated topology database of the network of brokers, in order to be tolerant to failures in one specific node and to be able to fast-switch to other nodes in case of failure.	HIGH
3. Self-Healing	The system should be able to automatically create new redundancy in case of node faults. If one broker or namespace fails and redundant one takes over the function, system's resilience capabilities are diminished. GEMOM should be capable of restoring its resilience and security profiles if resources are available.	HIGH
4. No single-point of failure	The communication highway shall not introduce a single point of failure in node to node communication	LOW
5. Sudden reconfiguration	The system should allow for sudden re-configurations of the available resources (such as the allocation of more messaging paths to deal with peak traffic rates and resources required under emergency situations)	LOW
6. Self-protection	GEMOM shall implement load balancing, topic mirroring, and shall be able to implement switchover to redundant components, and to spawn new hot standby components	LOW
7. JMS API support	GEMOM shall offer messaging services to JMS-based client application via proper bridging components	HIGH
8. Plug&play rule assisted semantics	"Plug-and-play rule assisted semantics" refer to the system capability of altering message delivery according to application-specific needs. GEMOM shall allow to attach plug and play rules to the exchange of various individual topics or groups, and so enhance its handling of exchange of messages with content transformation rules, routing or security semantics.	HIGH
9. Multiple bindings support	GEMOM shall prove bindings for Java	HIGH

 ISBN: 978-1-61208-166-3

designed to implement a fast-forwarding message-oriented middleware endowed with end-to-end resilience, security, scalability and self-adaptation capabilities.

GEMOM key features, and related research challenges, may be listed as follows [2]: a) system scalability in handling variable messaging volumes and clients cardinality; b) context-aware adaptive security via policy-based authorization, authentication and confidentiality techniques; c) new techniques and tools for pre-emptive and automated checking vulnerabilities to faults, oversights and attacks; d) message delivery reliability to message broker mirroring and workload distribution techniques; e) extensibility for accommodating application-specific requirements (e.g., content-based message filtering, JMS API support, message traceability).

Features d) and e) are particularly relevant to this paper, as discussed in the following section. For an extensive description of the other features, and the discussion of GEMOM contribution with respect to the state of the art, for the sake of brevity, we refer the reader to [2].

Above mentioned GEMOM key features are supported by the following specific research contributions:

- the architecture of an externalized system to support resilience and anomaly detection for MOM resilience and protection [2] [6].
- The design and implementation of a resource allocation mechanism for balancing brokers' workload [6].
- The integration of a mechanism for anomaly detection. Examples of target anomalies are high message rates, degradation of broker performance in the context of Denial of Service (DoS) and anomalous message content [7].
- Design of adaptive security mechanisms and security metrics for a distributed messaging system based on threat and vulnerability analysis and security requirements [8].

C. GEMOM Architecture

The GEMOM system architecture was modelled as a set of communicating nodes, distinguished into operational and managerial nodes.

The *Operational nodes* are those responsible for executing basic operational tasks according to a specific behaviour, and message exchange. Examples include Message Brokers and Clients (either message publisher or subscribers) and modules providing security and fault detection capabilities, i.e., the Authentication and Authorization Modules.

Managerial nodes are modules that, based on the system context awareness, take decisions about possible run-time adjustments of Operational nodes behaviour. Examples include modules responsible for elaborating adjustments for the broker topology and workload (Overlay and Resilience Managers) and modules responsible for adapting security policies (Adaptive Security Managers).

Therefore, GEMOM infrastructure can be devised as a network of GEMOM brokers (Gbroker) configured, protected, monitored and optimised by an overlay of Managerial nodes, as sketched in Fig.1.

A GEMOM Broker is designed in order to keep the message routing process as simple and fast as possible. To this extent, topic names follow schemes similar to those used in variables or class definitions in programming languages, while topic values are simply key-value pairs. Message brokers and API then add metadata to the stream of routed topics.

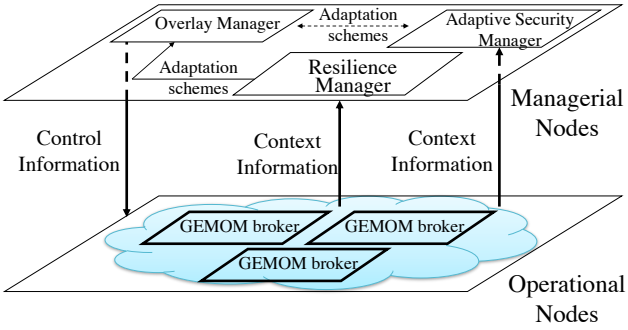


Figure 1. GEMOM Architecture

In addition to this simple messaging layer, the Overlay Manager is responsible for a range of functions to improve performance and resilience. It is external to the message forwarding system and receives data pertaining to security and QoS from a range of sensors that monitor the core messaging system. It then evaluates such data and performs the consequent actions using effectors deployed within the Operational Nodes, and the contextual information gathered by multiple nodes both at the Managerial and Operational Layers (e.g., Adaptive Security Manager, Vulnerability assessment tools, Monitoring Tools, Gbrokers collecting internal data, etc.).

In other words, the above actions are triggered by «fault» events that are detected by active and passive monitoring the QoS and Security parameters, according to specific SLAs. When a violation in the committed service guarantees occurs, GEMOM must react by executing a suitable series of actions.

Examples of actions suggested by the Overlay Manager to the Operational Nodes layer, that are also specifically relevant to the requirements described in the previous section for the Toll Collection scenario, are: rebalancing existing load, adding new GBrokers to the system and re-routing the traffic on some namespaces or individual topics. These actions are the basic mechanisms for realizing Gemom Broker Mirroring and Self-Healing capabilities.

Operationally, if there is a severe failure in the primary Gbroker, then message handling is passed to the mirror, which is re-labelled as primary (broker mirroring), and a new mirror for the primary found. This mechanism allows to automatically re-establish the required resource redundancy also after a fault occurrence (self-healing). The same happens if the failure is related to a link between two Gbrokers, or during a path between publishers and subscribers. Note that a failure could also concern the chosen QoS SLA profile. The following figure shows how the

 ISBN: 978-1-61208-166-3

GEMOM system reacts to a fault through broker switchover and how the self-healing capability is achieved by spawning a new broker acting as a mirror (Fig.2).

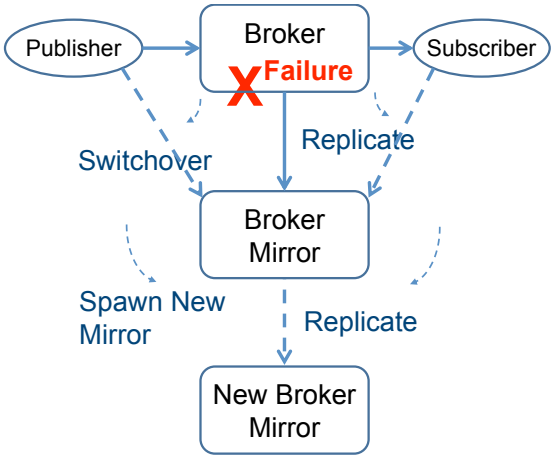


Figure 2. Broker Mirroring and Self ealing through new broker spawning acting as mirror

III. GEMOM EXPERIMENTATION IN A TOLL COLLECTION AND MANAGEMENT SCENARIO

The GEMOM middleware was conceived, developed, deployed and tested within the project lifetime by GEMOM partners.

The research challenges addressed and documented within the GEMOM project were experimented by carrying out suitable testcases in different real-life scenarios, each related to the major expertise of the corresponding GEMOM partner.

In particular, the case study reported in this paper had the twofold objective of: a) evaluating how GEMOM message-oriented infrastructure could be conveniently applied to cope with information distribution needs of highway operators b) validating a subset of GEMOM features, which were chosen according to the case study application requirements. The case study was designed with the collaboration of an Italian highway operator. More specifically, requirements were collected through face-to-face unstructured interviews with the operator representatives.

From these interviews it emerged that Toll collection management is an application scenario that is strategically relevant to the highway operator's purposes as well as potentially challenging for GEMOM validation. As a matter of fact, as already argued by Clark et al. [4], a wide-scale tolling system should cope with several requirements, including system reliability and availability, which are strongly required as money is involved.

Toll collection and management deals with the tools, techniques and processes involved in collecting revenue from a vehicle user for the use of road-space through road-use pricing [9].

Toll messages represent a significant volume of data exchanged within the target highway operator network as well as with external information systems of neighbour highway operators.

These issues motivate the need for a uniform, reliable, self-optimising, well-structured, extensible architecture for application-level communication and integration. Moreover, a uniform approach for data exchange based on message-oriented paradigm may facilitate the adoption of efficient and cost-effective system maintenance strategies.

A basic representation of a toll data collection system includes the following entities:

Highway Toll Central System. This system collects toll data from the infrastructure and performs toll data archiving, validation and processing for end users' accounting and monetary compensation with external operators.

Station Systems. Highway Stations may group lanes of both types: manual (i.e., with on-site payment) and electronic lanes.

Electronic Lanes. Electronic Lanes are equipped with RFID readers and sensing devices. This infrastructure is used to detect the transit of a vehicle equipped with an RFID transponder. The transit event (both in entrance and in exit) triggers the generation of a message (Electronic Toll message) which is sent to the Highway Toll Central System.

Manual Lanes. Entrance manual lanes provide drivers with a paper-based token registering the vehicle transit details. At destination, the driver shows the token at the exit lane. The lane system calculates the road fare, depending on the adopted pricing models, and the driver pays on-site. For each entrance and exit event, a message is created by the lane system and sent to the Highway toll central system. Updates on tolling policies are notified to Lanes via messages delivered by the Highway Toll Central System.

External toll systems. A target Highway Toll Central System should interact also with Toll Systems of external operators (e.g., for monetary compensation). Exchanged data include aggregated electronic toll messages and tolling policies update.

The case study scenario focuses on the distribution of two message types:

a) automatic toll payment data, which are data collected at toll lanes and transmitted periodically to the central control room for performing billing operations. Message size is limited. Data loss is not tolerated, while timing constraints are not hard real-time (Many-to-One message delivery).

b) tolling policy update records: update of tolling policy is performed once in a while and have to be communicated to all the peripheral nodes (i.e., toll lanes and stations) within a limited time interval. The system does not tolerate data loss. As regards timing constraints, the system is not specifically sensitive to single message delays. (One-to-Many message delivery)

 ISBN: 978-1-61208-166-3

These data represent a strategic and relevant information

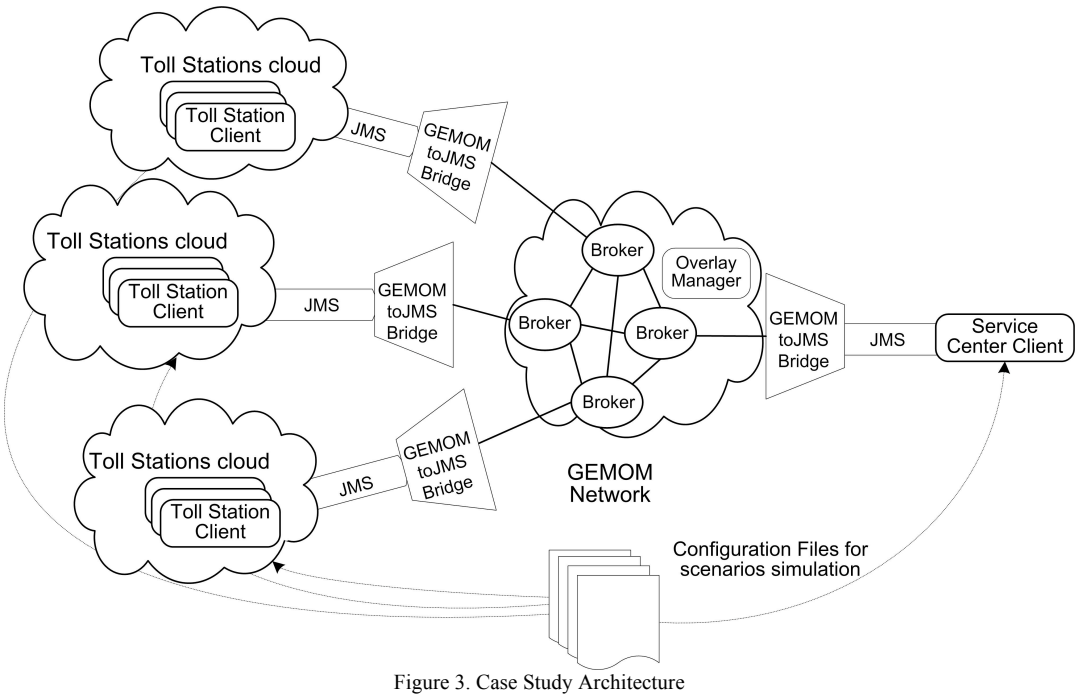


Figure 3. Case Study Architecture

asset for a highway operator and no information loss is tolerated.

This case study is thus particularly significant for testing GEMOM messaging service's continuous availability and robustness achieved via mirroring and self-healing features. As a matter of fact, GEMOM structural replication capabilities (self-healing) should assure robustness of the messaging infrastructure even under high volumes of traffic.

Moreover, in order to enable the interoperation of the GEMOM capabilities in the target operator technological environment, where Java-based standard and enterprise technologies are widely adopted, the case study exploits also the developed full-fledged java bindings to GEMOM C++ native interfaces. In order to facilitate interoperation with widely-diffused commercial messaging platforms, the case study architecture is based on the adoption of a component providing GEMOM-to-JMS bridging capabilities, as Java Message Service (JMS) [10] is a wide adopted specification for messaging services API.

A. Case Study Architecture

The case study architecture is composed of the following functional components:

- Application clients that publish/subscribe for toll and tolling policies data. Clients have been developed against JMS messaging interfaces.
- a JMS-GEMOM bridge, interfacing a JMS bus with GEMOM. The JMS-GEMOM bridge is responsible for transmission/receipt of messages over GEMOM. Bridging has been realized by mapping JMS topics onto GEMOM ones.
- A network of GEMOM brokers responsible for message exchange.

Applications clients are configured in order to simulate the behaviour of toll stations and the Service Centre. Toll station clients are spread on a set of virtual machines to resemble the highway operator physical wide area network. They may be configured in order to act as message producers (to simulate the delivery of electronic toll message) and as message consumers (to simulate the reception of tolling policy updates). Analogously, the Service Centre has been modelled as a JMS client capable of listening for toll data coming as JMS messages transferred by GEMOM and sending tolling policy updates.

Toll station clients simulate the production of Electronic Lane messages over a target time period and deliver the produced messages to the messaging system. Each toll station client may be configured in order to simulate different message traffic scenarios, resembling real-life message passing statistics during ordinary days. Toll gate working time is divided into time intervals whose starting time and duration can be configured; toll gate data are generated for each time interval according to Poisson distributions with different average values in order to simulate traffic flow at different hours over a day. It is possible to configure on each host the number of gates that have to be simulated and the desired message distribution over a target time interval.

The Service Centre simulates the generation of tolling policy updates. According to real practices, this event may be modelled as a one-shot event. Analogously to Toll station clients, the message generation process may be defined in a configuration file.

Figure 3 shows the proposed case study configuration for simulating the behaviour of the Highway Infrastructure toll stations network.

 ISBN: 978-1-61208-166-3

The toll station clients are grouped in set of toll stations clouds. Each toll station cloud represents the traffic to/from toll stations covering a specific geographical area. According to the characteristics of the target highway operator network, the case study will include at least three toll station clouds, one for each of devised geographical areas (north-, central, south Italy). To each area we can assign a given number of toll gates and/or toll stations, in order to reach an order of magnitude comparable to that of the real highway operator network.

As depicted in the figure, the application clients deliver and consume messages to/from a JMS MOM (i.e., Apache ActiveMQ). Messages are transferred to GEMOM network via the GEMOMtoJMS Bridge.

The GEMOM Broker Network is composed of a variable set of GEMOM Broker Agents and an Overlay Manager component is responsible for the overall network management and adaptation, as described in Section II.C.

B. Testing activities and results

The scenario analysis was carried out in collaboration with the Highway Infrastructure representatives. Details provided by the Highway Infrastructure on the current approach for message transfer handling and on typical message volumes have driven the design of the case study architecture and the configuration of the overall system for the demonstration activities.

Given the above-mentioned flexible configuration capabilities of the implemented case study, we were able to simulate different traffic scenarios by varying message size and number of toll gates involved, according to statistics data and requirements gathered during the meetings with the Highway Infrastructure representatives.

According to the risk and requirement analysis derived in Section III and to the architecture specification described above, the case study had the objective of functionally validating the following GEMOM capabilities:

1. offering a reliable messaging service via broker mirroring techniques (see req. 2 in Table I).
2. readjusting the structure of running nodes in order create new redundancy in response to failure-type events (req. 3 in Table I), as depicted in Fig. 2.
3. allowing clients to subscribe to topics and specify transformation rules (e.g., encoded in an XSLT file) in order to receive filtered/aggregated data (see req. 8 in Table I).
4. offering messaging services to JMS-compliant Java-based clients via proper bridging components (req. 7 and 8 in Table I).

For each toll station cloud, 150 toll lane clients were instantiated. We deployed a network of three brokers, as it is the minimum number of broker required to support GEMOM mirroring and self-healing features. Each machine was deployed on a separate host. All components were on the same LAN network.

We defined a set of test cases in order to test the system in different working conditions. Test cases are defined by varying the toll station clients configuration in order to resemble real-life road traffic scenarios.

A low-traffic scenario models the nightly traffic (with an average of 100 message per hour produced by single lane clients).

A medium-traffic scenario models the average traffic on an ordinary working day (four millions of messages per day).

Finally, a third scenario is defined in order to stress the system in a heavy traffic scenarios (even if unlikely to occur in real-life scenarios) characterized by an average of 1000 messages per hour produced by each lane client.Moreover, a set of messages related to price list updates were sent once for each test case in the opposite direction (from the Service Center to lane clients).

For each target GEMOM features (see list above), we ran each test case ten times. Table II summarizes the outcomes of the functional tests that were carried out in the testbed, with the corresponding most relevant issues and comments, representing the lessons learned from the experimental validation, and, hence, a sort of todolist for the next steps of the research activity.

Vertical and horizontal scalability were systematically tested in other GEMOM case studies [11].

For what concerns the testcase presented in this paper, the overall percentage of correctly received messages was 99,5%, while GEMOM highest measured throughput was 5000 msg/sec.

IV. CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

This paper reported on the design, development and testing results of a case study aiming at validating a set of GEMOM middleware features in a highway toll data management and collection scenario. In order to cope with the application scenario requirements, this work was mainly focused on the experimentation of mirroring and self-healing capabilities of the GEMOM system. We also tested interoperability with JMS API and the capability of configuring content transformation rules.

With respect to the related work on the GEMOM project, the remaining set of GEMOM features (e.g., adaptive security and authorization), were specifically addressed within the project lifetime in other case studies [11][12].

With respect to the related work in evaluation frameworks for MOM dependability and QoS [1] [7][13][14], this paper was based on requirements gathered from industry experts of highway infrastructures, where secure and reliable MOMs can be effectively applied, and it aimed at validating such requirements by means of experimental tests. However, given the mission-critical profile of the considered Highway operator infrastructure, it was not feasible – during the project lifetime - to validate the GEMOM middleware directly into the real operating messaging network. Further investigations could be focused on the deployment of GEMOM modules (especially those related to reliability and self-healing) into subsets of the real Highway Infrastructure and on testing and validation activities in more complex scenarios.

 ISBN: 978-1-61208-166-3

TABLE II. CASE STUDY TESTING RESULTS

GEMOM Feature	Test Description	Issues/Comments
Broker mirroring	At least two GEMOM brokers are running. Broker A is a master broker and Broker B is a mirror broker for a group of topics. After a blocking fault in Broker A was caused, we observed that messages have continued to flow from publishers to subscribers with no data loss, while the OverlayManager has correctly reported the re-instantiation of the Broker A	We simulated faults in a master broker by killing the corresponding process. Future tests could include the simulation of different faults (e.g., Distributed DoS, faults related to performance degradation).
Self Healing through broker spawning	The objective of the trial consisted in verifying that in case of failure of a master broker, the mirror broker will act as a master broker and a new mirror broker is spawned. We checked that messages continued to flow from publishers to subscribers.	This test was performed with a GEMOM network made by up to four brokers. Future test could be performed by increasing the GEMOM broker network size.
Plug-and-play rule assisted semantics	Toll station clients subscribe to the Price Listing topic and specify an XSLT transformation script file in order to receive transformed data. We checked that transformed messages were correctly received (via XML Schema validation).	Future tests could simulate the exchange of price listings with external operators' systems.
JMS API Support and Java bindings	The trialling activities verified that the message traffic is correctly handled by a system deployment made of the Java client applications compliant with the JMS API, the GemomToJMS bridging component and the GEMOM broker network (Fig. 4)	At present the GemomToJMS bridging component has been tested with the ActiveMQ messaging system. First testing iterations were useful to find bugs in the first releases of the Java-binding implementation. Future tests could include alternative JMS-compliant MOMs.

ACKNOWLEDGEMENTS

The Authors gratefully acknowledge the cooperation of "Autostrade per l'Italia" S.P.A and Dr. Eng. Paolo Tonani for his contribution to the requirements analysis and case study demonstration. They also thank Mr. Luca Capannesi for his technical support.

REFERENCES

[1] H. Yang, M. Kim, K. Karenos, F. Ye, and H. Lei, "Message-Oriented Middleware with QoS Awareness", in the Proceedings of the 7th International Joint Conference on Service-Oriented Computing (ICSOC-ServiceWave '09), Springer-Verlag, Heidelberg, pp. 331-345, 2009.

[2] A. Habtamu, R.M. Savola,., J. Bigham, I. Dattani, D. Rotondi,G. Da Bormida, "Self Healing and Secure Adaptive Messaging Middleware for Business Critical Systems", International Journal on Advances on Security, pp. 34-51, vol. 1&2, 2010.

[3] GEMOM Research Project Web Site, http://www.gemom.eu (last access date: July 31st, 2011)

[4] http://www.owasp.org The Open Web Application Security Project – Top Ten Web Application Security Risks (last access date: July 31st, 2011)

[5] http://www.sans.org The SANS (SysAdmin, Audit, Network, Security) Institute (last access date: July 31st, 2011)

[6] J. Wang, J. Bigham, B. Murciano, "Towards a Resilient Message Oriented Middleware for Mission Critical Applications", Proc. of the Second International Conference on Adaptive and Self-adaptive Systems and Applications (ADAPTIVE 2010), Lisbon, Portugal, 2010, pp. 46-51.

[7] J. Wang and J. Bigham, "Anomaly detection in the case of message oriented middleware", in Proc. of the 2008 Workshop on Middleware Security (MidSec '08). ACM, New York, NY, USA, pp. 40-42, 2008.

[8] R. Savola,H. Abie, Development of Measurable Security for a Distributed Messaging System, International Journal on Advances in Security, vol. 2, no. 4, 2009, pp. 358-380.

[9] C.J. Clark, P.T. Blythe, A.Rourke, "Design considerations for road-use pricing and automatic toll-collection systems" Electronics in Managing the Demand for Road Capacity, IEE Colloquium on, pp. 5/1-5/11, 5 Nov 1993

[10] Java Message Service (JMS), Official Web Page, http://www.oracle.com/technetwork/java/index-jsp-142945.html (last access date: July 31st, 2011)

[11] P. Ristau, S. Topham, F. Paganelli, L. Blasi, "GEMOM Platform Prototype Validation through Case Studies - Main Results and Viewpoints to Exploitation", in the Proc. of 30th IEEE Int. Conf. on Distributed Computing Systems Workshops (ICDCSW), pp. 290-291, 21-25 June 2010

[12] L. Blasi, R. Savola, H. Abie, and D. Rotondi. 2010, "Applicability of security metrics for adaptive security management in a universal banking hub system", in Proc. of the Fourth European Conference on Software Architecture: Companion Volume (ECSA '10), Carlos E. Cuesta (Ed.). ACM, New York, NY, USA, pp. 197-204, 2010.

[13] N. Looker and J. Xu, "Dependability Assessment of Grid Middleware", 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07), pp. 125-130, 2007.

[14] S. Chen, P.Greenfield, "QoS evaluation of JMS: An empirical approach", in: HICSS '04: Proceedings of the Proceedings of the 37th Annual Hawaii International Conference on System Sciences HICSS'04 - Track 9, IEEE Computer Society, Washington, DC, USA, pp. 1-10, 2004.

 ISBN: 978-1-61208-166-3

Enhancing DNS Security using Dynamic Firewalling with Network Sensors

Joao Afonso
Foundation for National Scientific Computing
Lisbon, Portugal
e-mail: joao.afonso@fccn.pt

Pedro Veiga
Department of Informatics
University of Lisbon
Lisbon, Portugal
e-mail: pedro.veiga@di.fc.ul.pt

***Abstract*— Security problems that plague network services today are increasing at a dramatic pace especially with the continuous improvement of network transmission rates and the total amount of data exchanged. This translates not only into more incidents but also to new types of attacks with network incidents becoming more and more frequent. A significant part of the attacks occur at Top Level Domains (TLD) who have the task of ensuring the correct functioning of Domain Name System (DNS) zones. In this article we discuss a solution developed and tested at FCCN (Foundation for National Scientific Computing), the TLD manager for the .PT domain. The system consists of a series of network sensors that monitor the network in real-time and can dynamically detect, prevent, or limit the scope of the attempted intrusions or other types of attacks to the DNS service, thus improving its global availability.**

Keywords—DNS; security; intrusion detection system; real-time; monitoring.

I. INTRODUCTION

DNS is a critical application for the reliable and trustworthy operation of the Internet. DNS servers assume a pivotal role in the normal functioning of Internet Protocol (IP) networks today and any disturbance to their normal operation can have a dramatic impact on the service they provide and on the global Internet. Although based on a small set of basic rules, stored in files, and distributed hierarchically, the DNS service has evolved into a very complex and, at the same time, very vulnerable system [1].

According to recent studies [2], there are nearly 11.7 million public DNS servers on the Internet. It is estimated that nearly 52% of them, due to improper configuration, allow arbitrary queries (thus allowing denial of service attacks or "poisoning" of the cache). About 31.1% of the servers also allow for the transfer of their DNS zones.

There are still nearly 33% of situations where the authoritative nameservers of an area are on the same network, which facilitates Denial of Service (DOS), a frequent attack to the DNS.

Furthermore, the types of attacks targeting the DNS are becoming more sophisticated, making them more difficult to detect and control in real-time. Examples are the attacks by Fast Flux (ability to quickly move the DNS information about the domain to delay or evade detection) and its recent evolution to Double Flux.

One of these attacks is the conficker [3] worm, first appeared on October 2008, but also known as Code Red, Blaster, Sasser and SQL Slammer.

Every type of computer, using a Microsoft Operating System can potentially be infected. Attempts to estimate the populations of conficker have lead to different figures but all these estimates exceed millions of personal computers. Conficker made use of domain names instead of IP address in order to make its attack networks resilient against detection and takedown.

The ICANN (Internet Corporation for Assigned Names and Numbers) created a list containing the domains that could be used in each TLD in such attacks to simplify the work of identifying attacked domains.

A central aspect of the security system that we propose and have implemented is the ability to statistically collect useful data about network traffic for a DNS resolver and use it to identify classes of harmful traffic to the normal operation of the DNS infrastructure.

In addition to collecting data, the system can take protective actions by detecting trends and patterns in the traffic data that might suggest a new type of attack or simply to record important parameters to help improve the performance of the overall DNS system.

The fact that the DNS is based on an autonomous database, distributed by hierarchy, means that whatever solution we use to monitor, it must respect this topology.

In this paper, we propose a distributed system using a network of sensors, which operate in conjunction with the DNS servers of one or more TLDs, monitoring in real-time the data that passes through them and taking actions when considered adequate.

The ability to perform real-time analysis is crucial in the DNS area since it may be necessary to immediately act in case of abuse or attack, by blocking a particular access and notifying other cooperating sensors on the origin of the problem, since several types of attacks may be directed to other DNS components.

 ISBN: 978-1-61208-166-3

The use of a Firewall solution, whose triggering rules are dynamically generated by the network sensors, is a fundamental component of the system. This way we can filter attacking systems efficiently and return to the initial status when the potential threat has ceased to exist.

With this approach we aim to guarantee an autonomous functioning of the platform without the need of human intervention.

The use of network alarms can also help in monitoring the correct functioning of the whole solution. Special care has been taken to minimize the detection of false positives and false negatives.

The remaining of the paper is structured as follows: Section II provides information regarding related work. Section III introduces our proposed methodology. In section IV, we describe the solution. Section V presents a case study used to validate the solution. In Section VI, the results gathered in the case study are analyzed. Section VII describes the process of evaluation and treatment of false positives and negatives. Finally, Section VIII presents some conclusions and directions for further work.

II. RELATED WORK

One of the first attempts in this area was a tool called sqldjbdns developed by Guenter and Kolar [4]. Their proposal uses a modified version of the traditional BIND [5] working together with a Structured Query Language (SQL) version inside a Relational database management system (RDBMS). For DNS clients, this solution is transparent and there is no difference from classic BIND.

Zdrnja presented a system for Security Monitoring of DNS traffic [6], using network sensors without interfering with the DNS servers to be monitored. This is a transparent solution that does not compromise the high availability needed for the DNS service.

Vixie proposed a DNS traffic capture utility called, DNSCap [7]. This tool is able to produce binary data using pcap format, either on standard output or in successive dump files. The application is similar to tcpdump [8] – command line tool for monitoring network traffic, and has finer grained packet recognition tailored for DNS transactions and protocol options, allowing for instance to see the full DNS message when tcpdump only shows a one-line summary.

Another tool available is DSC - DNS Statistics Collector [9]. DSC is an application for collecting and analyzing statistics from busy DNS servers. Major features include the ability to parse, summarize and search inside DNS queries detail. All data is stored in an SQL database. This tool, can work inside a DNS server or in another server that "captures" bi-directional traffic for a DNS node.

Kristoff also proposed an automated incident response system using BIND query logs [10]. This particular system, besides the common statistical analysis, also provides information regarding the kind of consultations operated. All information is available through the Web based portal. Each security incident can result in port deactivation.

III. METHODOLOGY

A. Architecture

The architecture of the system that we developed aims to improve the security, performance and efficiency of the DNS protocol, removing all unwanted traffic and reinforcing the resilience of a Top Level Domain. We propose an architecture comprising an integrated protection of multiple DNS servers, working together with several network sensors that apply live rules to a dedicated firewall, acting as a traffic shaping element.

Sensors carefully located in the network monitor all the traffic going to the DNS infrastructure, identify potentially harmful traffic using a algorithm that we have developed and tested and use this information to isolate traffic that has been identified as a security threat.

Several networks sensor monitor different parts of the infrastructure and exchange information related to security attacks. In this way, as shown in Fig. 1, it should also be possible to exchange critical security information between the sensors. In addition to an increase in performance, this operation should prevent an attack on a server from a source, identified by another sensor as malicious. This scenario is relevant since some kinds of attacks are directed to several components of the DNS infrastructure.

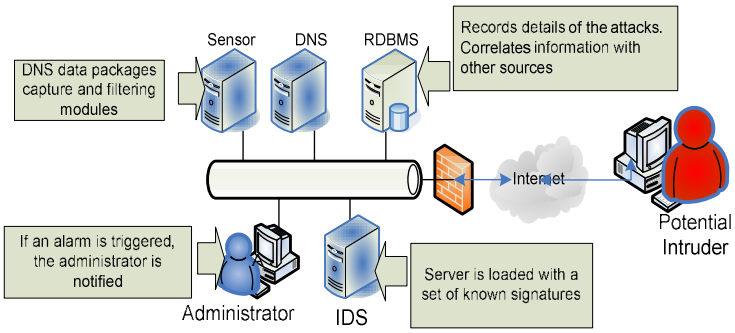


Figure1. Diagram of the desired solution

B. Heuristic

One of the crucial parts of our work is the algorithm to identify traffic potentially harmful to the DNS. In order to implement the stated hypothesis in the architecture and keep the DNS protocol as efficient as possible, it is necessary to apply a heuristic, which in real time, evaluates all the information collected from different sources and applies convenient weights to each component and act accordingly.

The components that we have chosen to have impact in the security incidents of DNS are: the number of occurrences, analysis of type of queries been made, the amount of time between occurrences, the number of probes affected and information reported from intrusion detection systems.

 ISBN: 978-1-61208-166-3

Our system uses the following formula to evaluate a parameter that measures the likelihood of the occurrence of a security incident:

$$f(x) = O \cdot 0{,}2 + C \cdot 0{,}2 + G \cdot 0{,}15 + N \cdot 0{,}25 + I \cdot 0{,}20$$

The following factors are considered:

- Occurrences (O) - Represents the number of times (instances) that a given source was blocked weighted according to the factors indicated in Table I.

TABLE I – CONTRIBUTION OF THE NUMBER OF OCCURRENCES OF A SOURCE IN MALICIOUS HEURISTIC

Occurrences	*Weight*
1	25%
2	50%
3	75%
4 or more	100%

- Analysis (C) - Real-time evaluation of the deviation of the values observed relatively to the average recorded, based on the criteria and weights identified in Table II.

TABLE II – CONTRIBUTION OF EVENTS TYPIFIED AS POTENTIALLY MALICIOUS ACCORDING TO THE HEURISTIC

Event	*Weight*
Entire zone transfer attempt (AXFR)	100%
Partial transfer zone attempt (IXFR)	50%
Incorrect query volume, 50 to 75% on average per source	75%
Incorrect query volume exceeding 75%	100%
Query volume, up 50%, the average number of access by origin	50%

Note that the estimates apply the moving average, for the determination of reference values, given the continuous collection of data.

- Time between occurrences (G) - time since last occurrence of a given event, distributed with the weights indicated below.

TABLE III – WEIGHT OF DIFFERENT TIME BETWEEN EACH OCCURRENCE

Time	*Weight*
Less than 1 Minute	100%
Less than 1 Hour	75%
Less than 1 Day	50%
Less than 1 Week	25%

- Incidence (N) - Number of probes that report blocks in the same source.
  For the calculation, we use the expression:

$$N = \frac{1}{\#Total\_Sensors - \#Sensors\_Attacked}$$

- Intrusion Detection Systems (I) - We considered the use of the Snort platform, a free tool that recognizes a large number of signatures of security incidents related to the DNS service.

TABLE IV – INTERCONNECTION WITH TEMPORAL DATA GATHERED FROM INTRUSION DETECTION SYSTEMS

Metric: Common Vulnerability Scoring System (CVSS)	*Weight*
Low level	34%
Middle level	67%
High level	100%

An activation of a rule in the Firewall will require:

1. The formula above has a value equal to or greater than 0.25;
2. The combination of two or more criteria of the formula.
   Exception: when receiving information from all the other sensors, in which case a single criterium is sufficient;
3. That the source is not in the White List, that contains privileged sources that should never be blocked.
   In this way we avoid compromising the Internet service, considering the key role played by DNS, the White List protects key addresses from being blocked in case of false positives events.
   This list is created from a record of trusted sources, allowing all addresses listed here to be protected from being added to the Firewall rules.
   One example is the list of internal addresses, and the DNS servers of ISPs.

On the opposite side, the removal of a rule in the firewall will require the following assumptions to occur simultaneously:

1. Exceeded the quarantine period, based on the parameters in use;
2. The expression of activation (heuristic) no longer checks the referenced source.

 ISBN: 978-1-61208-166-3

IV. PROPOSED SOLUTION

A. Diagram

As shown in Fig. 2, this solution is based on a network of sensor engines that analyze all traffic flowing into the DNS server in the form of valid or invalid queries, process the information received from other probes and issue restrictions for specific network addresses. In case an abnormal behavior is detected or there is suspicious behavior from a certain network address, it will be blocked in the firewall and the other probes notified so they can act accordingly. The system can also calculate the response time for each operation to evaluate the performance of the server.

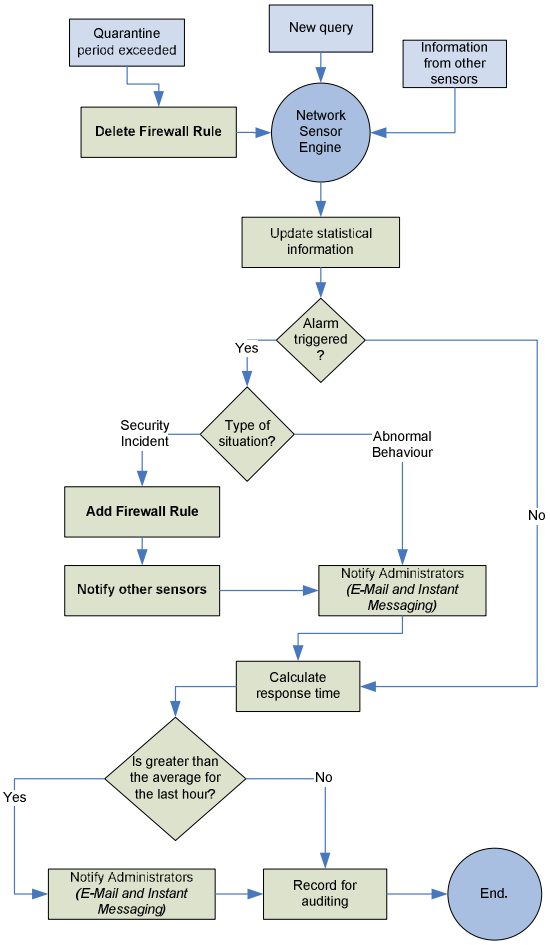


Figure 2.Block Diagram of proposed solution

For each rule inserted in the sensor firewall, there will be a period of quarantine and, at the end of this time, the sensor will evaluate the behavior of that source, to decide the needed to remove or keep that rule enabled, as shown in Fig. 2.

B. Network data flow

According to our design, all data that flows through the probe heading for the DNS server is treated according to a standard set of global firewall rules, followed by specific local rules regarding to the addresses that are being blocked in real time. The queries are then delivered to the parser to be analyzed and stored in the RDBMS. At the top is the system of alarms and the Web portal.

All information collected is stored in a database implemented in MySQL [11]. Taking into consideration the need to optimize the performance of the queries and to reduce the volume of information stored, the data is divided into a number of different tables.

The conversion of the IP address of source and destination (DNS server) into an integer format, has allowed for much more efficient data storage, and a significant improvement in the overall performance of the solution.

The information regarding all queries made, is stored daily into a log, and kept available during the next 30 days.

Two tables containing the set of rules that are dynamically applied – add or removed, based on situations that have been triggered - control the correct operation of the firewall. For auditing purposes every action is registered.

The information required for auditing and statistical tasks never expires.

C. Statistical analysis and performance evaluation

The statistical information collected and stored in the database has a significant amount of detail. It is possible, for example, to calculate, for each sensor, the evolution of queries per unit of time (hour, day, etc) badly formatted requests, DNS queries of rare types and determine the sources that produce the larger number of consultations. It is also possible to see the standard deviation of a given measure so we can relate it to that is seen with the other hits [14].

The performance of the DNS protocol responses is permanently measured, regarding the response time per request. Data is constantly registered and an alarm is raised in case normal response times are exceeded.

V. CASE STUDY

Our proposal have been under development since September 2006 at FCCN – who has the responsibility to manage, register and maintain the domains under the .PT TLD.

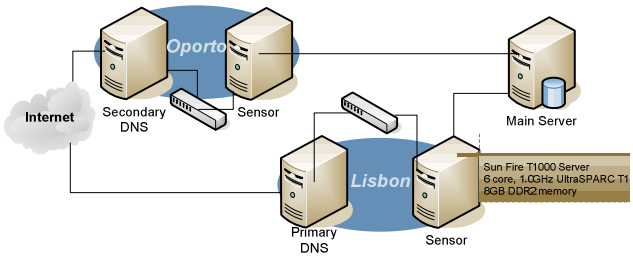


Figure 3.Working Sensors coupled with DNS servers

At present time, there are two sensors running, one at the primary DNS and another working together with a secondary DNS server.

The network analyzer is tshark [15], and the firewall used is IPFilter [12]. The real time parser was programmed in Java, collecting the information received from the tshark. The Web server is running Apache with PHP.

Regarding the Xmpp server [13], we choose the Jive messenger platform.

All modules are integrated together.

The entire sensor solution, as described above, as well as the web platform we developed is on-line from the 1st of January 2007, and the data from the various agents is being collected from the 10th of May 2008.

VI. RESULTS

We present here the results of 12 months of data collection (between 1st of May 2010 and 1st May 2011). The Average number of requests to the primary DNS server is up to 14,459,356 per day (167 per sec.).

The performance of the data analysis program is above 1240 requests processed per sec. (filtered, validated and inserted in the database).

Using the data collected by the sensors, during this time period, we were able to:

- Collect useful statistical information. E.g., daily statistics by type of DNS protocol registers accessed (Fig. 4).

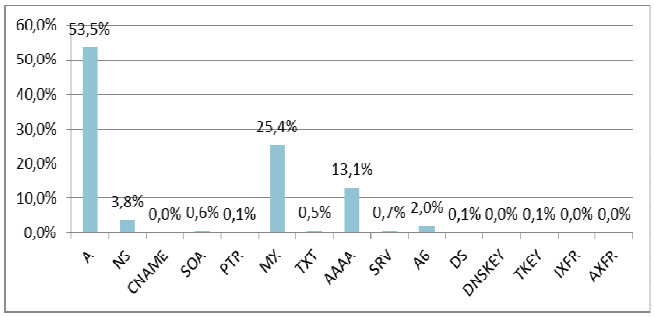


Figure 4. Statistical analysis by type of records accessed

- Detect examples of abnormal use (that are not security incidents). For example we were able to detect that a given IP was using the primary .PT DNS server as location resolver.
  The number of queries made was excessive when compared with the average value per source, reaching values close to some Internet Service Providers that operate under the .PT domain.
- Detect situations of abuse, including denial of service attacks, with the execution of massive queries. In last 12 months of analysis there are 17 DOS attacks triggered.
  They were instantly blocked, and addresses placed in quarantine (Table V).

TABLE V. EXAMPLES WHEN THE SENSOR DETECTED SITUATIONS THAT REQUIRED THE FIREWALL RULES TO CHANGE.

Source Address	*Date / Time*	*Operation*	*Sensor*
xx.xx.200.35	2011-07-12 01:03:12	Add rule	xx.xx.21.62
xx.xx.17.212	2011-07-12 03:25:19	Remove rule	xx.xx.32.63
xx.xx.117.51	2011-07-13 01:23:17	Add rule	xx.xx.21.62
xx.xx.94.139	2011-07-13 02:27:11	Add rule	xx.xx.31.63
xx.xx.13.231	2011-07-14 03:42:52	Remove rule	xx.xx.21.62

- Improve DNS protocol performance repairing situations of inefficient parameterization of the DNS server.
  On the DNS server side, considering the capacity of the probe to determine the processing time for each consultation, it is possible to detect cases of excessive delay, which was later confirmed to coincide with of moments of zone update.

Considering the daily progress of DNS queries, before and after applying shaping heuristic to the protocol we obtain an improvement between values of 5.3% (minimum) and 19.4% (maximum).

VII. REDUCING FALSE POSITIVES AND FALSE NEGATIVES

For the treatment of false positives and negatives, it is important to evaluate the results obtained with each of the components in separate – from intrusion detection solution and the solution proposed in the hypothesis presented here, and after evaluating the results that accrue from the application of heuristic indicated above.

It is inevitable given the occurrence of false positives - Type I error (when events are identified as security incidents that do not correspond to real situations) as well as false negatives – Type II error (when there are security incidents that are not detected by the solution in use).

And such an occurrence is the case both in traditional IDS solution - in this case the SNORT, as in the methodology implemented here in the form of prototype with the DNS server at . PT (Country-code top-level domain designed for Portugal).

The way to mitigate such situations is to combine the values obtained by both mechanisms, thus seeking an end result, as close to reality as possible, as identified in Table 6.

 ISBN: 978-1-61208-166-3

TABLE VI – ORIGINAL DECISION VS MID-TERM REVIEW

Original decision (intrusion detection system)	*Mid-term review*
True positive	Correct
False Positive	Type I error
True Negative	Correct
False Negative	Type II error

TABLE VII – DECISION WITH VS WITHOUT THE METHODOLOGY

Original decision	*Decision without the methodology*	*Decision with the methodology*
True positive	Accept	Correct
	Reject	Type II Error
False Positive	Accept	Type I Error
	Reject	Correct
True Negative	Accept	Correct
	Reject	Type I Error
False Negative	Accept	Type II Error
	Reject	Correct

The analysis of the data obtained for a period of 12 months, demonstrated a reduction in 21% of false positives identified by the IDS solution when operated in isolation. The identification of type II errors is now possible in 8% of cases, which previously went unnoticed.

Given the mutual dependence on heuristic established between the two data sources - IDS and the proposed platform, we cannot verify the occurrence of false positives as a result of implementation of the method proposed here. It is, however, possible that false negatives that arise due to situations considered in the IDS solution, can be canceled later in the final assessment.

In any case, considering the relevance of the DNS service on the proper operation of the Internet, the disruption caused by a blockage of a given origin and the fact that there is no absolute certainty that this is a clear case of a security incident, makes it preferable, in this particular case, to allow the occurrence of a controlled number of false negatives

VIII. CONCLUSION AND FUTURE WORK

The solution presented here builds upon the existing solutions that collect statistical information regarding DNS services, by adding the ability to detect and control security incidents in real time. It also adds the advantage of operating in a distributed way, allowing the exchange of information between cooperating probes, and the reinforcement of its own security, even before it is threatened.

In order to improve the ability to detect abnormal behaviors patterns, the solution can be evaluated using a data mining approach.

Currently, the solution presented does not allow the processing of addresses in the IPv6 format. The technical aspects that led to this situation are linked to the need to optimize the performance of the data recorder application making it possible to store the data from all consultations. Nevertheless, all queries made to IPv6 addresses are contained in this solution (AAAA types).

We are also working on extending the data correlation capabilities of the system by adding information collected from other sources (intrusion detection systems for instance). We anticipate that this could be a valuable approach to reduce considerably the number of false positives and negatives [16].

REFERENCES

[1] P. Vixie, “DNS Complexity”, ACM Queue vol. 5, no. 3, April 2007.

[2] D. Wessels, "A Recent DNS Survey", DNS-OARC, November 2007.

[3] Dave Piscitello, “Conficker Summary and Review”, ICANN, May 2010.

[4] SQLDNS website, [http://home.tiscali.cz:8080/~cz210552/sqldns.html]. Last accessed on 27 July 2011.

[5] BIND website, [http://www.isc.org/products/BIND]. Last accessed on 27 July 2011.

[6] Bojan Zdrnja, “Security Monitoring of DNS traffic”, May 2006.

[7] Paul Vixie, D. Wessels, ”DNSCAP – DNS traffic capture utility”, CAIDA Workshop, July 2007.

[8] Duane Wessels, "Whats New with DSC", DNS-OARC, November 2007.

[9] Lawrence Berkeley National Laboratory. Tcpdump website http://www.tcpdump.org.

[10] John Kristoff, "An Automated Incident Response System Using BIND Query Logs", June 2006.

[11] MySQL website – (Open Source Database), [http://www.mysql .com]. Last accessed on 27 July 2011.

[12] IP FILTER – TCP/IP Firewall/NAT Software, [http://coombs.anu.edu.au/~avalon]. Last accessed on 27 July 2011.

[13] P. Saint-Andre, Ed., Extensible Messaging and Presence Protocol (XMPP): Core, RFC 3920, 2004.

[14] Joao Afonso and Edmundo Monteiro, "Development of an Integrated Solution for Intrusion Detection: A Model Based on Data Correlation", in Proc. of the IEEE ICNS'06, International Conference on Networking and Services - ICNS'06, Silicon Valley, USA, July 2006.

[15] Tshark website – The Wireshark Network Analyzer, [http://www.wireshark.org]. Last accessed on 27 July 2011.

[16] Joao Afonso and Pedro Veiga, “Protecting the DNS Infrastructure of a Top Level Domain: Real-Time monitoring with Network Sensors”, WSNS 2008, 4th IEEE – International Workshop on Wireless and Sensor Networks Security, Atlanta, USA, 29 September – 2 October 2008.

 ISBN: 978-1-61208-166-3

Failure Analysis and Threats Statistic to Assess Risk and Security Strategy in a Communication System

Aurelio La Corte, Marialisa Scata'
Department of Electrical, Electronics and Computer Science Engineering
Faculty of Engineering, University of Catania
viale A.Doria 6, 95125, Catania, Italy
Email:lacorte@dieei.unict.it, lisa.scata@dieei.unict.it

***Abstract*—The paper presents and evalutes one of the most important aspects in an information and communication technology system that is to preserve the information from any attacks trying to ensure the protection of data while maintaining quality of service, confidentiality, availability and integrity. In recent years, the process towards convergence has been devoloped to take into account several evolving trends and new challenges. Most of this is about security. New security issues make it necessary to analyse and manage the safety of the information and communication systems. Thus, an economic investment can not ignore the technical evaluation of the system, vulnerabilities analysis, threats taxonomy, and the estimate of expected risk, in order to ensure proper countermeasures to limit the technological and economic damage over time. Risk analysis involves the technical, human and economic aspects, to guide strategy of investment. Following a bio-inspired approach, this analysis requires knowledge of the failure time distribution and survivor analysis to estimate risk. With this paper, we propose a step-by-step analysis based on bio-inspired models, showing and validating that the risk in the absence of explanatory variables that influence the impact of threats, and neglecting the possible relationships between them, does not change shape.**

Keywords-ICT; Security; Survivor Analysis; Bio-Inspired; VoIP.

I. INTRODUCTION

Information and Communication Technology (ICT) is the set of technologies to develop, communicate and share information through digital mean ICT represents the design, development, implementation, support and management of information systems through the use of telecommunications systems. The ICT links two components, the information technology (IT) with the Communication Technology (CT), and at the same time it is an essential resource in modern organizations, within which it becomes increasingly important to be manage to operate quickly and efficiently the use of data and the increasing volume of information. Information is defined in [1][7][8], as an important business asset, that can exist in many forms. Information can be managed, manipulate to be available to the users at any time. Then, we must take note of the means available to analyze the risk and issues to information security. In many processes the security risk has recently gained in significance. Risk analysis is important such as the planning phase of the information system architecture. The objective is to protect the infrastructure, and information from attacks that can compromise the safety requirements, such as confidentiality, integrity and availability. In recent years, technological evolution is faced with the problem of security methodologies that propose remedial actions, and not with estimates and analysis to assess the expected risk. From the Internet network to the future next generation network (NGN), switching to new concepts such as opportunistic communication networks and green, these networks arise from the interaction and the strong conceptual link that exists between the world of technological networks and biological networks. Many devices are now mobile and autonomous and must adapt to its surroundings in a distributed way, even in the absence of coordination central unit. In literature, there are many approaches and models inspired by biological processes as a strategy to design and manage modern networks. Many of these, however, focused only in certain areas. With this paper, we want to address the risk issue of a generic communication system such as voice over IP (VoIP), inspired by bio-inspired models, and making use of survivor analysis. We want to demonstrate, through case study and evaluation of the main threats facing it, that risk is not the shape function depends on the distribution of failure events due to an attack was successful.

After a brief introduction and related work, presented in Section I and Section II, in Section III and Section IV, we discuss about the security issues on communication systems and about the bio-inspired approach. In Section V, we introduce the survivor analysis for ICT security and the model to evaluate the failure time distrubutions. In Section VI, we present the model to estimate risk and failure in a VoIP system, and the test that we have done about three common threats. Finally, we present a conclusion and future works.

II. RELATED WORK

A general consolidated study on the degree of security of an ICT system is still lacking [1]. There is a general tendency to treat the issue of security in communications through taxonomies of vulnerabilities and threats [2][3][4].

 ISBN: 978-1-61208-166-3

About risk analysis and management for information system security [9][10][11][13] and statistical methods [5][6][14], there are some papers that deal with the relationship that exists between the two disciplines. About VoIP security we surveyed many research papers, such us [2][3][4]. Most current treatments concerning taxonomies, or security mechanism concerning particular aspects of communication. Recognizing the work presented in many papers also about bio-inspired approach [15][16][19][20], about risk perception and statistical models biologically inspired [12][13][14], and about comparison among computer virus and biological virus [17][18], we believe we can advance the hypothesis to investigate the security issue in a broader vision, to estimate the economic risk as a result of an investment in security, obviously linked to the technological risk of a communication system. This is important to assess in the future the best countermeasures to limiti the damage, to change the shape of risk, minimising the losses about information and about economic investments [21].

III. Bio-Inpired Models for ICT Security

In examining some of the most common structures or algorithms used today in telecommunications networks, we can find striking similarities with biological systems [13][14][15][16]. Evidence suggests that the nature and the designers of the networks have had to not only solve similar problems, but they are also arrived at similar solutions. Seems entirely reasonable, then, to think that the new problems in systems communication may have much in common with biological issues already known and have been resolved long ago. With the increase in size, interconnectivity and number of access points, computer networks have become increasingly vulnerable to various forms of attack. Similarly, biological organisms can be considered as interconnected complex systems with a high number of access points, subject to attacks by microorganisms [17][18]. However, during evolution, biological organisms have successfully developed the immune system that allows them to detect, identify and destroy pathogens outside. The technological challenges is leading us towards a world where myriad devices, fixed or mobile, interact with each other in many ways. Many of these devices are mobile and autonomous,and they must then adapt to its surroundings in a distributed way and without a coordination of a central entity. Recently, a number of approaches have been proposed, inspired by biological processes and mechanisms as a strategy to manage the complexity of distributed systems like Internet, sensor networks, wireless and ad hoc networks. The aim of bio-inspired approaches is to discover and adapt traditional principles of biological systems to technical solutions, which have characteristics of stability, adaptability and scalability. Many studies aim to highlight the achievements under the new Bio-Inspired Networks [19][20]. In particular, the topic that focuses identification of mechanisms and models applicable to biological technical solutions for ICT systems. This is the attempt to compare directly the technical solutions, the theoretical principles and mathematical models used by biological systems and the challenges of communication systems and information systems. We can summarize the main aspects of networking and communications systems that are addressed using an approach Bio-Inspired as follows:

- Self-organizing communication systems.
- Evolutionary and adaptive systems and protocols.
- Scalable and adaptive protocols and network architectures.
- Self-learning algorithms.
- Self-healing systems and protocols.
- Security mechanisms.
- Network algorithms and protocols.
- Congestion control mechanisms.
- Performance evaluation of bio-inspired networks.

The similarity between the defense mechanisms of living organisms and security problems of telecommunications networks has attracted great interest among researchers, who already have long studied the similarities. The thinking behind these efforts is to capture the dynamics that rule biological systems and understanding the foundations, to develop new methodologies and tools for the design and management of the information and communication systems. Communication systems such as biological systems are characterized by high complexity, high connectivity and dynamics. Both allow for extensive interaction between the components, and heterogeneity in terms of capacity. They have both vulnerability to external intrusion, intentional or not, which can cause system failures resulting in degradation of safety requirements. Thus the similarities are not limited to those between pathogenic agents that can infect a organism, and malicious code that can infect communication system. There is also similarity between the process of safety management, and global view of relationships between vulnerability, threat and asset, just like the relation between biological viruses, vulnerabilities, and people in a population. The final result is a risk of failure and impairment of confidentiality, integrity and availability in an ICT system, such as the risk of the occurrence of a disease in a biological organism. The analysis of risk requires knowledge of the probability and its distribution and the probability that an attack occurs [5][6][9][11]. We can asses the degree of the system security and analyse the existing countermeasures to try to decrease the risk and minimimise the losses, maintainng the security requirements for an ICT systems:

- Confidentiality
- Availability
- Integrity

IV. Overview of Survivor and Failure Analysis

In many biomedical applications, the variable is the time it takes a certain event to occur, that is, how much time

 ISBN: 978-1-61208-166-3

elapses from the beginning of the study of the "system" so that a given event occurs. For example, the event may be the death of an organism, from the time it takes for a patient to show signs of reaction to a therapy or the time to recurrence of a disease. In practical cases we may be interested in determining a statistical distribution of the times of occurrence of events for a population of individuals, or to compare the times of occurrence between distinct populations (for example the case of two populations, a subject to a therapy clinic another and not receiving any treatment), or to determine a relationship between the times of occurrence and other variables that may affect the entities in question. Both in biomedical applications as the observation of a telecommunications system, measurements of the times of occurrence of the events are carried out within a period of limited extent. A consequence of this limitation is that not all individuals will be affected by the occurrence of an event. All this characterizes what is called Survival Analysis [5][6]. We indicate with T a positive random variable representing the time of occurrence of our events. Thus, we can define the survival time as the interval between the birth of an individual after his death. For obvious reasons, the survival is linked to the notion of failure. A failure event in general, could be due to an attack by malevolent individuals or groups that want to damage the security system. A failure doesn't meaning the total distruction of the system, but even the impairment of the informations that it holds. Ryan and Ryan in [9][10][11] models a general information infrastructure in number of finite information systems $\{S_i : i \in I\}$, where, $S_i \neq S_j$ if $i \neq j$, and the set I= {0,1,2,3,.....}. Each system, which purpose is to preserve the information, can be thought as a finite collection of information assets S_i=$\{\alpha_k$:k $\in$ I $\}$. Threats can destroy or only degrade information, compromising the security requirements. For each individual asset and for the entire system it is possible to define the following functions:

- Survivor Function S(t), which is the probability of being operational at time t :

$$S[t] = P_r[T \geq t] = 1 - F(t) \quad (1)$$

  where F(t) is the Failure function, which tell us the probability of having a failure at time t.
- Failure Density Function f(t), which is the probability density function:

$$f(t) = \frac{dF(t)}{dt} = -\frac{dS(t)}{dt} \quad (2)$$

- Hazard Function h(t), which is the probability that an individual fails at time t, given that the individual has survived to that time:

$$h(t) = \lim_{\delta \to 0^+} P_r(t \leq T < t + \delta \mid T \geq t)/\delta \quad (3)$$

  where $h(t)\delta t$ is the approximate probability that an individual will die in the interval $(t, t + \delta t)$, having survived up until t
- Cumulative hazard function H(t):

$$H(t) = -\log S(t) \quad (4)$$

V. Risk and Failure in a VoIP System

The VoIP system, in this case we will discuss in this paper, is the "population" under observation and individuals of that population are so-called information assets. Each asset is involved in the processes that regulate VoIP, and each is vulnerable to a range of possible threats. An attack occurs when a threat occurs, using the right vulnerability and causing a failure. The risk is simply the probability that this event occurs. The damage is the impact on the system. In this case we do not consider the influence of an asset attacked to another asset not attacked, and how the spreading of risk within the system itself. In this paper we consider the global system failure and the events affecting it.

A. VoIP and Threats Taxonomy

The new trends of the communication is the move towards the transmission of voice over traditional packet switched IP network, voice over IP. VoIP is the rst step for the future convergence.The large-scale deployment of VoIP infrastructures has been determined by high-speed broadband access. This technology of communication includes a large variety of methods enabling the transmission of voice directly through the Internet and other packet-switched networks. VoIP is an attractive alternative compared to traditional telephony for several reasons, such as seamless integration with the existing IP networks, low cost phone calls not expensive end-users. The main advantages of VoIP are flexibility and low cost. The first comes from an open architecture and a software implementation, while the second is due to the emergence of a new business model, the unification of devices and network links for the transport voice and data. Thanks to these benefits, VoIP has seen a rapid spread in both enterprise that among private users. A growing number of companies has already converted or are being converted to VoIP, to allow the implementation of new features, both to reduce management costs. Among the private account, the main point of attraction of VoIP is the low cost service. To offset the high flexibility of VoIP we have an equally high complexity, due to architectural and protocol factors. The rapid adoption of VoIP introduced new weaknesses and more attacks, whilst new threats of networks have been recorded which have not be reported in traditional telephony[2][3][4]. The VoIP infrastructure is characterised by several assets:

- Network and Service Access.
- Protocols.
- Processes.
- Service Infrastructure.
- Physical Component Architectures.
- APIs and Network Peering.

 ISBN: 978-1-61208-166-3

Threats	C	I	A
Eavesdropping	x		
DoS			x
Vishing	x	x	
Fraud		x	
Masquerading		x	x
Physical Intrusion	x	x	x
Service Abuse		x	x
Social Threats		x	x

Table I
THREATS IMPACT ON CIA REQUIREMENTS

- Business Areas.

Although it is a technology that is being rapidly deployed, there are many security challenges and the benets of VoIP are as strong as security issues. We briey listed the main threats associated with this technology [2]:

- Eavesdropping.
- DoS.
- Vishing.
- Fraud.
- Masquerading.
- Physical Intrusion.
- Service Abuse.
- Social Threats.

In Table I, we listed the principal threats and the assessment of the impact on confidentiality, integrity and availability, that are the most important security requirements also called CIA requirements.

B. Analysis Model

A VoIP system, such as any other information systems or network communication can be compared to a biological system. Each of its constituent elements can be seen such as a individual of a population. From the perspective of the study of threats and resistance to their attacks, a VoIP system can be studied following the models and mathematical principles of Survival Analysis, which is widespread in the study of the effectiveness of therapies clinical population suffering from certain diseases. For this reason it is possible to characterize a VoIP system through its survival function, or through its hazard function. We have simulated a VoIP system under stressful conditions. The test is stopped after a fixed amount of time, Toss. As results, some items fail during the test, while other survive. We considered three types of threats during a fixed period of 100 days. The threats considered are those that statistically, are the most frequent: Denial of Service (58%), Eavesdropping (20%) and Social Threats (18%). These threats have a relapse rate of respectively cases of failure of a VoIP system. By hypothesis each of these threats gave rise to the failure of system that were distributed along the 100-day period and each of these threats acting on the system, and causes of failure, exploiting the vulnerability. We assume an observation time 100 days, and three possible cases of distribution:

- Case 1: The failure events caused by the three threats are distributed according to a Weibull distribution, with equal parameters, scale factor A=50, shape factor B=10, as in Figure 1.
- Case 2: The failure events caused by the three threats are distributed according to Weibull distribution, but are considered different values for each,DoS (A=50, B=3) Eavesdropping (A=50, B=5), Social Threats (A=50,B=10), as in Figure 2.
- Case 3: The failure events caused by the three threats are distributed according to 3 different distributions, Weibull, Exponential and Rayleigh, as in Figure 3.

Each of these distributions are "weighted" according to a coefficient given by the statistical impact of the threat.

$$F_{tot}[t] = th_{1\%}F_1[t] + th_{2\%}F_2[t] + ...th_{n\%}F_n[t] \quad (5)$$

$$H_{tot}[t] = -log(1 - F_{tot}[t]) \quad (6)$$

The trend of the function of the total hazard is independent of the particular case. From the viewpoint of security countermeasures to be taken in a VoIP system, it is not important to know in advance the distribution of failure associated with threats. This assertion is supported by the evidence that changing characteristic parameters of the distributions involved, the total hazard function did not show significant changes in its trend. This result shows that, with random distribution of possible threats, the distribution of failures and the shape of the risk remains unchanged at less than a constant. This suggests that the shape of the risk function is not depends on the timing distributions of failures. The risk increases dramatically if you do not act in any way with security investment. In this case, we can see the change of the survival distribution with different distributions. The curve move to the right if we change the distributions. This tells us that the only influence is in the delay of the distributions of failure events so this allows an extension of time for decisions and managing security in an information system. In this case we considered the total absence of security investment [21]. We showed that the risk in the absence of explanatory variables that influence the impact of each threat, and neglecting the possible relationships between the different threats, does not change shape. A good economic investment then applied in order to improve security, must take into account these claims. This is important for future consideration of countermeasures and the choice of strategy to use when referring to safety action to be taken.

VI. CONCLUSION AND FUTURE WORK

In this paper, we introduced and proposed a different bio-inspired approach for the security of information systems. The bio-inspired in the ICT should help inspire the design of a system for managing network security measure to

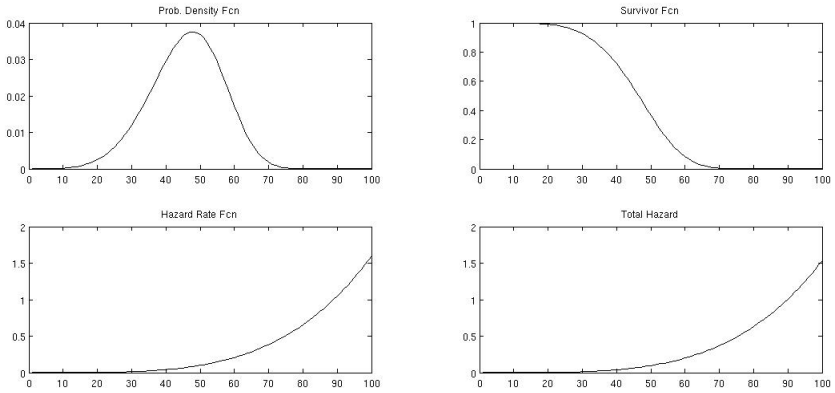


Figure 1. Weibull distribution

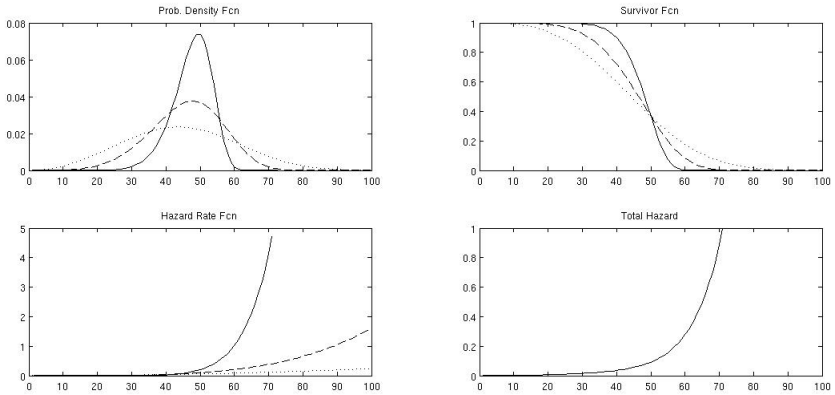


Figure 2. Weibull distribution with different parameters

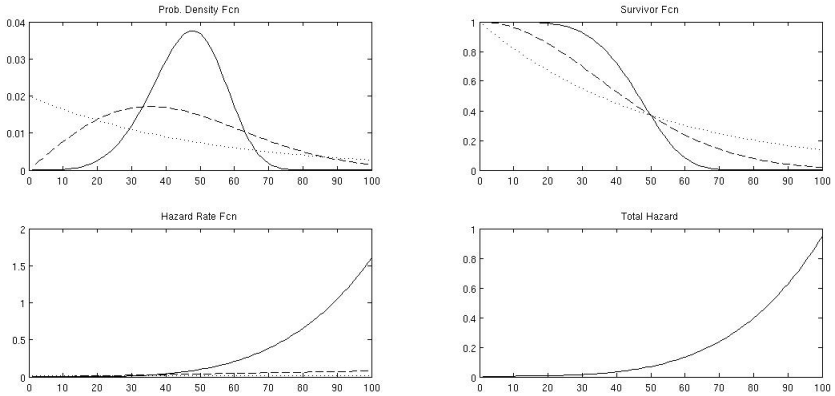


Figure 3. Weibull distribution, Exponential distribution, Rayleigh distribution

prevent the attack, and to estimate the risk, to assess the expected risk, to decide strategically technological and economic investments,maintaining good relationship between the quality of service, security and network reliability. Following the study of the behavior of a VoIP system in against a combination of these threats, each with a well defined distribution function of failure times within a 100-day period, the results allow us to say that in terms of countermeasures to be implemented for the protection of a VoIP system against threats how Denial-of-Service, Social Eavesdropping Threats, is not essential to know in advance distribution time of failure associated with them. In future the intention is to study the impact of a threat in terms of technological and economic risks, and the influence that an attacked asset, within a VoIP system, can have on asset logically associated with it. The study is a starting point for a deeper analysis of the risk in a VoIP system upon application of Bio-Inspired approach.

REFERENCES

[1] V. Leveque, 2006, *Information Security: A Strategic Approach*, IEEE Computer Society, J. Wiley and Sons.

[2] VoIP Security Alliance, *VoIP Security and Privacy Threat Taxonomy*, available at www.voipsa.org, [accessed: Oct., 2011].

[3] A. D. Keromytis, 2010, *Voice-over-IP Security: Research and Practice*, IEEE Computer and Reliability Societies, Secure Systems, Vol. 8, Issue 2, pp. 76-78.

[4] A. D. Keromytis, 2009, *Voice over IP: Risk, Threats and Vulnerabilities*, In Proc. of the Cyber Infrastructure Protection (CIP) Conference, New York, NY.

[5] D.Roxbee Cox and D. Oakes, 1984, *Analysis of Survival data*, CHAPMAN & HALL/CRC.

[6] D. Roxbee Cox, 1972, *Regression Models and life-tables*, Journal of the Royal Society, Series B (Methodological), Vol. 34, No. 2, pp. 187-220.

[7] International Standard ISO/IEC 27002:2005, *Information Technology Security techniques. Code of Practice for information security management*.

[8] International Standard ISO/IEC 27005:2008, *Information Technology Security techniques. Information Security Risk Management*.

[9] J. C. H. Ryan and D. J. Ryan, 2008, *Performance Metrics for Information security Risk management*, IEEE Computer Society, Security and Privacy, Vol. 6, Issue 5, pp. 38-44.

[10] J. C. H. Ryan and D. J. Ryan, 2008, *Biological System and models in information Security*, Proceedings of the 12th Colloquium for Information System Security Education, University of Texas, Dallas.

[11] J. C. H. Ryan and D. J. Ryan, 2006, *Expected benefits of information security investments*, Computer and Security, Vol. 25, Issue 8, pp. 579-588. ScienceDirect, www.sciencedirect.com.

[12] Stephan Kitchovitch and Pietro Lió, 2010, *Risk perception and disease spread on social networks*, International Conference on Computational Science, Vol. 1, Issue 1, pp. 2339-2348.

[13] J. M. Lachin, 2000, *Biostatistical Methods: The Assessment of Relative Risks*, John Wiley & Sons.

[14] J. D. Kalbfleish and R. L. Prentice, 2002, *The Statistical Analysis of Failure-Time Data*, 2nd edition, Wiley.

[15] W. H. Murray, 1988, *The application of epidemiology to computer viruses*, Computer & Security, Vol. 7, Issue 2, pp. 139-145.

[16] Falko Dressler and Ozgur B. Akan, 2010, *A Survey on Bio-Inspired Networking*, Elsevier Computer Networks, Vol. 54, Issue 6, pp. 881-900.

[17] Jun Li and Paul Knickerbocker, 2007, *Functional similarities between computer worms and biological pathogens*,Elsevier Computer & Security, Vol. 26, Issue 4, pp. 338-347.

[18] Michael Meisel, Vasileios Pappas, and Lixia Zhang, 2010, *A taxonomy biologically inspired research in computer networking*, Elsevier Computer Networks, Vol. 54, Issue 6, pp. 901-916.

[19] M. Wang and T. Suda, 2001, *The Bio-Networking Architecture: A Biologically Inspired Approach to the Design of Scalable,Adaptive, and Survivable/Available Network Applications*, in 1st IEEE Symposium on Applications and the Internet (SAINT), San Diego, CA, pp. 43-53.

[20] C. Lee, H. Wada, and J. Suzuki, 2007, *Towards a Biologically-inspired Architecture for Self-Regulatory and Evolvable Network Applications*, in: F. Dressler, I.Carreras (Eds.), Advances in Biologically Inspired Information Systems - Models, Methods, and Tools, Studies in Computational Intelligence (SCI), Springer, Berlin, Heidelberg, New York, Vol. 69, pp. 25.

[21] Aurelio La Corte, Marialisa Scatá, and Evelina Giacchi, 2011, *A Bio-Inspired Approach for Risk Analysis of ICT Systems*, Computational Science and Its Applications - ICCSA, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, pp. 652-666.

 ISBN: 978-1-61208-166-3

An Approach to Estimate Regulatory Performance

Kemal Huseinovic, Mirko Skrbic, Zlatko Lagumdzija
Communications Regulatory Agency, Faculty of Electrical Engineering, Faculty of Economy - University of Sarajevo
Bosnia and Herzegovina
khuseinovic@rak.ba, mirko.skrbic@etf.unsa.ba, zlatko.lagumdzija@efsa.unsa.ba

***Abstract*—In order to follow the trends imposed by globalization, the regulation should be based on technological neutrality and market orientation. The aim is to protect the interests of users, strengthen the competition, support involvement of new participants on the market and exert positive influence on the economic growth. Technological convergence enables all types of networks to provide almost any service, thus imposing the need for the regulation to follow the same trend. In order to minimize the differences among communication market beneficiaries, it is necessary to harmonize the communication market legislative framework among countries. In our view, the most efficient harmonization is achieved with support from convergent regulatory authorities of the communications market. The regulatory performance is measured using statistical techniques on data obtained from interviewing relevant European institutions and authorities.**

Keywords - Regulation; Organization; Competition

I. INTRODUCTION

In the world of increased global competitiveness, where the competitors are no longer limited only to the local market, the countries can no longer risk losing the opportunities and advantages brought on by the convergence of markets, technologies and services for the sake of artificial barriers of their regulatory frameworks.

These regulatory frameworks were set up at a time before the strong and aggressive wave of convergence struck all forms and spheres of the communications market. Consequently, one must come to a conclusion that they were not designed for this era of overall convergence.

In order to follow the trends imposed by globalization, regulation should be based on technological neutrality and market orientation,. This is all aimed at protecting the interests of users, strengthening competition, supporting involvement of new participants on the market and exerting positive influence on the economic growth.

Technological convergence enables all types of networks to provide almost any service, thus imposing the need for the regulation to follow the same trend..In such a situation, it would be almost impossible to have fair market services in different types of networks, where the subjects have different sets of regulatory rules and are under the jurisdiction of different regulatory authorities.

In case of separated regulatory authorities for telecommunications and media, there is a potential danger of the so called regulatory uncertainty (EC [6]). That is a situation when one service provider (e.g. «triple play») has to obtain a work permit from both regulatory authorities, which makes the process of its marker entry more complex, longer and more expensive. Quite frequently, but not necessarily, their market approach rests upon the concept of one bill per one user. One bill containing costs of transfer of data, voice, television and video presents a significant saving for the user. With a higher number of services included, the price of individual service in the package usually decreases. Somewhere, nevertheless, all obstacles have been removed and the operators may freely offer their type of television subscription.

As well as big media houses, the cable and telephone operators have shown significant interest in technology, creating the opportunity for the transmission of all three media through one network. Their goal is to seize upon the market potential offered by the service and to maintain the existing subscribers of the basic telecommunication services. In order to minimize the differences among the communication market beneficiaries, it is necessary to harmonize the communication market legislative framework among countries. The most efficient harmonization is achieved with support from convergent regulatory authorities of the communications market. The convergent has been present in Bosnia and Herzegovina since 2003.

This paper includes a clearly stated research goal followed by the description of the statistical techniques and interview design. It finishes with results confirming the organization of operators in Bosnia and Herzegovina.

II. THE RESEARCH FRAMEWORK

The conducted research proved the following hypotheses:
(1) the convergent form of communication market regulatory authorities improves the country's competitiveness;
(2) convergent rather than separate regulatory authorities are a more appropriate model for ensuring development of the communication market on the territory of a country;
(3) organizational form affects the ability of a regulator to implement European directives in the telecommunications sector.

 ISBN: 978-1-61208-166-3

The importance of research is established from the need to implement the standardization of regulatory practices on the international level and the influence of the practices on the competitiveness of national economies on a global scale.

It is quite clear why competitiveness has become one of the main preoccupations of governments and industries of almost every nation in the world (Porter [19]).

Development strategies of modern countries, this way or the other, are basically measured by the economies' achieved degree of competitiveness. According to the definition presented by the USA Economic Advisory Board, which was in a later stage accepted within the European Union, competitiveness in its essence has a goal to improve the living standard (Michalis [18]).

M. Porter [19] claims that the only importance of the concept of competitiveness at the national level is national productivity. The living standard progression depends on the capacity of national companies to achieve a high level of productivity and to increase this productivity in time (Porter [19]). Due to all-present information in the value chain, a fast change in ICT has an enormous influence on the competitive advantage and competitiveness (Porter [19]). New related technologies and are being taken as the main resource and a good indicator for global competitiveness (Castells [4]).

There are numerous models of measuring competitiveness in the world some of which include: Global Competitiveness Index – GCI, Network Readiness Index – NRI, ICT Development Index- IDI, etc.

The trend of convergence of regulation is also a form of accelerated and forced standardization. Namely, each country, particularly those in transition, are witnessing the integration of the communication sector and broadcasting, together with forced stimulation of modernization of these spheres at the level of the regions within the country itself. The optimal model of organization of regulatory authorities stimulates internationalization of standards, local development of these sectors, maximal degree of development of competition on the communication market, promotes foreign investments and, triggers the growth of living standard of citizens.

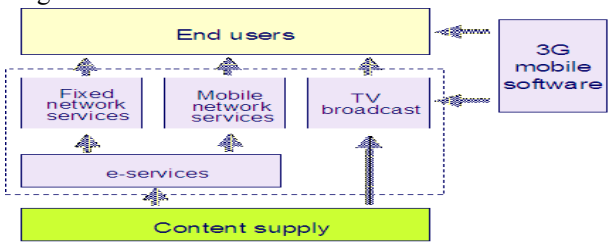


Figure l. Trend of convergence of telecommunication and broadcasting services

The model of a „convergent regulator" is being imposed as an optimal organizational structure from the point of view of convergence of technology and stimulation of technological and communication market development. The technological analysts have been stating for quite some time that all forms of electronic communications will merge into one.

In this view, radio and television broadcasters and telecom operators will extensively keep entering into each others' markets, directing them towards convergent approach to market/consumers (joint service packages), with a tendency towards the so called "free" services, so that costs of these services get redirected to advertisers and direct marketing clients.

III. The Methodology

Both primary and secondary data sources were used for the paper design. The following competitiveness models and indicators were applied: Global Competitiveness Index – GCI, Network Readiness Index – NRI and ICT Development Index- IDI.

The research of regulatory authorities in Europe was conducted on a sample of 79 regulators, based on the designed survey, close-end questions. Responses from 61 regulatory authorities, or 77% of the total number of respondents, have been obtained. Out of this number, responses were obtained from 8 convergent regulators, 27 media regulators and 26 telecommunication regulators. The methods of response collection included electronic mail, direct contacts of authors with the officials of other regulators on international gatherings, and by fax. During the design of survey questions, the system of Likert scale was used, with offered responses rated from 1 to 5 (Kukić and Markić [15]). The survey questions have examined the regulatory bodies' stances on the influence of a convergent regulator onto the quality of technological neutrality implementation and effects exerted by the regulatory authorities on the telecommunication and broadcasting development. In order to analyze the data, the structural analysis and descriptive statistics were used together with the application of „chi square" and „t" tests. The data was processed using the software package „Excel" and statistical package SPSS14, and the results were presented in tables and figures. Options of testing and descriptive statistics were used at the same time to examine the significance of the sample interval, as well as deduction on the basis of the achieved results.

The interview was also conducted on a sample of 51 experts in the fields of telecommunication, broadcasting and regulation services. The designed survey questions were related to organizational form of a regulator and its capacity to implement the European directives.

IV. The Results

USA and Canada have had combined regulatory agencies for telecommunication and broadcasting for decades. Within the last fifteen years, some other countries have started to establish single, merged regulatory authorities that regulate both broadcasting and telecommunication segments. In the recent years, a noticeable progressive trend in the number of convergent regulatory agencies has been present. It is

 ISBN: 978-1-61208-166-3

obvious that more and more countries have decided to choose this institutional form of the state regulatory authorities whose jurisdiction covers regulation of all forms of communication technologies, including both the broadcasting and telecommunications sectors.

It is more cost effective for countries to finance and maintain the work of one agency instead of several regulatory authorities.

The new regulatory framework of European Union provides for regulatory treatment of service convergence. The framework introduces the notion of "electronic communication services" instead of the previously used "telecommunication services + broadcasting services", pointing to a clear signal of convergent regulatory approach to a wider spectrum of communication services. Italy was the first country in Europe that has established convergent regulatory authorities for communications. It was followed by Finland, Bosnia and Herzegovina, Slovenia, Switzerland, and others. Following the introduction of the new EU framework, Great Britain responded by forming a convergent communication regulator in 2003, which replaced the previous five separate regulatory authorities in charge of telecommunication, radio-frequency spectrum and broadcasting.

Malaysia has had a convergent regulation in force since 1999, introducing a regulatory framework exclusively designed to adjust to the phenomenon of convergence. Malaysian convergent regulator (Malaysian Commission for Multimedia and Communications (MCMC) was among the first in the world to introduce a technologically and service-wide neutral system of issuing permits. Singapore was also one of the first in Asia who chose a convergent model of regulatory authorities. Brazil was the first in South America to introduce a convergent regulator (ANATEL), as early as in 2001. In Africa, it was South Africa that established a convergent regulation (ICASA) in 2000. During the last decade some of the developing countries have also established convergent regulators (ITU [11]).

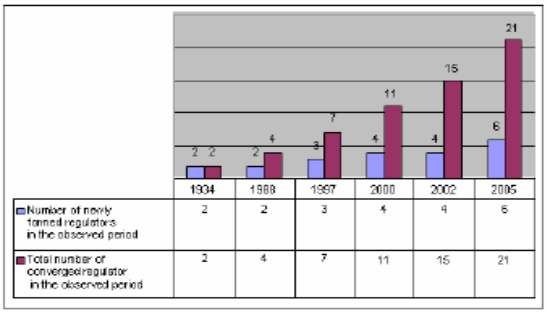


Figure 2. The formation trend and growth in the number of convergent regulators

The following results are based on the analysis of positions of the countries which have introduced a convergent form of communication market regulatory authorities from the aspect of different measures of competitiveness: Global Competitiveness Index – GCI, Network Readiness Index – NRI, ICT Development Index-IDI.

Table 1 presents the position of the countries with a convergent regulator against GCI index in the period 2004-2009 - the ranking list of countries with convergent regulators according to GCI, sources: [5] and [16] p. 13). According to the ITU research, there are 254 regulatory bodies in the world, with 21 countries, or less than 8% of the total number of countries, having a convergent form of regulatory authorities, According to GCI, on the top-ten list of countries in the world in the last five years, there are seven countries, or 70%, with a convergent form of regulatory authorities. Consequently, 8% of countries with a convergent regulator participate with 70% among the top ten ranked countries according to GCI.

This significant piece of data opens some dilemmas and raises a number of questions. Is the high ranking of countries, according to GCI index, the result, among other things, of their decision to choose a convergent form of a regulator? The fact that seven out of ten countries with most competitive economies in the world chose a convergent regulation may indicate that this is a trend to be followed. It can be stated that this analysis adds value to the claim that a convergent form of regulatory authorities has a positive impact on the development of a communication market and increases the level of competitiveness of a country.

TABLE I. THE RANKING OF CONVERGENT REGULATORS

Country / Economy	GCI 2004-2005	GCI 2005-2006	GCI 2006-2007	GCI 2007-2008	GCI 2008-2009
USA	2	1	1	1	1
Switzerland	8	4	4	2	2
Singapore	7	5	8	7	5
Finland	1	2	6	6	6
Germany	13	6	7	5	7
Japan	9	10	5	8	9
Canada	15	13	12	13	10
United Kingdom	11	9	2	9	12
South Korea	29	19	23	11	13
Austria	17	15	18	15	14
Australia	14	18	16	19	18
Malaysia	31	25	19	21	21
China	46	48	54	34	30
Slovenia	33	30	40	39	41
South Africa	41	40	36	44	44
Italy	47	38	47	46	48
Brazil	57	57	66	72	63
BiH	81	88	82	106	105
Tanzania	82	105	97	104	110
Malawi	87	114	117	n/a	n/a
Iraq	n/a	n/a	n/a	n/a	n/a

Table 2 presents global rankings of countries in the period 2005-2009 according to NRI index [5]. Among the top twenty countries in the last five years according to NRI index, there are twelve that have a convergent form of regulatory authorities, which makes 60% of the countries taking up the top-twenty positions.

 ISBN: 978-1-61208-166-3

TABLE II. RANKINGS ACCORDING TO NRI INDEX

Country/Economy	NRI 2005-2006	NRI 2006-2007	NRI 2007-2008	NRI 2008-2009
USA	1	7	4	3
Switzerland	2	3	5	4
Singapore	9	5	3	5
Finland	5	4	6	6
Germany	6	11	13	10
Japan	14	19	9	11
Canada	7	13	11	12
United Kingdom	15	15	14	14
South Korea	9	10	12	15
Austria	18	17	15	16
Australia	16	14	19	17
Malaysia	17	16	16	20
China	24	26	26	28
Slovenia	35	30	30	31
South Africa	42	38	42	45
Italy	37	47	51	52
Brazil	52	53	59	59
BiH	97	89	95	106
Tanzania	n/a	111	n/a	110
Malawi	84	91	100	119
Iraq	n/a	n/a	n/a	n/a

Having in mind that the NRI index rests upon three assumptions – environment, readiness and ICT use, it is obvious that well-developed countries which have enabled the convergence, have a stimulating regulatory framework of communication technologies which enhances the influence of ITC on economic development together with the level of development of the communication market. This information can also serve as contribution to the statement that a convergent form of regulatory authorities has a positive impact on competitiveness.

Table 3 presents the global rankings of countries in 2002 and 2007 according to the IDI index. It is evident that, out of the twenty highest ranked countries according to this index, twelve of these, or 60% have a convergent form of regulator. Therefore, according to the analysis of results of a relevant research conducted by the World Economic Forum and the International Telecommunication Union [5] [10], it can be stated that, among the top twenty countries in the world in terms of competitiveness, over 50% of the countries have convergent regulators.

These results contribute to proving a part of the main hypothesis, that a convergent regulatory authority is optimal from the point of view of achieving a maximal degree of the communication market development, protection of users and raising the level of competitiveness of a country. Most regulators also believe that a convergent rather than a separate organizational form of regulatory bodies has a positive influence on the development of telecommunication and broadcasting fields. What is significant is that although less than 10% of the countries in the world have convergent regulatory authorities, these countries are extremely highly ranked on all competitiveness measuring scales.

TABLE III: THE RANKING ACCORDING IDI INDEX

Country/Economy	Rank 2007	IDI 2007	Rank 2002	IDI 2002
South Korea	2	7.26	3	5.83
Switzerland	8	6.94	7	5.42
Finland	9	6.79	8	5.38
United Kingdom	10	6.78	10	5.27
China	11	6.70	12	5.10
Japan	12	6.64	18	4.82
Germany	13	6.61	14	5.02
Australia	14	6.58	13	5.02
Singapore	15	6.57	16	4.83
USA	17	6.44	11	5.25
Canada	19	6.34	9	5.33
Austria	20	6.32	20	4.64
Italy	22	6.18	24	4.38
Slovenia	28	5.88	22	4.47
Malaysia	52	3.79	50	2.74
BiH	58	3.54	66	2.33
Brazil	60	3.48	54	2.55
South Africa	87	2.70	77	2.11
Malawi	141	1.17	141	0.95
Tanzania	145	1.13	138	0.96
Iraq	n/a	n/a	n/a	n/a

Convergence of infrastructure based on the next generation of networks provides for access to a wide spectrum of services, requires convergence of regulation and, presents the optimal option from the perspective of the end user. In order to analyze and prove this auxiliary hypothesis we used an interview of regulatory authorities.

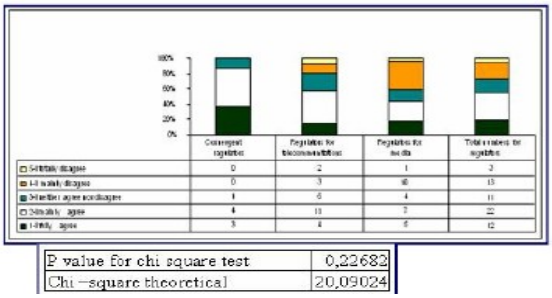
Table 4 presents the attitudes of the European regulatory bodies based on the question whether a convergent form of regulators provides a better quality implementation of the principle of technological neutrality in regulatory processes than separate regulatory authorities. A positive reply to this statement has been provided by 34 respondents, or 56% of the overall respondents. Eleven, or 18% of respondents, provided a neutral reply. Sixteen respondents, or 26% of them, expressed their disagreement with this statement, with only three respondents who fully disagreed with it.

Figure 3 provides a graphic structure of the expressed attitudes of regulatory authorities in percentage.

TABLE IV : THE INFLUENCE ON NEUTRALITY

Convergent regulator ensures better quality implementation of principle of technological neutrality in regulatory processes than separate regulatory authorities.	Convergent regulators	Regulators for telecommunications	Regulators for media	Total number of regulators
1	3	4	5	12
2	4	11	7	22
3	1	6	4	11
4	0	3	10	13
5	0	2	1	3
Total	8	26	27	61

 ISBN: 978-1-61208-166-3

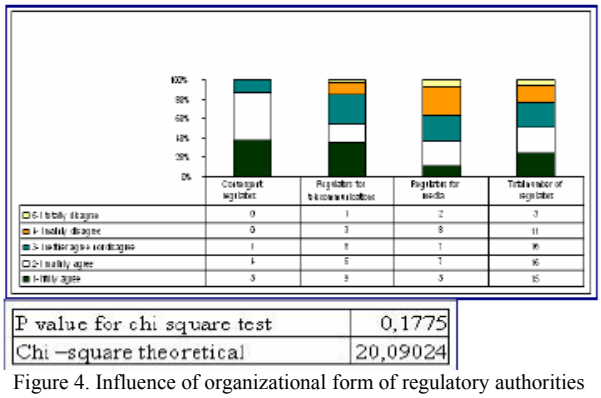


P value for chi square test	0,22682
Chi –square theoretical	20,09024

Figure 3. Influence of convergent regulator on implementation of technological neutrality

TABLE V: THE INFLUENCE ON DEVELOPMENT

Convergent form of organization of regulatory authority has more positive influence on development of telecommunications and broadcasting services than separate regulatory authorities for telecommunications and broadcasting	Convergent regulators	Regulators for telecommunications	Regulators for media	Total number of regulators
1	3	9	3	15
2	4	5	7	16
3	1	8	7	16
4	0	3	8	11
5	0	1	2	3
Total	8	26	27	61



P value for chi square test	0,1775
Chi –square theoretical	20,09024

Figure 4. Influence of organizational form of regulatory authorities on development of telecommunications and broadcasting

Table 5 gives an overview of results of the interview with European regulatory authorities based on the question whether a convergent form of a regulator has more positive influence on the development of broadcasting and telecommunication services than separate authorities. Out of 61 stated opinions of regulators, 31 assessed that a convergent form has a more positive influence, 16 viewed that its influence is neutral, whereas 14 evaluated that it does not have any more positive influence on development of telecommunication and broadcasting than separate regulatory authorities. It is obvious that the weight is on the side of convergent regulatory authorities in comparison to the separate ones.

Since p value of chi-square test of equivalence of proportion is higher than 0.01, we conclude that, according to the given rank, for the question or attitude «a convergent form of a regulator has a more positive influence on the development of broadcasting and telecommunication services than separate authorities» there is no significant difference among the observed groups, i.e., there is a dispersion of the given ranks on this attitude for all types of regulatory authorities.

Figure 4 presents a graphical overview of the expressed attitudes of regulatory authorities in percentage. Convergent regulators and regulators for telecommunications assess in over 50% the influence of convergent regulators more positive than the separate ones, while in case of media regulators this percent is somewhat lower, but the attitude that a convergent regulator has more positive influence is still slightly prevalent.

On the grounds of a conducted analysis, a conclusion can be drawn that the hypothesis that convergent regulatory authorities ensure better quality implementation of the principle of technological neutrality than the separate authorities has been proven.

(1) convergent form of communication market regulatory authorities improves competitiveness of a country.

(2) unlike the separate regulatory authorities, a convergent regulatory body is a more appropriate model for ensuring development of the communication market at the territory of a country.

(3) the organizational form affects the capacity of a regulator to implement the European directives in the telecommunication sector.

V. CONCLUSION

One of the main features of convergent regulation is the institutional simplicity of implementing technologically neutral regulations. The need for technologically neutral regulation lies in the fact that companies providing similar services or using similar technologies face different regulation in their service provision, thus taking up a less favorable competitive position. The principle of technological neutrality becomes markedly critical in the context of regulating the NGN networks. Regulators all over environment for promoting development and implementation of the NGN networks as an important element of communication market development [10].

All this has prompted governments across the world to consider options of merging regulatory authorities for broadcasting and telecommunications. It is very important for all governments to carefully consider the issue of establishing their regulatory authorities. In order to do this, it to the primary task is to precisely and legally formulate a set of duties these authorities would have within the scope of their competences, the power of authorities they can practice in their work, and their legal and institutional relations with other state institutions. Under such circumstances, institutional convergence, implying convergence or merging of institutions, makes for one of the most logical solutions.

 ISBN: 978-1-61208-166-3

REFERENCES

[1] Baldwin, R.et al.: "A Reader on Regulation", Oxford, Oxford University Press p. 3, (1998):

[2] Bezzina J. & Sanchez, B.: „Technological convergence and regulation, Challenges facing developing countries", The Economic Journal on Telecom, IT and Media Communications & Strategies (special issue), November 2005, Tunis, p. 19, (2005)

[3] Brown, A. C., et al.: „Handbook for Evaluating Infrastructure Regulatory Systems", The World Bank, Washington DC, USA, p. 5, (2006)

[4] Castells, M.:" Informacijsko doba Ekonomija, društvo i kultura, Uspon umreženog društva (Information age – Economy, society and culture, The Rise of network society)", Golden marketing Zagreb, Croatia, p. 99, (1998)

[5] Dutta, S. and Mia, I.: „The Global Information Technology Report 2006-2007, Connecting to the Networked Economy", World Economic Forum & INSEAD, Geneva, p. 10, (2007)

[6] European Commission: Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation Towards an Information Society Approach, Brussels, (1997)

[7] Gates, B.: „Adoption-and prosperity-trough public-private partnership, article in Publication", Connect- World, London, UK, Global issue 2008, p. 16, (2008)

[8] Haqqani, A.B.: „The Role of Information and Communication technologies in Global Development Analyses and Policy Recommendations", - ICT Task Force Series 3, United Nations, New York, p. 95, (2003)

[9] Hudson, H.E.: „Global Connections, International Telecommunications Infrastructure and Policy", Wiley, New York, p. 1, (1997)

[10] International Telecommunication Union – ITU : "Trends in Telecommunications Reform, Convergence and Regulation", Geneva, p. 8, (1999)

[11] International Telecommunication Union – ITU: "Trends in Telecommunication Reform 2002-Effective Regulation, Geneva, p. 42, (2002)

[12] International Telecommunication Union – ITU: "Measuring the Information Society, The ICT Development Index", Geneva, p. 32, (2009)

[13] Jenkins, H.: "Convergence Culture", Where Old and New Media Collide, New York University Press, New York and London, p. 2, (2006)

[14] Jordana, J., Levi and Faur, D.: "The Politics of Regulation, Institutions and Regulatory Reforms for the Age of Governance", p. 1, (2004)

[15] Kukić, S. and Markić, B.: „Metodologija društvenih znanosti – metode, tehnike, postupci i instrumenti znanstvenoistraživačkog rada (Methodology of social sciences – methods, procedures and instruments of science and research papers)", Ekonomski fakultet Sveučilišta u Mostaru, p. 192, (2006)

[16] Lagumdžija, Z.: „Kompetitivnost Bosne I Hercegovine i regiona Jugoistočne Evrope 2007-2008" (Competitiveness of BiH and region of South East Europe 2007-08), Regionalni ekonomski forum Jugoistočne Evrope i MIT Centar za menadžment i informacione tehnologije, Ekonomski fakultet Univerziteta u Sarajevu, p. 18, (2007)

[17] Lagumdžija, Z.: „Komptetitivnost zemalja i regiona Jugoistočne Evrope 2008-2009 (Competitiveness of BiH and region of South East Europe 2008-09)" Regionalni ekonomski forum Jugoistočne Evrope i MIT Cetar za menadžment i informacione tehnologije, Ekonomski fakultet Univerziteta u Sarajevu, p. 13, (2008)

[18] Michalis, M.: "Governing European communications, from unification to co-ordination", Lexington, Lanham, USA, p. 193, (2007)

[19] Porter, M. E.: "The Competitive Advantage of Nations", First Free Press Edition, New York, USA, p. 1, (1990)

[20] Porter, M.E.: "Konkurentska prednost: ostvarivanje i očuvanje vrhunskih poslovnih rezultata (The competitive Advantage and Presearving of Top Businesss Results)", Asee, Novi Sad, 2007, p. 176, (2007)

[21] Richards, E. et al.: „The International Communications Market 2008", OFCOM, London, p. 166, (2008)

[22] Serentschy, G.: „Regulation in the Light of Convergence", the Twenty Sixth Symposium on Novel Technologies in Postal and Telecommunication Traffic (PosTel), Slide2, Belgrade, (2008)

[23] Stanford Encyclopedia of Philosophy: "Globalization, The Metaphysics Research Lab, Stanford", California, p. 4, (2006)

[24] The World Bank : „Information and Communications for Development", Extending Reach and Increasing Impact 2009, Washington DC, USA, p. 19, (2009)

[25] World Economic Forum: „The Global Competitiveness Report 2005-2006", Davos www.weforum.org/en/ [Accessed 27/04/2009], (2006)

 ISBN: 978-1-61208-166-3

Scalable Embedded Architecture for High-speed Video Transmissions and Processing

Jiří Halák, Sven Ubik, Petr Žejdl
CESNET / CTU Prague
Zikova 4, Prague 6 / Kolejni 550, Prague 6
Czech Republic
email: {halak,ubik,zejdlp}@cesnet.cz

***Abstract*—In this paper, we present a scalable and extendable hardware architecture for processing and transfer of ultra-high-definition video over high-speed 10/40/100 Gbit networks with very low latency. We implemented this architecture in a single FPGA device. Data processing is divided between FPGA resources and an embedded operating system. The FPGA resources can be moved between various processing functions depending on the device mode. The resulting inexpensive and compact device is intended for high quality video transfers and processing with a low latency and to support deployment in education and remote venues.**

Keywords-HD-SDI, video, FPGA, network communication, high-speed

I. Introduction

Video transfers are an expected driver application area of the future Internet. Picture resolution has been increasing over time. Better-than-high-definition-resolution video (such as 4K) is already used in some areas, such as scientific visualization, the film industry or even medical applications.

For the ultimate quality, required for instance in film post-production or live remote surgery transmissions, working with a signal that has not been compressed is preferable. The productivity of a distributed team can be significantly increased when the video signal can be transferred over the network in a real time to enable cooperation that is more effective. Two of the main technical issues are high-data volume and time synchronization when transferring over an asynchronous network such as the current Internet.

Currently available solutions mostly consist of multiple devices (computers, conversion boxes, sync boxes, audio boxes, etc.), which are expensive and harder to setup, increasing the logistics costs. We designed an embedded modular and scalable architecture which fits into a single mid-size FPGA device including all the required functionality and reducing the complexness and costs of this solution. We implemented this architecture and developed a device called MVTP-4K (Modular Video Transfer Platform). We have already used several prototypes in field tests to support applications in film post-production and live medical applications.

This paper is organized as follows: In Section II, we summarize the hardware requirements of our design. In Section III, we present our architecture for video transfers and processing. In Section IV, we present our prototype. In Section V, we summarize our experience with device field tests, In Section VI, we compare our solution with other available devices.

II. Requirements

We have set the following set of requirements for our architecture:

- Video inputs and outputs SDI, HD-SDI or 3G channels
- 10/40/100 Gbit network interface or multiple interfaces
- Very small added latency
- Extendable design for additional processing such as compression or encryption
- Fit into available FPGA devices and fully implementable in one mid-size FPGA device with additional interfaces

The use of a single- and dual-link HD-SDI channel for the transmission of high definition video streams is now a common industry practice and it is specified in SMPTE 274 [1] and SMPTE 372 [2]. This includes HD (1920x1080) and 2K (2048x1080) formats. The 4K (4096x2160) signals are typically transferred in four quadrants, each in 2K format carried over a separate dual-link HD-SDI channel. 3D transmissions are typically transferred as two independent 2K or 4K channels, some require additional synchronization.

The FPGA circuit was chosen as the processing device due to its versatility that allows us to build a complete embedded solution and to host all required functionality to combine video transmissions with other functions, such as compression, encryption or transcoding.

The architecture must be scalable to allow multiple configurations based on currently available FPGA devices and interfaces, assuming the speed of communication interfaces will increase, and eventually be usable with future 100 Gigabit Ethernet networks and similar high-speed media.

We require an unnoticeable latency added to the network propagation delay for real-time applications. Unnoticeable

 ISBN: 978-1-61208-166-3

latency for audio/video applications is below 60 ms for untrained audience and below 30 ms for professional audience.

III. The Architecture

This section describes the proposed architecture.

A. Background

In our previous work we designed and implemented a scalable hardware architecture for network packet processing [3], [4]. This architecture consists of a set of reconfigurable modules for packet processing and a communication interface. The architecture was designed for maximum flexibility and multi-gigabit speeds starting at 10Gb/s. The main processing core was designed to be fully scalable for 10/40/100Gb speeds.

We have designed an interface and developed a prototype for 40Gb/s SONET/SDH networks [5] for basic data processing and testing of 40Gb/s networks and currently we are experimenting with 100Gb Ethernet interface in FPGA devices.

B. Design Overview

Real-time processing of multi-gigabit data rates is difficult on PC-based platforms with standard operating systems not designed for real-time operation. We were looking for a real-time design that is scalable to higher data rates (such as for 8K or UHDTV2 format), higher network speeds (such as 40 and 100 Gb/s) and can be integrated with commonly requested video processing functions, such as encryption, transcoding or compression. Real-time operation means to add a very low latency to a network delay and enable true live experience. This design is fully automated and all embedded in a single FPGA device.

The embedded architecture for real-time video transport and processing is based on our previous work. The core is the scalable architecture for network packet processing [3], [4] designed especially for Ethernet networks. This whole architecture operates at network clock domain of attached network interface and can be used for various modular data packet processing. Since video signal consists of special packets, we can make a simple conversion to transport the video packets to a network clock domain and back. This way we can use a network packet processing architecture for video packet processing.

When we convert data packets from network clock domain to video clock domain certain mechanisms need to be used. Ethernet Network is an asynchronous network, on the other hand, HD-SDI is a synchronous channel thus an advanced techniques for synchronization of data packets crossing from network domain to video domain are required [6].

Address range of all processing modules, routes and hardware configuration registers is mapped to an embedded processor logic bus (PLB) address range using a simple bus bridge of our own design. An embedded processor can be a

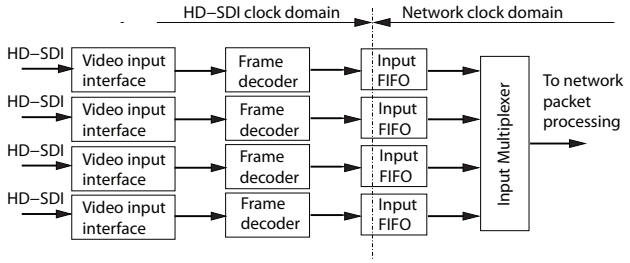


Figure 1. Input video processing and connection to packet processing for 4 channels.

dedicated Power PC processor or soft-core Microblaze [7] processor. An embedded processor is running a customized Linux distribution and all peripherals are managed by Linux drivers or dedicated software tools. The embedded Linux distribution also provides all means of communication with a device, such as ssh server, web server, display and keyboard controllers and eventually can also handle 10/100/1000 Mbit and multi-gigabit interfaces. The Multi-gigabit Ethernet Network Interface for an embedded processor is described in a subsection III-F.

C. Video Processing Modules

Video processing modules do a conversion between video and network packets, allowing video data to be processed in the network packet processing core (section III-D). There are two video processing modules, the input and output module, shown in Figures 1 and 2.

The input module consists of the video input interface and the frame decoder. The video input interface implements low-layer communication with the HD-SDI equalizer chips through Rocket IO channels and the frame decoder extracts video packets, converts them to network packets and attaches headers with video format parameters.

The output module consists of the video frame generator and the video output interface. The frame generator receives network packets and generates valid image to the video output interface based on information contained in network packet headers.

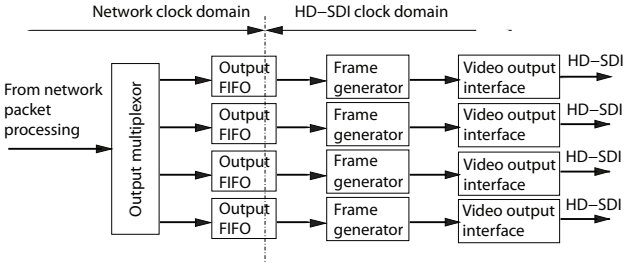


Figure 2. Output video processing and connection to packet processing for 4 channels.

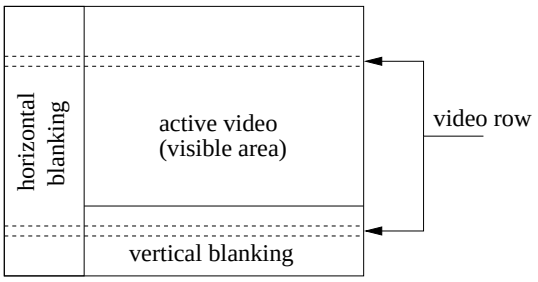


Figure 3. Video frame structure transported through HD-SDI channel

A video packet includes a video pixel row with specified headers and control characters. We use a dual-port memory as a packet FIFO to cross clock domain boundaries. The video processing modules are located in the HD-SDI clock domain and the network packet processing modules are located in the network clock domain. The example configuration in Figures 1 and 2 includes four HD-SDI channels. The channels are independent and can be added freely just with a simple modification of the channel multiplexer. This operation can be completely parameterized.

The HD-SDI interface has a bit rate of 1.485 Gbit/s [8] but not all data needs to be transferred. Video rows include blanking areas (horizontal blanking interval) and a video frame includes blanking video rows (vertical blanking interval). The whole situation is illustrated in Figure 3. Blanking areas can contain some secondary information such as audio, encryption or video format specification, which we can choose to transport or not. When we strip video packets of those blanking intervals, we get a bit rate between 1 Gb/s and 1.3 Gb/s depending on a picture resolution and frame rate. This means that the 10 Gbit Ethernet network can transfer up to eight HD-SDI video channels and with some video formats even including additional data, such as audio or encryption information.

The example bitrates of eight channels of selected video formats stripped of blanking intervals are summarized in Table I. The 30fps HD formats can be still transferred, but image crop must be applied.

TABLE I
VIDEO FORMATS BITRATES

Format	Bitrate eight channels (Gb/s)	Bitrate one channel (Gb/s)
2K/24	8,7	1,08
1080/24	8,2	1,025
1080/25	8,5	1,06
1080/30	10,4!	1,3
720/50	7,6	0,95
720/60	9,1	1,14

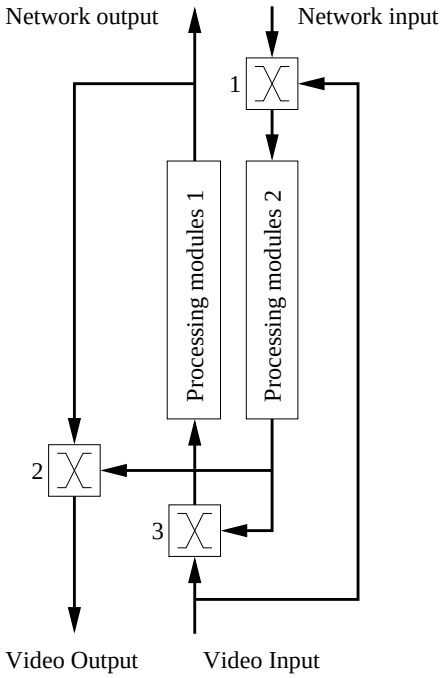


Figure 4. Schematic of interconnections in the processing core.

D. Network Packet Processing Core

The main processing core consists of two sets of processing modules. We have extended our original architecture [3], [4] with the video interface and video processing modules described in section III-C. The network packet processing core is divided into two parts. A set of switches can be arranged to allow a packet flow between the network and video domains in several ways. A schematic of this interconnection is shown in Figure 4. The following configurations are possible:

- From network input to network output through switch 1, processing modules 2, switch 3 and processing modules 1. All processing modules are dedicated for network to network packet processing.
- From network to video, full-duplex, one set of processing modules for each direction. From network input through switch 1 and processing modules 2 to video output. From video input through switch 3 and processing modules 1 to network output.
- From video input to video output through switch 3, processing modules 2, switch 3, processing modules 1 and switch 2. All processing modules are dedicated for video packet processing.

Data stream processing modules are inserted directly to the packet stream. Every processing module works as an individual processing unit. The advantage is that modules can occupy different FPGA devices. When we need to implement a complex module such as video encoder/decoder,

 ISBN: 978-1-61208-166-3

we may find more suitable to use more FPGA devices. For this purpose, the architecture is designed to relocate a packet stream through a high-speed FPGA ports to another device and make a cross-device interconnection of processing modules. Both options are shown in Figure 5. Option A: Modules are connected in a single device. Option B: Module interconnection crosses multiple devices over a high-speed interface.

E. Processing latency

The concept of intra-frame processing of video packets as network packets enables extra low latency of video processing and transmission. This opens a way to truly real-time collaboration support. The processing design itself has a low latency under 1 ms. Video packets are buffered only when synchronizing from the network asynchronous domain to the video synchronous domain. However, low delay variation in the network is required to allow design latency under 1 ms. In lower quality networks the buffering level needs to be obviously increased. The extreme cause is a single frame buffer adding a maximum latency of about 30 ms.

F. Network Interface

High-speed network interface consists of hardware and software parts, which are controlled by an embedded operating system. Incomming packets containing video data are sent to output video processing module, on the other hand network management packets such as ARP or ping are sent to software network driver. Outgoing packets have two different sources, packets containing video data are sent from input video processing module and network management packets are sent from software network driver.

The block diagram of the network interface is shown in Figure 6. Incoming packets are classified in the packet classifier and distributed between video processing modules (VPM) and RX FIFO. Outgoing packets are sent from VPM or from TX FIFO. Because there are two paths producing packets, packet multiplexer is included in the design. It is multiplexing packets in a round-robin fashion. RX and TX FIFO are connected to the CPU through the processor local bus. Therefore, both memories are accessible from software. The packet classifier is also connected to the CPU, but the connection is not shown. The CPU is embedded inside FPGA either.

The packet classifier contains memory for four classification rules. Each rule can be marked as going to the VPM and/or going to RX FIFO. The memory is configured from software. Currently we use three rules. The first rule is marked as going to the VPM and the other two rules are marked as going to RX FIFO. The fourth rule is not used and is reserved for future use.

The rules are as follows:

- Rule for UDP packets containing video data.
- Rule for ARP packets for address resolution.
- Rule for ICMP packets (ping command).

The software part is based on embedded Linux. Network interface is accessible through the Linux TUN/TAP driver [9], which provides packet reception and transmission for user space programs. The program controlling network hardware is running as a daemon in the user space, and through TUN/TAP driver provides a new network interface. This new interface behaves like an ordinary network interface such as eth. Therefore, all networking services are available through this interface.

IV. MVTP-4K PROTOTYPE

We have designed and build a MVTP-4K (Modular Video Transfer Platform) device which implements proposed architecture and validates it in field tests. The MVTP-4K is a

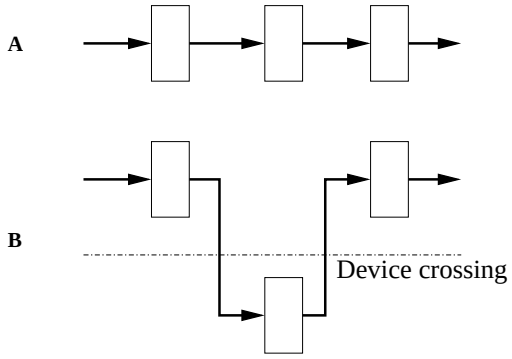


Figure 5. Processing modules

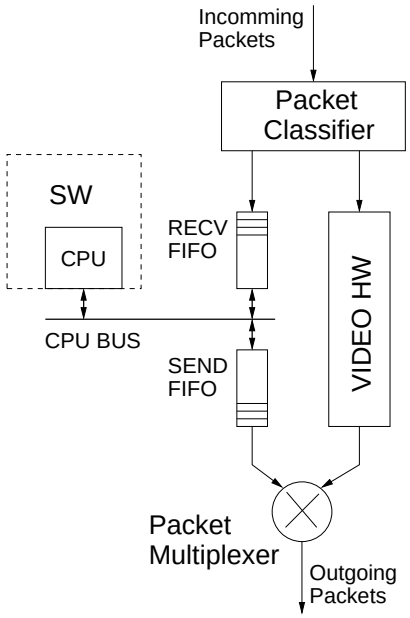


Figure 6. Ethernet Interface Block Diagram

 ISBN: 978-1-61208-166-3

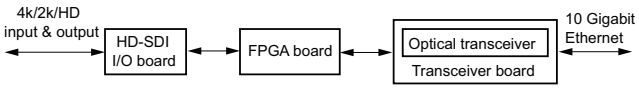


Figure 7. System architecture overview.

portable device of our own construction for transmission of multiple high-definition video streams including 4k, 2k and HD over a 10 Gigabit Ethernet Network. The device consists of a main FPGA board with 8 HD-SDI video interfaces and one 10Gbit Ethernet interface. Brief structure is shown in Figure 7. The device supports all 4K, 2K and HD resolutions and all corresponding frame rates. 3D transmissions are also supported. Because the data processing is based on data packet processing we can even transport data not fully supported without the need of unpacking them from video signal. This allows us to transport audio data or encryption data embedded in the video stream.

We have chosen a Xilinx Virtex FPGA series because it provides all building blocks and tools required to implement our architecture. The prototype is based on an extended platform for network packet processing called MTPP [3]. Whole architecture fits to a mid-size FPGA device Virtex 5 series XCV5LX110T. We have experimentally confirmed that the device adds a low latency of less than 1 ms.

Mid-size Xilinx FPGAs can be obtained under 3000$ a piece in a small quantities. For advanced hardware functions such as encryption or encoding, a larger FPGA or a second mid-size FPGA is required.

V. Practical Experience

We have demonstrated our system at the Cinegrid 2009 and Cinegrid 2010 workshops. The aim was to demonstrate that such technology can enable real-time remote cooperation of a distributed team and thus increase productivity. In the first event, a stream of uncompressed 4K video was transferred from the Barrandov studios in Prague to the venue in San Diego over a distance of more than 10000 km to perform remote color grading in a real-time. In the second event, a stream of 3D 2K video was transferred from the UPP Company in Prague to the venue in San Diego to perform remote real-time postproduction processing of 3D images. The 3D grading performed at the venue with the signal transferred by our device is illustrated in Fig.8.

Figure 8. Practical use of the technology at Cinegrid 2010 event

In order to evaluate the system suitability for e-Health applications, we transferred several surgical operations from the daVinci Surgical System [10] which produces HD stereoscopic signal in 1080i format. The picture quality was subjectively approved by invited medical experts as suitable for highly illustrative student training or presentations of surgical procedures on symposia.

VI. Related Work

There are several commercial products, which allow transport of SDI, HD-SDI or 3G channels over network.

Net Insight's [11] Nimbra 600 series switch can transport 8x HD-SDI or 3G SDI channels over an SONET/SDH network. There are several commercially available solutions for transport of compressed 4K video over the Internet, for example NTT Electronics [12] ES8000/DS8000 4K MPEG-2 encoder/decoder complemented with NA5000 IP interface unit and intoPIX's [13] system of PRISTINE PCI-E FPGA boards and JPEG 2000 IP cores.

UltraGrid from Laboratory of Advanced Networking Technologies is a software for real-time transmissions of high-defintion video [14]. This solution is a fully software based and requires dedicated PC with specialized hardware.

The architecture and design described in this article differs in that it is a hardware solution fully scalable to higher speeds. The number of video and network interfaces is parameterized and can be easily extended. The FPGA enabled parallelism allows our architecture to process several video channels at once and to transfer every video format contained in SDI, HD-SDI or 3G interface. The architecture is designed to be embedded to a single FPGA device but some larger processing modules can be relocated to other FPGA devices. Our design has a very small added latency around 1 ms that enables a true real-time distributed team cooperation.

VII. Conclusion

We have extended a scalable architecture for network packet processing [3], [4] by video interfaces options. The resulting architecture is designed to process or transport video data over an asynchronous network with very low added latency. The design enables true real-time distributed team cooperation. The real-time team cooperation was demonstrated in several applications in the cinema industry and e-Learning in medicine. The architecture also fulfills the hardware requirements that we set and we successfully

 ISBN: 978-1-61208-166-3

implemented this architecture in a single FPGA device and presented its capabilities.

ACKNOWLEDGMENT

This work has been supported by the Ministry of Education, Youth and Sports of the Czech Republic under the research intent MSM6383917201 Optical Network of National Research and Its New Applications.

REFERENCES

[1] "1920 x 1080 Image Sample Structure, Digital Representation and Digital Timing Reference Sequences for Multiple Picture Rates." Society of Motion Picture and Television Engineers., 2005.

[2] "Dual Link 1.5 Gb/s Digital Interface for 1920 x 1080 and 2048 x 1080 Picture Formats." Society of Motion Picture and Television Engineers., 2009.

[3] J. Halak and S. Ubik, "MTPP - Modular Traffic Processing Platform," in *12th IEEE Symposium on Design and Diagnostics of Electronic Systems, DDECS 2009*, Liberec, Czech Republic, April 2009, pp. 170–173.

[4] J. Halak, "Multigigabit network traffic processing," in *Proc. The International Conference on Field Programmable Logic and Applications, FPL 2009*. Prague, Czech Republic: IEEE Computer Society, August 2010, pp. 521–524.

[5] J. Halak, S. Ubik, and P. Zejdl, "Data stream processing for 40 Gb/s networks," in *Proc. Fifth International Conference on Digital Telecommunications, ICDT 2010*. Athens/Glyfada, Greece: IEEE Computer Society, June 2010, pp. 149–152.

[6] ——, "Receiver synchronization in video streaming with short latency over asynchronous networks." Vienna, Austria: IEEE Computer Society, April 2010, pp. 403–405.

[7] MicroBlaze Soft Processor Core. (Last accessed: July, 2011). [Online]. Available: http://www.xilinx.com/tools/microblaze.htm

[8] "1.5 Gb/s Signal/Data Serial Interface." Society of Motion Picture and Television Engineers., 2008.

[9] Universal TUN/TAP device driver, Linux Kernel Documentation. (Last accessed: July, 2011). [Online]. Available: http://kernel.org/doc/Documentation/networking/tuntap.txt

[10] The da Vinci Surgical System, Intuitive Surgical. (Last accessed: July, 2011). [Online]. Available: http://www.intuitivesurgical.com/products/faq/index.aspx

[11] Net Insight AB. (Last accessed: July, 2011). [Online]. Available: http://www.netinsight.se

[12] NTT Electronics. (Last accessed: July, 2011). [Online]. Available: http://www.ntt-electronics.com

[13] intoPIX. (Last accessed: July, 2011). [Online]. Available: http://www.intopix.com

[14] P. Holub, L. Matyska, M. Liska, L. Hejtmanek, J. Denemark, T. Rebok, A. Hutanu, R. Paruchuri, J. Radil, and E. Hladk, "High-definition multimedia for multiparty low-latency interactive communication," *Future Generation Computer Systems*, vol. "22", no. "8", pp. "856 – 861", October "2006". [Online]. Available: "http://www.sciencedirect.com/science/article/pii/S0167739X06000380"

 ISBN: 978-1-61208-166-3

Using Coordinated Clients to Improve Live Media Contents Transmissions

Ronit Nossenson
Faculty of Computer Science
Jerusalem College of Technology
Jerusalem, Israel
ronit.nossenson@gmail.com

Omer Markowitz
School of Computer Science
The Interdisciplinary Center
Herzliya, Israel
markowitz.omer@post.idc.ac.il

***Abstract* — This research examines the possibility to significantly improve the quality of private live video transmission over the internet, as opposed to on-demand service, such as YouTube. To achieve this goal collaboration and coordination between small numbers of agents is carried out, using several communication methods such as wireless or cellular connections. Experimental performance results indicate that this method can significantly improve some performance parameters including packets jitter, with limited overhead.**

Keywords-Live Content Transmission; Multimedia QoS

I. INTRODUCTION

The increasing availability of various commercial products for private/domestic live video transmission on the one hand, and the many ways such a transmission could be received (PDA's, PC's, Smart Phones, Media Streamers, etc.) on the other, make it possible to exploit this medium faster than ever before. For instance, it is possible to broadcast a live video of a private family event to those unable to attend, an online transmission of a lecture, and as a matter of fact – experience almost any event without the need to physically being present "on location". All these emphasize the gap facing the poor quality of live video transmission that could be viewed today.

The commercial sector can afford purchasing the required bandwidth in order to transmit high quality video signals. However, this is not the case for the private domestic sector. An attempt to broadcast a live video signal on the internet often encounters difficulties, most of which arise from the inability to guaranty end-to-end QoS for the private individual, such as appropriate bandwidth or low bound on packet delay. For example, the common way to improve quality of viewing a video file located on a server (via services such as YouTube) is with the use of buffering on the viewer's computer. However, anyone who had experienced watching video over the internet surely noticed that this is generally not sufficient, in particular for live video streaming [4].

Another problematic issue arises from the inability to guaranty a sufficiently large bandwidth, which is mainly due to the competition over the bandwidth between clients (oversubscription factor). This could become even worse with longer broadcasting, even if theoretically the user's ISP provides the client with potentially enough bandwidth.

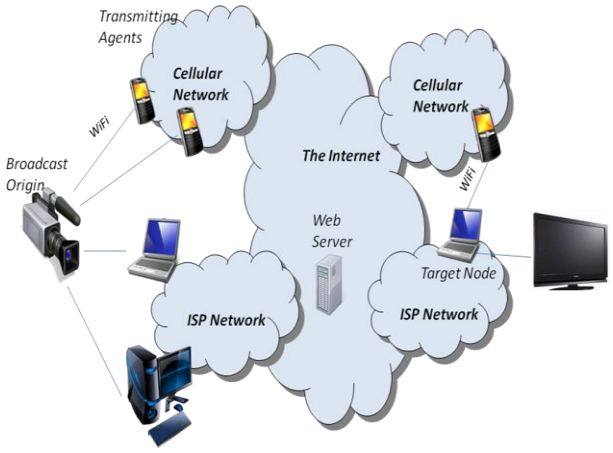


Figure 1: Coordinated agents uploading a private live video content.

Addressing the above issues usually aims at reducing the workload on the server and increasing the effective bandwidth. Most of the solutions are based upon Peer-to-Peer (P2P) or upon multicast at the network infrastructure level [5,6,7]. For instance, P2P based solutions assume a relatively large number of clients, enabling the information to be present simultaneously at several locations rather than just on the original server. Therefore, usually the information will contain 'public properties' such as a TV broadcast.

Private, non-commercial video transmission has a couple of limitations which differ from public broadcasting – privacy and a small number of designated consumers of the information. The private properties of the information might turn irrelevant certain solutions, in which the user doesn't control the information flow (this might be the case for P2P or multicast) or unable to encrypt the information (which is unpractical for the private user in the case of live video).

Alternatively, the small amount of the specific information consumers makes it almost irrelevant to establish designated P2P networks to improve the transmission's quality.

Our work examines a novel approach toward resolving the issues mentioned above, by using a *small* number of coordinated agents (not exceeding 5) for uploading and/or downloading the information as plotted in Figure 1. This is based on the assumption that the domestic user has numerous ways of connecting to the internet (ADSL, WiFi, cellular, etc.) enabling the transmission of information or parts of it through different devices or connections.

 ISBN: 978-1-61208-166-3

The agents are assumed to be located geographically close to each other and therefore there might be a highly statistical dependency between the different links. For example, several participants in a family event will use their cellular phones to broadcast the live video to family members not attending the occasion. In such a scenario, some of the cellular devices will probably connect to the internet using the same base station and thus, sharing the cell resources. In addition, they are all affected simultaneously by the same radio interferences.

Still, despite the high statistical dependency, the multiple transmissions have the potential of using de-facto larger bandwidth than that available to a single transmission. Alternatively, it can supply various new options for dealing with delays and/or disruptions in one of the connections, and thus achieve continuous uniform quality of the received transmission. Our initial performance evaluation results indicate that the packet jitter can be easily improved with a competitive overhead factor relative to other methods.

The complexity of the method arises from the need for coordination of the agents, synchronization of the redundant information and choice of the most appropriate packets to assemble the received video. We show that this can be resolved with a simple algorithm and without a significant increase of information at the different connections. We implement agents' control mechanisms between the Web receiving/transmitting server and the agents as a function of current conditions of transmission. Thus, network or server resources consumption is minimized as the received quality becomes sufficient.

II. RELATED WORK

Until recently most of the solutions for transmitting and watching video content over the internet were based upon on-demand services (such as YouTube). Over the last few years, research regarding Peer-to-Peer options were conducted, both as a solution for on-demand services, as well as for live video broadcasting. For instance, in [1] several typical P2P topologies are reviewed. P2P has mainly been used to minimize the number of connections (and transmissions) a server has to maintain simultaneously.

A key issue in P2P research is a fair distribution of resources among the network members and a minimization of the load from the original server. Solutions based on cooperative patches are presented in [2] and in [3] in order to handle re-transmit requests by other clients keeping different patches of information. Other aspects of P2P research deal with decreasing delay times as they are affected by the bandwidth available to the P2P network members [4].

A different approach, which is relevant to the commercial sector, is to optimize the various methods of transmission by dynamically 'activating' solutions. For example, CPM [5] is a solution which dynamically changes the transmission method of VOD as a function of video popularity, number of requests, numbers of clients, etc.

Our work resembles the concept of dividing a single broadcast into several transmissions and ‘reunites' it back at the client side. This approach appeared as a possible solution toward some of P2P issues. For example, SplitStream [6] is an algorithm which intelligently builds P2P forests with the assumption that the application is responsible for splitting the transmission. Another relevant concept is to use multiple transmissions for encoding video signals in order to improve resolution and quality [7].

So far, a solution which assumes a relatively small number of statistically dependent agents collaborating in the transmission has not been suggested and examined. In this paper we suggest a new algorithm for controlling a small number of agents to provide better live video streaming quality.

III. DATA COLLECTION

As mentioned above, the complexity of the method arises from the need for coordination of the agents, synchronization of the redundant information and choice of the most appropriate packets to assemble the received video. Another issue concerns the fact that theoretical models assume no dependencies between the transmitting agents. However, this is not the case with ‘real life’ domestic clients where the agents are statistically dependent due to the close distance between them. Therefore, our method for evaluating the suggested solution is by measurements of real traffic, rather than theoretical analysis.

First, we transmit video using several agents in various conditions in order to collect data that will be used for evaluating different algorithms for splitting and joining the transmission. The transmission of the agents was done using LU60 of LiveU [8], using one to five cellular modems connected to three different cellular networks. Each agent has a different connection to the internet. Next, a feasible solution for splitting and joining is implemented. Finally, we evaluate the method potential performance using the data collected at the beginning. By that we are evaluating the potential for improving home video transmission for the domestic user. We record the received data with LiveU's server (LU1000) and also using 'Wireshark' software. We collect data which is relevant to parameters such as delay, jitter and retransmission ratio. Therefore, for each packet in each transmission from each agent we record the Packet Sequence Number and Time of Arrival (to server).

IV. IMPLEMENTATION

In this section we described our novel algorithm for controlling the agents. The server and the agents operate in a master-slave mode where the server is the master and the agents are the slaves. Regarding the algorithm for the coordinated transmission, we use a simple selection of the **best k** agents based on history of transmission of a segment consisting of N packets (N is equal to ten in our measurements). As long as the transmission requirements are satisfied, the selected k agents continue to transmit the next segment. If the requirements are not satisfied then a new competition is generated. In a competition, a new set of “best k" agents is selected based on transmission performance of a new segment.

The value of k is selected as the minimum value which satisfies pre defined performance transmission parameters. It varies between 1 and the maximum allowed number of

 ISBN: 978-1-61208-166-3

agents for the same session. Here we assume that the maximum allowed number of agents is five, so, k is in {1,…,5}. By on-line choosing a minimum value for k we reduce the transmission overhead; by limiting its value we actually limit the method overhead.

To start a new session the first agent sends a transmission request to the server. The request includes authentication information such as user identification and password. In addition, the request includes information on the requested performance parameters (e. g., Jitter), the number of expected cooperative transmitting agents for this session and the number of expected receiving (target) nodes. Once the authentication is completed, a new session is established with the first agent. Then, other agents can join the session.

An on-line analysis is performed to verify that the requirements are satisfied. To avoid waiting, it is based on the previous transmitted segment of N packets and not on the segment which is transmitted currently. The algorithm can be adjusted to longer server response time by shifting the analysis to even earlier arrived segments. However, a long gap between the current analyzed segment and the current transmitted segment result a long period of transmission with un-optimized set of k agents.

The server generates the joined video stream based on the arrived segments. For each packet, its first instance (with minimum arrival time) is placed in the joined file. This video is transmitted to any target node which is register to the specific session.

Similar to the server operation, using the same algorithms, a target node can activate a few receiving / transmitting agents to create a better video stream. Note that the master-slave operation can be done directly between the target node and the transmitting agents, so the web server is not necessary in this scheme and it can operate in a pure peer-to-peer manner.

The pseudo code of the algorithm is described below. For the simplicity of the presentation we assume that the live video transmission is longer than 2 segments and 5 agents have contact the server with request to join this specific session. EOF (end-of-file) is a flag set by a special message from the agents indicating that the next two segments are the last segments. We assume that all agents' registration is completed at the beginning of the video transmission. Obviously, this simple algorithm can be easily adjusted to the case where new agents perform registration after the beginning of the video transmission.

```
Void ServerMain()
Begin
   1: integer Seg_ind = 0;
   2: Agt_List new_list(); Best_Agt();
   3: Initiate(new_list);
   4: new_list.send(Seg_ind);
   5: Seg_ind++;
   6: new_list.send(Seg_ind);
   7: Seg_ind++;
   8: Best_Agt= Compete(new_list, Seg_ind-1);
   9: While ((Not EOF) &&
    (Transmission_quality(Best_Agt,
        Best_Agt.long(), Seg_ind-1))
   /* The "best" is still the best */
     Do{
   9.1:    Best_Agt.send(Seg_ind);
   9.2:    Seg_ind++;
         }
   10: If (Not EOF) /* The "best" is NOT good */
   10.1:      GOTO 4;
       Else { /* send last 2 segment and close */
   10.2:    Best_Agt.send(Seg_ind);
   10.3:    Seg_ind++;
   10.4:    Best_Agt.send(Seg_ind);
   10.5:    new_list.close();
          }
   11: return();
End.
```

The verification of the "Transmission quality" condition is done by verifying the pre defined ratio of packet retransmission threshold and pre defined packet jitter in the segment.

```
Bool Transmission_quality(B_Agt,k,prev_seg_ind)
begin
   0: quality = false;
   1: For (i=1 to N) do {
   1.1: Best[i]=
        Min(B_Agt[1][prev_seg_ind].pkt_arr_t(i), …,
        B_Agt[k][prev_seg_ind].pkt_arr_t(i));
   1.2: ReTrns[i] =
        Min(B_Agt[1][prev_seg_ind].ReTrns(i), …,
        B_Agt[k][prev_seg_ind].ReTrns
        (i));
      }
   2: For (i=1 to N-1) do {
   2.1:     If (Best[i+1]- Best[i]> Jitter) Then
               return(quality);
   2.2:     Sum_ReTrns += ReTrns[i];
      }
   3: Sum_ReTrns += ReTrns[N];
   4: If (Sum_ReTrns > ReTrns_TH) Then
         return(quality);
   5: quality = True;
   6: return(quality);
End.
```

Before a competition is performed, all registered agents are instructed to transmit two segments. The best k agents are selected according to the performance of the arrived first segment (again, packet loss ratio and jitter). If more than k agents fulfill the quality condition then the *first* set of such agents is selected as the "best". If none of the sets of k agents fulfill the quality condition then k is incremented. The selected agents are instructed to continue transmission. The other agents are instructed not to transmit.

```
Agt_List Compete(A_List, S_ind)
begin
   0: quality = false;
   1: k=1;
   2: Best_Agt = next set of k agents from A_list;
   3: quality = Transmission_quality(Best_Agt,k,
      S_ind);
   4: If (quality == false and more sets exist)
         GOTO 2;
   4.1: Else If (quality == false and no more sets
         of size k exist){
               k=k+1;
               if (k<6) GOTO 2;
               Else return ('error');
               }
   4.2  Else {return (Best_Agt)};
   End.
```

V. PERFORMANCE EVALUATION

The performance evaluation of this new method is not completed yet. However, we are able to provide some initial promising results.

In the performance evaluation of our novel method we consider the following additional competing methods: single transmission (that is, the way live video is transmitted today by the domestic user) and simple (not controlled or coordinated) multiple transmission of 2-5 agents. In simple multiple transmissions, for every packet sequence number, the server considers the first arrived instance. That is, the resulting arrival times are the minimum arrivals times of every packet. The analysis of the best k method was performed twice, once with jitter requirement of 13 msec. and once with jitter requirement of 25 msec.

Table I presents the Jitter statistics of the competing methods. Each line describes the average number of times that the arrival processes violate the corresponding jitter condition. Each complete video transmission consists of 50,000 packets. For example, in line number three, the jitter condition is "smaller than 13", and the process "best k with parameter 25" violates this condition 1862 times in average out of 49,999 times (3.7%) while the process that use simple multiple transmissions of three agents violates this condition 3709 times in average out of 49,999 times (7.4%). As can be seen from this table, starting from jitter condition "smaller than 13" both best k processes outperform the other processes with significant small number of condition violation.

Regarding the average overhead, processes with one agent naturally have no overhead (factor 1), processes with two agents have overhead of factor 2 (every packet is transmitted twice), and so on. The best k process with parameter 13 has overhead factor of 2.7 and the best k process with parameter 25 has overhead factor of 1.66. The differences in the overhead factors are due to the fact that fewer competitions are generated when the best k algorithm requirement from the jitter is less demanding. In a competition all the potential 5 agents transmit a segment, thus, the overhead increases with the number of competitions.

TABLE I. JITTER STATISTICS

Jitter cond.	best k (25)	best k (13)	1 agt.	2 agt.	3 agt.	4 agt.	5 agt.
10	7254	7360	13213	9909	7657	5648	3905
13	1862	1402	7643	4984	3709	2842	2354
16	1767	1293	6877	4485	3291	2502	2027
19	1279	1006	5282	3503	2530	1894	1493
22	552	612	2891	2000	1498	1178	1017
25	517	582	2533	1825	1368	1086	938
30	444	537	2075	1536	1180	974	882
35	418	518	1891	1420	1094	911	835
40	408	508	1796	1353	1045	879	819
50	230	303	1007	842	756	743	785

VI. CONCLUSIONS AND FUTURE WORKS

This paper describes a new method to improve the quality of live video streaming for the private domestic sector. This method use a few agents installed for example, in the user laptop, smart phone and PDA. Upon registration, a server activates and coordinates the multiple transmission of the content from these agents in a way that improve the quality but with minimum overhead. In the downlink direction, the server can transmit the same stream to several agents. These streams can be joined again at the user computer using the same algorithm. We believe that this new web service is interesting as a complementary to sites such as MySpace and YouTube.

Future work includes:

- Additional analysis of the performance evaluation of this method.
- Improving the selection of the k transmitting agents. In our simple algorithm the *first* set of agents that fulfill the conditions is selected. We believe that different selection method can perform better.
- Dynamic estimation of actual performance conditions.

ACKNOWLEDGMENT

We thank LiveU, in particular, Noam Amram, for useful discussions, for allowing us to use the LU60 and for funding the required measurements over the cellular networks.

REFERENCES

[1] Liu, Y., Guo, Y., and Liang, C., A survey on peer-to-peer video streaming systems. In Peer-to-Peer Networking and Applications, 2008, vol. 1, no. 1, pp. 18–28.

[2] Guo, M., Ammar, M. H., and Zegura, E. W., 2004. Cooperative patching: A client based P2P architecture for supporting continuous live video streaming. In Proceedings of the 13th IEEE ICCCN. Chicago, USA, Oct. 2004, pp. 481-486.

[3] Guo, M. and Ammar, M. H., 2004. Scalable live video streaming to cooperative clients using time shifting and video patching. In Proceedings of the IEEE INFOCOM, 2004, pp. 1501–1511.

[4] Liu, Y., 2007. On the minimum delay peer-to-peer video streaming: how realtime can it be? In Proceedings of the 15th international conference on Multimedia, 2007, pp. 127-136.

[5] Gopalakrishnan, V., Bhattacharjeey, B., Ramakrishnan, K., Jana, R., and Srivastava, D., CPM: Adaptive video-on-demand with cooperative peer assists and multicast. In Proceedings of IEEE INFOCOM, Rio de Janeiro, Brazil, April 2009, pp. 91-99.

[6] Castro, M., Druschel, P. , Kermarrec A. M., Nandi A., Rowstron A., and Singh A., 2003. SplitStream: high-bandwidth multicast in cooperative environments. In Proceedings of the nineteenth ACM symposium on Operating systems principles, 2003, pp. 298-313.

[7] Schwarz, H., Marpe, D., and Wiegand, T., 2007. Overview of the Scalable Video Coding Extension of the H.264/AVC Standard. In IEEE Transactions on Circuits and Systems for Video Technology. September 2007, vol. 17, pp. 1103-1120.

[8] LiveU web site: http://www.liveu.tv/ accessed: June 2011.

 ISBN: 978-1-61208-166-3

New Block-Relationships Based Stereo Image Watermarking Algorithm

Mei Yu[1,2], Aihong Wu[1], Ting Luo[1]
1. Faculty of Information Science and Engineering
Ningbo University
Ningbo, China
{yumei2, wuaihong}@126.com, luoting@nbu.edu.cn

Gangyi Jiang[1,2], Fucui Li[1], Songyin Fu[1]
2. National Key Lab of Software New Technology
Nanjing University
Nanjing, China
jianggangyi@126.com, {lifucui,fusongyin}@nbu.edu.cn

***Abstract*—A new relationship based stereo image watermarking algorithm for three dimensional video system on the concept of intra-blocks and inter-blocks relationships is given. Corresponding coefficients of discrete cosine transform and discrete wavelet transform in the same position blocks are employed for defining intra-block relationship. Direct current coefficients for stereo pair in the same position blocks are used to describe inter-block relationship. Both of relationships are used to embed digital watermarks into stereo image pair; moreover, parity quantization is designed for watermark embedding when relationships can not work well. Experimental results show that the proposed algorithm can embed a watermark into images invisibly and the watermark can be detected blindly. At same time, the proposed algorithm is robust to attacks, such as JPEG compression, noise, filter, cropping, and so on.**

Keywords- Three dimensional video system; Stereo image watermark; Intra- and inter-block relationships.

I. INTRODUCTION

Three dimensional video (3DTV) systems [1] have been recently developed which significantly improve visualization. Many people believe that 3DTV will be next important development step towards a more natural and life-like home entertainment experience. Meanwhile, as computer network and multimedia-related technologies are in its rapid developing period, it is inevitable to transmit 3D media through communication channels in great quantity. A great chance of developing the copyright protection technologies of 3DTV will be produced as well. Watermarking [2] is one of technologies, which is the process of embedding the particular information inside the 3D digital contents as a solution to prove the ownerships.

In the past, many kinds of watermarking algorithms are designed for text, audio, digital still images, and video sequences, very few algorithms have been proposed for watermarking of stereo images. Patrizio described an object-oriented method for watermarking stereo images [3], and the watermark embedding is performed in the wavelet domain using quantization index modulations method, and the proposed algorithm is fragile against attacks. Hwang et al. proposed stereo image watermarking schemes based on discrete cosine transform (DCT) or discrete wavelet transform (DWT) [4][5]. The watermark is embedded into the right image of a stereo image pair in the frequency domain in [4], and is embedded into the left image of a stereo image pair by using DWT [5].

A stereo image includes left and right images which are composing the same scene are taken by two cameras corresponding to the right and left eye-views. Differences between left and right images are called the "disparity" between them. Stereo image pair must have some relations which can be used to embed digital watermarks. However few algorithms based on pair relationships are depicted in the literature. In the past years a lot of digital watermarking algorithms based on relationships are proposed for mono-images and videos. Langelaar used energy differences between DCT blocks [6] for watermarking. Ling et al. addressed the real time requirement of video watermarking based on energy difference. Chen et al. designed the watermark embedding based on the relationships between wavelet coefficients [8]. Kim et al. presented watermark algorithm based on relationship between blocks in DCT transform [9]. However, those above relationships are used in mono-image watermarking, and new relationships will be designed for stereo images in this paper.

Most of above algorithms employ transformations to embed watermark such as DCT and DWT. Haj presented combined DWT-DCT digital image watermarking [10] because of the advantages of DCT domain and DWT domain. Thus, DCT will be used in the proposed algorithm as well.

In this paper, a new relationships based stereo image watermarking algorithm is presented. The proposed algorithm is linked to the nature of the stereo pair and the watermark is embedded into both of left and right images partly, not only into one image for transparency. The experiments show the transparency and robustness against attacks such as noise, JPEG compression, filtering and cropping. The rest of paper is organized as follows: the proposed algorithm is described in section Ⅱ; section Ⅲ demonstrates some experimental results of the proposed algorithm; finally, Section Ⅳ gives the conclusions.

II. THE PROPOSED ALGORITHM

In this work, the left and right images are divided into non-overlapping $n\times n$ blocks. Let binary watermark denote W with $m\times m$ size, and $m\times m\leq(M\times N)/(n\times n)$, where $M\times N$ is the size of original images,. In the domain of the information security, the scrambling image is a usual way for image processing. Thus the 2-dimensional Arnold transformation is employed for watermarks and $\hat{W}=\{w_1,w_2,\ldots w_i;\ 0<i\leq m\times m\}$ is achieved. The watermark will be embedded into the intra-block, inter-block relationships or quantization as depicted in Fig.1. Either of three choices will be designed for watermark

 ISBN: 978-1-61208-166-3

embedding according to the preferences. Each component will be introduced in the following sections.

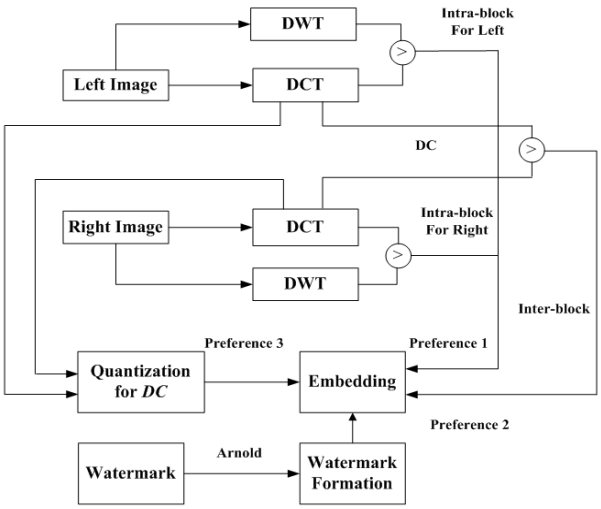


Figure 1. The main processes for embedding

A. Intra-block and Inter-block Relationships

The stereo image includes left image and right image with same size, which are divided into blocks with $n \times n$. DCT and DWT are applied in all blocks respectively. The direct current (*DC*) coefficient of the DCT domain and low frequency coefficient of two-level DWT domain have the similar transformation trend when images are on the attack. Thus the intra-block relationship is between *DC* coefficient in DCT domain and the second value ($LL2_{i2}$) of low frequency matrix in DWT domain, which are applied in the same blocks of images. Let the intra-block value denote IAB_i which is defined as

$$IAB_i = \begin{cases} 1 & DC_i > LL2_{i2} \\ 0 & DC_i \le LL2_{i2} \end{cases} \quad (1)$$

where DC_i is the *DC* coefficient of DCT domain for block *i*.

For left image and right image are high similarities, especially in the background area. *DC* strands for the basic energy of image block, therefore *DC* for both same position blocks of stereo pair have similar trends when attacks are on pair. The inter-block relationship is built on $DC_{L,i,}$ *and* $DC_{R,i}$. $DC_{L,i,}$ is *DC* coefficient of left image block *i* and $DC_{R,i}$ is *DC* coefficient of right image block *i*. If $DC_{L,i,}$ is greater than $DC_{R,i}$, the value of inter-block IRB_i is "1", and otherwise, IRB_i is "0".

Each w_i of the binary watermark only has one value "0" or "1". For relationship embedding, if IAB_i for left and right image are same as w_i, any coefficient of the blocks *i* is not to be modified. When three values are not the same, IRB_i will be compared with w_i. If they are same, any coefficient of the blocks is still unchanged, and otherwise, the *DC* coefficient of either left or right image needs to be changed and quantization step is required.

B. Parity Quantization

In this step, parity quantization is employed for the algorithm. $DC_{L,i,}$ and $DC_{R,i}$ are quantized by the quantization step value *S*, and $Q_{L,i}$ and $Q_{R,i}$ are calculated as

$$Q = \lfloor DC / S \rfloor \quad (2)$$

The processes for the quantization are described as follows.

If $w_i = 1$ and $Q_{L,i} \bmod 2 = Q_{R,i} \bmod 2$, neither of *DCs* will be update. Otherwise, either $DC_{L,i,}$ or $DC_{R,i}$ will be modified for same parity of $Q_{L,i}$ and $Q_{R,I}$. The modification rule is that the range of *DC* modification is least.

$$x' = \min\{|x|, Q'_{L,i} \bmod 2 = Q_{R,i} \bmod 2\} \quad (3)$$

$$y' = \min\{|y|, Q'_{R,i} \bmod 2 = Q_{L,i} \bmod 2\} \quad (4)$$

where $Q'_{L,i}=floor((DC_{L,i,}+x)/S)$, $Q'_{R,i}=floor((DC_{R,i,}+y)/S)$. If $x'/DC_{L,i}$ is less, the $DC_{L,i}$ should be modified, and vice verse. If $w_i = 0$ and $Q_{L,i} \bmod 2 = Q_{R,i} \bmod 2$, the *DC* coefficient will not be changed either, otherwise, $DC_{L,i,}$ or $DC_{R,i}$ will be modified according to the rule of quantization.

For the parameter *S*, it is related to the quality image, and according to transparency and robustness, *S* is set to 10 in the experiments.

C. Main Steps for Watermaring

Four secret keys are designed for the algorithm. 1×2 matrix *EM* is used for recording embedding methods as key_1, *L* times Arnold transformation is key_2 and cycle of transformation *T* is key_3 and *S* is key_4. The main steps for embedding watermark are depicted as following five steps.

Step 1: The left and right images are divided into non-overlap blocks of size 8×8 and it is block transformed using DCT and two-level DWT technique respectively. The watermark W is transformed to $\hat{W}$ with Arnold transformation, and set $i=1$;

Step 2: Compute intra-block IAB_i for block *i* of left and right image and inter-block IRB_i relationships..

Step 3: Preference 1: if IAB_i of left and IAB_i of right images are both equal to w_i, then EM_i="00", and go to step 4. Otherwise, the preference 2 is chosen. Preference 2: if IRB_i is equal to w_i, then EM_i="01", and go to step 4 as well. Otherwise, preference 3 will be selected. Preference 3: compute the $Q_{L,i}$ and $Q_{R,i}$, and set EM_i="10". Update corresponding *DC* coefficients according to the processes of the quantization.

Step 4: If $i \leqslant m \times m$, then i++ and go back to the step 3, otherwise, go to next step.

Step 5: Reconstruct the stereo images with watermark by inversing modified DCT transforms of left and right images.

D. Main Steps for Extracting Watermark

For a given stereo image pair, the recorded information about the embedded watermark (key_1, key_2, key_3 and key_4) should be provided for the watermark extraction from the

 ISBN: 978-1-61208-166-3

images. The detailed extracting procedure is described as follows.

Step 1: the given embedded watermark stereo image pair is divided into non-overlap blocks of size 8×8 and it is block transformed using DCT and two-level DWT respectively.

Step 2: set i=1, and get the DC coefficient $DCE_{L,i}$, $DCE_{R,i}$ for block i of left and right images, and get the second low frequency coefficient as well. If DC is greater than DWT coefficient in the same block, then intra-block value is "1", otherwise is "0". Thus $IABL'_i$ is the intra-block value for block i of left image, and $IABR'_i$ is the intra-block value for block i of right image. Suppose $DCE_{L,i}$ and $DCE_{R,i}$ are DC for block i of left and right image, and the inter-block relationship IRB'_i is calculated by

$$IRB'_i = \begin{cases} 1 & DCE_{L,i} > DCE_{R,i} \\ 0 & DCE_{L,i} \le DCE_{R,i} \end{cases} \quad (5)$$

Step 3: via key_1 get embedding methods matrix EM. Get the Arnold transformation watermark w'_i. When EM_i="00", w'_i is calculated by:

$$w'_i = \begin{cases} 1 & IABL'i = IABR'i = 1 \\ 0 & IABL'i = IABR'i = 0 \end{cases} \quad (6)$$

Suppose EM_i="01", w'_i is computed by:

$$w'_i = \begin{cases} 1 & IRB'_i = 1 \\ 0 & IRB'_i = 0 \end{cases} \quad (7)$$

If EM_i="10", and the quantization values for left and right images are calculated according to Eq.(1) and key_4. If they have same parity w'_i=1, otherwise w'_i =0.

Step 4: if $i \leqslant m \times m$, then i++ and go back to the step 2, otherwise, go to next step.

Step 5:the Arnold transformation watermark $W'=\{w'_1, w'_2 w'_3, \ldots, w'_{m\times m}\}$ is gained, and with key_2 and key_3, the final recovered watermark WN is achieved via (key_3 -key_2) Arnold transformation.

III. Experimental Results and Discussions

In order to show the transparency and robustness of the proposed algorithm, a series of experiments will be tested in this section. The first frame of stereo image pair of "Puppy" with 640×480 pixels are taken for test images as illustrated in Fig 2. And a binary watermark with 64×64 pixels as shown in Fig 4(a).

A. Watermark Evaluation

To evaluate the quality of watermarked stereo images, the watermark recovering rates is defined with HC.

$$HC = 1 - \frac{\sum W \oplus W'}{m \times m} \quad (8)$$

where $\oplus$ is exclusive-OR.

B. Transparency of Watermark

In the experiment, L=28, T=48, S=10. The watermark is transformed by Arnold as illustrated in Fig. 4(b). The watermark is embedded into the pair of stereo images shown in the Fig.3. Obviously the watermark is transparent to visualization. The peak signal to noise ratio (PSNR) is used to evaluate the perceptual distortion. The PSNR of watermarked left image and right image are 52.14dB 51.99dB, respectively. It means the proposed algorithm has transparency ability. Moreover the watermark can be detected by the algorithm totally as illustrated in Fig. 4(c) and 4(d) when images are not under the attacks, and HC is 1.

C. Robustness to Attacks

Here, JPEG compression, salt and pepper noise, filtering, and cropping are used to attack watermark embedding images (left and right images are attacked to the same extents) respectively, the experiments results confirms the robustness and stability of the proposed algorithm.

Figure 2. Original image. (a) left image and (b) right image

Figure 3. (a) left watermarked image; (b) right watermarked image.

(a) (b) (c) (d)

Figure 4. (a) original watermark; (b) Arnold transformation of watermark; (c) extractedArnold transforamtion watermark; (d) recovered watermark.

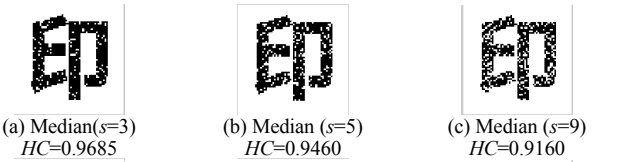
(a) Q=90 HC=0.9765 (b) Q=70 HC=0.9685 (c) Q=50 HC=0.9248 (d) Q=30 HC=0.8982

Figure 5. Recorvered watermarks after JPEG compression.

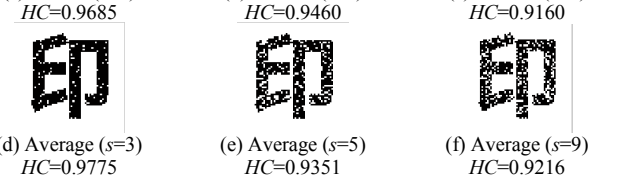
 ISBN: 978-1-61208-166-3

(a) r=1% *HC*=0.9231 (b) r=2% *HC*=0.9133 (c) r=3% *HC*=0.9055 (d) r=4% *HC*=0.9006 (e) r=5% *HC*=0.8943

Figure 6. Recorvered watermarks after salt and peppers noise



(a) Median(s=3) *HC*=0.9685 (b) Median (s=5) *HC*=0.9460 (c) Median (s=9) *HC*=0.9160



(d) Average (s=3) *HC*=0.9775 (e) Average (s=5) *HC*=0.9351 (f) Average (s=9) *HC*=0.9216

Figure 7. Recorvered watermarks after median filter and average of different sizes ($s \times s$).

(a) 1/4 left-top *HC*=0.8345 (b) 1/8 left-top *HC*=0.9614 (c) 1/4 middle *HC*=0.6506 (d) 1/8 middle *HC*=0.8284

Figure 8. Recorvered watermarks after cropped from different parts..

Attacks with JPEG Compression: Fig.5 shows recovered watermarks after JPEG compression with different quality and corresponding *HC*. Visually watermarks can be recognized and the values of *HC* are all around 0.9. It proves the robustness. When Q is from 90 to 30, the *HC* is decreased steadily and not dropped like Q decreased. So the proposed algorithm is still stabile.

Attacks with salt and peppers noise: after distorting the watermarked images by different rates salt and pepper noise, the recovered watermarks are shown in Fig. 6. The watermark can be detected clearly and the most of *HC* are greater than 0.9. It proves the robustness again. Moreover, the changing scope of *HC* is tiny, which shows the stability of the proposed algorithm.

Filtering: when the watermarked images are filtered by median and average filter of different sizes, all watermarks can be examined as illustrated in Fig. 7. Furthermore, the values of *HC* are all greater than 0.92. Thus, the proposed algorithm has the ability against filtering.

Cropped: the proposed algorithm is tested against cropping as well. Watermarked images are cropped from different parts: 1/4 top-left, 1/8 top-left corner, 1/4 middle and 1/8 middle. Apparently watermarks can be detected as shown in Fig. 8.

IV. CONCLUSTION

In this paper, a novel stereo image watermarking algorithm based on relationships and quantization is proposed. The intra-block and inter-block relationships are employed for embedding watermarks. Moreover quantization of direct current coefficients in DCT domain is used for watermark embedding when relationships cannot work well. The experiments demonstrate the transparency of the proposed algorithm. Furthermore, when watermarked pairs of stereo images are on the attack, the watermark can be still detected well and it proves the robustness. However, cropping attack affects the quality of watermarked images much, and we will improve it in the future work.

ACKNOWLEDGMENT

This work was supported by Natural Science Foundation of China (61071120, 60872094, 60832003), Natural Science Foundation of Zhejiang Province (Y1101240), the projects of Chinese Ministry of Education (200816460003), and Natural Science Foundation of Ningbo (2011A610197).

REFERENCES

[1] P. Benzie, J. Watson, P. Surman, I. Rakkolainen, K. Hopf, H. Urey, and et al., A survey of 3DTV dispalys: techniques and technologies. IEEE Transactions on circuits and systems for video technology, vol. 11, no. 17, 2007, pp. 1647-1658.

[2] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, Digital watermarking and steganography, the 2nd ed., Morgan: Kaufmann, 2007.

[3] P. Campisi. Object-oriented stereo-image digital watermarking. Journal of Electronic Imageing, vol. 17, no. 4, 2008, art. no. 043024.

[4] D. Hwang, K. Bae, M. Lee and E. Kim, Real time stereo image watermarking using discrete cosine transform and adaptive disparity map, Proc. SPIE 5241, 2003, pp. 233-242.

[5] D. Hwang, J. Ko, J. Park and E. Kim, Stereo watermarking scheme based on discrete wavelet transform and feature-based window matching algorithm, Proc. SPIE, 2004, pp. 182-191.

[6] G. Langelaar and R. Lagendijk, Optimal differential energy watermarking of DCT encoded images and video, IEEE Transactions on Image Processing, vol. 10, no.1, 2001, pp. 48-158.

[7] H. Ling, Z. Lu, and F. Zou, Improved differential energy watermarking (IDEW) algorithm for DCT encoded image and video, Int. Conf. on Signal Processing, 2004, pp. 2326-2329.

[8] Y. Chen, J. Su and H. Fu, Adaptive watermarking using relationships between wavelet coefficients, ISCAS, 2005, pp. 4979-4982.

[9] S. Kim, S. Lee, T. Kim, K. Kwon and K. Lee, A video watermarking using the 3-D wavelet transform and two perceptual watermarks. LNCS, 2005, pp. 294-303.

[10] A. Haj, Combined DWT-DCT digital image watermarking, Journal of Computer Science, vol. 3, no. 9, 2007, pp. 740-746.

 ISBN: 978-1-61208-166-3

An Efficient Access Control Scheme for Multimedia Content Using Modified Hash Chain

Shoko Imaizumi
Division of Information Sciences
Graduate School of Advanced Integration Science
Chiba University
Chiba, Japan
Email: imaizumi@chiba-u.jp

Masaaki Fujiyoshi, Hitoshi Kiya
Dept. of Information and Communication Systems
Tokyo Metropolitan University
Tokyo, Japan
Email: fujiyoshi-masaaki@tmu.ac.jp, kiya@sd.tmu.ac.jp

***Abstract*—This paper proposes an access control scheme for multimedia content consisting of several media such as text, images, sound, and so on. The proposed scheme simultaneously controls access to each medium of multimedia content in which a hierarchy based on the quality (resolution, frame rate, bit rate, and so on) is allowed to be in one medium. The proposed scheme derives keys through hash chains, and each medium/ entity is encrypted with each individual key. By introducing modified hash chains, the proposed scheme manages only a single key for multimedia content, and it delivers only a single key to a user for the content regardless of which parts in the content the user can access; whereas the conventional access control schemes having the above mentioned features manage and/or deliver multiple keys. The single managed key is not delivered to any user. Furthermore the proposed scheme is resilient to collusion attacks. Performance analysis shows the effectiveness of the proposed scheme. The proposed scheme is more secure and simpler than the conventional scheme in terms of key management and delivery.**

***Keywords-multimedia communication*; *access control*; *key derivation*; *hash chain*; *cryptography*.**

I. INTRODUCTION

With the growth in network technology, the exchange of digital images and sound as well as text become very common regardless of whether the digital content is used for commercial purpose or not. Since such digital content is easily duplicated and re-distributed, protecting copyrights and privacy is an important issue. *Access control* based on naïve encryption (encrypting the whole content) [1] or media-aware encryption [2]–[6] has been studied widely to protect digital content.

A simple and straightforward way for realizing versatile access control to multimedia content consisting of several media to which several entities belong is encrypting each entity individually. This approach, however, has to manage a large number of keys, according to the number of entities in multimedia content. Moreover, a user has to receive a number of keys, according to the number of accessible entities.

On the other hand, for JPEG 2000 [7] coded images and/ or MPEG-4 fine granularity scalability [8] coded videos, *scalable access control* schemes have been proposed [2]–[6]. These schemes utilize one- or multi-dimensionally *hierarchical scalability* provided by coding technologies so that a user can obtain an image or a video in the permitted quality from one common codestream. In addition, *hash chain* [9], [10] is introduced to several schemes for reducing the managed and managed keys [3]–[6].

Though a hash chain-based access control scheme has been proposed for multimedia content [11], the number of managed keys increases dependently on not only the number of media but also the dimensions of hierarchies in the media. The number of delivered keys is increased as many as the number of managed keys. Moreover, malicious users can share their keys to increase accessible media/entities in this scheme.

This paper proposes an access control scheme for multimedia content which the scheme manages and delivers only a single key. The proposed scheme assumes that content consists of several media and there is a scalable hierarchy on the quality in one of media. By introducing modified hash chains, the managed key is one as many as the delivered key regardless of which media/entities the user is allowed to access. The managed key is not delivered to any user in terms of security against key leakage. Moreover, the proposed scheme is resilient to collusion attacks which malicious users access much more portions beyond their rights illegally.

This paper consists of five sections. Section II mentions the conventional access control scheme for multimedia and describes the problems of the conventional scheme. The new scheme is proposed in Section III and is analyzed in Section IV. Finally, conclusions are drawn in Section V.

II. CONVENTIONAL ACCESS CONTROL SCHEME FOR MULTIMEDIA CONTENT

This section briefly describes the conventional access control scheme for multimedia content [11], and summarizes problems of the conventional scheme to clarify the aim of this work.

 ISBN: 978-1-61208-166-3

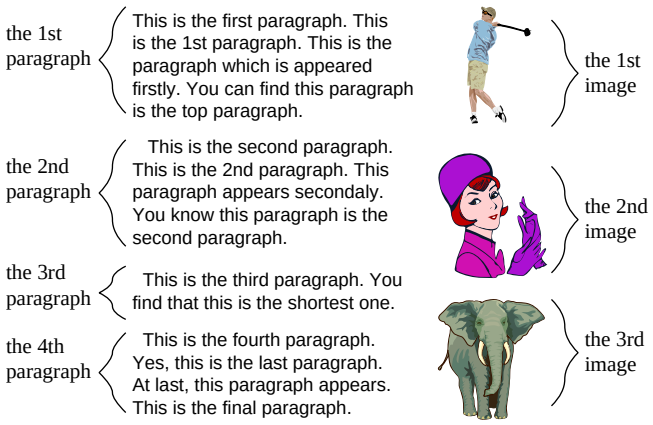


Figure 1. An example of multimedia content (the number of media $M = 2$, the number of entities in the first medium $D_1 = 4$, and the number of entities in the second medium $D_2 = 3$).

A. Conventional Scheme

The conventional scheme [11] assumes that content consists of M different media (image, video, sound, text, and so on) which a hierarchy (image/video resolution, frame rate, bit rate, etc) exists in each medium; In the text medium, the appearing order of paragraphs has its own meaning, and it is referred to as a *semantic* hierarchy. The scheme uses a symmetric encryption technique.

For multimedia content consisting of M different media, this scheme manages M keys. Fig. 1 shows an example of multimedia content where $M = 2$. For the m-th medium where $m = 1, 2, \ldots, M$, encryption keys are derived from managed key $K_m^{D_m}$ that corresponds to the m-th medium, where D_m represents the number of entities in the medium, i.e., the depth of the hierarchy. Encryption keys $K_m^{d_m}$'s are derived through a hash chain as

$$K_m^{d_m} = H^{D_m - d_m}\left(K_m^{D_m}\right), \ d_m = 0, 1, \ldots, D_m - 1, \quad (1)$$

where $H^{\alpha}(\beta)$ represents that cryptographic one-way hash function $H(\cdot)$ is applied to β recursively α times. The d_m-th entity in the m-th medium is encrypted with its corresponding encryption key, $K_m^{d_m}$.

A user receives M decryption keys. Each user receives different set of decryption keys, which are delivered keys, due to which media/entities the user is allowed to access, but all users receives the common encrypted multimedia content. From the delivered keys, the user derives keys for accessible entities in accessible media through the same hash chain as used in the encryption key derivation. That is,

$$K_m^{\delta_m} = H^{\Delta_m - \delta_m}\left(K_m^{\Delta_m}\right), \ \delta_m = 1, 2, \ldots, \Delta_m - 1, \quad (2)$$

where $K_m^{\Delta_m}$ is the delivered key for the m-th medium. By using Δ_m decryption keys, the user decrypts Δ_m entities from the first entity to the Δ_m-th entity.

A user who receives K_m^0 cannot access any entities in the m-th medium, because one-way property of $H(\cdot)$ prevents the user to generate any other valid keys for the m-th medium of the content. The conventional scheme introduced this *unusable key* concept in order to cope with medium-based access control.

B. Problems of the Conventional Scheme

The conventional scheme [11] has two major problems.

- the number of managed and delivered keys
- collusion attack-vulnerable

As mentioned in the previous section, the conventional scheme encrypts entities in a medium independently of other media. This feature of the conventional scheme requires managed and delivered keys as many as media in the multimedia content, i.e., M keys are managed and M keys are delivered to a user for content consisting of M different media. This conventional scheme employs ordinary hash chains [9] rather than cross-way hash trees [10] in essentials.

The latter problem is also attributed to the feature just described in the above paragraph. Though introducing unusable key concept in order to serve medium-based access control, the conventional scheme allows malicious users to collude to access inaccessible media. A user who can display images and another user who is allowed to read texts share their keys and obtain both images and text paragraphs.

In the next section, a new access control scheme for multimedia content is proposed. The proposed scheme manages only a single key and delivers also only a single key to a user regardless of which media/entities in the content the user can access. In addition, the proposed scheme is resistant to collusion attack.

III. Proposed Scheme

This section proposes a new access control scheme for multimedia content. The proposed scheme assumes that multimedia content C consists of M media and the first medium has a hierarchical structure;

$$C = \left\{G_1^1, G_2^1, \ldots, G_m^1, \ldots, G_M^1\right\}, \quad (3)$$

$$G_1^1 \supset G_1^2 \supset G_1^3 \supset \cdots \supset G_1^{D_m}, \quad (4)$$

where G_m^1 $(m = 1, 2, \ldots, M)$ represents the m-th medium content itself, and D_1 is the depth of the hierarchy in the first medium. The complementary sets represent entities in medium G_1^1 as

$$E_1^{d_m} = G_1^{d_m} - G_1^{d_m+1}, \quad d_m = 1, 2, \ldots, D_m - 1, \quad (5)$$

and

$$E_m^{D_m} = G_m^{D_m}. \quad (6)$$

The proposed scheme derives keys from single managed key K_C and encrypts content C by encrypting $E_m^{d_m}$'s using those corresponding keys. In addition, this scheme delivers only a single key to each user.

Fig. 2 shows an example conceptual diagram of the assumed multimedia content, where content C consists of

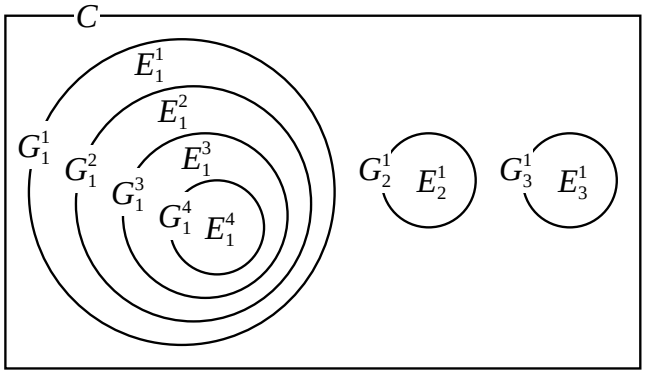


Figure 2. An example of multimedia content conceptual diagram in the proposed scheme (the number of media $M = 3$ and the depth of the hierarchical structure in the first medium $D_1 = 4$).

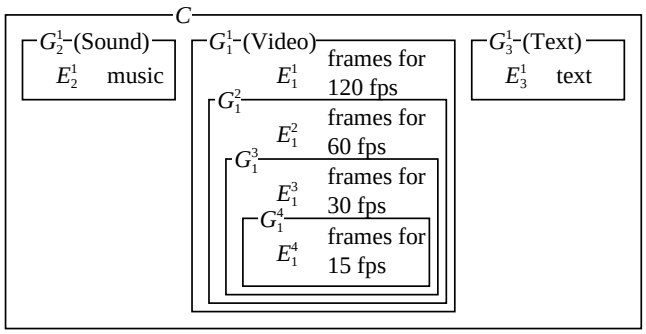


Figure 3. A practical example of multimedia content (the number of media $M = 3$ and the depth of video $D_1 = 4$).

three media, G_1^1, G_2^1, and G_3^1, i.e., $M = 3$, and the hierarchy depth of medium G_1^1 is four ($D_1 = 4$), i.e.,

$$G_1^1 \subset G_1^2 \subset G_1^3 \subset G_1^4. \quad (7)$$

E_1^1, E_1^2, E_1^3, and E_1^4 are entities in medium G_1^1.

A. Key Derivation and Encryption

This section provides the key derivation mechanism in the proposed scheme under the condition content C is abstracted as Fig. 2. For easy understanding, more practical example is given in Fig. 3. Content C in Fig. 3 consists of video, sound, and text, i.e., $M = 3$, and video has a hierarchy with four in depth in terms of the frame rate, i.e., $D_1 = 4$. In this example, G_1^1 is digital video, and it is playable in several frame rates; 120, 60, 30, and 15 frames per second (fps). Shown in Fig. 4, frames decoded at each rate are represented by G_1^1, G_1^2, G_1^3, and G_1^4, respectively. Media G_2^1 and G_3^1 are sound and text, respectively.

In the example here, access control is provided based on not only media but also the frame rates of video. For content C shown in Fig. 3, keys for encryption are derived as shown in Fig. 5, and each key is used to encrypt and decrypt the corresponding medium/entity. For the video, $K_{E_1^1}$ is

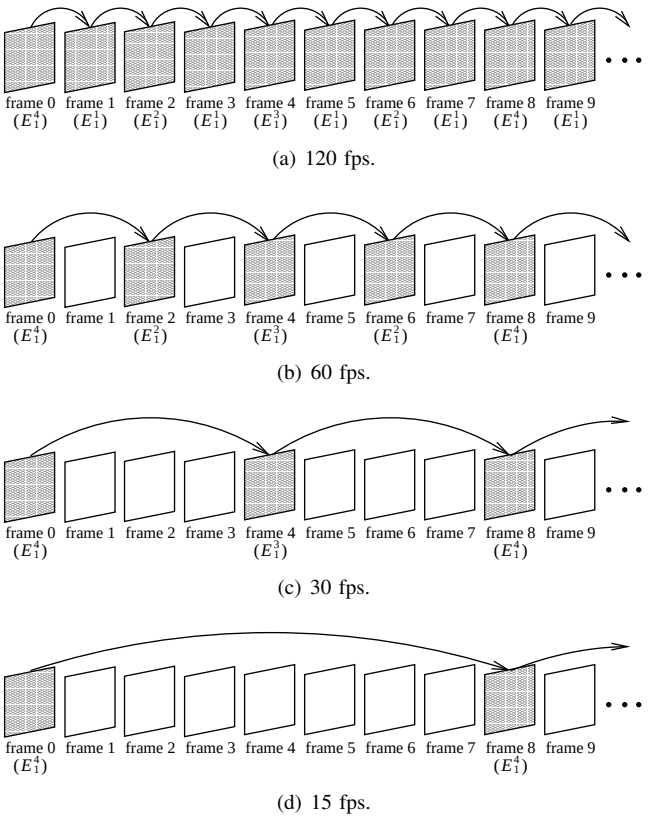


Figure 4. Decode of a movie in different frame rates (The shaded frames are decoded).

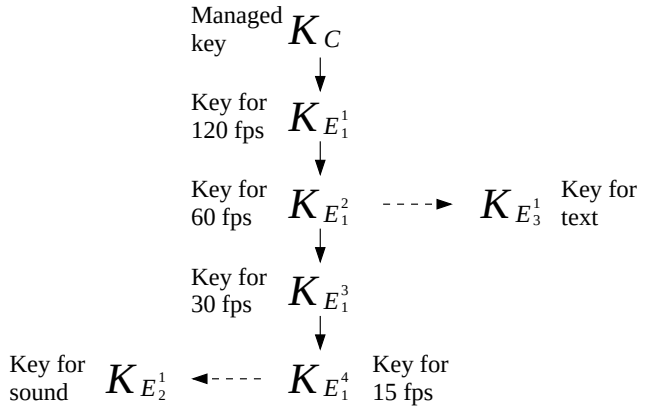


Figure 5. Key derivation to control access to the content shown in Fig. 3. All users who are allowed to access video with any frame rates can access sound medium. Users who are allowed to access video with 60 fps or 120 fps can view text data. A solid arrow is an ordinary hash function and a dashed arrow is a modified hash function.

for E_1^1 which represents frames decoded at 120 fps only. Similarly, keys $K_{E_1^2}$, $K_{E_1^3}$, and $K_{E_1^4}$ are for E_1^2, E_1^3, and E_1^4, respectively. Keys $K_{E_2^1}$ and $K_{E_3^1}$ are for sound and text, respectively. It is noted that key K_C is the single managed key.

Firstly in the proposed scheme, keys $K_{E_1^{d_1}}$ are derived from K_C as

$$K_{E_1^{d_1}} = H^{d_1}(K_C), \quad d_1 = 1, 2, \ldots, D_1, \tag{8}$$

where $H(\cdot)$ is a cryptographic one-way hash function. Eq. (8) represents an ordinary hash chain [9], and the chain is shown with solid arrows in Fig. 5.

Meanwhile, keys $K_{E_2^1}$ and $K_{E_3^1}$ are derived by modified hash chains in the proposed scheme. In this example, these keys are given as

$$K_{E_2^1} = H\left(f\left(K_{E_1^4}, H\left(K_{E_1^4}\right)\right)\right), \tag{9}$$

$$K_{E_3^1} = H\left(f\left(K_{E_1^2}, H\left(K_{E_1^2}\right)\right)\right), \tag{10}$$

respectively, where $f(\cdot)$ is an function with two input and one output in which the length of inputs and output are identical. A bitwise exclusive or operation is a simple example of function $f(\cdot)$. As shown in Eqs. (9) and (10) which represent modified hash chains introduced in this paper, keys given by Eq. (8) are repeatedly used to derive other hash chains that are different from the ordinary hash chains. The modified hash chains are shown with combination of solid and dashed arrows in Fig. 5.

Each entity $E_m^{d_m}$ is encrypted using each corresponding key $K_{E_m^{d_m}}$, and encrypted content C is opened to public.

B. Delivered Key for Each User and Decryption

1) User allowed to access video, sound, and text: A user permitted to decode frames at 120 or 60 fps receives $K_{E_1^1}$ or $K_{E_1^2}$ shown in Figs. 6 (a) and (b). Eq. (8) is same as,

$$K_{E_1^{d_1}} = H\left(K_{E_1^{d_1-1}}\right), \quad d_1 = 1, 2, \ldots, D_1. \tag{11}$$

The user can obtain $K_{E_1^{d_1}}$ $(d_1 = 1, 2, 3, 4)$ using an ordinary hash chain in Eq. (11).

As shown in Fig. 5, keys $K_{E_2^1}$ and $K_{E_3^1}$ for sound E_2^1 and text E_3^1 are generated from $K_{E_1^4}$ and $K_{E_1^2}$, respectively, using modified hash chains in Eqs. (9) and (10). Thus the user can also obtain $K_{E_2^1}$ and $K_{E_3^1}$ and play sound and read text in addition to watch the video.

2) User allowed to access video and sound: A user can access frames decoded at 30 or 15 fps receives $K_{E_1^3}$ or $K_{E_1^4}$ as shown in Figs. 6 (c) and (d). The user has $K_{E_1^4}$ but does not have $K_{E_1^2}$. Thus the user can obtain only $K_{E_2^1}$ for sound E_2^1 by Eq. (9) and play sound as well as the video.

3) User allowed to access sound: A user allowed to access only sound E_2^1 receives $K_{E_2^1}$ as shown in Fig. 6 (e). $K_{E_2^1}$ is a key generated by Eq. (9). Any keys cannot be generated from $K_{E_2^1}$.

4) User allowed to access text: A user allowed to access only text E_3^1 receives $K_{E_3^1}$ as shown in Fig. 6 (f). $K_{E_3^1}$ is a key generated by Eq. (10). $K_{E_3^1}$ can generate no other key.

Table I
COMPARISONS IN TERMS OF THE NUMBER OF MANAGED AND DELIVERED KEYS, DELIVERY OF MANAGED KEYS, AND COLLUSION ATTACK RESILIENCE.

	Proposed	Conventional [11]
The number of managed keys	1	M
The number of delivered keys	1	M
Delivery of managed keys	No	Yes
Collusion attack resilience	Yes	No

C. Features

Two main features of the proposed scheme are briefly summarized here.

By introducing modified hash chains, the proposed scheme reduces both the managed and delivered keys to one. In contrast, the conventional scheme [11] manages and delivers keys as many as media.

By using modified hash chains, multiple media are related to prevent malicious users to collude. The conventional scheme is collusion attack-vulnerable, because the conventional scheme encrypts each medium separately.

In addition to the above features, the single managed key is not delivered to any users in the proposed scheme while the conventional scheme delivered the managed keys to some users.

It is noted that any arbitrary function and key combination can be used for a modified hash chain and that any arbitrary key assign can be used to properly control access to the content.

IV. EVALUATION

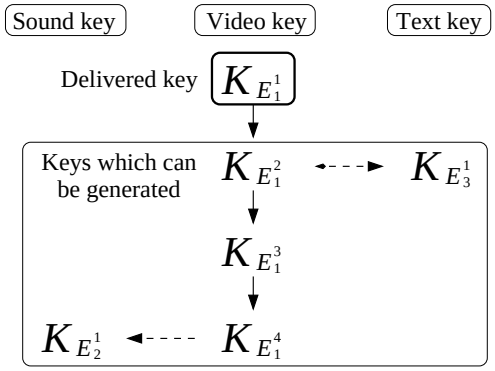
The proposed scheme is evaluated by comparing with the conventional scheme [11] which uses ordinary hash chains [9] only. Evaluation is given in terms of the number of managed and delivered keys, delivery of managed keys, and collusion attack resilience.

Table I shows the results of comparisons. The proposed scheme manages and delivers only a single key regardless of the number of media and the depth of the hierarchical structure in a medium, whilst the conventional scheme [11] must manage and deliver keys as many as media. The single managed key is not delivered to any user in the proposed scheme, whereas the managed keys are delivered to some users in the conventional scheme [11]. In addition, the proposed scheme is resilient to collusion attacks while the conventional scheme [11] is naive for collusion attacks. The table brings out the effectiveness of the proposed scheme.

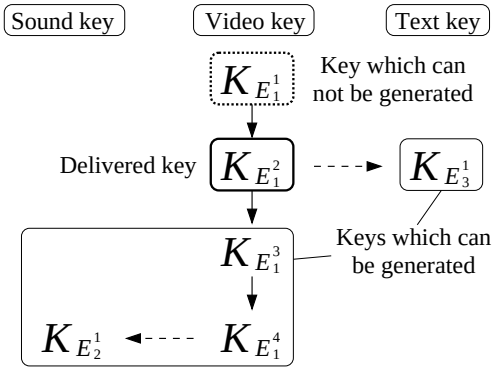
V. CONCLUSION

This paper has proposed a new access control scheme for multimedia content in which modified hash chains are employed. The proposed scheme manages only a single key. This scheme also delivers only a single key to a user regardless of which portions of the content to which the user can access. In the proposed scheme, the single managed

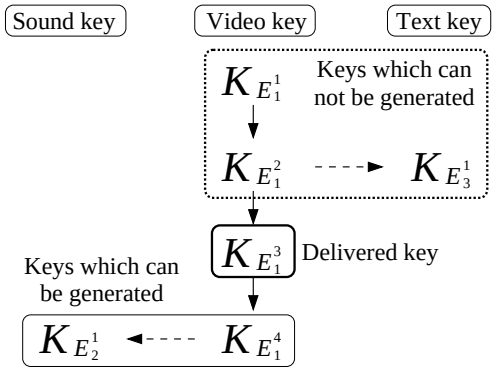
 ISBN: 978-1-61208-166-3



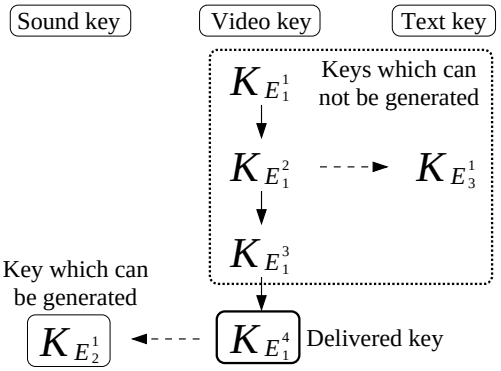
(a) A user whose delivered key is $K_{E_1^1}$.



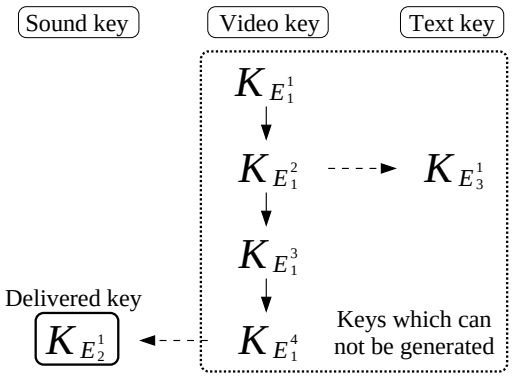
(b) A user whose delivered key is $K_{E_1^2}$.



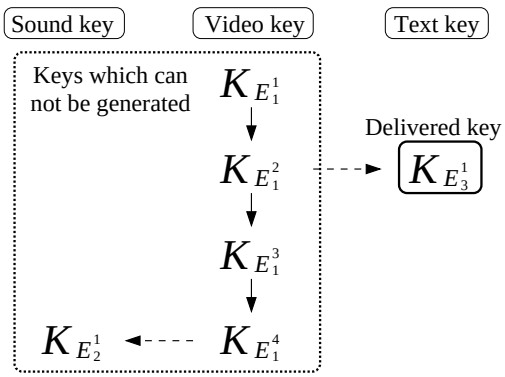
(c) A user whose delivered key is $K_{E_1^3}$.



(d) A user whose delivered key is $K_{E_1^4}$.



(e) A user whose delivered key is $K_{E_2^1}$.



(f) A user whose delivered key is $K_{E_3^1}$.

Figure 6. A delivered key and decryption keys for each user.

key is not delivered to any user. Furthermore, the proposed scheme prevents malicious users to collude for accessing much more portions. Comparison result summarizes the effectiveness of the proposed scheme. The proposed scheme thus controls access to mulimedia content securely and simply in comparison to the conventional scheme.

 ISBN: 978-1-61208-166-3

Applying the proposed scheme to content in which each medium has its own hierarchical structure is a further work. Moreover, we would like to apply the proposed scheme to other security technologies such as digital watermarking and secret sharing.

REFERENCES

[1] B. B. Zhu, M. D. Swanson, and S. Li, "Encryption and authentication for scalable multimedia: current state of the art and challenges," in *Proc. SPIE*, vol.5601, pp. 157–170, 2004.

[2] Z. Shahid, M. Chaumont, and W. Puech, "Selective and scalable encryption of enhancement layers for dyadic scalable H.264/AVC by scrambling of scan patterns," in *Proc. IEEE ICIP*, pp. 1273–1276, 2009.

[3] Y. Wu, D. Ma, and R.H. Deng, "Progressive protection of JPEG 2000 codestreams," in *Proc. IEEE ICIP*, pp. 3447–3450, 2004.

[4] Y. G. Won, T. M. Bae. and Y. M. Ro, "Scalable protection and access control in full scalable video coding," in *Proc. IEEE IWDW*, pp. 407–421, 2006.

[5] S. Imaizumi, Y. Abe, M. Fujiyoshi, and H. Kiya, "Collusion attack-resilient hierarchical encryption of JPEG 2000 codestreams with scalable access control," in *Proc. IEEE ICIP*, pp. II–137–II–140, 2007.

[6] S. Imaizumi, M. Fujiyoshi, and H. Kiya, "Efficient collusion attack-free access control for multidimensionally hierarchical scalability content," in *Proc. IEEE ISCAS*, pp. 505–508, 2009.

[7] *Information technology — JPEG 2000 image coding system – Part 1: Core coding system.* ISO/IEC IS–15444–1, 2000.

[8] *Streaming Video Profiles (FGS).* ISO/IEC 14496–2/FDAM 4, 2001.

[9] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol.24, no.11, pp. 770–772, 1981.

[10] M. Joye and S. M. Yen, "One-way cross-trees and their applications," in *Proc. IACR PKC*, pp. 355–358, 2002.

[11] M. Fujiyoshi, W. Saitou, O. Watanabe, and H. Kiya, "Hierarchical encryption of multimedia contents for access control," in *Proc. IEEE ICIP*, pp. 1977–1980, 2006.

 ISBN: 978-1-61208-166-3

Energy Efficient Target Tracking in Wireless Sensor Networks with Limited Sensing Range

Oualid Demigha *, Hamza Ould Slimane*, Abderahim Bouziani* and Walid-Khaled Hidouci †
*Ecole Militaire Polytechnique
Bordj El-Bahri, Algiers 16111. Algeria
Email: o_demigha@esi.dz, hamzabydos@gmail.com, abdou.bouzbouz@gmail.com
†Ecole Nationale Superieure d'Informatique
Oued-Smar, Algiers. Algeria
Email: w_hidouci@esi.dz

***Abstract*—In this paper, we propose a dynamic clustering protocol coupled with a consensus-based Kalman filter algorithm to self-organize Wireless Sensor Networks for localized tracking of a single moving target. Our proposed scheme takes opportunity from the fact that the target presence is a localized event. Therefore, We consider a WSN with limited sensing range to design a target tracking scheme using low-cost limited-energy nodes. Simulation results show a clear improvement in the network energy consumption, however state estimation quality degrades slightly compared with centralized approaches and other tracking schemes with limited sensing range that do not limit the set of tracking nodes. Our tracking scheme reduces the number of tasking nodes which reduces the network energy consumption.**

***Index Terms*—Energy conservation, dynamic clustering, localized target tracking, Kalman consensus filter, limited sensing range.**

I. INTRODUCTION

Wireless Sensor Network (WSN) is an emerging technology that consists of hundreds or thousands of tiny low-cost energy-limited nodes that have small capacities of sensing, processing and communication via radio medium. Typically, these nodes report captured data to a base station for further processing. They are equipped with a low-cost small-capacity batteries which are, in most cases, non-rechargeable and irreplaceable. Therefore, network lifetime is considered as an important issue for many key applications such as: target tracking [1].

In contrast to high-cost sophisticated surveillance technologies, WSNs use cheap technology that do not rely on any centralized infrastructure.

This technology which aims at providing the same performance as do traditional systems, brings up new challenges related to data processing algorithms, communication systems and network organization. In many cases, collaboration among nodes helps at solving these challenging open-issues.

In contrast to single-node tracking systems, collaborative target tracking fuses data transmitted by many nodes and produces state-estimation of the target. However, these measurements are noisy, redundant and non-synchronized and the inter-node communication is an energy-consuming task. Furthermore, neither reliable communication protocols nor complex data processing algorithms can be implemented on a sensor node because of its limited processing and communication capacities.

Therefore, energy efficiency in target tracking is a key issue in WSN and it can be achieved using different methods [2]. One of them is the prediction-based schemes coupled with selective activation. Sensor nodes can collaboratively generate predictions of the target location by executing an *in-network light-weight* data fusion algorithm. The gain of such algorithms is two-fold: (i) it generates state-estimates of the target, and (ii) it produces state-predictions for the next sampling period which are used to activate selected nodes (implicitly or explicitly by sending an activation message).

In many cases, this method requires collaboration among nodes to provide accurate data in presence of noisy sensor measurements transmitted over noisy communication links. Furthermore, sensor readings from the low-cost limited sensing range components are, in fact, less accurate but they are close to the target which, in turn, can be detected by more than one sensor at the same time. Hence, the sensor network can take profit form this data redundancy to improve the tracking quality.

In this paper, we consider a WSN with limited sensing range that *localizes* the data fusion algorithm within the target detection zone and *self-organizes* nodes within dynamic clusters that move along the target trajectory. It is interesting to study this type of WSN because they help at minimizing the network energy consumption and provide acceptable tracking quality by selecting the appropriate tasking nodes.

This paper is organized as follows: in Section II, we give some definitions and system models. In Section III, we describe some related works proposed in the literature to reduce energy consumption via distributed Kalman filter algorithm. In Section IV, we present our proposed method that consists of two main components: (1) the Kalman consensus filter and (2) the dynamic clustering protocol. In Section V, we discuss the simulation results and the tradeoff between the energy consumption and the estimation quality. Finally, in Section VI, we conclude the paper.

 ISBN: 978-1-61208-166-3

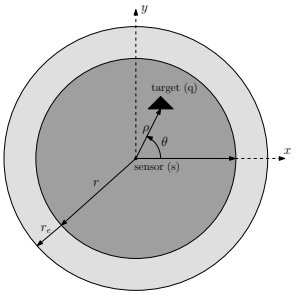


Fig. 1. Probabilistic detection model

II. BACKGROUND

In the following subsections, we give some basic definitions of the WSN model and the centralized Kalman filter. After that we describe the mathematical model of the distributed Kalman filter adopted in our proposed method.

A. System Model and Assumptions

We model the wireless sensor network by a non-oriented graph $G(V, E)$ where $V = \{s_1, s_2, \cdots, s_n\}$ is the set of nodes and $E = \{(s_i, s_j) \mid \|s_i - s_j\| \leq R_c\}$ is the set of communication links. R_c is the communication range of each node and $\|s_i - s_j\|$ is the Euclidean distance between nodes s_i and s_j. We assume that the sensing range R_s is uniform among all the nodes and it verifies the condition required for coverage and connectivity constraints, i.e., $R_c \geq 2R_s$.

We suppose that the target state is a 4-tuple vector:

$$X = (x, y, \dot{x}, \dot{y}) \in R^4$$

where (x, y) and $(\dot{x}, \dot{y})$ are respectively, the target position coordinates and its velocity along X and Y axes. Each node measures the distance to the target ρ and the angle between the X axis and the target position vector θ. For target detection, we use a probabilistic model expressed by the equation 1:

$$p_s(q) = \begin{cases} 0 & \text{if } r + r_e \leq \|s - q\| \\ e^{-\alpha(\|s-q\|-(r-r_e))^\beta} & \text{if } r - r_e \leq \|s - q\| \leq r + r_e \\ 1 & \text{if } r - r_e \geq \|s - q\| \end{cases} \quad (1)$$

where $\|s - q\|$ is the Euclidean distance between sensor s target q, r is the sensing range of s and r_e is the sensing error ($r_e \ll r$). α and β are constants (see Figure 1).

We assume also that nodes are initially in the sleep state which guarantees minimum energy consumption. In fact, in this state, all the nodes' hardware units are OFF, except the processing unit and a low-power *paging channel* to receive *wake-up* messages. Upon receiving a wake-up message, nodes start up all their hardware units. Nodes are supposed aware of their geographic positions and each node maintains a list of its neighboring nodes.

The first target detection is supposed done successfully and the first activation is performed via an *external* activation message.

B. Centralized Kalman Filter

We assume that the target state and the measurement models are respectively defined by the following linear equations:

$$x_{k+1} = A_k x_k + B_k u_k + w_k$$
$$z_k = H_k x_k + v_k$$

where: A is the matrix that relates the previous target state to the current one, B is the matrix that relates commands to the current target state, w_k is the system noise, H is the matrix that relates the measurements to the current target state and v_k is the measurements' noise at time step k. x_k is the target state vector at time step k.

We suppose that w and v are white noises with Q and R covariances respectively: $p(w) \sim N(0, Q)$ and $p(v) \sim N(0, R)$. Also, we suppose that matrices A and H are detectable and all matrices A, B, H, Q and R are time-independent. For *Constant-Velocity* target model, matrix A_k and H_k have these values:

$$A_k = A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, H_k = H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

We denote $\hat{x}_k^-$ and $\hat{x}_k$ as the *a priori* and the *a posteriori* target state estimations at the time step k, respectively.

As same, the a priori and a posteriori estimation error covariance matrices P_k^-, P_k at time step k are defined by:

$$P_k^- = E[(x_k - \hat{x}_k^-)(x_k - \hat{x}_k^-)^T]$$
$$P_k = E[(x_k - \hat{x}_k)(x_k - \hat{x}_k)^T]$$

The Kalman gain factor at time step k is defined by:

$$K_k = P_k^- H_k^T (H_k P_k^- H_k^T + R_k)^{-1}$$

We summarize the Kalman model by the following recursive steps:

1) Prediction Step:
   - Next step state prediction:
   $$x_{k+1}^- = A_k \hat{x}_k + B_k u_k \quad (2)$$
   - Next step error covariance prediction:
   $$P_{k+1}^- = A_k P_k A_k^T + Q_k \quad (3)$$
2) Update Step:
   - Kalman gain:
   $$K_k = P_k^- H_k^T (H P_k^- H^T + R)^{-1} \quad (4)$$
   - Estimation update:
   $$\hat{x}_k = \hat{x}_k^- + K_k(z_k - H_k x_k^-) \quad (5)$$
   - Error covariance update:
   $$P_k = (I - K_k H_k) P_k^- \quad (6)$$

 ISBN: 978-1-61208-166-3

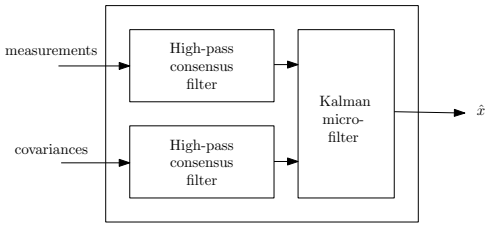


Fig. 2. Micro-filter architecture of a DKF node

C. Consensus on Kalman micro-filters

Decentralized Kalman filter gives target state estimation using a set of k micro-filters. This model requires *all-to-all* communications. In [3], the authors propose a Distributed Kalman Filter (DKF) that uses high-pass and low-pass filters to fuse data. It can fuse heterogeneous data obtained from non-linear sensing model:

$$y_i = h_i(x_k) + v_i^k$$

All the nodes have the same architecture as illustrated in Figure 2.

The system to be observed is modeled as follows: $x_k = A_k x_{k-1} + B_k w_k$ and $y_i^k = H_i^k x_k + v_i^k$

In addition to the Kalman filter model equations described in Section II-B, two new values are included into the model namely: (1) the fusion of the error covariance inverse matrix and (2) the fusion of the measurements. These two values are expressed respectively by:

$$S_k = \frac{\sum_{i=1}^{n} H_i^{kT} R_i^{-1} H_i^k}{n}$$

and

$$y_k = \frac{\sum_{i=1}^{n} H_i^{kT} R_i^{-1} y_i^k}{n}$$

Each node executes the following calculations:

$$M_i^k = (P_{i,k}^{-1} + S_k)^{-1}$$

$$\hat{x}_k = \hat{x}_k^- + M_i^k (y_k - S_k \hat{x}_k^-)$$

$$P_i^{k+1} = A_k M_i^k A_k^T + B_k Q_i^k B_k^T$$

$$\hat{x}_{k+1} = A_k \hat{x}_k$$

with: $Q_i^k = nQ_k$ and $P_i^0 = nP_0$. The estimations are identical in all nodes, i.e.,

$$\hat{x}_i^k = \hat{x}_k, \forall i$$

The filter dynamic is expressed by equation 7 (for more details see [4]):

$$\begin{cases} \dot{q}_i = -\beta \hat{L} q_i - \beta \hat{L} u_i \\ p_i = q_i + u_i \end{cases} \quad (7)$$

where $\hat{L} = L \bigotimes I_m$ is the m-dimension graph laplacian, u_i is the node input, q_i is the Kalman filter state and β ($\beta > 0$) is the gain (it should be big enough for random deployed topologies). The filter output is computed according to equation 8:

$$\begin{cases} \dot{q}_i = \beta \sum_{j \in N_i} (q_j - q_i) + \beta \sum_{j \in N_i} (u_j - u_i) \quad \beta > 0 \\ y_i = q_i + u_i \end{cases} \quad (8)$$

With N_i is the i^{th} node's neighbors set (the reader could refer to [5] to learn more about filter discreatization in connected graphs).

III. Related Work

The Kalman Consensus Filter (KCF) is proposed in [3]. It uses a set of *k Kalman micro-filters* to fuse heterogeneous data received from sensors with non-linear sensing models. There are two variants of this approach: one fuses measurements and the other fuses estimations. In the measurements' fusion variant, low-pass and band-pass filters are modified into *high-gain* high-pass filters. The other variant fuses estimations instead of measurements in order to accelerate the consensus convergence. This filter uses latency-generating power-consuming complex matrix computations which may fail at detecting fast targets. Furthermore, the algorithm makes the assumption that all nodes can observe the target which may not hold all the time.

In [6], the authors use biparti graphs to distribute the Kalman Filter (KF) model. In this approach, the KF model is distributed on the whole network and the global model is decomposed into n_l ($n_l \ll n$ and n is the network size) reduced sub-models, each one is executed by a micro-filter in a single node. Each node computes its local estimation and fuses it with the received estimations. Biparti graphs are used when dependencies exist between these sub-models. This method is suitable for estimations' fusion because it includes data correlation between local estimations.

Distributed Kalman filter with Gossip communications is proposed in [7]. Each node can sense only a part of the observed phenomenon, i.e., each node can measure or estimate a subset of the target state attributes and communicates them to its neighbors and then deduces the missed attributes. There are two drawbacks to this method: (1) message communication complexity, i.e., nodes exchange many messages (estimations and error covariance matrix) , and (2) topology-dependency model, i.e., strong network connectivity is required for estimations' communication between neighboring nodes.

Olfati et al. propose a distributed Kalman filter with limited sensing range [8] in which nodes implement local micro-filters and reach a consensus using message passing communication model. This scheme makes the assumption that passive nodes (nodes that do not detect the target) are considered with *no contribution*. Even that, they are included in the fusion step.

Instead of sending long messages, authors of [9] propose that nodes send only *one bit* information. A *quantification function* is defined to represent node's estimation and the filter is then executed in two distinct procedures: an observation-transmission procedure and a reception-estimation procedure.

 ISBN: 978-1-61208-166-3

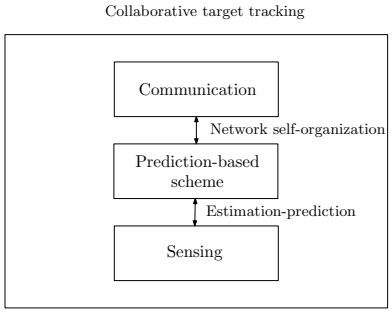


Fig. 3. Problem characterization

The main disadvantage of such approaches is that the quantification function may induce information loss when lossy links are present in the network.

IV. Proposed Method

All the above-mentioned approaches do not consider the problem of limiting the number of nodes participating in the tracking task and suppose that the target can be observed by the *whole* network. However, these two assumptions do not hold in all cases: i.e., in a 2D ground deployed WSN, only nodes that are close to the phenomenon can sense it; the other nodes can not. In addition, low-power nodes have limited sensing ranges and can communicate with a reduced set of neighbors.

This aspect can be exploited to reduce the energy consumption in a target tracking application. Figure 3 shows the relationship between the sensing component and the communication component in a sensor node that uses a prediction-based scheme. A *light-weight* estimation-prediction algorithm can be used to estimate the target state and predict its next position. This helps at waking-up the most appropriate nodes to track the target and at best organizing the network communications. Consequently, The other nodes remain in the *sleep* state which saves much more energy than in a *periodic sampling*-based target tracking scheme.

Indeed, periodic sampling provides more accurate data but it greatly reduces the energy resources of the nodes. Prediction-based schemes are more appropriate in a dense network where not all nodes are needed to be woken-up.

Therefore, two issues are to be considered here: (1) the estimation algorithm should be distributed over a subset of nodes that are close to the target, and (2) the tracking group should be dynamic depending on the target dynamic model. To resolve these issues we propose a Distributed Kalman Filtering approach with Dynamic Clustering (DKF_DC).

Our method is inspired by the work in [8], but instead of tasking all the network nodes, it uses a dynamic clustering to limit messages exchanges between nodes participating in the estimation process. Our clustering protocol consists of two phases: (1) leader election phase and (2) cluster reconfiguration phase.

Leader election is executed among *active* nodes that are close to the target. The other nodes stay inactive to save their energy resources. Therefore, nodes wake-up only when they receive activation messages to adhere to the current cluster. Unlike centralized fusion methods, the cluster-head in our method is not considered as a fusion center but as a cluster manager that is responsible for its reorganization. Hence, communications are performed between all the active nodes and not only between the active nodes and the cluster-head.

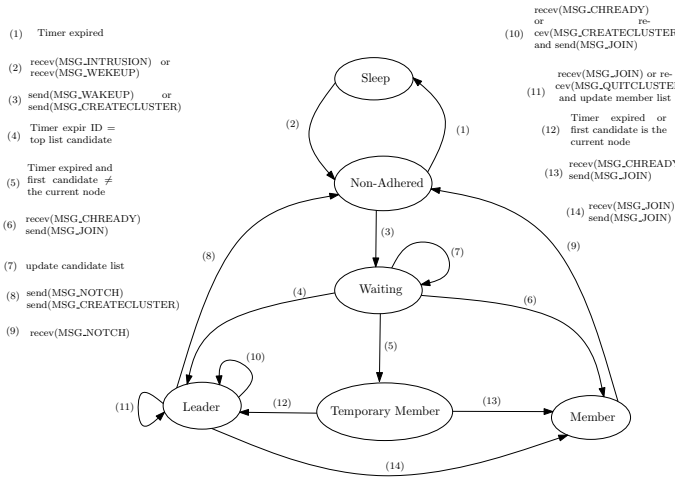


Fig. 4. State-transition diagram of the proposed clustering protocol

Continuous target tracking is guaranteed by allowing a subset of the last cluster members to adhere to the current cluster. That is what ensures the propagation of the estimation information along the target trajectory.

A. Cluster Formation and Leader Election

When a node receives an external intrusion message MSG_INTRUSION that contains the target state estimation recorded by some border nodes, it wakes-up and triggers the leader election phase. First, it sends a wake-up message MSG_WAKEUP to all its neighboring nodes, then it broadcasts a cluster creation message MSG_CREATECLUSTER that contains the first detected position.

Nodes that receive a MSG_CREATECLUSTER message compute a *local decision value* using measures like: (1) the distance between the node and the target, (2) the last estimation quality measured by the covariance matrix P_k issued from the Kalman filter or (3) the residual energy of the node.

As illustrated in the state-transition diagram in Figure 4, a node leaves the *non-adhered* state to go either back to the *sleep* state when a waiting timer expires or to the *waiting* state upon receiving a MSG_CREATECLUSTER message. The node within this state, computes the decision value and broadcasts it to its neighbors. If it receives a value sent from some neighboring node then it updates its *candidates' list* that contains couples (sender, value). Another timer is alarmed to wait for receiving such values. After its expiration, the waiting node decides to become a leader if it is the top list candidate. Otherwise, it becomes a *temporary member*. During the waiting time, if the node receives a MSG_CHREADY

 ISBN: 978-1-61208-166-3

message that contains the cluster-head ID, then it adheres as a member to this cluster.

Temporary-member node discards the top list candidate and waits for receiving a MSG_CHREADY message to adhere to that cluster. If it does not receive such message, it becomes leader if it is the top list candidate.

Similarly, a member node leaves this state upon receiving a MSG_NOTCH message sent by a leader. Consequently, it goes back to the non-adhered state.

B. Cluster Reconfiguration

The leader node checks the target state estimation to decide about the cluster reconfiguration. When it detects that the target is lost, then it performs the following two tasks:

1) Sending back a MSG_JOIN message to force the sender of a MSG_CREATECLUSTER or a MSG_CHREADY message to adhere to its cluster.
2) Updating the cluster members list upon receiving a MSG_JOIN or a MSG_QUITCLUSTER messages.

A leader leaves this state when one of the following events occurs:

- Receiving a MSG_JOIN message to become a member of the message sender's cluster.
- Losing the target: the cluster should be reconfigured and the nodes return back to the non-adhered state.

The cluster reconfiguration operation consists of updating the candidates' list and informing member nodes that the leadership has changed using a MSG_NOTCH message. Upon receiving this message, nodes trigger a new election process that may include previous members.

On the contrary to the scheme proposed in [10], our dynamic clustering protocol prevents multi-cluster tracking by letting only direct neighboring nodes to adhere to the cluster and force the other nodes to return back to the sleep state. After constructing the tracking cluster, the data fusion phase comes into play to generate target state estimation.

C. Target State Estimation

The member nodes of the current cluster perform the sampling to detect the target. They (including the leader node) compute their information matrix u_i and U_i as follows:

$$u_i = H_i^T R_i^{-1} z_i \tag{9}$$

$$U_i = H_i^T R_i^{-1} H_i \tag{10}$$

Equations 9 and 10 contain respectively the measurements information and the measurements errors information. The Kalman filter fuses estimation errors to generate updated state estimations. After that, each node broadcasts a message $m_i = \{u_i, U_i, \bar{x}_i\}$ containing the measurements, the measurements errors and the last state estimation $\bar{x}_i$ to all the cluster members. Each node waits then for receiving such messages from the other members to fuse the information matrix and the vectors y_i and S_i as follows: $y_i = \sum_{j \in J_i} u_j$ and $S_i = \sum_{j \in J_i} U_j$.

At the end of the data fusion phase, each node estimates the target state using KCF:

$$M_i = (P_i^{-1} + S_i)^{-1} \tag{11}$$

$$\hat{x}_i = \bar{x}_i + M_i(y_i - S_i \bar{x}_i) + \gamma M_i \sum_{j \in N_i} (\bar{x}_j - \bar{x}_i) \tag{12}$$

After that, nodes update their respective micro-filter states using equations 13 and 14:

$$P_i = A M_i A^T + BQB^T \tag{13}$$

$$\bar{x}_i = A\hat{x}_i \tag{14}$$

The leader checks the distance to the target and eventually the number of the active nodes in its cluster or the residual energy to decide about the cluster reconfiguration. Consequently, it updates its list of candidates and assigns the leader task to the most appropriate member.

V. Simulations and Results

We use TOSSIM [11] to validate our proposed method by simulation. TOSSIM is a discrete-time simulator of TinyOS operating system for wireless sensor motes. We compared our method with three different target tracking schemes discussed in Section III which are: (1) centralized Kalman filter (CKF) [12], (2) distributed Kalman filter with limited sensing range (DKF_LSR) [8], (3) distributed Kalman filter with gossip communications (DKF_GOSSIP) [7]. The CKF is considered as the base reference for our comparisons.

A. Simulation Setup

Simulation parameters that we vary are: (1) the sampling period, (2) the network size (or network density) and (3) the target velocity. The communication range is set to $50m$, the sensing range is set to $15m$ and the target model is Gauss-Markov.

The nodes' energy consumption is evaluated using POWER-TOSSIM and the estimation quality is measured by the mean square error between the real target position and estimated position:$\epsilon = \sqrt{(x - \hat{x})^2 + (y - \hat{y})^2}$.

In the following subsections, we present the simulation results we have obtained regarding two metrics, namely: energy consumption and estimation quality.

B. Energy Consumption

First, we simulate a 100 nodes WSN that consists of randomly deployed on a 2D area of $200 \times 200m^2$ surface. By varying the sampling period within the set of values from $1s$ to $3s$ we obtain the graphs in the figure 5.

As shown in this figure, the network average energy consumption of the different simulated schemes is inversely proportional to the sampling period time because of the number of data messages exchanged between nodes. CKF and DKF_LSR consume much more energy than DKF_GOSSIP and our method DKF_DC because of the centralized nature of CKF and the non-limited number of nodes that participate in the target state estimation in DKF_LSR. The reduced network

 ISBN: 978-1-61208-166-3

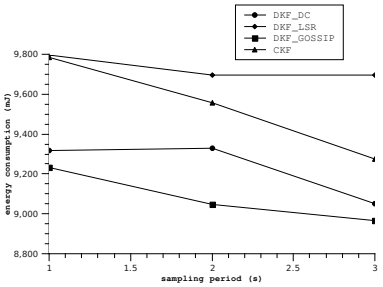


Fig. 5. Energy consumption of the network vs. Sampling period

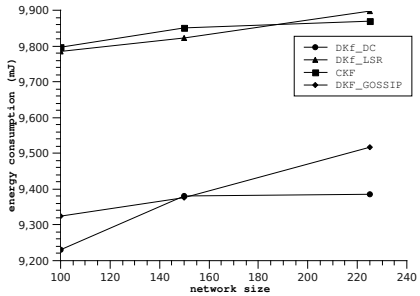


Fig. 6. Energy consumption of the network vs. Network density

energy consumption in DKF_DC is due to the fact that the dynamic clustering protocol limits the number of nodes involved in the tracking task.

We also evaluate the network energy consumption by varying the network size within $\{225, 150, 100\}$ and setting the deployment area surface to $200 \times 200m^2$. The sampling period is set to $1s$. We obtain the results in figure 6, in which we observe that the dense nature of a WSN influences the network energy consumption. In CKF and DKF_LSR methods, the number of tasking nodes is high which induces an excessive energy consumption because each node executes a sensing operation every tracking step. Sensing and communication energy consumption is high than computation consumption that is what explains why DKF_DC outperforms these two methods.

C. Estimation Quality

The estimation quality of CKF, DKF_DC and DKF_LSR schemes are evaluated for different sampling periods (see Figures 7, 8, 9).

As we can see in the three figures, the estimation quality of our method is less than those of CKF and DKF_LSR, and CKF outperforms all the other schemes in respect to the different sampling periods. In our method, the reduced set of participating nodes in the estimation process may decrease the total nodes' utility when less-appropriate nodes are chosen. Therefore, including all the network nodes in the estimation process and considering a uniform distributed noise model, this improves the estimation quality and convergence, because much data are fused despite the fact that they contribute or not in the estimation. Picks can be also observed on the graphs of

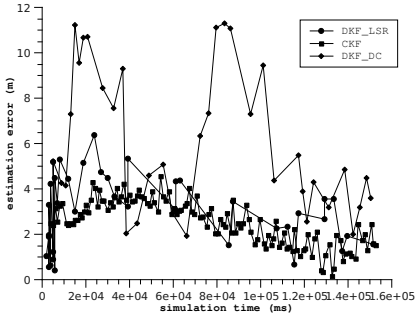


Fig. 7. Estimation quality for a $1s$ sampling period

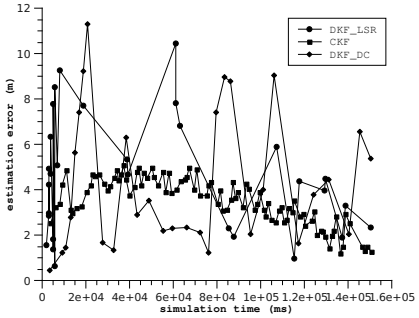


Fig. 8. Estimation quality for a $2s$ sampling period

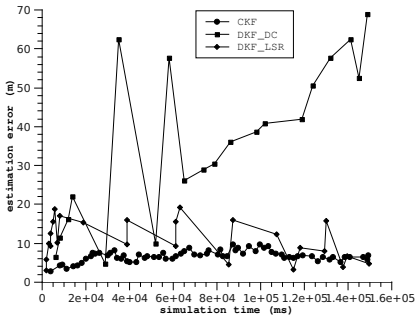


Fig. 9. Estimation quality for a $3s$ sampling period

DKF_DC due to the cluster reconfiguration process. Figure 9 shows that with a large sampling period, our method presents poor estimation quality because of the latency generated by the clustering protocol. This can be considered as a drawback of DKF_DC.

Finally, the estimation quality of CKF, DKF_LSR and DKF_DC schemes when varying the target speed within $\{1m/s, 2m/s, 4m/s\}$ is presented in Figures: 10, 11, 13, respectively.

In figure 10, we can see that the estimation error of CKF decreases for different target speeds. Indeed, we realize that the Kalman filter presents some picks in the beginning of the estimation process, but they disappear after that and the estimation error converges to zero due to the recursive nature of KF. Figure 11 shows that for targets with relatively low speeds, the estimation error of DKF_DC converges to zero. However, when the target speeds up, it overcomes the cluster

 ISBN: 978-1-61208-166-3

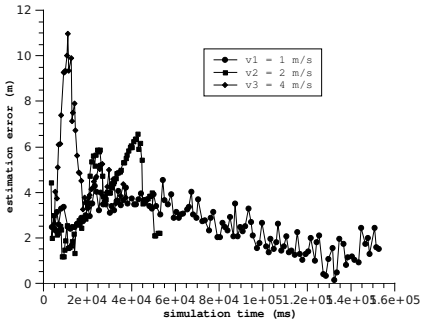


Fig. 10. CKF estimation quality vs. Target velocity

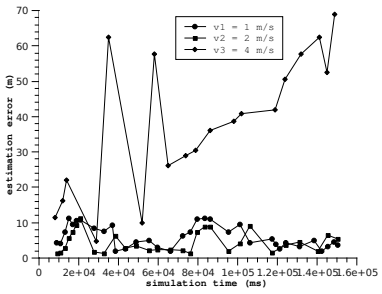


Fig. 11. DKF_DC estimation quality vs. Target velocity

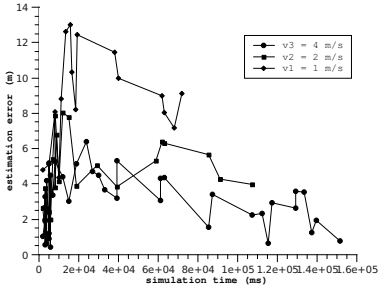


Fig. 12. DKF_LSR estimation quality vs. Target velocity

reconfiguration process. Thus, we observe a degeneration of the estimation quality for targets with velocity $v_3 = 4m/s$. A recovery process should be setup here to deal with this problem. The estimation error of DKF_LSR is presented in figure 13. As we can see, this method converges also for different target speeds but in a slow rate compared with CKF, because the state vector and the covariance matrix are exchanged between large and large sets of nodes when the simulation progresses.

We show in figure 13 the convergence speed of the different simulated methods. We see that the estimation error of all the methods converges to zero but with different rates. CKF converges with high speed than the other methods.

VI. Conclusion and Future Work

The energy problem remains a key issue for emerging WSN applications such as target tracking. Our distributed Kalman filtering method coupled with dynamic clustering protocol

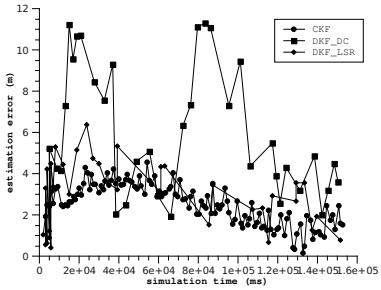


Fig. 13. Estimation quality of the different schemes

(DKF_DC) helped at reducing the network energy consumption in WSN with limited sensing range. We prevented nodes from waking up periodically and limited the selection process within the area close to the target which we organize as a cluster. We manage then this cluster to follow-up the target trajectory. We improved the energy efficiency of the network but the estimation quality has slightly degraded. Including the sensing capabilities of nodes into the selection process and integrating a recovery process when losing targets with complex state model appear as the most promising track for future work.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] G. Anastasi, M. Conti, M. D. Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey," *Ad Hoc Networks*, vol. 7, no. 3, pp. 537–568, 2009.

[3] R. Olfati-Saber, "Distributed kalman filter with embedded consensus filters," in *Proceedings of the 44th IEEE Conference on Decision and Control, and the European Control Conference*. IEEE Computer Society, Dec. 2005, pp. 8179–8184.

[4] D. Spanos, R. Olfati-Saber, and R. Murray, "Dynamic consensus on mobile networks," in *The 16th IFAC World Congress, Prague, Czech*, 2005.

[5] R. Olfati-Saber, J. Fax, and R. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, 2007.

[6] U. A. Khan and J. M. F. Moura, "Distributed kalman filters in sensor networks: Bipartite fusion graph," *SSP*, 2007.

[7] S. Kar, "Large scale networked dynamical systems: Distributed inference," Ph.D. dissertation, Carnegie Mellon University Pittsburgh, PA, May 2010.

[8] R. Olfati-Saber and N. F. Sandell, "Distributed tracking in sensor networks with limited sensing range," in *American Control Conference, 2008*. IEEE, Jun. 2008, pp. 3157–3162.

[9] A. Ribeiro, G. B. Giannakis, and S. I. Roumeliotis, "Soi-kf: Distributed kalman filtering with low-cost communications using the sign of innovations," *IEEE Transactions on Signal processing*, vol. 54, no. 12, pp. 4782–4795, Dec. 2006.

[10] H. Medeiros, J. Park, and A. C. Kak, "Distributed object tracking using a cluster-based kalman filter in wireless camera networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 02, no. 04, pp. 448–463, Aug. 2008.

[11] P. Levis, N. Lee, M. Welsh, and D. Culler, "Tossim: accurate and scalable simulation of entire tinyos applications," in *Proceedings of the 1st international conference on Embedded networked sensor systems*. ACM, 2003, pp. 126–137.

[12] G. Welch and G. Bishop, "An introduction to the kalman filter," *University of North Carolina at Chapel Hill, Chapel Hill, NC*, 1995.

 ISBN: 978-1-61208-166-3

Wireless Ad hoc and Sensor Network Underground with Sensor Data in Real-Time

Emmanuel Odei-Lartey, Klaus Hartmann
Center for Sensor Systems, University of Siegen
Paul-Bonatz-Str. 9-11, 57068 Siegen, Germany
elartey@zess.uni-siegen.de, hartmann@zess.uni-siegen.de

***Abstract*— This paper describes an innovative approach using a wireless ad hoc and sensor network solution in a borehole telemetry system. This contribution is in line with the wireless network track of the conference with regards to channel modeling and characterization as well as wireless applications and services. The paper further validates the feasibility of achieving a reliable wireless communication network underground with real-time data acquisition with respect to the described borehole telemetry system.**

Keywords-Wireless communication; drilling; sensor node; tubes; underground

I. INTRODUCTION

The Intelligent Tube (ITUBE) Project, is an on-going project at the Center for Sensor Systems, University of Siegen. This is a borehole telemetry system where the objective is to obtain the latest information in real time on all relevant data during a drilling operation. This data is taken into account for faster complex decision-making processes, which affect the actual drilling (drilling, completion, intervention and process control). This is motivated by but not limited to the in situ soil mixing drilling process where quality and accurate vertical drilling is essential to save cost [8]. In connection with this soil mixing process, the pressure conditions at the nozzle exit and the temperature are of particular interest [7]. To ensure quality of work, pressure should be continuously monitored closely at the outlet to control the process, which is presently a challenge in the in situ soil mixing process [8]. During the drilling process, real-time information about the drill head progress is important, thus the need to cluster the essential sensors within the drill head to gather the relevant data to ensure the quality of the drilling process. For this to be achieved, a flexible, robust, fast and reliable communication structure needs to be put in place. Hence, in this paper, we analyze the feasibility of achieving such a reliable wireless communication underground for real-time data acquisition with regards to the borehole telemetry system.

Section II describes the proposed structure of the network nodes, as embedded in drill tubes, for communication. The succeeding section, Section III, explains the theoretical concept and the related work drawn from the works of [1][2] required to justify the feasibility of the approach. Section IV then shows MATlab simulations and analysis using the model equations described in the previous section. Finally, the last section, Section V, deals with open questions and future work.

II. PROPOSED NETWORK STRUCTURE

For data communication, as shown in Figure 1, the nodes are designed such that the radio transceivers are placed at the ends of each drill tube, therefore, enabling a closer proximity to each other (in this instance about 100mm to 300mm apart) within the ground, thereby, reducing the gap to be overcome by the signals. Within each tube, the end to end transceivers are connected to each other via a microcontroller and a power supply by cable to form a node as again shown in Figure 1. The microcontroller is programmed to enable for routing of data in the wireless ad hoc network setup. In accordance with the joining of the drill tubes into a strand during the drilling process, the individual wireless nodes will automatically form an ad hoc network strand irrespective of the order of the tubes. Sensor functionality is located in the drill head, which serves as a data source. The data collected in the drill-head sensor node is wirelessly sent to the next node located in the mechanically flanged pipe of the drill string. On the surface, the last node used in the drill string pipe connects with the base station communication interface outside of the drill string. The base station forms the interface to various system controls.

III. UNDERGROUND COMMUNICATION

This section focuses on the modeling and analysis of the underground communication to verify the feasibility of a reliable communication framework. For reliable communication between the nodes in the underground environment, the radio signals transmitted should be received independent of the prevailing conditions of the soil medium. This explains the close proximity of the transceiver modules to each other at adjoining ends of the tubes or pipes as described in the previous section.

A. Related Work

A modification of the Frii's Transmission Equation of the received signal strength, as described in [1], expressed in the logarithmic form is given as

$$P_r(dBm) = P_t(dBm) + G_r(dB) + G_t(dB) - L_0(dB) - L_m(dB) \quad (1)$$

where $P_r(dBm)$: power at receiver, $P_t(dBm)$: power at transmitter, $G_r(dB)$: receiver gain, $G_t(dB)$: transmitter gain, $L_0(dB)$: path loss in free space, $L_m(dB)$: path loss in soil medium.

 ISBN: 978-1-61208-166-3

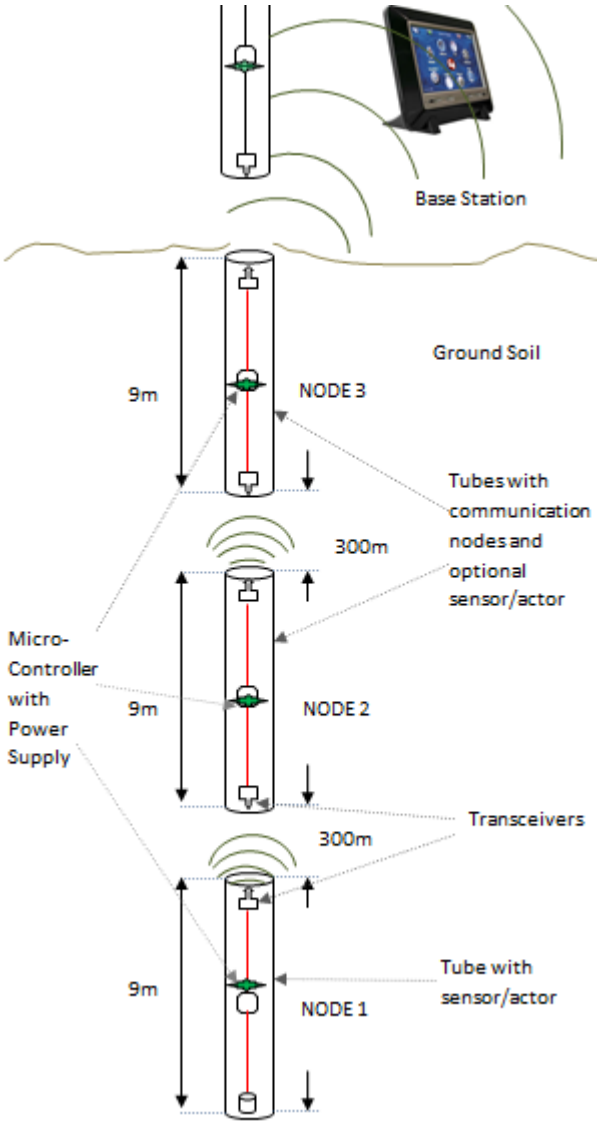


Figure 1. The schematic of the interconnecting drilling tubes with the integrated wireless ad hoc network. Each tube is a node, which consists of two transceivers, a micro-controller, and a power supply. The approximate distance between each tube is 300mm while each tube measures about 9m in length.

As observed in (1), this modified equation takes into account the path loss of the signal in the soil medium. The path loss is the reduction in power density (attenuation) of the radio signal as it propagates through a medium. Further deductions as described in [1], shows that the direct path loss considering both free space and the soil medium is given as

$$L_p = 6.4 + 20\log(d) + 20\log(\beta) + 8.69\alpha d, \quad (2)$$

$$L_p = L_0 + L_m . \quad (3)$$

where α and β represent the attenuation constant (1/m) and the phase shift constant (radian/m) respectively. These quantities depend on the dielectric permittivity of the medium through, which the signal passes as described also in [1]. It is represented as

$$\alpha = w\sqrt{\frac{\mu_o \epsilon_o \epsilon'}{2}\left[\sqrt{1+\left(\frac{\epsilon''}{\epsilon'}\right)^2}-1\right]}, \quad (4)$$

$$\beta = w\sqrt{\frac{\mu_o \epsilon_o \epsilon'}{2}\left[\sqrt{1+\left(\frac{\epsilon''}{\epsilon'}\right)^2}+1\right]}, \quad (5)$$

where ϵ' and ϵ'' represent the real and imaginary dielectric permittivity of the mixture of and water medium through, which signal transmission takes place. These quantities, according to Peplinski's principle [2], are represented as

$$\epsilon = \epsilon' + j\epsilon''$$

$$\epsilon' = 1.15\left[1 + \frac{\rho_b}{\rho_b}(\epsilon_s)^{\alpha'} + (m_v)^{\beta'}(\epsilon'_{fw})^{\alpha'} - (m_v)\right]^{\frac{1}{\alpha'}} - 0.68 , \quad (6)$$

$$\epsilon'' = \left[(m_v)^{\beta''}(\epsilon''_{fw})^{\alpha'}\right]^{\frac{1}{\alpha'}}. \quad (7)$$

where α' represents an empirically determined constant, β' and β'' are also empirically determined constants depending on soil types given as

$$\alpha' = 0.65,$$

$$\beta' = 1.2748 - 0.519S - 0.152C, \quad (8)$$

$$\beta'' = 1.33797 - 0.603S - 0.166C. \quad (9)$$

where ϵ'_{fw} and ϵ''_{fw} represents the relative real and imaginary dielectric constant of water respectively, which are also given as

$$\epsilon'_{fw} = \epsilon_{w\infty} + \frac{\epsilon_{w0} - \epsilon_{w\infty}}{1+(2\pi f \tau_w)^2}, \quad (10)$$

$$\epsilon''_{fw} = \frac{2\pi f \tau_w(\epsilon_{w0} - \epsilon_{w\infty})}{1+(2\pi f \tau_w)^2} + \frac{\sigma_{eff}(\rho_s - \rho_b)}{2\pi\epsilon_o f \rho_s m_v}, \quad (11)$$

$$\sigma_{eff} = 0.0467 + 0.2204\rho_b - 0.4111S + 0.6614C . \quad (12)$$

where S: mass fraction of sand, C: mass fraction of clay, μ_o: magnetic permeability of free space, ϵ_o: permittivity of free space, m_v: volumetric water content of the soil, ϵ'_{fw} and ϵ''_{fw}

the real and imaginary parts of the relative dielectric constant of water, ϵ_{w0}: static dielectric constant of water, $\epsilon_{w\infty}$: high-frequency limit of ϵ'_{fw} , σ_{eff} : effective conductivity of water, f: operating frequency, τ_w: relaxation time of water, ρ_s : specific density of the solid soil particles, ρ_b : bulk density

B. *Antenna Design*

As the signals move through the soil medium there is a decrease in wavelength as compared to transmission through air [6]. This suggests the antenna should be designed for a higher frequency other than the given free space frequency of the transceiver modules (868MHz) or should have a wide bandwidth. From the above results the range of the resulting frequencies in the ground soil could be deduced using the following relation as again described in [1]

$$\lambda_n = \frac{2\pi}{\beta}, \quad \beta = w\sqrt{\frac{\mu_o \epsilon_o \epsilon'}{2}\left[\sqrt{1+\left(\frac{\epsilon''}{\epsilon'}\right)^2}+1\right]}, \qquad (13)$$

$$f_n = \frac{c}{\lambda}, \qquad (14)$$

where β is the phase shift constant, λ_n is the new wavelength in the ground soil, f_n represents the corresponding frequency and c is the speed of light in free space as described by (13)(14). From computational results, for a typical configuration setting, the theoretical new frequency in the ground soil is found to range from 1.7GHz to 1.9GHz. An integrated chip or ceramic antenna designed for such high frequencies is most appropriate for such underground wireless communication.

IV. FEASIBILITY OF COMMUNICATION

The model equations as described in the previous section were coded and simulated using MATLab software.

A. *Matlab Simulations and Results*

From the model equations, (2)-(12), in Section III, it is observed that the path loss depends on the frequency, distance between the transceiver nodes, clay soil content, sand soil content and the volumetric water content of the soil [3]. In conformance to the ITUBE project, the frequency of the radio module is fixed at 868MHz with a fixed maximum distance of approximately 300mm between any two adjoining transceiver nodes where wireless communication takes place. Using the above model equations, the range for the direct path loss as well as the power received at the receiver node (Received Signal Strength) was simulated with varying values of the parameters stated (clay content, sand content and water content) to determine the feasibility of the underground communication network in different soil conditions. These parameters are used to simulate a wide range of possible constituents of the ground soil since there is no much control over such ground soil characteristics on the field where the drilling takes place. The best case scenario with a Volumetric Water Content (VWC) of 1% is observed and compared to a worse situation of a VWC of 80%. VWC here is defined as the ratio of water contained in the soil to the total volume of the soil. The effect of the different proportions of clay to sand content in the soil on the path loss and consequently the Received Signal Strength Indicator (RSSI) is observed. RSSI is the measurement of the power present in the received radio signal.

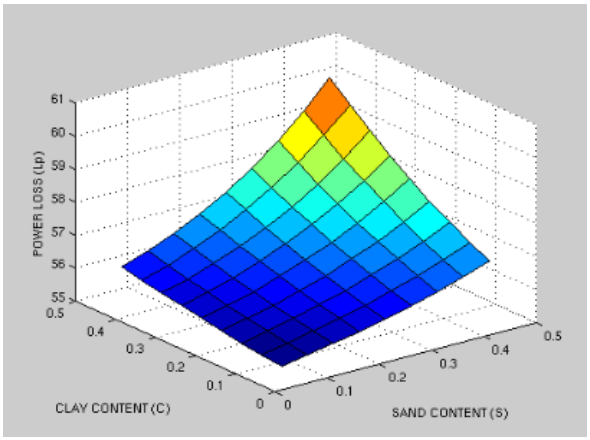


Figure 2. Path loss graph with volumetric water content (VWC) at 1% volume

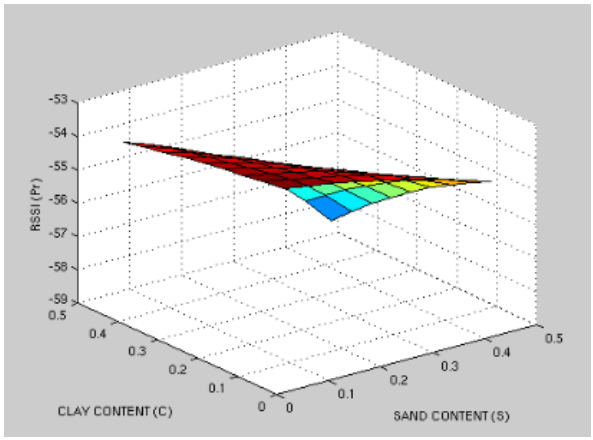


Figure 3. Received signal strength indicator graph with volumetric water content (VWC) at 1% volume

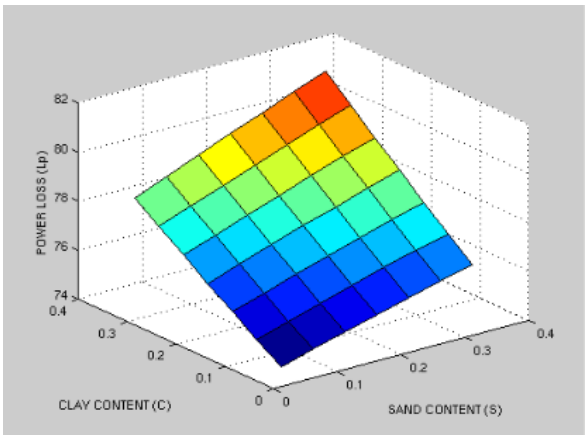


Figure 4. Power loss graph with volumetric water content (VWC) at 25% volume

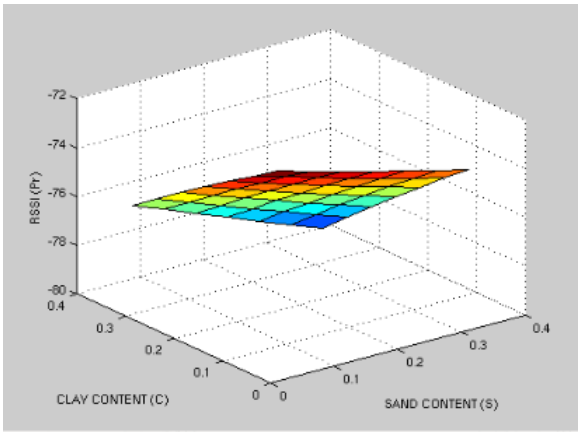


Figure 5. Received signal strength indicator graph with volumetric water content (VWC) at 25% volume

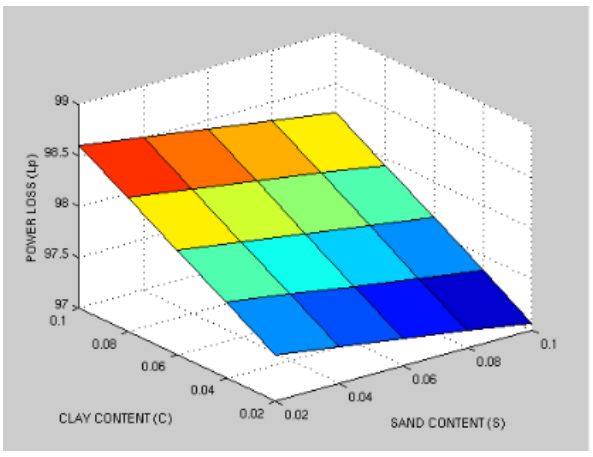


Figure 6. Power loss graph with volumetric water content (VWC) at 80% volume

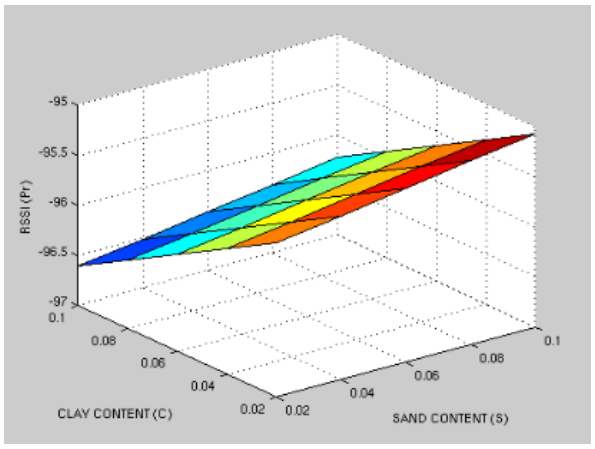


Figure 7. Received signal strength indicator graph with volumetric water content (VWC) at 80% volume

From the datasheet of the wireless transceiver module, AMB8420 [5], the minimum sensitivity of the receiver is -102dBm (-110dBm at 50Ω) and the output power of the transmitter is typically 2dBm (10dBm at 50Ω). From the results, as indicated in Figures 3, 5 and 7 above, the RSSI value in all cases falls within the RF sensitivity limit, thus indicating feasibility of the application given such conditions as described by the graphs. From the graphs, it can also be seen that the RSSI value at the receiver tends to decrease with increase in sand and clay content of the soil. This is more significant with the increase in the VWC of the soil. In Figure 2, the VWC is at 1%. This value is increased to 25%, as shown in Figure 4, and finally, to 80%, also as shown in Figure 6. With this trend, a steep increase in the path loss is observed. Consequently, the RSSI value is observed to fall from about -54.5dBm with 1% VWC to about -95.1dBm with 80% VWC, as shown in Figures 3 and 7, which does not exceed the threshold of -103dbm (the minimum receiver sensitivity). This observation establishes the feasibility of a reliable communication within the underground soil at the given fixed distance of 300mm and frequency of 868MHz.

V. CONCLUSION AND FUTURE WORK

From the analysis in the previous section, it is observed that for a frequency of 868MHz and a proximity gap of 300mm between transceiver modules, reliable communication underground is highly feasible under a wide range of possible soil conditions. However, on the work field, certain properties of the ground soil such as the chemical or salt content also have a significant effect on the dielectric characteristics of the soil [4]. Salty ground soil conditions tend to increase the path losses; therefore, decreasing the power at the receiver node (RSSI value) to a great extent [4]. Future work will include the possibility of transmission power control depending on the prevailing conditions of the soil as well as using cognitive radio techniques to enable automatic switching of transmission frequency to accommodate conditions in the ground soil.

 ISBN: 978-1-61208-166-3

REFERENCES

[1] L. Li, M. C. Vuran, and I. F. Akyildiz, "Characteristics of Underground Channel for Wireless Underground Sensor Networks," Med-Hoc-Net '07, Corfu, Greece, pp. 92-99, June 13-15.

[2] N. R. Peplinski, F. T. Ulaby, and M. C. Dobson, "Dielectric Properties of Soils in the 0.3-1.3-GHz Range", IEEE Transactions on Geoscience and Remote Sensing, Vol. 33, No. 3, pp. 803-807, May 1995

[3] I. F. Akyildiz, Z. Sun, and M. C. Vuran, "Signal propagation techniques for wireless underground communication networks," Elsevier Journal, Physical Communication, pp. 167-183, 2009.

[4] R. J. Edwards, "RF Skin Depth in the Ground vs. Frequency for Given Soil Characteristics," Ground Systems, Tigertek Inc, 2010, http://www.smeter.net/grounds/rf-skin-depth-in-soil.php [Last Accessed: 18 July 2011].

[5] "AMB8420 Compact Low-Cost Radio Module 868MHz ISM Band," datasheet, Amber Wireless, 2009.

[6] A. R. Silva and Mehmet C. Vuran, "Communication with Aboveground Devices in Wireless Underground Sensor Networks: An Empirical Study," IEEE Communications Society, IEEE ICC, pp. 1-6, 2010.

[7] S. Kazemian and B. K. Haut, "Assessment of Stabilization Methods for Soft Soils by Admixtures," International Conference on Science and Social Research, Kuala Lumpur, Malaysia, pp. 118-121, 2010.

[8] R. D. Andrus and R M. Chung, "Ground Improvement Techniques for Liquefaction Remediation Near Existing Lifelines," U.S. Department of Commerce, National Institute of Standards and Technology, pp. 1-85, Ocotober 2005.

 ISBN: 978-1-61208-166-3

On Design of Mobile Agent Routing Algorithm for Information Gain Maximization in Wireless Sensor Networks

Maryam Alipour
Electrical and Computer Engineering Department
Qazvin Islamic Azad University
Qazvin, Iran
malipour@qiau.ac.ir

Karim Faez
Electrical Engineering Department
Amirkabir University of Technology
Tehran, Iran
kfaez@aut.ac.ir

***Abstract*— Mobile agent routing for data aggregation in wireless sensor networks may considerably decrease the data traffic among sensor nodes. Finding an appropriate route which leads to the highest aggregation ratio is a major challenge in these networks. Complexities on the design of a mobile agent routing algorithm are related to the precise selection of source nodes and their visiting sequence during mobile agent migration. In this paper, the improvement of mobile agent routing for the dynamic model designed by Xu and Qi is proposed. Xu-Qi's model is developed to solve the problem of target tracking application using the mobile agent migration. The pattern of source nodes selection is based on the cost function, the trade-off between increasing the information gain and decreasing the energy consumption. In this paper, a method is proposed to expand the cost function; our method improves the impact of both information gain and power efficiency in source nodes selection; also, it increases the accuracy of aggregated data. The scope of wireless sensor networks covered by this paper is suitable for many applications. Simulation results in NS2 show that for networks with different number of nodes, the proposed method has less delay and energy consumption compared to Xu-Qi's model.**

Keywords- wireless sensor networks; data aggregation; mobile agent; dynamic routing; information gain

I. INTRODUCTION

A WSN *(Wireless Sensor Network)* typically consists of hundreds or even thousands of sensor nodes scattered in a geographical region to perform sensing, processing, and communication tasks. The sensor nodes have limited resources, such as battery power, processing capacity, memory, and network bandwidth. The data collected by sensor nodes are transmitted to the unlimited resource PE *(processing element)* or sink, where a higher degree of processing is performed. In the dense networks, sensor nodes are geographically close to each other. Therefore, nearby nodes may sense the environmental data with negligible differences. If all sensed data are transmitted to the PE, the network bandwidth utilization will be unnecessarily increased. In order to eliminate the redundant data, an aggregation scheme is used [1]. Data aggregation scheme can be classified in two categories: CS *(Client-Server)* and MA *(Mobile-Agent)* based [2]. Data aggregation schemes can be integrated with routing concepts. The *data-centric routing* aims to find the route with the highest ratio of data aggregation.

In traditional CS scheme, all data packets are passed to the PE for further processing. The packets enter the PE arrival queue and wait for their turn to be processed. Due to the asynchronous data processing and congestion taken place on arrival queue, delay and packet loss rate may be increased. This scheme is not scalable for large-scale wireless sensor networks, where node density is high. Therefore, as increasing nodes number in the network, energy and bandwidth consumption will be increased.

In the new MA scheme, a different processing model is employed. MA is a piece of software code that is initially dispatched by the PE and subsequently moves among source nodes to collect data. The sensor nodes that will be visited along the route by an MA are known as the source nodes. Structure of the MA consists of four main components: The *identification*, which identifies an MA specially; *processing code*, which is used to process sensed data locally; *route*, which is a set of source nodes and their visiting sequence during mobile agent migration; *data space*, which carries aggregated results. When the MA arrives at the source node: First, it takes a local processing on the sensed data; then, it aggregates the data from source nodes that have already been visited; finally, it stores aggregation results in its own data space. After the MA leaves the current source node, it migrates to another one. Eventually, MA will return to the PE. Transmitting collected data through an MA packet to a PE may consume less energy and bandwidth in WSNs [3].

The route design problem means selecting a sequence of source nodes which will be visited by MA. The node selection process should lead to increase in the energy-time efficiency and data aggregation ratio. The routing problem can be divided into two categories: the *static*, and the *dynamic* routing [4]. In the static scheme, the entire topology information is needed. PE uses it to construct an efficient route for MA migration. The main drawback of this scheme is that it is not scalable. In the dynamic scheme, a node is selected as the next source node locally; The MA based route is specified autonomously and through migration from one node to another one. Therefore, MA can dynamically adapt itself to any variable environmental conditions.

The rest of this paper is organized as follows: In Section 2, the related work on mobile agent routing for data aggregation is presented. In Section 3, the assumptions and problem statement are described. The problem solution approach is explained in Section 4, including the trade-offs in the route selection. In Section 5, the details of proposed algorithm are discussed. The high performance of our

 ISBN: 978-1-61208-166-3

proposed method is approved by simulation results in Section 6. The paper is concluded in Section 7.

II. RELATED WORK

In this section, we intend to review some algorithms which have been proposed to find appropriate MA routes in WSNs.

In [5], authors proposed two simple heuristic algorithms, LCF *(Local Closest First)* and GCF *(Global Closest First)*, to design a route for MA migration. In LCF, the node with the shortest distance to the current source is selected as the next node, while in GCF, the shortest distance to PE is considered. These algorithms are static and centralized. Since the entire network topology information is needed, these algorithms are not scalable. Also, the route selection is only depended on the spatial distance of source nodes, but not on energy consumption.

Authors of [6] proposed two static routing algorithms, IEMF *(Itinerary Energy Minimum for First-source-selection)* and IEMA *(Itinerary Energy Minimum Algorithm)*. The list of *N* source nodes which will be visited by the MA has been specified in PE. Using the round robin method in IEMF, each node is temporarily replaced as the first source node, and then the LCF algorithm will be applied to route among the other *N-1* source nodes. Therefore, *N* routes are designated among which only one route with minimum communication cost will be selected. Communication cost is formulated by considering energy consumption and data aggregation models. Consequently, the performance of the LCF algorithm is improved by taking into account the energy constraint in MA routing. The IEMA is the iterative version of the IEMF, where the IEMF is used to determine the next source node in each hop. Thus, IEMA selects the order of the remaining source nodes besides the first one. Although both algorithms find an energy efficient route for MA, these are still based on the non scalable LCF algorithm.

In [7], Y. Xu and H. Qi proposed an algorithm for the dynamic MA migration in the target tracking application. In this algorithm, an MA is dispatched in the network with Gaussian distributed sensor nodes to follow a moving target at different times. MA migrates to nodes which can obtain more accurate information about the target location by consuming the lower migration energy. Hence, a cost function is defined to decide about selecting the source nodes. Cost function is a trade-off between the energy expenditure on MA migration and benefit of high information gain. The neighbors of current source are known as the next node candidates, among which one node with minimum cost value is selected as the next source. Information gain model is used to compare the data accuracy collected by nodes. By collecting the more accurate data about the target, the node will have a greater probability for selection as the next source. In order to gain the maximum information about the target; the MA should migrate to the nodes with higher signal strength. The closer a sensor node is to the target, the higher signal energy and information gain would be achieved. Here, a zero mean Gaussian function is used to model the relationship between the information gain of candidate node *k* at time *t*, $I_k(t)$, and target distance as [7]:

$$I_k(t) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{\left\|\widehat{x(t)} - x_k\right\|^2}{2\sigma^2}}, \quad (1)$$

where σ is the standard deviation, $\left\|\widehat{x(t)} - x_k\right\|$ is the distance of the node *k* from the target at time *t*, x_k is the location of node *k*, and $\widehat{x(t)}$ is the target location at time *t* which can be estimated by trilateration localization algorithm.

In [8], the heuristic TBID *(Tree-Based Itinerary Design)* algorithm is presented to find near-optimal routes for multiple MAs. The algorithm is executed statically at the PE. The area around the PE is divided into concentric zones to construct the MA routes from the inner zones to the outer ones. The number of routes is assigned to MAs is equal to the maximum number of first-zone nodes. At each round of algorithm runs, the lowest costly node will be attached to a tree. The objective is to minimize the total energy cost of routes. Although this algorithm is designed for static routing, the use of proper data structures can adapt it to the dynamic network conditions.

In this paper, a data-centric routing algorithm based on MA is proposed. The algorithm is an improvement of MA routing for the dynamic model designed by Xu and Qi in [7]. Xu-Qi's model is developed for target tracking application in WSNs. The source nodes are determined by the minimum value of the cost function, the trade-off between the information gain and energy consumption. At each hop along the route, selection of the next source node is performed among neighbors of current source. Hence, two consecutive source nodes may gain the similar information. The improvements of our algorithm for route selection include:

- Our algorithm is not limited to special applications.
- The possibility of visiting the more selective nodes is decreased due to their lower remaining energy.
- The algorithm seeks the nodes which consume the lower power for transmitting an MA to the next hop.
- If none of the current node neighbors obtain the higher information gain, then MA can migrate to the nearest 2^n-hop nodes *(n≥1)* by consuming the minimum transmission energy.
- The higher aggregation ratio can be achieved by traversing the smaller number of source nodes.
- Our algorithm has less end-to-end delay and energy consumption.

Finally, we evaluate the solution performance in terms of both energy and delay to verify the practicality of our algorithm.

III. ASSUMPTIONS AND PROBLEM STATEMENT

In this section, we will define the purpose of our research along with main assumptions in this paper.

A. Network Model

A wireless sensor network is modeled as a graph *G(V, E)*, where *V* is the set of static sensor nodes, $V=\{v_1, v_2, \ldots, v_n\}$, and *E* is the set of bidirectional links e_{ij} between nodes, $E = \{e_{ij} = \{v_i, v_j\} | v_i, v_j \in V, i \neq j\}$. The network consists of *N*

sensor nodes that are scattered in a rectangular field A with Gaussian distribution. The PE is denoted by v_0, considered as both the start and end points of MA migration route. It is supposed that except for the PE, all sensor nodes are resource-constrained especially in terms of energy and bandwidth. The sensor nodes are aware of their remaining energy and geographical location in the form of (x, y) coordinates. The sensor nodes have maximum transmission range R, where they can recognize their neighbor nodes in every time intervals. Each sensor node broadcasts a list including the amount of remaining energy, the geographical location, and the number of times which it was visited by MA. It is supposed that the current source node being met by MA is denoted by v_i. The candidates of next source node are shown with v_j, as one of them will be selected as the next hop of MA. The data aggregation operation is performed by MA during moving among the source nodes. The MA packet only passes through the intermediate nodes between current and next source nodes. Mobile agent migration in a wireless sensor network is illustrated in Fig. 1.

B. Problem Statement

In this paper, we study the MA as a processing component which aggregates the collected data by the source nodes in the WSN. The scope of the network is not limited to special applications. The MA is dispatched by the PE to aggregate the data sensed by source nodes during migrating from one node to another. After completing the mission, it returns to the PE.

The problem is to design a dynamic and informative route for MA migration by considering the following parameters:

- Increasing the network lifetime by taking into account of the remaining energy level of each node as well as the required power for transmitting an MA.
- Improving the accuracy of aggregated data by selecting the source nodes with maximum information gain.
- Decreasing the end-to-end delay of MA migration when it is dispatched until it is returned.

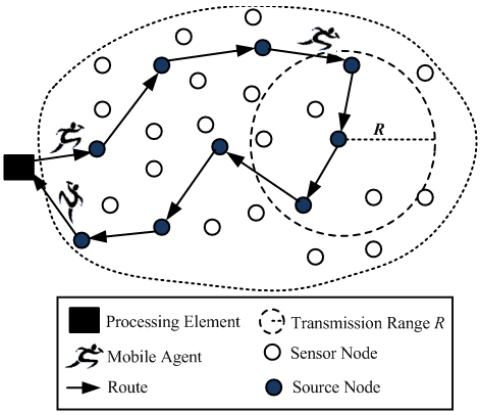


Figure 1. The mobile agent migration in the wireless sensor network to aggregate the sensed data of source nodes along the route.

IV. Solution Approach

To design an efficient route for MA migration in the network, it is important to select the source nodes which have minimum migration cost. To decide whether a node could be chosen as the next source, a cost function is defined. This function consists of the following components.

A. Information Gain, $I_j(x, y)$

It is supposed that the sensor nodes are scattered by Gaussian distribution in the field A. Once a source node v_i senses data, all its nearby neighbors may collect the same data with small differences. In result, instead of migrating to the adjacent nodes, MA could migrate to farther nodes to achieve higher degree of information gain. Therefore, the information gain is directly related to the nodes distance. In order to demonstrate the relationship between the information gain and the nodes distance, the inverse Gaussian function in two-dimension would be used as:

$$I_j(x, y) = \left(\sigma^2\sqrt{2\pi}\right)e^{\left(\frac{d_{ij}^2}{2\sigma^2}\right)}, \quad (2)$$

where σ is the standard deviation and the value of mean is selected as zero, d_{ij} is the distance between nodes v_i and v_j which is calculated as:

$$d_{ij} = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2}, \quad (3)$$

where $\left(x_i, y_i\right)$ and $\left(x_j, y_j\right)$ are the coordinates of nodes v_i and v_j in the network.

B. Migration Energy, E_{ij}

The energy cost for sending an MA from node v_i to v_j equals to sum of the transmitting energy e_{tx}^{ij}, the receiving energy e_{rx}^{ij}, and the energy consumption in their intermediate nodes along the route. Also, it is supposed that the needed energy for the data processing is the same for each node in the network.

The amount of energy for transmitting and receiving an MA is measured as [6]:

$$e_{tx}^{ij} = c_{tx} \times S_{tx} + O_{tx}, \quad (4)$$

$$e_{rx}^{ij} = c_{rx} \times S_{rx} + O_{rx}, \quad (5)$$

where c_{tx} and c_{rx} are the energy consumption per bit for both transmitting and receiving an MA packet, S_{tx} and S_{rx} are the size of MA packet which is transmitted and received respectively, O_{tx} and O_{rx} are the constant components of the channel usage overhead.

The intermediate nodes between the two source nodes can only forward the incoming MA packet. The average number of intermediate nodes which are located between the nodes v_i and v_j along the route is calculated as $\left\lceil \frac{d_{ij}}{R} \right\rceil$. Therefore, the energy spent by each intermediate node in

transmitting and receiving of an MA packet is equal to e_{tx}^{ij} and e_{rx}^{ij}, respectively [6]. In result, the forwarding energy consumed by all these nodes will be calculated by $\left\lceil \frac{d_{ij}}{R} \right\rceil \times \left(e_{tx}^{ij} + e_{rx}^{ij}\right)$.

The total energy for sending an MA from node v_i to v_j is measured as:

$$E_{ij} = \left(e_{tx}^{ij} + e_{rx}^{ij}\right) \times \left(1 + \left\lceil \frac{d_{ij}}{R} \right\rceil\right) \quad (6)$$

where E_{ij} is the sum of the transmitting energy of node v_i, the receiving energy of node v_j, and the energy consumption of their intermediate nodes.

C. Remaining Energy, e_j

A candidate node v_j will be designated as the next source, if its remaining energy is higher than the other nodes. Due to the prolonging network lifetime, a candidate node with the lower energy level would not be selected.

D. Transmission Power, P_j

As pointed out in (2), a candidate node v_j which is farther from the current source may gain the more precise information. In contrast, a farther node may entail more power consumption to send out an MA. Hence, a trade-off between the information gain and the transmission power is defined. We use the number of neighbors around a candidate node v_j as an approximation of its transmission power. Once a candidate node with the more neighbors is selected as the next source, it usually can consume less transmission power during its next hop. The transmission power P_j is inversely related to the number of v_j's neighbors, N_{neigh}^{j}, shown as $P_j \approx \frac{1}{N_{neigh}^{j}}$.

E. Migration Cost, C_{ij}

Decision of selecting the best candidate node as the next hop is made by the cost function, C_{ij}. Cost function C_{ij} indicates the migration cost spent to transfer an MA from current node v_i to candidate node v_j. The cost function is the trade-off between increasing the benefits and decreasing the losses as follows. Cost function tries to increase the information gain and network lifetime as well as to decrease the energy consumption on MA migration. Therefore, it increases the probability of selecting the lowest-cost node among the candidate nodes. The cost function C_{ij} for transferring an MA from v_i to v_j can be defined as:

$$C_{ij} = \alpha\left(1 - \frac{I_j(x,y)}{I_{max}}\right) + \beta(N_{visit} + 1)\left(1 - \frac{e_j}{e_{max}}\right) + \gamma\frac{E_{ij}}{E_{max}} + (1-\alpha)\frac{P_j}{P_{max}} \quad (7)$$

$$0 \le \alpha, \beta, \gamma \le 1, \quad N_{visit} \ge 0,$$

where $I_j(x, y)$ is the information gain of a candidate node v_j, I_{max} is the maximum information gain of nodes, E_{ij} is the energy consumption for transferring an MA from node v_i to v_j, E_{max} is the maximum transmission energy for sending MA from one node to another, e_j is the remaining energy of node v_j, e_{max} is the same initial energy of nodes, and N_{visit} is the number of times that node v_j has already been visited by MA; Numerous selection of node v_j as the next source will cause its more energy loss and reduction of the network lifetime. Therefore, the number of times that a node can be visited by an MA is limited. α, β and γ are the weighed factors, P_j is the power consumed to transmit an MA from node v_j to its next hop, and P_{max} is the maximum power to transmit an MA in the network; P_{max} is inversely proportional to the maximum number of a node neighbors, $P_{max} \approx \frac{1}{N_{max}}$, where N_{max} is calculated as [9]:

$$N_{max} = (N-1) \times \frac{\pi R^2}{A}, \quad (8)$$

where N is the number of scattered sensor nodes in the network, R is the maximum transmission range of nodes, and A is the area of network. The cost consumption on the MA migration is decreased by increasing the number of node neighbors. Thus, the possibility of selecting that node as the next source would be increased.

V. Algorithm Description

Data will be aggregated in the selected source nodes. Other intermediate nodes will forward the MA packet. When a node is selected as the next source, the value of its information gain will be stored in MA packet as the latest.

Once MA is dispatched from the PE, it migrates to the nearest node with the minimum cost measured according to the (7). After receiving the MA by the first source node, data will be aggregated. Then, MA tries to find the next source: First, the entire one-hop neighbors will be checked according to the (7) to designate the least costly candidate node; second, the difference of information gain in this candidate node with the current value is calculated. If it is higher than the specific threshold, the MA will be migrated to that node and aggregate data. Otherwise, the MA will migrate to the nearest node two-hop away from the current node for which data is aggregated. Since, the MA has no knowledge of network topology; it first migrates to the nearest one-hop neighbor that hasn't been selected; thereafter, it moves from there to the next closest neighbor. After the MA arrived in the node two-hop away, the threshold condition of the information gain is checked. If condition does not satisfy, the MA will be moved to the nearest node four-hop away of the current node. The process of searching will be continued in all 2^n-hops nodes *(n≥1)*, until a most informative node is selected as the next source. Once, the informative node is found, the MA starts again to aggregate and find the next node in all one-hop neighbors. Finally, MA will return to the PE at the end of the migration. If MA cannot find any next node, it will return back to the PE. Note that in all the above

 ISBN: 978-1-61208-166-3

steps, the next node is selected from the non common neighbors of current and previous nodes. The proposed scheme has been suggested for selecting the next node with the highest information gain and the lowest transmission power. A pseudocode description of our scheme is given in Fig. 2.

VI. SIMULATION RESULTS AND DISCUSSION

This section represents the simulation results on the proposed scheme by using NS-2 *(Network Simulator)* [10] as a simulator. The simulation parameters are summarized in Table 1. We consider all types of energy consumptions for both computational and communication costs in our simulations. In simulation results, each data point represents an average of 40 simulation trials. The results include 95% confidence interval for each data point. We first evaluate the impact of using the different values for factor-α on the performance metrics of our scheme. According to (7), α is the weighted factor of information gain with the value ranging from 0 to 1. The evaluated metrics are given below:

- Aggregation Precision Ratio: refers to the precision of aggregated data by MA. If the MA visits all of the nodes in the network, the precision will be one.
- Average End-to-End Delay: refers to the time interval between transferring MA from processing element and its recurrence to this point.

Fig. 3 illustrates the impact of the factor-α on the aggregation precision ratio in our scheme. There is a direct relationship between the information gain and the factor-α. Therefore, increasing the value of factor-α directly enhances the information gain effectiveness on the cost function (7). In result, the data aggregation is performed with more precision.

Fig. 4 shows the average end-to-end delay versus the values of factor-α. Here, are two related points: First, the more information is gained by increasing the factor-α (see Fig. 3); second, the more information is gained in farther nodes of current source in (1). Given these two points, the MA migrates to farther source nodes by increasing the value of factor-α. Therefore, the end-to-end delay will be increased.

We next compare our scheme with Xu-Qi's model, when the number of nodes varies from 100 to 400. The comparison is in terms of average remaining energy and end-to-end delay. The average remaining energy refers to the energy consumption ratio of the nodes at the end of the simulation process after several rounds of MA migrations in the network.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Terrain Area	2000 m×2000 m
Number of nodes	100 – 400
Transmission Range	115 m
MAC	IEEE 802.11
Simulation time	600 S

Fig. 5 compares the percentage of average remaining energy in our scheme with Xu-Qi's model. Our scheme selects the nodes which consume less power for transmitting the MA along the route; it balances the energy consumption among multi-hop source nodes. Also, the required accuracy of the data aggregation is obtained by visiting the fewer number of source nodes. Hence, our scheme can save up to 52% energy compared to the work in [7].

Fig. 6 shows the average end-to-end delay of MA migration in our scheme comparing with the existing one. Increasing the number of nodes in the network, the end-to-end delay will be increased. However, our scheme has lower delay than the existing model. The reason is that our scheme can find the most informative route by traversing the less number of source nodes; thus, MA takes less time to return to PE. Our scheme can reduce the average end-to-end delay by 13%.

The simulation results verify the practicality of our algorithm. The results show that our algorithm improves the Xu-Qi's model in terms of aggregation precision, energy consumption and end-to-end delay.

```
In PE (v_0) :
  find first source node according to (7)
  set last gain to the current gain
  can_fusion =1; hop_count =1; hop_jump =1;
In Sensor Node (v_i, i ≠ 0) :
  if can_fusion = 1 then {
    find next node according to (7)
    diff = current gain – last gain;
    if diff ≥ threshold then {
      select this node as next source
      set last gain to the current gain
      can_fusion =1; hop_count =1; hop_jump =1;
    }
    else {
      find the nearest neighbor that hasn't been selected
      can_fusion =0; hop_count = (hop_count)×2;
      hop_jump = hop_count;
    }
  }
  else
   if can_fusion=0 then  {
    hop_jump =(hop_jump) – 1
    if hop_jump == 0 then {
       diff = current gain – last gain;
       if diff ≥ threshold then {
          select this node as next source
          set last gain to the current gain
          can_fusion = 1; hop_count = 1;
          hop_jump = hop_count;
        }
       else {
          find the nearest neighbor that hasn't been selected
          can_fusion =0, hop_count = (hop_count)×2
          hop_jump = hop_count;
        }
    }
    else
      find the nearest neighbor that hasn't been selected
   }
```

Figure 2. The pseudocode of mobile agent migration process.

VII. Conclusion And Future Work

In this paper, we proposed a dynamic mobile agent routing algorithm in wireless sensor networks. Our proposed algorithm is an improvement of the dynamic model designed by Xu and Qi. The Xu-Qi's model is developed for target tracking application, but our scheme is not limited to special ones. In Xu-Qi's model, the node selection process is determined by the minimum value of cost function. The cost function is the trade-off between the information gain and the energy consumption. We improved the cost function so that, the highest information gain is achieved along the route by consuming the minimum energy. Therefore, our algorithm can increase the accuracy of the aggregated data. We verify the practicality of our algorithm using simulations and compare its performance to Xu-Qi's model. The simulation results show that our proposed algorithm outperforms the existing model in terms of energy and end-to-end delay. Future work includes extending this work to support multi-cooperative mobile agent to achieve more precision and less delay. Also, we would like to extend the proposed scheme for selecting a source node in the hostile environment by considering the reliability and security factors in the cost function.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Computer Networks, Vol. 38, pp. 393–422, 2002.

[2] M. Chen, T. Kwon, Y. Yuan, and V.C.M. Leung, "Mobile agent based wireless sensor networks," Journal of computers, Vol. 1, No. 1, pp. 14-21, April 2006.

[3] H. Qi, Y. Xu, and X. Wang, "Mobile-agent-based collaborative signal and information processing in sensor networks," in Proceeding of the IEEE, Vol. 91, No. 8, pp. 1172-1183, August 2003.

[4] P.K. Biswas, H. Qi, Y. Xu, " Mobile-agent-based collaborative sensor fusion," Information Fusion Journal, Vol. 9 ,No. 3, pp. 399 – 411, 2008.

[5] H. Qi and F. Wang, "Optimal itinerary analysis for mobile agents in ad hoc wireless sensor networks," in Proceeding of the IEEE ICC'01, Helsinki, Finland, June 2001.

[6] M. Chen, V. Leung, S. Mao, T. Kwon, and M. Li, "Energy-efficient itinerary planning for mobile agents in wireless sensor networks," in Proceeding of the IEEE ICC'09, Dresden, Germany, pp. 14-18, 2009.

[7] Y. Xu and H. Qi, "Mobile agent migration modeling and design for target tracking in wireless sensor networks," Ad Hoc networks Journal, Vol. 6, No. 1, pp. 1–16, 2008.

[8] C. Konstantopoulos, A. Mpitziopoulos, D. Gavalas, and G. Pantziou, "Effective determination of mobile agent itineraries for data aggregation on sensor networks," IEEE Transactions on Knowledge and Data Engineering, vol. 22, no. 12, pp. 1679–1693, 2010.

[9] J. C. Hou, N. Li, I. Stojmenovic, Sensor networks: algorithms and architectures. John Wiley & Sons, chapter 10, pp. 313-317,2005.

[10] Network simulator ns version 2. http://isi.edu/nsnam/ns/

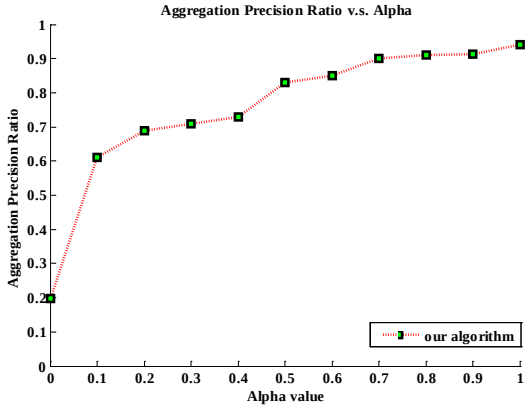


Figure 3. Aggregation precision ratio, when the factor-α varies from 0 to 1.

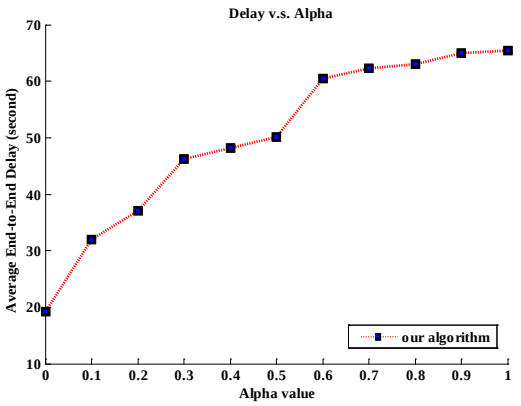


Figure 4. Average end-to-end delay, when the factor-α varies from 0 to 1.

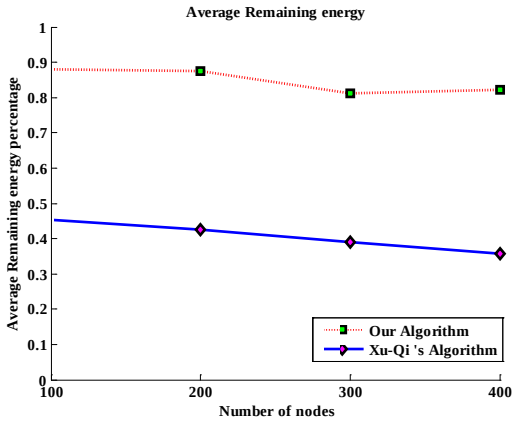


Figure 5. Comparison of average remaining energy percentage, when the number of nodes varies from 100 to 400.

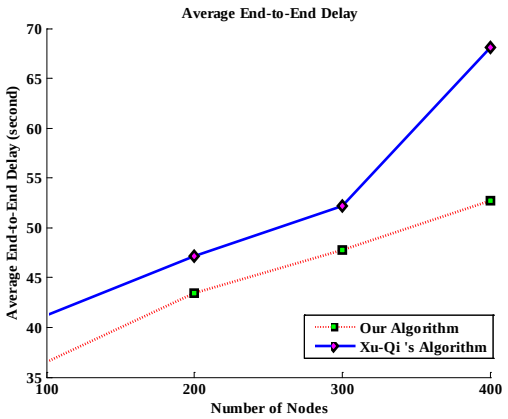


Figure 6. Comparison of average end-to-end delay, when the number of nodes varies from 100 to 400.

Priority-based Time Slot Assignment Algorithm for Hierarchical Time Sliced Optical Burst Switched Networks

Yahaya Coulibaly *, Muhammad Shafie Abd Latiff *, Abu Bakar Mohammad † and Abubakar Muhammad Umaru *
* Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia, 81300 Johor Bahru , Malaysia
Email: cyahaya@gmail.com,shafie@utm.my,amumaru@yahoo.com
† Faculty of Electrical Engineering, Universiti Teknologi Malaysia
81300 Johor Bahru , Malaysia
Email: bakar@utm.my

***Abstract*—Bandwidth-greedy applications are in continuous development. These applications are testing the bandwidth limit of current telecommunication and computer network infrastructures. Optical Burst Switching (OBS) is a promising optical switching technology to meet bandwidth requirements of such applications in the near-future. However, due to lack of matured and cost effective optical equipments, such as optical memories, this technology still suffers from high burst drops ratio as a result of contention in the core node. Many approaches have been proposed and evaluated to address this issue. In this paper, a priority-based time slot assignment algorithm, which we named as Priority-based segmented train algorithm (PSTA) is introduced and analyzed for Hierarchical Time Sliced OBS (HiTSOBS) a newly developed slotted OBS variant. The evaluation aims at comparing the performance of PSTA and that of HiTSOBS in terms of burst loss ratio and delay. Simulation results demonstrate that PSTA outperforms time slot assignment scheme used in HiTSOBS**

***Index Terms*—Optical Burst Switching (OBS); Hierarchical Time Sliced Optical Burst Switching (HiTSOBS); Burst Loss Probability (BLP); Time Slot; Contention.**

I. INTRODUCTION

Greedy-bandwidth applications are in continuous increase. Such applications require bandwidths that are not easily affordable by current telecommunication technology and infrastructures. Thus, alternative solutions are being searched to satisfy the needs of these applications. Optical networks are known for their high bandwidth support due to the nature of the fiber optic cable. Wavelength Division Multiplexing (WDM) technology and its derivatives such as Dense Wavelength Division Multiplexing (DWDM and Ultra-dense Wavelength Division Multiplexing (UDWDM) are emerging as a future evidence platform to transport advanced bandwidth demanding services, Currently, three optical switching paradigms have been proposed for that purpose. These technologies are: Optical packet Switching (OPS) [1] [2] [3] [4], Optical Circuit Switching (OCS) [5] and Optical Burst Switching. (OBS) [2] [6]. Among these three proposals, Optical Burst Switching technology is seen as the most feasible and viable solution to satisfy the needs of large bandwidth applications in the near future. Despite such favoritism for OBS, burst contention in the core network stands out as a major roadblock for its implementation. Burst contention occurs when flows from different input lines are sent to the same output port on the same fiber channel (wavelength) at the same time. In electronic networks, this problem is solved by using electronic memories (RAM) as buffers. Since there, are no mature and cost effective optical memories [7], OBS paradigm does not assume the use of buffer in the core network. Therefore, burst loss probability became a real hindrance to the deployment of OBS [8] and it is the focus of research in OBS. Before OBS can benefit the telecommunication service providers, contention must be solved so as to recue burst loss ratio. Various architectures of OBS have been proposed in the literature in an attempt to materialize the implementation of OBS. These attempts are based on two principles: non-slotted OBS and Slotted OBS. On one hand, non slotted OBS switch bursts in wavelength domain; on the other hand, slotted-OBS switch bursts in time domain [9]. The main advantage of slotted-OBS over non-slotted OBS is the optional use of non-cost effective wavelength converters and fiber delay lines (FDLs). In this paper, we focus on time slotted OBS variants where we propose and evaluate a priority-based segmented- train time slot allocation algorithm (PSTA) for the latest slotted OBS variant known as Hierarchical Time sliced Optical Burst Switching (HiTSOBS) [10]. To our best knowledge, this is the first time such algorithms are being proposed and evaluated for HiTSOBS. The rest of this paper is organized as follows: Section II goes through related works; Section III describes architecture of HiTSOBS. In Section IV, we discuss the PSTA algorithm. Simulation parameters, scenarios and results are discussed in Section V. Concluding remarks and future works are described in Section VI.

II. RELATED WORK

In this section, we review route, wavelength and time slot assignment schemes used in slotted WDM networks. RWA

 ISBN: 978-1-61208-166-3

for non-slotted OBS were largely studied and reviewed. An early review of RWA can be found in [11]. From there on, new RWA schemes were proposed and analyzed as discussed in [12] [13], [14] [15] [16], [17] [18] [19] and others. For more details on these schemes, the reader is referred to listed references at the end of this paper. In [20], the authors studied routing and wavelength and time slot assignment problem for a circuit-switched time division multiplexed (TDM) wavelength-routed (WR) optical WDM network. So as to overcome the shortcomings of non-TDM based RWA. The algorithm was applied on a network where each individual wavelength is partitioned in the time-domain into fixed-length time-slots organized as a TDM frame. Moreover, multiple sessions are multiplexed on each wavelength by assigning a sub-set of the TDM slots to each session. A set of RWTA algorithms was proposed and evaluated in terms of blocking probability. Shortest path routing algorithm was used for the routine part of the algorithm. Least Load (LL) wavelength selection scheme was used for wavelength assignment, while a Least Loaded Time Slot (LLT) technique was proposed for time slot assignment. The researchers claimed that, their proposed RWTA algorithm performs better than random wavelength and timeslot assignment schemes. However, the use of SP as routing algorithm is performance hindrance in the algorithm. The work done by Wen et al. in [21] is similar to that proposed in [20] and suffers for the same performance problems. In [22], Rajalakshmi and Jhunjhunwala also proposed a RWTA solution for wavelength routed WDM networks to increase to increase the channel utilization when the carried traffic does not require the entire channel bandwidth. As in any TDM-WDM architecture, multiple sessions are multiplexed on each wavelength by assigning a sub-set of the TDM slots to each session. Different from the work in [20], the authors used fixed routing (FR) and alternate routing (AR) algorithms for route computation. First Fit (FF) channel assignment algorithm was used for both wavelength and time slot assignment. In this algorithm, when a call gets blocked, the already established calls in the network are rerouted; wavelength and timeslot reassigned so as to accommodate the blocked call. Based on the results obtained, it was reported that the proposed RWTA scheme can be used to maximize the time of first call blocking hence increasing the overall network performance. The use of FR, AR and FF algorithms make the algorithm less complex and easy to implement, but performance wise the algorithm lacks scalability and dynamism. The works done by the researchers in [23] and [22] are similar except that a dynamic routing algorithm was used in [23]to compute the routes in addition to FR and AR algorithms. In [24], Um et al. proposed a centralized control architecture and a time-slot assignment procedure for time-slotted optical burst switched (OBS) networks. In this centralized resource allocation technique, ingress nodes request time-slots necessary to transmit optical bursts, and a centralized control node makes a reply according to the slot-competition result. The aim is to improve burst contention resolution and optical channel utilization. Although the algorithm did achieve high resource utilization, it did so at the cost of high buffering delay at the ingress node. Additionally, the centralized nature of the algorithm makes it non-scalable. Thus it is not appropriate for large networks and expected implementation environment for OBS networks. The researchers in [25] considered dynamic traffic grooming issue in WDMTDM switched optical mesh networks without wavelength conversion capability and proposed an adaptive grooming algorithm to solve the problem. The goal was to efficiently route connection requests with fractional wavelength capacity requirements onto high- capacity wavelengths and to balance the load on the links in the network at the same time. A cost function that encourages traffic grooming and load balancing was used to achieve the aforementioned objective. The authors concluded that, their algorithm outperforms similar routing algorithms. However, nothing was mentioned about time slot assignment and its effect on network performance. In [26], Yang and Hall proposed and evaluated a distributed Dynamic RWTA algorithm based on dynamic programming approach. Their goal was to minimize blocking probability. The proposed consists of three distinct parts; each part solves a sub problem of the RWTA: Routing part; wavelength assignment section and finally, wavelength assignment section. The results were compared with SP algorithm and were reported to perform better than that algorithm. The drawback of this solution is the use of SP for route discovery. Noguchi and Kamakura [27] proposed a hybrid of one-way and two-way signalling algorithm for slotted optical burst switching (SOBS) [28]. Through numerical analysis with comparison two-way signalling algorithm, the researchers argued that their hybrid signalling algorithm performs better than its competitor in terms of end-to-end delay. In [29], the scientists observed that next generation metro network is most likely to be based on high-capacity agile all- optical networks and considered a star metro network architecture that consists of a number of buffers-less all-optical core switches. They developed three resource sharing techniques. The first scheme is reservation-based, in which decisions are made at each core switch to avoid collision and it is called Centralized TDM (CTDM). In the second scheme, distributed and independent decisions are made at edge switches, but dropped packets at the core nodes are retransmitted; this algorithm is called Distributed TDM (DTDM). Finally, a combination of the above two techniques named Hybrid TDM (HTDM) was developed to support different optical network architectures. According to the simulation results, the authors reported that, among the three schemes, HTDM performs better because. This high performance of HRDM is attributed to the fact that it can achieve a better performance under both low and high traffic loads most of the time. However, HTDM needs more evaluations under different classes of service to confirm such claims. The researchers in [30] proposed a new dynamic RWTA algorithm based on a principle known as: the maximum contiguous principle. The proposed algorithm is called: Most-Continuous-Same-Available (MCSA) resources. K shortest path routing algorithm was used to compute the routes in accordance with hops from small to large stored in the network nodes routing table.

 ISBN: 978-1-61208-166-3

Although the simulation results suggest that, the algorithm did reduce the blocking probability and achieved high resource utilization, the algorithm has a high network overhead due to the fact it needs the real-time information such as network wavelength utilization, time slots allocation. Finally, in [31], the researchers proposed and evaluated the optical time-slot switching (OTS) technology, in which the fixed size time-slot is adopted as the basic switching granularity, and switching is done in the time domain, rather than wavelength domain. They also studied the issue routing, wavelength and time-slot assignment (RWTA) problem. To this end, they introduced an adaptive weight function to the routing and wavelength selection algorithm, and proposed several approaches for time slot assignment such as the train approach, wagon approach and p-distribution approach. They have demonstrated that, OTS and the underlying dynamic RWTA scheme performs better than conventional non time-based OBS in terms of burst loss probability (BLP), quality of service (QoS) and class of service (CoS). In this OBS design, time slots are reserved in groups. Such constraint lead to high burst loss rate. The authors did not include loss investigation results in their paper. Thus, the architecture needs further studies and modifications. However, it is worth noting that, this is the only paper, at the time of this writing, which has studied RWTA issue in the context of WDM OBS.

III. FRAME ARCHITECTURE AND OPERATION OF HITSOBS

In the HiTSOBS understudy, time-slots are numbered serially, starting at 0. The frame size known as radix and denoted by N represents the number of slots in each frame in the HiTSOBS hierarchy. i represents the time slot at which current burst transmission starts (Equation 2). The frame structure of HiTSOBS is depicted in Fig. 1. As in [10], a slot in the level-1 frame may expand into an entire level-2 frame and so on. However, in this paper, the maximum number of frame is fixed at 3. Beyond three levels, network performance is expected to degrade especially for delay sensitive applications. Bandwidth occupation per slot in a given level is determined by Equation 1

$$S_c = (\frac{1}{kN})W_c \quad (1)$$

where S_c is the share of a slot out of the total bandwidth of a particular wavelength of a fibre link denoted by W_c and k is the order of level transporting the burst and N is the frame size in time slot. Similar to conventional OBS, in HiTSOBS, ingress edge node accumulates data from different client networks (IP, ATM, and SONET/SDH, etc) into bursts, and classifies them into three classes: Bandwidth-greedy applications (Class 0), delay sensitive applications (Class 1) and finally loss sensitive applications (Class 2). Class 0 data are transmitted at level-1; class 1 data are transported at level-2; level-3 frames are used to transport class 2 bursts.

A. Control Plane Operation

Prior to the transmission of a burst, a burst header packet (BHP) is sent to reserve necessary resources. The BHP contains four types of information as depicted in Figure 3.0: the QoS of a burst, the start slot, and the burst length. Moreover, the BHP carries the initial routing information. Such information is not available in the BHP of [10] because routing was not studied. When a core node receive the control packet, it first deduces the outgoing link for the bursts and its QoS requirements and then using the PSTA algorithm determines where the slot lies in its hierarchy corresponding to that output link. The details of the algorithm are described in Section IV.

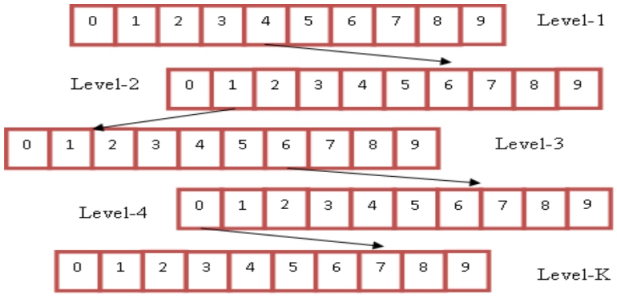


Fig. 1. Illustration of Frame Structure

Fig. 2. Burst Header Packet Contents

B. Data plane operation

Based on the routing information and the hierarchy constructed by the control plane, the data plane processes the incoming bursts and sends them to the reserved output link. A counter is maintained for each frame in the hierarchy, corresponding to the slot last served in that frame. Each time-slot, the counter for the level-1 frame is incremented by one, and the corresponding slot entry is checked. If it is a leaf entry containing a burst, the optical crossbar is configured so that the input line corresponding to that burst is switched to the output link under consideration. If on the other hand, the slot entry points to a lower level frame, the counter for the lower-level frame is incremented, and the process resources.

IV. PRIORITY-BASED SEGMENTED TIME SLOT ASSIGNMENT ALGORITHM

After a burst is assembled and sent to the network, a routing, wavelength and time slot assignment algorithm is responsible for choosing the appropriate route, wavelength and time slot to transport that burst. In this paper, shortest path routing and first fit wavelength assignment algorithms are assumed. For time slot assignment, a prioritized Segmented-Train time slot assignment algorithm (PSTA) is developed and implemented. See Fig 4. In this algorithm, time slots are allocated in a given level depending on the priority of the burst to be transported. Different form reservation technique used in [10], Equation 2

 ISBN: 978-1-61208-166-3

is used for time slot reservation.

$$S_R = i + (B - [\frac{(B-1)}{z}](z-1)z + [\frac{(B-1)}{z}]N \quad (2)$$

In the above equation, B represents burst size, N is the frame size, z represents the size of the train (number of coaches) and k is the initial position of time slot reservation. For instance, lets assume that, we have an optical time slot switch (OTS) that is capable of switching frames of 10 time slots (i.e., the frame size is 10 time slots). If a burst of high priority arrives at this core node, after being assigned the highest level in the hierarchy (i.e., level 1), High-PSTA(z), where the number of coaches of the train is fixed at 3, will be invoked. If the burst size is 10 time slots, time slot assignment is done as follows: The first 3 segments of the burst will be transmitted in slots No. 0, 3 and 6. And so on. Using the same OTS, if a burst of medium priority arrives at the core node, it is transmitted at the second highest level in the hierarchy (i.e., level 2) and Med-PSTA(z), where number of coaches is 2, is executed. The assignment procedures are similar to that of high priority burst except that time slots are reserved by pairs. When a low priority burst arrives at this core node, the lowest level in the hierarchy (i.e., level 3) is used to transport the burst and Norm-PSTA(z), where the train consists of only one coach will be called and the reservation of time slots is done one at a time as in the original HiTSOBS.

Algorithm 1 PSTA Algorithm

1: **Notations**:
t_a: Arrival time of a burst. $\mathbb{C}$: Class of the Burst. B_{qreq}: Burst QoS requirements. B: Burst to be transmitted. z: Number of coaches in a train. b : Minimum Bandwidth requirement. D: Maximum delay requirement.L: Maximum loss requirement.
2: **for all** B **do**
3: initialize candidate time slots
4: $T_n^m \leftarrow t$
5: **if** $\mathbb{C} = 0$ **then**
6: $B_{qreq} \leftarrow b$
7: Execute High_PSTA(z)
8: **else if** $\mathbb{C} = 1$ **then**
9: $B_{req} \leftarrow D$
10: Execute Med_PSTA(z)
11: **else**
12: $\mathbb{C} = 2$
13: $B_{qreq} \leftarrow L$
14: Execute Low_PSTA(z)
15: **end if**
16: **end for**

V. Simulation Factors and Results

A. Simulation Factors and Scenarios

To test the efficiency of HiTSOBS in a mesh WDM OBS network environment and implement the newly developed time slot assignment algorithm, we have modified the discrete-event simulator developed by the researchers in [10] to integrate Shortest Path (SP) and first fit wavelength algorithms for routing and wavelength assignment purposes. The algorithm was evaluated using the 14 nodes NSFNET topology as shown in Fig refsec5:fig1. We assumed that, the nodes are interconnected with fiber links of 8 wavelengths each. Bursts for flow j arrive as a Poisson process at rate $\frac{\lambda_i}{B}$ bursts per timeslot where B represents the average burst size. The timeslot size was chosen to correspond to $1\mu s$, which is consistent with the switching speeds of solid-state optical switching technologies available in the industry [32] and [33]. Two wavelength capacities were analyzed: 1 Gbps and 10 Gbps. Burst size was fixed at 125 KB [10]. The number of levels was chosen to be 3. Three classes of burst were assumed: class 0 (High Definition Multimedia Video/audio), class 1 (High Definition Multimedia streaming) and class 2 (normal data: FTP, email, telnet, etc...). Each flow is assigned to a level depending on its class. Upon arrival of a flow's burst at the edge node, the following processing happens: if the arriving burst encounters a non-empty queue, the burst is queued in the buffer if it is not full and awaits service. If on the other hand the arriving burst encounters an empty queue, the edge node reserves a time slot according to PSTA using equation 2. Time slots are reserved over a number of frames equal to the burst length and the burst is transmitted on to the core node. As in [10], the slot positions for burst slices for any given flow vary each time the flow becomes newly backlogged; this is important because it helps prevent synchronization and phase locking which complicates the implementation of OPS. Simulation parameters are summarized in Table I.

TABLE I
Simulation factors and Levels

Factors	Levels
Wavelengths per link	8
Wavelength Capacity (Gbps)	1, 10
Frame Size (Time slot)	10
Burst Size (KB)	9
Time Slot size (μs)	1, 2
Buffer Size (Time slot)	10
Number of Flows	1000
Topology	NFSNET
Number of Simulation run	20

 ISBN: 978-1-61208-166-3

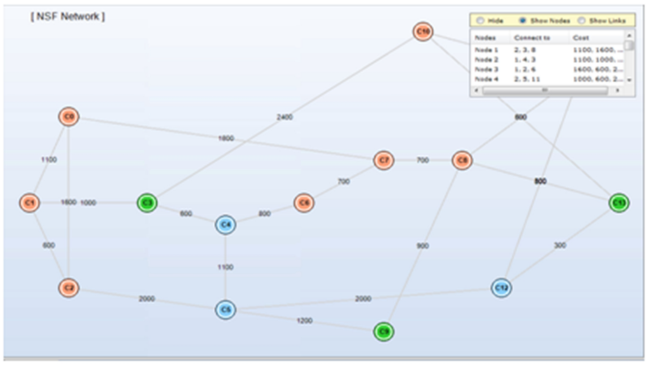
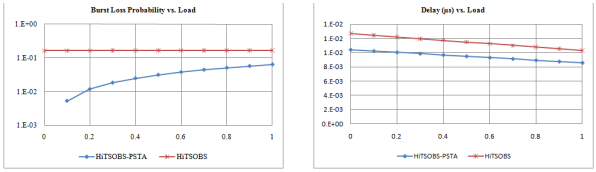


Fig. 3. Simulation Topology



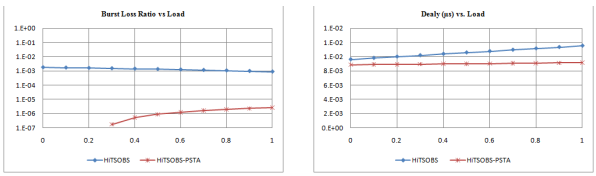
(a) Loss vs. Load for 1 Gbps (b) Delay vs. Load for 1 Gbps

Fig. 4. Investigating the effect of 1 Gbps Channel Capacity

B. Results Analysis

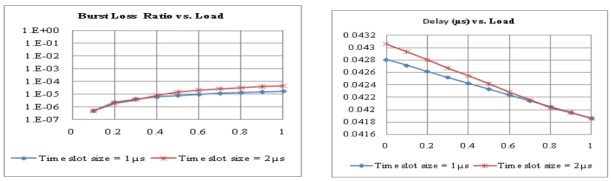
In this section, different simulation results are discussed. Fig 4 shows the burst loss ratio (BLR) and the delay performance for HiTSOBS and HiTSOBS-PSTA for wavelength capacity of 1 Gbps. In Fig 5, the same comparison is made for wavelength capacity increased to 10 Gbps. Fig 6 compares the performance of both algorithms for different time slot size in μs. Similar to the work in [10], the burst size and frame size were chosen to be 125 KB and 10 respectively. Shortest path algorithm was used for route selection and first-fit technique was used for wavelength assignment.

From the above figures, it can be observed that, the proposed time slot assignment algorithm (PSTA) performs better than the scheme used in [10] for time slot assignment. This is due to the fact that, in PSTA, when a burst is announced, we try to reserve more than one time slot in one frame based on the QoS requirements of the burst. Also, the way bandwidths are allocated to each time slot contributes to the superiority of our algorithm. Fig 5 demonstrates similar results as in Fig 4 and the arguments of the superiority are similar. However, in this case, wavelength capacity was increased to 10 Gbps which has,



(a) Loss vs. Load for 10 Gbps (b) Delay vs. Load for 10 Gbps

Fig. 5. Investigating the effect of 10 Gbps Channel Capacity



(a) Loss vs. Load (b) Delay vs. Load

Fig. 6. Investigating the effect of Time Slot size

remarkably, pulled the performance up. To study the effect of time slot size on both loss and delay for HiTSOBS, we run two cases of simulation; one with $1\mu s$ and the other with $2\mu s$ as time slot size for both algorithms. For space limitation, we only show the results of this investigation for HiTSOB-PSTA in Fig 6. These results suggest that longer time slots have negative impact on loss and delay of a burst inverse especially at low and medium load (0.5). This is not surprising, because longer time slot means more time to process, so at low load, burst will have to wait longer before they are assigned a time slot (more delay) and this lead to more loss as load increases and the delay starts to decrease at very high load and the size of time slot size becomes negligible.

VI. Conclusion

In this paper, we have proposed and evaluated a prioritized time slot assignment algorithm for HiTSOBS. Simulation results demonstrate that, the newly propose algorithm (PSTA) does help in improving HiTSOBS in terms of loss and delay as compared with the technique used in [10]. However, the authors believe that, HiTSOBS-PSTA should produce better results when better route and wavelength selection algorithms are used. Additionally, we think that HiTSOBS should perform better than traditional OBS. To prove these hypothesis, the authors have integrated PSTA with an adaptive and QoS based route and wavelength assignment algorithms that is integrated with PSTA and it is under evaluation.

Acknowledgments

The authors would like to thank the Islamic Development (IDB) for its financial support as well as the Ministry of Higher Education (MOHE) of Malaysia. Additionally, the authors thank Universiti Teknologi Malaysia (UTM) for supporting this work through Vote. No: Q.J B0000.7128.00J94.

References

[1] C. Guillemot, M. Renaud, P. Gambini, C. Janz, I. Andonovic, R. Bauknecht, B. Bostica, M. Burzio, F. Callegati, and M. Casoni, "Transparent optical packet switching: The european acts keops project approach," *Journal of Lightwave Technology*, vol. 16, no. 12, p. 2117, 1998.

[2] D. Chiaroni, M. Renaud, G. Eilenberger, F. Masetti, A. Jourdan, and P. Bonno, "Optical packet switching matrix: a key system for the next generation of multi-terabit routers/switches for flexible optical networks," *Alcatel Telecommunications Review*, no. 3, pp. 183–185, 2001, 484ZY Times Cited:2 Cited References Count:3.

 ISBN: 978-1-61208-166-3

[3] T. El-Bawab and J. Shin, "Optical packet switching in core networks: between vision and reality," *Communications Magazine, IEEE*, vol. 40, no. 9, pp. 60–65, 2002.

[4] J. Jue, W. Yang, Y. Kim, and Q. Zhang, "Optical packet and burst switched networks: a review," *Communications, IET*, vol. 3, no. 3, pp. 334–352, 2009.

[5] A. Ghafoor, M. Guizani, and S. Sheikh, "Architecture of an all-optical circuit-switched multistage interconnection network," *IEEE Journal on Selected Areas in Communications*, vol. 8, no. 8, pp. 1595–1607, 1990.

[6] C. Qiao and M. Yoo, "Optical burst switching (obs)a new paradigm for an optical internet," *Journal of High Speed Networks*, vol. 8, no. 1, pp. 69–84, 1999.

[7] T. Venkatesh and C. Siva Ram Murthy, "Introduction to optical burst switching," in *An Analytical Approach to Optical Burst Switched Networks*. Springer, 2010, pp. 1–41.

[8] J. Triay and C. Cervello-Pastor, "An ant-based algorithm for distributed routing and wavelength assignment in dynamic optical networks," *Selected Areas in Communications, IEEE Journal on*, vol. 28, no. 4, pp. 542–552, 2010.

[9] F. Farahmand, V. Vokkarane, and J. Jue, "Practical priority contention resolution for slotted optical burst switching networks," 2003.

[10] V. Sivaraman and A. Vishwanath, "Hierarchical time-sliced optical burst switching," *Optical Switching and Networking*, vol. 6, no. 1, pp. 37–43, 2009.

[11] H. Zang, J. Jue, and B. Mukherjee, "A review of routing and wavelength assignment approaches for wavelength-routed optical wdm networks," *Optical Networks Magazine*, vol. 1, no. 1, pp. 47–60, 2000.

[12] D. Zhemin and M. Hamdi, "Routing and wavelength assignment in multi-segment wdm optical networks using clustering techniques," *Photonic Network Communications*, vol. 8, no. 1, pp. 55–67, 2004.

[13] J. Hwang, J. Jung, Y. Park, J. Bae, H. Song, and S. Kim, "A rwa algorithm for differentiated services with qos guarantees in the next generation internet based on dwdm networks," *Photonic Network Communications*, vol. 8, no. 3, pp. 319–334, 2004.

[14] T. Fischer, K. Bauer, and P. Merz, "A multilevel approach for the routing and wavelength assignment problem." IEEE, 2008, pp. 225–228.

[15] K. Liu, "Routing and wavelength assignment algorithm in multi-fiber wdm optical networks," in *Symposium on Photonics and Optoelectronics, 2009.* Wuhan: IEEE, 2009, pp. 1–4.

[16] R. Randhawa and J. Sohal, "Static and dynamic routing and wavelength assignment algorithms for future transport networks," *Optik-International Journal for Light and Electron Optics*, vol. 121, no. 8, pp. 702–710, 2010.

[17] U. Rathore Bhatt and S. Tokekar, "Routing and wavelength assignment algorithms for multiclass wdm optical networks," *Optik-International Journal for Light and Electron Optics*, 2010.

[18] A. Wason and R. Kaler, "Generic routing and wavelength assignment algorithm for a wavelength-routed wdm network," *Optik-International Journal for Light and Electron Optics*, 2010.

[19] A. Wason and R. S. Kaler, "Routing and wavelength assignment in wavelength-routed all-optical wdm networks," *Optik*, vol. 121, no. 16, pp. 1478–1486, 2010, 645VZ Times Cited:0 Cited References Count:10.

[20] B. Wen and K. Sivalingam, "Routing wavelength and time-slot assignment in time division multiplexed wavelength-routed optical wdm networks," pp. 1442–1450, 2002.

[21] B. Wen, R. Shenai, and K. Sivalingam, "Routing, wavelength and time-slot-assignment algorithms for wavelength-routed optical wdm/tdm networks," *Journal of Lightwave Technology*, vol. 23, no. 9, p. 2598, 2005.

[22] P. Rajalakshmi and A. Jhunjhunwala, "Routing, wavelength and timeslot reassignment algorithms for tdm based optical wdm networks-multi rate traffic demands," pp. 1–6, 2006.

[23] ——, "Routing wavelength and time-slot reassignment algorithms for tdm based optical wdm networks," *Computer Communications*, vol. 30, no. 18, pp. 3491–3497, 2007.

[24] T. Um, J. Choi, S. Choi, and W. Ryu, "Centralized resource allocation for time-slotted obs networks." IEEE, 2006, p. 40.

[25] A. Vishwanath and W. Liang, "On-line routing in wdm-tdm switched optical mesh networks," *Photonic Network Communications*, vol. 11, no. 3, pp. 287–299, 2006, 035EH Times Cited:0 Cited References Count:37.

[26] W. Yang and T. Hall, "Distributed dynamic routing, wavelength and timeslot assignment for bandwidth on demand in agile all-optical networks," pp. 136–139, 2007.

[27] H. Noguchi and K. Kamakura, "Effect of one-way mode of hybrid reservation on slotted optical burst switching networks," pp. 1–6, 2009.

[28] Z. Zhang, L. Liu, and Y. Yang, "Slotted optical burst switching (sobs) networks," *Computer Communications*, vol. 30, no. 18, pp. 3471–3479, 2007.

[29] A. Rahbar and O. Yang, "Agile bandwidth management techniques in slotted all-optical packet switched networks," *Computer Networks*, vol. 54, no. 3, pp. 387–403, 2010.

[30] L. Jia, J. Fang-yuan, and X. Xiao-xiao, "A dynamic routing, wavelength and timeslot assignment algorithm for wdm-tdm optical networks," pp. V1–533 – V1–537, 2010.

[31] G. Shan, J. Dai, S. Sun, G. Zhu, and D. Liu, "Study on the problem of routing, wavelength and time-slot assignment toward optical time-slot switching technology," pp. 335–339, 2010.

[32] S. Yao, S. Dixit, and B. Mukherjee, "Advances in photonic packet switching: An overview," *IEEE Communications Magazine*, vol. 38, no. 2, pp. 84–94, 2000.

 ISBN: 978-1-61208-166-3

[33] M. Reisslein, "Measurement-based admission control for bufferless multiplexers," *International Journal of Communication Systems*, vol. 14, no. 8, pp. 735–761, 2001.

 ISBN: 978-1-61208-166-3

Optimization of link capacity for telemedicine applications

Karol Molnar*, Jiri Hosek*, Lukas Rucka*, Pavel Vajsar* and Otto Dostal†
*Department of Telecommunications
FEEC, Brno University of Technology
Purkynova 118, 612 00 Brno, Czech Republic
Email: molnar@feec.vutbr.cz, hosek@feec.vutbr.cz, rucka.lukas@phd.feec.vutbr.cz, pavel.vajsar@phd.feec.vutbr.cz
†Institute of Computer Science
Masaryk University
Botanicka 554/68a, 602 00 Brno, Czech Republic
Email: otto@ics.muni.cz

***Abstract*—Interactive telemedicine services have become very popular due to their cost efficiency and low response times. On the other hand, several acquisition units connected to a network can significantly increase the network load on communication links connecting hospital facilities to the Internet. Since these links are often leased from commercial ISPs, there is much interest in minimizing the cost, i.e. the capacity of leased links, without a significant degradation of the quality of telemedicine services. The paper presents the results of the initial analysis of network traffic generated by Computed Radiography, introduces the corresponding statistical model, and presents the simulation results obtained by optimizing the network capacity from the point of view of application response time.**

***Keywords*-Computed Radiography; medical image processing; OPNET Modeler; transmission capacity; WFQ;**

I. INTRODUCTION

The number of digitized medical facilities which can take advantage of integrated solutions for data handling, storing and transmitting, according to the DICOM standard, is rapidly increasing [1]. The demand of current telemedicine equipment on instantaneous bandwidth varies from tens of kbps to tens of Mbps. It causes that the requirement on the capacity of communication links is highly affected by the type and exact number of such equipment items (modalities) in the medical facility. Usually these facilities are connected to a regional centre for medical image processing and storing, which coordinates data sharing and mutual exploitation of technical resources of the collaborating parties. These centres also provide sophisticated analyses of traffic flows to estimate traffic profiles, time-distributions, delays, etc. This paper presents the results of such an investigation.

The aim of our work was to estimate the minimum link-capacity towards commercial ISPs which still preserves acceptable service quality for telemedicine applications. The quality was expressed as the delay of images transmitted from the medical modality. We also conducted an investigation into differentiated traffic treatment and analysed how significantly preferential treatment of selected traffic-flows affects the response-time in the case of different services.

The methods used for analysis, modelling and evaluation are described in the following structure: section II describes our initial premises, ways of collecting and the methods of statistical processing of measured data. Section III contains the description of the simulation models built based on the statistical description of the modality investigated. This section also evaluates the simulation results with and without preferential traffic treatment. The last section concludes our activities and presents our plans for future investigation.

II. INITIAL PREMISES AND STATISTICAL ANALYSIS

Current hospital facilities are usually equipped with several modalities such as MRI (Magnetic Resonance Imaging), US (UltraSound), CT (Computed Tomography) or CR (Computer Rentgen/X-ray). The last of these modalities is the most common representative of current telemedicine applications. For this reason our analysis was primarily focused on the CR modality.

Information required for the analysis was obtained by direct measurement of corresponding traffic-flow parameters. To preserve the faithfulness of data, these measurements were conducted between 7 am and 4 pm only. Traffic flows from non-working days were also excluded to avoid additional statistical errors. Additionally, to eliminate the influence of transport network, the measurements were carried out only on modalities which were connected to the regional centre via 100 Mbps or faster links. The whole traffic generated by these modalities was captured by the tcpdump tool and it was then statistically analysed. Pearson's chi-square test [2] was used to validate the fidelity of distribution functions and their parameters, which were chosen to describe traffic flows generated by CT and CR modalities.

A. Computed Radiography Modality

In the case of CR modality there were 392 inter-request times identified and measured between subsequent TCP connections. The values measured ranged from 8s to 25963s. It was also evident that a CR transmission consisted of random

 ISBN: 978-1-61208-166-3

bursts of TCP connections. Each burst contained from one to seven separate connections. Therefore it was desirable to analyse separately the period between subsequent bursts, the number of TCP connections in a burst and the duration between TCP connections within a burst.

Without a detailed semantic analysis of the traffic-flows it is quite difficult to specify the boundaries of the bursts and decide if a given TCP connection belongs to the current burst or represents the beginning of the next burst. We empirically chose a period of 150 seconds to limit the length of each burst. After excluding the extremely outlying values, the periods between subsequent bursts were ranged in the interval from 150s to 3986s with a sample mean of 837.63s and a sample standard deviation of 840.01s.

We assumed that the length of the period between bursts was of exponential distribution with probability density according to (1).

$$f(x) = \frac{1}{\lambda} e^{-\frac{x}{\lambda}} \tag{1}$$

for x $>$ 0, where $\lambda > 0$ is the parameter to be specified based on the measurement results.

In the case of exponential distribution parameter λ equals the mean-value of the random variable. The sample counterpart of the mean is the average of the values in the selective statistical population, which means that the period between the beginnings of two subsequent TCP bursts can be described by exponential distribution with parameter λ = 837.63s.

The period between subsequent TCP connections within a burst ranges from 8s to 150s. After excluding the most outlying values, we obtained 150 values between 8s and 116s. These values were symmetrically centred around an obvious mean. A random variable with normal probability distribution was therefore assumed with the probability density according to Eq. (2):

$$f(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp(-\frac{(x-\mu)^2}{2\sigma^2}), \tag{2}$$

-$\infty <$ x $< \infty$, where $\mu \in$ (-∞, ∞) and $\sigma > 0$ are constants and can be derived from the values measured.

The mean value of a random variable with normal distribution is equal to parameter μ and the standard deviation is equal to parameter σ. The selective counterpart of the mean is the average of the values in the statistical population. The selective counterpart of the standard deviation is represented by the sample standard deviation according to Eq. (3):

$$\overline{\sigma} = \frac{1}{n-1} (\sum (x_i - \overline{x_s})^2)^{\frac{1}{2}}. \tag{3}$$

After applying these presumptions on the values measured we found that the period between the beginnings of two subsequent TCP connections within a burst is normally distributed with parameters μ = 57.87s and σ = 27.88s.

Each of the bursts examined contained a random number of TCP connections, from one to seven. Based on an empirical evaluation we assumed that the number of TCP connections in a burst has a Poisson probability distribution with the following probability function Eq. (4):

$$P(x) = \lambda^x e^{-\lambda} / x!. \tag{4}$$

The mean value of a random variable with the Poisson distribution is equal to parameter λ. The selective counterpart of this mean is the average of the values in the statistical population.

In our analysis we dealt with a total of 225 values of one to four connections and found that the number of TCP connections in a burst can be described by the Poisson probability distribution with parameter λ = 1.45s.

Finally we had to statistically describe the amount of data transmitted within the TCP connections. In total we had 401 TCP connections captured for the CR modality. From these connections, 301 represented a transmission of 10.25MB of data and the remaining 100 cases corresponded to a transmission of 8.5MB each. This behaviour can clearly be described by an alternative distribution of probability 0.25 for 8.5MB and 0.75 for 10.25MB.

B. Final notes on statistical analysis

For any of the CR modalities neither the beginnings of the TCP sessions nor the amount of transmitted data shows any sign of dependence, which means that in the simulation model we can consider the beginnings of the TCP sessions and the amount of data to be independent. We used the pivot table to verify the independence of these parameters.

III. SIMULATION OF TELEMEDICINE APPLICATION

A. Description of the simulation model

Within our simulations we examined the impact of total link capacity and differentiated queue management on the response-time of the CR modalities. For this purpose a simulation model was built in the OPNET Modeler simulation environment [3]. The model consisted of 8 traffic sources with CR traffic-profile. Additional background traffic was modelled by TCP sources generating traffic bursts with Poison distribution. During the simulations, the application-level response-time was evaluated. Because of close behavioural analogy, the FTP (File Transfer Protocol) protocol was used to model the TCP communication of the modalities. To simulate limited link capacities, rate-limiting was applied to the common communication link. All the other communication links operated at a full speed of 1Gbps. The inter-request time, file size and number of repetitions were configured according to the results of the statistical analysis. The influence of controlled queue management was verified by using the WFQ (Weighted Fair Queuing) [4], [5] scheduling scheme. This scheduling scheme was chosen due to its frequent use in real networks installations.

 ISBN: 978-1-61208-166-3

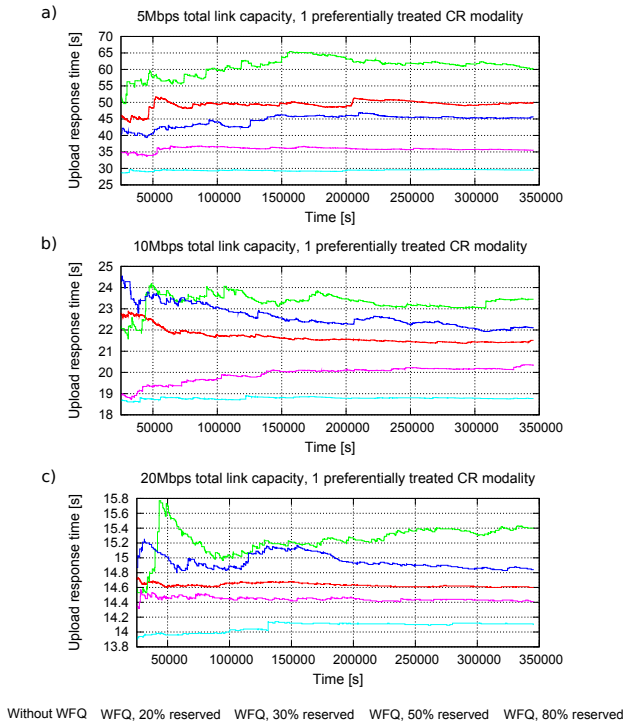


Figure 1. Impact of the relative distribution of link-capacity between WFQ queues for 5Mbps (a) 10Mbps (b) and 20Mbps (c) links in the case of 8 CR modalities

B. Simulation results

The impact of the bandwidth distribution between WFQ queues on the response time of one preferentially treated CR modality is shown in Fig. 1a) to 1c). The background traffic is processed by the second queue, which can use the remaining capacity of the communication link. It is evident that for the CR modality the bandwidth guarantee has a clearly positive impact on the response time. It is also evident that the resulting effect of WFQ scheduling depends on the total link capacity. More exactly, in the case of the 5Mbps total link-capacity at least 50% of the capacity must be guaranteed for the selected CR modality to achieve a shorter response time than without the use of WFQ. For higher link capacities already the guarantee of 20% of capacity brings improvements. Simulation results show that the improvement is relative and the absolute response times are dependent on the actual connection speed.

IV. Conclusion

After a comparison of the simulation results with the network administrators' practical experience we found that our simulation model showed very good matching with the measurement results obtained from real networks. It means that the simulation model can be used to estimate the required link capacity if we know the type and number of corresponding modalities.

The simulation scenarios clearly showed that for a given combination of devices it is possible to specify a minimum data rate for which the average response time will remain within the required limits. It was also found that preferential treatment can decrease the response time for Computed Radiography.

We have for some time been working on the statistical models for the remaining modalities. If completed, they will also be integrated into the simulation model and used for the optimization.

Acknowledgment

This paper has been supported by the Grant Agency of the Czech Republic (Grant No. GA102/09/1130) and the Ministry of Education of the Czech Republic (Project No. MSM0021630513).

References

[1] K. Slavicek, M. Javornik, O. Dostal, "Technology background of international collaboration on medicine multimedia knowledge base establishment", Proc. 2nd WSEAS International Conference on Computer Engineering and Applications (CEA'08), Acapulco, Mexico, pp. 137-142, 2008.

[2] P. E. Greenwood, M. S. Nikulin, *A guide to chi-squared testing*, Wiley-Interscience, New York, 1996.

[3] OPNET Technologies, *OPNET Modeler Product Documentation Release 15.0*, 2009.

[4] K. I. Park, *QoS in Packet Networks*, Springer, New York, 2004.

[5] L. Rucka, J. Hosek, K. Molnar, "Advanced Modelling of DiffServ Technology", Proc. 32nd International Conference on Telecommunications and Signal Processing, Budapest, Hungary, pp. 1-6, 2009.

 ISBN: 978-1-61208-166-3

20 Gb/s Absolute Polar Duty Cycle Division Multiplexing-Polarization Division Multiplexing (AP-DCDM-PolDM) Transmission System

Amin Malekmohammadi
Dept. of Electrical and Electronic Engineering
The University of Nottingham
Aminmalek_m@ieee.org

***Abstract*— The performance of Absolute Polar Duty Cycle Division Multiplexing (AP-DCDM) over Polarization Division Multiplexing (PolDM) system is presented based on the simulation results, in order to double the capacity in optical fiber links. It is demonstrated that the spectral width occupied by 10 Gb/s RZ is 40 GHz whereas, this value can be reduced to 20 GHz over 2 channels of the proposed system. Simulations show that the maximum attainable dispersion-limited transmission distance for 20-Gb/s AP-DCDM-PolDM data over standard single-mode fiber can be extended to 200 km for a 2-dB penalty.**

Keywords- Optical Communication; AP-DCDM; PolDM

I. INTRODUCTION

There has recently been a capacity explosion of optical fiber links due to techniques such as Wavelength-Division Multiplexing (WDM) [1]. However, WDM systems are straining to accommodate either smaller channel wavelength spacing or wider wavelength ranges in order to continue the growth in capacity. The minimum channel spacing and the total wavelength range are limited by many factors, including optical filters, wavelength drifts, signal bandwidth, Erbium-Doped Fiber Amplifier (EDFA) bandwidth, and dispersion and nonlinearities [1, 2].

Next generation systems working at 40-Gb/s data rates and incorporating Dense Wavelength-Division Multiplexing (DWDM) will require bandwidth efficient transmission formats to minimize the chromatic dispersion penalty [3]. Bandwidth efficiency is also important for maximizing the spectral efficiency of the WDM transmitters, whilst maintaining low levels of crosstalk. Bandwidth efficient transmission has previously been achieved in several ways including advanced modulation formats such as Differential Quadrature Phase Shift Keying (DQPSK) However, this technique increase the complexity of the receiver by the introduction of the temperature-stabilized Mach-Zehnder Interferometer (MZI) [4].

Absolute Polar Duty Cycle Division Multiplexing (AP-DCDM) is an alternative multiplexing which appears promising for its spectral width and its chromatic dispersion tolerance [5, 6]. The narrow optical spectrum on AP-DCDM reduces the inter channel coherent crosstalk in AP-DCDM-WDM systems. The possibility of setting channel spacing as narrow as 62.5 GHz for 40 Gbit/s AP-DCDM signals over WDM was confirmed [6]. As reported in [6], a capacity of 1.28 Tbit/s (32 x 40 Gbit/s) was packed into a 15.5 nm EDFA gain-band with 0.64 bit/s/Hz spectral efficiency by using 10 Gbit/s transmitter and receiver. Good propagation format together with a simple transmitter implementation make AP-DCDM very interesting for uncompensated optical links [5].

Polarization Division Multiplexing (PolDM) is well known technique for doubling the spectral efficiency. In PolDM system two signals are transmitted at the same wavelength with orthogonal States of Polarization (SOP). At the receiving end the polarization channels are demultiplexed at polarization beam splitter and detected independently. PolDM allows the transmission at an equivalent double bitrate without reducing the reach to a fourth due to chromatic dispersion [7, 8]. PolDM has the advantage that it can be implemented without major changes to the existing systems. PolDM can be implemented by adding a transceiver and associated polarization multiplexer/demultiplexer at each end of the fiber link, while leaving the rest of the system unchanged [9].

In this paper, for the first time to the best of our knowledge, the AP-DCDM system has been exploited together with PolDM in order to achieve, a reach of 200 km at an overall bitrate of 20 Gb/s (2 x 2 x 5 Gb/s), without dispersion compensation.

This paper is organized as follows. Section II describes the simulation setup of AP-DCDM-PolDM over 200 km single mode fiber. Section III discusses the implementation issues in comparison against other techniques and Section IV discusses the performance of AP-DCDM over PolDM.

II. SIMULATION SETUP

In this study, two commercial software, OptiSystem and MATLAB were used to access the system performance. The performance evaluation of the system is based on Bit Error Rate (BER) which is described in [5].

Fig.1 shows the model of AP-DCDM over PolDM system. The evaluation starts with 2 AP-DCDM channels

 ISBN: 978-1-61208-166-3

setup. Data1, Data 2, each at 5 Gb/s with Pseudo Random Binary Sequence (PRBS) of 2^{10} -1 are carved with one electrical RZ pulse carvers at 50% of duty cycle and NRZ pulse carver, respectively.

The voltages for all users at the multiplexer input are identical. All users' data are multiplexed via a power combiner (electrical adder) resulting in a bipolar signal. Subsequently, the absolute circuit is used to produce an absolute polar signal [5]. The signals are used to modulate a Laser Diode (LD), which operates at 1550 nm wavelength using a Mach-Zehnder Modulator (MZM). The modulated AP-DCDM signal is split in two replicas uncorrelated by means of a fiber spoil, with a delay of about 15 µs.

The two replicas, equalized in power, are orthogonally polarized by adjustable fiber Polarization Controller (PC) and recombined by a pig-tailed micro-optic Polarization Beam Combiner (PBC).

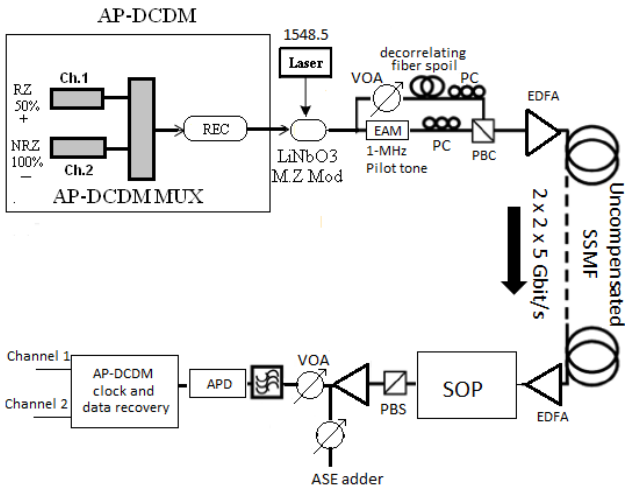


Figure 1. AP-DCDM-PDM Setup

A polarization multiplexed signal at an overall bit-rate of 20 Gb/s is generated and then it is boosted by an Erbium-Doped Fiber Amplifier (EDFA) and launched in a uncompensated Single Mode Fiber (SMF) link. At the receiver, the multiplexed channels are optically preamplified by an EDFA and a variable amount of Amplified Spontaneous Emission (ASE) noise, generated by a filtered ASE source, is added in order to modify the Optical Signal-to-Noise Ratio (OSNR).

The 20 Gb/s AP-DCDM-PolDM performance is assessed over lengths ranging from back-to-back to 200 km. nonlinear effects are negligible due to low lunch power [10, 11].

At the end of the fiber link, the two orthogonally polarized PolDM channels at the same wavelength are then optically demultiplexed by a fiber Polarization Beam Splitter (PBS) after an adjustable fiber PC.

A single demultiplexed channel is detected by a Avalanche Photodiode (APD) and passed through a Low-Pass Filter (LPF) and a Clock-and-Data-Recovery (CDR) unit. The regeneration and error detector are programmed, using sampling points and threshold value. The samples are taken at two sampling points (S_1 and S_2) at the first two slots in every symbol [5]. The sample values are fed into the decision and regeneration program. In this program, the sampled values are compared against threshold value and the decision is performed based on the operation shown in Tables I and II [5, 6]. These tables contain the regeneration rules for a two-channel AP-DCDM system that the data recovery program uses to regenerate original data for each channel. For example for user one, binary 0 is regenerated when sampling values at S_1 and S_2 are less than threshold value (Table 1 rule 1). Binary 1 is regenerated when sampled amplitude at S_1 is equal or greater than threshold, while amplitude at S_2 is less than threshold (Table 1 rule 3) [5].

TABLE I. DATA RECOVERY RULES FOR USER 1 (U1)

No	Rules					
1	if	(S_1 < Thr)	&	(S_2 < Thr)	then	U1 = 0
2	if	(S_1≥ Thr)	&	(S_2 ≥ Thr)	then	U1 = 0
3	if	(S_1 ≥ Thr)	&	(S_2 < Thr)	then	U1 = 1
4	if	(S_1 < Thr)	&	(S_2 ≥ Thr)	then	U1 = 1

TABLE II DATA RECOVERY RULES FOR USER 2 (U2)

No	Rules			
1	if	(S_2 < Thr)	then	U2 = 0
2	if	(S_2 ≥ Thr)	then	U2 = 1

III. IMPLEMENTATION ISSUES IN COMPARISON WITH OTHER TECHNIQUES

AP-DCDM like NRZ-OOK requires only one Modulator and one Photodiode (PD) for n number of users at the transmitter and the receiver side, respectively. This is very economical in comparison to other modulation formats such as NRZ-DPSK, which require one Delay Interferometer (DI) and two PDs at the receiver [5], or RZ-DQPSK which requires two MZM at the transmitter, and two DIs together with four PDs at the receiver [5] or duobinary which require one dual-arm MZM modulator including driver amplifier for each modulator arm at the transmitter and one PD in the receiver.

Referring to the AP-DCDM data recovery concept, one may argue that the complexity of AP-DCDM receiver is higher than other systems. However, the complexity is due to additional electronics components and devices, the solutions of which are available in term of technology and experts [5].

 ISBN: 978-1-61208-166-3

IV. PERFORMANCE OF AP-DCDM-POLDM

Fig. 2 shows the optical spectra measured after the MZM. Considering the null–to–null bandwidth, the spectral width of 10 Gb/s AP-DCDM is around 20 GHz and it is equivalent to that of a 10 Gb/s NRZ-OOK signal. Comparing the optical spectral width at the same aggregate bit rate (10 Gb/s) between RZ-OOK (which is around 40 GHz), and AP-DCDM, AP-DCDM shows a great spectral width reduction (~20 GHz). This is because AP-DCDM divides the symbol to n slots where n is the number of channels [5]. Thus, it requires a null-to-null spectral width of 2 × [n × single channel bit rate], whereas RZ-OOK requires 2 × (2 × aggregate bit rate). This amount of saving in the spectral width is will leads to better spectral efficiency and tolerance to chromatic dispersion [5].

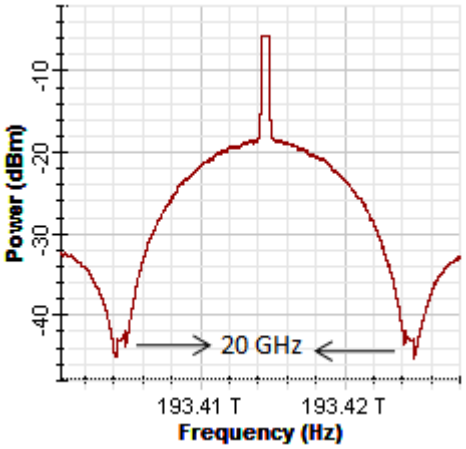


Figure 2. Optical spectra for AP-DCDM

The PolDM-AP-DCDM system at 20 Gb/s with the SOP stabilizer is tested for different SSMF propagation lengths up to 200 km. we have measured the BER as a function of the single demultiplexed channel OSNR, which is detected after polarization demultiplexing. Note that the optical power at the APD input is kept constant to -15 dBm. The performance of the PolDM-AP-DCDM transmission is compared with single channel transmission. Fig. 3 shows the required OSNR for a BER value of 10^{-9} versus propagation length. In the case of back to back because of the around 35 dB polarization extinction ratios of both polarization beam combiner and polarization beam splitter and to the good constancy of the SOP at the demultiplexing polarization beam splitter there is no penalty in transitory from the case of single channel transmission to the case of both polarization multiplexed channels. The cross-talk between the channels after polarization demultiplexing is thus small therefore with respect to the single channel case the penalty is negligible.

On the other hand in correspondence of the BER measurements for propagation length of around 70 km and more a penalty is found due to the cross-talk which is generated by small SOP fluctuations and enhanced by the fiber propagation, at the polarization beam splitter after polarization demultiplexing.

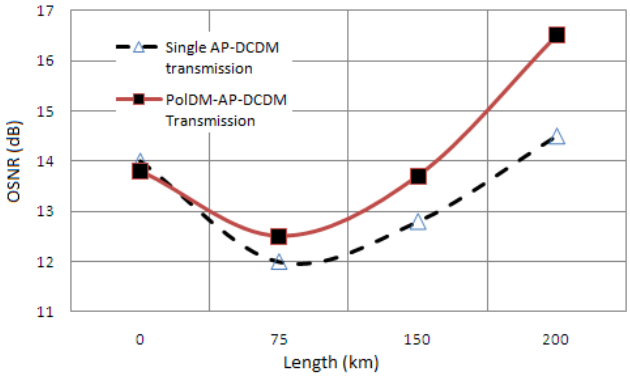


Figure 3. OSNR for a BER of 10^{-9} versus length of propagation over uncompensated SMF

In the case below, 150 km refer to the channel whose performance is slightly worse than the orthogonally polarized channel. the penalties remain however not higher than 1 dB but at 200 km OSNR penalty increases to around 2 dB and a change in the slope is obvious as can be seen in Figure 4, where BER carve versus OSNR are shown.

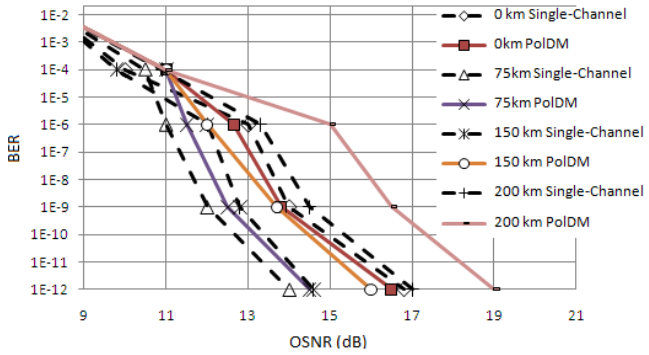


Figure 4. BER curves versus OSNR for different length of propagation over uncompensated SMF

V. CONCLUSION

Absolute Polar Duty Cycle Division Multiplexing over Polarization Division Multiplexing has been proved an attractive technique to double the transmission rate, while preserving the 10 Gb/s dispersion tolerance of the AP-DCDM format. The numerical results confirm that using this electrical multiplexing/demultiplexing technique, more than two users can be carried over the same PolDM channel. Consequently, the capacity

 ISBN: 978-1-61208-166-3

utilization of the PolDM channels can be increased tremendously; which is achieved at a lower spectral width in comparison to conventional techniques. Transmission over 200 km SSMF was also demonstrated. Based on the simulation results it can be concluded that AP-DCDM is suitable for implementation in PolDM transmission systems.

REFERENCES

[1] S. Bigo, Multiterabit DWDM terrestrial transmission with bandwidth-limiting optical filtering, *IEEE J. Sel. Topics Quantum Electron*., vol. 10, pp. 329–340, 2004

[2] G. Charlet, E. Corbel, J. Lazaro, A. Klekamp, R. Dischler, P. Tran, W. Idler, H. Mardoyan, A. Konczykowska, F. Jorge, and S. Bigo, WDM transmission at 6 Tbit/s capacity over transatlantic distance and using 42.7 Gb/s differential phase-shift keying without pulse carver, in Proc. Optical Fiber Communication Conf. (OFC), 2004, Paper PDP36, pp. 1-3

[3] K. Fukuchi, T. Kasamatsu, M. Morie, R. Ohhira, T. Ito, K. Sekiya, D. Ogasahara, and T. Ono, 10.92-Tb/s (273 x 40-Gb/s) triple-band/ultra-dense WDM opticalrepeatered transmission experiment, in Proc. Optical Fiber Communication Conf. (OFC), 2001, Paper PD24, pp. 1684-1686

[4] A. F. Abas, A. Hidayat, D. Sandel, B. Milivojevic and R. Noe, 100 km fiber span in 292 km, 2.38 Tb/s (16×160 Gb/s) WDM DQPSK polarization division multiplex transmission experiment without Raman amplification, *Opt. Fiber Technol*. vol.13, pp. 46-50, 2004

[5] A. Malekmohammadi, M. K. Abdullah, G. A. Mahdiraji, A. F. Abas, M. Mokhtar, M. F. A. Rashid and S. M. Basir, Analysis of return-to-zero-on-off-keying over Absolute Polar Duty Cycle Division Multiplexing in Dispersive Transmission Medium*,* *IET Optoelectron.*, vol. 3, pp. 197–206, 2009

[6] A. Malekmohammadi, A. F. Abas, M. K. Abdullah, G. A. Mahdiraji, M. Mokhtar, M. F. A. Rasid, Absolute Polar Duty Cycle Division Multiplexing over Wave Length Division Multiplexing System, *Optics Communications*, vol. 282, pp. 4233-4241, 2009

[7] M. I. Hayee, M. C. Cardakli, A. B. Sahin, and A. E. Willner, Doubling of bandwidth utilization using two orthogonal polarizations and power unbalancing in a polarization-division-multiplexing scheme, *IEEE Photon.Technol. Lett.*, vol. 13, pp. 881–883, 2001

[8] S. Bhandare, D. Sandel, B. Milivojevic, A. Hidayat, A. A. Fauzi, H. Zhang, S. K. Ibrahim, F. Wust, and R. Noe, 5.94-Tb/s 1.49-b/s/Hz (40 x 2 x 2 x 40 Gb/s) RZ-DQPSK polarization-division multiplex C-band transmission over 324 km*, IEEE Photon. Technol. Lett.* vol. 17, pp. 914-916 , 2005

[9] P. Winzer and R. Jean, Advance modulation formats for high-capacity optical transport networks, *J. Lightwave Technol*. vol 24 pp.4711–4728, 2006

[10] H. Kim and R. J. Essiambre, Transmission of 8 × 20 Gb/s DQPSK signals over 310-km SMF with 0.8-b/s/Hz spectral efficiency, *IEEE Photon. Technol. Lett.*, vol. 15, pp. 769–771, 2003.

[11] C. Xie, I. Kang, A. H. Gnauck, L. Moller, L. F. Mollenauer, and A. R. Grant, Suppression of intrachannel nonlinear effects with alternate-polarization formats*, J. Lightw. Technol.,* vol. 22, no. 3, pp. 806–812, 2004.

 ISBN: 978-1-61208-166-3

Cooperative Clustered Architecture and Resource Reservation for OBS Networks

Ihsan Ul Haq[1,2,3], Henrique M. Salgado[1,2] , and Jorge C. S. Castro[1]

[1]INESC PORTO, Porto Portugal.
[2]Faculdade de Engenharia, Universidade do Porto, Portugal
[3]Dept. of CSE, NWFP University of Engineering & Technology Peshawar, Pakistan
ihaq@inescporto.pt, hsalgado@inescporto.pt, jcastro@inescporto.pt

***Abstract*-- Resource contention is a major concern in Optical Burst Switching networks that leads to relatively high burst loss probability. This article presents a clustered architecture for OBS networks, called Cooperative Clustered Optical Burst Switching (C2OBS) network architecture. In this architecture, the network is divided in overlapping zones/clusters with a zone/cluster head having the knowledge of available resources within the zone called Zonal Information Base (ZIB) and maintains a short resource usage history called Short History Base (SHB). Furthermore, a resource reservation strategy for the proposed Cooperative Clustered OBS network architecture (C2OBS-RR) is also presented which is centralized within the zone and distributed in the overall network, for combining the benefits of both the centralized and the distributed resource reservation schemes. This novel approach uses the zonal state of the resource availability, ZIB, so that the bursts originating at the ingress nodes in the same part of network having been assigned the same wavelength, can be assigned different time offsets. This will proactively reduce the probability of contention at the intermediate nodes within a zone and is expected to significantly reduce the overall network burst loss probability. For illustration purpose, the proposed C2OBS architecture has been applied to the European Optical Network.**

Keywords- Optical Burst Switching; Resource Reservation; Resource Contention Avoidance.

I. INTRODUCTION

Optical Burst Switching (OBS) is a promising technology for supporting the next generation Internet over Dense Wavelength Division Multiplexing (DWDM) network. An OBS network consists of Edge and Core nodes. Edge nodes may be ingress or egress nodes. The edge nodes are the electronic transit points between the burst-switched backbone and the legacy networks. In the existing OBS architecture, the ingress node performs burst assembly, routing, wavelength assignment, signaling and edge scheduling. The main tasks performed by core nodes are signaling, core scheduling, routing/forwarding, and contention resolution. The core nodes are mainly composed of an optical switching matrix and a switch control unit which is responsible to forward optical data bursts [1][2] [3][8].

The ingress node receives packets from the client network, assembles a burst and sends a corresponding Burst Header Packet (BHP) on the control channel. The BHP is received at the input module of core node containing source and destination addresses, burst offset time, burst length and the Class of Service (CoS) of the corresponding data burst. The purpose of the BHP is to reserve the necessary resources at each core node along the path for transmitting the burst. Three reservation schemes have been proposed, namely the Centralized Resource Reservation [4], the Distributed Resource Reservation [5], and the Intermediate Node Initiated (INI) Resource Reservation scheme [6][7].

The Centralized two-way Resource Reservation mechanism proposed in Wavelength Routed OBS networks [4], exploits the knowledge of network wide resources availability to optimize resource reservation, but is more complex to implement and increases the transmission latency due to its two way resource reservation process. The advantages and limitations of this reservation scheme are mentioned in [8].

In the Distributed Resource Reservation mechanism, resources can either be reserved using two-way resource reservation, labeled as Tell-And-Wait (TAW), or one-way resource reservation, designated as Tell-And-Go [8][9] (TAG). TAW relies on establishing a virtual circuit prior to starting burst transmission. More precisely, a BHP is sent from the ingress node towards the egress node to reserve transmission capacity at all the intermediate nodes along a given routing path. When the reservation is successful in the entire path, an acknowledgment message is sent back to the ingress node, which then starts transmitting the data burst. Otherwise, the node detecting resource shortage sends a negative acknowledgment message back to the ingress node to release the reserved resources. Importantly, the delay imposed to data bursts by the resource reservation mechanism, which for TAW is defined as the time elapsed between assembling a data burst and initiating its transmission at the ingress node after receiving the acknowledgment, is equal to or larger than the Round Trip Time (RTT) between the ingress and egress nodes. This is the major limitation of TAW, which may adversely affect the quality of real time delay sensitive traffic.

One-way resource reservation, or TAG, shortens the delay imposed on data bursts by starting the burst transmission shortly after sending the BHP to the core nodes along the routing path without waiting for an acknowledgment of a successful reservation. In this reservation scheme, the reservation may be immediate like in JIT [10], JIT+ [5] and E-JIT [12][13] or delayed as in JET[5] and Horizon [5]. However, in TAG, the burst loss probability is relatively high but end-to-end delay is less

 ISBN: 978-1-61208-166-3

than TAW. Therefore, neither TAG nor TAW reservation schemes can have both low latency and low burst loss at the same time.

In the INI Resource Reservation scheme, the reservation request is initiated at an intermediate node, called the initiating node. In the first part of the path, from ingress node to the initiating node, the INI Resource Reservation works with an acknowledgement for the BHP, similar to TAW, and from the initiating node to egress node, it follows the JET reservation scheme. The burst loss probability with INI is less than with JET, and the end-to-end delay in less than with TAW. However, the selection of the initiating node in INI resource reservation scheme is a critical issue, and may be considered as a bottleneck of the proposed solution [8]. Moreover, the intermediate node does not have knowledge of network wide resource availability and cannot optimize the resources reservation and utilization.

This article proposes a novel clustered architecture (C2OBS) and resource reservation strategy for clustered OBS network (C2OBS-RR). The C2OBS-RR strategy will decrease resource contention, reduce the burst drop probability as compared to TAG, and the reservation waiting time as compared to the centralized reservation scheme and TAW as explained in Section III. In C2OBS, the whole network is divided into overlapping zones with a Zone Head (ZH) and Backup Zone Head (BZH). A centralized reservation scheme is utilized only within the zone exploiting the zonal knowledge of resources available at the ZH, while the distributed reservation is employed across the zones. The purpose of the combined strategy is to overcome the shortcomings of the centralized and the distributed resource reservation techniques, while retaining the best of both approaches where appropriate. Across zones a distributed reservation is employed to reduce overall latency while keeping a centralized approach within the zone for reducing the burst loss probability.

A further improvement included in the C2OBS architecture consists of the utilization of a single shared module of Wavelength Convertors (WCs) and Fiber Delay Lines (FDLs) bank placed either at a central location or at the ZH within each zone for resolving contention within the zone. This solution is also attractive from network planning perspective because this module can be easily enhanced or replaced keeping in view the future estimated traffic load.

The article is organized as follows. In Section II, an enhanced architecture called Cooperative Clustered Optical Burst Switching Network architecture is presented. In this section, the same concept has been applied to the European Optical Network (EON) for illustration. Section III presents the proposed resource reservation strategy for reducing the overall network burst loss probability. This section also provides an application of C2OBS-RR to EON topology for illustration. Section IV discusses the expected benefits of the proposed C2OBS architecture and of the C2OBS-RR strategy by comparing it with the existing resource reservation paradigms. Finally, Section V provides conclusion and highlights future work directions.

II. PROPOSED COOPERATIVE ARCHITECTURE

In the C2OBS architecture, the network is partitioned into overlapping zones/clusters as shown in Figures 1 and 2. The zone is defined in terms of number of hops and not physical distance, because we can limit the dissemination of control information based on the number of hops, by using the Time to Live (TTL) value as in IPv4 header, or the HopLimit value as in the IPv6 header [14]. The zone size should be small to reduce dissemination of control information. Furthermore, the gateway (explained later) does not allow the broadcast "Hello messages" from the Zone Head (ZH) to pass through, as such information is not required in adjacent zones. As the zones are overlapping, there will be one or more nodes that will be part of more than one zone and acts as gateway and backup gateway. For example, in Figure 2, Copenhagen (COP) serves as a gateway among Z-3, Z-4 and Z-5 because it is common to the three zones. Similarly, Prague (PRA) is common between zone two and four and functions as a gateway between these zones. Each zone has a Zone Head (ZH) and Backup Zone Head (BZH). For example, the node at Paris (PAR) is a ZH for Z-1. The ZH keeps the information of all of the nodes within the zone. The BZH duplicates the tasks performed by the ZH, either in case of failure of the ZH or if the ZH is overburdened with other processing tasks like performing the job of a gateway and stops broadcasting its "Hello messages". The role of the ZH is further elaborated in section III. The other members of the zone are referred to as Zone Members (ZMs).

The ZH is dynamically elected with a criterion as the node with the highest degree in the zone. This condition has been imposed because in most cases the ZMs will be directly connected to the ZH and it will be possible for ZMs to communicate with the ZH with the least propagation delay for resource reservation. Furthermore, the ZH needs not to be fixed, because if a node is busier in processing other jobs and cannot efficiently process the ZM's requests, it will leave its role as ZH and BZH will take over its responsibility. As the BZH will become the ZH, other ZMs will take part in election to become BZH and the node with highest degree will win and will become the BZH. Even in case of failure of ZH, the similar procedure will take place.

Each zone will have common shared wavelength convertors (WCs)/ Fiber Delay Lines (FDLs) bank for contention resolution. This shared bank of WCs/FDLs in a zone is our novel idea and has never been proposed in literature as per our knowledge. This shared bank can be installed at a central location as in Figure 1 or may be placed along with of optical switch having highest degree as shown in Figure 2.

Optimal wavelength converter placement in optical networks has been shown to be NP-hard, and many heuristics have been proposed [15], but still this is an open research area. In optical networks, where do we optimally place the WCs/FDLs is a vital question.

 ISBN: 978-1-61208-166-3

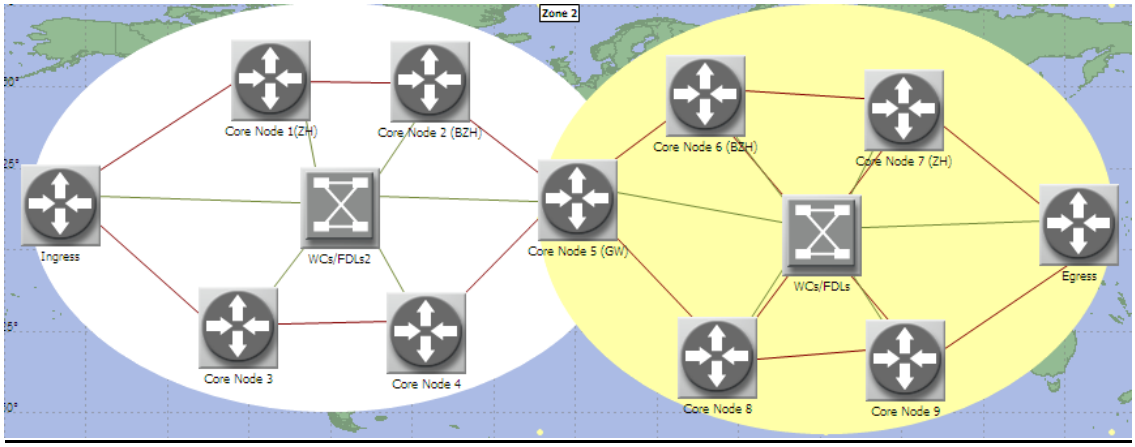


Figure 1. OBS Network Architecture showing ZH, BZH and shared WCs/FDLs

One of the possible solutions is to place the WCs at each output port of the optical switch. This solution is not cost effective as WCs may not be required all the time and it is the wastage of expensive resource. As wavelength convertors are still expensive, providing dedicated wavelength convertors is not a cost effective solution [3][15], the proposed shared WCs/FDLs bank architecture provides a reasonable solution for placement of WCs in OBS network. The WCs/FDLs bank can be accessed by any incoming burst that needs wavelength conversion/buffering. This will also make the network planning simpler and economical because this module can be upgrade as per requirement keeping in view the future increase in traffic without upgrading/replacing the optical switches. This shared architecture will also improve the utilization of this resource (WCs/FDLs) because all the nodes within the zone will use the same resource for wavelength conversion and optical buffering. This will make the OBS networks economically more feasible as augmenting each node with WCs/FDLs is an expensive solution [15]. Although, the use of WCs/FDLs will be minimized as much as possible by using effective resource reservation scheme explained in the next section and this will act as a last resort to save the burst from blocking. In this way, the requirement for number of WCs/FDLs will be reduced, which is technically and economically more attractive.

The proposed architecture has been named Cooperative Clustered Optical Burst Switching architecture because the Gateway nodes in the network cooperate for successful resource reservation in the adjacent zone and tries to reduce the burst blocking probability.

As an illustration, the clustered network architecture model has been applied to European Optical Network (EON) topology [16][17] as shown in Figure 2. The EON topology consists of 20 nodes and 38 links. The network has been divided into five zones (Z-1 to Z-5) and detail about the role of each node in the zone is depicted in Table 1. The table shows the status of each node in its respective zone, i.e. whether the node is Zone Head (ZH), Zone Member (ZM) and Gateway (GW). It also indicates the degree of the node in the network, which is a key selection criterion for the role of ZH. In Figure 2, the WCs/FDLs bank has been shown along with the ZH and the circle, oval and cloud shapes has been used to represent different zones in EON and has been labeled as Z-1 to Z-5.

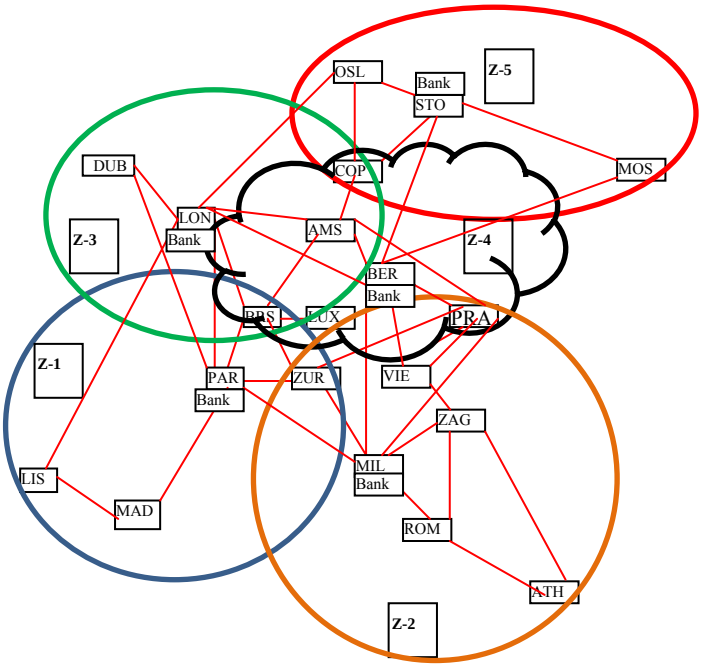


Figure 2. Cooperative Clustered OBS Network Architecture for EON

Table.1. Node Description of EON

S.No	Location of Node	Zone Member	Member Status	Degree of Node
1.	Libson (LIS)	Z-1	ZM	2
2.	Madrid (MAD)	Z-1	ZM	2
3.	Paris (PAR)	Z-1	ZH	**6**
4.	Brussels (BRS)	Z-1, Z-3 & Z-4	ZM & GW	5
5.	Zurich (ZUR)	Z-1 & Z-2	ZM & GW	4
6.	Athens (ATH)	Z-2	ZM	2
7.	Rome(ROM)	Z-2	ZM	3
8.	Zagreb (ZAG)	Z-2	ZM	4
9.	Vienna (VIE)	Z-2	ZM	3
10.	Milan (MIL)	Z-2	ZH	**6**
11.	Prague (PRA)	Z-2 & Z-4	ZM & GW	5
12.	London (LON)	Z-3	ZH	**7**
13.	Dublin (DUB)	Z-3	ZM	2
14.	Amsterdam (AMS)	Z-3 & Z-4	ZM & GW	5
15.	Berlin (BER)	Z-4	ZH	**7**
16.	Luxemburg (LUX)	Z-4	ZM	1
17.	Copenhagen (COP)	Z-5 & Z-3	ZM & GW	3
18.	Moscow (MOS)	Z-5	ZM	2
19.	Stockholm (STO)	Z-5	ZH	**4**
20.	Oslo (OSO)	Z-5	ZM	3

III. PROPOSED RESOURCE RESERVATION STRATEGY

The C2OBS-RR scheme utilizes centralized reservation for intra-zonal traffic. Centralized reservation is also used for inter-zonal traffic between the ingress node and the zone gateway. Then the gateway prompts the next ZH which becomes responsible for reserving the necessary resources for the upcoming burst. The process is repeated until the burst reaches the zone where the egress node is located.

Although resource reservation is centralized within each zone, it may also be considered as distributed for inter-zonal traffic because a degree of cooperation is required among multiple ZHs and gateways.

In the C2OBS-RR scheme, the ZH acknowledges the BHP by consulting its Zone Information Base (ZIB) and Short History Base (SHB) thereby reducing delay compared to wavelength routed OBS (WROBS) which requires end-to-end acknowledgement [4].

Moreover, while also employing distributed reservation for inter-zonal traffic, the proposed strategy does not require end-to-end acknowledgement like Tell & Wait (TAW) thus reducing delay, and uses zonal knowledge for resource reservation, thereby reducing the burst loss probability compared to Tell & Go (TAG).

For intra-zonal traffic, the ingress node requests resources from the ZH by transmitting a BHP using a control channel. The ZH consults both its Zone-Base, for assigning route and free wavelength, and its Short History Base (SHB) to assign a suitable offset time for avoiding contention at the intermediate core nodes. The SHB is dynamically updated with offset times assigned to bursts as the transmissions from different ingress nodes proceed within the zone. The ZH acknowledges the BHP by transmitting amended BHP containing information about offset time, routing and wavelength assignment for the incoming burst transmission, which is estimated/predicted based on knowledge inferred from the data stored in the ZH. The same amended BHP is forwarded to the intermediate nodes and the egress node for the necessary switching configuration. The routing and wavelength assignment problem has been dealt with in a separate article in detail while the suitable offset time issue is discussed below.

The minimum offset time can be given by [5][7]

$$T_{offset}^{\min} = kT_{BHP} + T_{SW} \quad (1)$$

where k is the number of hops along the path from the ingress node to the egress node, T_{BHP} is the header processing time, and T_{SW} is the switch configuration time. However, the ingress node may also use a larger value for service differentiation [5][18], if necessary.

In the C2OBS-RR strategy the ZH calculate T_{offset}^{total} by looking at the ZIB for the number of hops in the burst route. Then, for avoiding contention it calculates an extra offset time δT by looking for all previously scheduled channels in the SHB. The extra offset is meant to isolate traffic form different ingress nodes that are using overlapping paths. The total offset time for the burst can be finally given by

$$T_{offset}^{total} = kT_{BHP} + T_{SW} + \delta T \quad (2)$$

The ZH forwards the amended BHP to the ingress node and multicasts the same to the intermediate nodes in the zone for resource reservation. Upon receiving the amended BHP multi-casted by the ZH, the intermediate nodes check the value of δT and their location in the routing path and assign that value to k. The parameter k has a different meaning for both the ingress nodes and intermediate nodes. For the ingress node and intra-zonal traffic, k represents the number of hops along the path from the ingress node to the egress node while for inter-zonal traffic, it represents the number of hops from the ingress node to the zone gateway. For intermediate nodes, the node checks its position within the routing path and assigns that value to k. The intermediate nodes perform delayed reservation by using equation (2) and knowledge of both T_{BHP} and T_{SW} to calculate the burst arrival time.

 ISBN: 978-1-61208-166-3

Early release is also used as the amended BHP informs about the burst length.

For the inter-zonal traffic, the ingress node also starts off by requesting resources from its own ZH. The ZH assigns a free wavelength, a suitable offset time and a route only up to the zone gateway, and amends the BHP with this information. The amended BHP is also forwarded by the ZH to all intermediate nodes till the zone gateway. Then, it is the gateway's responsibility to cooperate with the ingress node for reserving resources in the next zone, by forwarding the amended BHP to the next ZH (NZH). Subsequently, the NZH assigns the necessary resources for the upcoming burst, and the zone by zone reservation procedure is repeated until the burst reaches the zone where the egress node is located.

A. *An Application of the C2OBS-RR to the EON Topology*

In the following, the C2OBS-RR scheme is applied to the EON topology as depicted in Figure 2 for illustration. The assignment of nodes to each zone has been described in section II.

In case of intra-zonal traffic say within zone-one (Z-1) from Lisbon to Zurich, the ingress node at Lisbon sends a BHP including burst length, Class of Service (CoS) and source and destination addresses to the ZH (Paris). The ZH inspects the BHP and examines both its Zonal Information Base (ZIB), for routing and wavelength assignment, and its SHB for assigning a suitable offset time. The ZH returns the amended BHP to the ingress node and multicasts the same to intermediate nodes. The amended BHP adds information to the BHP about route, i.e., LIS-MAD-PAR-ZUR, a free wavelength along the route, say λ_1, and suitable offset time for the ingress node. The intermediate nodes and destination calculate the offset time as explained above and reserve the resources using delayed reservation. The ingress node transmits the burst after the offset time elapses, which propagates transparently along the route to the destination. As the burst passes through the intermediate nodes, the resources are released and the ZH updates its SHB accordingly so that the resources may be assigned efficiently to other subsequent burst.

In case of the inter-zonal traffic, e.g., for traffic from Lisbon (Z-1) to Amsterdam (Z-3), the last address along the path will be the zone gateway's address, Brussels, which is a member of both Z-1 and Z-3. As the gateway node (Brussels) receives the amended BHP with the destination address of Amsterdam (egress node), it forwards the BHP to the next Zone Head (NZH), London, with the information about the wavelength on which the burst will arrive. This wavelength is considered as "preferred" wavelength by the NZH. The NZH, looking at the destination address and preferred wavelength channel information in the BHP, checks its own ZIB, and classifies the traffic as intra-zonal or inter-zonal. Since the traffic is now intra-zonal, the NZH checks both its ZIB and SHB to decide whether the same wavelength channel is available on the path within the new zone. If it is available, the NZH returns the amended BHP to the gateway and multicasts the same BHP to the intermediate nodes and egress node (Amsterdam) for resource reservation. If the preferred wavelength channel is not free, the NZH checks the CoS of the burst to find whether the incoming burst belongs to either delay insensitive or delay sensitive class of service. For delay insensitive class, the NZH adds a suitable δT to the calculated offset time using equation (2) and directs the incoming burst to the shared FDL bank. For delay sensitive class, it assigns a new free wavelength to the incoming burst and directs it to the shared WCs bank. This reduces delay for delay sensitive traffic, thus ensuring Quality of Service provisioning. When the data burst arrive at the gateway, it is transparently forwarded towards the egress node.

In summary, the strategy of the C2OBS-RR scheme for contention avoidance is that the ZH should provide a routing path with a free wavelength, and an appropriate offset time to each burst to isolate traffic originating from different ingress nodes using overlapping paths.

IV. EXPECTED BENEFITS of C2OBS

The aim of this section is to discuss the expected benefits of the C2OBS architecture & the C2OBS-RR strategy and compare it with the extant reservation schemes. In C2OBS, the whole network has been divided into more manageable smaller units called zones, with a ZH that maintains both a ZIB and a SHB. The information contained in both these information-bases is utilized for effective reservation of resources. The C2OBS-RR strategy aims to lessen the inherent problems of both centralized and distributed resource reservation techniques while combining the best features of both approaches. The centralized two way resource reservation technique introduces longer delays, is more complex and adds more processing burden on a central node than the one way reservation technique. On the other hand, the distributed resource reservation schemes suffers from a relatively high burst loss probability because nodes have only partial knowledge about resource availability limited to its outgoing links.

The C2OBS-RR will have a shorter delay and will be easier to implement than the centralized reservation scheme because the ZH is normally located only one hop away from the ingress nodes within the zone and the processing burden is shared by multiple ZHs. On the other hand, the C2OBS-RR approach will have less wavelength contention compared to the distributed resource reservation schemes, because the ZH takes advantage of its complete resource availability knowledge within the zone for assigning suitable offset times such that contention is avoided among bursts using partially or totally overlapping paths.

As compared to the centralized reservation scheme, where all resource assignment is accomplished by a single central node, the proposed scheme is following a distributed strategy having ZHs in each zone for resource assignment and reservation. In the case of the centralized reservation

 ISBN: 978-1-61208-166-3

scheme, when the central node fails, the whole network performance will be affected. So the central node becomes a performance bottleneck in the network. In contrast, in the C2OBS architecture and the C2OBS-RR scheme, failure of a ZH will affect a single zone within the network till the BZH takes the responsibility of ZH.

A further advantage of the proposed architecture is its scalability. If the number of nodes in the network is increased, the network can be redesigned by either adding the new node to an existing zone or creating a new zone to maintain the network performance. However, the distributed reservation protocols such as JET, JIT, JIT+, or E-JIT are not flexible to accommodate further nodes without deteriorating the network performance. Furthermore, the central node in case of central reservation scheme has a limited processing capability. The number of nodes offering load beyond this processing capacity will worsen the performance of the network as well.

Wavelength convertors are still immature and expensive, full wavelength conversion (i.e., any wavelength entering a node can exit on any free wavelength on any output fiber) [3][18] is still not a realistic solution. The alternative solution is to place the wavelength convertors sparsely. Optimal placement of sparse wavelength convertors in optical networks is a vital question but it has been shown to be NP-hard. The proposed shared WCs bank in the zone is comparatively a more feasible alternative because the WCs bank is either placed at a central location or at a node having the highest degree in the zone, which will mostly provide direct connectivity between any switching nodes and the bank. This solution is also attractive from network planning perspective because this module can be easily enhanced or replaced keeping in view the future estimated traffic load. In existing architecture where wavelength convertors are an integral part of the switch, there is no such flexibility.

Finally, in the proposed resource reservation strategy, the ingress node does not have to wait for resource reservation acknowledgment as in TAW where acknowledgement delay is equal to RTT between ingress & egress node. Additionally, unlike the central reservation scheme, the ingress node does not have to wait for RTT between ingress node and central node for resource confirmation. In this work, the ZH is mostly available at one hop from the ingress node as the ZH has a highest degree in the zone; the latency is comparatively low as compared to TAW and central reservation technique which is comparatively suitable for real time delay sensitive traffic.

Based on the above comparative analysis with existing reservation techniques, it appears that the proposed scheme is both more flexible and scalable. It is also expected that the C2OBS-RR will offer less delay as compared to TAW and centralized reservation schemes. Moreover, the blocking probability is also expected to be lower than that of TAG (JET, JIT, JIT+, E-JIT, and Horizon).

V. CONCLUSION AND FUTURE WORK

In this article, a divide and conquer approach has been applied to OBS networks by splitting the whole network into more manageable small units called zones. Each zone has a Zone Based information repository and Short History Base in the Zone Head. The ZIB contains information about routing and wavelength assignment while SHB dynamically records information about scheduled channels. Since it is not realistic to provide full wavelength conversion in the optical networks, an improvement in the network architecture has been suggested by implementing the bank of WCs/FDLs as a separate module from the switch within the zone and all zone members can use the same bank when required.

A resource reservation strategy for C2OBS network architecture with the focus on gathering the advantages of both the centralized and the distributed reservation mechanism has been presented. It will help to reduce the burst drop probability. The innovative methodology uses the zonal state of resource availability in the zone such that the bursts at the ingress nodes in the same part of the network, having being assigned the same wavelength, are assigned different offset to avoid contention.

It is expected that the proposed scheme will shorter the delay and will be easier to implement then the reservation scheme proposed for WROBS networks. Furthermore, it will have less probability of wavelength contention at the intermediate nodes as compared to distributed resource reservation schemes. The proposed scheme appears more scalable and flexible as compared to both extent centralized and distributed schemes.

As for as future work is concerned, the next objective is to implement a simulation model for analyzing the performance of the C2OBS network architecture and the C2OBS-RR strategy, and compare it with the extant resource reservation schemes for verification and validation.

ACKNOWLEDGEMENT

The authors wish to acknowledge the support of FCT (Ministry of Science, Technology and Higher Education, Portugal), under the Associated Laboratory contract with INESC Porto, Portugal.

REFERENCES

[1] C. Siva Ram Murthy and Mohan Gurusamy, "WDM Optical Networks: Concepts, Design and Algorithms" Prentice Hall PTR, 2002.

[2] Jason P. Jue and Vinod M. Vokkarane, “Optical Burst Switching Networks”, Springer Science + Business Media Inc, 2005

[3] Biswanath Mukherjee, “Optical WDM Network”, Springer Science + Business Media Inc, 2006.

[4] Polina Bayvel, “Wavelength-Routed or Burst-Switched Optical Networks,” 3rd International Conference on Transparent Optical Networks, 2001, Page 325.

 ISBN: 978-1-61208-166-3

[5] Jing Teng and George N. Rouskas, " A Detailed Analysis and Performance Comparison of Wavelength Reservation Schemes for Optical Burst Switching Networks", Photonic Network Communications, vol. 9, no. 3, 2004,Page(s) 311-335.

[6] R. Karanam, V.Vokkarane, and J. Jue, "Intermediate Node Initiated (INI) Signaling: A Hybrid Reservation Technique for Optical Burst Switched Networks", Optical Fiber Communication Conference, 23-28 March 2003, Page(s) 213-215.

[7] Joel J.P.C. Rodrigues and Binod Vaidya, "Evaluation of Resource Reservation Protocols for IP over OBS Networks", 11th International Conference on Transport Optical Networks, 28th June to 2nd July 2009, Page(s) 1-4.

[8] Ihsan Ul Haq, Henrique Salgaso, and Jorge Castro, "Survey and Challenges for Optical Burst Switching Networks: A High Data Rate Network for Future Internet" 2nd International Conference on Intelligence and Information Technology, 28-30 October, 2010, Lahore, Pakistan, Page(s) 381-386.

[9] I. Widjaja, "Performance Analysis of burst admission control protocols, IEEE Proceeding- Communications, vol. 142, no. 1, 1995, Page(s) 7-14.

[10] I. Baldine, George N. Rouskas, H.G. Perros, and D. Stevenson, "JumpStart: A Just-in-Time Signaling Architecture for WDM Burst Switched Networks" IEEE Communications Magazine, vol. 40, no. 2, 2002, Page(s) 82-89.

[11] Joel J.P.C. Rodrigues, Mario M. Freire, Nuno M. Garcia, and Paulo M.N.P Monteiro, "Enhanced Just-in-Time: A New Reservation Protocol for Optical Burst Switching Networks", 12th IEEE Symposium on Computer and Communications, 1- 4 July 2007, Page(s) 121-126.

[12] Joel J.P.C. Rodrigues and Mario M. Freire, "Performance Assessment of Enhanced Just-in-Time Protocol in OBS Networks Taking into Account Control Packet Processing and Optical Switch Configuration Times", 22nd International Conference on Advanced Information Networking and Applications- Workshop, 25-28 March 2008, Page(s) 434 – 439

13] Yang Chen, Chunming Qiao, and Xiang Yu, "Optical Burst Switching: A New Area in Optical Network Research", IEEE Network, vol. 18, no. 3, May-June 2004, Page(s) 16-23.

[14] Larry L. Peterson and Bruce S. Davie, "Computer Networks: A Systems Approach" 3rd Edition, 2003, Morgan Kaufmann Series in Networking.

[15] Bo Li and Xiaowen Chu, "Routing and Wavelength Assignment vs Wavelength Converter Placement in All-Optical Networks", IEEE Communication Magazine, vol. 41, no. 6, 2003, Page(s) 522-528.

[16] M.J.O' Mahony, "A European Optical Network: Design Considerations", IEEE Colloquium on Transport Optical Networks: Applications, Architectures and Technology, 1994, Page(s) 1-6.

[17] M.J.O' Mahony and D. Simeonidou, A. Yu, and J. Zhou, "The Design of a European Optical Network", Journal of Lightwave Technology, vol 13, no. 5, May 1995, Page(s) 817-828.

[18] Kee Chiang Chua, Mohan Gurusamy, Yong Liu, and Minh Hoang Phung, "Quality of Service in Optical Burst Switched Networks", @007 Springer Science + Business Media, LLC.

 ISBN: 978-1-61208-166-3

Performance Evaluation of the Nanosecond Resolution Timestamping Feature of the Enhanced Libpcap

Peter Orosz, Tamas Skopko, Jozsef Imrek
Faculty of Informatics
University of Debrecen
Debrecen, Hungary
e-mail: oroszp@unideb.hu, skopkot@unideb.hu, mazsi@unideb.hu

***Abstract* — In a previous work we modified the libpcap library in order to feature nanosecond resolution timestamping. However the precision and the accuracy of this high resolution software based solution has not been investigated so far. Since very short inter-arrival times are present on Gigabit Ethernet links, the precision of the software based timestamps generated for each incoming packet should be analyzed and validated. In this paper, the performance metrics of the nanosecond resolution software timestamping is compared to a hardware-based solution (Endace DAG3.7GP measurement card) and to a reference source. The factors that determine and limit the precision and accuracy of the nanosecond resolution software timestamping will be investigated. We present how the operation mode of the network device driver affects the timestamping behavior.**

Keywords-libpcap; timestamp precision; inter-arrival time; Linux kernel; high speed network; hardware timestamping.

I. INTRODUCTION

Measurement of high performance networks requires high performance timestamping [1][2]. Using libpcap based capturing limits both the resolution and the precision of the generated timestamps [3]. Although in a recent work we enhanced the timestamping resolution of the original libpcap library [4], it is hard to improve the precision of the nanosecond resolution software based timestamping to meet the needs of the Gigabit Ethernet and faster networks. Even with the most sophisticated optimization, the precision of the software timestamp could not compete with the hardware based one [5]. In this paper, we will investigate the precision of the high resolution timestamping feature of the enhanced libpcap library. A widely used high performance Gigabit Ethernet NIC (Network Interface Card) and driver combination was selected for our measurements. According to the result of the investigation, the question arises with good reason: Is there any measurement type where the application of nanosecond resolution software timestamping is reasonable? To answer this question, we performed comparative measurements: one test setup was assembled for fixed packet size generated at high, fixed rate and the other one for replayed VoIP traffic including variable packet size. Measurement with fixed packet size and inter-arrival time is suited to analyze the deviation of inter-arrival times presented by the generated timestamps. Whereas replayed traffic consisting of packets with variable sizes is adapted to show how precisely the high resolution software timestamping could represent traffic characteristics.

II. MEASUREMENT SETUP

In both measurements two independent hosts were used: one for software timestamping and the other one for reference hardware timestamping, with both systems simultaneously capturing the same traffic. In every measurement we made sure that no packet loss occurred.

A. *Line-rate traffic generator*

In our first measurement setup a NetFPGA-1G card [6] was used for mirroring the ingress traffic on its PORT A to two of its Gigabit Ethernet ports (PORT B and PORT C). An FPGA (Field Programmable Gate Array: Xilinx Virtex-4 FX12) based configurable line-rate packet generator device was connected to the PORT A of the NetFPGA-1G board. PORT B was connected to an Endace DAG 3.7GP monitoring card (installed in a dedicated host) [7], and PORT C was connected to an Intel PRO/1000 PT Gigabit Ethernet network interface card (Fig. 1) [8].

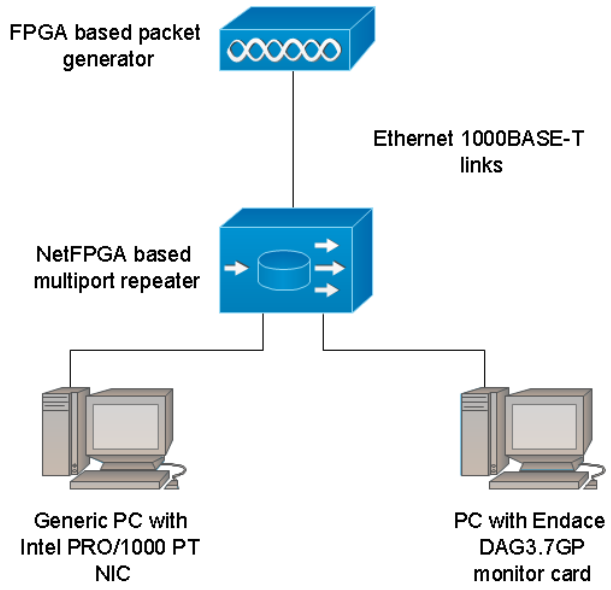


Figure 1. Layout of the first measurement setup

 ISBN: 978-1-61208-166-3

The packet generator was controlled by UDP packets using a proprietary protocol sent from the NetFPGA-1G host. Our NetFPGA-1G loopback module makes it possible to directly loop back certain ports of the board to other ones with a minimal, fixed amount of latency, using no store-and-forward mechanisms.

In this configuration, any traffic received by PORT A is directly forwarded to PORT B and C but not the traffic transmitted on PORT A (which was used to send control packets to the generator). Software timestamps were created based on a TSC clock source by capturing on the Intel PRO/1000 NIC, and Endace's hardware timestamping feature was used to create reference timestamps on the DAG board [9].

B. *NetFPGA-1G multiport packet generator*

In the second setup, we utilized an existing NetFPGA.org project ("Packet generator" [10]) as to perform another measurement series using variable packet size. This generator can replay any previously recorded stream of packets stored in PCAP format. In this setup, the NetFPGA's PORT B was connected to the Endace DAG3.7GP and its PORT C was connected to the Intel PRO/1000 NIC (Fig. 2).

For these measurements the Packet Generator code was loaded into the NetFPGA-1G board, and it was configured to send the same traffic stream on both PORT B and PORT C. Similarly to the previous configuration, the host with the Intel PRO/1000 NIC captured packets with software timestamps based on the system's TSC clock source and the other host with the DAG3.7GP board provided the reference hardware timestamps.

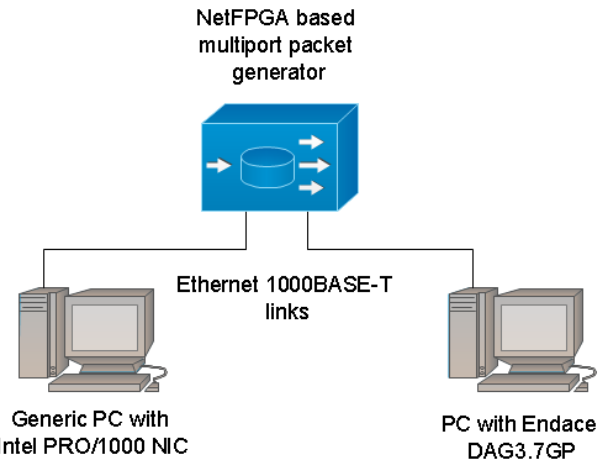


Figure 2. Layout of the second measurement setup

All of the measurements were performed on a non-preemptive 2.6.35.7 Linux kernel.

III. MEASUREMENT RESULTS

It is important to note that hardware timestamps show inter-arrival times of the packets as seen in the MAC layer. In contrast, the software based timestamps represent the time of the enqueuing of the received packets into the Linux kernel's input packet queue [11].

Nevertheless, there is an obvious difference between the hardware and software timestamps in absolute time since their generation occurs at different points of the data path.

Parameter settings of the Intel e1000e Linux driver for the Intel PRO/1000 NIC family affect the kernel-level processing of Ethernet frames, and therefore the generation of software timestamps. The interrupt-handling parameters of the driver can be tuned at module loading. The increasing rate of the received packets increases the rate of the interrupts as well, and this increased number of interrupts can be served by the processor only up to a certain threshold value. Above this threshold more frames should be transmitted to the kernel within one interrupt to maintain the lossless packet reception.

The *InterruptThrottleRate* parameter of the driver and the incoming packet rate together defines the timing of frame processing. When the value of *InterruptThrottleRate* is 0, there is no critical value for the interrupt rate above, which the driver would explicitly decrease their number by transmitting more frames from the card to the kernel during an interrupt (i.e., no coalescing occurs). This is the classic one frame per interrupt mode, which works well with low packet rate and provides low latency, but leads to the exhaustion of hardware resources when traffic load is heavy. To avoid this exhaustion dynamic modes can be used: *InterruptThrottleRate=1* and the conservative *InterruptThrottleRate=3* modes. For more details on the interrupt throttling modes of the Intel E1000E Linux driver, see [12].

The measurements were performed in all three modes of the Intel device driver. The advantage of the nanosecond resolution timestamping recurs significantly with low packet inter-arrivals (i.e., high packet rate and small packet size). However, the nanosecond resolution does not guarantee precision with a similar magnitude at all. Besides that the generation cost of software timestamps in CPU time is significantly higher than the hardware timestamp's production, the length of generation time can display notable fluctuations. The main reason for this can be traced back to shared hardware resources. The timestamp is created in the kernel context, the execution of the producing function call series are being scheduled similarly to every other kernel process. Furthermore, the process of the timestamp-creation can be suspended, e.g., by a hardware interrupt. These factors all contribute to the apparent high fluctuations of inter-arrivals represented by the timestamps. In order to avoid preemption of the execution of the timestamping kernel code, all of our measurements were performed using a non-preemptive Linux kernel.

 ISBN: 978-1-61208-166-3

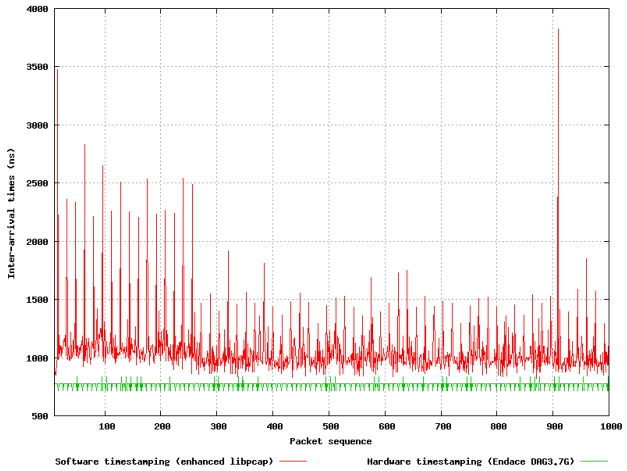


Figure 3. Packet inter-arrival times for IFG=12 bytes and InterruptThrottleRate=0. Green line represents the inter-arrival times measured by the Endace DAG board, while the red line shows the inter-arrival times measured by the enhanced libpcap.

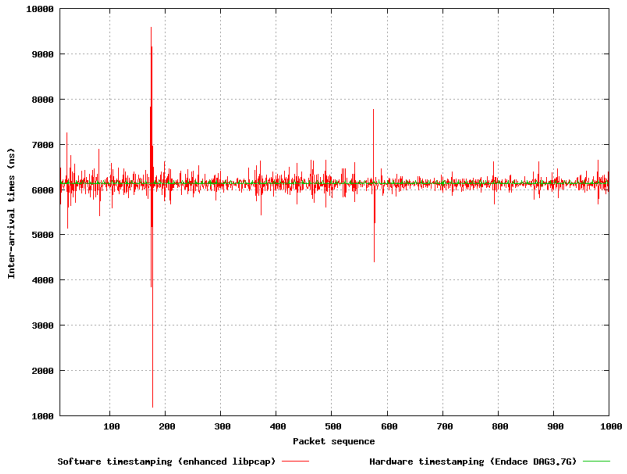


Figure 4. Packet inter-arrival times for IFG=684 bytes and *InterruptThrottleRate=0*

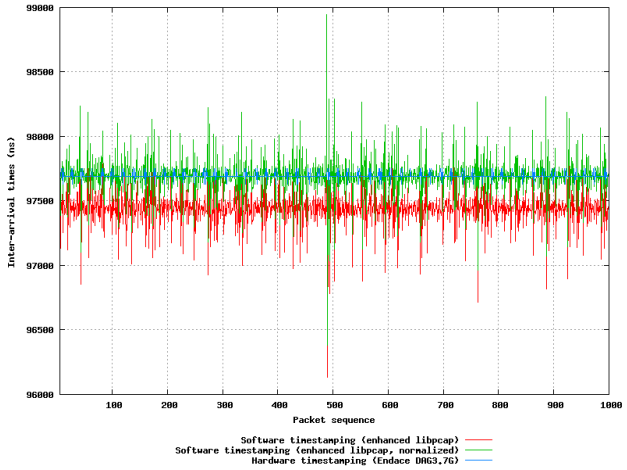


Figure 5. Packet inter-arrival times for IFG=12188 bytes and *InterruptThrottleRate=0,* normalized software timestamps

The traffic generator used in the first measurement environment generates line-rate packet sequences with a fixed packet size and IFG (inter-frame gap) value. Due to the traffic being generated in hardware, the inter-arrival times of the packets are constant. The FPGA traffic generator's clock signal is 125 MHz (nominal), resulting in a 8 ns clock signal period. In case of Gigabit Ethernet network the minimum of packet inter-arrival times is 672 ns.

During the measurements a fixed packet size (72 bytes, excluding the 8-byte preamble and 4-byte CRC fields) was used together with the following IFG values: 12, 684 and 12128 bytes. In fact, the packet size and the IFG value together define the arrival rate, which, according to our presumptions directly affects the Intel NIC driver's operation.

Every measurement was carried out using traffic data consisting of 1000 packets with the parameters described above. During the measurements the focus was on the arrival intervals of the packets, thus relative timestamps were used.

The resolution of the timestamps generated by the Endace DAG3.7GP monitor card is 60 ns. The inter-arrival times indicated with green on the figures were calculated on the bases of hardware timestamps.

Figure 2, 3, and 4 show a ±60 nanosecond (±1 clock) deviation of the packet arrival-intervals, which is caused by the fact that the traffic generator and the Endance measurement card are running on asynchronous (unrelated) clocks.

A. Packet reception with no interrupt throttling

When the Intel e1000e driver runs with *InterruptThrottleRate=0* parameter, it does not apply interrupt moderation. The arrival intervals calculated from the software timestamps showed large deviation regardless of the measurements, they could not produce the estimated 672 ns Δt values in case of 12-byte IFGs as expected (Fig. 3) [13][14]. The reason for this is that it takes more time to generate the software timestamps than the inter-frame arrival times. The short burst of the 1000 packets used for the measurement was stored in the device driver's ingress queue (in the DMA buffer area allocated by the driver), and the packets were moved into the input packet queue of the Linux kernel's network stack in a pace determined by the execution time of the timestamp generation and other additional housekeeping duties associated with packet reception.

As it clearly shows on Figure 3, the Intel e1000e driver has an adjustment period (the first 260 packets, approx.) according to which it configures the interrupt parameters. Thereafter the deviation of the timestamps is reduced significantly; however, it is not at all free of unexpected peaks (around the 900th packet). Each of the inter-arrival times derived from the software timestamps represents higher values compared to the hardware based arrival

 ISBN: 978-1-61208-166-3

times, which could lead to packet loss in a long term measurement.

This phenomenon is almost impossible to eliminate in case of software timestamping due to the kernel pacing and the interruptions during the course of operation. The frequency of these kinds of peaks increases during longer measurement periods. In the second measurement (IFG=684 bytes) the mean value of the inter-arrival times based on software timestamps aligns with the values calculated on the basis of hardware timestamps, but their deviation magnitude lies within the microsecond-range (Fig. 4). The third measurement shows similar results to the second one in terms of timestamp deviation, however the mean values has an obvious difference (Fig. 5). The reason for this can be traced back to the fact that the host with software timestamping and the Endace measurement card are running on asynchronous (unrelated) clocks.

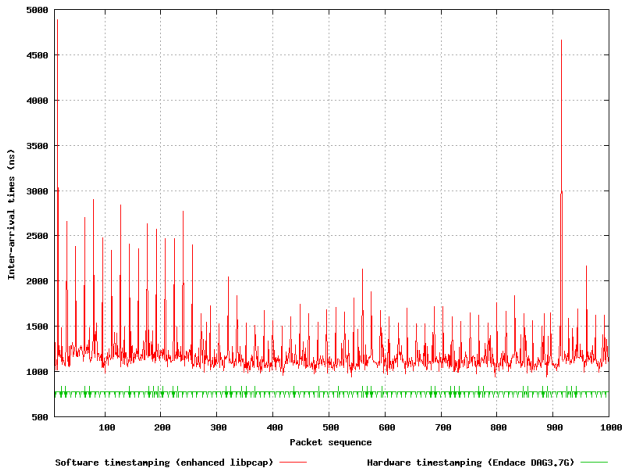


Figure 6. Packet inter-arrival times for IFG=12 bytes and *InterruptThrottleRate=1*

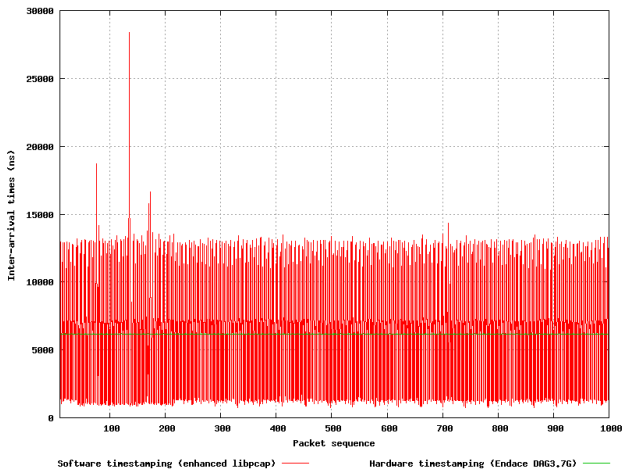


Figure 7. Packet inter-arrival times for IFG=684 bytes and *InterruptThrottleRate=1*

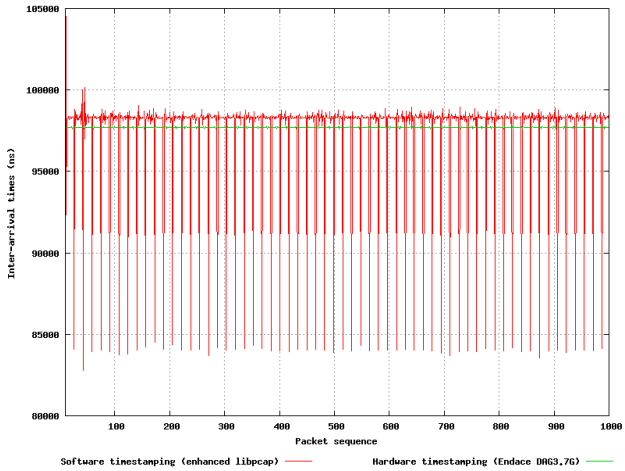


Figure 8. Packet inter-arrival times for IFG=12188 bytes and *InterruptThrottleRate=0*

Accordingly, the Endace DAG hardware clock was designated for reference clock that the software timestamp sequences have to be normalized to. We calculated the average of the Δti (time difference between the arrival of the ith and 1000 – 50 + ith, where i=0…49) for both the software and hardware packet sequences. The quotient of the averages resulted in a normalizing constant, which was used to correct the software based timestamps (Fig. 5).

B. Packet repection with dynamic interrupt throttling

When the *InterruptThrottleRate* parameter of the e1000e driver is 1, the driver adjusts to the incoming traffic rate by dynamically tuning the value of the interrupt moderation (polling mode).

In case of high arrival rate (IFG=12 bytes) the precision of the software timestamps deteriorates compared to the zero-throttle mode used in the previous measurement series (Fig. 6).

The advantage of the polling mode in case of heavy traffic is the lower hardware resource requirement. In case of polling mode the inter-arrival times defined by software timestamps reflect the polling mechanism's frame enqueuing rate and timing rather than the temporal relation experienced on the MAC level.

At lower arrival rate the results gathered from the hardware and software timestamping are significantly different. With higher IFG it is more conspicuous that due to the polling-based processing the timestamps reflect the enqueueing time intervals of the incoming frames rather than the MAC-level time intervals (Figs. 7, 8). The question emerges whether the high resolution (1 ns) context-dependent timestamping mechanism combined with a polling-based NIC driver can be used for high speed traffic analysis.

For measuring the time relation of the frames as seen in the MAC layer the right solution is clearly the high resolution and precision hardware timestamping. However, if we are interested in the frame arrival interval

 ISBN: 978-1-61208-166-3

to the kernel, the relevant information can be gathered from the software timestamps produced by the kernel.

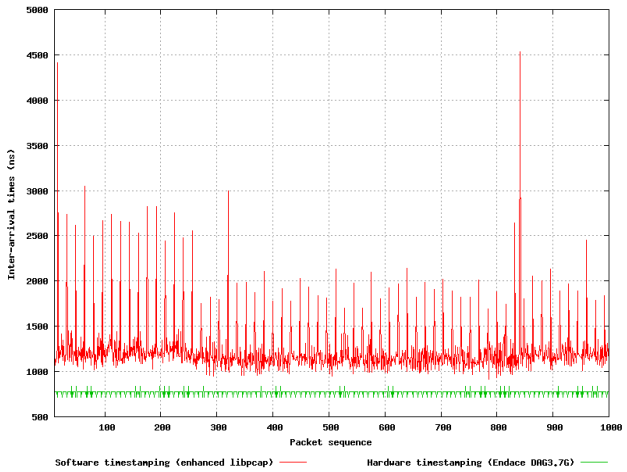


Figure 9. Packet inter-arrival times for IFG=12 bytes and *InterruptThrottleRate=3*

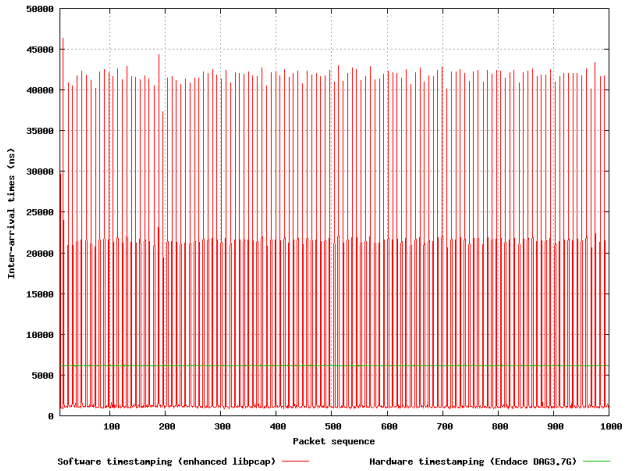


Figure 10. Packet inter-arrival times for IFG=684 bytes and *InterruptThrottleRate=3*

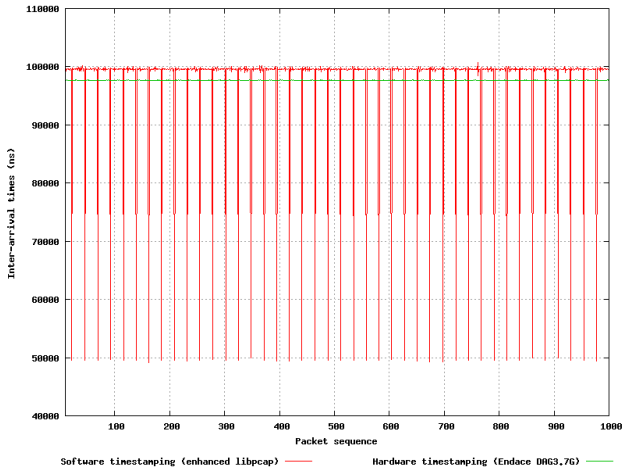


Figure 11. Packet inter-arrival times for IFG=12188 bytes and *InterruptThrottleRate=3*

C. *Packet reception with conservative dynamic interrupt throttling*

The results of the measurements with *InterruptThrottleRate=3* settings show that the lack of low latency processing significantly increases the deviation of the measured arrival intervals (Fig. 9).

The resulted maximum of arrival intervals develops between those consecutive frames, which were processed in two time adjacent interruption contexts. Meanwhile, due to the polling mechanism the arrival interval of the frames processed consecutively during one interrupt are much closer to each other. This low value is derived solely from the host's processing latency: enqueueing and timestamping (Figs. 10, 11). Nevertheless, contrary to the conventional microsecond resolution the high resolution software timestamping of the packets can represent the arrival moment of the packets to the operation system with higher accuracy.

D. *Replayed VoIP traffic*

In the second round of the investigation a measurement environment was created where arbitrary, previously recorded traffic samples could be replayed, while preserving the original packet inter-arrival times.

Variable packet size was the primary aspect in choosing the PCAP traffic sample. The aim of this measurement series was to examine the accuracy of the high resolution software timestamps generated by replaying and capturing a real VoIP traffic sample (RTP transmission with G.711 audio data).

As it is apparent from the results of measurements performed with *InterruptThrottleRate=0* settings, even though the arrival intervals defined by software timestamps have larger deviation, in this case they can reflect the time relation denoted by the hardware timestamp sequence (Fig. 12).

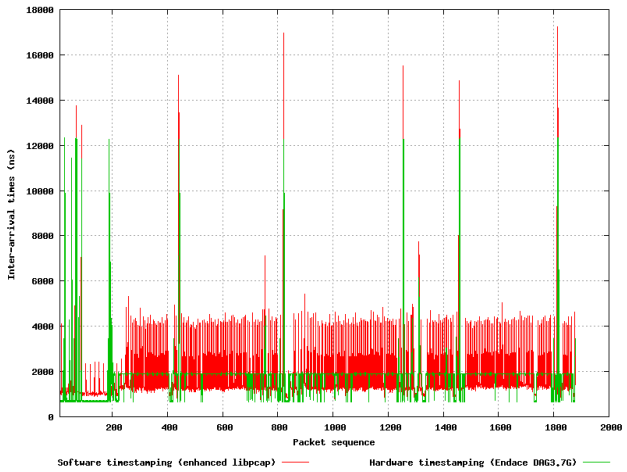


Figure 12. Packet inter-arrival times for *InterruptThrottleRate=0* (variable packet size)

 ISBN: 978-1-61208-166-3

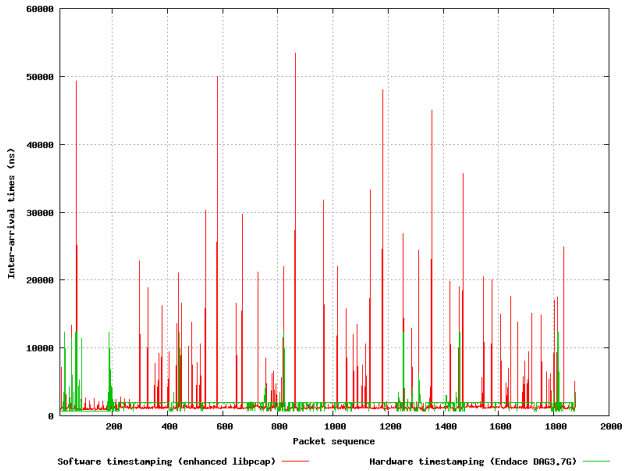


Figure 13. Packet inter-arrival times for *InterruptThrottleRate=1* (variable packet size)

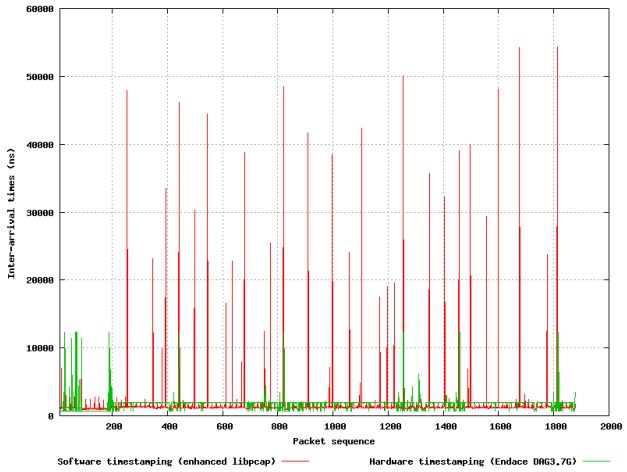


Figure 14. Packet inter-arrival times for *InterruptThrottleRate=3* (variable packet size)

Due to the effect of interrupt moderation and polling applied in dynamic (*InterruptThrottleRate=1)* and conservative (*InterruptThrottleRate*=3) modes, the packets are added to the kernel's input packet queue according to the process pacing, thus their MAC-level temporal relation is lost (Figs. 13, 14).

IV. CONCLUSION

At high arrival rate, to measure the time relation of the incoming frames as seen in the MAC layer the right solution is the high resolution and precision hardware timestamping. However, if we are interested in the arrival interval of the frames to the kernel network stack, then the relevant information can be obtained from the high resolution software timestamps produced by the kernel. At low arrival rate the results derived from software timestamps could come close to the ones represented by hardware timestamps. Besides that the generation cost of software timestamps in CPU time is significantly higher than the hardware timestamp's production, the length of generation time can display notable deviations. A possible solution to mitigate this problem is to store the raw value of the time reference as a timestamp (i.e., the value of the TSC counter), and convert it into time of the day (i.e., nanoseconds) format offline.

Nevertheless, contrary to the conventional microsecond resolution, the high resolution software timestamping of the packets can represent the arrival moment of the packets to the operation system with higher accuracy.

ACKNOWLEDGMENT

The work was supported by the TÁMOP 4.2.1./B-09/1/KONV-2010-0007 project. The project was implemented through the New Hungary Development Plan, co-financed by the European Social Fund and the European Regional Development Fund.

REFERENCES

[1] Jörg Micheel, Stephen Donnelly, and Ian Graham, "Precision timestamping of network packets," Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement, November 1-2, 2001, San Francisco, California, USA

[2] Gianluca Iannaccone, Christophe Diot, Ian Graham, and Nick McKeown, "Monitoring very high speed links," Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement, November 1-2, 2001, San Francisco, California, USA

[3] Attila Pasztor and Darryl Veitch, "PC based precision timing without GPS," Proceedings of the 2002 ACM SIGMETRICS international conference on Measurement and modeling of computer systems, June 15-19, 2002, Marina Del Rey, California, USA

[4] Peter Orosz and Tamas Skopko, "Performance evaluation of a high precision software-based timestamping solution for network monitoring," the International Journal on Advances in Software, ISSN 1942-2628, in press.

[5] Peter Orosz and Tamas Skopko, "Timestamp-resolution problem of traffic capturing on high speed networks," January 28-30, 2010, ICAI international conference, Eger, Hungary

[6] NetFPGA, http://www.netfpga.org/, 23/07/2011

[7] The DAG project, http://dag.cs.waikato.ac.nz, http://www.endace.com, 23/07/2011

[8] Intel PRO/1000 PT NIC, http://www.intel.com/products/server/adapters/pro1000pt-dualport/pro1000pt-dualport-overview.htm, 23/07/2011

[9] TSC, Intel 64 and IA-32 Architectures Software Developer's Manual, http://developer.intel.com/Assets/PDF/manual/253667.pdf, 23/07/2011

[10] Packet generator, NetFPGA.org, http://netfpga.org/foswiki/bin/view/NetFPGA/OneGig/PacketGenerator, 23/07/2011

[11] Christian Benvenuti, Understanding Linux Network Internals, O'Reilly, 2006

[12] Intel E1000E driver documentation.

[13] IETF RFC2679, A one-way delay metric for IPPM, http://www.ietf.org/rfc/rfc2679.txt, 23/07/2011

[14] IETF 3393, IP Packet Delay Variation Metric for IPPM, http://www.ietf.org/rfc/rfc3393.txt, 23/07/2011

 ISBN: 978-1-61208-166-3

Remote Vehicle Diagnostics over the Internet using the DoIP Protocol

Mathias Johanson
Alkit Communications AB
Mölndal, Sweden
mathias@alkit.se

Pål Dahle
Volvo Car Corporation
Gothenburg, Sweden
pdahle@volvocars.com

Andreas Söderberg
SP Technical Research
Institute of Sweden
Borås, Sweden
Andreas.Soderberg@sp.se

***Abstract*—Next generation vehicles will provide powerful connectivity and telematics services, enabling many new applications of vehicle communication. We will in this paper study the opportunities of performing remote vehicle diagnostics, where the diagnostic tool (test equipment) and the vehicle are separated by an internetwork, e.g., the Internet. The development of a prototype system for remote vehicle diagnostics, based on the emerging Diagnostics over IP (DoIP) ISO standard, is presented and early usage experiments with synchronous remote diagnostic read-out and control are described. A number of safety related issues are identified that will need closer study before a broad deployment of remote diagnostics services is feasible. Furthermore, a classification of vehicle diagnostics applications is provided, which is intended to elucidate the differences between synchronous (online) and asynchronous (offline) operation in local and distributed settings.**

Keywords-vehicle diagnostics, vehicular communication

I. Introduction

Access to diagnostic data from Electronic Control Units (ECU) in vehicles is of great importance in the automotive industry, both from a life cycle support perspective and during product development. Through diagnostic services, the state-of-health of components and subsystems can be monitored to detect and prevent failures by means of predictive maintenance, which improves operational availability and lowers support costs. For pre-series test vehicles, diagnostic services are crucial in order to be able to track problems as early as possible in the development process, preventing serious faults to pass undetected into production vehicles or as a tool during verification and validation activities. In the aftermarket, diagnostics form an important part of the service and maintenance process, with Diagnostic Trouble Codes (DTC) routinely being read out from customer vehicles during service for state-of-health monitoring and fault tracing. Automotive manufacturers rely on diagnostic systems in order to improve customer satisfaction by increasing the service technicians' ability to diagnose and remedy problems in the increasingly complex electronically controlled vehicles. As an added value for the automotive manufacturer, the diagnostic data retrieved during service can be uploaded to the manufacturer's database over the Internet. Statistical analysis of collected DTCs is important in order to monitor the quality of components and subsystems, to prioritize in which order problems should be addressed and to find correlations between different faults, or between faults and the operating environment.

A. Remote vehicle diagnostics

With the tremendous proliferation of wireless communication networks, telematics systems and services have been designed that make it possible to access diagnostic data from vehicles remotely, without requiring physical access to the vehicle. Presently, telematics services for diagnostics of general purpose passenger cars are mainly used during testing and validation of pre-series vehicles, but aftermarket services are also emerging in premium segments, for improved service and maintenance offerings [1]. Next generation vehicles will have sophisticated on-board connectivity equipment, providing wireless network access to the vehicle for infotainment and other telematics services. This will make it possible to realize remote diagnostic services for large-scale collection of diagnostic data from ECUs at level previously unattainable. Furthermore, this will enable many new aftermarket services and will also improve the opportunities of collecting diagnostic data for use during product development.

B. Integrated automotive diagnostics

Since automotive diagnostic systems are important both for aftermarket services and during many stages of product development, a common framework for capture, analysis and management of diagnostic data is highly desirable. Campos et al. argue that previous generations of diagnostics systems have not been well integrated, resulting in unnecessary duplication of effort in developing different diagnostic applications, each with its own infrastructure, components and software [2]. This leads to inefficient use of resources and high costs for development and maintenance of the diagnostics applications.

The key to realizing integrated diagnostic systems is to rely on standardized interfaces for communication and systems integration and to base the diagnostic software development on a component-based software architecture. This facilitates re-use of software components and makes integration of components and subsystems from many different vendors possible in an interoperable way.

Automotive diagnostics has a long history of standardization efforts, driven both by industrial inter-operability initiatives and legislation. One recent such effort is the emerging DoIP standard.

II. The DoIP standard

The standardization of automotive diagnostics technology was initiated by legislative regulations for emission control. These initiatives have led to numerous

 ISBN: 978-1-61208-166-3

standardization efforts of automotive diagnostic services, on virtually all technological levels, from hardware interfaces to communication protocols and software APIs. The perhaps most visible and influential initiative to date is the OBD-II specification issued by the California Air Resource Board (CARB), which is now mandatory for all cars sold in the US and the EU. Building further on this, the United Nations has initiated work on a new standardization framework called WWH-OBD (World Wide Harmonized On-Board Diagnostics), with the aim of rendering regional standards of vehicle diagnostics for emission control unnecessary and to replace them with a global standard. Moreover, this new standard will be a great leap forward in terms of new technology and protocols, enabling entirely new applications and services. One of the results of the WWH-OBD effort is the choice of using the Internet Protocol (IP) for communication between off-board and on-board diagnostic systems and for this purpose the Diagnostics over IP (DoIP) protocol is being developed by ISO, the International Organization for Standardization, under the formal name ISO 13400 [3].

The main motivation for introducing IP into the family of automotive diagnostics protocols is that the recent developments of new in-vehicle networks has led to the need for communication between external test equipment and on-board ECUs using many different data link layer technologies. To avoid having to implement, maintain and optimize transport and data link layer protocols for each new communication equipment development, and to easily be able to introduce new physical and data link layer technologies, a common internetworking protocol is needed, which is exactly what IP was designed for.

There is however a very interesting side-effect of this choice of network protocol, since it will improve the opportunities of interconnecting in-vehicle networks with the Internet for many new applications, including online, remote automotive diagnostics, which is the focus of this paper.

A. DoIP protocol overview

The ISO 13400 standard consists of four parts:

- Part 1: General information and use case definition
- Part 2: Transport protocol and network layer services
- Part 3: IEEE802.3 based wired vehicle interface
- Part 4: Ethernet-based High-speed Data Link Connector

In Part 1, the use cases that have guided the design of the protocol are outlined and a number of typical communication scenarios are described. Five main use case clusters are identified: (i) Pre-defined information request (such as state-of-health monitoring or road-worthiness assessment), (ii) vehicle inspection and repair (e.g., vehicle diagnostic fault tracing or vehicle readiness qualification), (iii) vehicle/ECU software reprogramming (i.e., firmware upgrade of ECUs during service or manufacturing), (iv) vehicle/ECU assembly line inspection and repair (similar to (ii) but in a manufacturing environment) and (v) multi-purpose data transfer from and to the vehicle, which involves non-diagnostic data exchange between vehicle and external equipment, including mobile customer equipment such as smart phones or PDAs.

The use case descriptions and communication scenarios described in ISO 13400-1 shows a considerable focus on communication between an in-vehicle network and external equipment in the immediate vicinity of the vehicle, such as test equipment connected through an Ethernet cable or a local area network (LAN), or mobile devices connected through wireless LAN (WLAN) technology. Uses cases such as the one focused in this paper, i.e., the opportunity of doing vehicle diagnostics with the external test equipment (or mobile device) being arbitrarily far away from the vehicle, interconnected by a true internetwork (i.e., a routed, packet-switched network like the Internet) is not specifically discussed. This is also reflected in the design of the DoIP communication protocol itself, for instance in the reliance on subnet broadcasts for vehicle announcements.

Part 2 defines network and transport layer protocols and services for vehicle diagnostics. This includes IP address assignment, vehicle announcement and vehicle discovery, connection establishment, communication protocol message format, data routing to in-vehicle nodes, status information and error handling. The focus on applications where the external test equipment is in the immediate vicinity (i.e., on the same subnetwork) as the vehicle is manifest primarily in the mechanism designed for vehicle announcement and discovery. This mechanism is intended to make external test equipment aware of the IP address and Vehicle Identification Number (VIN) of the vehicles connected to the same subnetwork. This is performed through subnet broadcasts of Vehicle Announcement and Vehicle Identification Request messages. Once the external test equipment has learned the IP address of a vehicle, a direct TCP connection to the vehicle's gateway node can be established, and the diagnostic data (or other data) exchange can be initiated. The message format designed for carrying the data is a lightweight message format based on a generic header and a payload specific header. The 8 byte generic header contains the DoIP protocol version number, payload type identifier and payload length field. The payload format for diagnostic data exchange adds a 4 byte header containing the 16-bit source and destination addresses (identifying the test equipment and ECU respectively), followed by the variable length data (up to 4 Gbytes). The connection set-up and data exchange can be carried out according to the DoIP specification regardless of whether the external test equipment and the vehicle are on the same local network or separated by an internetwork, providing that some mechanism external to DoIP is used for vehicle discovery. This is the basis for the remote online diagnostics application that will be described in detail in Section V.

Parts 3 and 4 of the standard specifies the data link layer and physical layer requirements, which are based on the Ethernet (IEEE 802.3) protocol and the ISO 15031-3 (SAE J1962) connector.

Note that, despite the name Diagnostics over IP, the DoIP protocol specifies several payload types that are not directly related to diagnostics in terms of the ISO 14229 scope [4]. (Only payload types 8000 and 8001 are intended for ISO14229 diagnostics.)

 ISBN: 978-1-61208-166-3

III. Remote Online Diagnostics

We use the term Remote Online Diagnostics to refer to data communication for vehicle diagnostics between one or more in-vehicle network nodes and an external test equipment that are interconnected by an internetwork. Thus, "remote" here means that the communication endpoints are not required to be connected to the same local subnetwork. This means that the physical distance between the external test equipment and the vehicle can be arbitrarily large, providing there is a network infrastructure available. We use the "online" qualifier to characterize our intended use of the DoIP protocol to perform diagnostic data exchange synchronously over a TCP connection set up between the endpoints. This is in contrast to "offline" or asynchronous diagnostic data exchange being performed by an on-board test equipment that performs the read-out locally in the vehicle, possibly remotely triggered, and then uploads the result to a server at a suitable time using whatever network connection is available.

A. A classification of vehicle diagnostics

It will be useful to study the different modes of diagnostics a bit more closely, to identify possible applications and to distinguish the technological solutions needed to implement them, their advantages and drawbacks. We will start this by classifying vehicle diagnostics applications according to whether the diagnosis is performed with the vehicle and the external test equipment being in the same place (connected to the same local subnetwork) or in different places (connected by an internetwork) and whether the diagnostic data exchange is performed synchronously (at the same time) or asynchronously (at different times). This classification, inspired by the classic time/space taxonomy of Groupware by Ellis et al. [5] is shown in Figure 1.

	Same time (synchronous)	*Different times (asynchronous)*
Same place (local network)	Traditional Diagnostics	Local Offline Diagnostics
Different places (internetwork)	Remote Online Diagnostics	Remote Offline Diagnostics

Figure 1. Time / space taxonomy of automotive diagnostics applications

The *same place / same time* case is the "traditional" diagnostic application, wherein a service technician (or automotive engineer) connects an external tester to the vehicle's OBD-II connector, reads out and analyzes diagnostic data for fault tracing or state-of-health purposes.

The *different places / same time* case is the application we focus on in this paper (remote online diagnostics), which gives the possibility for a service technician or engineer to do the same diagnostic read-out and fault tracing without being at the same place as the vehicle. A specific use scenario might be that a customer detects a malfunction in a vehicle and calls a service technician for support. The technician can then perform the fault tracing remotely and online, detecting and possibly solving the problem, and instructing the customer on how to proceed.

The *different places / different times* case is a remote offline diagnostic application. A typical example of when this type of service is useful is when large scale diagnostic data collection from a fleet of test vehicles (or possibly customer vehicles) is set up to gather performance data or statistics for use in product development. In such a scenario, a batch of diagnostic queries is scheduled for download to a number of vehicles. At a suitable time (when they have come online), the vehicles' telematics systems download and execute the diagnostic queries, assemble the responses, and upload the results to a central database, possibly at a much later time.

The *same place / different times* case does not have as immediately obvious applications as the others, but one can envision a situation where a service technician (or an automotive engineer) performs time consuming diagnostic tests of vehicles available locally, by downloading a diagnostic script file to an onboard tester that performs the tests, assembles the results, and then sends the results back to the test equipment (or a server), notifying the technician when the process is done.

The most interesting case for analysis in our present context is the distinction between the online and offline modes of remote diagnostics.

B. Diagnostic read-out versus diagnostic control

A distinction must be made between diagnostic read-out and diagnostic control. The purpose of diagnostic read-out is to query the status of the ECUs, typically by reading out DTCs for fault tracing or state-of-health applications. In diagnostic control applications, diagnostic commands that may alter the behavior of the vehicle are generated, for instance to turn the lights on and off. Thus, diagnostic read-out is a read-only operation, whereas diagnostic control is read/write.

C. Wireless versus wired diagnostics

Note that our definition of remote versus local diagnostics does not depend on whether the communication is performed using wired or wireless networks. A wireless local diagnostic application is for instance when a service technician connects to a locally present vehicle over a short-range wireless communication technology such as Bluetooth or IEEE 802.11 for diagnostics. In the wireless remote diagnostics case, some wide area wireless network technology is used (such as GPRS, 3G or 4G), or a combination of short range wireless communication and wired networks.

D. Online versus offline diagnostics

Although elements of the DoIP standard could be used to implement both the online and offline modes of remote diagnostics described above, it is clear that the DoIP protocol has been primarily designed with synchronous operation in mind. Since the main use cases that governed the design of the protocol are actually in the *same place / same time* category of Figure 1, this is not surprising. An interesting point to observe is that systems designed for *same place / same time* applications can, if implemented using the DoIP protocol, with very minor changes be used also for *different places / same time* applications, i.e., for remote online diagnostics. For instance, a traditional diagnostic read-out tool used in a service repair shop for fault tracing could with small modifications be used to remotely diagnose a vehicle on another continent. A drawback of using the online approach for remote

 ISBN: 978-1-61208-166-3

diagnostics is that applications that perform a complete diagnostic read-out of DTCs from all ECUs typically generate a large number of query/response transactions. With a considerable round-trip delay, as is often unavoidable in internetwork configurations, this can lead to a long total read-out time. The obvious remedy for this is to instead download a batch of queries, perform them locally in the vehicle, assemble the responses and send back. This is the offline approach described above. However, it is not always easy to design a generic batch of diagnostic queries, since the choice of which queries to include depends on the answer to previous queries. This means that a lot of logic needs to be present in the onboard tester in order to be able to execute the diagnostics properly in all situations. It is generally beneficial to keep this complexity at the infrastructure (server) side, rather than in the vehicle.

The main technological difference between the synchronous and the asynchronous case is that in the synchronous case the diagnostic queries or commands are sent by the external test equipment and directly responded to by the ECUs, whereas in the asynchronous case there is a time difference between query and response, and the network connection is not required to be kept alive during this time interval in the asynchronous case. The division between the two is not clear-cut however, and one can imagine hybrid approaches combining the two modes.

E. Remote online diagnostics using DoIP

As previously discussed, the core of the DoIP protocol can be used unmodified for remote online diagnostics, provided that the vehicle discovery and identification mechanism is supported by some additional means. Recall that the problem of the DoIP-mechanism for vehicle announcement and discovery is that it relies on subnet broadcasts, and thus these messages will not be accessible outside the local IP subnet the vehicle is connected to. One approach to overcome this problem is to establish a Virtual Private Network (VPN) connection from the vehicle to some enterprise network from where the operation of remote testers is supported. Alternatively, the VPN connection is terminated at a proxy server that listens to the vehicle announcements and keeps track of the IP addresses and VIN identifiers of the connected vehicles. The test equipment also connect through VPN to the proxy server, send vehicle identification requests, and receive the VIN identifiers and IP addresses of the currently connected vehicles. Clearly this approach will have scalability implications, when a very large number of vehicles are connected, typically for aftermarket applications. Performance scalability issues at the server side can be easily resolved by scaling up the number of proxy servers for load-balancing, using some simple heuristic method for deciding which server handles which subset of vehicles (e.g., based on IP subnet masks or similar). The problem that will appear at the external tester side is that the tester might get overly many responses to an unqualified vehicle identification request (i.e., a vehicle identification request message without VIN or EID). This can be resolved by only allowing vehicle identification request messages with EID or VIN at the proxy servers. Another problem is that all vehicle announcement messages will be propagated to the connected external testers, which might cause network connection congestion or processing overload. This can be solved by filtering out vehicle announcement packets from the VPN connections of the external testers. A side benefit of using a VPN based approach is the resolution of several security issues.

An alternative to the VPN approach to the vehicle identification problem is to develop a dedicated vehicle identification mechanism for remote online diagnostics applications. In the prototype application development described in Section V, a very simple vehicle identification mechanism is used, wherein each vehicle that comes online connects using TCP to a proxy server, reports its VIN number and then waits for a DoIP session to begin (keeping the TCP connection alive). The external tester connects to the proxy, queries for a particular VIN and if the vehicle is connected to the proxy the two TCP connections are interconnected and the DoIP session can begin. An additional benefit of this approach is that it also solves the problem that appears if the vehicle is not assigned a public IP address, due to Network Address Translation (NAT) firewalls being used.

For security reasons, and practical reasons, it might be desirable to let the vehicles use private IP addresses. This is often the case with addresses being assigned to mobile network devices in commercial wireless Internet access services. The problem with this is that private IP addresses are not reachable from outside; all communication sessions must be initiated from the mobile device (the vehicle in our case). Both mechanisms for vehicle discovery described above avoid this problem by having the VPN and DoIP TCP connections respectively initiated from the vehicle side.

IV. Safety aspects of remote diagnostic operations

Introducing the possibility to remotely control a vehicle using diagnostic operations creates a new range of safety related problems to address.

Safety can generally be divided into two main cases; safety in normal operation and safety for a system that is under influence of one or several system faults. The former, safety in normal operation, mainly addresses the task of creating a system that is safe with respect to usage, whereas the latter is about what is generally referred to as functional safety or system safety. This involves building more reliable or even fault tolerant systems and addresses issues about the process of reducing faults due to systematic (i.e., design) errors.

A. Normal operation

By introducing a remote diagnostic function, even if used by trained multi-skilled technicians, we may have introduced the possibility of the following new safety implications:

- the mechanic cannot directly observe the situation that the vehicle is in,
- the mechanic may not get visual feedback on what is really happening with the vehicle when it is under diagnostic control,
- the mechanic cannot interact with the vehicle in any other ways than using the terminal and an established communication session,

 ISBN: 978-1-61208-166-3

- the connection between the operator and the vehicle may be unreliable in terms of latency and bandwidth,
- there might be significant (non-deterministic) delays between the issuing of a diagnostic command and the moment when action is taken in the vehicle,
- there may be persons nearby or even inside the vehicle, e.g., the driver of the vehicle.

In connection to the prototype development of a remote diagnostics system described in Section V, a safety mechanism involving the remote user in diagnostic actions has been designed. In this solution we have concluded that

- the user of the vehicle needs to confirm her or his presence at the vehicle,
- the user needs to understand and subsequently approve the action to be taken,
- the user needs to be in charge of triggering of the remote action.

The mechanic, with diagnostic and service expert knowledge, is initiating the diagnostic request by down-loading a diagnostic task to the vehicle. The mechanic has to be in contact with the remote user (e.g., by phone) to be able to give instructions and get confirmation of understanding and approval to proceed. Presence control can easily be achieved by interacting with the vehicle (e.g., entering a code in the vehicle). Finally a trigger device (e.g., the remote key-fob) connected to the vehicle will trigger the diagnostic action to be taken.

It is believed that pure diagnostic read-out poses no safety risk, whereas only a limited set of diagnostic control actions can be considered safe under all circumstances. A large amount of actuators in the vehicle are risk related, especially in certain situations, such as when the vehicle is moving. Approval of safety limited synchronous diagnostic control therefore leads to a complex task of actuator safety classification. Furthermore, combinatory effects between sensors and other actuators complicate this matter even further.

B. *Functional safety*

A soon to be finalized ISO standard being applied intensively by many vehicle OEMs, ISO26262 [6], that addresses functional safety for E/E systems within passenger cars is the natural starting point when studying the system safety aspects of the diagnostic (sub-)system. The standard, which comes in 10 parts, has been jointly developed within a global automotive engineering community for the last 5-10 years. It is expected to become the de facto platform for system safety within the automotive domain, since it spans the fields of system engineering, hardware and software development, but also is specifically tailored to fit how automotive development is traditionally organized by OEMs and suppliers.

Specifically, we have done work within the "concept phase" (part 3 of the standard) by considering the diagnostic sub-system as the system under focus in the *Item definition*. This has proven to be difficult considering the natural characteristics of the diagnostic system: it contains limited functionality, but spans virtually all (electrical) sensors and actuators in the vehicle. Moreover, the system is constantly expanding as new sensors and actuators are introduced in the vehicle and it is hard to predict what the function developers will introduce in the future. Thus, the key has been to find a generalized way to analyze the system faults instead of looking at specific actuators that may be involved in the cause of the hazard. The general findings need then be applied at the various subsystems that use diagnostics as a tool, by considering faulty diagnostics as a source of hazards as well as any other root cause.

Note that nothing of the above makes any difference between traditional off-board diagnostics and remote diagnostics. The diagnostic subsystem is present even in today's vehicles. However there is one specific difference: the test equipment that is traditionally connected to the OBD connector in the vehicle would now usually (from a business case point of view) be integrated within the vehicle and is always present even if inactive. This *internal tester* needs special attention when it comes to the analysis of the source of any hazards.

V. Prototype system implementation and experiments

In order to gain practical experiences from remote online diagnostics and to explore how this can be realized using the DoIP protocol, a prototype system was implemented and tested in a controlled environment. Since no vehicle with an on-board DoIP gateway was available, it was decided that a DoIP gateway would be implemented on a Linux-based telematics system that could be connected to a standard vehicle's CAN buses through the OBD-II connector. The telematics platform has GPRS, EDGE and WLAN network interfaces as well as Ethernet interfaces. The DoIP entity implemented in the telematics unit handles the routing of diagnostic data between the in-vehicle (CAN) networks and the DoIP TCP connection on the wireless network interfaces.

To avoid having to develop a full-fledged diagnostics application from scratch the aftermarket diagnostics software VIDA, developed by Volvo Cars, running on an ordinary Windows PC was used as the external tester. Since there were no DoIP functionality implementation in VIDA at the time of this work, and since the implementation of this in VIDA itself was deemed not to be feasible within the time frame of the project, the client side DoIP interface was implemented in a dynamically liked library (DLL) that VIDA can access through the J2534 interface. This way we were able to develop an online remote vehicle diagnostics system without modifying the vehicle or the actual diagnostics tool.

With this approach, the diagnostics application (VIDA) on the PC will communicate ISO 14229 diagnostic messages through the J2534 DLL in the same way as if the PC was connected directly to the vehicle's CAN bus. What really happens is that the DLL encapsulates the ISO 14229 messages in DoIP messages that are transmitted over the IP network to the DoIP gateway in the vehicle, that decapsulates them, relays them onto the CAN bus, reads and assembles the responses (if any) and returns over the DoIP connection back to the DLL that forwards the result to the application. The diagnostics application can then process the response and go on to send the next query. The DoIP protocol is in this situation completely transparent to the diagnostic application.

Except for being a resource efficient way to implement our prototype system for experimentation, demonstration

 ISBN: 978-1-61208-166-3

and proof-of-concept, this approach is also interesting in that it provides a way to integrate diagnostics software completely unmodified into a DoIP-based infrastructure. This could help migration towards DoIP of the large installed base of tools and services based on J2534. A drawback of the design is that some of the complexities of the transport protocol used for implementing ISO 14229 diagnostics services over CAN (i.e., ISO 15765-2), such as the management of flow control filters, needs to be duplicated between the DLL and the DoIP gateway in the vehicle.

A. Experiments

The experiments carried out with the remote online diagnostics system prototype was first of all to demonstrate that a complete diagnostic read-out session could be performed over a wireless Internet connection, using the GPRS interface of the telematics unit. The PC was located in an office environment connected to the Internet using a LAN connection. A complete read-out of DTCs and additional data from the approximately 20 ECUs on the two CAN buses of a Volvo V70 takes around 10 minutes over a GPRS network connection. This is primarily due to the significant round-trip delay in GPRS networks. When using a WLAN connection, significantly shorter read-out times were measured: around 3 minutes, which is similar to local read-out using a directly connected CAN device.

In addition to the DRO experiments, diagnostic control commands were also tested, for instance recording of pedal positions, with real-time visualization of the pedal positions in the diagnostic application. Commands requiring write access were also tested, but limited to relatively safe operations, in the context of the experiments, like turning the engine fan or the lights on and off.

In principle, remote ECU reprogramming should also be possible to do in this way, but this was not tested, due to practical obstacles. In practice, remote reprogramming of ECUs is much more likely to be implemented based on a remote offline diagnostics model. This is because reprogramming of ECUs is typically time consuming, and the requirement to keep an online connection alive throughout the reprogramming will in many cases be failure prone. If the connection is disrupted during the reprogramming, the entire session will have to be rolled back. A better alternative is to download the software update to the vehicle asynchronously, perform the reprogramming in offline mode, and then reestablish the connection to report the status. Such an approach is described by Nilsson and Larson [7].

VI. Conclusions

In this paper we have shown how remote online vehicle diagnostics can be realized based on the DoIP protocol. To define what we mean by remote online diagnostics, we performed a classification of automotive diagnostics applications, based on whether the diagnosis is performed over a local network or over an internetwork spanning an arbitrarily large distance, and whether the diagnostic session is synchronous or asynchronous. We then outlined the salient features of the DoIP protocol, which has been designed first and foremost for synchronous, local applications. However, since DoIP is using the IP protocol, which is also the network protocol of the Internet, truly remote diagnostic applications are possible. The feasibility of designing such remote, online diagnostic applications was demonstrated through a prototype implementation, wherein a legacy vehicle diagnostics system was adapted to use the DoIP protocol. Experiments with the prototype shows that remote diagnostic read-out over relatively narrowband wireless internetworks is possible. Remote diagnostic control applications were also demonstrated.

One of the biggest challenges for introducing remote vehicle diagnostic services at a large scale is how to ensure the safety of the users of the vehicles. Our safety analysis shows that pure diagnostic read-out can be safely implemented, whereas diagnostic control applications in the general case are problematic. A related critical issue is how to protect a remote diagnostic service from illicit malevolent access. A comprehensive analysis of security issues in remote vehicle diagnostics is currently being conducted in relation to the work being presented here. The outcome of this analysis will have a profound impact on the design of the remote diagnostic system.

Our main conclusion from this work is that the DoIP protocol, when deployed broadly throughout the automotive industry, will enable many new applications of remote vehicle data access and control. This will pose many challenges in terms of performance, scalability, security, safety and resource management, but will at the same time give rise to very interesting new added-value services for the customers, and will also bring great opportunities to improve automotive product development.

Acknowledgment

This work was supported by the SIGYN-II project co-funded by VINNOVA, the innovation agency of Sweden.

References

[1] Hiraoka, C. "Technology Acceptance of Connected Services in the Automotive Industry," Gabler, ISBN 978-3-8349-1870-3, Wiesbaden, 2009.

[2] Campos, F.T., Mills, W.N. and Graves, M.L. "A reference architecture for remote diagnostics and prognostics applications," Proceedings of Autotestcon, pp. 842-853, ISBN 0-7803-7441-X, Huntsville, USA, October 2002.

[3] ISO/CD 13400, "Road vehicles — Diagnostic communication between test equipment and vehicles over Internet Protocol (DoIP)," 2009.

[4] ISO 14229-1, "Road vehicles - Unified diagnostic services (UDS) -- Part 1: Specification and requirements," 2006.

[5] Ellis, C., Gibbs, S. and Rein, G. “Groupware - Some Issues and Experiences,” Communications of the ACM, Vol. 34 No. 1, pp. 38-58, 1991.

[6] ISO/FDIS 26262, "Road vehicles – Functional safety," Parts 1-10, 2010.

[7] Nilsson, D. and Larson, U. "Secure Firmware Updates over the Air in Intelligent Vehicles," Proceedings of the First IEEE Vehicular Networks and Applications Workshop (Vehi-Mobi), pp. 380-384, Beijing, People's Republic of China, May 2008.

 ISBN: 978-1-61208-166-3

CoHoN: A Fault-Tolerant Publish/Subscribe Tree-Based Middleware for Robots with Heterogeneous Communication Hardware

Steffen Planthaber and Jan Vogelgesang
DFKI GmbH - RIC
German Research Center for Artificial Intelligence
Robotics Innovation Center; Bremen, Germany
Email: {steffen.planthaber, jan.vogelgesang}@dfki.de

Eugen Nießen
University of Bremen
Bremen, Germany
Email: eugen.niessen@uni-bremen.de

***Abstract*—The increasing functionality and capability of current mobile robots is partially a result of an increased number of sensors and actors. But this larger amount of sensors and actors results in more communication between the robot's components. Nevertheless, mobile robots also have to be lightweight, they have limited size and benefit from long operation times. These constraints are limiting the choice of components, which again can result in a situation where different communication hardware has to be integrated. In general, communication in robotic systems incorporates a lot of small-sized messages of some bytes and messages of several kilobytes but very few in between. Reconfigurable robots and multi-robot systems also have some similarities to mobile ad-hoc networks as their connectivity may change during operations. CoHoN is a transparent, connection-based, publish/subscribe communication middleware for networks with heterogeneous hardware which addresses the needs of communication in robotics. It provides failure resiliance, multipath routing, quality-of-service capabilities, and very low message overhead.**

***Keywords*-Middleware; Distributed Systems; Robotics.**

I. Introduction

Communication in robotics takes place between components of a robotic system (e.g., sensors, computers, actors) and between different robots in a multi-robot system. The communication can be **heterogeneous** in the hardware used to communicate, and it can have a **changing topology**. Small messages occur often in communication between components of a robot, mostly as sensor values like joint positions, desired angles, status messages, and control commands. Thus, a low message overhead is crucial for efficiency and bandwidth. Most middleware solutions used in robotic software frameworks [1] do not take these into account.

The amount of data sent through a robotic network is often not known when constructing and building a robot. Robots in science have a long lifetime and adding additional hardware and sensors in a later stage is not uncommon, resulting in situations where the available bandwidth between the components is too low. Changing the communication normally involves reprogramming the communication routines of the software. A robotic system is composed of a large number of different electronic components, employing different communication hardwares. Each communication hardware provides a distinct set of capabilities (e.g., speed, latency, reliability etc.).

Also, the network topology may change dynamically. This happens in multi-robot-systems when one robot moves out of range and also in single robots when communication hardware fails or a reconfiguration of the system occurs. A robotic network has a limited number of participating nodes, typically in the range of 100 nodes, due to space and weight restrictions.

Thus, a robotic communication middleware should operate with heterogeneous communication hardware and changing topology, but should require only a small message overhead. CoHoN is based on these requirements.

Two components of a robot are sometimes connected over more than one communication path. These cycles in the communication graph could be used for load distribution and increased failure resilience. CoHoN includes multipath routing capabilities to exploit these possibilities.

II. Related Work

Regarding communication, there are two types of robotic control frameworks. Some are using available communication middlewares, and some include custom communication abilities. In this overview only middlewares are covered that are able to communicate within a distributed network in contrast to a single device.

In the area of frameworks for robotics, supporting distributed computing an component-based infrastructure, ROS (Robot Operating System) [2] and Microsoft Robotics Developer Studio (MRDS) [3] are prominent solutions. A request and reply service is included in those two frameworks among other features. The ROS framework uses mainly publish/subscribe-based communication where messages are attributed to some topics [4]. The communication in MRDS is based on SOAP [5], which is a XML-based protocol built on top of TCP/IP. Other robotic frameworks employ existing

The project CoHoN is funded by the Space Agency of the German Aerospace Center (DLR), grant no. 50RA1024 and 50RA1025, with federal funds of the Federal Ministry of Economics and Technology (BMWi) in accordance with the parliamentary resolution of the German Parliament

 ISBN: 978-1-61208-166-3

communication middlewares [1]. OROCOS [6] and Miro [7], [8], e.g., are based on the CORBA middleware [9] while the ORCA framework [10] uses ICE [11].

CORBA and ICE, designed for large scale networks, have very low overhead compared to MRDS. But they still carry a message header size of more than 10 byte at best, hence they introduce a considerable overhead when sending small messages like sensor values. For CoHoN we want to avoid a centralized routing because this would introduce a single point of failure. Also, we have to deal with changing topology and different communication capabilities.

These requirements are solved by routing protocols developed for ad-hoc networks. An introduction and overview is given in [12] and [13].

The routing algorithm developed for CoHoN is based on directed diffusion [14] but is adapted from ad-hoc networking to the context of robotics. In [15] the directed diffusion approach is extended towards multipath routing and increased resilience against connection failures. Our routing approach is similar, but is based on a one-to-many instead of one-to-one communication paradigm.

III. Basic concepts

CoHoN is based on a topic-based publish/subscribe communication. Compared to other publish/subscribe variants, the topic-based approaches offer limited expressiveness but can be implemented very efficiently [4].

The messages sent by the publisher are called TopicItems and consist of a sequence number, used to detect duplicated and missing TopicItems, and the payload data. Each TopicItem is attributed to exactly one topic. CoHoN will integrate different kinds of communication hardwares into one network, i.e., it acts as an overlay network protocol. The TopicItems are routed by CoHoN at the interconnection points. The routing is based on a virtual circuit network, for each topic transfered between two neighbors a virtual circuit or *channel* is set up. This greatly reduces the network overhead on long-lasting subscriptions, as there is no need to transfer a unique topic identifier together with each TopicItem. The channels also allow TopicItem distribution with quality of service (QoS) by reserving the required resources during channel setup.

CoHoN uses a decentralized, request-based routing approach. Each subscription request is flooded through the network. If a node can deliver the topic, it did not forward the subscription request but returns an answer. The requesting node receives one or more answers from his neighbors and then selects where to receive the TopicItem from. This selection process continues towards the publisher.

Through this selection process a multicast tree is built up, and thus the data does not have to be sent to each subscriber separately. Although requesting a subscription through flooding results in considerable network traffic, the benefit is that this procedure discovers all possible routes and their properties in a completely distributed approach.

In robotics and many other applications, subscription requests are predominantly issued when the system is started. Later there are almost no additional subscription requests. Moreover, the subscription traffic is assigned a very low priority, thus it won't interfere with the delivery of the TopicItems. The routes may be saved to allow skipping the initial subscription request phase along with its overhead at the next startup. CoHoN also offers the possibility to disable the automatic discovery completely and to set the routes manually. There can be multiple paths between two nodes in the network. To take advantage of these cycles, additional connections can be appended to the multicast tree and used for multipath routing or as backup paths. This is similar to the braided multipath routing from [15].

In the following, the term "connection" is used for direct connection between two nodes. The term "path" is used for an indirect connection of two nodes, i.e., a path consists of one or more connections.

IV. Topic Routing

To subscribe to a given topic with unique id τ, three steps are executed. Between all connected nodes a point-to-point connection is assumed.

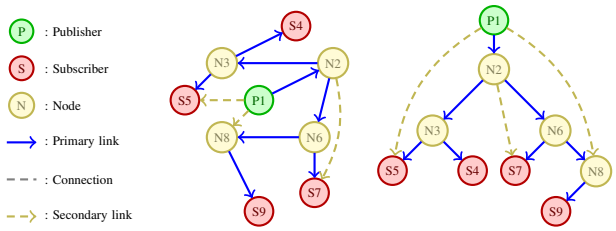
1) The subscription request message (SubReq) is flooded through the network. Included in the SubReq are the topic id τ and QoS constraints if required. A node receiving a SubReq and not having any current information regarding the topic forwards the SubReq to all connected nodes. It then waits for an answer.

2) A node that can deliver the topic, i.e., the publisher or a node being already part of the publication tree, sends back a subscription-acknowledge message (SubAck) over the reverse path if this path is able to comply with the given QoS constraints. Otherwise, the node returns a subscription-not-acknowledge message (SubNAck). The SubAck and SubNAck messages are forwarded over the reverse path of the SubReq message.

3) After receiving some SubAck messages over different connections, the subscribing node has multiple possible sources of the topic's publications. The node then selects one connection as the primary connection and reinforces it by sending a ReinforcePrimary message. Only over reinforced connections the actual publications will be forwarded. Each node receiving a primary reinforcement acts likewise: select a connection towards the publisher and send a ReinforcementPrimary. The process terminates if the publisher or a node on an already reinforced path is reached. The reinforcement of a connection has to be renewed in regular intervals, thus subscribers not anymore connected to the network will be removed from the.

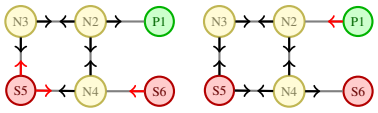
For steps 1 and 2, each communication direction is treated separately. This allows to detect all available paths

 ISBN: 978-1-61208-166-3



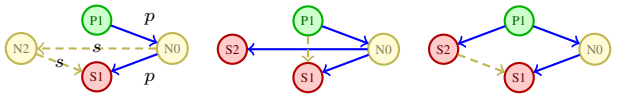
(a) Legend (b) Topolocical view (c) Topic route tree

Figure 1. Different views on the same network with one topic



(a) Step 1: SubReq (b) Step 2: SubAck

Figure 2. Messages Sent



(a) all (b) no bundling (c) no multipath, only backup path

Figure 3. Multipath possibilities

to the source even in cyclic topologies (Figure 2). Since the information gathered at step two is cached at each node, at most two SubReq and two SubAck/SubNack are exchanged over each connection within the cache lifetime. By selecting only one connection as the primary connection in step three, a tree structure is defined. This *primary tree* of τ is a spanning tree, connecting all subscribers and the publisher of τ. The publisher is the root of the tree and the TopicItems are distributed downwards in the primary tree (Figure 1).

Topic-based routing allows to use different routes for different topics of the same publisher. This is important to be able to add Quality of Service (QoS) in a later stage. Two topics of one publisher can be sent over different routes to one subscriber. Important data, like control commands, can be sent over real-time capable paths, while non real-time data, like log data, may use another path one without delaying the commands. The network traffic during subscription flooding can be decreased by using routing information already known by the nodes. Nodes, which are in the publication tree may answer directly. Additionally, nodes may cache the outcome of a request (received SubAcks or SubNacks per connection) and directly answer new requests, without further flooding. Moreover, the TopicID consists of two parts, a PublisherID and a topic number, thus routing information of other topics of the same publisher can also be used to limit the flooding of subscription requests.

To archive resilience against broken connection additional connections might be attached to the primary tree. These backup connections, called secondary connections, are reinforced by ReinforceSecondary messages. The secondary reinforcements continues towards the publisher until the primary tree, another secondary connection or the publisher is reached. Each node is aware of its depth in the primary tree from the subscription phase, this information is used to ensure the correct direction of the secondary path.

Secondary connections might be used in different ways:

As backup path: The connection is not used until the primary connection breaks. The breakdown is detected either by the driver layer or because a periodic transmission has been missing for some time. However, the latter is only possible for periodic transmissions, which are quite common in the sensor domain. When a breakdown is detected, the node selects one of the secondary connections as the new primary connection. The selection is communicated by sending a ReinforcePrimary message.

As auxiliary path: The secondary connection may help to detect lost topic items. For this, so-called TopicStubs are send via the secondary connections. A TopicStub contains only the most recent sequence number the sending node has seen. The node receiving the TopicStub is then able to detect lost topic items and either asks for a retransmission or selects the secondary connection as new primary connection. The use as auxiliary connection is especially suited for aperiodic and large messages, e.g., environment maps.

As alternative path: The secondary connection may be used as alternative connection if the primary connection is congested. This is also known as *multipath routing*.

V. Multipath Routing

When CoHoN determined multiple path possibilities, multipath routing may be available given certain circumstances. Let the secondary path s and the primary path p converge at node N0, i.e., the reinforcement of s stops at N0 (see Figure 3(a)). Let S1 be the node in p just below N0. If s heads into the tree rooted at S1, then s could be used used as an alternative to the connection from N0 to S1. If the connection does not head into the same subtree, multipath is not possible (Figure 3(c)) The prerequisites just given are checked by a *cycle probe*. The cycle probe is a special message, which starts at N0, travels down into the tree over s and then back to N0 over p. Only if the given prerequisites are fulfilled, the cycle probe will reach again N0.

A TopicItem received via an alternative route is forwarded down the primary tree (as usual) and also up towards the parent node in the primary tree. The TopicItem is sent upwards the primary tree as long as needed, i.e., till all subscribers in the tree below S1 could be reached (Figure 3(b)).

If there are no other subscribers or multiple primary outgoing links within this cycle, both routes (primary and secondary) can be bundled. This means the sending node

 ISBN: 978-1-61208-166-3

may send the topics in an alternating way via the one or the other interface. This bundling would be possible in Figure 3(a), but not in Figure 3(b). Mulitpath routing helps to distribute bandwidth utilization, but may result in an disordered delivery of the TopicItems. The subscriber has to reorder the messages using the included sequnce numbers.

VI. Future Work

Currently, the project is within its implementation phase and thus there are no experimental results available. A first implementation of the routing algorithm in a network simulator showed the general feasibility of the approach.

Further development will include the Quality of Service (QoS) functionalities. The possibilities provided will be strongly dependent on the communication hardware used. Some QoS features are in particular useful in the field of robotics: latency and jitter. A minimum latency must be supported for control commands, e.g., security shutdowns. A minimum jitter, which is a maximum deviation of the latency value, must be applied for sensor values, which are used in motor or joint controllers.

The implementation will be followed by an valuation of the re-routing capabilities and the resulting fault-tolerance of CoHoN. To evaluate CoHoN, connections will be disturbed or completely disconnected in order to test the re-routing and the detection of failures. The hardware test setup will include Ethernet, CAN Bus, PROFIBUS, and SpaceWire. Other common communication methods, like RS232, will be added later.

The selection of hardware covers most of the communication principles used in robotics, i.e., Single Master Bus (PROFIBUS), Multi-Master Bus (CAN), Point to Point (SpaceWire), and Ethernet (Point to Point on driver interface level). The straightforwardness of the underlying routing (virtual connections with channels) was also chosen in order to be able to implement CoHoN nodes on micro-controllers or FPGAs in a later stage of development. These have low processing power but are used frequently by sensors and actors.

VII. Outlook

We have presented the design prinicipal and routing approach of CoHoN. CoHoN is not meant to replace existing robotic frameworks but rather to provide an alternative for exchanging their data between distributed nodes. It does not include data marshaling but is designed to submit blocks of data, thus CoHoN can be adapted easily to existing communication methods. The chosen publish/subscribe approach is used by many frameworks (e.g. ROS) and has already proven to be flexible and powerful.

CoHoN will allow an additional topic naming based on textual tags. In a Service Discovery process, the tags are resolved to actual topics. This allows to support different naming schemes used by robotic frameworks.

References

[1] N. Mohamed, J. Al-Jaroodi, and I. Jawhar, "Middleware for robotics: A survey," in *Robotics, Automation and Mechatronics, 2008 IEEE Conference on*. IEEE, 2008, pp. 736–742.

[2] M. Quigley, B. Gerkey, K. Conley, J. Faust, T. Foote, J. Leibs, E. Berger, R. Wheeler, and A. Ng, "ROS: an open-source Robot Operating System," in *International Conference on Robotics and Automation*, 2009.

[3] J. Jackson, "Microsoft robotics studio: A technical introduction," *Robotics & Automation Magazine, IEEE*, vol. 14, no. 4, pp. 82–87, 2007.

[4] P. T. Eugster, P. A. Felber, R. Guerraoui, and A.-M. Kermarrec, "The many faces of Publish/Subscribe," *ACM Computing Surveys*, vol. 35, pp. 114–131, 2003.

[5] F. Curbera, M. Duftler, R. Khalaf, W. Nagy, N. Mukhi, and S. Weerawarana, "Unraveling the web services web: an introduction to soap, wsdl, and uddi," *Internet Computing, IEEE*, vol. 6, no. 2, pp. 86–93, 2002.

[6] H. Bruyninckx, "Open robot control software: the OROCOS project," in *Robotics and Automation, 2001. Proceedings 2001 ICRA. IEEE International Conference on*, vol. 3. IEEE, 2005, pp. 2523–2528.

[7] H. Utz, S. Sablatnog, S. Enderle, and G. Kraetzschmar, "Miro-middleware for mobile robot applications," *Robotics and Automation, IEEE Transactions on*, vol. 18, no. 4, pp. 493–497, 2002.

[8] G. Kraetzschmar, H. Utz, S. Sablatnög, S. Enderle, and G. Palm, "MiroMiddleware for Cooperative Robotics," *RoboCup 2001: Robot Soccer World Cup V*, pp. 95–110, 2002.

[9] T. H. Harrison, D. L. Levine, and D. C. Schmidt, *The design and performance of a real-time CORBA event service*, ser. OOPSLA '97. New York, USA: ACM Press, 1997.

[10] A. Makarenko, A. Brooks, and T. Kaupp, "Orca: Components for robotics," in *International Conference on Intelligent Robots and Systems (IROS)*, 2006, pp. 163–168.

[11] M. Henning, "A new approach to object-oriented middleware," *Internet Computing, IEEE*, vol. 8, no. 1, pp. 66 – 75, 2004.

[12] J. N. Al-karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wireless Communications*, vol. 11, pp. 6–28, 2004.

[13] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, pp. 325–349, 2005.

[14] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed Diffusion for Wireless Sensor Networking," *IEEE/ACM Transactions on Networking*, vol. 11, pp. 2–16, 2003.

[15] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 4, p. 11, Oct. 2001.

 ISBN: 978-1-61208-166-3

A Framework for Assessing the Security of the Connected Car Infrastructure

Pierre Kleberger*, Asrin Javaheri*†, Tomas Olovsson*, and Erland Jonsson*
*Department of Computer Science and Engineering
Chalmers University of Technology
SE–412 96 Gothenburg, Sweden
Email: {pierre.kleberger, asrin.javaheri, tomas.olovsson, erland.jonsson}@chalmers.se
†Volvo Car Corporation
SE–405 31 Gothenburg, Sweden

***Abstract*—In this paper, a framework for assessing the security of the connected car infrastructure is presented. The framework includes a model of the infrastructure and a security assessment tree. The model consists of a managed infrastructure and the vehicle communication. The managed infrastructure is further divided into five parts; automotive company applications' centre, third party applications' centre, trusted network, untrusted network, and the Internet backbone. The model clarifies the different communication possibilities between the managed infrastructure and the vehicle. Furthermore, the assessment tree defines four categories that need to be addressed in securing vehicular services; the actors, Vehicle–to–X communication technologies, network paths, and the dependability and security attributes. Moreover, we demonstrate the benefit of the framework by means of two scenarios. In this way, the communication in these scenarios are mapped to the model, which makes it possible to analyse the security issues for the scenarios according to the assessment tree. The intention with such an analysis is to identify possible weaknesses of services in the connected car.**

***Keywords*-security assessment; vehicle service; connected car; infrastructure.**

I. Introduction

In the world of connectivity, almost all applications and systems today are communicating and using the Internet. So far, vehicles have been an exception. The demand for new services are quickly changing this field which makes the vehicle a connected car [1]. However, these new services have to be properly secured for their new communication infrastructure. In this paper, we present a framework for assessing the security of services delivered by the connected car infrastructure.

The connected car is a vehicle equipped with a wireless network gateway connecting the in–vehicle network to an external network. Today, the in–vehicle network consists of 50–100 embedded computers called electronic control units (ECUs), a number which has rapidly been increasing over the last years. With the introduction of wireless access to the vehicle, these ECUs will be exposed to external traffic and the need of securing the vehicle and its communication becomes crucial [2, 3]; it is reasonable to believe that many of the security related problems present on the Internet will be introduced into the vehicle domain.

Protocols developed for traditional vehicular services, such as vehicle diagnostics [4] and software download [5] where a wired connection is used to access the vehicle, as well as new services in development, now have to be adapted for secure remote usage. Furthermore, by introducing a wireless gateway to the vehicle, enabling the vehicle to communicate with mobile devices and other vehicles, the system becomes even more complex. Hence, a model to clarify the communication with the vehicle for conducting security assessment on its services is essential.

The framework presented in this paper consists of a model for the infrastructure of the connected car and a security assessment tree. It will help us understand and evaluate how to implement and secure protocols and applications in different vehicle settings. The connected car will contain a large number of services, communication technologies, and network types, which makes the assessment of security far from trivial [6–8]. The proposed model together with the security assessment tree makes it possible to understand the weaknesses of the system and the existence of threats both when designing new services and when using current ones.

The paper is organized in the following way. After giving an overview of related work in Section II, we present a background to the problem in Section III. In Section IV, we describe in detail the proposed model of the infrastructure, which is further extended with the security assessment in Section V. In Section VI, the security assessment is applied to two services. We discuss the proposed framework and possible future work in Section VII. Finally, Section VIII concludes the paper.

II. Related Work

Although there is a lot of research going on in vehicular communication (VC) systems [6], there is very little research found referring to models of the connected car and how to assess the security of emerging vehicle services, i.e., remote diagnostics, remote software download, and other Internet services brought into future vehicles.

Nilsson et al. [9] present a model of the connected car. The model is divided into three domains; the *portal*, the *vehicle*, and the *communication link* connecting the vehicle

 ISBN: 978-1-61208-166-3

to the portal. A risk assessment is conducted for each of the domains and protective security mechanisms are discussed for the identified risks. However, in their model, details of the networks between the portal and the vehicle are not specified, and the possibility of other vehicles and mobile devices to connect to the vehicle is not addressed.

The Car 2 Car Communication Consortium (C2C–CC) describes a reference architecture which is divided into three domains; the *in–vehicle*, the *ad hoc*, and the *infrastructure* [10]. The in–vehicle domain is represented by the vehicle, its applications, and mobile devices directly associated to the vehicle. The ad hoc domain is represented by the vehicles and the road–side units (RSUs), where the RSU further can be connected to the infrastructure domain. In their architecture, the access network, the Internet, and possible nodes connected to the Internet are shown as part of the infrastructure domain, but are not further considered. These parts were out of their scope.

An architecture for providing a continuous connection to the vehicle is presented by the CALM Forum [11]. The aim is to make the best possible use out of available external communication media in the vehicle. A nice overview of the network is shown, but the focus is not in securing the communication infrastructure.

Koscher et al. [2] recently showed on the lack of security in the in–vehicle network. By using techniques such as packet sniffing, packet fuzzing, and reverse-engineering, a number of possible attacks toward the in–vehicle network was performed. The focus of their work is on the security of the vehicle. Thus, the communication link with the vehicle is not addressed.

In [3], Brooks et al. discuss a set of automotive applications and they propose and use an adapted version of the CERT Taxonomy for analysing the security of these applications. Among the applications analysed are business related services, which integrates the vehicle into the automotive company, i.e., remote software download, remote diagnostics, and other applications related to the comfort of the vehicle.

Research in a security architecture for VC systems have been performed within the SeVeCOM project [12]. In [13], Papadimitratos et al. present necessary security requirements to provide the services of secure beaconing, secure neighbour discovering, and secure geocasting in VC systems. Certificates are used for securing the communication between vehicles and pseudonyms for addressing the introduced privacy problem of using certificates; the certificate gives the vehicle a unique identity, which makes it possible to trace the vehicle and its driver. In [14], Kargl et al. present implementation details of the security architecture. Furthermore, the integration of mobile devices and different communication technologies into the VC system are briefly discussed.

Two more research project that currently are running are the EVITA project [15] and the OVERSEE project [16]. The aim of the EVITA project is to provide a security architecture for the in–vehicle network and to support secure Vehicle–to–X (V2X) communication. The aim of the OVERSEE project is to develop an open and secure platform for running applications, with the possibility for internal and external communication, in the vehicle.

However, we are still missing a structured approach in assessing the security of services to the connected car, i.e., services from the automotive company or other third party application providers. Thus, a model of the infrastructure for assessing the security of the connected car is needed.

III. Background

As more and more services are introduced into the vehicle, the complexity of the vehicle is increased correspondingly. Therefore, the work with securing the connected car requires a holistic understanding of the system. In the lack of a model describing the infrastructure, the development of a unified security solution is far from trivial. This may lead to that different security solutions, possibly incompatible with each other, are chosen when applications are implemented in the connected car. Therefore, for a model to be useful for further security analysis, it must be possible to map almost all possible scenarios into it; which actors need to be considered, and which V2X communication technologies and network paths are available. However, a model for mapping services and their corresponding communication protocols, to be used for security assessment, has not been found.

The model proposed in [9] is a simple model which only describes the infrastructure of the connected car and leaves out details about communication links, network entities, and possible communication technologies. The model presented here is an extension of that model and takes into account the different communication technologies, various remote vehicular services, and possible threats and security risks which may exist.

We believe that the use of a framework can help in relaxing some requirements in different situations, e.g., the need of protecting confidentiality in the repair shop when using wireless LAN (WLAN), or the integrity of the diagnostics data while connecting through the Internet. Considering the first example, the same level of security as for a wired connection could be reached.

IV. A Model of the Infrastructure

In this section, we present a model of the infrastructure of the connected car. This model is shown in Figure 1. We divide the infrastructure into two domains, the managed infrastructure and the vehicle communication. The managed infrastructure is further divided into five regions, automotive company applications' centre, third party applications' centre, trusted network, untrusted network, and the Internet backbone. The vehicle communication describes the possible means of communication with the vehicle. These communication means are classified in two categories, bi–directional and uni–directional.

A. Managed Infrastructure

The five regions of the managed infrastructure are further described below.

 ISBN: 978-1-61208-166-3

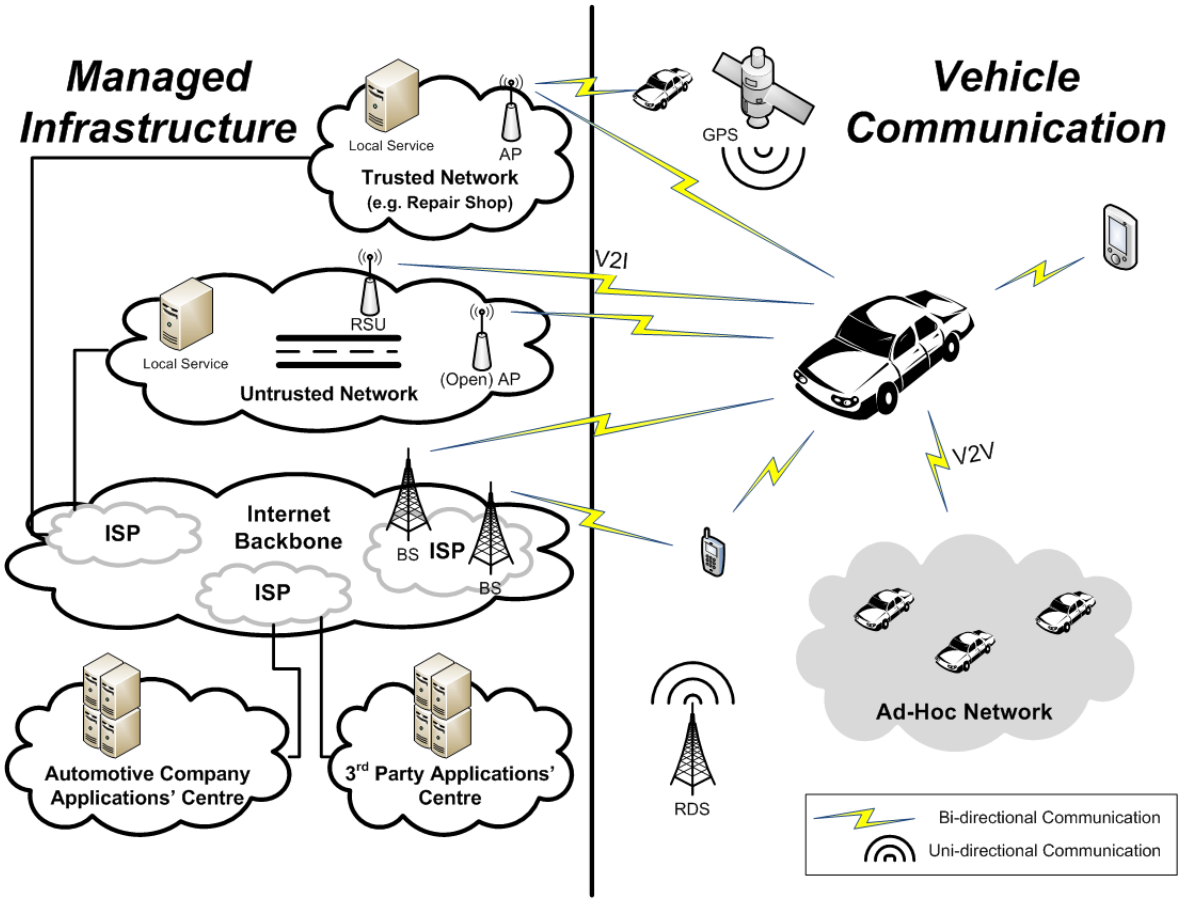


Fig. 1. Model of the connected car infrastructure

1) Automotive Company Applications' Centre: In the literature, the automotive company applications' centre have had different names. In [9], it is called *portal*. In [4], the remote diagnostics is performed from a *remote service centre*. To summarise, it consists of a set of servers providing services to their vehicles. It holds necessary information about the vehicle, such as information from previous services (e.g., diagnostics data), configuration data, cryptographic keys, as well as new software available for the ECUs.

2) Third Party Applications' Centre: Apart from services provided by the automotive company, third party services can be provided to the vehicle. We could imagine that large "application stores" for vehicles will be available in the future. These applications can provide any kind of service to the vehicle.

3) Trusted Network: Some networks can be considered to be trusted by the applications' centres and the vehicle. For example, a repair shop may be considered to be a trusted network by the automotive company and the vehicle. In delivering a service to this network, it may well be that some requirements in an implementation can be relaxed. Furthermore, other local services can be available in these networks for running the local infrastructure and providing service to the vehicle.

4) Untrusted Network: All networks, except for the trusted networks, are considered to be untrusted. In these networks, the services provided to the vehicle have to be adapted to the hostile environment of the Internet. In the same way as for the trusted networks, other local services may also be provided in these networks.

5) Internet Backbone: The Internet backbone, with its Internet Service Providers (ISPs), is the core network for connecting the other four regions together. A backbone network is usually well protected and operated by network specialists in a Network Operation Centre (NOC). Therefore, when network traffic has reached the Internet backbone, we assume it is very unlikely that the data will be intentionally modified.

B. Vehicle Communication

The vehicle communication domain includes two possible types of communication means, bi–directional and uni–directional. They are further described below.

1) Bi–directional Communication: The bi–directional communication mean includes the possible communication between:

(1) the vehicle and the managed infrastructure,
(2) the vehicle and mobile devices, and
(3) the vehicle and other vehicles.

 ISBN: 978-1-61208-166-3

We will now go through possible communications within these three groups:

- *vehicle to wireless access point (AP)*. The vehicle can establish a connection to a wireless AP in the managed infrastructure. All open APs (hotspots) are considered to be part of the untrusted network. Furthermore, a protected AP, where the vehicle needs authentication keys, can be available in both the trusted network and the untrusted network. An example of a wireless AP in an untrusted network is one provided by subscription from a telephone network provider; these wireless APs can be considered to be shared with other unknown users in the same way as for open APs.
- *vehicle to RSU*. The RSUs can be used for establishing a connection from the vehicle to the managed infrastructure.
- *vehicle to cellular base stations*. A mobile data network, e.g., 3G, can be used for establishing a connection from the vehicle to the managed infrastructure. In this case, the vehicle connects to a cellular base station in the Internet backbone. This connection requires a subscription to a mobile data network service at a telephone network provider.
- *vehicle to mobile devices*. Mobile devices can be connected to the vehicle. For example, a connection can be established to a mobile phone, a laptop, or a personal digital assistant (PDA). Furthermore, the vehicle can also act as a gateway for the mobile device, so that the mobile device can reach the same network as the vehicle.
- *vehicle to cellular base station via mobile device*. If the vehicle lacks the possibility to connect directly to a cellular base station, another mobile device with a connection to the cellular base station can be used as a gateway. One example is to use the driver's mobile phone. By using the mobile phone, a connection to the managed infrastructure can be created.
- *vehicle to other vehicles*. Finally, the vehicle can connect to other vehicles and create a vehicle ad–hoc network (VANET). This Vehicle–to–Vehicle (V2V) communication will be critical in future traffic- and safety-related services.

It should be noted that the description of the vehicle communication above is based on just one vehicle; any connected car will have the same communication surroundings. This means that the vehicle may possibly reach the managed infrastructure, via other vehicles or other mobile devices acting as gateways.

2) Uni–directional Communication: Broadcast devices that only sends signals to the vehicles are classified as uni–directional communication. Two uni–directional communication means have been identified:

- *the global positioning system (GPS)*. The GPS system can be used by services in the vehicle.
- *the radio data system (RDS)*.

V. Using the Model to Assess the Security of Vehicle Services

From the model of the infrastructure of the connected car, there are different aspects that can be discussed regarding the V2V and the Vehicle–to–Infrastructure (V2I) communication. One of them is the security of the services delivered to the vehicle. Figure 2 presents a brief taxonomy of the security of these services. Four categories are described; the *actors*, the *V2X communication technologies*, *network paths*, and the *dependability and security attributes*. A description of them follows bellow.

- *actors*. Six different actors that can be involved in a service have been identified. Common for them all are that they have interests in how the service is being designed and delivered; the automotive company and the application provider can state requirements, the car owner and the user can have concerns on how the data from a service is processed, the authorities can issue legal requirements, and an attacker can try to manipulate the service in an unwanted way.
- *V2X communication technologies*. A number of communication technologies are available for connecting the vehicle to other devices. Examples of these are listed in this branch. An extended list, including classifications of the communication technologies, can be found in [17].
- *network paths*. The service may be delivered to the vehicle using one of several network paths. The model describes four possible network paths that the service can be delivered through (see Figure 1); the trusted network, the untrusted network, the Internet backbone, and an ad-hoc network.
- *dependability and security attributes*. To deliver the service in a secure and safe manner, the six attributes for dependability and security [18] need to be considered. In this paper, we are mainly focusing on the security attributes.

From these four categories, an analysis can be made to further clarify how a service will work in the infrastructure and also highlight the dependability and security attributes that need to be addressed in providing such a service.

VI. Conducting Security Assessment on two Services

We will now show the benefits of using the framework for assessing the security of the services delivered to the connected car. We will describe two scenarios to illustrate the approach; a remote diagnostics service and a map service with GPS positioning.

A. Remote Diagnostics

Remote vehicle diagnostics is one of the emerging vehicle services in the connected car [4, 5]. Thus, work is being performed by the International Standard Organisation (ISO) in defining a standard protocol for performing Diagnostics over IP [19–21].

 ISBN: 978-1-61208-166-3

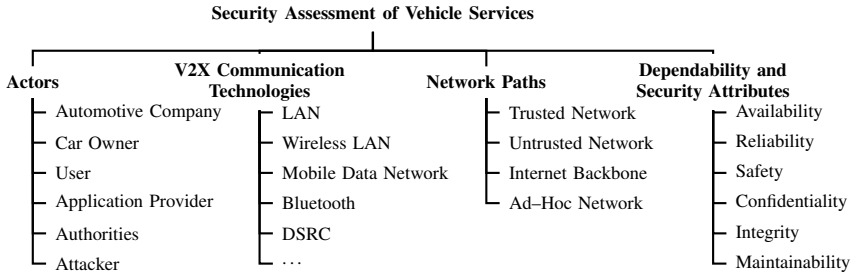


Fig. 2. Security Assessment Tree

In analysing a remote diagnostics service, the first step will be to clarify how the diagnostics will be performed. In the model of the infrastructure (see Figure 1), we find two cases:

(1) *remote diagnostics performed by repair shop*. The vehicle connects to the trusted network at the repair shop through an AP. The diagnostics session is provided as a local service at the repair shop.
(2) *remote diagnostics performed by the automotive company applications' centre*. The vehicle connects to a cellular base station in the Internet backbone. The diagnostics session is performed by the automotive company applications' centre through the Internet backbone and the cellular base station.

To further clarify these cases, the security assessment tree in Figure 2 is used. For case (1), the following question can be derived:

> What is the *automotive company's* concern with respect to the *confidentiality* of the submitted diagnostics data when the vehicle is connected to the repair shop in the *trusted network* using a *wireless LAN*?

This question reflects the following set of aspects from the tree:

> {*automotive company, wireless LAN, trusted network, confidentiality*}

We note that although the network at the repair shop is considered a trusted network, its AP can be shared with other vehicles. Therefore, if the confidentiality requirements of the wireless link is fulfilled, the same level of security might be acquired as if a cable was used.

For case (2), another question can be derived:

> What is the *automotive company's* concern with respect to the *integrity* of the diagnostics data transmitted between the vehicle and the automotive company applications' centre when the vehicle is connected to the *Internet backbone* using a *mobile data network*?

This question reflects the following set of aspects from the tree:

> {*automotive company, mobile data network, Internet backbone, integrity*}

In this case, we see that by fulfilling the integrity requirement, modified diagnostic codes sent by an attacker will not pose any security risk to the vehicle.

B. Map with GPS Positioning

A possible service in a vehicle is a map provided by an Internet service (e.g., Google Maps) with positioning using the vehicle's built–in GPS. A further add–on to this service may be to get local traffic conditions from the road authorities. This service leads to three sources of information that need to be provided to the vehicle, the map, the GPS-coordinates, and the current traffic condition in the area. We will now analyse this service with respect to the model of the infrastructure and the security assessment tree.

The first step will be to clarify how the map is provided to the vehicle. From the model in Figure 1, four suitable links between the vehicle and the managed infrastructure can be found;

(1) vehicle to RSU,
(2) vehicle to AP,
(3) vehicle to cellular base station, and
(4) vehicle to cellular base station via a mobile device.

These four links are located in the untrusted network and the Internet backbone, which are further connected to the third party applications' centre providing the map to the vehicle. Furthermore, for the GPS-positioning, the data is retrieved from the GPS-satellites. A security analysis of the retrieved data is not considered here. However, for the current traffic condition, the service needs to be mapped into the model of the infrastructure to clarify its communication. The same four links as above can connect the vehicle to the managed infrastructure. The current traffic condition is provided by the two networks, untrusted network and the Internet backbone, which are further connected to the road authorities (in the third party applications' centre).

To further clarify the security issues of delivering the map to the vehicle, the second step is to inspect the security assessment tree in Figure 2. For the map service, several questions can be derived with respect to the different possibilities to deliver the map to the vehicle. To illustrate the concept, only one question will be highlighted;

> What is the *user's* concern with respect to the *confidentiality* of the data submitted (i.e., GPS-coordinates) to the map service when communicat-

 ISBN: 978-1-61208-166-3

ing with the server over the *mobile data network* through the *Internet backbone*?

This question reflects the following set of aspects from the tree:

{*user, mobile data network, Internet backbone, confidentiality*}

The question above is relevant if the user does not want any other party, except for the server, to be able to identify the user's current location by eavesdropping on the transmitted data.

For the traffic conditions, the following question can be derived:

What is the *user's* concern with respect to the *integrity* of the data distributed by the road authorities, when the data passes the *Internet backbone* and the *untrusted network*, and the vehicle is connected to the RSU in the *untrusted network* over a *Dedicated Short–Range Communication (DSRC)*-link?

This question reflects the following set of aspects from the tree:

{*user, DSRC, (untrusted network, Internet backbone), integrity*}

In this case, the user is not concerned about whether any other party can eavesdrop on the traffic condition information, but rather that the *correct* information is delivered to the vehicle.

VII. Discussion and Future Work

We believe that in analysing some scenarios and solutions with respect to security, it might be that some of the security requirements could be relaxed. One such example is: if the confidentiality of the communication link between the vehicle and the AP in the trusted network can be properly established; will security of the link then be comparable with that of a wired cable? If so, a service can, as a first step, easily be introduced also for this wireless link without any modification. This will reduce the time for adapting already established services, and save cost for developing new ones. However, for other scenarios the service might need to be modified.

The security assessment tree helps us state questions regarding the security of the services delivered to the vehicle. In the future, we would like to investigate how to extended this security assessment tree to cover more aspects, e.g., security mechanisms. A complete security analysis of a vehicle service is also an important next step.

VIII. Conclusion

There is a clear trend of offering remote services, third party applications, and critical information exchange between various entities in the connected car. Even though there has been a lot of research conducted in the field of securing VC systems, not much work has been done in assessing the security of these services for the connected car. We believe that, by using our proposed framework, scenarios such as remote vehicle diagnostics, remote software download, multimedia streaming, Internet browsing and the exchange of information between vehicles and the infrastructure can be discussed and assessed from a security viewpoint.

References

[1] P. Papadimitratos, A. d. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, "Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation," *IEEE Communications Magazine*, vol. 47, no. 11, pp. 84–95, 2009.

[2] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *Proc. of the 31st IEEE Symposium on Security and Privacy*, 2010, pp. 447–462.

[3] R. Brooks, S. Sander, J. Deng, and J. Taiber, "Automobile Security Concerns," *Vehicular Technology Magazine, IEEE*, vol. 4, no. 2, pp. 52–64, Jun. 2009.

[4] S. You, M. Krage, and L. Jalics, "Overview of Remote Diagnosis and Maintenance for Automotive Systems," in *2005 SAE World Congress*, Detroit, MI, USA, 2005.

[5] M. Shavit, A. Gryc, and R. Miucic, "Firmware Update Over The Air (FOTA) for Automotive Industry," in *14th Asia Pacific Automotive Engineering Conference*. Hollywood, CA, USA: SAE, 2007.

[6] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions," *IEEE Communications Surveys & Tutorials*, no. 99, pp. 1–33, 2011.

[7] T. L. Willke, P. Tientrakool, and N. F. Maxemchuk, "A Survey of Inter-Vehicle Communication Protocols and Their Applications," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, pp. 3–20, 2009.

[8] M. L. Sichitiu and M. Kihl, "Inter-Vehicle Communication Systems: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 2, pp. 88–105, 2008.

[9] D. K. Nilsson, U. E. Larson, and E. Jonsson, "Creating a Secure Infrastructure for Wireless Diagnostics and Software Updates in Vehicles," in *Proc. of the 27th International Conference on Computer Safety, Reliability, and Security (SAFECOMP '08)*. Newcastle upon Tyne, UK: Springer-Verlag, 2008, pp. 207–220.

[10] *C2C-CC Manifesto*, v1.1 ed., CAR 2 CAR Communication Consortium, Aug. 2007. [Online]. Available: http://www.car-to-car.org/. 2011-08-06.

[11] *The CALM Handbook*, v3 (060326) ed., The CALM Forum Ltd., 1 Beverly Hall, Halifax, West Yorkshire, HX2 6HS, UK, Mar. 2006. [Online]. Available: http://www.isotc204wg16.org/pubdocs/The CALM Handbookv6-070301.pdf. 2011-08-06.

[12] "Secure Vehicle Communication (SeVeCOM)." [Online]. Available: http://www.sevecom.org/. 2011-08-06.

[13] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communication Systems: Design and Architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[14] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110–118, Nov. 2008.

[15] "E-safety Vehicle Intrusion Protected Applications (EVITA)." [Online]. Available: http://www.evita-project.org/. 2011-08-06.

[16] "Open Vehicular Secure Platform." [Online]. Available: https://www.oversee-project.com/. 2011-08-06.

[17] K. Dar, M. Bakhouya, J. Gaber, M. Wack, and P. Lorenz, "Wireless Communication Technologies for ITS Applications," *IEEE Communications Magazine*, vol. 48, no. 5, pp. 156–162, 2010.

[18] A. Avižienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, 2004.

[19] *ISO/DIS 13400-1: Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 1: General information and use case definition*, ISO Std.

[20] *ISO/DIS 13400-2: Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 2: Network and transport layer requirements and services*, ISO Std.

[21] *ISO/DIS 13400-3: Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 3: IEEE802.3 based wired vehicle interface*, ISO Std.

 ISBN: 978-1-61208-166-3

Performance Evaluation of Large-Scale Charge Point Networks for Electric Mobility Services

Christian Lewandowski, Stephan Haendeler, Christian Wietfeld
Communication Networks Institute
TU Dortmund University
Dortmund, Germany
Email: {christian.lewandowski, stephan.haendeler, christian.wietfeld}@tu-dortmund.de

***Abstract*—Today's public charge points for Electric Vehicles (EV) are equipped with numerous ICT components for communication with vehicle and back-end systems for authentication, billing and invoicing. The rollout of EVs will inevitably lead to a higher demand for charging infrastructure and will increase the operational and management costs for operators. In order to minimize costs, this paper evaluates applicable local networking technologies for large scale charge point scenarios and takes into account IEEE 802.11g, IEEE 802.3 and Homeplug GreenPHY, which is currently discussed in the ISO/IEC Joint Working Group for defining the Vehicle 2 Grid Communication Interface where TU Dortmund is an active member. A Web-Service based Charging Process Protocol for data exchange between all involved entities is presented to determine the data rates for XML and EXI encoded packet transmission. The V2G communication between EV and charge point is analyzed as well as the goodput for back-end communication. For this, hubs including data concentration are proposed to minimize billing data amount for the clearing center. For examination of the possible charge point network size, an overview of current predictions for EVs is given and the proposed system is evaluated within a parking area at TU Dortmund, where we expect the installation of 61 charge points by 2030. With optimization of the presented load coordination service, the data rate in the charge point network could be reduced by 99.8 %.**

***Index Terms*—Electric Mobility; Charge Point Networks; Powerline Communications (PLC); IEEE 802.11g**

I. Introduction

The market penetration of electric vehicles will raise to approximately 1 million in 2020 and 2 million in 2030 in Germany [1]. Based on this prediction that is aimed by the German government for the next years, a charging at work application scenario is examined in this paper. This scenario is described in detail in Section II. To include important services like *load coordination* to prevent local substation blackouts and the possibiliy to feed back energy into the smart grid communication between EV and Electric Vehicle Supply Equipment (EVSE) is inevitable. For coordinated charging processes in parking areas a network beetween EVSEs and a Load Coordinator (LC) needs to be considered. The connection needs to be cost-effective, integrable in existing infrastructures and reliable. Hence, we propose the IEEE 802.11 standard due to high market penetration. If new parking areas are planed IEEE 802.3 is an alternative due to low costs and high data rates, which is sufficient for the next years regarding possible value added services. Section III introduces prEVail, a simulation environment for evaluation of the ICT for EV connectivity. The charging process communication protocol is presented and packet sizes for an XML based communication and an EXI encoded message exchange are determined using the MORE middleware [10]. With these measured packet sizes, Section III-A analyses the V2G communication based on the charging process protocol regarding the Powerline Communications standard Homeplug GreenPHY. After this the inter charge point communication is analyzed including back-end communication with data concentration for an effective transfer of clearing data. Afterwards a worst-case scenario including a fair load coordination is introduced, and the realization of the charging at work scenario can be verified regarding the predictions in Section I and Section II.

II. Charging at Work Scenario

The central scenario for charging an electric vehicle will be charging at home. 90 % of the people in Germany drive less than 50 km per day. These distances can be covered by most of todays EVs with a night charge. Hence, charging at public charge points is not inevitable. For commuters with a long travel to work, charging at work is the second major charging scenario. This scenario is discussed in the following chapters. The Federal Motor Transport Authority (KBA) of Germany published a study for January 2011 [3] where Germany currently has 42,3 million registered private vehicles. In [4], a slow increase of prices for transportation and hence a slow behaviour modification of the population is predicted, which results in an increasing number of vehicles in Germany.

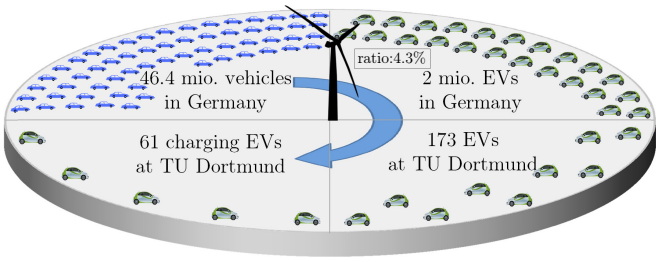


Fig. 1. Estimated number EVs at TU Dortmund in 2030

Therefore, 46.4 million vehicles are assumed on german streets in the year 2030, which include 2 million EVs (ratio

 ISBN: 978-1-61208-166-3

of 4.13%). Figure 1 shows the calculation for EVs at TU Dortmund depending on the predictions before. With 4000 available parking spaces and an EV percentage of 4.13% a maximum of 173 EVs are available at TU Dortmund. Although the range of today's EVs is sufficient for 90 % of the german inhabitans, in future it will be important to plug in the EV to provide an operating reserve. In peak times pluged in EVs can help to stabilize the grid because renewable energy sources like wind parks and solar collectors are not reliable energy sources at all times. Indeed, not all of the cars need to be recharged at work and also not everybody wants to provide an operating reserve because of the anxiety that the battery gets damaged. Hence, we assume that in the year 2030 35% of the 173 EVs need the opportunity to plug in considering enhancements in the battery technology and EV owners who want to provide an operating reserve. Hence, we propose the installation of 61 charge points at TU Dortmund until 2030.

III. ICT Simulation Environment prEVail

prEVail is an ICT validation environment for different communication technologies and is based on the simulation environment presented in [2] using OMNeT++ 4.0 [5] and the INET Framework [6]. For electric vehicle charging processes, the four main entities EV, EVSE, Emobility Hub (EMHub) and the optional LC are integrated (see Figure 2).

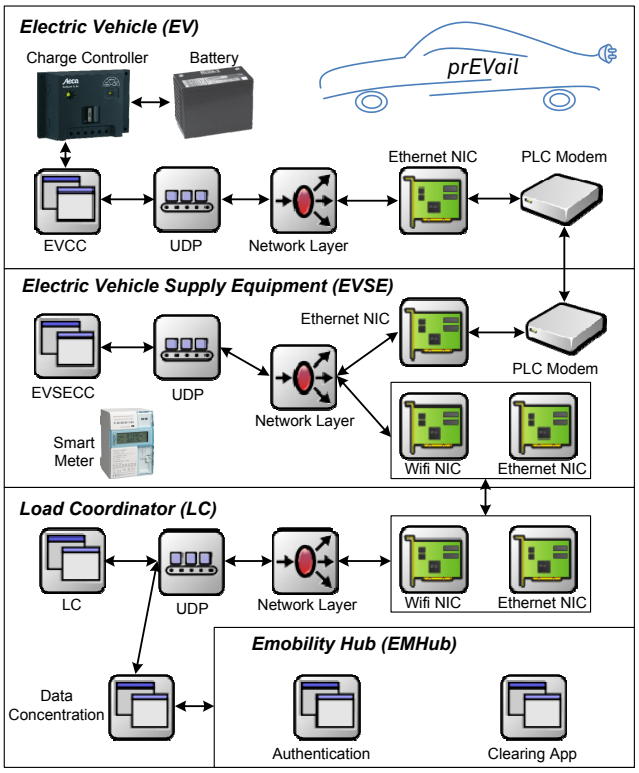


Fig. 2. prEVail, simulation environment for electric vehicle charging infrastrucutres

The modules UDP, network layer, ethernet nic and wifi nic are integrated within the INET framework and all other modules have been implemented by the authors. The *Electric Vehicle* (EV) consists of a full adjustable battery model, which is configured to act as a lithium ion battery, a charge controller and the Electric Vehicle Communication Controller (EVCC), the central communication module of the EV. It mediates between the internal modules of the EV and the charging infrastructure. The other modules of the EV (battery and charger) are implemented as traffic generators for the communication processes. Current EVs typically use high performance lithium ion batteries with charging characteristics shown in Figure 3. Before a deep discharge threshold is reached, the battery will be charged with a minimal current (a preconditioning charge). From this point the battery can be charged with a constant current until it reaches its maximum cell voltage. In the third stage the battery will be charged with a constant voltage leading to a decreasing charge current. The gradients of the voltage graphs in stage 1 and 2 are constant, although a saturation curve will be expected. In stage 3 the charging current is modeled as discrete saturation curve. These assumptions are made because it has no major effect on the characteristics of the modules with respect to traffic generation.

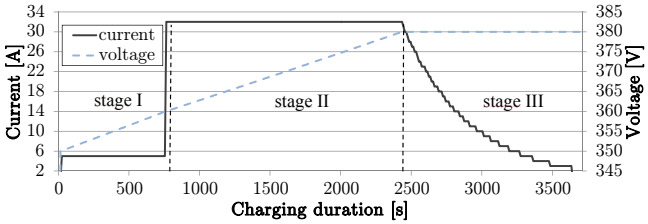


Fig. 3. Simulated charging characteristics of a lithium ion battery

The EVSE and the EV are connected via Powerline Communications (PLC). Due to current discussions in the ISO/IEC Joint Working Group for defining the V2G Communication Interface [8] Homeplug GreenPHY [7] was choosen for evaluation with prEVail. Results are shown in Section III-A. The Electric Vehicle Supply Equipment Communication Controller (EVSECC) is modeled as a gateway and only forwards messages from EV to LC and back. The smart meter generates meter readings for the charging process regarding parameters of the EV's battery, which will be needed for the clearing. The clearing data are send to the *Emobility Hub* (EMHub), which is responsible for authentication and clearing.

The *Load Coordinator* (LC) is parametrized by only one parameter, the total capacity, which is available for the whole parking area. This capacity is fairly assigned to all charging vehicles. To arrange multiple EVSEs in a local network, the EVSEs and the LC can be connected with different communication technologies. In this work Ethernet (IEEE 802.3) and Wifi (IEEE 802.11g) will be evaluated. For higher layer communication a web-service based protocol is discussed including XML and the Efficient XML Interchange (EXI) encoding format [9]. The charging process protocol including authentication, start of the ChargingPprocess (CP), clearing and optional capacity updates for the load coordination is

 ISBN: 978-1-61208-166-3

presented in Figure 4.

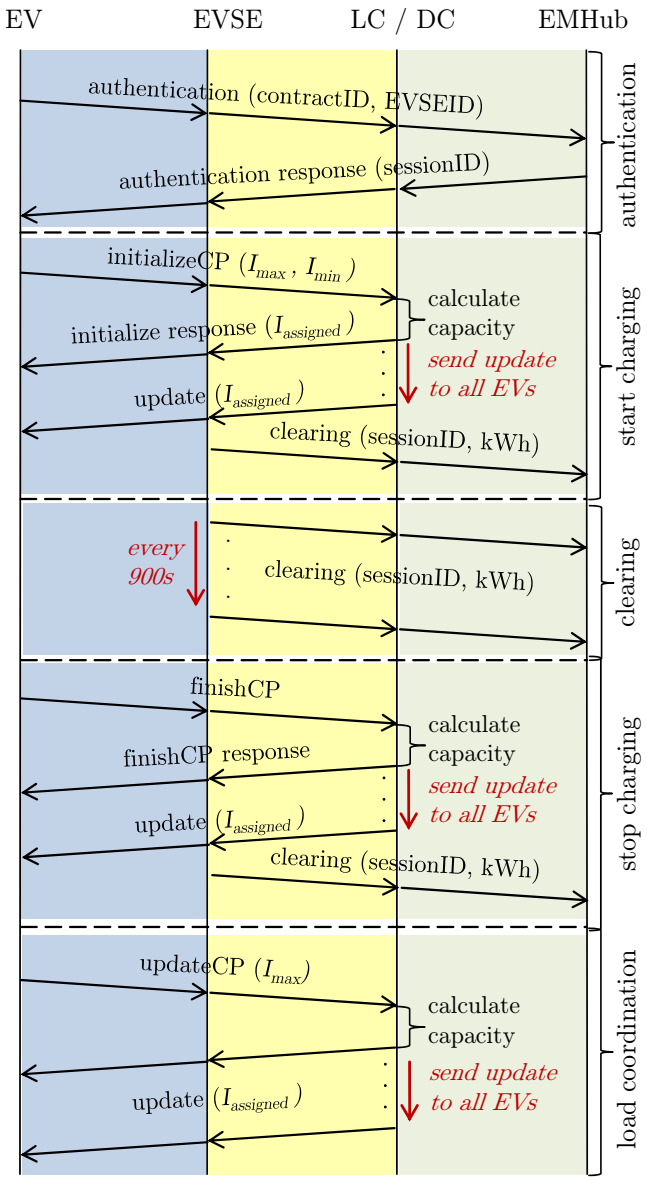


Fig. 4. Charging Process Protocol

For authentication the EV sends an *authentication* message with a contractID and the EVSEID via the LC with integrated Data Concentrator (DC) to the EMHub. The EMHub replies with an *authentication response* containing a sessionID for the new charging process, which is needed for the clearing later on. After successful authentication the EV initializes the CP by sending an *initializeCP* message containing I_{max} and I_{min}. With these information, the LC calculates new capacity assignements and sends updates to all charging EVs. After receiving the assigned capacity from the LC the EVSE sends a first clearing message including the initial meter reading to the EMHub. Afterwards the clearing will be done by the EVSE every 900s (15 min.) using the sessionID from the authentication process and the meter reading. When CP is finished the EV notifies the LC, which calculates new capacities for the other charging EVs and the EVSE initiates the last clearing message. The same recalculation of capacities is done during the load coordination. Every time the EV does not need the whole assigned capacity anymore it sends *updateCP* messages with the currently used power to the LC, in order to deallocate the excess power for use in other charging processes. Subsequently the LC recalculates the power allocation and replies with an *update* to all other active EVs.

For an estimation of packet sizes for authentication and clearing on the one hand and load coordination on the other hand, a web-service was developed using the MORE Middleware [10]. Table I shows the measured packet sizes for messages within the charge point network.

Type / Name	XML [byte]	EXI [byte]
Clearing Message		
authentication (P_{auth})	865	475
authentication response ($P_{authRes}$)	898	493
clearing ($P_{clearing}$)	960	550
Load Coordination		
initialize CP (P_{init})	883	477
initalize response / update ($P_{initRep}$)	829	448
update CP (P_{update})	867	461
finish CP (P_{full})	875	471

TABLE I
PACKET SIZES FOR AUTHENTICATION, BILLING AND LOAD COORDINATION MESSAGES IN THE CHARGE POINT NETWORK

These packet sizes provide a basis for further analyses.

A. Vehicle 2 Grid Communication

In this section, the V2G communication between EV and EVSE is analyzed based on the charging process protocol presented before. Due to the fact that EV and EVSE are generally connected with the charging cable (except inductive charge), this communication medium can be used with a PLC communication technology.

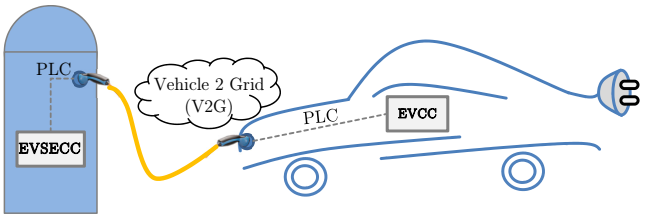


Fig. 5. Vehicle to Grid Communication Overview

Homeplug GreenPhy standard [7] is currently discussed in [8]. The advantage is the compatibility with Homplug AV and the reduction of cost and power consumption to 25% of Homeplug AV. Hence, the complexity is decreased, and e.g., TDMA mode was removed and the dynamic channel adaption was limited. The result is that only one subcarrier modulation format is supported (QPSK) as well as only one Turbo Code with rate 1/2 for Forward Error Correction and a limited PHY rate of 10 Mbps maximum. The number of 1155 subcarriers

 ISBN: 978-1-61208-166-3

and subcarrier spacing of 24.414 kHz is unmodified to support the compatibility to Homeplug AV and hence the compatibility with in-house PLC networks. For further analyses the *MINI-ROBO_AV* mode with a PHY Rate of 3.7716 Mbps and a Physical Block (PB) size of 136 bytes and the *STD-ROBO_AV* with PB size of 520 Byte and a PHY Rate of 4.9226 Mbps are evaluated. An overview of the GreenPHY PB format is given in Figure 6.

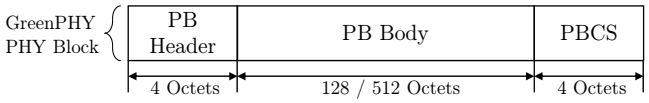


Fig. 6. Homeplug GreenPhy Physical Block format [7]

Each PB consists of a 4 octets *PB Header* containing e.g., a Segment Sequence Number (SSN). Depending on the PB size, data have to be padded to either 512 or 128 octets to fit exactly into the *PB Body*. The PHY Block Check Sequence (PBCS) contains a 32-bit CRC and is computed over the PB Header and the encrypted PB Body.

Based on this standard, the V2G communication is analyzed. Figure 7 depicts the occurence of messages during a whole fast charging process without getting influenced by the LC due to other charging vehicles and recalculation of the capacity assignment. The measurement was made with EXI encoding right before the encapsulation into the PB Body to see, if the messages fit into one PB Body. It can be determined that all sent messages and the *authentication response* do not fit into the PB520 Body of 512 octets (see dottet line in Figure 7). Hence, the messages are fragmented into 2 PBs with size of 520 octets each due to the needed padding.

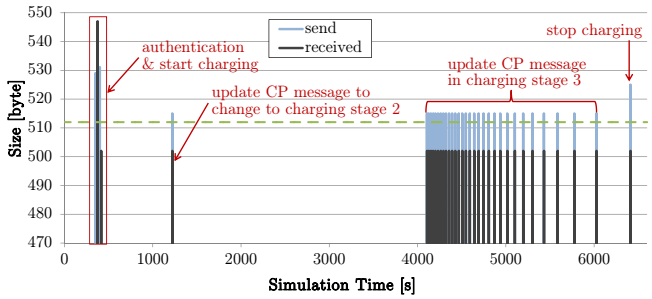


Fig. 7. Message occurence of charging process protocol in V2G communication using EXI encoding in a fast charging scenario

The CP begins at approximately 400s simulation time with the authentication and the response. After that, the charging process is initialized by the *initializeCP* message and the corresponding response. The next *updateCP* message at 1200s is the change over to charging stage 2 of the battery where the EV requests more capacity from LC. The third charging stage starts after approximately 4100s. In this stage the EV deallocates the excess capacity $\mathrm{N_{CPupdates}}$ times.

$$\mathrm{N_{CPupdates}} = (I_{\max} - I_{\min} + 2) \tag{1}$$

With $I_{\max} = 32$ and $I_{\min} = 3$, 31 CP updates are initiated by the EV before the CP finishes with a *finishCP* and corresponding response message. Figure 8 shows the XML and EXI data rate for HP GreenPHY PB sizes of 136 and 520 octets as a function of simulation time.

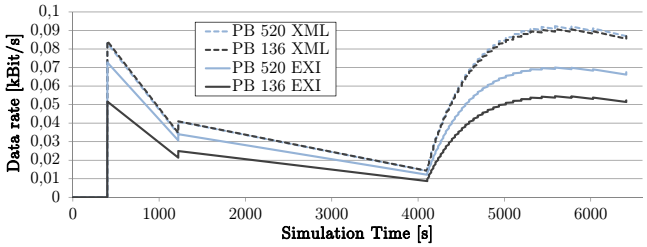


Fig. 8. Average data rate for V2G communication with XML and EXI encoded XML as a function of simulation time

It can be seen that the average data rate correlates with the message occurence in Figure 7. Because of the padding, in EXI transmision 2 PBs need to be transmitted and the data rate for PB520 is much higher, although PB136 has more fragments. With ongoing time when the CP goes over to stage 3, PB136 data rate is still a bit lower and PB520 data rate increases until the end of the CP. The last result is also the average data rate for a full CP. Using PB136 for the presented charging process protocol will save 23% of the needed data rate when using EXI encoding.

As stated in Table I, all XML messages including protocol overhead fit into 2 PB520 Bodys and the utilization of the PB Body gets more effective in comparison to EXI and the data rates for both modes are more or less equal. Nevertheless the data rate can be reduced from 87 Bit/s to only 51 Bit/s by using EXI and PB136 mode. This corresponds to an enhancement of 41 %.

B. Inter Charge Point Communication

For communication with EV and back-end, today's charge points are equipped with numerous ICT components, which increases the prices for the infrastructure. Especially the contracts for mobile radio for the back-end communication are very expensive and can be saved when organizing multiple EVSEs into a local network. Figure 9 gives an example for connecting EVSEs in a network using IPv4. This network includes one EVSE acting as a data hub for back-end communication, which concentrates the clearing data in one message and transfers it to the EMHub. Hence, protocol overhead can be reduced. In future work IPv6 will be integrated into prEVail to support analyses of larger networks.

$$d_{CSN/BE} = x \cdot \left[P_{auth} + P_{authRes} + \left(2 + \left\lfloor \frac{t}{900s} \right\rfloor \right) \cdot P_{clearing} \right] \cdot \frac{8}{t} \tag{2}$$

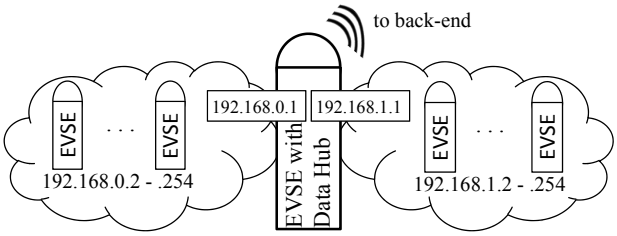


Fig. 9. Design of large-scale charge point networks using multiple IPv4 subnetworks

Considering the packet sizes of Table I, the goodput in the charge point network without load coordination $d_{CSN/BE}$ can be calculated with (2) for x charging process. In this context the goodput is defined as the data rate within the presentation layer. Thus protocol overhead is excluded. The goodput includes the authentication P_{auth} and the corresponding authentication response $P_{authRes}$, the clearing messages at the beginning and at the end of the charging process and periodic clearing messages every 15 minutes. For a charging process with $t = 3h$ the needed data rate is 6.42 *Bit/s* for EXI communication. This goodput is also valid for the communication link to the back-end. In order to reduce the needed data rate for this link, the clearing messages can be concentrated at the data hub, so that only one message is periodicaly sent to the back-end including the clearing data of all ongoing charging processes.

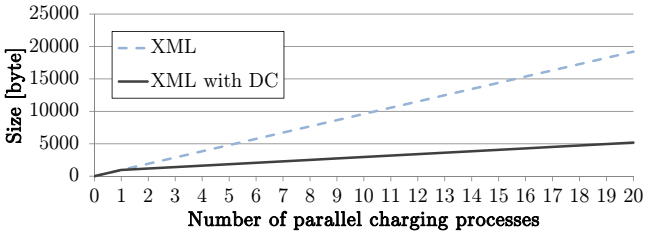


Fig. 10. Data Concentration (DC) with XML for back-end communication

A comparison between the concentrated messages using XML and XML with EXI encoding is shown in Figure 10 and Figure 11.

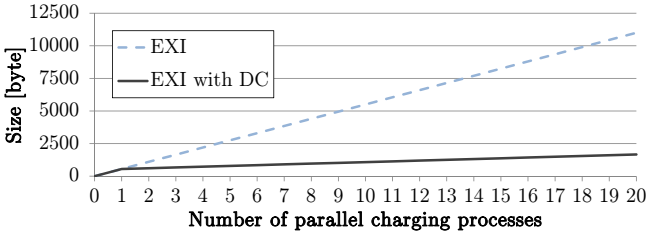


Fig. 11. Data Concentration (DC) with EXI encoded XML for back-end communication

When XML is used for sending clearing information to the back-end it can be seen that the data concentration is very effective and 73% of the transmitted data can be saved. If this XML stream is encoded with EXI the data can be reduced by a factor of one third. Because of the efficient encoding of information repeatedly used in the same message [9], only 8.6% of the clearing data need to be transfered to the EMHub in comparison to XML without data concentration. Formula (3) calculates the goodput for the concentrated back-end communication link d_{CBE} depending on the number of parallel charging processes and the *clearingSize* shown in Figure 10 for XML and in Figure 11 for EXI.

$$d_{CBE} = \left[(P_{auth} + P_{authRes}) \cdot x + \left(2 + \left\lfloor \frac{t}{900} \right\rfloor \right) \cdot clearingSize(x) \right] \cdot \frac{8}{t} \quad (3)$$

An exemplary result for the back-end communication goodput is indicated in Figure 12 with 20 parallel charging processes for XML and EXI communication with and without data concentration.

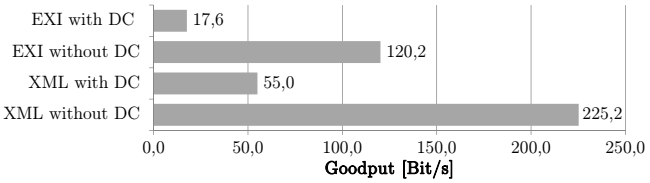


Fig. 12. Comparison of the goodput for data concentration mechanisms

If the clearing data of 20 charging processes are merged into only one message, the goodput for XML concentration can be reduced to 24% and for EXI Schema concentration to 14%. The concentration will be even more effective by increasing the parallel charging processes.
For estimation of a worst-case data rate for a charge point network, the LC is integrated into the parking area [2]. The LC coordinates all charging processes on the parking area to reduce the risk of local substation blackouts. The maximum power for the parking area can be defined depending on the scenario and is allocated equitably to each charge point.

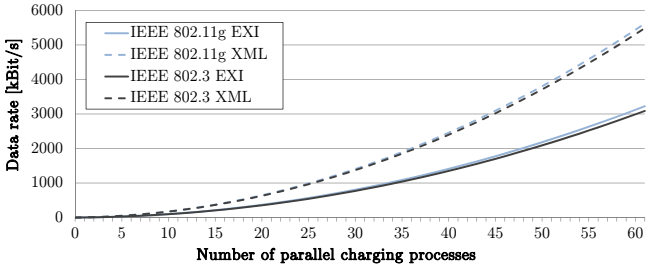


Fig. 13. Overview of the data rate for inter charge point communication using IEEE 802.3 and IEEE 802.11g with unoptimized LC

To analyze the data rate for communication between the EVSEs and the LC containing the data hub, a scenario for 61 expected EVs at TU Dortmund is created. To measure a

worst case data rate, all EVs charge in the third stage to get a maximum of data traffic in the simulation. Figure 13 shows first results for an unoptimized load coordination message exchange where the *updateCP* messages in the third charging state were sent in periodic time intervals $t_{akt} = 5s$ instead of a fixed number shown in formula (1). This time interval guaranteed an optimal power allocation for all EVs.

IEEE 802.3 and 802.11g are analyzed regarding communication with pure XML and EXI encoded XML. The data rate of IEEE 802.11g is marginal higher for XML and for EXI communication than the one of IEEE 802.3 due to protocol overhead. Hence, a maximum data rate of 5.5 MBit/s for XML and 3.1 MBit/s for EXI encoded data traffic is needed. Figure 14 depicts the data rate for inter charge point communication after optimization of LC service without losing functionality.

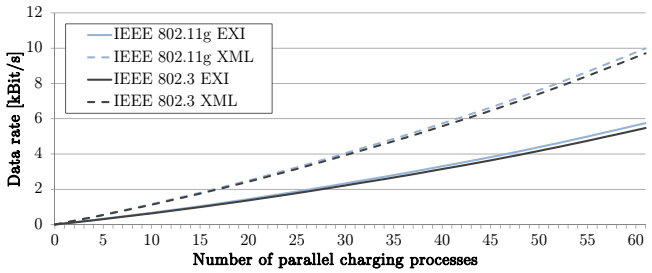


Fig. 14. Overview of the data rate for inter charge point communication using IEEE 802.3 and IEEE 802.11g with optimized LC

It can be seen that 99.8 % of inter charge point data traffic can be saved using the optimized load coordination. Only 5.7 kBit/s are needed for EXI encoding. Because of the low data rates, no packet errors occur in this scenario. In future work higher scale networks are analyzed e.g., for the year 2050 where we expect a maximum of 502 charge points regarding predictions of [11].

IV. Conclusion

This paper analyzed an application scenario for charging electric vehicles at work. At the beginning predictions of the German Government on the market penetration of EVs are presented. Based on these predictions a parking area at TU Dortmund was determined for installing a charge point network with a sufficient number of charge points supporting fast charging. For evaluating the ability of IEEE 802.11g, IEEE 802.3 and Homeplug GreenPhy for this scenario, the simulation environment prEVail based on OMNeT++ was presented. After that an optimized Charging Process Protocol was introduced, which supports communication between EV, EVSE, LC and EMHub. After that the V2G communication between EV and EVSE using Homeplug GreenPHY and the charging process protocol was analyzed and enhancements are presented for XML and EXI transmission. 41 % of data could be save using EXI and the small PB Size of 136 octets. For the communication link to the back-end a data concentration mechanism was presented showing an optimized data volume of factor 7 with 20 parallel charging processes. The data traffic within the charge point network was determined for authentication, billing and a worst case scenario enabling load coordination was introduced. With 61 charging EVs a data rate of only 5.7 kBit/s is needed for optimized load coordination and clearing, where the data traffic can be reduced by 99.8 %. Hence, no packet errors could be detected in this large scale application scenario for the year 2030.
In future work wide area communication technologies can be integrated into the simulation environment in order to calculate the data rates for the back-end communication depending on the physical layer. Also an integration of IPv6 is useful for higher scale charge point networks to simulate charging infrastructures for the year 2050. Furthermore the optimal position of a data-hub at the parking area at TU Dortmund will be determined using a raytracing environment for an estimation of the radiowave propagation of mobile communication networks. An analysis of a charging at home scenario would also lead to interesting results.

Acknowledgment

The work in this paper was partly funded by the German Federal Ministry of Economics and Technology as part of the e-IKT project with reference number 01ME09012 and as part of the TIE-IN project with reference number 64.65.69-EM-1022A funded by th *NRW Ziel 2* Program 2007-2013 (EFRE) of the European Union, the MWEBWV NRW and the MKULNV NRW. The authors would like to thank all partners for fruitful discussions in both projects.

References

[1] German Federal Ministry of Economics and Technology, *Energieszenarien für ein Energiekonzept der Bundesregierung (Case scenario for an energy strategy issued by the German Government), http://www.bmwi.de*, 2010

[2] C. Lewandowski, J. Schmutzler, and C. Wietfeld, *A Simulation Environment for Electric Vehicle Charging Infrastructures and Load Coordination*, Informatik für die Energiesysteme der Zukunft, Gesellschaft für Informatik e.V. (GI), 2010

[3] *Fleet of vehicles in January 2011, http://www.kba.de*, February 2011

[4] Federal Ministry of Transport, Building and Urban Development, *Szenarien der Mobilitätsentwicklung unter Berücksichtigung von Siedlungsstrukturen bis 2050 (Mobility development scenarios with consideration of settlement patterns in 2050)*, Final Report, 2004

[5] A. Varga and R. Hornig. *An overview of the OMNeT++ simulation environment*, In Proc. of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks (EFRE)tems (ICST), pages 110, Brussels, Belgium, 2008.

[6] INET Framework for OMNeT++ 4.0 Documentation. http://inet.omnetpp.org/, March 2010

[7] *HomePlug GREEN PHY Specification, Release Version 1.00*, 14-June 2010

[8] *JWG ISO/TC 2/SC 3 - IEC/TC 69: Vehicle to grid communication interface (V2G CI)*

[9] D. Peintner, H. Kosch, and J. Heuer, *Efficient XML Interchange for rich internet applications*, IEEE International Conference on Multimedia and Expo 2009, pp. 149-152, New York, USA

[10] J. Schmutzler, U. Bieker, and C. Wietfeld, *Network-centric Middleware supporting dynamic Web Service Deployment on heterogeneous Embedded Systems*, 14th International Conference on Concurrent Enterprising, 23rd-25th June 2008, Lisboa, Portugal.

[11] German Institute of Economic Research, *Elektromobilität: Kurzfristigen Aktionismus vermeiden, langfristige Chancen nutzen (Electric Mobility: Avoid short-term activism, use long-term opportunities), Weekly Report of DIW No.27-28/2010*

 ISBN: 978-1-61208-166-3