EMERGING 2013

The Fifth International Conference on Emerging Network Intelligence

ISBN: 978-1-61208-292-9

September 29 - October 3, 2013

Porto, Portugal

EMERGING 2013 Editors

Michael D. Logothetis, University of Patras, Greece

EMERGING 2013

Foreword

The Fifth International Conference on Emerging Network Intelligence (EMERGING 2013), held between September 29 and October 3, 2013 in Porto, Portugal, continued a series of events meant to present and evaluate the advances in emerging solutions for next-generation architectures, devices, and communications protocols. Particular focus was aimed at optimization, quality, discovery, protection, and user profile requirements supported by special approaches such as network coding, configurable protocols, context-aware optimization, ambient systems, anomaly discovery, and adaptive mechanisms.

Next-generation large distributed networks and systems require substantial reconsideration of exiting 'de facto' approaches and mechanisms to sustain an increasing demand on speed, scale, bandwidth, topology and flow changes, user complex behavior, security threats, and service and user ubiquity. As a result, growing research and industrial forces are focusing on new approaches for advanced communications considering new devices and protocols, advanced discovery mechanisms, and programmability techniques to express, measure and control the service quality, security, environmental and user requirements.

We take here the opportunity to warmly thank all the members of the EMERGING 2013 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 who dedicated much of their time and efforts to contribute to EMERGING 2013. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

Also, this event could not have been a reality without the support of many individuals, organizations, and sponsors. We are grateful to the members of the EMERGING 2013 organizing committee for their help in handling the logistics and for their work to make this professional meeting a success.

We hope that EMERGING 2013 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in the area of emerging network intelligence.

We are convinced that the participants found the event useful and communications very open. We hope that Porto, Portugal, provided a pleasant environment during the conference and everyone saved some time to enjoy the charm of the city.

EMERGING 2013 Chairs:

EMERGING Advisory Chairs

Raj Jain, Washington University in St. Louis, USA
Michael D. Logothetis, University of Patras, Greece
Tulin Atmaca, IT/Telecom&Management SudParis, France
Phuoc Tran-Gia, University of Wuerzburg, Germany
Nuno M. Garcia, Universidade Lusófonas de Humanidades e Tecnologias, Lisboa, Portugal

EMERGING 2013 Industry Liaison Chairs

Tadashi Araragi, Nippon Telegraph and Telephone Corporation – Kyoto, Japan
Robert Foster, Edgemount Solutions - Plano, USA

EMERGING 2013 Research Chairs

David Carrera, Barcelona Supercomputing Center (BSC) / Universitat Politecnica de Catalunya (UPC), Spain
Daniel Scheibli, SAP Research, Germany

EMERGING 2013

Committee

EMERGING Advisory Chairs

Raj Jain, Washington University in St. Louis, USA
Michael D. Logothetis, University of Patras, Greece
Tulin Atmaca, IT/Telecom&Management SudParis, France
Phuoc Tran-Gia, University of Wuerzburg, Germany
Nuno M. Garcia, Universidade Lusófonas de Humanidades e Tecnologias, Lisboa, Portugal

EMERGING 2013 Industry Liaison Chairs

Tadashi Araragi, Nippon Telegraph and Telephone Corporation – Kyoto, Japan
Robert Foster, Edgemount Solutions - Plano, USA

EMERGING 2013 Research Chairs

David Carrera, Barcelona Supercomputing Center (BSC) / Universitat Politecnica de Catalunya (UPC), Spain
Daniel Scheibli, SAP Research, Germany

EMERGING 2013 Technical Program Committee

Mercedes Amor-Pinilla, University of Málaga, Spain
Richard Anthony, University of Greenwich, UK
Tadashi Araragi, NTT Communication Science Laboratories - Kyoto, Japan
Tulin Atmaca, IT/Telecom&Management SudParis, France
M. Ali Aydin, Istanbul University, Turkey
Robert Bestak, Czech Technical University in Prague, Czech Republic
Christian Blum, IKERBASQUE - Basque Foundation for Science University of the Basque Country, Spain
Indranil Bose, Indian Institute of Management – Calcutta, India
Mieczyslaw Brdys, University of Birmingham, UK
Horia V. Caprita, "Lucian Blaga" University of Sibiu, Romania
Chin-Chen Chang, Feng Chia University - Taichung, Taiwan
Chi-Hua Chen, National Chiao Tung University, Taiwan, R.O.C.
David Chen, University of Bordeaux – Talence, France
Dong Ho Cho, Korea Advanced Institute of Science and Technology (KAIST) - Daejeon, Republic of Korea
Carl James Debono, University of Malta, Malta
Frank Doelitzscher, Furtwangen University, Germany
Rolf Drechsler, University of Bremen, Germany
Jean-Michel Dricot, Université Libre de Bruxelles, Belgium
Dimitris Drikakis, Cranfield University, UK
Thaddeus Onyinye Eze, University of Greenwich, U.K.

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

A Lightweight Messaging Protocol for Smart Grids

Eric MSP Veith*, Bernd Steinbach† and Johannes Windeln‡

*‡Institute of Computer Science
Wilhelm Büchner Hochschule
Pfungstadt, Germany
e-mail: eric.veith@wb-fernstudium.de

*†Institute of Computer Science
Freiberg University of Mining and Technology
Freiberg, Germany
e-mail: veith@mailserver.tu-freiberg.de

***Abstract*—The smart grid concept introduces more software control at both endpoints of the energy consumption chain: The consumer is integrated into the grid management using smart metering, whereas the producer will be host to a distributed agent-based software approach. Including more renewable energy sources in the energy mix will increase the necessity for a finer-grained, automatic control of changes in the energy level. Such changes need to be communicated for a distributed system to be able to calculate supply and demand. We therefore propose in this paper a lightweight protocol, which can be implemented on top of existing technology providing the needed communication interface. We also specify common behavior and protocol semantics for all implementing nodes, which forms the basis of a distributed, decentralized demand and supply calculation in a future energy grid.**

Keywords*—*smart grid; messaging; protocol description; renewable energy sources

I. Introduction

The term "smart grid" unifies a number of concepts related to an automated, information-supported management of the energy grid. In his paper "integration is key to smart grid management" [1], J. Roncero shows how different technologies are involved in the rather abstract smart grid concept.

Although a tighter integration of customers via smart metering is considered one of the cornerstones of a smart grid, the increased usage of renewable energy sources will also play an important role. However, although better appliances lead to a more efficient usage of renewable energy sources, this also leads to a higher dependence on energy which is not entirely controllable by the utility, since energy generated by wind parks or solar panels depends on the wind speed or solar radiation, more specifically, the weather.

This means that there are variances on both sides of the producer-consumer chain. Forecasting, as it is already employed via, for example, standard load profiles, helps to create more certainty regarding the variances itself, but it will also increase the number of calculations needed and the amount of data analyzed. One could therefore argue that a "divide et impera" approach is necessary, which leads to a decentralized, agent-based infrastructure. Such an approach, however, needs an information interchange protocol.

In this paper, we propose a lightweight protocol which can be used in such a grid based on distributed software and control. It will define certain basic protocol semantics which will enable this grid to organize itself based on the information available. This protocol, as described here, is not based on a specific implementation: We propose the fields required and how they are used but refrain from creating a bit-for-bit specification. This protocol can, however, easily be implemented on layer 7 of the ISO/OSI protocol stack using, for example, JavaScript Object Notation [2] (JSON) as a common data interchange format.

The remainder of the paper is structured as follows: After describing our initial motivation in Section II, we will outline the basic protocol structure in Section III, along with common behavioral rules in Section IV. Afterwards, Section V will describe the different types of messages available in the protocol. The discussion in Section VI will show how the protocol can be applied and outlines several scenarios and the protocol's behavior therein. We conclude with our plans for future work in Section VII.

Since this paper describes a protocol, requirement levels for implementors must be clear. In Sections III–V, this paper makes use of the keywords listed in RFC 2119 [3]. This includes "must", "must not", "required", "shall", "shall not", "should", "should not", "may" and "optional".

II. Motivation

The International Electrotechnical Commission's IEC 61850 standard has first been issued for communication within a subsystem automation system [4], but, in the meantime, has been expanded to other applications as well [5]. Higgins et al. [6] show how IEC 61850 can effectively be used for automatic failover.

While IEC 61850 proposes a rich data model for smart grid devices, it does not define mechanisms for a pro-active, decentralized interaction of the different components. The increasing inclusion of renewable energy sources tied to external influences — like wind or solar radiation — also increases the need for an higher frequency of control messages.

These messages could be issued by a central control unit which observes the state of the whole or a part of the energy grid and, given all information available, decides on the proper course of action. Such a central control unit, however, must be properly equipped to handle the information load, must be equally well connected to avoid that the communications infrastructure becomes a bottleneck, and must be extendible to add features which help towards a more pro-active operation, such as forecasting.

 ISBN: 978-1-61208-292-9

Since such a central control unit also poses a single point of failure, it is often assumed that a de-centralized layout of cooperating agents would be a better approach [7]. This would not concentrate the control logic in one point, but distribute it over the grid. Such a distributed system would need a protocol that would allow for interchanging information critical to the actual operation.

IEC 61850 offers a very fine-grained data model for electric grids. However, it misses a simple protocol mechanic that would be applicable in the distributed supply-demand calculation that immediately becomes necessary in a smart grid consisting of distributed agents. These agents would have to interchange information about the energy state, i.e., demand or over-supply that is introduced by weather changes or consumer behavior. A projected increase in wind speed at evenings would lead to an over-supply, whereas employees returning home at a projected time of 6pm would mean a demand.

These two simple examples show how the need for a distributed supply-demand calculation arises. We therefore propose a lightweight, simple high-level protocol that can form the basis of this calculation.

While the protocol as it is described here is not based on IEC 61850 per se, it can still be used on top of IEC 61850 by employing an appropriate application programming interface (API). In fact, we avoid to enforce implementation details wherever possible to make a widespread adaption possible.

III. Basic Protocol Structure

Nodes within the grid exchange data via *Connections*. A connection is, to the protocol, a virtual concept which resides in layer 7 of the ISO/OSI protocol stack. As such, it is not tied to Internet Protocol (IP) addresses or other concepts of lower levels in the ISO/OSI stack. Connections must be end-to-end; they are bi-directional communication channels between exactly two nodes. Concepts such as multicast must be realized on top of this.

A connection serves two purposes. First, it identifies the two endpoints. Second, by establishing a (largely virtual) network of nodes and connections, this protocol creates a communications structure that resembles the actual power grid, recreating it on top of any other networking structure, such as an IP-based wide-area network (WAN). This way, the power grid and the telecommunications infrastructure do not have to match in their layout. The layout recreation algorithm must be implemented by the actual connection facilities which, e.g., map to an IP network.

Having those virtual connections represent the actual physical power supply line also enables us to model “dumb” cables, which have no other properties than a maximum capacity and a line loss. Taking these attributes into account, the actual power transfer becomes part of the protocol. Smart power supply lines which are equipped with, e.g., metering devices, become nodes of their own. The simple power line–connection unit then evolves into a connection–power line–connection building block, which also adheres to the protocol semantics described in the following section.

Messages can travel further than the node–connection–node boundary. To enable nodes to answer to requests which do not originate from their immediate neighbors, each node must be uniquely identifiable. The *Sender ID* of a node must be unique at any given time. It is an opaque bit array of arbitrary length and must not contain any additionally information about the node itself or anything else. Generating an universally-unique identifier (UUID) [8] whenever the node’s software boots is one way to get such an identifier.

Each message must contain an unique identifier (*ID*). This is important since messages fall into two distinct categories: requests and answers. A request is sent actively by a node because of an event which lies outside the protocol reaction semantics, such as a changed power level. Answers are reactions which occur because of the protocol semantics as described below. Since any reaction pertains to an original action, it needs to identify this action, which is the reason for the unique identifier of each message. Reactions must carry a new, unique identifier, too.

The type of the message must be denoted by a *Message Type* field. The mapping is outlined in Table 1. These numbers are simple integer values with no coded meaning whatsoever. We do not distinguish between message classes or priorities here: The goal of the protocol is to remain simple, and we believe that the message types outlined here suffice in reaching the primary goal of the protocol, i.e., energy supply-demand mediation.

A message must also contain a *Timestamp Sent* field denoting the time and day when the message was initially sent as an Unix Timestamp (see [9] for the definition of the Unix Timestamp).

To prevent messages from circulating endlessly, a time-to-live (TTL) field is introduced. This TTL has the same semantics as the IP TTL [10] field: It starts at a number greater than 0. Whenever a message is forwarded or sent, the TTL is decremented by 1. If the TTL reaches 0, the packet must not be forwarded or otherwise sent but must be discarded. Messages with a TTL value of 0 may be processed.

Additionally, an *Hop Count* is introduced. The Hop Count is the reverse of the TTL: It starts with 0 and must be incremented upon sending a message. It allows to measure the distance between two nodes in the form of hops.

A message must carry an *Is Response* flag to distinguish original requests from responses. If the *Is Response* flag is set, the ID of the original message is contained in the *Reply To* field. If Is Response is not set, the Reply To field must not be evaluated; however, if a response is indicated, *Reply To* must contain a value which must be evaluated by the receiving system.

An answer must also contain the original message’s *Timestamp Sent* field (in addition to its own), and the *Timestamp Received* denoting the time when the original message was received.

To summarize, each message must contain at least the fields of the following enumeration. In parentheses, we give a proposition of the identifier that could be used in an actual

 ISBN: 978-1-61208-292-9

Value	Type
0	Null Message
1	Echo Request
2	Echo Reply
3	Online Notification
4	Offline Notification
5	Demand Notification
6	Offer Notification
7	Offer Accepted Notification
8	Offer Acceptance Acknowledgement
9	Offer Withdrawal Notification

Fig. 1. Message Types

implementation.

1) message ID (`ID`)
2) message type (`type`), see Figure 1 above
3) original sender ID (`sender`)
4) timestamp sent (`sent`)
5) TTL (`TTL`)
6) hop count (`hops`)
7) is response (`isResponse`)

The message type defines what additional values a message carries; these message types are described in Section V. The message type itself is a simple integer value field with type-to-number mapping shown in Table 1.

If *Is Response* is true, the following fields must be added:

1) reply to (i.e., original message ID) (`replyTo`)
2) timestamp received (`received`)

IV. Common Protocol Semantics

The following rules must be applied to each message, regardless of their type.

First, a message must not be ignored ("no-ignores" rule).

All messages except the *Null Message*, the *Echo Request Message* and the *Echo Reply Message* must be forwarded, partially answered and forwarded, or answered. This is the "match-or-forward" rule. It becomes important with requests and offers and is it further specified in Subsections V-F and V-G.

Forwarding denotes the general process of receiving a message and resending it. The message may be modified in this process, for example, the requested energy level must be lowered when a node can fulfill a portion of the request (see below).

When forwarding, a given message must be sent on all connections except the connection on which the original message was received. This prevents message amount amplification: Would the receiver also send the message on the connection on which it was originally received, it would be useless since the original sender already knows about its offer or request. It would thus only lead to additional processing and unnecessary use of bandwidth ("forwarding" rule).

Each node must keep a cache of recently received messages. If a message is received again, it must not be answered or forwarded ("no-duplicates" rule).

V. Message Types

A. Null Message

The *Null* message is the simplest message available in the protocol. It contains no additional information besides the basic protocol fields each message carries.

Null messages can be used as a form of heartbeat information. This is especially useful on weak links, for example for a remote wind park which might only have a mobile phone (GSM) connection. It thus can be sent at regular intervals to keep the line open.

A Null message in JSON representation is shown as an example in Figure 2.

B. Echo Request Message

An *Echo Request* can be sent on any connection to see if the endpoint is still alive and reachable. It must be answered. An Echo Request must not be an answer, and it also must not contain any additional information.

C. Echo Reply Message

An *Echo Reply* is the answer to an *Echo Request*. It must always be an answer and thus cannot be sent independently. This message type also does not contain any additional information; the proposed common fields (*Timestamp Sent* and *Timestamp Received*) are sufficient for Round-Trip-Time measurements.

D. Online Notification

Using this message, a node in the grid can notify its neighbors that it is going online or will be online at a certain point in the future.

To actually be able to carry the second kind of information, i.e., going online at a certain point in the future, this message contains two additional fields: *Valid From* (`validFrom`) and *Valid Until* (`validUntil`). A message using validity dates must use the *Valid From* field and may optionally make use of the *Valid Until* field.

This concept of validity dates is used by other message types, too. It denotes a timespan between the time indicated by *Valid From* and *Valid To*, both inclusive. Both fields are Unix timestamps like, e.g., the *Timestamp Sent*. Whenever a node wants to indicate that a message is valid immediately, it places the current time and date in the *Valid From* field. A "valid until further notice" semantic can be achieved by omitting the *Valid Until* field entirely.

Any protocol implementor, however, must take care to adjust his implementation whenever the Unix timestamp data type changes. As the time of writing, a Unix timestamp of 64 bit width is typically used in modern operating systems, which provides enough seconds since 1.1.1970 for the whole lifetime of this protocol. Previously, the `time_t` C type was specified as having 32 bits, which meant that an overflow would happen on 19.01.2038, the so-called "year 2038 problem".

Note that the Unix timestamp also allows for negative values to represent times before 1.01.1970. Although this would not be a necessary feature in the terms of this protocol, we advise

 ISBN: 978-1-61208-292-9

```
{
ID: "c3e5aca2-616f-4003-bbc6-eb9e90335495",
type: 0,
sender: "2d60a262-903e-4f70-a9de-e4d9b83d2bb7",
TTL: 42,
sent: 1367846889,
hops: 23,
isResponse: false
}
```

Fig. 2. An example for a null message, encoded as JSON

against choosing an unsigned type as it would introduce the need for additional programing quirks for implementors.

An *Online Notification* may be forwarded, but can also be discarded. This type of message is important for all directly connected nodes, because it has influence on the wires connecting the originating and its neighbor nodes. Any change in power levels, however, will be communicated using demand/supply messages which will be described later.

E. Offline Notification

The *Offline Notification* is the counterpart of the aforementioned *Online Notification*. It notifies the neighboring nodes that the originating node will be offline (i.e., possibly disconnected from the grid), utilizing the same *Valid From* and *Valid To* timestamp fields.

Unlike the *Online Notification*, this type of message must be forwarded. It provides additional information to the energy supply/demand solving algorithms of other nodes, which get a chance to re-calculate their supply plans. It is assumed that a demand or supply message which reaches the node sending the *Offline Notification* means that the *Offline Notification* will also be received by the original sender of the demand/supply message since the hop count is the same both ways.

However, since the *Offline Notification* message does not contain a field supplying the change in the grid energy level when the shutdown happens, an additional supply/demand message must be sent if the node has influence on the grid's energy level.

F. Demand Notification

A *Demand Notification* message indicates the need for energy of a particular node. It carries the *Valid From* and *Valid To* fields.

Additionally and primarily, it carries the quantified demand for energy in watts in the *Power* (`power`) field. Fractions of watts are not supported, i.e., the lowest amount that can be requested is 1 W. The field must not be 0, as this would make the message itself superfluous. This field must not carry negative values; those would mean an offer which has its own message type.

Demand Notification messages must be forwarded if they cannot be (completely) fulfilled. Each node must try to react to a demand message, i.e., try to match it and supply the energy requested. This is called the "match-or-forward" rule as described above. If it cannot fulfill the demand, it must at least forward it under the semantics outlined in Section III.

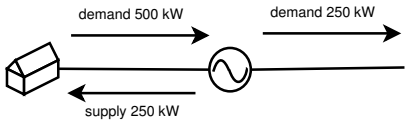


Fig. 3. A *Demand Notification* having the "match-or-forward" rule applied

If the node can supply the requested amount of energy completely, it must notify the requester using an *Offer Notification* message. It must not forward the original *Demand Notification* then.

If, however, the demand can only be partially fulfilled, the node must send an *Offer Notification* indicating the amount of energy that can be offered. It must then subtract this value from the original value indicated in the request and forward the thusly modified message. It must not change the message's ID or the message's sender ID ("same-ID" rule). The partial matching described in this paragraph is depicted in Figure 3.

A *Demand Notification* message must not be an answer.

G. Offer Notification Message

This type of message indicates an offer to the grid. It carries the fields *Valid From* and *Valid Until* as they are described in Subsection V-D and the amount of energy offered in the field *Power*. This number is an unsigned integer and is expressed in units of watts with no fractions possible.

Additionally, the offer includes a field *Cost*, which carries the cost of this offer in cents per kilowatt hour (ct/kWh). This allows for implementing cost-based policies, such as accepting energy only if it is cheap.

An *Offer Notification* may be an answer. If so, it is an answer to a previous *Demand Notification*, as described in the above subsection. A node receiving multiple offers must prefer offers of lower hop count over those with higher hop count. This favors micro-grids and reflects the actual flow of energy.

However, *Offer Notification* messages may also be sent as a request. This is the case whenever the agent estimates that it will output more power than it currently does. Consider for example a wind park which is dependent on the weather. If the agent's forecasting module predicts an increased wind speed in an hour and therefore an increased energy output, it may send an *Offer Notification* instead of pitching or stalling the wind turbines.

Just like a *Demand Notification*, such an original offer must be matched by nodes in the grid. The difference between an original offer and one that is an answer to a request is the value of the *Is Answer* field: If set to 0, the offer must be matched.

For matching and forwarding, the same mechanics as for the *Offer Notification* message type applies, especially if it can only be partly fulfilled.

H. Offer Accepted Notification

Whenever a request for energy is made and the offers have been received, there may arise a situation when more energy

 ISBN: 978-1-61208-292-9

is offered by all nodes than originally requested. For example, if a wind park, a solar park and a traditional power plant send *Offer Notification* messages after a request has been sent, the sum of energy offered is likely to exceed the original amount requested.

For this reason, a node must indicate which offer it accepts. Otherwise, all offers would be fulfilled, leading to an over-supply of energy in the grid which would be fatal.

As soon as the node finishes its demand/supply calculation, it must send *Offer Accepted Notification* messages to all nodes that were offering energy. In the body of the message, it must list the IDs of those nodes whose offer it takes. All other nodes will notice that their ID is missing from the notification and thus not actually deliver the energy they offered.

An *Offer Accepted Notification* must be an answer. It must also be sent of the node is taking on an original offer (as indicated above). In that case, the *Offer Accepted Notification* must be addressed to the offering node only, while the original offer must be forwarded if it cannot be completely fulfilled as described in Subsection V-G.

I. Offer Acceptance Acknowledgement

After an offering node has received an *Offer Accepted Notification*, it must reply with an *Offer Acceptance Acknowledgement* to indicate that the offer is still valid. This message type must always be an answer.

J. Offer Withdrawal Notification

If a node has offered a certain amount of energy, be it as an answer or as an original offer, and it can no longer stand up to the offer, it must withdraw it. This type of message is always an answer, carrying the ID of the original offer (in case of an original offer that was withdrawn) or the ID of the original request in the *Reply To* field.

If a node can still offer energy, but the amount has changed, the original offer must be withdrawn using this message type, and the new amount must be announced separately.

VI. Discussion

Based on the message types, the protocol structure and the semantics defined in the corresponding section, we will now illustrate how the protocol helps in a distributed supply-demand calculation. Therefore, we will not only discuss general properties of the protocol, but also present scenarios to show the protocol's behavior.

To support the goal of a distributed supply-demand calculation, the protocol must first and foremost help to make a demand or over-supply known. This is, of course, in the first place the task of the node itself; the protocol assists by merely providing a means to transport this change in the grid's energy level via the *Demand Notification* and *Supply Notification* messages.

A wind park, which is dependent on the weather, can already use the supply message to indicate changing power levels. Together with the validity dates, the wind park can also employ a forecasting algorithm to notify other nodes in the grid of the changed energy production beforehand.

Since the protocol uses virtual connections, the layout of the grid does not have to correlate with the layout of the communications network. That way, a simple WAN connection can be used and maintained while the virtual connections still allow all grid nodes to keep the same, consistent logical view on the energy grid.

This is important considering the normal current flow in a grid, which cannot be easily directed. Together with the protocol's rule to prefer messages with a lower hop count, a correct implementation of this protocol steers node behavior to mimic the energy grid's behavior. Thus, it automatically favors local micro grids and reduces load on the transmission system.

A change of the energy level, may it be imminent or forecasted, cannot go unnoticed since the "match-or-forward" rule applies to every node. Provided that a transport-layer protocol such as the Transport Control Protocol (TCP) [11] or the Stream Control Transmission Protocol (SCTP) [12] provides transport layer safety, a demand or supply message will reach other nodes. This separation of concerns accords with the ISO/OSI stack design principles.

However, the "match-or-forward" rule has one corner case where it can lead to an endless amplification in the number of messages currently circulating in the network: When none of the nodes can match the demand. In this case, a message must be discarded after a certain amount of time. This is done based on the TTL (time-to-live), which is a common rule also applied to IP packets. The initial TTL shall be user-configurable and must be high enough for a node's message to reach a destination which can answer the request.

The simplest layout involving a consumer and a producer exists when producer and consumer are directly connected. In this simple case, when the consumer demands more energy and the producer can match the request, it will answer with a message indicating the offer of the required amount of energy. This basic behavior is dictated through the requirement that each offer or demand message must be matched or forwarded.

On this basis, more complex layouts can also be tested. Consider the still rather simple, circular grid layout in Figure 4.

The consumer (labeled C), the factory pictured above, requests more energy. The request reaches the northern of the two transformers, which cannot influence the energy balance, but has to forward it based on the "match-or-forward" rule. The request message is copied and sent along both links, since a message must be sent on all links except the receiving one when forwarding ("forwarding" rule). The message reaches the two wind turbines P1 and P2 simultaneously, meaning that link latencies are ignored in this example.

If each one of them can provide half the amount of energy requested in the time frame it was requested for, it will send an offer and re-send the modified request. All four messages will then reach the conventional power plant, P3. This will also answer, in this example with the total amount of energy requested. The five messages on the wire will eventually reach

 ISBN: 978-1-61208-292-9

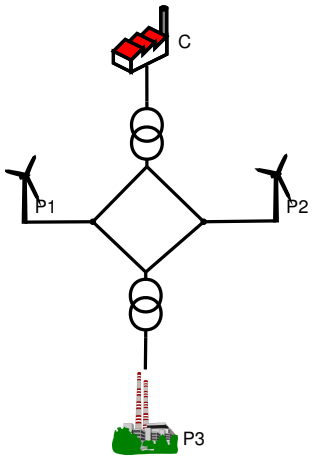


Fig. 4. A simplified, circular grid layout

P1, P2 and P3 again. By examining the message ID, which will remain the same even if the request was previously modified ("same-ID" rule), they can re-identify the message and will remain silent ("no-duplicates" rule).

The answers will eventually reach the requester, C. It will examine the offers and choose those made by P1 and P2 over the offer made by P3 since the message's hop counts are lower. This way, local renewable energy sources near to a requester are automatically preferred. Finally, the *Offer Accepted Notifications* are sent out, reaching P1, P2, and P3. Since P3 doesn't find its offer listed in the acceptance notifications, it will refrain from powering up later. As the last step, P1 and P3 acknowledge the process by sending out their *Offer Acceptance Acknowledgements*. The demand-supply calculation algorithm C has started when the need for energy became apparent then stops.

Please note that in both examples, the power line loss has been ignored. Such power line losses can either be described using the Connection attributes, or by creating "smart lines", which then become nodes of their own. Due to the "match-or-forward" and "forward" rules, the line loss is simply subtracted from the message's Power value.

It can easily be noted that neither the protocol's semantics nor its basic representation make an effort at security: We do not propose a message encryption or impose an authentication algorithm.

Partly, this is intentional: All nodes in the network shall be treated equally. However, using a public transport such as the Internet of course requires additional security measures to be taken. Since this protocol would be part of the ISO/OSI stack at level 7, we deem it sufficient to use the encryption/authentication facilities this stack already offers, such as IP Secruity [13] (IPsec).

IPsec offers the ability to create a public key/certificate chain infrastructure. Certificates would authenticate nodes in the same way as they authenticate an online-banking web server today. Certificate revocation lists can be used to block compromised nodes within the smart grid.

VII. Conclusion and Future Work

In this paper, we have outlined the ground rules of a messaging protocol which allows proactive communication of nodes in the Smart Grid. The goal was to enable each node, consumer and producer alike, to communicate their changing needs or offer for energy, while allows other nodes to pick up these pieces of information and act accordingly. This forms the basis of a tighter integration of renewable energy sources and allowing them to become more dominant in the energy mix, even though those sources might be dependent on external sources of influence outside our control, like the weather.

Proceeding further from that basis, we are going to propose an agent architecture for the Smart Grid nodes that adheres to this protocol. It will use the protocol semantics to implement a solver for the demand/supply calculation process.

We are also going to demonstrate how this protocol can be implemented using a standard IP network.

VIII. Acknowledgments

This paper has been created as part of a cooperative doctorate programme between TU Bergakademie Freiberg and Wilhelm Büchner Hochschule, Pfungstadt.

The author E. Veith would like to thank Nike C. Schmidt for her continuous organizational support.

References

[1] J. R. Roncero, "Integration is key to smart grid management," *CIRED Seminar 2008 SmartGrids for Distribution*, no. 9, pp. 25–25.

[2] D. Crockford, "RFC 4627 - The application/json Media Type for JavaScript Object Notation (JSON)," IETF RFC, IETF, Tech. Rep. [Online]. Available: http://tools.ietf.org/html/rfc4627 [Retrieved 2013-05-26]

[3] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," Internet Engineering Task Force, Fremont, CA, Tech. Rep. RFC 2119, March 1997. [Online]. Available: http://www.ietf.org/rfc/rfc2119.txt [Retrieved 2013-05-03]

[4] M. Kosakada, H. Watanabe, T. Ito, Y. Sameda, Y. Minami, M. Saito, and S. Maruyama, "Integrated substation systems-harmonizing primary equipment with control and protection systems," in *Transmission and Distribution Conference and Exhibition 2002: Asia Pacific. IEEE/PES*, vol. 2, 2002, pp. 1020–1025 vol.2.

[5] "Iec 61850 for power system communication."

[6] N. Higgins, V. Vyatkin, N.-K. Nair, and K. Schwarz, "Distributed power system automation with iec 61850, iec 61499, and intelligent control," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 41, no. 1, pp. 81–92, 2011.

[7] G. Zhabelova and V. Vyatkin, "Multi-agent Smart Grid Automation Architecture based on IEC 61850/61499 Intelligent Logical Nodes," *IEEE Transactions on Industrial Electronics*, no. 5, pp. 2351–2362.

[8] P. Leach, M. Mealling, and R. Salz, "Rfc 4122: a universally unique identifier (uuid) urn namespace," *Proposed Standard, July*, 2005.

[9] K. Thompson and D. M. Ritchie, *UNIX Programmer's Manual*. Bell Telephone Laboratories, 1975.

[10] S. Deering and R. Hinden, "RFC 2460 - Internet Protocol," 1998. [Online]. Available: http://tools.ietf.org/html/rfc2460 [Retrieved 2013-05-14]

[11] J. Postel, "Rfc 793: Transmission Control Protocol," 1981. [Online]. Available: http://tools.ietf.org/html/rfc793 [Retrieved 2013-03-19]

[12] R. Stewart, "Stream Control Transmission Protocol," RFC 4960 (Proposed Standard), Sep. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4960.txt [Retrieved 2013-05-13]

[13] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," RFC 4301 (Proposed Standard), 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4301.txt [Retrieved 2013-06-22]

 ISBN: 978-1-61208-292-9

Proposal and Evaluation of a Predictive Mechanism for Ant-based Routing

Naomi Kuze*, Naoki Wakamiya*, Daichi Kominami† and Masayuki Murata*
*Graduate School of Information Science and Technology, Osaka University
1-5 Yamadaoka, Suita, Osaka 565-0871, Japan
Email: {n-kuze, wakamiya, murata}@ist.osaka-u.ac.jp
†Graduate School of Economics, Osaka University
1-7 Machikaneyama, Toyonaka, Osaka 560-0043, Japan
Email: d-kominami@econ.osaka-u.ac.jp

***Abstract*—To tackle problems emerging with rapid growth of information networks in scale and complexity, bio-inspired self-organization is considered one of promising design principles of a new generation network, which is scalable, robust, adaptive, and sustainable. However, self-organizing systems would fall into a local optimum or converge slowly under some environmental conditions. Therefore, it may take a long time for self-organizing systems to adapt to environmental changes. In order to adapt to dynamically changing conditions of information networks, each component needs to predict the future state of its neighbors from their past behaviors and to adapt its movement to conform to the predicted states. There are several investigations into self-organization with prediction in the field of biology, but its application to information network systems and technologies needs more discussion. In this paper, we take AntNet, an ant-based routing protocol, as an example and consider a mechanism to accelerate path convergence with prediction. The proposed mechanism is compared with AntNet from viewpoints of the recovery time, path length, and control overhead. Simulation results show that our predictive mechanism can accelerate path convergence after environmental changes.**

Keywords-self-organization; prediction; routing; Ant Colony Optimization (ACO)

I. INTRODUCTION

Due to rapid growth of information networks in scale and complexity, conventional information network systems and technologies, which are based on central control or distributed control with global information, are to face limitations. An information network system adopting conventional control technologies suffers from the considerable overhead in managing up-to-date information to grasp dynamically changing conditions as the scale and mobility increase. Considering the problems that would emerge in future networking, there have been research activities such as GENI [1] and NSF FIA [2] in the USA, FP7 [3] in Europe, and the AKARI Project [4] in Japan to establish a novel network architecture and relevant technologies. Taking into account requirements for new generation networks, i.e., scalability, adaptability, robustness, and sustainability higher than ever before, the paradigm shift is needed to organize and control the whole network system in a fully distributed and self-organizing manner. Moreover, in order to realize information network systems and technologies, which can adapt to dynamically changing conditions in a timely manner, it is necessary that systems should be controlled considering the future state of systems, which is predicted by observing behaviors of systems.

Self-organization is a natural phenomenon of distributed systems, where components behave individually and autonomously. In a self-organizing system, they behave in accordance with simple rules and information locally available to a component. Through direct or indirect interactions among components, a global behavior or pattern emerges on a macroscopic level without central control. In a self-organizing system, the cost of information management can be considerably reduced since none needs up-to-date information of the entire system or many other components. Moreover, local failures and small environmental changes are handled locally and immediately by neighbor components without involving the entire system. Therefore, self-organizing system can recover from failures and adapt environmental changes automatically. In particular, biology is mines of self-organization models that can be applied to information networking such as routing, synchronization, and task assignment since biological systems are inherently self-organizing [5].

However, it is pointed out that self-organizing control has some disadvantages [6]. First, in a large-scale system, it may take a long time for a global pattern to emerge because it appears as a consequence of interaction between autonomous components. Second, self-organization, which uses only local information, would fall into a local optimum while a conventional system using global information can reach an optimal solution in most cases. Furthermore, a self-organizing system is not controllable in general, whereas unnecessity of control is one of the significant aspects of self-organization. These disadvantages lead to the slow adaptation to environmental changes in a self-organizing system. Ant Colony Optimization (ACO), which is a heuristic in the traveling salesman problem, is a mathematical model of foraging behavior of ants [7]. Because of the similarity, it has been adopted as a routing mechanism by many researchers [8], [9], [10]. Previous research shows

 ISBN: 978-1-61208-292-9

that AntNet is superior to conventional mechanisms in robustness against failure, control overhead, and communication performance [11]. However, the time required for path establishment to converge depends on the length of the path, i.e., the distance between a source node and a destination node [12]. Moreover, a considerable amount of control messages generated in path establishment depletes network bandwidth and hinders data message transmission.

In [13], a predictive mechanism was proposed for faster consensus in flocking birds. In self-organized flocking with a predictive mechanism, each component predicts the future state of its neighbors from their past behaviors and adapts its movement to conform to the predicted states. When applied to self-organized behavior of flocking birds, a predictive mechanism is considered to contribute to faster self-adaptation to environmental changes. There are several investigations into self-organization with prediction in the field of biology [14], [15], but its application to information network systems and technologies needs more discussion. In this paper, we adapt a predictive mechanism to ant-based routing since ant-based routing is a typical self-organizing system and its property and performance have been researched well.

In this paper, we take AntNet [16], which is an ant-based routing, as an example of self-organization based control and propose a predictive mechanism for AntNet. In an ant-based routing mechanism, a shorter path collects more pheromones than longer paths. Then the preferentially accumulated pheromones attract more ants that further deposit pheromones on the path. Such positive feedback eventually leads to all ants' following a single path. Therefore, a increase rate of pheromone values implicitly indicates the goodness of a path. In our mechanism, each node predicts a path that will obtain a large amount of pheromones from historical information about pheromone accumulation. Then, it boosts pheromone accumulation on the predicted path for faster convergence. We show that prediction helps adaptation to environmental changes through simulation experiments.

The reminder of this paper is organized as follows. First, we describe AntNet in Section II. Then we propose and explain a predictive mechanism for AntNet in Section III and give simulation results and discussion of our proposal in Section IV. Finally, in Section V, we provide conclusion and future work.

II. ANTNET

We use AntNet as a basis of our investigation of self-organization with prediction. In this section, we give a summary of a mechanism of AntNet.

A. Overview

AntNet [16] is an adaptive best-effort routing algorithm in packet-switched wired networks based on the principles of ACO. AntNet introduces two types of control messages called ants, i.e., *forward ants* and *backward ants*. A source node proactively launches mobile agents called forward ants at regular intervals. A forward ant stochastically selects a neighbor node to visit in accordance with the amount of *pheromones*, which are laid by ants. On a way to a destination node, a forward ant records its path and the time of arrival at each node in order to evaluate the quality of the travelled path.

When a forward ant arrives at the destination node, it changes to a backward ant. A backward ant returns to the source node on the disjoint reverse path of the forward ant, updating pheromone values along the way. When the path has better quality, i.e., smaller delay, a backward ant increases a pheromone value for the neighbor node it came more.

Each data packet is forwarded to a neighbor node as a next hop node according to the pheromone values that backward ants have updated. Since a neighbor node with a larger pheromone value is more likely to be selected, a data packet reaches a destination node following a shorter path.

B. Self-Organization based Path Establishment and Maintenance

In AntNet, each node has a pheromone table $\mathcal{T}^k$ as routing information. $\mathcal{T}^k = \{\mathcal{T}_d^k\}$ where $\mathcal{T}_d^k$ is a list of pheromone values $\tau_{nd}^k \in [0,1]$ for all neighbor node $n \in N_k$ regarding destination node d, i.e., $\mathcal{T}_d^k = \{\tau_{nd}^k\}$. N_k is a set of neighbor nodes of node k. Source node s establishes and maintains a path to destination node d by sending forward ants at regular intervals. A forward ant stochastically selects a next hop node to visit. The probability p_{nd} that neighbor node $n \in N_k$ is selected as a next hop node of node k for destination node d is given as follows.

If there is no pheromone information for destination node d at node k, a next hop node is randomly chosen.

$$p_{nd} = \begin{cases} 1, & \text{if } |N_k| = 1 \\ \frac{1}{|N_k|-1}, & \text{if } |N_k| > 1 \wedge n \neq v_{i-1} \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

Otherwise, selection is performed based on the pheromone value τ_{nd}.

$$p_{nd} = \begin{cases} 1, & \text{if } |N_k| = 1 \\ \frac{1}{|N_k|-1}, & \text{if } |N_k| > 1 \wedge {}^{\forall}n \in V_{s\to k} \wedge n \neq v_{i-1} \\ \frac{\tau_{nd}^k + \alpha l_n}{1+\alpha(|N_k|-1)}, & \text{if } |N_k| > 1 \wedge {}^{\exists}n \notin V_{s\to k} \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

where $V_{s\to k} = \{s, v_1, v_2, \cdots, v_{i-1}\}$ is a list of nodes that the forward ant has visited before arriving at node k at the i-th step and v_{i-1} is an identifier of the $(i-1)$-th node on the path. l_n is a variable indicating the degree of congestion for neighbor node n at node k, which is given by $1 - \frac{q_n}{\sum_{j\in N_k} q_j}$ and q_n is the number of messages waiting in a sending buffer for neighbor node n. $\alpha \in [0,1]$ is a coefficient. A

larger α allows forward ants to select a next hop node in accordance with local traffic condition. As a consequence, path convergence becomes hard to accomplish. On the contrary, with α close to zero, a path traversing congested links would be established. A forward ant whose travelled hop count reaches the predetermined TTL is discarded at a node.

A forward ant changes to a backward ant when it reaches the destination node d and returns to the source node s following the disjoint path that the forward ant traversed while updating pheromone values at visited nodes. The pheromone value τ_{nd}^k for neighbor node $n \in N_k$ at node k is updated by (3).

$$\tau_{nd}^k \leftarrow \begin{cases} \tau_{nd}^k + r(1-\tau_{nd}^k), & \text{if } n = f \\ \tau_{nd}^k - r\tau_{nd}^k, & \text{otherwise} \end{cases} \quad (3)$$

where f corresponds to the previous node that the backward ant visited just before arriving at node k, i.e., the first node of the path from the node to the destination node. r reflects the goodness of the path, on the transmission delay from node k to the destination node d. The smaller the delay is, the larger r is. Consequently, the shortest path among paths that forward ants found has the largest amount of pheromones and attracts most of forward ants.

The parameter r, which determines the increasing amount of pheromones, is evaluated from the trip time $T_{k\to d}$ and the local statistical model $\mathcal{M}^k = \{\mathcal{M}_d^k\}$, where $\mathcal{M}_d^k = \{W_k^d, \mu_d^k, \sigma_d^k\}$.

$$r = c_1 \left(\frac{W_k^d}{T_{k\to d}} \right) + c_2 \left(\frac{I_{sup} - I_{inf}}{(I_{sup} - I_{inf}) + (T_{k\to d} - I_{inf})} \right) \quad (4)$$

where $T_{k\to d}$ is the ant's trip time from node k to destination node d. W_k^d is the best traveling time of ants from node k to destination node d over the last observation window of size w, and (μ_d^k, σ_d^k) are the average and dispersion of the traveling time of ants over the last observation window. I_{sup} and I_{inf} are estimates of the limit of an approximate confidence interval for μ, which are given by (5) and (6).

$$I_{inf} = W_k^d \quad (5)$$

$$I_{sup} = \mu_d^k + z(\sigma_d^k/\sqrt{w}), \text{ with } z = 1/\sqrt{1-\gamma} \quad (6)$$

where c_1, c_2, and γ are coefficients, and (c_1, c_2, γ) is set to $(0.7, 0.3, 1.7)$ in [16].

C. Transmission of Data Messages

A data message is forwarded to a next hop node based on pheromone values, where the selection probability R_{nd}^k that neighbor node n is chosen as a next hop node for destination node d is given as $\frac{(\tau_{nd}^k)^\epsilon}{\sum_{j\in N_k}(\tau_{jd}^k)^\epsilon}$ ($\epsilon \geq 0$). Therefore, data messages follow the shortest path established by forward and backward ants.

III. Predictive Mechanism for AntNet

In this section, we propose a predictive mechanism for AntNet. We consider prediction only from pheromone changes and pheromone control with updating it independently of internal control in AntNet.

A. Overview

It is difficult for components to adapt faster to dynamically changing conditions of networks in a self-organizing system because each component uses only local current information. Therefore, we take AntNet as example of self-organization based control and consider a predictive mechanism in which components observe their past behaviors, predict the future state of the system, and then control their behaviors in accordance with the predicted future state.

In our proposal, we introduce *predictive ants* in addition to two types of control messages, i.e., forward ants and backward ants, and *increase rates of pheromone values* are adopted as an indicator for predictive control. Each node launches predictive ants at regular intervals. A predictive ant that arrives at a neighbor node remembers increase rates of pheromones in the neighbor node and returns to its originating node. On its return, the predictive ant boosts pheromone accumulation for the neighbor node for faster path convergence if its increase rates are high.

Each node has a pheromone table $\mathcal{T}^k$ as routing information. $\mathcal{T}^k = \{\mathcal{T}_d^k\}$ where $\mathcal{T}_d^k$ is a list of pheromone values $\tau_{nd}^k \in [0,1]$ for all neighbor node $n \in N_k$ regarding destination node d, i.e., $\mathcal{T}_d^k = \{\tau_{nd}^k\}$. N_k is a set of neighbor nodes of node k. At the beginning, τ_{nd}^k is initialized to $\frac{1}{|N_k|}$. In our proposal, forward ants and backward ants behave similar to AntNet. That is, a forward ant stochastically selects a next hop node to visit in accordance with pheromone values by (1) and (2), and the pheromone value is updated by backward ants by (3). The pheromone value is used for next-hop selection by ants and data messages.

B. Increase Rates of Pheromone Values

In our proposal, each node also has a increase rate table $\mathcal{E}^k$ for prediction. $\mathcal{E}^k = \{\mathcal{E}_d^k\}$ where $\mathcal{E}_d^k$ is a list of increase rates of the pheromone values $e_{nd}^k \in [0,1]$ for all neighbor node $n \in N_k$ regarding destination node d. At the beginning, e_{nd}^k is initialized to zero.

Node k that receives a backward ant from node $f \in N_k$ updates the increase rate $e_{nd}^k \in [0,1]$ of all its neighbor nodes $n \in N_k$ regarding destination node d by (7).

$$e_{nd}^k \leftarrow \begin{cases} (1-\beta)e_{nd}^k + \beta, & \text{if } n = f \\ (1-\beta)e_{nd}^k, & \text{otherwise} \end{cases} \quad (7)$$

where $\beta \in [0,1]$ is a parameter that determines the weight of individual increment of pheromones.

 ISBN: 978-1-61208-292-9

C. Behavior of Predictive Ants

In our proposal, each node k predicts better paths that will obtain a large amount of pheromones from sending predictive ants to its all neighbor node at regular intervals Δt_p. A predictive ant that arrives at neighbor node $f \in N_k$ remembers node f's increase rate table, i.e., $\mathcal{E}^f$, and returns to its originating node k while updating pheromone values at node k. The pheromone value τ^k_{nd} for neighbor node $n \in N_k$ at node k is updated by (8) if the max value in the increase rate table of node f regarding destination node d, i.e., max $e^f_{n'd}$ ($n' \in N_f$), exceeds 0.5.

$$\tau^k_{nd} \rightarrow \begin{cases} \tau^k_{nd} + p(1 - \tau^k_{nd}), & \text{if } n = f \\ \tau^k_{nd} + p\tau^k_{nd}, & \text{otherwise} \end{cases} \quad (8)$$

where p is a parameter that determines the increasing amount of pheromones. Even if the max value of $e^f_{n'd}$ exceeds 0.5, the pheromone values are not updated when $\mathcal{E}^f_d$ has not been updated since node f received a predictive ant from node k at the last time.

Each node starts to send predictive ants when it receives a backward ant, and it stops sending predictive ants when it does not receive backward ants for a fixed period of time.

D. Transmission of Data Messages

A data message selects a next hop node based on pheromone values in the same way as AntNet, where the selection probability R^k_{nd} that neighbor node n is chosen as a next hop node for destination node d is given as $\frac{(\tau^k_{nd})^\epsilon}{\sum_{j \in N_k} (\tau^k_{jd})^\epsilon}$ ($\epsilon \geq 0$). Therefore, data messages follow the shortest path established by forward and backward ants.

IV. Performance Evaluation

In order to evaluate adaptability to environmental changes of our proposal, we evaluate the time to recover from traffic changes.

A. Simulation Settings

We distribute 100 nodes on a 10×10 grid with separation of 30 m. We appoint a node at the top-left corner as a source node and one at the bottom-right corner as a destination node. The communication range is set to 30 m. Therefore, each node can communicate with four neighbors. The coefficient α in (2) is set to 0.004. Other parameters of AntNet are set in accordance with their default settings [16].

In order to establish the path considering the traffic, l_n, which is a variable indicating the degree of congestion for neighbor node n at node k, is given by

$$l_n = 1 - \frac{\lambda_{kn} T_s}{\sum_{j \in N_k} \lambda_{kj} T_s} \quad (9)$$

where λ_{nk} corresponds to the average arrival rate of data packets to the queue for sending to node n at node k, and T_s corresponds to the average processing time per one data packet. The one-hop transmission delay at link (n, k) is given by

$$cost(n, k) = \frac{|(n, k)|}{15} + \frac{\rho_{nk}}{1 - \rho_{nk}} T_s \text{ [ms]} \quad (10)$$

where ρ_{nk} is the average utilization rate of link (n, k), which is given by $(\lambda_{nk} + \lambda_{kn})T_s$, and $|(n, k)|$ corresponds to the Euclidean distance between node n and node k ($= 30$ m). The average processing time T_s is set to 6.5 ms.

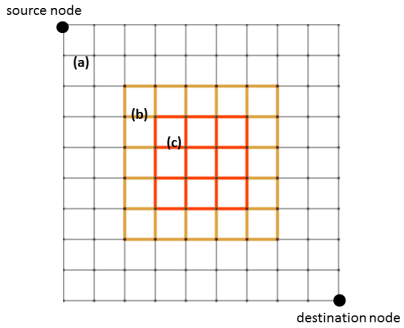


Figure 1. Network and congestion model in simulation where traffic near the center of the network increases after the network converges as shown in Table I.

Table I
Traffic changes in simulation

	(a)	(b)	(c)
λ (before)	$20 + R$	$10 + R$	$5 + R$
λ (after)	$20 + R$	$40 + R$	$60 + R$

In this evaluation, we evaluate the recovery time, control overhead, convergence rate of AntNet with and without prediction. We first have the network converge to a state where ants repeatedly select the same path using original AntNet. Convergence of the network is defined as a state where the same path is selected by forward ants for 10 consecutive times. Convergence check is done everytime a backward ant reaches a source node. After the network converges, we cause traffic changes. At the beginning of the simulation, λ_{nk} of links between 6×6 nodes in the center of the network is set to $10 + R$ packet/s, λ_{nk} of links between 4×4 nodes in the center of the network is set to $5 + R$ packet/s, and λ_{nk} of other links is set to $20 + R$ packet/s (R is a random number in $[-0.5, 0.5]$). Once the network converges, λ_{nk} of links between 6×6 nodes in the center of the network is increased to $40 + R$ packet/s, and λ_{nk} of links between 4×4 nodes in the center of the network is increased to $60 + R$ packet/s as shown in Figure 1 and Table I.

Regarding performance measures, the recovery time is defined as the time from the occurrence of environmental change till path recovery. Path recovery is defined as the time when the network is converged and total delay of a created path from the source node to the destination node is smaller than (the minimum delay) $\times$ 1.05. Path recovery

 ISBN: 978-1-61208-292-9

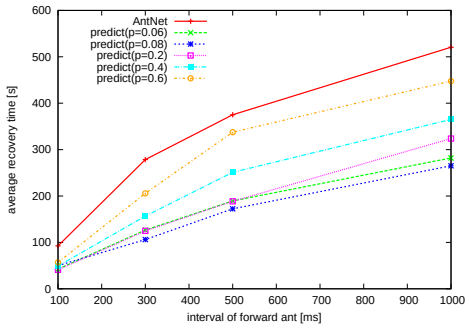


Figure 2. Path recovery time ($\Delta t_p = 100$ ms)

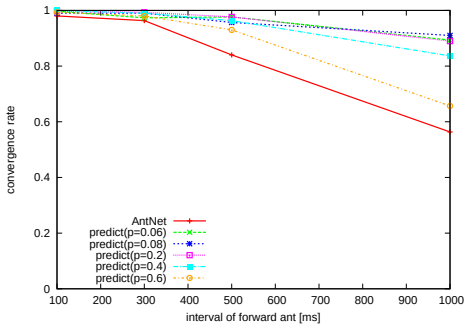


Figure 3. Convergence rate ($\Delta t_p = 100$ ms)

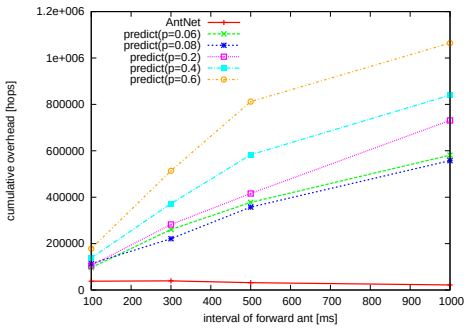


Figure 4. Cumulative overhead ($\Delta t_p = 100$ ms)

check is done everytime a backward ant reaches a source node. The control overhead corresponds to the total number of travelled hops of control messages until path recovery. The convergence rate is defined as ratio of path recovery within given simulation time, i.e., 1,000 s, to 300 simulation runs.

B. Results and Discussion

In this evaluation, the interval of predictive ant emissions, i.e., Δt_p, is set to 100 ms, and we change the interval of forward ant emissions from 100 ms to 1 s. The parameter β, which determines the weight of individual increment of pheromones in the increase rate of pheromones ((7)), is set to 0.2. The parameter p in (8) is changed from 0.06 to 0.6.

In each simulation, a path that runs through the center of the network is established by AntNet at first because the amount of traffic in the center of the network is small at the beginning of the simulation. Then, another path is reestablished avoiding the center of the network by AntNet or our proposal after traffic changes, i.e., the amount of traffic in the center of the network increases.

We show simulation results in Figures 2, 3 and 4. In these figures, the recovery time, convergence rate, and control overhead for the interval of forward ant emissions are depicted. The recovery time and control overhead in these figures show averaged values over 300 simulation runs for each interval of forward ants except for cases that convergence cannot be achieved by the end of a simulation run, i.e., paths fluctuate.

As shown in Figures 2 and 3, the recovery time of our proposal is shorter and the convergence rate of our proposal is higher than AntNet. Furthermore, our proposal is superior to AntNet regardless of the value of parameter p although we changes p widely. In original AntNet, a forward ant selects a next hop node in accordance with only current pheromone values. Then, most forward ants go through the path that has more pheromones than others even if there are other better paths. Therefore, it takes a long time to reestablish a shorter path when the quality of the existing path falls off because of environmental changes such as traffic changes. On the contrary, a next hop node is selected while taking changes of pheromone values into account in our proposal. Our proposal boosts pheromone accumulation on a shorter path whose pheromone values are still low but increasing, and this is the reason why path reestablishment after environmental changes is accelerated.

In our proposal, the recovery time is shorter and the convergence rate is higher especially when the parameter p is low as shown in Figures 2 and 3. In an ant-based routing mechanism, the stochastic path exploration in accordance with pheromone values plays an important role in the discovery of shorter paths. However, a forward ant selects a next hop node in an almost deterministic manner if the increasing amount of pheromones in our proposal is too large, i.e., p is too high. In consequence, a loose control with lower p leads to a better recovery time and a high convergence rate. Moreover, when p ranges between 0.06 and 0.2, there is not much difference in the recovery time and convergence rate in our proposal. In other words, we do not need to take so much care of parameter p setting.

As shown in Figure 4, control overhead of our proposal is much higher than that of AntNet. It is because each node that receives a backward ant regularly sends predictive ants to all its neighbor nodes for a fixed period of time in order to obtain neighbor nodes' information in our proposal. However, overhead of forward and backward ants is reduced because the recovery time is shortened with prediction. Moreover, overhead of predictive ants becomes trivial as the number of sessions becomes larger since predictive ants can collect increase rates for different destination nodes at one

 ISBN: 978-1-61208-292-9

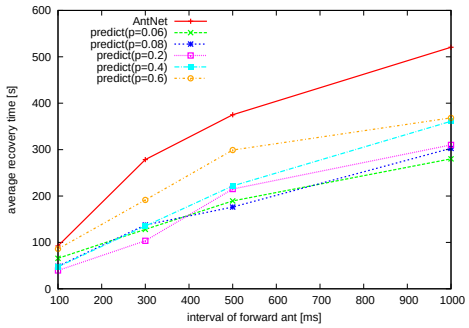


Figure 5. Path recovery time ($\Delta t_p = 1.0$ s)

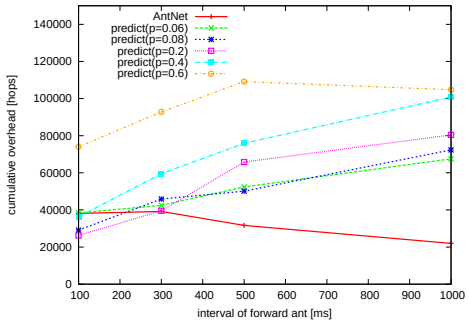


Figure 6. Cumulative overhead ($\Delta t_p = 1.0$ s)

time. It is noteworthy that control overhead can be much reduced with a larger interval ($\Delta t_p = 1.0$ s) of predictive ant emissions while the recovery time is kept shorter as shown in Figures 5 and 6.

In conclusion, the path recover from traffic changes is accelerated with prediction in this simulation settings. However, we need more discussion because the simulation setting is mere one case of network conditions.

V. Conclusion and Future Work

In a self-organizing system, each component behaves in accordance with only local current information, which leads to slow adaptation to environmental changes. Therefore, in order to adapt to dynamically changing conditions in a timely manner, it is necessary that systems should be controlled considering the future state of systems, which is predicted by observing behaviors of systems. In this paper, as an example of a predictive mechanism for self-organizing system, we propose and evaluate a predictive mechanism for AntNet. Simulation results show that our proposal can facilitate path reestablishment when the environment of the network changes. Even in a more realistic environment where ants are lost in the network, ants can reestablish other paths fast because they explore the network not deterministically but stochastically and positive feedback through pheromones leads to ants' following shorter paths.

As future work, we will evaluate our predictive mechanism in more real network environment, such as multiple sessions and a random topology.

References

[1] Global environment for network innovations (GENI), National Science Foundation, http://www.geni.net [retrieved: July, 2013].

[2] NSF future internet architecture project, National Science Foundation, http://www.nets-fia.net/ [retrieved: July, 2013].

[3] Seventh Framework Programme (FP7), European Commission, http://cordis.europa.eu/fp7/home_en.html [retrieved: July, 2013].

[4] New generation network architecture AKARI conceptual design, AKARI project, October 2007.

[5] M. Meisel, V. Pappas, and L. Zhang, "A taxonomy of biologically inspired research in computer networking," Computer Networks, vol. 54, no. 6, April 2010, pp. 901–916.

[6] F. Dressler, Self-organization in sensor and actor networks. Wiley, January 2008.

[7] M. Dorigo, M. Birattari, and T. Stutzle, "Ant colony optimization," Computational Intelligence Magazine, IEEE, vol. 1, no. 4, November 2006, pp. 28–39.

[8] K. Sim and W. Sun, "Ant colony optimization for routing and load-balancing: survey and new directions," Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, vol. 33, no. 5, September 2003, pp. 560–572.

[9] M. Saleem, G. Di Caro, and M. Farooq, "Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions," Information Sciences, vol. 181, no. 20, October 2011, pp. 4597–4624.

[10] K. Saleem and N. Fisal, "Enhanced ant colony algorithm for self-optimized data assured routing in wireless sensor networks," in Networks (ICON), 2012 18th IEEE International Conference on. IEEE, December 2012, pp. 422–427.

[11] S. Dhillon and P. Van Mieghem, "Performance analysis of the AntNet algorithm," Computer Networks, vol. 51, no. 8, June 2007, pp. 2104–2125.

[12] L. Carvelli and G. Sebastiani, Some Issues of ACO Algorithm Convergence. InTech, February 2011, ch. 4.

[13] H. Zhang, M. Chen, G. Stan, T. Zhou, and J. Maciejowski, "Collective behavior coordination with predictive mechanisms," IEEE Circuits and Systems Magazine, vol. 8, no. 3, August 2008, pp. 67–85.

[14] P. Montague, P. Dayan, C. Person, and T. Sejnowski, "Bee foraging in uncertain environments using predictive hebbian learning," Nature, vol. 377, no. 6551, October 1995, pp. 725–728.

[15] C. Summerfield, T. Egner, M. Greene, E. Koechlin, J. Mangels, and J. Hirsch, "Predictive codes for forthcoming perception in the frontal cortex," Science, vol. 314, no. 5803, November 2006, pp. 1311–1314.

[16] G. Di Caro and M. Dorigo, "AntNet: Distributed stigmergetic control for communications networks," Journal of Artificial Intelligence Research, vol. 9, December 1998, pp. 317–365.

 ISBN: 978-1-61208-292-9

Tiers-Lieu: Exploratory Environments for Service-Centred Innovations

Michel Leonard, Anastasiya Yurchyshyna
Institute of Services Science, University of Geneva
Battelle, Bâtiment A, 7 route de Drize,
Carouge, Geneva, Switzerland
{Michel.Leonard,AnastasiyaAnastasiya.Yurchyshyna}@unige.ch

***Abstract*—This paper introduces the concept of Tiers-Lieu, which is envisaged as an exploratory environment for service-centred innovations, and discusses its rationale within the context of the collaborative inter-disciplinary society. We present the approach facilitating discovery of initiatives as the result of the collaboration of actors from various domains: developing them in the process of negotiations and concretising them, in order to be further enabled by services. We discuss the difference between Tiers-Lieu and other types of collaborative environments, by illustrating its role in ensuring freedom in participation and semantic exchange for all creativity-oriented actors, independently from their domain, profession, and/or way of thinking.**

Keywords-Tiers-Lieu; service; initiative; service-centred innovation; interorganisational and interdisciplinary collaboration; collaborative environments.

I. INTRODUCTION

How may one characterise the current trends in Information Science and Service Science that have recently entered our world? Their growing importance reflects the requirements of the emerging world; a world transcending the familiarities of centuries past, due to the explosion of exchanges of every kind, in all its parts, the intermingling of cultures and the desire of individuals for cognitive freedom.

This emerging world requires the discovery of new cognitive environments, in order to organise different models for living together on all levels of Society, in all public, private and international sectors, in regional, national and international contexts. These cognitive environments will transcend those which we currently know. In particular, they will offer new answers to crucial challenges, such as disastrous hunger, epidemic cataclysms, poverty, energy deficits, and environmental, sanitary, medical, demographical, economic and financial crises.

This emerging world is born of a desire for universality to be facilitated by Internet technologies delivering an intensification of exchange that is without precedent in human history and has become one of the major factors defining the development of our society. It is remarkable that, despite a certain level of confidentiality and anonymity of Internet environments, they foster collaboration between the multitudes of initially unrelated actors and enable collective decision-making in innovation processes. In its turn, such collaboration ensures sustainability and coherent development of underlying processes, interoperability and service orientation in different domains (e.g., Internet of services [3], public service innovation [13], etc.).

By underlining the role of service orientation at multiple levels of technology and business, it is essential to clarify its meaning. It is stated that everything (i.e., good or activity) is seen as a service, and is analysed by an interdisciplinary approach of Service Science that brings together study, design, and implementation of services in which specific arrangements of people and technologies take actions that provide value for others [5]. This allows thus to concretise one of the leading visions for the systems development and integration [6], thanks to the service-oriented architecture (SOA).

These services-oriented trends, characteristic for our emerging world, lead to the shift of the role of Information and Communication Technologies, which are traditionally structured around isolated or specific services, and allow them to overcome the limits of their initial domains and to spread over trans-disciplinary branches of science and business. In this way, they support the dissemination of interoperable scientific knowledge and contribute to the development of practical intelligence [18] in our society, in general, and throughout these domains, in particular.

This paper is structured as follows. In Section 2, we analyze the role of creativity and innovation in developing business-oriented services. Some aspects of collaborative environments related to innovation are also discussed. In Section 3, the Tiers-Lieu concept is introduced and its characteristics are described. In Section 4, we discuss the main principles of Tiers-Lieu organisation. Finally, Section 5 concludes with the acquired results of this exploratory paper, and the scope of future works for developing Tiers-Lieu is identified.

II. TOWARDS INNOVATION: FROM KNOWLEDGE TO SERVICES THROUGH COLLABORATIVE ENVIRONMENTS

It is impossible to overestimate the role of knowledge for the development of our society. From one side, it is the primary production of resource; from the other side, knowledge ensures the possibility of value co-creation in services [17]. This nature explains the interdependence of knowledge and services-based characteristics of our emerging world, supports a tight interconnection between the phenomenon of services innovation and the requirements of the emerging society and guarantees the consistency of sustainable co-creation of the fundamental concepts of innovation-based information systems and services [9].

 ISBN: 978-1-61208-292-9

With the increasing role of Information Technologies (IT) in its everyday functioning, our society benefits from new and expanding communication channels that foster knowledge production and nurture its creativity-focused characteristics.

Indeed, the new society encourages its members to enact their willingness and ability to innovate and create and in doing so, to increase the added value of the corresponding economic processes. The innovation in services is thus seen as a process, whose objectives include the efficient delivery of existing services, service quality, and the generation of new types of services. This process requires continuous collaboration between different people of different skills and responsibilities, from multiple organisations and – very often – within an international and multicultural context.

From a different side, the increasing complexity of its processes, the multitude of involved actors, and the interdependence of the related domains is largely based on multiple collaboration processes. Recently, one can witness how the importance of collaboration grows exponentially, as the result of the development of Information and Communication Technologies, social networks and thematic clouds, which seem to contribute to decision-making processes, concretise the decisional context for different actors and remove geographical boundaries.

It has already become a common practice that enterprises and societies require certain level of collective intelligence from their members. Indeed, to ensure that a group of individuals successfully act together in a certain concrete environment [7], they should possess the ability to learn and reason, being willing and capable to act collectively thanks to their competences.

There have been numerous works aiming to support collaboration and collaborative group decisions. In [2], it is suggested to model collaboration by identifying its layers: goals, products, activities, patterns, techniques, tools and scripts, and by integrating all these layers into an organizing scheme, a conceptual representation of the next generation of collaboration support systems.

Another aspect of collaborative group decisions is studied in [8]: Keeney introduces a collaborative group decision model based on decision analysis techniques. The accent is put here on the explicit knowledge differences of judgments and values among group members, and an approach for taking them into account in the decision process is debated.

Some works specifically address the methods and techniques to improve group ideation [14]: to balance between the quantity and the quality of ideas generated and analysed during the process of ideation. Reinig and Briggs particularly note how cognitive inertia and scarcity of solution space may affect the ideation process and suggest the ways to overcome the possible negative effects.

In our previous research, we also address the problem of collaborative decision-making and discuss some challenges typical for collaborative environments [24]. This work presents the initial classification of the corresponding risks and introduces our approach for decision-constructing by the cross-pollination space, a collaborative environment for innovation in services.

The diversity of profound research aiming to encourage different aspects of innovation in services corresponds not only to the sectors of activity, but also the rationale for organisations, their business models, their relationships with their environments, especially in the international context. It becomes obvious that interdisciplinary work is required, which is to be translated into trans-disciplinary services and built using information technology. It is focused on combining human and collective knowledge with the computational capabilities of informatics, as well as combining human and collective activities with services. This will allow decision makers to move from a default position of reacting to events in their organisations to a more active one of anticipating them.

More concretely, on the level of the European Union, there has been achieved a significant success in the projects supporting innovation in services. For example, the set of initiatives facilitating public support for innovation and increasing its effectiveness is presented by the European Commission [12], whilst the measurability of innovation policies and their impact on productivity, quality and employment of services are analysed by Rubalcaba [F15]. Despite the acquired positive results, there are still important service innovation challenges to be addressed in services economies of our society. There are still a variety of obstacles that might stand on the way of the sustainable service innovation growth: e.g., market and systemic failures, over-regulation, market fragmentation and competition, to mention but a few. Probably less obvious, but more serious obstacles lie in the sphere of cognitive barriers and fears of all kinds (e.g., unemployment, professional non-security, unwillingness or incapacity to adapt to new types of organisations, etc.).

III. TIERS-LIEU: COLLABORATIVE ENVIRONMENTS FOR INNOVATIONS

The complexity of business, academic and social processes of our society, as well as the increasing role of collaborative creativity in development and innovation, require new advanced approaches and forms of organisation. To answer these challenges, we introduce the concept of Tiers-Lieu, study its characteristics and analyze its potential benefits.

A. Concept of Tiers-Lieu

Initially, the concept of Tiers-Lieu ("third place") was introduced by Roy Oldenburg [10] who identified third places, or "great good places", as new places intermediate between home and work, which are adapted to the new lifestyle with its elements of urbanisation, mobility and individualism and are central to local democracy as well as community vitality.

Such third places are neither private, nor public, and they offer the extended possibilities to work in a more informal environment, a certain hybrid between a personal and an open space. These are coffee shops, cultural centres, smoking lounges; the third places are largely the product of

 ISBN: 978-1-61208-292-9

human relationships, creative interaction and modes of social organisation and professional dominant contemporary societies [1].

In the spirit of Tiers-Lieu, several places of co-working have been recently developed. They are, for example, La Cantine [20], Festival Temps d'Images [21], tiers_lieu{x} [22]; all share the idea of open and creative co-working. As a different example, one can witness the work around meetings of Autrans 2012 [19], which gather international researchers and entrepreneurs interested in innovative Internet-related issues, open data, Tiers-Lieu, collaborative consumption new usages, etc.

It is important to note that this initial definition of Tiers-Lieu has significantly evolved during the recent years, and is no longer limited by geographical boundaries of places of co-working.

In our approach, we envisage Tiers-Lieu as an open environment of "third place" that motivates collaboration, intellectual creativity and surpasses the limits of traditional disciplines-defined collaborative spaces, by allowing defining new services.

B. Tiers-Lieu: What is different?

By its origin, Tiers-Lieu has an exploratory nature and creates the environments where transformations and changes are institutionalised and enable movements of innovations. We note also that Tiers-Lieu benefits from the work of the people from different organisations, but does not belong to any of them.

Tiers-Lieu aims to go beyond the creation of an environment when actors (professional or not, individuals or groups, formal or informal) gather around a discussion table, in order to exchange their ideas about a situation, an identified challenge, or a proposed initiative. In the majority of the existing collaborative environments, the skills of involved actors are to some extent pre-defined, according to the discipline of the discussed idea. Such a pre-definition ensures a certain level of consistency in these discussions; however, it seldom overcomes the cognitive closeness of the discussed idea, and is not truly trans-disciplinary.

It is the ambition of Tiers-Lieu to overcome the limits of such semantic closeness and to give the actors the possibility not only to discuss the problem but also to be able to understand it in terms of their own professions and beyond them. In this context, it is not merely the question of understanding the conceptual framework, technical principles, or usability of an innovative idea but beyond this, Tiers-Lieu aims at ensuring the acceptance of this idea by the actors, despite their possible resistance, lack of knowledge or foreseen expectations.

This way, Tiers-Lieu differs from traditional collaborative environments, as they are themselves the creators of values. This means they generate activities common for creative participants, independent from and not belonging to any participating organisation. Also, compared to traditional environments, the successful functioning of Tiers-Lieu relies on a higher level of interaction between non-professional actors and openness to their networks. By allowing such heterogeneity, Tiers-Lieu is boosting "cognitive interaction" between project leaders, managers and just interested people, the project leaders will develop their knowledge and skills to implement their entrepreneurial project. At the same time, it also encourages the democratisation of the action undertaken by accepting a wider audience.

As a result, Tiers-Lieu allows achievement of the unity of the idea, so that it must be concretised as a service. By answering this challenge, Tiers-Lieu thus proposes not only the creativity-oriented environment fostering innovations, but also the way how it can be concretised by services. It means that, in addition to the achieved results of traditional collaborative environments, Tiers-Lieu also ensures the development of services – either on the meta-level (by offering a methodology to propagate the discussed knowledge between and beyond the involved actors, e.g., how knowledge related to smart medicine is widespread in medicine and other involved domains), or for the concrete complex situation, which is the objective of this Tiers-Lieu (by offering a set of services aiming at solving this problem, e.g., usage of smart phones in the context of smart medicine).

C. Objectives of Tiers-Lieu

By summarizing the ideas towards the development of Tiers-Lieu, we can briefly describe its objectives as follows:

- Tiers-Lieu represents an utility, which is created to *develop a service*,
- Tiers-Lieu aims at *supporting an activity*,
- by *enabling initiatives*, suggested by involved actors and oriented to improve this activity;
- which can be achieved thanks to a *collaborative platform*,
- *concretised*, according to the requirements of sustainability of this activity and the general "*common sense*" vision;
- and which is developed upstream of the projects improving this activity.

In other words, Tiers-Lieu can be seen as a certain meeting that leads to service creation. As the result of its functioning, coherent and sustainable services will be developed. We note, however, that management and governing of such created services can remain within the scope of the initial Tiers-Lieu but can also overpass it, by extending their existance in other domains of business, government activities, private sector, etc.

D. Initiative as Key Concept of Tiers-Lieu

Tiers-Lieu is envisaged as an environment supporting innovations, which are concretised thanks to initiatives.

Let us study in more detail the phenomenon of the initiative, classically introduced at [4], and developed in the context of Service Science by [11], by analysing it in the context of Tiers-Lieu.

We envisage an initiative as a breakthrough proposition, which is inter-organisational, inter-disciplinary, inter-domain, aiming the creation of human-oriented and/or economic value and that concretises the semantics and leads to the realisation of one or several corresponding services.

 ISBN: 978-1-61208-292-9

We particularly note that an initiative with the related knowledge is not an object of protection (by copy-right, for example). It does not have the nature of consulting or project management; neither is it an instrument of education.

In Tiers-Lieu, initiatives are seen *upstream* of projects or services, which help to create the services for commercial products, research or business-oriented methodologies.

To conclude, the activities of Tiers-Lieu are thus regrouped around its initiatives, which respect the following conditions:

- An initiative of Tiers-Lieu must be *inter-organisational*: it should not belong to the only one organisation, but it must represent a general interest;
- An initiative of Tiers-Lieu must be *inter-disciplinary*: it should not be related to the only domain, but naturally aims to address interdisciplinary situations;
- It should take into account international aspects;
- It should create values in human, social and economic aspects;
- The initiative must be concretised in the form of one or several *trans-organisational* and *trans-disciplinary* services.

The results of an initiative could furthermore generate partnership agreements, internal or inter-organisational projects, new forms of organisations, innovative start-ups, especially in the context of interconnected services, net-ups, or other forms of value-creating organisations. Naturally, an initiative of Tiers-Lieu can give a start for new initiatives of the same – or different – Tiers-Lieu.

IV. ORGANISATION OF TIERS-LIEU

Tiers-Lieu is envisaged as an environment supporting innovations, which are concretised thanks to initiatives.

The activities that are supported by Tiers-Lieu are naturally discussed during the meetings of co-opetative nature concerning strategic questions typical for complex competition-based environments. Despite certain contradictions between the objectives of each actor, such environments require nevertheless a high level of collaboration in achieving common objectives. For example, while introducing new forms of bank services, IT standards or compliance norms, the necessity of coherent collaboration between direct competitors (e.g., leading companies in the sector), standardisation organisations and other interested parties have become a crucial factor.

There are no special limitations on the form of such meetings: they can be face-to-face, diffused by Internet, supported in real-time or asynchronous, or the mix of different forms.

In many cases, the main actors taking part in Tiers-Lieu are top executives of enterprises or non-commercial organisations, or – in general – decision-makers. However, the participation is open for other contributors: actively interested people, and is highly beneficial if various interesting – and multi-domain – ideas are exchanged.

In this context, it is important to underline that the participation in Tiers-Lieu is based on the acceptance of its members of the main principles of team creativity, their desire and ability to create collectively, to share the expert knowledge and the acquired results, to avoid innovation resistance [16] and to ensure participative safety, to improve the quantity and quality of attempts to introduce or develop new ideas [23].

It is agreed between the actors that innovative ideas are represented through initiatives which can dynamically change, according to the discussions. Before being selected and approved by all actors, initiatives can be modified, reorganised, abandoned, etc.

This implies the necessity for a formal definition of a protocol for such a meeting, allowing tracking the history and dynamics of ideas exchange, some principles for regulating roles and access of actors. In other words, the whole Tiers-Lieu infrastructure supporting creation and implication of initiatives for services creation should be established (Fig. 1).

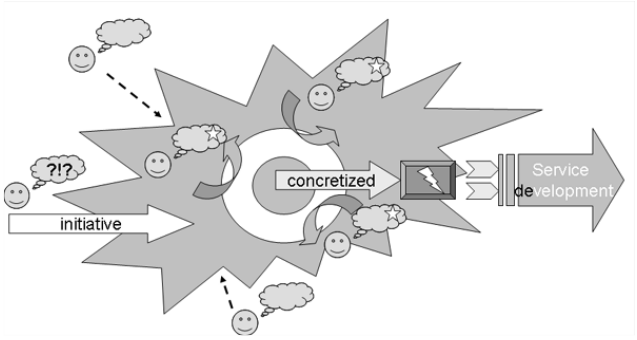


Figure 1. Tiers-Lieu: from initiative to service.

Since Tiers-Lieu represents creative collaborative environments that involve a lot of multidisciplinary actors, the organisation of Tiers-Lieu should respect certain principles.

Firstly, Tiers-Lieu is motivated by the spirit of the PPPP approach: they support and are oriented to private (P), public (P) partnerships (P) and people (P).

Secondly, to ensure the smooth organisation of discussions and the effectiveness of taken decisions, there should be a system of roles within Tiers-Lieu.

We start by identifying the following 6 roles:

- Initiators: actors, who come with a new innovative idea, define an initiative and invite other actors to discussions. Initiators are those who take the final decision, once the initiative is discussed and developed by others.
- Participants: actors, who actively contribute in discussions and help to develop the proposed initiative.
- Moderators: actors supporting the process of Tiers-Lieu functioning.
- Observers: actors, who assist at discussions and follow them, but are not actively participating in

 ISBN: 978-1-61208-292-9

them, i.e.,, the ones who do not have a word. Observers might have educational purposes (e.g., students) or just share the general interest for the discussed subject, without offering any concrete solutions (e.g., public).

- Historians (or secretaries): actors who play a supporting role: helping to register and track discussions and contributions of participants, introducing required information, keeping in order the agreed planning, etc.
- Developers: actors, whose aim is to develop a service, once the initiative has been defined and validated.

The role of the initiator is characterised by a high level of responsibility and is crucial for functioning of Tiers-Lieu. Indeed, it is the initiator who not only introduces a new initiative as a subject of innovation, but also defines the scope of participation within the scope of Tiers-Lieu. The initiator is also the one who evaluates the expressed ideas and has the final word on accepting or refusing them.

To facilitate the discussion procedure and to minimise the uncertainty in discussions, the initiator has a set of measures to keep the discussions fruitful, by attributing the participants a yellow card (warning about the semantic inconsistency or non-respect of the ethics of Tiers-Lieu) or a red card (serious breach of the rules or consistent contradiction with the main idea of the current initiative; this leads to the exclusion of the participant from this Tiers-Lieu). Analogically to football rules, two yellow cards in the same meeting constitute a red card.

A participant with a red card (or in fact any participant at any time) may leave this initiative and eventually launch an alternative initiative and a different Tiers-Lieu, which might have the same participants of the initial Tiers-Lieu. All initiatives are launched under the Creative Commons License, used when an author wants to give people the right to share, use, and even build upon a work that they have created.

It is remarkable that there are no limitations for the participants to contribute for multiple initiatives, as well as to leave them at any time.

It is important to develop a balanced system of ethics principles concerning the supported activity, and, consequently, the ethics principles defining the developed service.

Despite the self-motivation of the actors to participate in Tiers-Lieu, there should be developed a balanced approach for supporting their interest in sharing and increasing their knowledge about the complex situations, which require common effort, even under the risk of competition. Tiers-Lieu is becoming thus a good choice of a neutral environment, which can put together various actors for their "winning-winning" collaboration.

V. CONCLUSION AND FUTURE WORK

This exploratory paper addressed the challenge of supporting creative development of services with the help of collaborative environments. To answer the new requirements of our emerging society, it seemed insufficient merely to support existing working relationships between organisations, enterprises and academic institutions but necessary to offer them an independent "third place", Tiers-Lieu, which would help to people from different organisations to work together for and in benefit of their organisations. We noted that the results of their collaborative work should be concretised by the development of a service (or several services), might lead to defining a new project, and are, for example, supported by Creative Commons License.

In this paper, we introduced the concept of Tiers-Lieu, discussed its characteristics and analysed its role as an exploratory environment, allowing creativity-oriented actors freedom in participation, yet concretised by a system of rules. Such conceptual architecture reflected the idea that initiatives should not be limited to bottom-up or top-down ones but might come from everywhere, beyond the limits imposed by a certain form of organisation and/or conventions accepted within certain professions. This also meant that Tiers-Lieu was defined in the way to enable freedom of semantic exchange, and to overcome the limits of one domain, one profession, and/or one way of thinking.

Our future work is focused on formal definition of codes and principles of functioning of Tiers-Lieu. We also explore the role of the University, identify the risks and challenges of its current form for innovation-oriented discovery and services development, and analyse its potential improvement in the context of the vision of Tiers-Lieu. We envisage this approach to become a profound base in our work on exploring the phenomenon of the university, and its consecutive extension as a result of the new challenges our society has been currently offering.

REFERENCES

[1] P.Genoud, and A. Moeckli, "The third places, Places of emergence and creativity / Les Tiers-lieux, Espaces d'émergence et de créativité", 2010, retrieved online at http://lamusegeneve.files.wordpress.com/2010/03/03_patrick-genoud-alexis-moecli-2.pdf , last accessed 9/7/2013

[2] R. Briggs, G. Kolfschoten, G.-J. de Vreede, C. Albrecht, D. Dean, and S. Lukosch, "A Seven-Layer Model of Collaboration: Separation of Concerns for Designers of Collaboration Systems". In: Proc. ICIS 2009, Phoenix, Arizona, USA, December 15-18, 2009.

[3] J. Cardoso, K. Voigt, and M. Winkler, "Service Engineering for the Internet of Services". Enterprise Information Systems, Lecture Notes In Business Information Processing (LNBIP), Vol. 19, 2009, pp. 15–27

[4] R. Cohen, C. Allaby, C. Cumbaa, M. Fitzgerald, K. Ho, B. Hui, C. Latulipe, F. Lu, N. Moussa, D. Pooley, A. Qian, and S. Siddiqi, "What Is Initiative?" In: User Modeling And User-Adapted Interaction, 8(3-4), 1998, pp.171–214

[5] H. Demirkan, R. Kauffman, J. Vayghan, H. Fill, D. Karagiannis, and P. Maglio, "Service-oriented technology and management: Perspectives on research and practice for the coming decade". In: Electronic Commerce Research and Applications 7(4): 2008, pp. 356-376

[6] T. Erl, "SOA: Principles of Service Design", ISBN: 0132344823, Prentice Hall/PearsonPTR, 2008

[7] W. Guangbin, and C. Dongping, "Research on the Project-Level Influencing Factors on Information Technology

 ISBN: 978-1-61208-292-9

Implementation in Construction Industry". In: Proc. the Int. Conference on Management and Service Science MASS 2010: pp. 1-4, 2010

[8] R.L. Keeney, "The foundations of collaborative group decisions". In: International Journal of Collaborative Engineering, Inderscience Publishers, vol. 1, no. 1-2/2009, pp. 4-18

[9] M. Leonard, and A. Yurchyshyna, "Decision constructing as conceptualisation of service innovation". In: Proc. IJCSS2011, the International Joint Conference of Service Sciences, 25-27 May 2011, Taipei, Taiwan, 2011

[10] R. Oldenburg, "The Great Good Place: Cafes, Coffee Shops, Community Centres, Beauty Parlors, General Stores, Bars, Hangouts, and How They Get You Through the Day". New York: Paragon House, 1989.

[11] W. Opprecht, A. Yurchyshyna, A. Khadraoui, and M. Léonard, "Governance of initiatives for e-government services innovation". In: Proc. Electronic Government and Electronic Participation : Joint Proceedings of Ongoing Research and Projects of IFIP EGOV and ePart 2010. pp. 203-210

[12] PRO Inno Europe, "Making public support for innovation in the EU more effective". Paper No 13, 2009, available online at http://ec.europa.eu/enterprise/policies/innovation/files/swd_effectiveness_en.pdf, last accessed 13/08/2012

[13] D. Pym, R. Taylor, and C. Tofts, "Public services innovation through technology". Hewlett-Packard 2007, http://www.hpl.hp.com/techreports/2007/HPL-2007-22.pdf, 2007

[14] B.A. Reinig and R.O. Briggs, "On the Relationship Between Idea-Quantity and Idea-Quality During Ideation", Group Decision and Negotiation, 17(5), 2008, pp. 403-420

[15] L. Rubalcaba: "Service innovation and innovation policies: key challenges and implications", UNECE Applied Policy Seminar, 25 March 2010, available online at http://www.unece.org/fileadmin/DAM/ceci/ppt_presentations/2010/ic/rubalcaba.pdf, last accessed 13/08/2012

[16] J.N. Sheth, "Psychology of Innovation Resistance: The Less Developed Concept (LDC) in Diffusion Research". In: Research in Marketing ed. J. N. Sheth. 4. Jai Press Inc. 1981, pp. 273-282

[17] A. Smedlund, "Value Cocreation in Service Platform Business Models", In: *Service Science* March 2012 4:79-88

[18] J.M. Tien, and D. Berg, "A case for service systems engineering". In: Journal of Systems Science and Systems Engineering, Vol. 12, No. 1, 2003

[19] Web resource Autrans 2012, http://www.autrans.net/ [retrieved: June, 2013]

[20] Web resource La Cantine, http://lacantine.org/, [retrieved: June, 2013]

[21] Web resource Festival Temps d'Images, http://www.104.fr/, [retrieved: June, 2013]

[22] Web resource tiers_lieu{x}, http://www.tierslieux.net/ [retrieved: June, 2013]

[23] M.A. West, (Ed); and J.L. Farr, (Ed), "Innovation and creativity at work: Psychological and organisational strategies". Oxford, England: John Wiley & Sons, 1990, pp. 309-333

[24] A. Yurchyshyna, W. Opprecht, and M. Leonard, "Collaborative decision constructing supported by Cross-Pollination Space". In: Proc.International Conference on Advanced Collaborative Networks, Systems and Applications, COLLA'11, Luxembourg, 2011

 ISBN: 978-1-61208-292-9

Wireless Health: Making Your Devices Talk

A Review, Solution, and Outlook for Wireless Health Connectivity

Stephan Hengstler

MeshEye Consulting
Campbell, California, United States
hengstler@alumni.stanford.edu

Abstract—**With the technological revolution in digital networking and connectivity over the past two decades, the healthcare sector is at the beginning of a dramatic overhaul. These technologies have already made their way into our everyday lives and thus changing the way we do things. The healthcare industry with its resistance to change has started considering, evaluating, and embracing the way connectivity can change medical treatment and personal health. In this paper, we review the state-of-the-art in medical device connectivity with a focus on wireless solutions. Throughout the paper, the discussion separately studies the three major care delivery settings: clinical, office, and home. Based on the challenges and requirements that each of these settings present, we discuss the key aspects needed for medical device connectivity to succeed from both a technological and financial perspective. Cellular connectivity can satisfy many of these key aspects. Therefore, we have proposed and operated a testbed for cellular connectivity into Electronic Health Record (EHR) systems, which we present and report on here for the first time. The paper concludes with a longer term outlook on the adoption of digital networking and connectivity in the healthcare sector.**

Keywords-cellular; connectivity; devices; health; wireless

I. INTRODUCTION

There is much excitement in the electronic health (eHealth) and mobile health (mHealth) industry about the promise that wireless technologies can bring to healthcare. Many grassroots efforts are underway promising everything from vital sign monitoring to aging in-place. Naturally, one may ask which technologies and solutions truly create value, which will survive in the end and ultimately benefit us humans.

The business environment feels similar to the beginnings of cellular technology in the mid to late 1990s. Many companies offer complementary, overlapping, or competing product solutions for improving healthcare through the use of wireless connectivity—the same kind of wireless connectivity we already use on a daily basis in our laptops, tablets, and cell phones. Although they share the same base technology, the rules of engagement differ for the healthcare sector in many aspects from consumer markets. It is us, as the end–user, driving market success in consumer markets and hence deciding the fate of a product solution or technology. Not so in the healthcare industry. With all the parties involved in the chain of treatment, who have a stake in deciding the means of treatment, it is us, as the patient, who has the least say in the medical devices that facilitate our diagnosis and treatment.

In this paper, we will cover and discuss the deployment and usefulness of wireless connectivity technology in a variety of medical instruments. The paper starts out in Section II with a survey of existing connectivity solutions used in medical devices today. In Section III, we look at several key aspects that are necessary for a connectivity solution to succeed in the healthcare market. Section IV applies these keys to cellular connectivity exclusively and presents our technology solution for connecting medical devices equipped with cellular modems to Electronic Health Record (EHR) systems. In Section V, we discuss the direction that we see the market taking and our view of what the future holds for connectivity solutions in healthcare. Section VI concludes the paper with a summary of the insights gained and final remarks.

II. EXISTING CONNECTIVITY SOLUTIONS

The deployment of wireless technology in care delivery settings today is widespread. Many solutions already exist or are under development aiming to streamline the healthcare system [6]. But, as varied as the patient groups are, so are the treatment offerings. Today, wireless solutions in healthcare are highly fragmented with little standardization beyond the medium access layer. While this fragmentation facilitates a high degree of targeted solutions, which address specific needs, it makes it difficult for medical instrument companies to capitalize on their R&D investments. Two different ways of categorizing solutions in use today help to shed light on wireless deployment: (i) grouping by the intended healthcare setting (clinical, office, and home setting) and (ii) grouping by the target patient group (teenagers, baby boomers, and general population). Let us take a closer look at which connectivity solutions have made their way into different care delivery settings.

A. Clinical Setting

In clinical settings, i.e., clinics and hospitals, the objective of connected devices lies in preventing medical errors and reducing the cost of treatment. Connected devices

 ISBN: 978-1-61208-292-9

TABLE I. WIRED VERSUS WIRELESS CONNECTIVITY

	Advantages	Disadvantages
Wired	• Robust and reliable • Access control on premise	• Higher cost of installation • More complicated to scale
Wireless	• Easy to install and deploy • Supports device mobility	• Security more challenging • Devices need to be configured individually

facilitate this through streamlining the flow of admission, diagnostic, billing, and release information.

Clinical healthcare providers still prefer wired solutions for most of their medical instruments. Table I lists the main advantages and disadvantages of wired and wireless connectivity in medical devices. For one, wired solutions are more secure, reliable, and easier to maintain once installed and configured. Such wired instruments include for example vital sign monitors, surgical instrumentation, and hospital lab equipment. The use of mobile devices that doctors and nurses carry around is limited to smart phones, tablets, personal digital assistants, and most notably bedside monitors [14]. Both wired and wireless devices that are used in diagnosis and treatment typically integrate into the facility's Health Information System (HIS) and Laboratory Information System (LIS) through the use of instrument middleware.

With few exceptions, IEEE 802.11 Wi-Fi [27] is the preferred connectivity technology for such devices. Cellular technology [20] is only used for text message notifications to personnel involved in patient care activities. So far, wireless connections only make sense for instruments that doctors and nurses carry with them to perform routine tasks or for patient bedside monitors according to a clinical laboratorian at the Palo Alto Medical Foundation. The primary motivators for connecting medical devices into electronic medical records lie in the reduction of the overall cost structure and, in the United States, by federal mandate [25], in the reduction of the rate of readmission.

B. *Office Setting*

Doctors' offices are currently undergoing a fundamental change. The federal incentives and mandate towards the adoption and meaningful use of electronic health records [9] causes smaller doctors' offices to switch from primarily paper-based record keeping to electronic health records for their patient base. With it, the use of instrumented testing becomes also more lucrative as test results can automatically find their way into a patient's digital record. However, very few of such devices are in use today; let alone advanced devices offering cellular connectivity.

Especially for smaller practices, the main hurdle is the affordability of diagnostic test instruments and their limited insurance reimbursement. Test labs service most diagnostic testing needs arising in doctors' offices with an established cost structure for reimbursement. This flow of patient testing is more cost efficient as long as the cost of ownership of testing equipment exceeds the testing volume of a doctor's office.

The situation is very different in an adjacent point-of-care setting: minute clinics. They specialize in the rapid diagnosis and immediate treatment of only the most commonly occurring infections and diseases. Their volume of tests performed is large enough to justify the use of instrumented testing. Therefore, medical instruments have started to make their way into these point-of-care facilities. Instrument connectivity is of little value thus far unless it can relay the prescribed drug treatment through the patient's health record to the pharmacy or send reminders of dosage or refill to the patient's cell phone [21].

Figure 1. The BD Veritor™ System.

C. *Home Setting*

There is a plethora of solutions already available in the wireless health market today. The industry has come up with enticing catch phrases to market the products in this market segment: quantified self, patient-centric, personalized medicine, and aging in place. Products ranging from vital sign monitoring, such as body weight, body fat, heart rate, blood glucose, and oxygen saturation to dieting, fitness and sleep trackers are readily available. They generate massive amounts of data which, in most cases, are continuously uploaded via Bluetooth, WiFi, or USB to an associated smart phone app, which analyzes and visualizes the data. The ultimate objective has to be the improvement of individual personal health [24] through changes in behavior and lifestyle. Reduced healthcare cost for the people using these devices on a regular basis is often a desired side effect.

There are two sizeable markets in the United States for these personal health products: the teenage population and the baby boomers. The two population groups have different health challenges and hence the solutions are tailored to their needs. Baby boomers are entering the retirement age and with it come the onset of several health concerns such as congestive heart failure, hypertension, and diabetes. Hence, baby boomers spend money on solutions that enable graceful "aging in place," i.e., detect, prevent, or manage such chronic conditions in the convenience of their homes [1]. In case of the teenage population, who are sometimes referred to as "the fat kids of America," the primary health concerns are obesity, diabetes, and asthma. The objective here is not only the management of these chronic conditions under the

 ISBN: 978-1-61208-292-9

supervision of the teenager's parents, but to maintain or improve his or her overall health through creating a persistent change in behavior.

III. KEYS TO SUCCESS

After this review of medical device connectivity in the three care delivery settings, which is summarized in Table II in terms of opportunities and challenges, let us take a closer look at the keys required for a solution to succeed in each setting. The overarching key for success of any new healthcare solution is overall cost reduction in the healthcare delivery process. And that is the premise of wirelessly connected medical devices: their attraction lies in cost reduction, detection objectivity, and ease of use. While the above mentioned keys are common across all care delivery settings, each setting weighs them differently or has additional keys to success.

For illustration purposes, a good example of a medical device that exhibits detection objectivity and ease of use is the BD Veritor™ System [18], which has recently been FDA approved for the clinical as well as the point-of-care care delivery setting. It is a rapid testing platform for the detection of infectious diseases such as Influenza Type A and B and Group A Streptococcus. The BD Veritor System [2], as shown in Fig. 1, consists of the device and the consumables, that is, the mobile reader and the sample extractor and test cartridge (in the figure, the cartridge is shown inserted in the reader), respectively. The reader is however lacking the option of connectivity into HIS or LIS installations.

A. Clinical Setting

Since the hospital's clinical lab along with external central labs cover most of the testing needs arising in patient treatment, there is not a great deal of potential for adding wireless medical devices in hospital settings. The exceptions are devices that doctors and nurses use in routine patient treatment or patient bedside monitors.

There is however another emerging class of devices that can greatly benefit from wireless connectivity: devices that track the state of health of a patient after his release from the hospital. To achieve this, the patient could be given a monitoring device that facilitates home testing and wireless data upload into the hospital's HIS or LIS. One advantage is that the patient could recover in the comfort of his own home while the critical parameters of his or her state of health are still being monitored by the hospital's medical staff. The other benefit is that this would lower the readmission rate while reducing the cost of care at the same time.

The key to making this a reality is to combine a test approved for home usage with an easy-to-use device that is able to wirelessly transmit the patient's health parameters reliably and securely into the hospital's HIS or LIS.

B. Office Setting

To successfully place wireless medical devices in the point-of-care setting, minute clinics or physician offices, requires foremost that the solution makes financial sense. In this setting, a patient testing service has a fixed reimbursement amount no matter how the test is performed (visually read, instrument read, or by a central lab). Hence, doctors' offices will have a difficult time financially justifying the expense of instrumented testing if the per annum test volume for that particular test is low. In other words, wireless medical instruments can only succeed in this market if they prove to be less expensive to purchase, install, and operate than the already existing solution in place. Although the federal mandate towards the use of medical health records may aid in deploying more wirelessly connected instrument, most instruments are just too expensive to be financially viable testing solutions for most doctors' offices.

Nevertheless, rapid tests that occur frequently such as for infectious diseases (Influenza, Streptococcus, sexually transmitted diseases, etc.) may justify usage of wireless medical instruments. The keys here are that such instruments are cleared for the point-of-care setting, i.e., Clinical Laboratory Improvement Amendments (CLIA) waived, and that their cost of ownership lies roughly below $500 per year.

TABLE II. WIRELESS CONNECTIVITY IN HEALTHCARE SETTINGS

Care Setting	Opportunities	Challenges
Clinical	• Bedside monitoring during routine patient visits • Patient self-monitoring after hospital discharge	• Clinics are slow in adopting new technologies • Reduction in overall cost of care not yet proven
Office	• Facilitate adoption of electronic health records • Seamlessly relay treatment to pharmacy or insurance	• Insurance reimbursement limits return on investment • Smaller offices not setup for wireless connectivity
Home	• Detect, prevent, and manage chronic conditions • Self-tracking to create persistent lifestyle changes	• Monitoring products lack standard and aggregation • Gap between tracking and persistent behavior change

C. Home Setting

While each of the solutions offered for home deployment may address a particular health issue quite adequately, there are many challenges facing the wireless health home market today. For one, there is little to no standardization. Each solution works on its own independent of other health products in use. Each solution also requires frequent interaction and manual data entry by its user—something a society governed by convenience strongly shuns. For this reason, the average duration of regular usage does not exceed 30 days for the majority of these health improvement apps: just 5% of all apps (including health apps) are still in use 30 days after download [8]. In short, they are too intrusive to many people's already hectic and packed life. Decentralized storage of data collected through different personal health solutions creates another significant challenge. How is one to get a comprehensive picture of one's health if the data resides in several different, unique applications? There are of course a few solutions like Google Health (discontinued as of January 2013) and Microsoft HealthVault [17] attempting to address the need of centralized data storage. But, most personal health products do not interface with them and

 ISBN: 978-1-61208-292-9

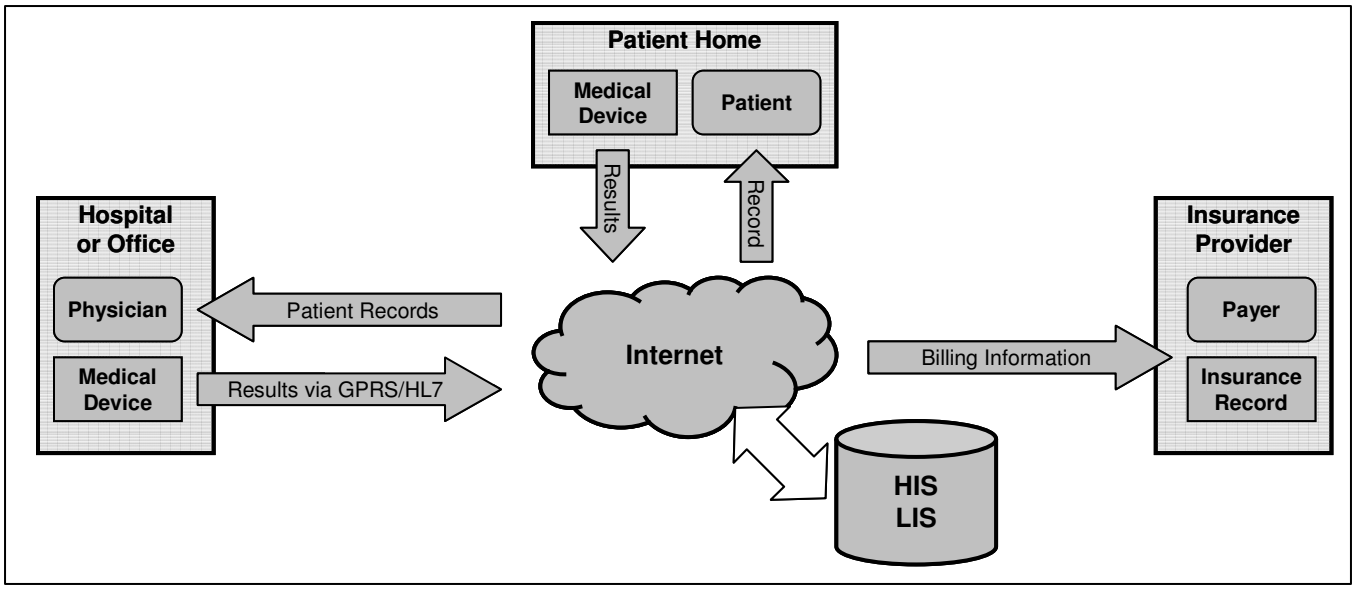


Figure 2. Healthcare information flow with cellular connectivity of medical devices.

hence data would have to be manually entered. Therefore, a major key to succeed in this market is easy and seamless integration of the medical sensing devices, that is, the ones that provide personal health metrics, into personal health record systems. This can only be achieved effectively through standardization of the health data interfaces. The Continua Health Alliance [5] and the Institute of Electrical and Electronics Engineers [11] for instance are actively pushing this standardization and have been issuing design guidelines and standards for interoperability in personal healthcare [3].

Another fundamental issue of personal health tracking is that it is not sufficient to create persistent and lasting lifestyle changes. In fact, Joseph Kvedar [25] has found "that only a small portion of the population, around 10 percent, will change their behavior based on tracker information alone." Knowing the right thing and doing the right thing are worlds apart. Even if personal health trackers provide us with vital information of what foods to avoid for example, we are still subjected to the marketing exposure of unhealthy eating habits. In the United States, good examples are the Carl's Jr. TV commercials for its selection of big and juicy burgers [4]. How can one not watch one of these commercials without leaving with the thought that relishing one of these irresistibly delicious burgers results in tremendous pleasure? Knowing that they are an unhealthy diet will likely not kill that thought! It is like running a marathon with a rock tied to one ankle. In essence, our lifestyle choices are not only impacted by reading our personal health statistics, but also by what we exposure ourselves to in the form of billboards, commercials, and magazines. And to extract oneself from this omnipresent exposure in the United States is a deliberate effort that has to be made daily. To assist us in this effort, our personal health systems would also have to tie into our flat panel TVs and block out commercials that are inappropriate for our current health condition.

IV. THE CASE FOR CELLULAR

At this point, it should have become clear that there is no one size fits all solution. The three care delivery settings considered have overlapping but also diverging requirements, which cannot be met by one solution all at once. Therefore, there are many product offerings from small to large companies, which focus on one or a few aspects in the healthcare delivery process. In short, the market is highly fragmented and proprietary solutions are prevalent.

But for solutions to be cost effective and scalable demands standardization and interoperability that in turn can proliferate integrated solutions [10]. Therefore, in the near-term, healthcare solutions will have to target seamless integration into the flow of care from patient over provider to payer [1]. Clearly, this is a good idea in theory but not enough to succeed in the healthcare market. The present reality is that the adoption of mHealth connectivity standards has been inconsistent [19].

We strongly believe that the adoption of cellular connectivity in medical devices is the starting point to enabling higher levels of standardization and interoperability—at least at the front-end, where patient health data needs to make it into the digital medical record. It is crucial for subsequent treatment to consistently store this data digitally in a secure and reliable manner. But, if the interface method is lacking any of these attributes, the patient data will not be stored consistently leading to patchy health records. While there are several connection technologies and dataflow models conceivable, cellular technology is already dominating the personal consumer space and, as a result, has been widely adopted, is standardized, and continuously increases in data throughput and geographical coverage. Moreover, cellular hardware cost is held down by the large scale consumer market and service providers continue driving down data transmission costs. Therefore, medical

 ISBN: 978-1-61208-292-9

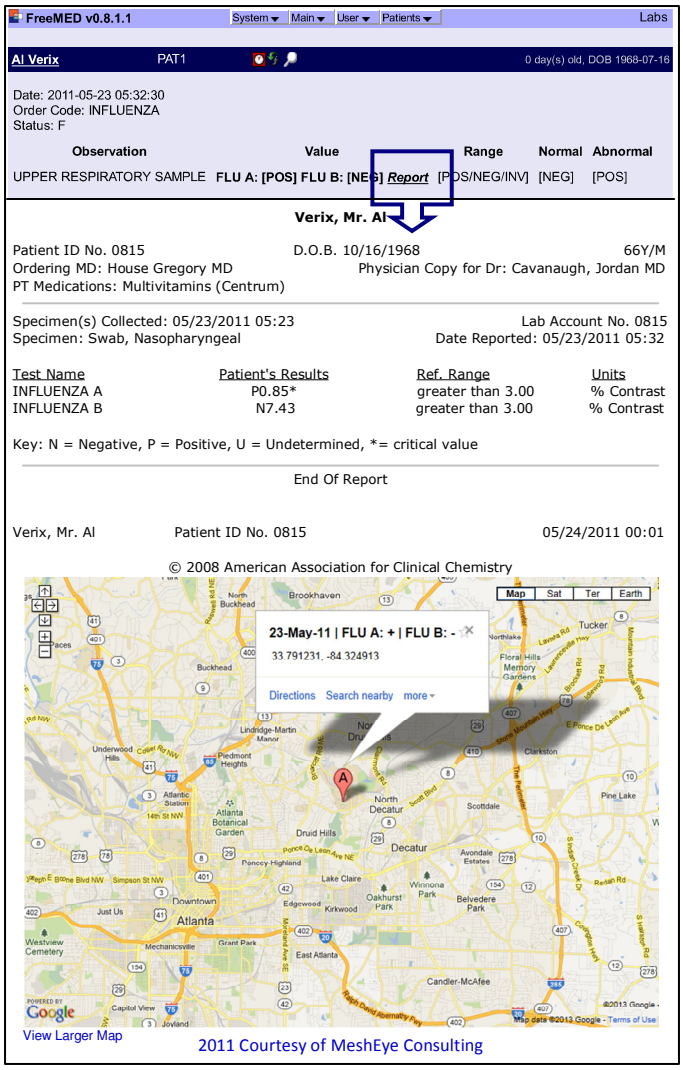


Figure 3. Patient test record (top) and instrument test report (bottom) of the MeshEye EMR Connectivity Testbed.

devices equipped with cellular modems can meet several of the keys for success discussed in Section III.

Let us discuss this cellular connectivity solution in more detail. Fig. 2 illustrates the flow of healthcare information when medical devices are equipped with a cellular GSM modem. This enables them to directly communicate with the HIS/LIS, or, more generally, the EHR system, through a General Packet Radio Service (GPRS) Internet connection. Test results can then readily be uploaded into the patient health record via the HL7 protocol [11]. Note that this direct connection eliminates the need for and expense of middleware software, a "middle man", which only reformats the device's proprietary data output to the standardized EHR data format. Once the patient results have been uploaded to the EHR, which can either occur from a hospital, physician office, or the patient's home, other need-to-know parties can readily access or be notified of the results. Such parties are the primary care physician, the insurance payer, as well as the patient itself.

To explore and validate the feasibility of this cellular connectivity solution, MeshEye Consulting has been operating an Electronic Medical Record (EMR) connectivity testbed with an HL7 portal for test record upload since November 2010. The testbed deploys the open-source EMR software FreeMED [6] in lieu of the HIS/LIS software. The FreeMED installation has been modified to accept test records from medical devices in the form of HL7 requests encapsulated in XML-RPC requests. A medical device prototype equipped with a cellular GSM modem was designed to upload its test records to this EMR system via GPRS. The testbed proved that this approach is feasible and easy to implement.

To notify the physician of completed tests, the EMR connectivity testbed has been configured to send out text messages with the test results. The end-to-end delay commonly encountered is in the order of 10 to 20 seconds. Considering that rapid diagnostic tests typically take at least 10 minutes to complete, such quality of service (QoS) would be acceptable. But cellular network carriers do not make any guarantees of end-to-end delay for text messaging, and hence it is only a solution good enough for demonstration purposes but not for professional deployment. Moreover, text messaging does not lend itself to encryption, which brings us to another area of frequent concern: compliance with the Health Insurance Portability and Accountability Act (HIPAA).

HIPAA compliance requires the implementation of reasonable safeguards for the protection of patient-identifiable information. Although the EMR connectivity testbed does not transmit any information that would allow identification of a patient by name, only an assigned patient identifier, it makes sense to encrypt the entire payload. This usually diffuses any concerns around patient privacy but adds the burden of encryption key management.

The EMR connectivity testbed was demonstrated to several hospitals in California as well as to the Centers for Disease Control and Prevention (CDC) in Atlanta, GA, in May 2011. Fig. 3 shows the patient test record and instrument test report that the testbed generated during the demonstration. The top of the figure shows the view of the patient's test result entry while the bottom of the figure shows the automatically generated instrument test report. The report contains all the fields expected of a lab test report. In addition, it maps the rough location of the testing site, which is available from the cellular network registration. Most importantly, the test result upload completes in real-time, i.e., it usually takes less than a minute. This solution would allow the CDC to publish their "Influenza Surveillance Report" in real-time rather than with data lagging by two weeks. Especially CDC's recently launched influenza app [20] could benefit greatly from real-time reporting of infectious disease testing.

V. LONGER TERM OUTLOOK

There is no doubt that interoperability through standardization will continue to increase in healthcare solutions. From a technology perspective, that is what is required to make any medical device talk to any EHR system

 ISBN: 978-1-61208-292-9

[14]. It also makes sense from a business perspective since interoperability is an essential component for a scalable connected health market [19]. In short, interoperability through standardization will likely pave the way for widespread use of connected medical devices.

But, knowing the right thing does not necessarily translate into doing the right thing. In fact, the healthcare industry is known for its resistance to change and slow rate of technology adoption. For instance, Thompson states that "I feel frustrated that physicians don't quite seem to be practicing in the 2012 world of technology I see on the exhibit floor [at the annual AACC Clinical Lab Expo 2012]" [16]. Healthcare investor G. Kurtzman puts it this way [13]: "Unless there is a "pull" from customers, patients, providers, or payers, an entrepreneur in healthcare IT won't be able to capitalize on just a good idea." Along these lines, the two parties that still need to more convincingly drive the idea of connected health are the payers and the regulators.

The regulatory agencies' mandate includes issuing regulations for marketability of medical devices and enforcing them in the marketplace. There still remains a lot of uncertainty concerning the regulation of mobile health applications and related connected health devices. Therefore, the regulatory agencies have to clarify the approval process of these emerging technologies. The next step is to speed up their approval process. This will also make their pursuit more attractive to the investment community.

The healthcare payers, that is, the insurance providers, have to be persuaded that connected healthcare solutions not only make sense but also reduce the overall cost of treatment. This is especially important in the United States, which has the highest cost structure in healthcare. It will require several more case studies and clinical trials to make a convincing case for the overall reduction in healthcare cost. Such studies and trials are however intricate and costly since the entire chain of healthcare services involved in patient treatment has to be accounted for.

Finally, a strong push for wireless connectivity in healthcare is coming from several players at the bottom of the food chain of healthcare reimbursement: medical device manufacturers and cellular network providers. Device manufacturers have an increasing interest in equipping their products with connectivity. This would provide them with easier access to test results, which may allow them to move up in the food chain. Network providers see the opportunity in high-volume data contracts in machine-to-machine (M2M) communication, which is viewed as their next big market after the cell phone market has started to level off.

With respect to cellular connectivity in medical devices, the outlook is the same as for connectivity in general. Nevertheless, it has to bear the additional burden of subscription fees paid to cellular network service providers. But, there is hope in sight [23]: "[…] The number of devices with integrated cellular connectivity increased from 0.73 million in 2011 to about 1.03 million in 2012, and is projected to grow at a CAGR rate of 46.3 percent to 7.1 million in 2017." And by the laws of supply and demand, increased deployment will result in lower cost of cellular connectivity in medical devices. Most likely countries other than the United States will lead the way—countries, in which cellular subscription fees adapt more rapidly to market supply and demand, as is the case in most countries across Europe and Asia.

VI. Conclusion and Future Work

We reviewed the current state of connectivity technology for medical devices in the healthcare sector giving special attention to wireless connectivity. The review highlighted the diversity and fragmentation of existing solutions to address the demands in the clinical, office, and home care setting. Therefore, the one key aspect to increase adoption of connected medical devices is interoperability through standardization. Cellular connectivity can enable standardized, seamless, and ubiquitous integration of medical devices into EHR systems. For this reason, we proposed and presented a cellular connectivity testbed that confirms and demonstrates the validity of this approach. Our connectivity testbed indicates that medical devices can be seamlessly integrated into the flow of patient treatment across all three care settings. However, it remains to be seen whether wireless connectivity can actually lead to an overall reduction in the cost of care and change towards healthy lifestyle choices. Moreover, regulators and payers still have a long way to go before wireless connectivity becomes the norm in everyday patient diagnosis and treatment.

Acknowledgment

The author gratefully acknowledges the discussions, inspiration, and involvement of his colleagues at Alverix Inc. in San Jose, CA, and the Becton, Dickinson and Company (BD) Diagnostics Group located in Baltimore, MD, and San Diego, CA.

References

[1] L. C. Baker, S. J. Johnson, D. Macaulay, and H. Birnbaum (2011), "Integrated Telehealth and Care Management Program for Medicare Beneficiaries with Chronic Disease Linked to Savings," Health Affairs, vol. 30, no. 9, Sept. 2011, pp. 1689–1697.

[2] BD Veritor System, Product Website, [retrieved: September, 2013] Available: http://www.bd.com/ds/veritorsystem/

[3] D. Bowman, "Continua Health Alliance Releases 2011 Design Guidelines," FierceHealthIT, iss. 9, Sept. 2011, pp. 1–2.

[4] Carl Karcher Enterprises, Inc., Company Website, [retrieved: September, 2013] Available: http://www.carlsjr.com

[5] Continua Health Alliance, Organization Website, [retrieved: September, 2013] Available: http://www.continuaalliance.org

[6] "mHealth in an mWorld: How mobile technology is transforming health care," Deloitte Center for Health Solutions, Deloitte, 2012, pp. 1–21.

[7] FreeMED Electronic Medical Record Software, Product Website, [retrieved: September, 2013] Available: http://freemedsoftware.org

[8] R. Gary, "Why 95% of Mobile Apps are Abandoned—and Tips to Keep Your Apps from Becoming Part of that Statistic," Nuance Communications Inc., iss. 20, Nov. 2011, pp. 1–2.

 ISBN: 978-1-61208-292-9

[9] Government Health IT, Policymaking, Regulation, & Strategy: Meaningful Use, [retrieved: September, 2013] Available: http://www.healthit.gov/policy-researchers-implementers/meaningful-use

[10] J. Hatcliff et al., "Rationale and Architecture Principles for Medical Application Platforms," Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems (ICCPS '12), Apr. 2012, pp. 3–12.

[11] Health Level Seven International, Introduction to HL7 Standards, [retrieved: September, 2013] Available: http://www.hl7.org/implement/standards/

[12] IEEE Standards Association, IEEE Standard 11073-10103-2012 – Health informatics—Point-of-care medical device communication, [retrieved: September, 2013] Available: http://standards.ieee.org/findstds/standard/11073-10103-2012.html

[13] G. Kurtzman, GUEST POST: The question every healthcare IT startup must answer, [retrieved: September, 2013] Available: http://venturebeat.com/2012/08/25/healthcare-it-startup-tips/

[14] P. B. Luppa, C. Müller, A. Schlichtiger, and H. Schlebusch (2011), "Point-of-care testing (POCT): Current techniques and future perspectives," TrAC Trends in Analytical Chemistry, vol. 30, no. 6, Jun. 2011, pp. 887–898.

[15] B. Malone, "The Cutting Edge of Lab Connectivity: Will New Standard Deliver Plug-and-Play Solutions?" Clinical Laboratory News, vol. 38, no. 9, Sept. 2012, pp. 1–5.

[16] B. Malone, "Spotlight on Point-of-Care Testing: Innovation, Expansion Evident at AACC Clinical Lab Expo in Los Angeles," Clinical Laboratory News, vol. 38, no. 10, Oct. 2012, pp. 1–8.

[17] Microsoft HealthVault, Product Website, [retrieved: September, 2013] Available: https://www.healthvault.com

[18] A. Paxton, "Rx for optimizing rapid flu test performance," CAP Today, vol. 27, no. 1, Jan. 2013, pp. 1–5.

[19] "Interoperability: An essential component for scalable mHealth," mHealthInsights, PwC, Mar. 2013, pp. 1–3.

[20] S. Saw, T. P. Loh, S. B. L. Ang, J. W. L. Yip, and S. K. Sethi (2011), "Meeting Regulatory Requirements by the Use of Cell Phone Text Message Notification With Autoescalation and Loop Closure for Reporting of Critical Laboratory Results," American Journal of Clinical Pathology, vol. 136, no. 1, Jul. 2011, pp. 30–34.

[21] I. Sachpazidis, S. Fragou, G. Sakas, "Medication adherence system using SMS technology," Proc. Intelligent Sensors, Sensor Networks and Information Processing Conference (ISSNIP 2004), IEEE Press, Dec. 2004, pp. 571–575.

[22] G. Slabodkin, "CDC's influenza app should be more reliable," Editor's Corner in FierceMobile Healthcare, iss. 15, Jan. 2013, pp. 1–2.

[23] G. Slabodkin, "Research predicts strong growth of patient home monitoring systems by 2017," FierceMobile Healthcare, iss. 18, Jan. 2013, pp. 1–2.

[24] P. Sonnier, POLL RESULTS: What is the single greatest health benefit afforded by Digital Health solutions? [retrieved: September, 2013] Available: http://popperandco.com/2012/07/

[25] United States Department of Labor, Affordable Care Act, [retrieved: September, 2013] Available: http://www.dol.gov/ebsa/healthreform/

[26] E. Waltz, "How I Quantified Myself: Can self-measurement gadgets help us live healthier and better lives?," IEEE Spectrum Magazine, vol. 49, no. 9, Sept. 2012, pp. 43–47.

[27] Wi-Fi® in Healthcare: Security Solutions for Hospital Wi-Fi Networks", White Paper, Wi-Fi Alliance, Feb. 2012, pp. 1–11.

 ISBN: 978-1-61208-292-9

Mobile Device Biometric Touch Gesture Information Used to Give User Identity Evidence

Thomas Ruebsamen, Julia Bayer, Christoph Reich
Cloud Research Lab
Furtwangen University of Applied Science
Furtwangen, Germany
{Thomas.Ruebsamen, Julia.Bayer, Christoph.Reich}@hs-furtwangen.de

***Abstract*—Mobile devices, such as smart phones and tablets, are as popular as never before. Even corporations encourage their employees to use company services such as email and document management services on these kinds of devices. However, the security of mobile devices, especially when used in a professional environment, is still lacking behind compared to company controlled infrastructures. In our previous work, we described a novel system for securing mobile devices while leveraging the potential of seemingly unlimited resources provided by cloud computing. In this work, we extend this idea and focus on user identification using touch gesture analysis as part of the MoSeC architecture. We show that, using artificial neural networks, the analysis of user's touch behavior while using a mobile device can support authentication processes. This technology will also enable the collection of information for tracing legitimate as well as malicious access attempts and we will show how our proposed system may provide digital evidence.**

Keywords*—*Cloud Computing, Digital Forensics, Evidence, Mobile Security, Authentication

I. INTRODUCTION

In our increasingly networked world, IT security plays a more and more important role, especially in enterprise environments, where sensitive business information is stored and processed. Also, the widespread use of mobile devices such as smart phones and tablets in a professional environment is no longer limited to management staff. These devices, when used for work, are usually integrated into the enterprise's IT infrastructure and contain possibly sensitive information. However, these devices are not always under direct control by the enterprise. For example, employees are often encouraged to use their devices at home, which essentially means the risk of loss or theft is significantly higher, because of the uncontrolled environment. The user identification verification and assurance is of importance for enterprises providing their employees access to sensitive data. To support building a chain of evidence or chain of custody additional information about the user's identity is helpful.

Attacks on mobile devices can be classified into two groups: the ones where an attacker is in possession of the device and where attacks are carried out remotely. This paper deals exclusively with the former scenario, where the attacker has gained possession of the device. In such cases, additional access protection mechanisms are of utmost importance to prevent an attacker from accessing data stored on the device as well as enterprise services, which grant mobile devices access to the corporate network.

The most common protection for mobile devices against unauthorized access is locking it down using an additional password or personal identification number (PIN). This mechanism is easy to implement. However, to provide a reasonable addition to device security, the password must be complex enough. Secure complex passwords usually are hardly memorable. Additionally, to lock down the device, the user is usually required to enter the password on every device wake-up or screen activation and after a defined period of time. This is not a user-friendly solution.

In case of a breach of security caused by a mobile device, it is usually most important to gather as much information about the attack as possible. Therefore, evidence gathering systems, which monitor certain system and network related security parameters like unauthorized device accesses or even authorized device accesses, might prove useful for tracing and analyzing.

The remainder of this paper is structured as follows: After this section, we describe related work done in the field of advanced user authentication on mobile devices and continuous authentication. The integration of the gesture identification in the overall framework to give identity evidence can be found in Section III. In Section IV, we give an overview about touch gesture recording and analysis of touch attributes. In the following Section V, we describe our approach to using artificial neural networks (ANN) to analyze collected information in the cloud. In Section VI, we present our evaluation results, followed by a conclusion and the description of possible future research directions in Section VII.

II. RELATED WORK

Wong et al. [1] focus in their work on keystroke analysis for user authentication by analyzing users typing their passwords. The analysis process is carried out using artificial neural networks and the k-nearest algorithm. However, their conclusion is that keystroke analysis is too reliant on the physical condition of the user. In contrast to this work, their approach relies on keyboards being used, whereas our approach focuses on the increasingly popular current smart phone generations, where there usually is only a soft-keyboard, which is used rather sparsely in favor of touch gesture control.

Pannell et al. [2] follow a more comprehensive approach. Besides using keystroke analysis, they include other attributes like running applications and a classification of users into ones with basic computer knowledge or profound knowledge. With this information they build user models. In their system, intruders do not fit those user models and can therefore be detected. By including multiple attributes, the detection rate

 ISBN: 978-1-61208-292-9

can be increased significantly. However, data recording and analysis is performed locally, whereas, in our work, a remote proxy instance is used.

A similar approach is followed by Anand et al. [3], where they try to identify users by using data collected on mobile devices. This data includes the call history and typing patterns. Their main conclusion is that a balance has to be found between the Masquerade Detection Rate, the relation between detected attacks and all attacks, and the time to detect an attack. To accomplish this, some parameters need to be adjusted (e.g., the time frame for data collection).

Imsand et al. [4] try to identify users by analyzing how they are using graphical user interfaces. A simple example is how a user copies text to the clipboard, either by using primarily keyboard shortcuts or context menus. Similar to Pannell's approach, this information is then stored in user profiles, which are compared to the current user's behavior. However, their evaluation didn't seem to be very successful. One reason, which the authors are giving is the small amount of test data sets and the overfitting of their neural network.

Another gesture-based approach for user identification is followed by Guse et al. [5]. It is based on capturing motions of users with 3D acceleration sensors and gyroscopes. However, they acknowledge several problems with this approach. It is difficult to consistently perform the same gestures for identification and those gestures have to be performed in secure locations, because it might be very easy to imitate them. Nevertheless, Guse et al. come to the conclusion that gesture based identification could be a viable alternative to PINs and are significantly less cumbersome than entering PINs. The main difference to our approach is, that we are focusing on smart phone touch gestures without any additional hardware.

SenGuard [6] is a system, which leverages virtualization techniques on mobile devices. It collects information about the voice of the user, GPS location, multi touch gestures and the user's movement. If SenGuard detects possibly non-authorized usage of the device, traditional authentication mechanisms (e.g., PINs) are cut in. SenGuard runs on the device and compared to our approach does not use any external resources. However, the authors recognized power consumption of their system as one of the major issues and try to solve this, by selectively removing data collection sensors the lower the state of charge gets. SenGuard reaches very good user authentication results by combining all of the collected attributes. However, touch gestures on their own are regarded as not sufficient for reliable user authentication by Shi et al. In our approach, touch gestures are used in conjunction with additional continuous authentication mechanisms. As part of the decision making system, touch gestures may very well add to device security.

Schneier et al. [7] describe an approach to logging information while protecting against malicious manipulation to those logs. Several other papers work on similar systems and extend the idea of collecting logging information in a tamper-evident way for making such logs available as evidence. Most of these approaches build on the idea of hash chaining.

III. User Identification Evidence Architecture

In a previous project called Mobile Security by Cloud Computing (MoSeC) [8] at the HFU Cloud Research Lab [9], we addressed these problems by designing a scalable cloud architecture for enhancing mobile device security. Every mobile device is assigned to a proxy instance inside the cloud. The proxy is used to offload performance-intensive tasks to the cloud, where computing resources are seemingly unlimited or at least can be easily scaled out. The mobile device uses a lightweight software agent to communicate with its cloud proxy via a virtual private network (VPN). Besides other information, the agent transmits recorded and aggregated touch gesture profiles of the current user to the cloud, where sophisticated analysis methods are used to detect suspicious activity.

The primary goal of this MoSeC module is providing information for the decision making process for whether a user of a mobile device is authentic or not. In a broader sense, this also means a theft and loss detection for mobiles devices. Additionally, this module provides information for assigning a device to an adequate security level. In MoSeC, security levels are used to control which corporate services and data are accessible by mobile devices. The security level is computed using different information sources like device management, intrusion detection, malware detection, traffic analysis and the gesture analysis depicted in this paper. Depending on the security scores collected in each of these modules devices and their users are classified ranging from *critical* to *highly secure*, resulting in the previously mentioned access control decisions. This effectively leads to a more secure integration of mobile devices (also private devices as in bring-your-own-device) in enterprise environments while protecting sensitive corporate information.

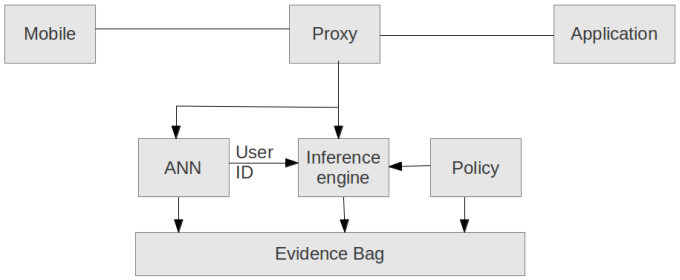


Fig. 1. Architecture Overview

Figure 1 depicts an architectural overview of the continuous authentication process in MoSeC. The Proxy takes control of communication of mobile devices with enterprise applications and services. It also provides the runtime environment for the Inference engine, which uses an ANN specifically trained to detect gestures not performed by the device owner. ANNs were chosen based on their ability to provide a reasonably accurate input about user authenticity to the authentication process. Additionally, company policies are considered by the inference engine (e.g., assigning an appropriate security level depending on the policy, and the analysis results). For further company-wide evidence collection, an evidence bag [10] is provided, which allows retrospective analysis of the collected data (e.g., tracing authorized as well as suspicious accesses for forensics in case of an intrusion). The evidence bag may be used internally, but may also prove useful during the prosecution of security breaches. One key feature of the digital evidence

 ISBN: 978-1-61208-292-9

bag is storing information in a tamper-proof or at least tamper-evident way.

IV. Collecting Input Data on Android

To demonstrate the recording of touch gesture information and the evaluation using an artificial neural network, an Android application has been developed. In this section, we will describe how touch gestures are recorded in our prototype application. Furthermore, a list of different touch attributes are presented and discussed according to their suitability for identifying users of mobile devices.

A. Data Collection

Touch gestures are characterized by the movement of one or more fingers (multi-touch) on a touch-sensitive display and result in actions performed by the device. The Android SDK provides developers with the ability to capture information about touch gestures using the *MotionEvent* class. The most important gestures are scrolling (usually performed by swiping horizontally or vertically over the touchscreen, this is also called flicking), zooming-in (the movement of two fingers away from each other) and zooming-out (the movement of two fingers towards each other). Figure 2 illustrates these basic touch gestures. Starting with scrolling on the left, followed by zooming-in and zooming-out.

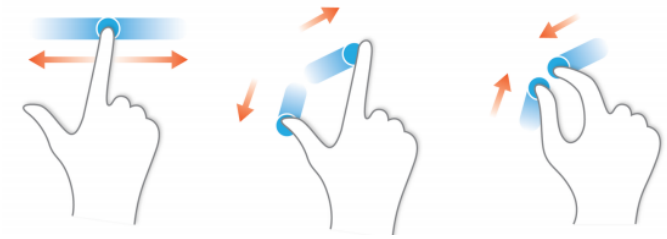


Fig. 2. Multi Touch Gestures [11]

To identify users according to their different touch gesture behavior, a profile of the user has to be created first. In our case, this means that an ANN has to be trained for every user. For this purpose, an Android App has been developed, which records the touch characteristics of users. For gestures like scrolling and zooming, parameters like x/y-coordinates, pressure applied by the finger on the screen, and the length of the gesture are recorded. To get a precise profile of the users touch gestures, this gesture collection course has to be completed multiple times.

B. Touch Attributes

Touch gestures have multiple attributes, which characterize different users. The course App records a total of 87 attributes (e.g. position, no. of fingers, pressure, speed, etc.). Depending on the performed touch gesture, a subset of these attributes is included. For the simple scrolling gesture 23 of the total 87 attributes are used. Zooming-in uses 32 and zooming-out an additional 32. The most significant difference between normal touch gestures like scrolling and multi-touch gestures like zooming is the amount of different attributes, which can be identified. This is reasonable, because normal touch gestures only use one finger and therefore inherently have less attributes which need to be considered.

Additionally, some of the attributes are more significant than others. For example, the overall duration, distance, average pressure applied by the fingers and distance between the fingers during gestures have been identified as very significant and at least in combination possibly unique to a user.

V. Analyzing Touch Gestures Using Neuronal Networks

For making the decision whether or not the current user of a mobile device is the actual owner of the device, an interconnected feed forward neural network is used. In this section we describe the structure, training (supervised) and validation process.

A. Structure of the Neural Network

The neural network consists of three layers (input, hidden and output). The input layer consists of 87 input neurons, each of them representing one of the touch gesture attributes (see Sec. IV). The activation function for the input neurons is the identical function. Additionally, there are three hidden layers with each of them having 60 hidden neurons. The hidden neurons use the logistic function:

$$f(x) = \frac{1}{1 + e^{-3*x}}$$

The output layer consists of two neurons. The value “one” signals that the neural network suspects that the user is authentic, the other neuron signals the opposite case. The number of input and output neurons have been decided according to the input attributes and the two possible results. The amount of hidden layers and number of neurons contained within them have been chosen carefully during the design process of the neural network. The resulting network is rather huge, but the size is justified by the promising results.

B. Training the Neural Network

Artificial neural networks in the MoSeC architecture operate according to a specific life cycle depicted in Figure 3.

In the **Data Collection Phase (DCP)** (1) touch gesture data generated by the user is recorded. Subsequently, the ANN is trained using this data. One essential requirement in this phase is that the device is used exclusively by the legitimate owner. Otherwise, the training data gets tainted, which may lead to the ANN not being able to detect gesture patterns and to a significantly higher rate of false positives.

After the DCP, follows the **Kickoff Learning Phase (KLP)** (2), during which the ANN is trained the first time using the previously collected data. The target network error and desired count of learning iterations is determined empirically. This process is described in Section VI.

After the ANN has been trained, the **Monitoring Phase (MP)** (3) is started. This phase constitutes the main operational phase, where the ANN is actually used to identify unauthorized device access. Touch gesture data, which is collected during the normal usage of the device, is validated against the previously trained ANN during this phase. If irregularities

 ISBN: 978-1-61208-292-9

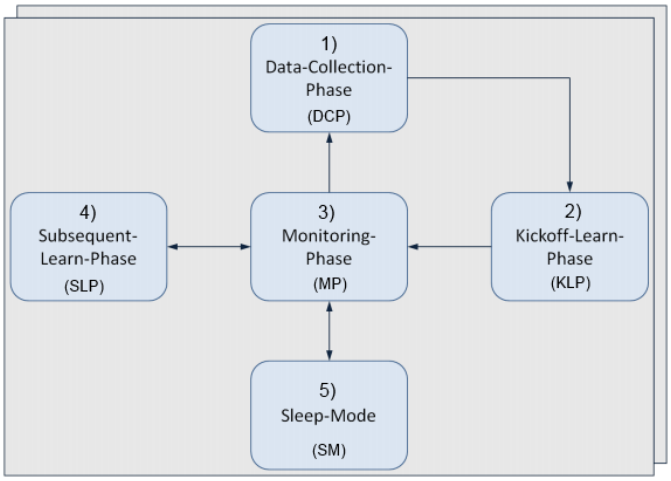


Fig. 3. ANN Lifecycle

are detected, strong authentication mechanisms (such as PIN request, biometric authentication etc.) are triggered. To adapt the ANN to possible changes in behavior of the user, new learning data is collected during the Monitoring Phase.

This new learned data is used to further train the ANN in the **Subsequent Learn Phase (SLP)** (4). To trigger the SLP, different approaches are possible:

- After the user has been authenticated using strong authentication mechanisms (e.g., PINs), the SLP is triggered. This can be done after each or n-th authentication in a given duration.
- Regardless of the authentication state of the user, the SLP is triggered in set intervals.
- The SLP is triggered manually by an administrator either to reset the state of the ANN.

Selecting data, which is being used during the SLP, can be selected using different strategies:

- Learning all previously recorded data including the data collected during the KLP may prove problematic, because more recent changes in behavior are not weighed strong enough (overfitting of old data).
- Only recently recorded data is used to generate training lessons for the ANN. This approach reacts to behavior changes in a very agile way, but may "forget" old behavior too soon.
- The middle-ground between the previous two approaches is using newly acquired data as well as old data collected over a given duration, merged into a lesson for the ANN.

After the SLP is complete, the operation mode is switched back to the MP. To address the problem of a user changing in behavior over time, a backup AAN can be trained in parallel. When needed, the running ANN is replaced by the backup ANN. Another approach would be to introduce a forgetting-factor. However, in our work we focused on the first approach.

The last operation mode is **Sleep Mode (SM)** (5). This deactivates the gesture authentication process temporarily. This mode is supposed to be used by an administrator or by the user after he has been authenticated using a strong mechanism. But, after switching to this mode, the security level of the mobile device is reduced significantly, which results in blocked access to corporate services and information.

VI. Evaluation

As previously mentioned, an application which records information about touch gestures has been developed to show whether or not using artificial neural networks on the cloud for identifying mobile device users is a feasible approach. In this section we will describe our evaluation methodology and results.

The pattern recognition for the detection of unauthorized users is done using neural networks. During the implementation process "Membrain" [12], a neural network editor and simulator which also provides JAVA bindings, has been used for editing and simulating neural networks. The Samsung Nexus S served as a development platform.

A. Results

To test the effectiveness of our approach, 6 persons were selected for testing the application. The number of people has been chosen arbitrarily. Table I shows how often each test person completed the course for recording touch profile information sorted by whether the data is collected for network training or actual testing.

TABLE I
Number of Course Passed by Test Person

	Courses Passed (learning)	Courses Passed (checking)
Person 1	15	15
Person 2	15	15
Person 3	22	15
Person 4	76	15
Person 5	20	20
Person 6	50	15

An example for how data sets for the training phase of the neural network look like is shown in Table II. The attribute columns contain the normalized values of the attributes extracted from the touch gesture (e.g., coordinates, length, applied pressure etc.). The learning behavior of the network is heavily dependent on the amount and quality of learning data as well as the ratio between positive and negative learning data and the network error. Because our approach to training the network involves observed learning, a learning data set also contains the values of the output neurons. Positive learning data sets have the value "1" for the "yes" output neuron and negative ones vice versa. It is obviously very important to find the right ratio between positive and negative patterns to get the best results. To get negative patterns for each person, patterns from the other test persons were included.

To find a suitable ratio between the amount of positive and negative patterns, 4 training passes have been carried out. The amount of positive learning patterns remains constant for each

 ISBN: 978-1-61208-292-9

TABLE II
EXEMPLARY LESSON STRUCTURE

Attribute 1	Attribute 2	Attribute 3	...	Output YES	Output NO
0.4979	0.7892	0.1983	...	1	0
0.5043	0.7721	0.2112	...	1	0
0.3094	0.9798	0.6983	...	0	1
0.3176	0.9943	0.7002	...	0	1

TABLE III
POSITIVE AND NEGATIVE LEARNING PATTERNS COUNT BY PASS

	Positive Pattern Count	Negative Pattern Count			
		Pass 1	Pass 2	Pass 3	Pass4
Person 1	15	10	10	15	20
Person 2	15	10	10	15	20
Person 3	22	10	15	20	25
Person 4	76	55	60	65	70
Person 5	20	10	15	20	25
Person 6	50	35	40	45	50

pass, while the amount of negative patterns has been varied arbitrarily. Table III depicts the evaluated ratios.

Another parameter, which had to be evaluated is the desired network error. The lower the network error, the longer it takes to train the ANN. Therefore, several different values (3%, 6%, 9%, 12% and 15%) have been evaluated using different ratios of learning patterns. In our experiments we came to the conclusion that a ratio of 1:1 regarding positive and negative learning data results in a minimal occurrence of false positives and false negatives during the MP. Figure 4 shows the trend for the ratios described in Table III. Figure 4 also depicts the summed up values (and therefore seems unusually high) for false-positives and shows how results change depending on different combinations of positive-negative learning patterns. Therefore we restricted our further evaluation to the use of the 1:1 ratio for positive and negative learning patterns. Based on this information, Table IV shows a detailed evaluation of the detection rate for unauthorized users. It shows for each user and lesson the output values of the neurons: The higher value wins. For example, for person 1 and the learning data of person 1 (first row, column) the YES-neuron fires 70 times whereas the NO-neuron fires 30 times. Therefore, the user is successfully authenticated. However, we also detected some false positives. For instance, person 2 is the authorized user and checking patterns of person 5 fed to the neural network results in a false positive. The same applies to person 5.

TABLE IV
RESULTS OF EVALUATION WITH NETWORK ERROR 0.12

	P1	P2	P3	P4	P5	P6
P1(learn)	72/30	7/95	32/41	12/85	19/75	27/93
P1(verify)	64/39	28/38	24/60	10/89	31/71	31/86
P2(learn)	18/90	85/4	35/66	9/78	16/84	1/96
P2(verify)	15/85	44/12	39/67	1/80	16/86	52/67
P3(learn)	28/78	18/93	74/21	61/73	10/80	42/73
P3(verify)	26/86	26/60	69/19	5/75	13/69	33/70
P4(learn)	16/87	3/99	22/77	71/45	18/67	19/75
P4(verify)	14/86	18/56	19/88	92/24	18/79	36/61
P5(learn)	21/91	26/88	7/88	34/78	88/20	9/92
P5(verify)	23/88	58/21	14/93	32/89	83/63	6/89
P6(learn)	20/81	16/95	47/79	4/79	18/66	75/20
P6(verify)	10/87	23/79	32/98	1/61	87/22	75/27

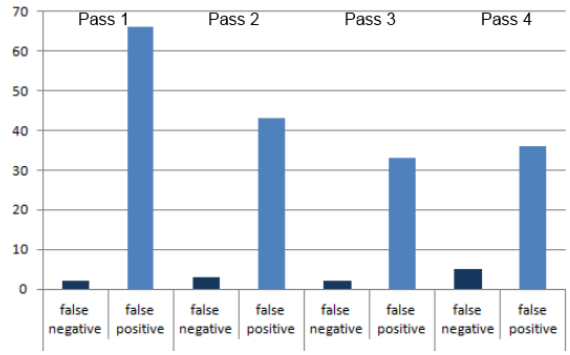


Fig. 4. False Positives and False Negatives for Different Ratios

B. Data Collection Optimisation and Compression

Currently, learning data sets as well as actual input for the neural network during normal usage of the mobile device is collected and recorded into simple CSV files. This may prove to be a problem regarding the size of collected data. Transmission of data using WLAN or 3G networks is a very expensive task in terms of power consumption. Therefore, compression techniques may need to be applied on the device to reduce the size of transmitted data. However, this has not been considered to date.

VII. CONCLUSION

In this paper, we analyzed whether or not and to which certainty users of mobile devices can be authenticated based on their touch gesture attributes. As a part of the MoSeC architecture this module is not required to achieve a 100% success rate, but rather serves as a supporting mechanism for detecting possibly unauthorized accesses in combination with other techniques. One major aspect of this system is to offload as much resource-intensive tasks as possible into the cloud to preserve battery power. Therefore, we use the mobile device only to record and save touch gesture information. After transmitting the data to a proxy virtual machine in the cloud, a neural network evaluates this data. Depending on the result, the agent on the mobile device is informed on which action must be taken (e.g., force re-authentication using strong mechanisms like passwords). Additionally, the authentication information is used to trace usage of the device retrospectively for evidence collection, when a breach of security is detected.

As we have shown, touch gesture analysis based on artificial neural networks is a suitable solution for detecting unauthorized access to mobile devices. However, the inherent uncertainty of the analysis results provided by the network need to be considered. We have shown that by choosing a 1:1 ratio between positive and negative learning patterns relatively stable results can be reached. Another important factor is the training time. Because users might change their touch gesture behaviour over the time, the network has to be re-trained in defined intervals.

In our future work, we focus on widening our pool of test users, to achieve even more stable results. Also, further optimisation needs to be considered. This includes the integration of tamper-proof recording of touch gesture information, compression of data as wells as finding the right balance

 ISBN: 978-1-61208-292-9

between transmission frequency and power consumption due to active WLAN or 3G. Also, network traffic generated by our solution is a big concern and needs to be measured and quite possibly optimized in our application to reduce resource consumption to a minimum, which in turn would also reduce power consumption.

REFERENCES

[1] F. W. M. H. Wong, A. Supian, A. Ismail, L. W. Kin, and O. C. Soon, "Enhanced user authentication through typing biometrics with artificial neural networks and k-nearest neighbor algorithm," in Conference Record of the Thirty-Fifth Asilomar Conference on Signals, Systems and Computers, vol. 2, 2001, pp. 911–915.

[2] G. Pannell and H. Ashman, "User modelling for exclusion and anomaly detection: a behavioural intrusion detection system," in Proceedings of the 18th international conference on User Modeling, Adaptation, and Personalization, ser. UMAP'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 207–218.

[3] A. Gupta, D. Gupta, and N. Gupta, "Infosec-mobcop framework for theft detection and data security on mobile computing devices," in Contemporary Computing, ser. Communications in Computer and Information Science, S. Ranka, S. Aluru, R. Buyya, Y.-C. Chung, S. Dua, A. Grama, S. Gupta, R. Kumar, and V. Phoha, Eds. Springer Berlin Heidelberg, 2009, vol. 40, pp. 637–648.

[4] E. Imsand, D. Garrett, and J. Hamilton, "User identification using gui manipulation patterns and artificial neural networks," in Symposium on Computational Intelligence in Cyber Security (CICS 2009), 2009, pp. 130–135.

[5] D. Guse, N. Kirschnick, S. Kratz, and S. Möller, "Gesture-based user authentication for mobile devices," in Proc. MobileHCI 2011, Workshop on Body, Movement, Gesture & Tactility in Interaction with Mobile Devices, 2011.

[6] W. Shi, J. Yang, Y. Jiang, F. Yang, and Y. Xiong, "Senguard: Passive user identification on smartphones using multiple sensors," in WiMob'11, 2011, pp. 141–148.

[7] B. Schneier and J. Kelsey, "Secure audit logs to support computer forensics," ACM Trans. Inf. Syst. Secur., vol. 2, no. 2, pp. 159–176, May 1999.

[8] T. Ruebsamen and C. Reich, "Enhancing mobile device security by security level integration in a cloud proxy," in CLOUD COMPUTING 2012, The third International Conference on Cloud Computing, GRIDs, and Virtualization, 2012, pp. 159–168.

[9] "HFU Cloud Research Lab," http://www.wolke.hs-furtwangen.de/, [retrieved: july, 2013].

[10] P. Turner, "Unification of digital evidence from disparate sources (Digital Evidence Bags)," Digital Investigation, vol. 2, no. 3, pp. 223–228, Sep. 2005.

[11] "Wikipedia on Multi Touch Gestures," http://en.wikipedia.org/wiki/Multi-touch, [retrieved: july, 2013].

[12] "Membrain," http://www.membrain-nn.de/, [retrieved: july, 2013].

 ISBN: 978-1-61208-292-9

A Real Virtuality Application: The Real Farmer Game

Michail I. Tourlos, Aris I. N. Paraskevopoulos, Christos T. Pezirkianidis, Stavros S. Stavrianidis, Iakovos A. Pavlopoulos, George S. Tselikis, Nikolaos D. Tselikas and Anthony C. Boucouvalas
Department of Informatics and Telecommunications
University of Peloponnese
Tripoli, Greece
{tst09001, tst09012, tst09032, tst09041, tst07048, tselikis, ntsel, acb}@uop.gr

Abstract—**The paper presents the concept of "Real Virtuality" and applies it to online games, by implying the real-time integration of real life conditions and elements into the virtual world of a game, rendering it as lifelike as possible. On this basis and by taking into account the real weather conditions in real-time, we designed a simple game prototype (i.e., the Real Farmer) based on the main concept of the popular game FarmVille. The concept, the architecture and the implementation issues of the Real Farmer game are all presented and analyzed. Finally, as a proof of concept and for measuring the efficiency and the reliability of the implemented algorithms that mix real and virtual environments in the game context, a comparison between the results in a real life farm and the corresponding ones in the game is presented, which validated our implementation.**

Keywords-Real Virtuality; Game development.

I. INTRODUCTION

For many people, computer as well as internet games' entertainment is part of their everyday life. Most of these games are trying to set the player into a fictional, and sometimes virtual, environment, following the virtual reality concept [1]. Thus, the game industry targets products with attractive virtual environments, in order to set the players even deeper in this virtual world, while, on the other hand, the virtual environment is sometimes preferred to be designed as realistic as possible [2].

The latter is following the "Real Virtuality" concept. The basic idea of "Real Virtuality" starts in 1991 from Mark Wiser when he published the article "The Computer for the 21st century", and describes that the "Virtuality" of computers, i.e., the ability to compute, view and alter data with a computer, will exist within our physical world, outside of an electronic shell [3]. In computer games, this could be achieved by implying the real time integration of real life conditions and elements into the virtual world of a game, in order to render it as lifelike as possible.

Having the above ideas in mind, we designed and developed a prototype online computer game, i.e., the "Real Farmer" game. The game is based on the main concept of the popular game FarmVille [4], that adopts the "Real Virtuality" concept, by taking into account in near real time the real weather conditions and using them in the gameplay.

The rest of the paper is organized as follows. Section 2 cites the related work on computer games that follow the "Real Virtuality" concept. Section 3 presents the concept of "Real Farmer" game. Section 4 presents system's architecture as well as the corresponding implementation issues. It analyses technical issues and explains the operation and the logic of its components. Section 5 tries to validate the reliability and the accuracy of the game, based on a real life experiment. The paper is summarized in Section 6.

II. RELATED WORK

There are several computer games trying to mix the real and the virtual world of the game. Ingress is a game developed by Google specially designed for Android mobile devices [5]. The players are divided into two factions and their ultimate target is to conquer the whole field of a specific geographical map of the real world. By using the GPS receivers of their mobile devices, the players are able to control and examine their nearby area and can interact with objects of this map, so, in most cases, the game requires physical presence in the corresponding area. The mobile client represents each player as a small triangle, surrounded by a circle area (20m radius), within which the interaction is possible through the corresponding game interface.

Lego has also developed a game for Android and iOS mobile devices, following the Real Virtuality concept. The game is called "Life of George" and the objective is to build specific constructions indicated by "George" (i.e., the mobile device), with real Lego bricks [6]. George indicates a construction that must be built quickly and accurately. Construction's rating depends on virtuosity. If a construction is a virtuosic one it will be ranked with a high rate; otherwise, with a low one. In order to get to the next level, each construction instructed by George has to be completed

 ISBN: 978-1-61208-292-9

within a specific time period. In this period, the player also has to use the camera of the mobile device, in order to capture a photo of the construction, to upload it through the corresponding interface and get to the next level of the game.

"Save 'Em" was designed to explore the challenge of making computer games more immersive [7]. Inspired by Lemmings [8], a classic computer game, Save 'Em is based on maneuvering a group of slow-witted characters called Dudes through a treacherous maze. Using augmented reality techniques, Save 'Em places virtual game entities directly within the player's physical environment; gameplay takes place on a real game board rather than on a computer screen, and the Dudes' fate is tied directly to the player's physical actions.

There are also many games and platforms that try to feed the virtual world of the game with elements from real life, by using, in many cases, special joysticks or external control devices. Most of them are about real time "music", "dancing" or "sports" games. For example, in "Dance Dance Revolution" by Konami, the player steps and dances on an appropriate arrow plastic mat to match the on screen arrow [9]. In "Guitar Hero" by Harmonix for Playstation 2 platforms, the player has to use a miniature of a Gibson guitar, while in "Donkey Konga" by Nintendo the player has to clap and drum in rhythm by using two small bongo drums [10]. Last, but not least, the Wii by Nintendo, was the first game platform that popularized new concepts like force-feedback in many games through the corresponding proprietary interface [11].

To conclude from all the above, we can see that the target of game industry is to design and produce more interactive games. Nevertheless, there are still very few games on the market based on the "Real Virtuality" concept. Probably the answer is that "Real Virtuality" needs more time to mature as a concept in order to be absorbed by the game industry. This is also another reason to present the "Real Farmer" game.

III. THE "REAL FARMER" GAME

The "Real Farmer" is a farming simulator online game, targeting to promote the most productive farmer. Through this game, the player has the opportunity to become a real farmer in a virtual world. Similar to every real farmer, the player has his/her own farmstead and he/she has to take care of it in order to achieve as bigger harvest as possible, and finally, get a corresponding profit by selling it. With this profit, he/she would be able to buy essential supplies such as fertilizers, seeds and farming equipment and use them to improve the productivity of the farm.

The first step of the player is to choose a region to build his/her own farm. By default, the proposed region is the one where the player lives, but there is also the opportunity to buy land for a second farm in another place, if he/she posses the required budget. The price of the land varies, depending on the corresponding fertility; more fertile land means more expensive to acquire. After this step, the game begins and involves the "Real Virtuality" concept in its own concept by applying in near real time the real weather conditions of the corresponding farm's region, since the weather conditions differ from a region to another. In order to make the concept even more realistic, there is also a kind of help in the game providing useful agricultural information about the kind of vegetables or fruits that thrive in specific regions or climates. This information includes the proposed plants per region, some basic requirements for each plant (climate conditions, water, suitable fertilizers, etc.), the whole life cycle of the plant (in days), the cost of the seeds and the estimated profit from each plant (both in euros per kilo).

Based on all the above, the farmer takes a decision about his/her final virtual farming and up to this point the game follows the real life rhythm, with the mean that the actual time for the virtual plants growing up, the plants' condition as well as the weather conditions in the farming will follow the corresponding real ones.

IV. SYSTEM ARCHITECTURE AND IMPLEMENTATION

The Real Farmer is a network game designed for windows and mac operating systems. It follows the client-server model and requires an Internet connection.

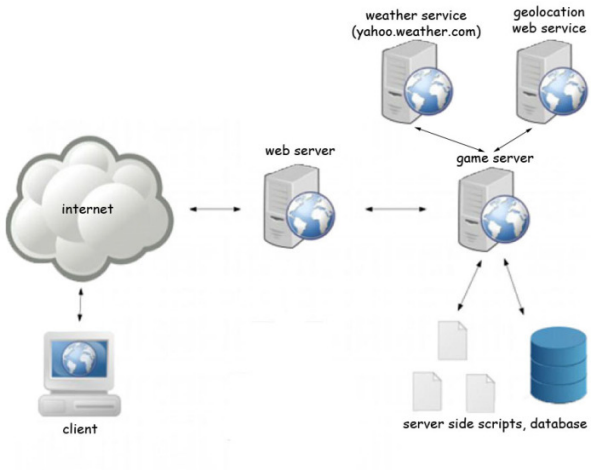


Figure 1. Real Farmer high-level architecture.

As shown in Figure 1, on the server side, there are two deamon applications, both developed in Java, residing in the game server. The first one is responsible to discover the location of a new player, by using a corresponding geolocation web service, while the second one is used to get the required weather information, from a reliable and hourly up to date weather forecast site [14]. Further up, the demon parses the data and stores it into the database as game parameters in an hourly rate. The above function is periodically triggered for every region where a subscribed

 ISBN: 978-1-61208-292-9

user resides. Furthermore, the game server includes also the required scripts, which are handled via AJAX technique [15] by the client-side, in order to connect with, query and get response from the database.

The client-side is a graphical environment developed in Unity platform [12]. It illustrates the land with the vegetables or trees that the farmer decided to farm. The farming life-cycle is directly affected by weather conditions such as temperature, wind speed, rain emission, snow emission and cloudiness. These parameters alter in real-time (or, at least, in near real-time) based on the information stored into database in hourly rate. From a software perspective, both plants and weather conditions are Javascript classes that interact with each other. Actually, the state of the latter (i.e., the weather condition object) affects the corresponding methods of the former (i.e., the plants objects).

Following the Real Virtuality concept, the growth rate of the game's plants has to follow the corresponding one of a real plant. On the other hand, for the smoothness of a scene, game developers are usually updating game's variables per game frame. But in the Real Farmer case, the corresponding functions for updating a vegetable's growth is not required to be triggered every frame. Thus, they're periodically triggered in per second rate. Actually, this time interval is also short enough and makes the plant to appear stagnant, but we used it, in order to have a common basis in time scale (1 day = 24 hours = 1440 min = 86400 sec) in conjunction with the reality.

To be more specific, we chose one vegetable (i.e., the carrot) to describe the corresponding pseudo-code regarding plants' growth and how weather conditions may affect it, as described in Figure 2. Similar methods have also been defined for all supported plants of the game.

Essential weather parameters affecting carrots' health and growth rate are rain emission (a carrot needs about half liter of water per day), cloudiness (the farming must be ideally hit by sunlight about eight hours a day) and snow emission (snowfall destructs carrots). Wind speed is not affecting it at all, since carrot is actually a root and it's growing up into the ground. All vegetables support one main method for their growing, let us call this `plant_growing()`. They also include variables about their growth, growth rate, sun exposure, health and humidity. This is an abstract method, and it's specially modified for each plant available in Real Farmer game, rendering this way the game more realistic. If the farmer sows a number of seeds, an equal number of the corresponding plant objects are created (actually one object is created and the number of seeds is defined as constructor's parameter) and the corresponding attributes are set to fixed values, by default.

In the pseudo-code of Figure 2, `-15 * 10^(-5)` is the dehydration rate of the carrot, while `10^(-7) * rain_emission` is his hydration rate when it rains, and depends on rain emission.

```
growth = 0;
humidity = 50;
sun_exposure = 100;

plant_growing() triggered every second {
humidity = humidity -15 * e^(-5) + e^(-7) *
rain_emission;

if (sun is up AND cloud_cover_percentage < 100)
  sun_exposure = (sun_exposure + (100-
cloud_cover_percentage))/ 86400;
else
  sun_exposure = sun_exposure - 1/86400;

health = 2*humidity/3 + sun_exposure/3;
growth_rate = 1.5 * e^(-7) - 0.5 *(100-
health)*e^(-7);

if (health==0 OR humidity==0)
  object dies;

if (growth < 1)
  growth = growth + growth_rate;
else
  print("Harvest your carrots!");
}
```

Figure 2. Weather conditions affecting carrot's life (pseudo code)

If a player disconnects from the Real Farmer, all data concerning his/her game progress are uploaded into the server and are stored in the database. Subscribers' data will keep updating even if they are offline, because, as aforementioned, the plants in the Real Farmer grow up in real time. When a player resumes the game, all previously saved information, as well as the time he/she was offline, will be sent back to his client. The game's plants never stop growing up, unless they die or if they are ready to be harvested. To fill the gap about what happened when a user was offline, a feature has been implemented to play in fast forward a mini clip of the farming evolution or destruction. The fast forward factor is equal to 3600/5 (i.e., one real time hour is equally simulated to five seconds in the mini clip).

V. REAL FARMER VALIDATION

In order to validate the simulation activities that take place in Real Farmer, we had only one alternative, i.e., to be real farmers ourselves. This way, we can demonstrate not only the validation of the graphic representation of weather conditions (this is the easy part), but also the reliability and accuracy of the algorithms used for plants' growth.

For the first test, the left part of both Figure 3 and Figure 4 depicts captured photos from Tripoli, Greece, during a

 ISBN: 978-1-61208-292-9

sunny and a cloudy day, respectively. In the same figures, at the right, you can also see the corresponding screenshots taken from the Real Farmer at the same date and time. It is obvious that a satisfactory depiction of the real weather has been achieved. On the other hand, since the Real Farmer depends on an internet weather forecast and not in real time weather data, the accuracy of weather depiction depends on the accuracy of our internet data source. Even if there are several internet weather forecasts which are more reliable for the weather conditions in specific countries (e.g., [14] for Greece), we preferred to use Yahoo weather forecast and render Real Farmer maybe less reliable in that sense, but applicable to any region worldwide, on the other. Regarding the delay on depiction of changing weather conditions, the mean delay time is about 3 sec. This is actually the required time for the weather update in data base entries by the weather forecast service plus the time needed for re-initialization of weather parameters in the game. The delay of 3 sec can be safely characterized as negligible compared to the time that the respective weather conditions are depicted in the game (i.e., 1 hour, since the weather is updated in hourly rate).

Figure 3. A sunny day (reality vs. Real Farmer)

Figure 4. A cloudy day (reality vs. Real Farmer)

For the second test, as aforementioned, we had to be real farmers by ourselves in Tripoli, Greece. So, we sowed 10 seeds of carrot at the University of Peloponnese campus and we started the Real Farmer game in parallel. The experiment lasted for three months (November 2012 to January 2013) and the results were encouraging enough, since, as depicted

 ISBN: 978-1-61208-292-9

in Figure 5, in 88 days we were ready to harvest the real carrots, while in Real Farmer we needed only 4 more days, 92 in total.

Some additional information that is not mentioned in Figure 5 is that during the 92 days that the experiment lasted, we observed 23 sunny, 40 cloudy and 29 rainy days.

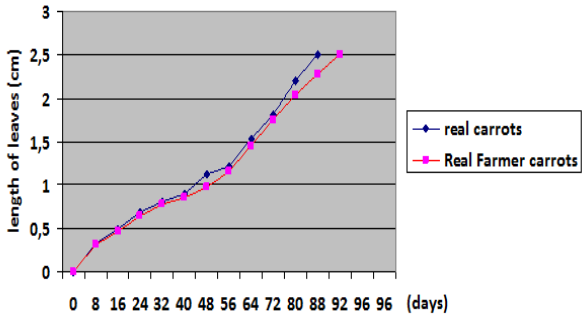


Figure 5. The carrot life cycle (reality vs. Real Farmer)

We totally calculated 94mm of rainfall and 0mm of snowfall. The mean temperature was 10.5^{o} C and the mean humidity was 76,8%. The wind speed does not affect carrots' life at all; thus, we didn't calculate it. Last, but not least, the carrot's growth is associated with the length of its leaves, since carrots are ready to harvest if the mean length of their leaves is 2.5 cm.

VI. CONCLUSION AND FUTURE WORK

Based on the "Real Virtuality" concept, we presented and analyzed the concept, the architecture and the implementation issues regarding the "Real Farmer", a simple game prototype. We also described the experiment that took place and we presented the corresponding results in order to evaluate its reliability and accuracy and validate the implemented algorithms.

In order to make "Real Farmer" more realistic, we are currently working on fine-tuning of the growth algorithm regarding most of the supported plants. Furthermore, we also plan to give a business-oriented perspective in the game, by trying to bind the final prices of the fruits and vegetables to the real market ones, at least for European and North American counties where this info is available. Finally, following the current trend, we are about to deploy the "Real Farmer" for Android mobile devices, expecting more registrations and, thus, more feedback to improve our work.

REFERENCES

[1] G. Burdea and P. Coffet, "Virtual Reality Technology", Second Edition, John Wiley & Sons, 2003.

[2] P. Zackariasson and T. L. Wilson, "The Video Game Industry: Formation, Present State, and Future", New York: Routledge, 2012.

[3] M. Weiser, "The computer for the 21st Century," IEEE Pervasive Computing, vol. 1, no. 1, 2002, pp. 19-25.

[4] FarmVille, online: http://en.wikipedia.org/wiki/FarmVille, [retrieved: July, 2013].

[5] Ingress,online: http://en.wikipedia.org/wiki/Ingress_(game), [retrieved: July, 2013].

[6] Life of George, online: http://george.lego.com/en-us/, [retrieved: July, 2013].

[7] C. Watts and E. Sharlin, "Save 'Em: physical gameplay using augmented reality techniques", ACM conference on Future Play, 2007, pp. 160-165.

[8] Lemmings, online: http://en.wikipedia.org/wiki/Lemmings_(video_game), [retrieved: July, 2013].

[9] Dance Dance Revolution, online: http://en.wikipedia.org/wiki/Dance_Dance_Revolution, [retrieved: July, 2013].

[10] Donkey Konga, online: http://en.wikipedia.org/wiki/Donkey_Konga, [retrieved: July, 2013].

[11] Nintendo-Wii, online: http://www.nintendo.com/wii, [retrieved: July, 2013].

[12] Unity online: http://unity3d.com/, [retrieved: July, 2013].

[13] Yahoo weather online: http://yahoo.weather.com, [retrieved: July, 2013].

[14] Meteo weather online: http://www.meteo.gr, [retrieved: July, 2013].

[15] C. Draganova, "Asynchronous JavaScript Technology and XML (AJAX)", 11th Annual Conference of Java in the Computing Curriculum, 2007, London.

 ISBN: 978-1-61208-292-9

Algorithms for Network Discovery and Detection of MAC and IP Spoofing Security Attacks

Paulo Lopes, Paulo Salvador, António Nogueira
DETI, University of Aveiro / Instituto de Telecomunicações
Aveiro, Portugal
{pjl90, salvador, nogueira}@ua.pt

***Abstract* — Data Link and Network layers of the OSI model use, respectively, MAC and IP addresses to provide communication between different network devices. Since this is a widely used model, it is frequently explored for various malicious activities. MAC and IP spoofing attacks are the origin of many security threats; so, preventing them is essential to obtain a protected and trustful network. This paper presents an efficient mechanism to detect and block these attacks based on the use of the SNMP protocol, which allows remote access to network devices in order to retrieve their MIB information and is supported by most of the existing network equipment. On a first stage, network discovery is used to identify the devices that are present on the network; then, by selecting and manipulating the MIB information retrieved from these devices, appropriate algorithms are proposed to detect both IP and MAC spoofing attacks. Many performance evaluation tests were conducted and the results obtained proved that these approaches are able to quickly and efficiently detect and block these network security attacks.**

Keywords-SNMP; Network Discovery; MAC Spoofing; IP Spoofing.

I. INTRODUCTION

Today, networks have a fundamental role in our lives, being used for business, communication, data exchange, entertainment, and so on. Due to this increasing importance, networks have been improved in order to become more resilient, secure and able to cope with the appearance of new technologies and applications. The seven layer Open Systems Interconnection (OSI) model was adopted by most of the systems to provide communication between devices. Layer 2, also called Data Link layer, uses a physical Media Access Control (MAC) address to provide communication between the different devices in a local network. This address is a serial number that uniquely identifies the device. Layer 3, also called Network Layer, is responsible for packet routing functions, using the Internet Protocol (IP) to deliver packets from source to destination based on their IP addresses.

Network security vulnerabilities have been intensively explored with the appearance of tools that are able to retrieve critical information, access to unauthorized networks or even overload servers and network connections. This paper focuses on two types of network security attacks: MAC and IP spoofing. MAC spoofing attacks take advantage of the fact that even though a MAC address is supposed to be permanent it can be changed in most of the devices. In this way, an attacker can easily impersonate any user on the network by changing the MAC address of his machine in order to match the MAC address of his target host. Spoofing MAC addresses is one of the most common network attacks and is mostly used to get access to an unauthorized network, using the identity of an authorized client. IP spoofing attacks are similar to MAC spoofing attacks but, in this case, the IP address must be configured to match the IP address of the victim, while the MAC address remains unchanged. Again, the intruder will impersonate an authorized client, getting access to the network.

The approaches proposed in this paper to prevent these types of network attacks are based on the Simple Network Management Protocol (SNMP) protocol [1]. SNMP is used to remotely manage network devices by using data stored on their Management Information Base (MIB) [2] and is supported by most of the network devices. A MIB is a virtual database with information about the network and the device itself; this information is hierarchically organized and each object is identified by the Object Identifier (OID). It is possible to detect and block MAC and IP spoofing attacks, as well as perform network discovery, simply by retrieving and managing the information contained on the MIB of each network device. As will be shown later, the developed algorithms proved to be reliable and efficient in the detection and blocking of both types of network security attacks.

In order to detect and prevent this type of security threat, it is crucial to have a complete knowledge of the network topology. So, this paper will also present a network discovery algorithm that is able to find and distinguish the different network devices, whether they are Layer 2 or Layer 3 equipments. For all network simulations that were carried out, the network discovery method was able to identify the different devices and retrieve network information from their forwarding and Address Resolution Protocol (ARP) tables. The deployment of these methodologies is very simple, so they can be applied on any network, assuming that all devices have been correctly configured.

The rest of this paper is organized as follows. Section II presents the related work on remote access tools and methodologies used to prevent MAC and IP spoofing security attacks; Section III describes a method to perform network discovery using SNMP; Sections IV and V describe the methodologies used to prevent MAC and IP spoofing security attacks using SNMP, respectively. Both sections are divided in two parts: part A presents a method to detect attacks, while part B discusses a solution to block them. Section VI describes the experimental tests that were carried out and the main results obtained and, finally, Section VII concludes the paper.

 ISBN: 978-1-61208-292-9

II. RELATED WORK

A. Remote Access Tools

Many protocols and tools have been developed to remotely manage network devices. Telnet, Secure Shell (SSH) and SNMP are some of the most commonly used protocols.

Telnet is a network protocol used to connect to remote machines located in the same LAN or in the Internet. A Transport Control Protocol (TCP) connection is established to log into a remote machine, using its IP address and port number [3]. The most relevant advantages of this functionality are the fact that it is supported by most operating systems and it provides access to several network services. However, Telnet has some security problems: by default, it doesn't support encryption and most implementations do not even have any authentication, so passwords and other secret information exchanged between devices can be easily intercepted and read. Due to this lack of security, Telnet has been discontinued and replaced by more secure tools.

SSH (Secure Shell) is another network management protocol developed to provide remote access, being primarily used in UNIX and Linux environments [4]. Unlike Telnet, SSH provides encryption and prevents attackers from accessing secret information included in the data packets. Nowadays, it is the most secure and used tool for remote access.

SNMP (Simple Network Management Protocol) is a management protocol that allows a client or manager to poll network devices (agents) running on a network for specific information [1]. This information is contained in a text file, called MIB, and is hierarchically organized. SNMP uses specific commands to access and manage this information. Unlike previous remote access tools, which operate by getting access to a remote machine and then executing commands as if we were working directly on the device, SNMP commands are sent from the local machine to retrieve information from the server. Thus, we only need to execute commands from the local machine in order to get information from any network device that supports SNMP. This allows the user to easily develop scripts that can automatically retrieve and manage information contained on the MIB of each network device; this is why we choose this protocol to implement the methodology for preventing IP and MAC spoofing attacks.

To correct the security deficiencies of SNMPv1 and v2 (the first two versions that were released), SNMPv3 defines an overall SNMP architecture and a set of security capabilities, including three important services: authentication, privacy, and access control. Using SNMPv3, users can securely collect management information from their SNMP agents without fear that the data has been tampered with. Also, confidential information, such as SNMP set packets that change a device's configuration, can be encrypted to prevent their contents from being exposed on the wire. Also, the group-based administrative model allows different users to access the same SNMP agent with varying access privileges.

B. Prevention of MAC and IP spoofing attacks

Several works have addressed the same subject that is studied in this paper, the prevention of MAC and IP spoofing network attacks. Sasu et al. [5] proposes a method to detect MAC spoofing attacks based on the Destination Traffic Fingerprint (DTF). The general idea of this method is to generate constant traffic, which is used as a reference fingerprint, from an end device to a set of IP destinations. The IP address and the traffic percentage are recorded for each fingerprint and, based on this reference, the method establishes an Overall Degree of Recognition that will be used to determine if a MAC address is being spoofed or not.

In Puangpronpitag et al. [6], an egress Network Access Controller NAC () is used to authenticate internal users before they access the external network. Since MAC spoofing attacks can bypass the egress NAC by spoofing the MAC address of an authenticated client in order to get access to the network, the proposed solution is based on an authentication visa checking mechanism. This solution is mostly used on Wi-Fi hotspots, although it can also be used on wired connections using Ethernet ports.

The approach proposed in Wang et al. [7] to prevent IP spoofing attacks is based on the fact that even though an attacker can forge any field of the IP header, he cannot fake the number of hops an IP packet travels to reach its destination. Then, it is possible to create a map of the IP addresses corresponding to the different hops in order to detect spoofed IP packets. The filtering technique is called Hop-Count Filtering (HCF) and detects IP spoofing attacks using an IP-To-Hop-Count (IP2HC) mapping table.

Yao et al. [8] proposes a method to perform IP spoofing filtering that presents resource consumption proportional to the size of the attack. The filtering mechanism, called Virtual Anti-Spoofing Edge (VASE), uses sampling and on-demand filter configuration to detect IP spoofing attacks. Due to the intermittent nature of the attacks, unnecessary overhead is reduced.

In Gonzalez et al. [9], the authors propose a method, based on a Bayesian inference model, to detect attacks that are triggered by access routers. The model evaluates the trustworthiness of a router based on the packets it forwards: a judge router samples all traffic forwarded by each access router and computes the corresponding trust values.

Finally, the approach proposed by Ma [10] provides a defense against IP spoofing attacks using the traceroute utility and relying on the cooperation between trusted adjacent nodes in order to detect and block intruders from external networks. From the obtained results, it is possible to conclude that this approach provides an easy way to effectively detect and prevent IP spoofing attack.

Mopari et al. [11] provides a framework for detecting the DDoS attack and dropping the spoofed packets. By analyzing the number of hops that packets travelled before reaching the destination, the legitimacy of a packet can be found out. In fact, an attacker can forge any field in the IP packet but he cannot control hop count. So, by generating an IP to Hop-Count

 ISBN: 978-1-61208-292-9

mapping table and inspecting it, spoofed packets can be identified.

III. NETWORK DISCOVERY

As previously stated, the main objective of this work is the development of an integrated management tool, based on the SNMP protocol, which can be used to discover the different network elements, detect and prevent MAC and IP spoofing network security attacks. The next three sections will consecutively present the network discovery approach that was devised, as well as the network security attack detection and prevention methodologies that were developed for both types of security flaws.

When an algorithm is used to prevent network security attacks, every device present on the network should be individually analyzed. These devices operate at layers 2 and 3 of OSI model and, in order to find them, network discovery mechanisms should be deployed.

A. Basic Principle

The mechanism illustrated in Fig. 1 is able to perform equipment discovery on the whole network. It starts by accessing an already known router in the network. Then, it retrieves information from the MIB of this router using the "snmpwalk" SNMP command, putting it in an array that can be easily accessed later. This data is retrieved from the MIB objects shown in Table I, which contain information about destination networks, network masks, next-hop IP addresses, used interfaces and route types.

After this step, information from the objects represented in Table II is also retrieved. These objects contain information about the IP addresses corresponding to the media-dependent physical addresses, as well as the associated address types (static or dynamic), MAC addresses and interfaces [12][13][14]. These objects contain all information that it is necessary to perform network discovery, so they must be retrieved every time a router is analyzed.

TABLE I. SOME MIB OBJECTS FROM CISCO IP-FORWARD-MIB

MIB Object	OID	Description
ipCidrRouteDest	.1.3.6.1.2.1.4.24.4.1.1	Destination networks
ipCidrRouteMask	.1.3.6.1.2.1.4.24.4.1.2	Masks of the destination networks
ipCidrRouteNextHop	.1.3.6.1.2.1.4.24.4.1.4	Next hop IP addresses
ipCidrRouteIfIndex	.1.3.6.1.2.1.4.24.4.1.5	Used interfaces
ipCidrRouteType	.1.3.6.1.2.1.4.24.4.1.6	Route types
ipCidrRouteMetric1	.1.3.6.1.2.1.4.24.4.1.11	Route metrics

Each router can have several IP addresses associated to each interface. When performing network discovery, each device only needs to be analyzed once; however, since it can have more than one IP address, the algorithm can analyze the same router more than once. This is why the next step records all IP addresses associated to each interface in order to assure that the device is analyzed only once. This information is found in the router MIB object *ipAdEntAddr* (OID .1.3.6.1.2.1.4.20.1.1).

In order to move to the next network device, destination networks are retrieved from the router MIB. For each destination network, the algorithm must check the route type. If the route type to that network is indirect, the value of the next-hop IP address is read and the algorithm moves to the router with this IP address, following all the previous steps. Since this is the first router, we can move to the next device without checking if it was already analyzed. However, from now on it is necessary to compare the next-hop IP address with the list of IP addresses corresponding to the devices where we have already been.

TABLE II. SOME MIB OBJECTS FROM CISCO IP-MIB AND RFC1213-MIB

MIB Object	OID	Description
ipNetToMediaNetAddress	.1.3.6.1.2.1.4.22.1.3	IP address of media-dependent physical interfaces
ipNetToMediaType	.1.3.6.1.2.1.4.22.1.4	Address type
atPhysAddress	.1.3.6.1.2.1.3.1.1.2	MAC address
atIfIndex	.1.3.6.1.2.1.3.1.1.1	Interface

If the route type to a destination network is of the direct type, the IP addresses of all Layer 2 devices present on that network must be read. Whenever the algorithm finds in the list an IP address corresponding to a network device that was not already analyzed and whose address type is defined as dynamic (because static IP addresses usually belong to the interfaces of the device that it is being analyzed), then the algorithm moves to this new network device. After all Layer 2 devices present on a given network have been analyzed, the next destination network from the array is read and the route type is checked again. Since this is a recursive algorithm, when there are no more destination networks to reach, we must go back to the previous router that was being analyzed. When the first router that was analyzed is finally reached and there is no more destination networks to move to or Layer 2 devices to analyze in a given network, then it means that all network devices have been discovered.

For Layer 2 devices the task is much simpler. A list of devices belonging to a given network is analyzed using the *ipNetToMediaNetAddress* MIB object and when a Switch or Access Point that was not analyzed is found, the algorithm has simply to move to there, retrieve the necessary information and read the next IP address from the list. So, the first thing to do with Layer 2 devices is to record its IP address and then retrieve information about its forwarding table. This can be done by retrieving information from the following MIB objects: *dot1dTpFdbAddress* (OID .1.3.6.1.2.1.17.4.3.1.1) and *dot1dTpFdbPort* (OID .1.3.6.1.2.1.17.4.3.1.2). These objects represent, respectively, the MAC addresses and the corresponding bridge ports from the forwarding table of the device.

 ISBN: 978-1-61208-292-9

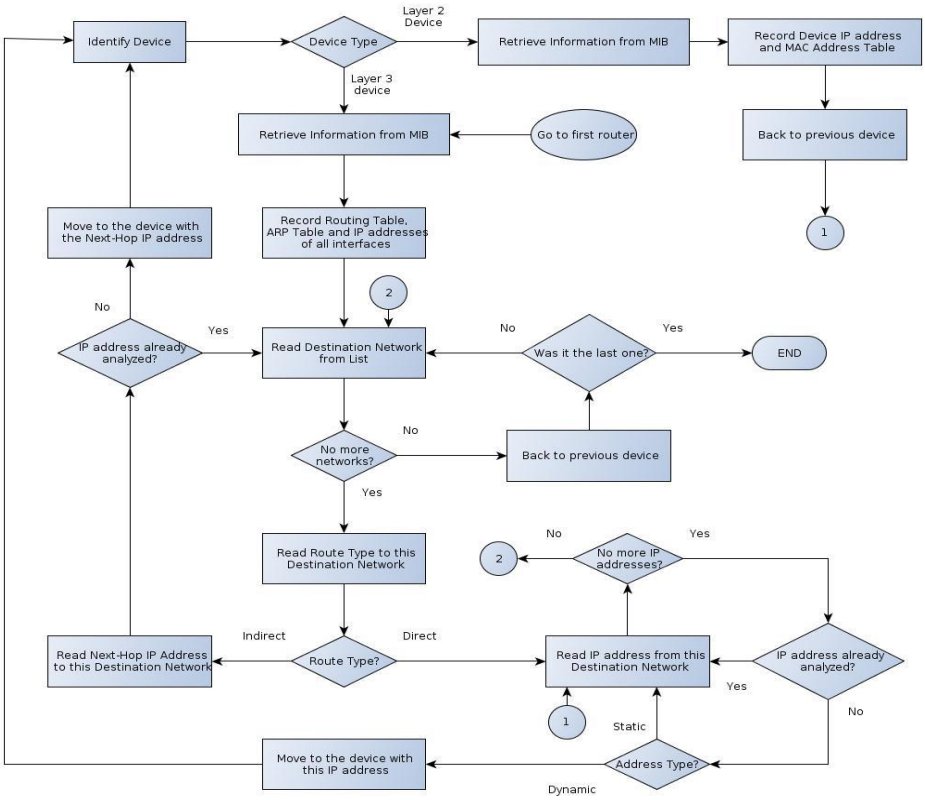


Figure 1. Network discovery algorithm

To convert the bridge port into the actual device interface, two MIB objects should be used: *dot1dBasePortIfIndex* (OID .1.3.6.1.2.1.17.1.4.1.2), to get the interface index, and *ifDescr* (OID .1.3.6.1.2.1.2.2.1.2), to get the interface name [15]. This process allows retrieving the same information that is obtained when the "show mac-address-table" command is executed in Cisco devices.

B. Some considerations

Although most of the network devices support the SNMP protocol, there are still some exceptions: we can consider that all Layer 3 devices support SNMP, but Layer 2 devices can be managed (devices that support SNMP) or unmanaged. If a network has any unmanaged switch, it won't be detected by the network discovery mechanism. To solve this problem, a counter can be created to check how many Layer 2 devices the algorithm analyzes in a certain Local Area Network (LAN). This counter will obviously count the number of managed devices. On a managed switch, the *atPhysAddress* MIB object can be used to count the number of Layer 2 devices present in the LAN (even the unmanaged ones). The difference between the two counters corresponds to the number of unmanaged devices. These unmanaged switches must be manually checked every time a MAC spoofing or IP spoofing attack can not be blocked.

Another point that has to be taken into account is the fact that Layer 2 devices include switches and access points. They have different characteristics and consequently they must be treated differently. This paper will describe in detail the steps to detect any network attack and block it in case the attacker is accessing the network from a switch. In this case, the port it is connected to must be blocked. On the other hand, if we are dealing with an attack triggered from an access point, then the attack can only be detected when it belongs to the IP spoofing attack type. This is due to the fact that, using this method, MAC spoofing attacks are detected based on the MAC address and interface that the intruder is using to access the network. In case the attacker is accessing the network from the same access point of the authorized client, there is no way to distinguish between them, because they are using the same MAC address and the same interface. That situation does not happen on IP spoofing attacks because in this case IP addresses and MAC addresses are compared and, once the MAC address of the intruder is found, the task is simply to find it on the network and block it. If the attacker is accessing the network from an access point, the procedure is similar to the case of switches but, instead of blocking the interface that the attacker is using (the wireless interface), the MAC address of the device that is being used to perform the attack is blocked; otherwise, the other devices that are using the interface could not access the network anymore. Blocking the MAC address of an end host must be done manually via SSH, for example, through the MAC Access Control List (ACL) of the access point. When

 ISBN: 978-1-61208-292-9

performing MAC spoofing detection, access points are considered unmanaged devices.

Finally, it is important to refer the case of routers that are working with a switch module. Although they are routers by default, they can work like switches and have exactly the same behavior. They can also be accessed via SNMP and its information can be retrieved, similarly to any other network device. But during this work we have seen that most of these devices have a lack of information on their MIBs, which do not allowed us to retrieve the necessary information from this type of devices. For this reason, any router working with a switch module will be considered as an unmanaged switch.

IV. MAC SPOOFING

As previously said, Layer 2 devices use MAC addresses as their LAN identifiers. This address is assigned by the manufacturer to each interface of the device and is controlled by the Organizationally Unique Identifiers (OUI) to be globally unique for all LAN-based devices. However, MAC addresses can easily be changed in most devices without any consequences on their performance. This means that faking MAC addresses is a simple way for an attacker to perform network security attacks. There are several reasons to perform this kind of attacks [16], but one of the most common is to impersonate an already authenticated user. In this case, the attacker just needs to know the client MAC address and change its own address accordingly. In this way, and since the user is already authenticated on the network, the attacker can send and receive traffic disguised by the MAC address of the user.

In the next sub-section, we will present a procedure, based on SNMP protocol, to detect these Layer 2 attacks and block the access of the intruder to the network.

A. Attack Detection

Fig. 2 describes a method to detect and block MAC spoofing attacks. This mechanism will basically create a record of the MAC addresses of all interfaces of the different network end devices. If someone tries to fake a MAC address, then the port or even the switch will change because that MAC address will appear on another location. This algorithm is able to detect such situation and figure out if it is really a MAC spoofing attack or if the client has simply changed the physical location of the device.

The algorithm starts by performing the network discovery procedures described in the previous section in order to find and identify all network devices. When dealing with MAC spoofing attacks, we just have to analyze switches. After selecting these devices, each one is analyzed individually. Then, useful information is retrieved from the MIB of the switches. Information that it is needed to detect MAC spoofing attacks should be selected, retrieved using the SNMP "*snmpwalk*" command and put in an array in order be easily accessible. The necessary MIB objects are *dot1dTpFdbAddress*, *dot1dTpFdbPort* and *atPhysAddress*, as already mentioned in the previous section. Below, we will show why this information is so important and we will mention other MIB objects that are used in this detection approach.

Switch access ports are needed because end hosts are connected there. Since all ports are already known, access ports can be selected using the MIB object *vlanPortIslOperStatus* (OID .1.3.6.1.4.1.9.5.1.9.3.1.8), which returns value '1' for Trunking and '2' for Not Trunking. However, an access port can also be connected to another network device instead of an end host. In this case, the MIB object *atPhysAddress* should be used. If any of the MAC addresses associated to an access port belongs to the list of MAC addresses of the *atPhysAddress* object, it means that the access port is not connected to an end device and should be excluded from the list of ports to analyze.

The first stage is completed and we now have all the necessary information. The next step consists of reading each MAC address associated to the selected access ports. When a MAC address is analyzed, the method should check if it was already recorded. We choose to maintain a record of all MAC addresses of the end hosts that are found on the network. If the MAC address that it is being analyzed does not exist yet in this historic, then a record must be added, containing the MAC address, the corresponding network device and the port where it is connected to. The access port is already known and the information about the device can be retrieved through the MIB object *hostName* (OID .1.3.6.1.4.1.9.2.1.3). The registration time is also recorded, as well as a counter whose value is 0. This is all the information that is needed regarding each MAC address that is detected in the network. Then, the next MAC address in the array should be read. When there are no more MAC addresses to read, the algorithm moves to the next Layer 2 device.

When a MAC address is already registered, its location in the network should be checked to verify if it is in the same place or if it has moved to another location. The historic already contains the switch and port associated to this MAC address. So, the recorded information is compared to the switch and port that the MAC address is using now: if they are equal, it means that the end host is in the same place; otherwise, we can be sure that the end host has changed its physical location or someone is faking this MAC address and is using it to connect to the network from another location.

TABLE III. SOME MIB OBJECTS FROM CISCO BRIDGE-MIB AND CISCO STACK-MIB

MIB Object	OID	Description
dot1dTdbAddress	.1.3.6.1.2.1.17.4.3.1.1	MAC addresses from the MAC address table
dot1dTpFdbPort	.1.3.6.1.2.1.17.4.3.1.2	Bridge ports from the MAC address table
dpt1dBasePortIfIndex	.1.3.6.1.2.1.17.1.4.1.2	Interface index
vlanPortlslOperStatus	.1.3.6.1.4.1.9.5.1.9.3.1.8	Trunk or access port

 ISBN: 978-1-61208-292-9

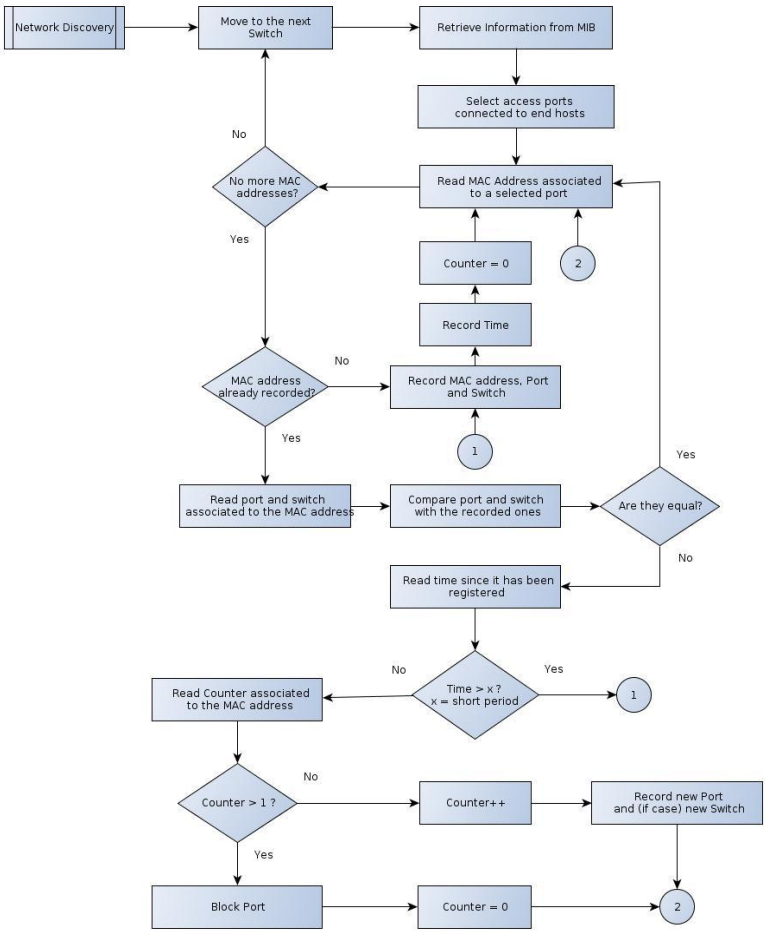


Figure 2. MAC Spoofing detection and blocking algorithm

B. Attack Blocking

Once a possible attack is detected, it is important to verify if it is a real attack or if the user has just moved the end device to another location on the network. The first question that should be answered in order to understand the reason for this change is: how much time has passed since the MAC address has been registered? When the MAC address was recorded for the first time, many parameters were saved, including the registration time. In this way, it is possible to check how much time has elapsed since that instant. When there is a MAC spoofing attack, a client is communicating and the attacker is using the same MAC address to send and receive traffic from the network, but from another location. This means that in a real MAC spoofing attack changes will be detected in the port (and possibly in the switch) associated to the MAC address in a short period of time (few seconds). So, if the time elapsed since the MAC address has been registered is greater than this short time interval, it means that probably the client has just changed his location and the network is not under attack. In this case, the new port has to be recorded and, if it is the case, the new switch. The registration time is also updated and the counter is set to value 0 (if it was not 0 already).

On the other hand, if the time since the MAC address registration is shorter than the time period that is considered normal when the network is under attack (in our tests this value was considered as equal to 30 seconds), then another question arises: how many times this MAC address has changed its location during the short time period we are considering? The counter parameter can be used to answer this question. If a change was detected in the last seconds, then the counter associated to the MAC address must be checked. If the counter has a value of 0 or 1, then it means that in the last seconds that MAC address has not changed its location or has changed it only once, which can be considered as normal. In this case, the counter is incremented and the new port is updated. The time parameter is not updated because it is necessary to check if there will be more changes in the next few seconds. If the counter reaches a value greater than 1, it means that a change of location was detected more than once in a short period of a few seconds, which can be considered as an unusual behavior and consequently there is a high probability that the network is under a MAC spoofing attack.

When a MAC spoofing attack is detected, it must be blocked. Using this method, this operation is really easy to accomplish because a record of the previous ports and switches is maintained and compared to the port and switch that a given MAC address is using now to access the network. So, if a MAC spoofing attack is detected and the attacker is using a switch to perform the attack, the port where the MAC address

 ISBN: 978-1-61208-292-9

is connected to at the moment will be blocked. Using information corresponding to the bridge ports associated to the different MAC address (available from the *dot1dTpFdbPort* MIB object), the interface index of the device that has to be blocked can be retrieved using the SNMP "snmpget" command over the *dot1dBasePortIfIndex* MIB object (OID .1.3.6.1.2.1.17.1.4.1.2). Finally, we can block the port using the SNMP "snmpset" command over the MIB object *ifAdminStatus* (OID .1.3.6.1.2.1.2.2.1.7), which will shut down the interface and block the attack. In case the attacker is accessing the network from an unmanaged device, the device must be checked manually, as previously said.

V. IP SPOOFING

After the analysis of Layer 2 network attacks, it is time deal with Layer 3 attacks or IP spoofing attacks. Unlike MAC addresses, IP addresses must be configured whenever new equipment is connected to the network; otherwise, communication will fail. But, when IP addresses are not assigned automatically through Dynamic Host Control Protocol (DHCP) and the user does not know all IP addresses of the network, there is always the risk to configure a device with an IP address that is already in use. IP spoofing attacks are based on the principle that if the intruder impersonates an authorized client by using its IP address, then he can get access to the network because all devices will believe that those packets come from a trusted host [17].

There are several tools to prevent this kind of network attacks. Here, we will present a simple methodology based on the SNMP protocol. Like we did in the previous section, the approach will be divided in two parts: detecting the IP spoofing attack and blocking it.

A. Attack Detection

Fig. 3 illustrates a method to detect IP spoofing attacks. For each detected end host a record is created containing its IP and MAC addresses. If an attacker tries to use an IP address that is already in use, that occurrence will be detected by the simple reason that the MAC address of his device is different from the MAC address of the victim. This is the basic principle of this method. As shown in Fig. 3, the first thing to do is a network discovery to find all routers, switches and access points of the network. Since we are talking about Layer 3 attacks, all routers must be analyzed until an IP spoofing attack is detected. When that happens, the attacker access to the network must be blocked. To do so, all Layer 2 devices have to be checked until the intruder is found. First of all, after having a complete list of all Layer 2 and Layer 3 devices, each router of the network is analyzed separately. Then, it is necessary to retrieve and select information from its MIB in order to detect the attack. The MIB objects that should be retrieved and put in an array are: *ipNetToMediaNetAddress*, *ipNetToMediaType* and *atPhysAddress*. All of them were already mentioned in previous sections.

With this information, it is possible to have access to all IP addresses of the router forwarding table, as well as the correspondent MAC addresses and address types. A new cycle must be initiated in order to analyze all these IP addresses until there are no more addresses to read, and then move to another router and perform the same steps. When an IP address is analyzed, the first thing to do is to check for the address type. An IP address can be selected to be static or dynamic, but in this case we are only interested on dynamic addresses because we are looking for IP addresses of end devices and these are always dynamic. If an IP address is static, then the next IP address from the array must be read. If that IP address is dynamic, we have to check if it was already recorded. Like happened for MAC spoofing attacks, a record including some different parameters is kept in order to have a comparison base for the future. For each end host IP address, the corresponding MAC address and registration time are saved. If a given IP address was already registered, then recorded information must be checked. First, the MAC address that was recorded should be read and compared to the MAC address of the device that is using the same IP address at this moment. If they are equal, then it means that the IP address is being used by the same equipment and nothing wrong is happening, so the next IP address from the array can be read. If the MAC address is different, two possible things could have happened: the user simply started using a new device and configured it with the same IP address in order to have access to the network or someone is trying to perform a network attack by using the IP address of an authorized client.

In order to distinguish between these two situations, the registration time parameter is used. It is not common that an IP address is associated to different end devices in a short period of time. It can happen occasionally, for example when an end host leaves the network and the IP address that was associated to it is available to be assigned to another device. It is expected that once an end host is configured with an IP address, no one else will get the same IP address for a period of time of at least some minutes. Based on this principle, if different MAC addresses are detected for the same IP address, it must be verified how many time has passed since it was registered.

If this time is greater than the time period that is considered as normal, then a new record for this new MAC address must be created, besides updating the new registration time. On the other hand, if only a short period of time has elapsed since it was registered, then there is a great probability that some user is using the IP address of someone else to perform an IP spoofing attack against the network. In this case, we have to move on to the next stage in order to find the location of this new MAC address in the network and block the port of the switch or access point where it is connected to.

B. Attack Blocking

At this point, the IP spoofing attack was detected and the MAC address of the device that it is being used to perform the attack is already known. So, each Layer 2 device on the network should be analyzed in order to localize this MAC address. Fig. 4 describes the approach that was devised to block IP spoofing attacks.

 ISBN: 978-1-61208-292-9

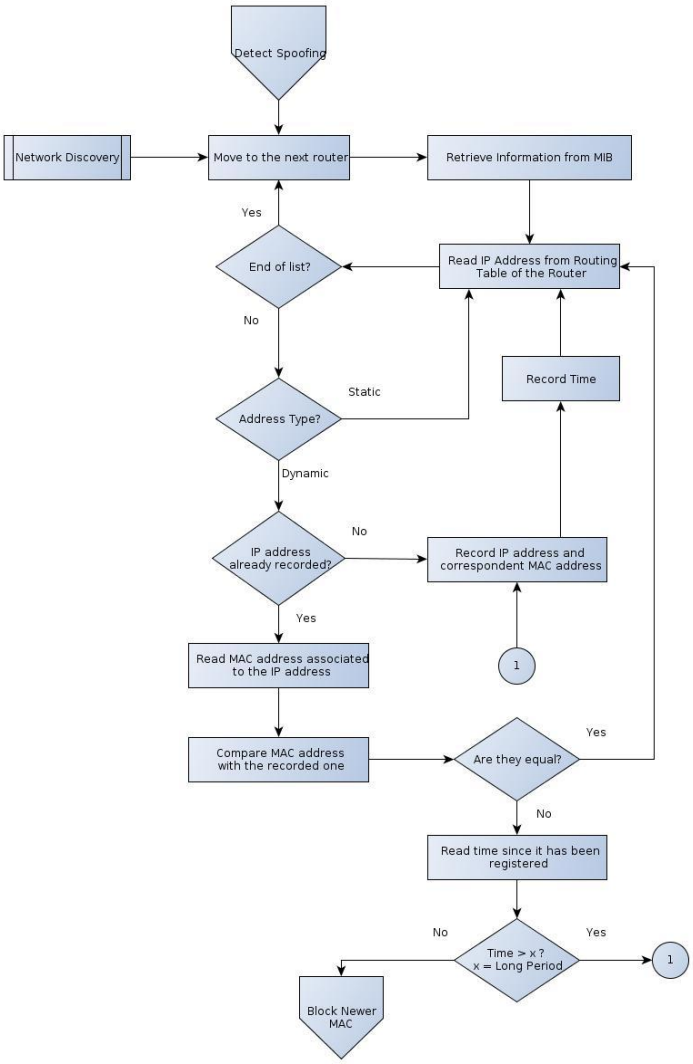


Figure 3. IP Spoofing Detection algorithm

The first thing to do is to retrieve the necessary information from the MIB of each Layer 2 device, as was previously done every time we needed to analyze any network device. In this case, the MIB information that it will be used is the same that was mentioned before to detect MAC spoofing attacks. So, the MIB objects retrieved from the switch or access point are the following: *dot1dTpFdbAddress*, *dot1dTpFdbPort* and *atPhysAddress*.

In the case of switches, ports that are being used exclusively by end devices should be identified. In order to do that, switch access ports are selected using the MIB object *vlanPortIslOperStatus* (OID .1.3.6.1.4.1.9.5.1.9.3.1.8). Then, the ports that are connected to other network devices must be excluded. If the MAC address associated to any of these ports is present in the list of MAC addresses retrieved from the *atPhysAddress* MIB object, it means that this port is not connected to an end host and can be excluded. After performing these steps, we only have the necessary switch ports.

The next step is to analyze each one of the selected ports until there are no more ports to read and, then, move to the next Layer 2 device. For each port, the associated MAC address in this particular instant is read; this address is compared with the MAC address that was previously identified as belonging to the intruder. If they are different, it means that the end device that is connected to the port is not the one we are looking for and we should move to the next port. When the right MAC address is finally found, the associated port is blocked. The interface index is necessary to block the port.

 ISBN: 978-1-61208-292-9

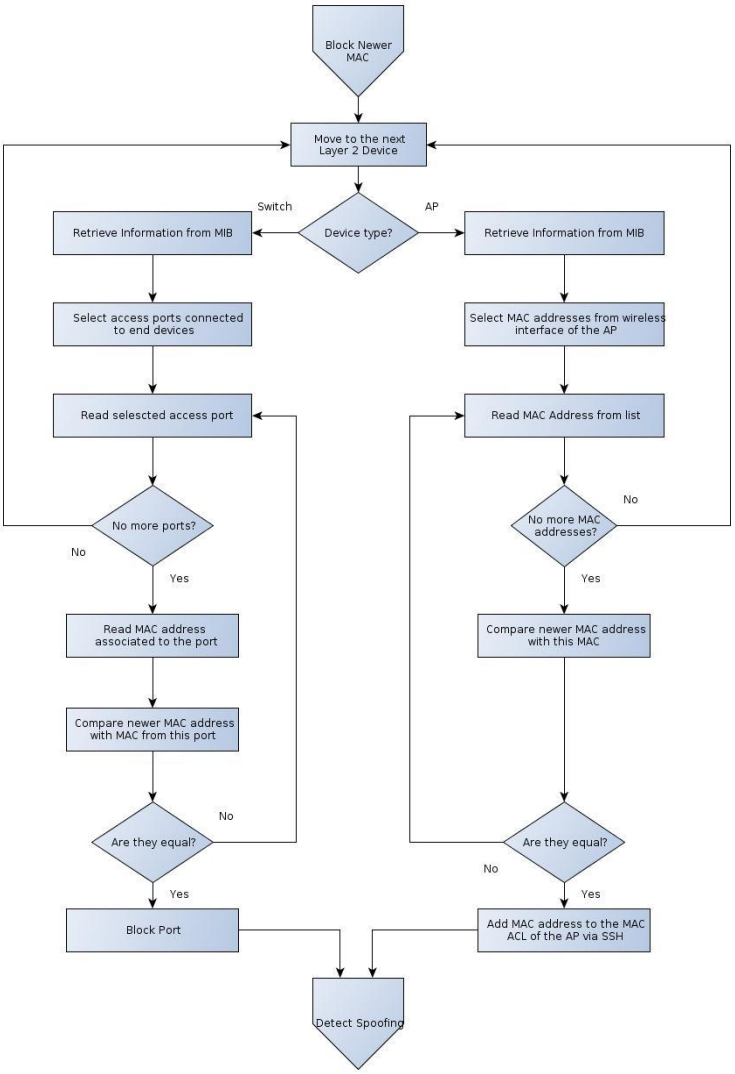


Figure 4. IP Spoofing Blocking algorithm

Using the bridge port retrieved from the *dot1dTpFdbPort* MIB object, it is possible to get the corresponding interface index using the *dot1dBasePortIfIndex* MIB object (OID .1.3.6.1.2.1.17.1.4.1.2) and executing the "snmpget" SNMP command. To turn the interface down, the "snmpset" command is executed over the *ifAdminStatus* MIB object (OID .1.3.6.1.2.1.2.2.1.7).

In case the attacker is accessing the network from an access point, all MAC addresses connected to the wireless interface will be read. If the MAC address of the intruder is not present on this list of MAC addresses, it means that it is not connected to the access point and we can move to the next Layer 2 device. Otherwise, if the MAC address we are looking for is detected in a certain access point, it must be added to the MAC ACL of the access point via SSH in order to block the access of the host to the network.

This methodology is an efficient way to block IP spoofing attacks from intruders that are accessing the network using switches or access points.

VI. EXPERIMENTAL RESULTS

In order to evaluate the performance of the proposed methodologies, the simulation scenario illustrated in Fig. 5 was set up and several simulation tests were carried out. This network is composed by four Cisco C3640 routers connected to each other, in a mesh structure.

The first mechanism that should be tested is network discovery. As previously said, the network discovery algorithm has to be sure that all managed devices are analyzed once, which is assured by this network topology. The device identified as PC represents the local machine that will work as the monitoring station to manage the network. This machine is a common laptop running Linux Ubuntu 11.10. Router R1 and

 ISBN: 978-1-61208-292-9

PC are connected to a Cisco C3725 router using a switch module (SWR1), which is considered an unmanaged device. Finally, router R3 is connected to a Cisco C3750 Catalyst switch (SW1), which is also connected to two hosts. These hosts will be used to simulate MAC and IP spoofing attacks by simulating a user with authorized access to the network and an intruder that will impersonate the user to get access to the network. Before running the algorithms, some initial information has to be inserted. For the network discovery algorithm, it is necessary to provide the IP address of any one of the network routers; it is irrelevant which router is introduced because the algorithm was developed in order to discover all network devices, independently of the first router. Then, depending on the SNMP version that it is being used, the user has to insert the same community string (version 2) or authentication password (version 3) that was configured on the devices. This allows the correct execution of the SNMP commands at the local machine. When running the network discovery algorithm, an IP address of each router and the IP address of the switch were recorded for posterior use. This information will be useful for the attack detection algorithms. The router with the switch module was undetected, as supposed. It was also possible to arrange the information retrieved from the MIB of the devices in order to graphically consult the routing tables and ARP tables from each router and the forwarding table from each switch.

For the chosen network scenario, the network discovery algorithm took 3 minutes and 15.7 seconds from the beginning of its execution until it finished the whole discovery process. This time value was obtained using the “time” command, which returns the exact time that a process takes to be executed. When the algorithm execution finally stopped, it was possible to retrieve information from all network devices that support SNMP.

For detecting MAC spoofing attacks, the corresponding detection algorithm was executed in an infinite loop. Then, one of the hosts was assigned with an IP address. The MAC address of the other host was changed in order to match the one that was in use by the first host and the host was configured with a different IP address. As previously explained, this method detects MAC spoofing attacks based on the time that has elapsed since a MAC address is registered, which is approximately equivalent to the moment when the host executes a ping command for the first time. Thus, for simulation purposes, we defined a time period of 30 seconds to distinguish between an attack and a change on the device location.

For simulating a MAC spoofing attack, both hosts have to continuously send packets to the local machine. When the first host executes a ping command, the MAC address is registered, together with the corresponding information. Then, when the second host (the intruder) started sending packets, consecutive changes on the origin of the MAC address were detected and the attack was actually blocked. The switch interface where the attacker was connected to was shutdown and the real host kept accessing the network without its performance had been affected. To confirm the efficiency of this algorithm, 20 attack simulations were performed and the results obtained can be observed in Table IV. It was verified that the attacks were detected in 18 of the 20 simulations and once the attacks were detected they were always blocked. The time since the intrusion starts until the intruder's access is blocked was quite variable, with a mean value that falls, with 95% confidence, in interval [9.368; 12.429].

TABLE IV. MAC SPOOFING ATTACK RESULTS

Simulation	Detected	Blocked	Blocking Time (s)
1	✓	✓	12.181
2	✓	✓	7.271
3	✓	✓	8.544
4	×	×	-
5	✓	✓	9.732
6	✓	✓	18.548
7	✓	✓	15.572
8	✓	✓	10.348
9	×	×	-
10	✓	✓	12.835
11	✓	✓	7.649
12	✓	✓	8.640
13	✓	✓	12.248
14	✓	✓	13.800
15	✓	✓	11.561
16	✓	✓	9.825
17	✓	✓	12.216
18	✓	✓	7.459
19	✓	✓	6.836
20	✓	✓	10.909

To test if the algorithm is able to distinguish the situation of a simple change on the location of the device, the same hosts and the same configuration were used. The first host started sending packets to the local machine and, after some time, it stopped. The MAC address and its origin were registered by the algorithm. After a time period greater than 30 seconds, the second host executed a ping command. Since both hosts have the same MAC address, this procedure simulates a change on the location of the first host. As expected, the new MAC address information was registered and no attack was detected. So, this method is able to distinguish between an attack situation, where two computers with the same MAC address are accessing the network, and the situation where a device changes its physical location in the network.

Finally, in order to test the defense mechanism against IP spoofing attacks, the corresponding detection algorithm was executed in an infinite loop. The two hosts that were previously presented were used again. The host representing the victim was configured with an IP address and the same address was assigned to other host. Let us recall that this method detects IP spoofing attacks based on the time elapsed since an IP address is registered. In practice, this time period corresponds to some minutes, but for simulation purposes it was defined as 2 minutes.

To simulate the attack, the first host executed a ping command to the local machine. When the second host accessed the network and sent packets within a time period shorter than 2 minutes, the attack was immediately detected. The switch interface where the host was connected to was blocked and the performance of the first host was not affected.

 ISBN: 978-1-61208-292-9

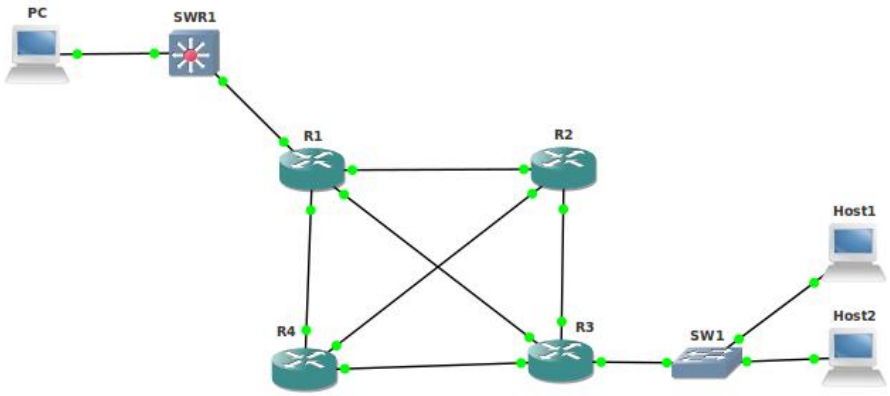


Figure 5. Testing Network

TABLE V. IP SPOOFING ATTACK RESULTS

Simulation	Detected	Blocked	Blocking Time (s)
1	✓	✓	8.079
2	✓	✓	8.352
3	✓	✓	8.469
4	✓	✓	9.042
5	✓	✓	9.040
6	✓	✓	10.848
7	✓	✓	8.612
8	✓	✓	9.292
9	✓	✓	9.076
10	✓	✓	7.536
11	✓	✓	9.071
12	✓	✓	7.863
13	✓	✓	8.795
14	✓	✓	8.920
15	✓	✓	8.613
16	✓	✓	8.424
17	✓	✓	8.560
18	✓	✓	9.264
19	✓	✓	8.452
20	✓	✓	8.517

To test the real efficiency of the algorithm, 20 attack simulations were performed. The simulation results are shown in Table V: 20 out of the 20 attacks were detected and all of them were also blocked. In terms of blocking time, it was quite regular, or at least more regular than in the MAC spoofing detection case, with a 95% confidence interval for the mean time equal to [8.426; 9.057].

On the other hand, in order to test if the algorithm is able to detect the situation of a second machine that is assigned with the same IP address but does not have any malicious purpose, the first host executed a ping command and stopped after some time. The second host has also executed a ping command but more than 2 minutes after the first one; in this case, the attack was not detected and information regarding the origin of the IP address was updated.

These experimental tests proved the efficiency of the proposed methodologies for detecting and blocking MAC and IP spoofing attacks by distinguishing between the situations corresponding to real network security attacks and to changes on the network layout. The proposed methodologies are easily deployed and work in any network, assuming that all devices are correctly configured.

VII. CONCLUSION

This paper presented several methodologies to perform network discovery and prevent MAC and IP spoofing attacks. The proposed tools are very simple to implement and can be deployed in any network that requires monitoring and has stringent security requirements. The proposed tools were developed for Cisco equipment but can be easily extended to devices from any other vendor by adapting the MIB objects that should be retrieved. There are several approaches in the literature for the detection of MAC and IP spoofing network security attacks. The great advantage of the proposed methodologies relies on the fact that they are based on the popular SNMP protocol, are very simple to use and have the potential to simultaneously perform other network monitoring tasks.

ACKNOWLEDGEMENTS

This work was supported by Fundação para a Ciência e a Tecnologia (FCT) of Portugal.

REFERENCES

[1] A. Clemm, Network Management Fundamentals, Cisco Press, 2006, pp 249-261.

[2] K. McCloghrie and M. Rose, RFC1213 - Management Information Base for Network Management of TCP/IP-based internets: MIB-II, March 1991.

[3] G. Sanjing and H. Lihui, "Research of the Telnet Remote Login", Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops (ISECS '10), Guangzhou, P.R. China, 29-31 July, 2010, pp. 219-221.

[4] T. Ylönen, "SSH – Secure Login Connections over the Internet", Sixth USENIX Security Symposium, San Jose, California, USA, 22-25 July, 1996, pp. 37-42.

[5] E. Sasu and O. Prostean, "Network simulation for MAC spoofing detection, using DTF method", 7th IEEE Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 24-26 May, 2012, pp. 291-296.

[6] S. Puangpronpitag and A. Suwannasa, "A design of egress NAC using an authentication visa checking mechanism to protect against

 ISBN: 978-1-61208-292-9

MAC address spoofing attacks", 8th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Thailand, 17-19 May, 2011, pp. 300-303.

[7] H. Wang, C. Jin and Kang Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering", IEEE/ACM Transactions on Networking, vol. 15, Issue: 1, Feb. 2007, pp. 40-53.

[8] G. Yao, J. Bi and P. Xiao, "VASE: Filtering IP spoofing traffic with agility", International Journal of Computer Networks, vol. 57, Issue 1, Jan. 2013, pp. 243-257.

[9] J. Gonzalez, M. Anwar and J. Joshi, "A trust-based approach against IP-spoofing attacks", 9th Annual International Conference on Privacy, Security and Trust (PST), 19-21 July, 2011, pp- 63-70.

[10] Y. Ma, "An Effective Method for Defense against IP Spoofing Attack", 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), 23-25 Sept., 2010, pp. 1-4.

[11] I. Mopari, S. Pukale and M. Dhore, "Detection and defense against DDoS attack with IP spoofing", Proceedings of the International Conference on Advances in Computing, Communication and Control, 2008, pp. 489-493, http://dx.doi.org/10.1145/1523103.1523200

[12] Cisco Tools & Resources, "SNMP Object Navigator", URL: http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en, (20 Feb 2013).

[13] Y. Qiuxiang, "Algorithm Research of Topology Discovery on SNMP", International Conference on Computer Application and System Modeling (ICCASM), 22-24 October, 2010, vol. 12, pp. 496-497.

[14] K. Qin and C. Li, "Network Topologic Discovery Based On SNMP", Proceedings of the 5th International Conference on Ubiquitous Information Technologies and Applications (CUTE), 16-18 December, 2010, pp. 1-3.

[15] Cisco IP Application Services, "Using SNMP to Find a Port Number from a MAC Address on a Catalyst Switch", URL: http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00801c9199.shtml, (25 Feb 2013)

[16] A. Pandey and J. Saini, "Counter Measures to Combat Misuses of MAC Address Spoofing Techniques", Int. J. Advanced Networking and Applications, 2012, vol. 3, Issue 05, pp. 1358-1361.

[17] S. Rana and T. Bansod, "IP Spoofing Attack Detection using Route Based Information", International Journal of Advanced Research in Computer Engineering & Technology, vol. 1, Issue 4, June 2012.

 ISBN: 978-1-61208-292-9

QoS Equalization in a Multirate Loss Model of Elastic and Adaptive Traffic with Retrials

Ioannis D. Moscholios[1], Vassilios G. Vassilakis[2], Michael D. Logothetis[3] and Michael N. Koukias[3]
1. Dept. of Telecommunications Science and Technology, University of Peloponnese, Tripolis, Greece.
Email: idm@uop.gr
2. School of Computer Science & Electronic Engineering, University of Essex, Colchester, U.K.
Email: vasilak@essex.ac.uk
3. WCL, Dept. of Electrical and Computer Engineering, University of Patras, Patras, Greece.
Emails: m-logo@wcl.ee.upatras.gr, koukias@wcl.ee.upatras.gr

***Abstract*—In this paper, we consider a single-link modeled as a loss system, which accommodates multirate traffic of elastic and adaptive calls. Calls arrive in the link according to a Poisson process, have a peak-bandwidth requirement while their service time is exponentially distributed. If the available link bandwidth is lower than the peak-bandwidth requirement of a new call, then the call can retry to be connected in the link with reduced bandwidth, one or more times (single/multi-retry loss model). If the available link bandwidth is still lower than the last bandwidth requirement of the call, then the call can be accepted in the link by compressing the bandwidth of all in-service calls (of all service-classes) together with its last bandwidth requirement. In this multirate loss system, we study the effect of the bandwidth reservation (BR) policy on Call Blocking Probabilities (CBP) and link utilization. The BR policy achieves CBP equalization among calls of different service-classes, or guarantees a certain quality of service for each service-class. The proposed single/multi-retry loss models under the BR policy do not have a product form solution, and therefore we propose approximate recursive formulas for the efficient calculation of CBP and link utilization. Simulation results validate the results obtained by the analytical models.**

Keywords-Poisson process, elastic/adaptive traffic, call blocking, reservation, recurrent formula.

I. INTRODUCTION

Multirate loss models based on recursive formulas provide an efficient way for the call-level QoS assessment in modern communication networks which accommodate elastic and adaptive traffic. In-service calls whose bandwidth can tolerate compression while at the same time their service time increases (so that the product *service time* by *bandwidth* is constant) compose elastic traffic. Adaptive traffic is a variation of elastic traffic in the sense that in-service adaptive calls tolerate bandwidth compression without altering their service time. The call-level analysis of a single link that behaves as a loss system and accommodates elastic and adaptive calls of different service-classes is based on the classical Erlang Multirate Loss Model (EMLM) ([1]-[2]).

In the EMLM, calls arrive in the link according to a Poisson process (i.e., an infinite number of traffic sources is assumed) and compete for the available bandwidth under the Complete Sharing (CS) policy. According to the CS policy, new calls are blocked and lost only if their required bandwidth is higher than the available bandwidth of the link. Accepted calls cannot compress their assigned bandwidth and remain in the link for an arbitrarily distributed service time [1]. The calculation of the steady-state probabilities in the EMLM is based on a formula that has a Product Form Solution (PFS). The latter leads to an accurate calculation of Call Blocking Probabilities (CBP) via the well-known Kaufman-Roberts recursive formula [1], [2]. The existence of this recursive formula has led to numerous extensions of the EMLM in wired (e.g., [3]-[7]), wireless (e.g., [8]-[11]) and optical networks (e.g., [12]-[15]). In [16], an extension of the EMLM is proposed, whereby blocked calls can immediately retry one or more times (Single- and Multi-Retry Loss Model, SRM and MRM, respectively) to be connected in the link by requesting less bandwidth units (b.u.). A retry call is blocked and lost if its last bandwidth requirement is still higher than the available bandwidth of the link. In [17], an extension of [16] is considered, whereby a single link accommodates elastic and adaptive traffic with single/multi retrials. We name the models of [17], Elastic-Adaptive Single-Retry Loss Model (EA-SRM) and Elastic-Adaptive Multi-Retry Loss Model (EA-MRM). Contrary to [16], if the available link bandwidth is less than the last bandwidth requirement of a retry call, the system compresses this bandwidth down to a minimum proportion of the last bandwidth requirement, together with the bandwidth of all in-service calls of all service-classes. If the resulting bandwidth requirement is not higher than the available link bandwidth, the retry call is accepted; otherwise is blocked and lost. When a call, whose bandwidth is compressed, departs from the system, then the remaining in-service calls expand their bandwidth. Due to retrials/compression, the EA-SRM and EA-MRM do not have a PFS. However, in [17], approximate recursive formulas are proposed for the calculation of the link occupancy distribution and CBP. In [18], elastic/adaptive calls have several bandwidth requirements and request for bandwidth, upon their arrival, according to the occupied link bandwidth (i.e., calls do not retry).

 ISBN: 978-1-61208-292-9

In this paper, we study the effect of the Bandwidth Reservation (BR) policy in the EA-SRM and EA-MRM. The BR policy is used in order to achieve CBP equalization among different service-classes, or guarantee a certain QoS for each service-class. Although the proposed models do not have a PFS, we propose approximate but recursive formulas for the calculation of the link occupancy distribution, and consequently, CBP and link utilization. Simulation results validate the proposed models and show very good accuracy.

This paper is organized as follows. In Section II, we review the EA-SRM and the EA-MRM. In Section III, we present the proposed models under the BR policy and provide formulas for the approximate calculation of the link occupancy distribution, CBP and link utilization. In Section IV, we present analytical and simulation results in order to evaluate the models' accuracy. We conclude in Section V.

II. REVIEW OF THE EA-SRM AND EA-MRM

A. Review of the EA-SRM

Consider a link of capacity C b.u. that accommodates K service-classes. Let K_e and K_a be the set of elastic and adaptive service-classes (K_e+K_a=K), respectively. Let also $T > C$ be the limit (in b.u.) that determines the maximum permitted bandwidth compression among calls. Service-class k calls (k = 1,…, K) follow a Poisson process with rate λ_k, request b_k b.u. (peak-bandwidth requirement) and have an exponentially distributed service time with mean μ_k^{-1}.

Let j be the occupied link bandwidth, j=0,1,…,T, when a service-class k call arrives in the link. Now, we consider the following cases: a) If $j+b_k \le C$, the call is accepted in the link with b_k b.u. b) If $j+b_k > C$, then the call is blocked with b_k and retries immediately to be connected in the link with $b_{kr} < b_k$. Now if: b1) $j + b_{kr} \le C$ the retry call is accepted in the system with b_{kr} and $\mu_{kr}^{-1} > \mu_k^{-1}$, so that $b_{kr}\mu_{kr}^{-1} = b_k\mu_k^{-1}$, b2) $j + b_{kr} > T$ the retry call is blocked and lost and b3) $C < j + b_{kr} \le T$ the retry call is accepted in the system by compressing its bandwidth requirement b_{kr} together with the bandwidth of all in-service calls of all service-classes. In that case, the compressed bandwidth of the retry call becomes $b_{kr}^{'} = rb_{kr} = \frac{C}{j+b_{kr}} b_{kr}$ where r is the compression factor, common to all service-classes. Similarly, all in-service calls, which have been accepted in the link with b_k (or b_{kr}), compress their bandwidth to $b_k^{'} = rb_k$ (or $b_{kr}^{'} = rb_{kr}$) for k = 1,…,K. After the compression of all calls the link state is j = C. The minimum value that the compression factor can take is given by $r_{\min} = C/T$.

When a service-class k call, with bandwidth $b_k^{'}$ (or $b_{kr}^{'}$), departs from the system, the remaining in-service calls of each service-class i (i=1,…,K), expand their bandwidth in proportion to their initially assigned bandwidth b_i (or b_{ir}). After bandwidth compression/expansion, all elastic service-class k calls (k =1,…,K_e) increase/decrease their service time so that the product *service time* by *bandwidth* remains constant. Adaptive service-class calls do not alter their service time.

The existence of retrials and the bandwidth compression mechanism destroys reversibility in the model and therefore no PFS exists. However, in [17] an approximate recursive formula is proposed for the calculation of the un-normalized values of the link occupancy distribution, $G(j)$:

$$G(j)=\left\langle \begin{array}{c} 1 \; for \; j=0 \\ \frac{1}{j}\left[\sum_{k\in K_u} a_k b_k \gamma_k(j) G(j-b_k) + \sum_{k\in K_u} a_{kr} b_{kr} \gamma_{kr}(j) G(j-b_{kr})\right] + \\ \frac{1}{min(C,j)}\left[\sum_{k\in K_e} a_k b_k \gamma_k(j) G(j-b_k) + \sum_{k\in K_e} a_{kr} b_{kr} \gamma_{kr}(j) G(j-b_{kr})\right] for \; j=1,\ldots,T \\ 0 \; otherwise \end{array} \right\rangle \quad (1)$$

where: $\alpha_k=\lambda_k \mu_k^{-1}$ is the offered traffic-load (in erl) of service-class k calls, $\alpha_{kr}=\lambda_k \mu_{kr}^{-1}$, $\gamma_k(j)=\begin{cases} 1 \; for \; 1\le j\le C \; and \; b_{kr}>0 \\ 1 \; for \; 1\le j\le T \; and \; b_{kr}=0 \\ 0 \; otherwise \end{cases}$ and $\gamma_{kr}(j)=\begin{cases} 1 \; for \; C-b_k+b_{kr} < j \le T \\ 0 \; otherwise \end{cases}$.

The proof of (1) is based on: 1) the application of local balance between adjacent states, which exists only in PFS models, 2) an approximation, expressed by $\gamma_{kr}(j)$ in (1), which assumes that the occupied link bandwidth from retry calls of service-class k is negligible when $j \le C-(b_k-b_{kr})$ and 3) an approximation that refers only to those service-class k calls whose $b_{kr} > 0$; it is expressed by $\gamma_k(j)$ in (1) and assumes that the occupied link bandwidth from service-class k calls accepted in the system with b_k b.u. is negligible when $j > C$.

Having determined $G(j)$'s we can calculate CBP and link utilization. The final CBP of a retry service-class k call, B_{kr}, is given by:

$$B_{kr} = \sum_{j=T-b_{kr}+1}^{T} G^{-1} G(j) \quad (2)$$

where $G=\sum_{j=0}^{T} G(j)$ is the normalization constant.

The link utilization, U, is calculated according to the formula:

$$U = \sum_{j=1}^{C} jG^{-1}G(j) + \sum_{j=C+1}^{T} CG^{-1}G(j) \quad (3)$$

B. Review of the EA-MRM

In the Elastic-Adaptive Multi-Retry loss Model (EA-MRM), a service-class k call that is not accepted in the system with its peak-bandwidth requirement, b_k, may have many retry parameters $(b_{kr_l}, \mu_{kr_l}^{-1})$ for l=1,…,$s(k)$, with

$b_{kr_{s(k)}} < \ldots < b_k$ and $\mu_{kr_{s(k)}}^{-1} > \ldots > \mu_k^{-1}$. Similar to the EA-SRM, the EA-MRM does not have a PFS and therefore the calculation of $G(j)$'s is based on an approximate but recursive formula:

$$G(j)=\left\langle \begin{array}{c} 1 \; for \; j=0 \\ \frac{1}{j}\left[\sum_{k\in K_a} a_k b_k \gamma_k(j) G(j-b_k)+\sum_{k\in K_a}\sum_{s=1}^{s(k)} a_{kr_s} b_{kr_s} \gamma_{kr_s}(j) G(j-b_{kr_s})\right]+ \\ \frac{1}{min(C,j)}\left[\sum_{k\in K_e} a_k b_k \gamma_k(j) G(j-b_k)+\sum_{k\in K_e}\sum_{s=1}^{s(k)} a_{kr_s} b_{kr_s} \gamma_{kr_s}(j) G(j-b_{kr_s})\right] for \; j=1,\ldots,T \\ 0 \; otherwise \end{array} \right\rangle \quad (4)$$

where: $\alpha_{kr}=\lambda_k \mu_{kr}^{-1}$ and $\gamma_k(j)=\begin{cases} 1 \;\; for \;\; 1\le j\le C \;\; and \;\; b_{kr_s}>0 \\ 1 \;\; for \;\; 1\le j\le T \;\; and \;\; b_{kr_s}=0 \\ 0 \;\; otherwise \end{cases}$

$$\gamma_{kr_s}(j)=\begin{cases} 1 \;\; for \;\; C-b_{kr_{s-1}}+b_{kr_s} < j \le C \;\; and \; s\ne s(k) \\ 1 \;\; for \;\; C-b_{kr_{s-1}}+b_{kr_s} < j \le T \;\; and \; s=s(k) \\ 0 \;\; otherwise \end{cases}.$$

If only elastic service-classes are accommodated by the link, then (4) takes the form [19]:

$$G(j)=\left\langle \begin{array}{c} 1 \; for \; j=0 \\ \frac{1}{min(C,j)}\left[\sum_{k\in K_e} a_k b_k \gamma_k(j) G(j-b_k)+\sum_{k\in K_e}\sum_{s=1}^{s(k)} a_{kr_s} b_{kr_s} \gamma_{kr_s}(j) G(j-b_{kr_s})\right] for \; j=1,\ldots,T \\ 0 \; otherwise \end{array} \right\rangle \quad (5)$$

If the link accommodates elastic and adaptive service-classes whose blocked calls are not allowed to retry, then (4) takes the form [20]:

$$G(j)=\begin{cases} 1 & \text{for } j=0 \\ \frac{1}{min(j,C)}\sum_{k\in K_e} a_k b_k G(j-b_k)+\frac{1}{j}\sum_{k\in K_a} a_k b_k G(j-b_k) & \text{for } j=1,\ldots,T \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

where $\alpha_k = \lambda_k \mu_k^{-1}$ is the offered traffic-load (in erl) of service-class k calls.

If calls of all service-classes are not allowed to compress their bandwidth during their service time, then the MRM results and (4) takes the form [16]:

$$G(j)=\left\langle \begin{array}{c} 1 \; for \; j=0 \\ \frac{1}{j}\left[\sum_{k\in K} a_k b_k G(j-b_k)+\sum_{k\in K}\sum_{s=1}^{s(k)} a_{kr_s} b_{kr_s} \gamma_{kr_s}(j) G(j-b_{kr_s})\right] for \; j=1,\ldots,C \\ 0 \; otherwise \end{array} \right\rangle \quad (7)$$

where: $\alpha_{kr}=\lambda_k \mu_{kr}^{-1}$ and $\gamma_{kr_s}(j)=\begin{cases} 1 \;\; for \;\; C-b_{kr_{s-1}}+b_{kr_s} < j \le C \\ 0 \;\; otherwise \end{cases}$.

The CBP of a retry service-class k call with its last bandwidth requirement, $B_{kr_{s(k)}}$, is given by:

$$B_{kr_{s(k)}} = \sum_{j=T-b_{kr_{s(k)}}+1}^{T} G^{-1} G(j) \quad (8)$$

The calculation of the link utilization in the EA-MRM is based on (3) where the values of $G(j)$'s are determined by (4).

III. THE PROPOSED EA-SRM & EA-MRM UNDER THE BR POLICY

The application of the BR policy in the EA-SRM and EA-MRM follows the analysis of Roberts in [21], who proposed an approximate but recursive formula for the calculation of $G(j)$'s in the EMLM under the BR policy.

The calculation of the un-normalized values of $G(j)$'s in the EA-SRM under the BR policy (EA-SRM/BR) is based on the following recursive formula:

$$G(j)=\left\langle \begin{array}{l} 1 \; for \; j=0 \\ \frac{1}{j}\sum_{k\in K_a} a_k D_k(j-b_k)\gamma_k(j)G(j-b_k)+ \\ \frac{1}{j}\sum_{k\in K_a} a_{kr} D_{kr}(j-b_{kr})\gamma_{kr}(j)G(j-b_{kr})+ \\ \frac{1}{min(C,j)}\sum_{k\in K_e} a_k D_k(j-b_k)\gamma_k(j)G(j-b_k)+ \\ \frac{1}{min(C,j)}\sum_{k\in K_e} a_{kr} D_{kr}(j-b_{kr})\gamma_{kr}(j)G(j-b_{kr}) \; for \; j=1,\ldots,T \\ 0 \; otherwise \end{array} \right\rangle \quad (9)$$

where:

$$D_k(j-b_k)=\left\langle \begin{array}{ll} b_k & for \;\; j\le T-t(k) \\ 0 & for \;\; j>T-t(k) \end{array} \right\rangle \quad , \quad D_{kr}(j-b_{kr})=\left\langle \begin{array}{ll} b_{kr} & for \;\; j\le T-t(k) \\ 0 & for \;\; j>T-t(k) \end{array} \right\rangle$$

and $t(k)$ is the reserved bandwidth (BR parameter) in favor of calls other than service-class k calls.

The calculation of the un-normalized values of $G(j)$'s in the EA-MRM under the BR policy (EA-MRM/BR) is based on the following recursive formula:

$$G(j)=\left\langle \begin{array}{l} 1 \; for \; j=0 \\ \frac{1}{j}\sum_{k\in K_a} a_k D_k(j-b_k)\gamma_k(j)G(j-b_k)+ \\ \frac{1}{j}\sum_{k\in K_a}\sum_{s=1}^{s(k)} a_{kr_s} D_{kr_s}(j-b_{kr_s})\gamma_{kr_s}(j)G(j-b_{kr_s})+ \\ \frac{1}{min(C,j)}\sum_{k\in K_e} a_k D_k(j-b_k)\gamma_k(j)G(j-b_k)+ \\ \frac{1}{min(C,j)}\sum_{k\in K_e}\sum_{s=1}^{s(k)} a_{kr_s} D_{kr_s}(j-b_{kr_s})\gamma_{kr_s}(j)G(j-b_{kr_s}) \; for \; j=1,\ldots,T \\ 0 \; otherwise \end{array} \right\rangle \quad (10)$$

where:

$$D_k(j-b_k)=\left\langle \begin{array}{ll} b_k & for \;\; j\le T-t(k) \\ 0 & for \;\; j>T-t(k) \end{array} \right\rangle, \; D_{kr_s}(j-b_{kr_s})=\left\langle \begin{array}{ll} b_{kr_s} & for \;\; j\le T-t(k) \\ 0 & for \;\; j>T-t(k) \end{array} \right\rangle.$$

The recursive formulas (9), (10) are based on the assumption that the population of service-class k calls is negligible in states $j>T-t(k)$. This assumption is incorporated in (9), (10) by the variables $D_k(j-b_k)$, $D_{kr}(j-b_{kr})$ and

$D_{kr_s}(j-b_{kr_s})$. The BR policy is used to attain CBP equalization among calls of different service-classes that share a link by a proper selection of the BR parameters. If, for example, CBP equalization is required between two service-classes whose calls require b_1=1 and b_2=5 b.u., respectively, then $t(1)$ = 4 b.u and $t(2)$ = 0 b.u. so that $b_1 + t(1) = b_2 + t(2)$. Note that $t(1)$ = 4 b.u means that 4 b.u. are reserved to benefit calls of the 2nd service-class.

If only elastic service-classes are accommodated by the link, then (10) takes the form:

$$G(j)=\left\langle \begin{array}{c} 1 \; for \; j=0 \\ \frac{1}{min(C,j)}\sum_{k\in K_e} a_k D_k(j-b_k)\gamma_k(j)G(j-b_k)+ \\ \frac{1}{min(C,j)}\sum_{k\in K_e}\sum_{s=1}^{s(k)} a_{kr_s} D_{kr_s}(j-b_{kr_s})\gamma_{kr_s}(j)G(j-b_{kr_s}) \; for \; j=1,\ldots,T \\ 0 \; otherwise \end{array} \right\rangle \quad (11)$$

If the link accommodates elastic and adaptive service-classes whose blocked calls are not allowed to retry, then (10) takes the form [22]:

$$G(j)=\left\langle \begin{array}{c} 1 \; for \; j=0 \\ \frac{1}{j}\sum_{k\in K_a} a_k D_k(j-b_k)G(j-b_k)+ \\ \frac{1}{min(C,j)}\sum_{k\in K_e} a_k D_k(j-b_k)G(j-b_k) \; for \; j=1,\ldots,T \\ 0 \; otherwise \end{array} \right\rangle \quad (12)$$

If calls of all service-classes may retry but are not allowed to compress their bandwidth during their service time, then the MRM under the BR policy results (MRM/BR) and (10) takes the form [23]:

$$G(j)=\left\langle \begin{array}{c} 1 \; for \; j=0 \\ \frac{1}{j}\sum_{k\in K} a_k D_k(j-b_k)G(j-b_k)+ \\ \frac{1}{j}\sum_{k\in K}\sum_{s=1}^{s(k)} a_{kr_s} D_{kr_s}(j-b_{kr_s})\gamma_{kr_s}(j)G(j-b_{kr_s}) \; for \; j=1,\ldots,C \\ 0 \; otherwise \end{array} \right\rangle \quad (13)$$

In the EA-SRM/BR, the CBP of a retry service-class k call with its last bandwidth requirement, B_{kr}, is given by:

$$B_{kr} = \sum_{j=T-b_{kr}-t(k)+1}^{T} G^{-1}G(j) \quad (14)$$

In the EA-MRM/BR, the CBP of a retry service-class k call with its last bandwidth requirement, $B_{kr_{s(k)}}$, is given by:

$$B_{kr_{s(k)}} = \sum_{j=T-b_{kr_{s(k)}}-t(k)+1}^{T} G^{-1}G(j) \quad (15)$$

The calculation of the link utilization in the EA-SRM/BR and EA-MRM/BR is based on (3) where the values of $G(j)$'s are determined by (9), (10), respectively.

IV. APPLICATION EXAMPLE - EVALUATION

We present an application example in order to compare the analytical CBP and link utilization results of the EA-MRM/BR with those obtained by simulation. To show the necessity of the proposed model we also present the analytical results of the MRM, MRM/BR and EA-MRM. Simulation results are mean values of 7 runs. In all figures of this section we present only mean values, since the reliability ranges of the measurements (assuming 95% confidence interval) are very small. The simulation language used is Simscript II.5 [24].

Consider a link of capacity C = 80 b.u. that accommodates Poisson arriving calls from three different service-classes. Calls of the 1st and 2nd service-class are adaptive and are not allowed to retry while calls of the 3rd service-class are elastic and may retry two times. Their bandwidth requirements are: b_1=1 b.u., b_2=2 b.u. and b_3=6 b.u., respectively. The reduced bandwidth of the 3rd service-class calls for two retrials is: $b_{3_{r1}}$=5 b.u. and $b_{3_{r2}}$=4 b.u. To equalize the final CBP of all service-classes we choose the BR parameters $t(1)$=3, $t(2)$=2, $t(3)$=0, since: $b_1 + t(1) = b_2 + t(2) = b_{3_{r2}} + t(3)$. The call holding time is exponentially distributed with mean value: $\mu_1^{-1}=\mu_2^{-1}=\mu_3^{-1}=1$.

The initial values of the offered traffic-load are: α_1=20 erl, α_2=6 erl and α_3=2 erl. For the retrials of the 3rd service-class we assume that: $\alpha_3 b_3 = a_{3_{r1}} b_{3_{r1}} = a_{3_{r2}} b_{3_{r2}}$. In the x-axis of all figures, we keep constant the value of α_3=2 erl, while α_1, α_2 increase in steps of 1.0 and 0.5 erl, respectively. The last values are: α_1=28 erl, α_2=10 erl. Three values of T are examined: a) $T = C$ =80 b.u., where no bandwidth compression takes place and the EA-MRM/BR gives the same CBP and link utilization results with the MRM/BR, b) T =82 b.u. where $r_{min} = C/T$ =80/82 and c) T =84 b.u. where $r_{min} = C/T$ =80/84. In Figs. 1-3, we present the analytical and simulation CBP results of the 1st, 2nd and 3rd service-class (CBP of calls with $b_{3_{r2}}$), respectively, for all values of T. In Fig. 4, we present the corresponding link utilization results. All figures show that the analytical results obtained by the EA-MRM/BR are of absolutely satisfactory accuracy, compared to simulation and that the MRM/BR fails to approximate the behaviour of EA-MRM/BR. This is expected since in the MRM/BR the bandwidth compression/expansion mechanism is not incorporated. Similarly, the results obtained by the MRM and the EA-MRM fail to approximate the behaviour of the EA-MRM/BR since the BR policy is not applied in these models. Furthermore, Figs. 1-3 show that the existence of the bandwidth compression/expansion mechanism in the EA-MRM/BR reduces CBP even for small values of T. This CBP decrease results in the increase of link utilization in the EA-MRM/BR compared to the MRM/BR (Fig. 4).

 ISBN: 978-1-61208-292-9

V. CONCLUSION

We propose multirate loss models for a link that accommodates elastic and adaptive calls, under the bandwidth reservation policy. Calls of all service-classes arrive in the link according to a Poisson process and have an initial peak-bandwidth requirement. If this bandwidth requirement is not available then calls are blocked and may immediately retry to be connected in the system one (EA-SRM/BR) or more times (EA-MRM/BR). If a retry call is blocked with its last bandwidth, it can still be accepted in the system by compressing its last bandwidth together with the bandwidth of all in-service calls of all service-classes. We propose approximate but recursive formulas for the efficient CBP calculation. Simulation CBP and link utilization results verify the corresponding analytical results.

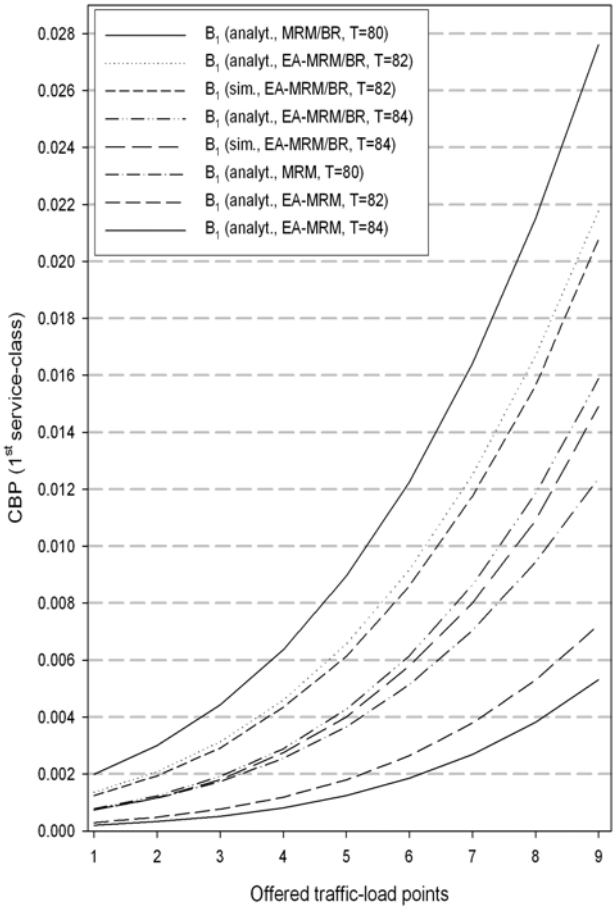


Figure 1. CBP (1st service-class, adaptive).

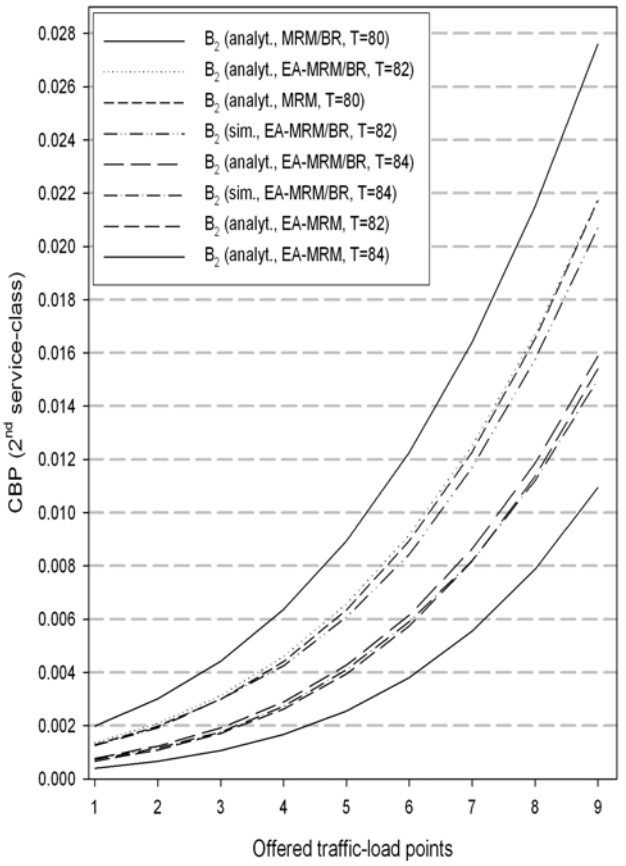


Figure 2. CBP (2nd service-class, adaptive).

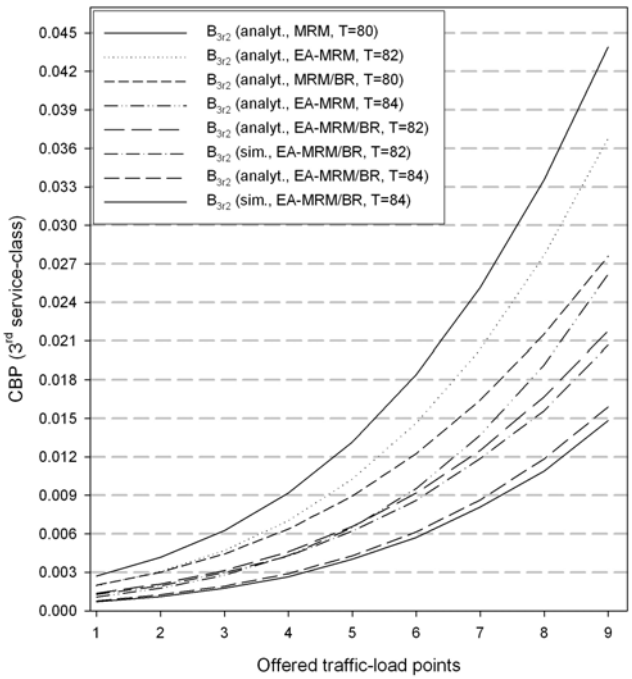


Figure 3. CBP of retry calls with b_{3r2} (3rd service-class, elastic).

 ISBN: 978-1-61208-292-9

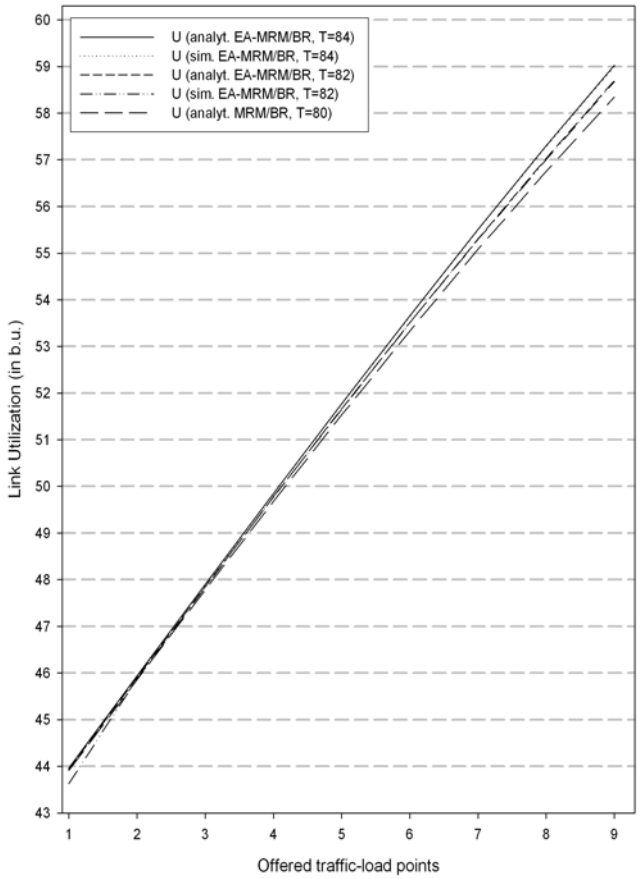


Figure 4. Link utilization (in b.u.).

REFERENCES

[1] J. Kaufman, "Blocking in a shared resource environment", IEEE Trans. Commun. vol. 29, no. 10, pp. 1474-1481, October 1981.

[2] J. Roberts, "A service system with heterogeneous user requirements", in: G. Pujolle (Ed.), Performance of Data Communications systems and their applications, North Holland, Amsterdam, pp.423-431, 1981.

[3] T. Bonald and J. Virtamo, "A Recursive Formula for Multirate Systems with Elastic Traffic", IEEE Communications Letters, vol. 9, no. 8, pp. 753-755, August 2005.

[4] I. Moscholios, M. Logothetis and M. Koukias, "A State-Dependent Multi-Rate Loss Model of Finite Sources with QoS Guarantee for Wireless Networks", Mediterranean Journal of Computers and Networks, vol. 2, no. 1, pp. 10-20, January 2006.

[5] I. Moscholios, M. Logothetis, and M. Koukias, "An ON-OFF Multi-Rate Loss Model of Finite Sources", IEICE Trans. Commun., vol. E90-B, no. 7, pp.1608-1619, July 2007.

[6] Q. Huang, King-Tim Ko and V. Iversen, "Approximation of loss calculation for hierarchical networks with multiservice overflows", IEEE Trans. Commun., Vol. 56, Issue 3, pp. 466-473, March 2008.

[7] I. Moscholios and M. Logothetis, "The Erlang multirate loss model with Batched Poisson arrival processes under the bandwidth reservation policy", Computer Communications, Vol. 33, Supplement 1, pp. S167-S179, Nov. 2010.

[8] D. Staehle and A. Mäder, "An Analytic Approximation of the Uplink Capacity in a UMTS Network with Heterogeneous Traffic", Proc. 18th International Teletraffic Congress, Berlin, pp. 81-90, Sept. 2003.

[9] V. Iversen, V. Benetis, N. Ha, and S. Stepanov, "Evaluation of Multi-service CDMA Networks with Soft Blocking", Proc. International Teletraffic Congress Specialist Seminar, Antwerp, Belgium, pp. 223-227, August/September 2004.

[10] V. Vassilakis, G. Kallos, I. Moscholios and M. Logothetis, "On the Handoff- Call Blocking Probability Calculation in W-CDMA Cellular Networks", Proc. of 4th Advanced Int. Conf. on Telecommunications, AICT 2008, Athens, Greece, 8-13 June 2008.

[11] M. Glabowski, M. Stasiak, A. Wisniewski, and P. Zwierzykowski, "Blocking Probability Calculation for Cellular Systems with WCDMA Radio Interface Servicing PCT1 and PCT2 Multirate Traffic", IEICE Trans. Commun., vol.E92-B, pp.1156-1165, April 2009.

[12] K. Kuppuswamy, D. Lee, "An analytic approach to efficiently computing call blocking probabilities for multiclass WDM networks", IEEE/ACM Trans. Netw., vol. 17, issue 2, pp. 658-670, April 2009.

[13] J. Vardakas, I. Moscholios, M. Logothetis and V. Stylianakis, "An Analytical Approach for Dynamic Wavelength Allocation in WDM-TDMA PONs Servicing ON-OFF Traffic", IEEE/OSA Journal of Optical Commun. Networking, vol. 3, no. 4, pp. 347-358, April 2011.

[14] J. Vardakas, I. Moscholios, M. Logothetis and V. Stylianakis, "Blocking performance of Multi-rate OCDMA PONs", Proc. of 3rd Int. Conf. on Emerging Network Intelligence, EMERGING 2011, Lisbon, Portugal, 20-25 November 2011.

[15] J. Vardakas, I. Moscholios, M. Logothetis and V. Stylianakis, "On Code reservation in Multi-rate OCDMA Passive Optical Networks", Proc. of IEEE International Symposium on Communication Systems, Networks and Digital Signal Processing – 8th CSNDSP' 2012, Poznan, Poland, 18-20 July 2012.

[16] J. Kaufman, "Blocking with retrials in a completely shared resource environment", Performance Evaluation, vol. 15, issue 2, pp. 99-113, June 1992.

[17] I. Moscholios, V. Vassilakis, J. Vardakas and M. Logothetis, "Call Blocking Probabilities of Elastic and Adaptive Traffic with Retrials", Proc. of 8th Advanced Int. Conf. on Telecommunications, AICT 2012, Stuttgart, Germany, 27 May-1 June 2012.

[18] V. Vassilakis, I. Moscholios and M. Logothetis, "Call-level Performance Modeling of Elastic and Adaptive Service-classes", Proc. of IEEE International Conference on Communications, ICC 2007, Glasgow, U.K., 24-28 June 2007.

[19] I. Moscholios, V. Vassilakis, J. Vardakas and M. Logothetis, "Retry loss models supporting elastic traffic", Advances in Electronics and Telecommunications, Poznan Univ. of Technology, Poland, Vol. 2, No. 3, Sept. 2011, pp. 8-13.

[20] S. Racz, B. Gero and G. Fodor, "Flow Level Performance Analysis of a Multi-service System Supporting Elastic and Adaptive Services", Performance Evaluation, Vol.49, Issues 1-4, pp. 451-469, Sept. 2002.

[21] J. Roberts, "Teletraffic models for the Telecom 1 Integrated Services Network", Proceedings of ITC-10, Mondreal, Canada, 1983.

[22] I. Moscholios, V. Vassilakis, M. Logothetis and J. Vardakas, "Bandwidth Reservation in the Erlang Multirate Loss Model for Elastic and Adaptive Traffic", Proc. of 9th Advanced Int. Conf. on Telecommunications, AICT 2013, Rome, Italy, 23-28 June 2013.

[23] I. Moscholios, M. Logothetis and G. Kokkinakis, "Connection Dependent Threshold Model: A Generalization of the Erlang Multiple Rate Loss Model", Performance Evaluation, vol.48, issues 1-4, pp. 177-200, May 2002.

[24] Simscript II.5, http://www.simscript.com.

 ISBN: 978-1-61208-292-9

A Bandwidth Assignment Method for Downloading Large Files with Time Constraints

Ken Katsumoto, Kazuhiko Kinoshita, and Koso Murakami
Department of Information Networking,
Graduate School of Information Science and Technology,
Osaka University
1-5 Yamadaoka, Suita-shi, Osaka, Japan
Email:{katsumoto.ken,kazuhiko,murakami}@ist.osaka-u.ac.jp

Nariyoshi Yamai
Center for Information Technology and Management,
Okayama University
3-1-1 Tsushima-naka,
Kita-ku, Okayama-shi, Okayama, Japan
Email: yamai@cc.okayama-u.ac.jp

***Abstract*—In recent years, the numbers of requests to download large files via large high-speed computer networks have been increasing rapidly. Typically, these requests are handled in a "best effort" manner, resulting in unpredictable completion times. In this paper, we consider a model where a download request either must be completed by a user-specified deadline or must be rejected if the deadline cannot be satisfied. We propose a dynamic bandwidth assignment method for reducing the call-blocking probability in a bandwidth-guaranteed network. Finally, we present simulations that show its excellent performance.**

Keywords*—file downloading; time constraints; bandwidth assignment.

I. INTRODUCTION

In recent years, various types of data have become available in large quantities via large high-speed computer networks [1]. Users hope to be able to access these data files routinely and rapidly by fast downloading.

There are many studies on file downloading, but most focus on shortening the average download-completion time [2][3][4]. In such studies, it is difficult to predict and/or guarantee download completion times, because they depend strongly on the network conditions [5][6].

To overcome this problem, one study has introduced a model where a download request must either be completed by a user-specified deadline or be rejected if the deadline cannot be satisfied [7][8]. Note that, in this model, it is not necessary to shorten the downloading time below its deadline, and it is preferable to accept requests wherever possible, thereby reducing the number of rejected requests. To handle many requests that will meet their deadline and to reduce the call-blocking probability, it is important to consider the bandwidth assignment for each request and to allow a margin in the network for handling future requests.

In this downloading model, a dynamic bandwidth assignment method called $ChangeRates$ has been proposed [8]. This achieves a reduction in call-blocking probability by considering the minimum bandwidth that will meet the deadline.

To be able to accept additional requests, it is preferable that there be as many ongoing requests with loose deadlines as possible in the network. In this paper, we propose a dynamic bandwidth assignment method that reduces the call-blocking probability by giving a higher priority to those requests that potentially allow wider margins.

The remainder of the paper is structured as follows. Section II presents the method for downloading within a deadline, using an existing bandwidth assignment method. In Section III, we propose a dynamic bandwidth assignment method and evaluate its performance in Section IV. Section V concludes the study.

II. DOWNLOADING FILES WITH TIME CONSTRAINTS

A. Problem Formulation

A download request with time constraint $R_i (i = 1, 2, ...)$ is defined by the tuple [9]:

$$R_i = (s_i, d_i, A_i, F_i, D_i). \quad (1)$$

As suggested by their names, s_i = source node, d_i = destination node, A_i = arrival time of the request, F_i = file size, and D_i = the request's deadline. In this formulation, request i must be completed by $A_i + D_i$. Note that, as time elapses, F_i and D_i will decrease. We therefore describe them as $F_i(t)$ and $D_i(t)$, respectively, where t denotes the current time.

For each request R_i, $MinRate_i(t)$ is defined as the minimum average transfer rate that will meet the request's deadline. $MinRate_i(t)$ can be determined from the file size $F_i(t)$ and deadline $D_i(t)$:

$$MinRate_i(t) = \frac{F_i(t)}{D_i(t)}. \quad (2)$$

In addition, $MaxRate_i(t)$ is defined as the maximum bandwidth that can be assigned to R_i, i.e., the available bandwidth for the path [10]. This is given by the minimum available bandwidth among all links within the path. The available bandwidth for each link will vary according to the bandwidth assignment method. For example, if the assigned bandwidth is fixed, the available bandwidth is just the residual capacity of the link. However, if the assigned bandwidth is adaptive, the available bandwidth will be the link capacity minus $MinRate$ for the existing requests.

 ISBN: 978-1-61208-292-9

Fig. 1 shows an example of the available bandwidth for a path. The link capacities for links A–B, B–C, and C–D are all 100 Mbps. The existing request is assigned 30 Mbps for link A–B and 50 Mbps for link C–D. The assigned bandwidth is fixed. In this case, the available bandwidths for A–B, B–C, and C–D are 70, 100, and 50 Mbps, respectively. As a result, the $MaxRate$ for the path A–D is 50 Mbps, which is the minimum available bandwidth for the links A–B, B–C, and C–D.

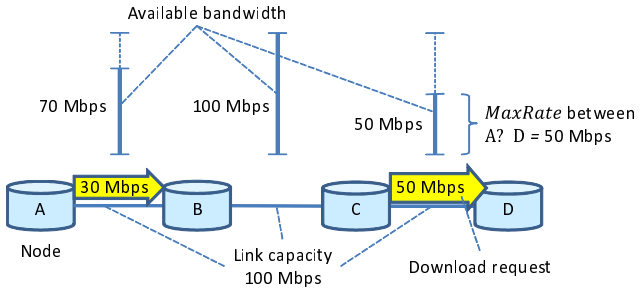


Figure 1. $MaxRate$ for the path

B. Download Model

In this paper, we assume the following network characteristics. The bandwidth assigned to each download connection is guaranteed. There is a database for managing essential information, such as network topology, link capacity, and ongoing requests, for path finding and bandwidth assignment [11]. The access networks are sufficiently fast that they cannot become potential bottlenecks.

For such a network, we consider the following download model. First, a user requests a download within an allowable deadline. For this new download request, a search is made for a feasible route that will satisfy the request. If such a route is not found, the request is rejected. Otherwise, the request's route is decided, and the assignment of an adequate bandwidth is considered. The assignment of appropriate bandwidth for meeting the deadline is an important problem.

C. Existing Methods

We introduce two typical bandwidth assignment methods [9].

- Max: always assigns $MaxRate$ on demand.
- Min: always assigns $MinRate$ on demand.

Max's advantage is that the whole bandwidth is used and almost no bandwidth remains idle, but it tends to lead to resource competition at high network loads and to rejection of future requests.

Conversely, downloading is inefficient and takes more time when using Min. However, much bandwidth will remain idle for future requests, and the method can handle many requests in parallel.

For these fixed bandwidth assignment methods, if no path with at least $MinRate$ bandwidth is available for the request, the request is rejected.

Therefore, we consider an existing method called $ChangeRates$ that changes the assigned bandwidth dynamically [12]. For this method, the bandwidth assigned to request R_i is proportional to $MinRate_i(t)$. Note that this will change during downloading. The specific behavior of this method is as follows.

When a new request occurs, $ChangeRates$ first searches for a path with at least $MinRate$. If found, $MaxRate$ is assigned to the request. Otherwise, a process that reassigns the bandwidths for ongoing requests is invoked, as follows.

For each link C_j, θ_j is computed by:

$$\theta_j = \frac{C_j}{\sum MinRate_i}, \tag{3}$$

where $\sum MinRate_i$ is the sum of the $MinRate$ values for ongoing requests using link C_j. For cases where $\theta_j \geq 1$, a new request can use the link by changing the assigned bandwidths for the ongoing requests. A path that only uses links with $\theta_j \geq 1$ is therefore sought. If such a path for assignment to the new request cannot be found, the request is rejected. Otherwise, for each link C_k on the path, $Rate_{C_k}$, the assigned bandwidth for R_i, is calculated by:

$$Rate_{C_k} = \theta_k \times MinRate_i. \tag{4}$$

R_i's assigned bandwidth $Rate_i$ is the bottleneck bandwidth for the path and is determined by the minimum $Rate_{C_k}$:

$$Rate_i = \min(Rate_{C_k}). \tag{5}$$

$ChangeRates$ can reduce the blocking probability to below that for the fixed bandwidth assignment methods.

III. A Bandwidth Assignment Method

A. Proposed Method

For $ChangeRates$, the assigned bandwidth is simply proportional to $MinRate$. However, to reduce the blocking probability, it would be more effective to handle requests preferentially, thereby producing a greater time margin for the network. A time margin is defined as a download time that could be shortened by assigning a bandwidth greater than $MinRate$. We therefore consider a bandwidth assignment method with the following policies.

- Define an evaluation value for each request. This value indicates a time margin to be obtained by considering the use of bandwidth resources and the use of time.
- Assign bandwidths in descending order of evaluation value.

We define E_i, which is an evaluation value for each request R_i, using the residual file size F_i, the number of hops of the assigned path H_i, the maximum assigned bandwidth $MaxRate_i$, and $MinRate_i$ as follows:

$$E_i = F_i \times H_i \times (1 - \frac{MinRate_i}{MaxRate_i}). \tag{6}$$

A large value for F_i shows that there is room to produce a time margin for R_i. A large H_i indicates that R_i tends to use network resources heavily. Finally, a large

 ISBN: 978-1-61208-292-9

$1 - MinRate/MaxRate$ shows that a greater time margin may be obtained when R_i receives $MaxRate$ compared with $MinRate$. By assigning $MaxRate_i$ to the R_i that has the largest E_i, a greater time margin is obtained and the flexibility in bandwidth assignment is improved. As a result, this method is able to handle more requests and reduces the blocking probability.

We now explain the specific procedures in the proposed method. Suppose that a new request R_{n+1} arrives while requests $R_i (i = 1, ..., n)$ are ongoing. First, the proposed method searches for a feasible path for R_{n+1}. In this process, Dijkstra's algorithm is applied using the inverse of the available bandwidth of a link as the link cost.

Next, the proposed method calculates the evaluation value for all requests, and assigns $MaxRate$ to the request that has the largest evaluation value. The evaluation value is then recalculated for the requests that are yet to be assigned a bandwidth, with the assigned bandwidth also being determined as $MaxRate$. These processes are repeated until the assigned bandwidths for all requests are determined. Furthermore, on the completion of an ongoing request, the same bandwidth assignment procedure is invoked.

Figs. 2–5 show an example of the execution of the proposed algorithm.

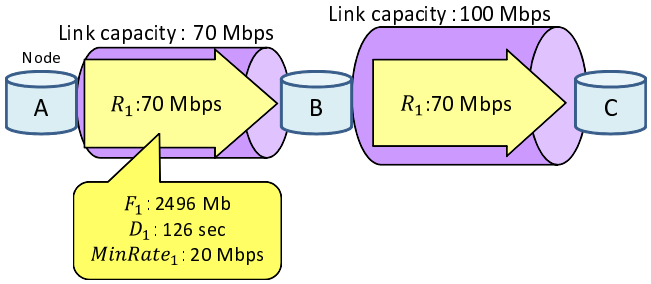


Figure 2. Execution example (1/4)

First, Fig. 2 shows the arrival of a new request R_1 with an F_1 of 2496 Mb and a D_1 of 126 sec. $MinRate_1$ is therefore 20 Mbps. However, in the absence of other requests, R_1 receives 100 Mbps, which is the capacity of the link A–B.

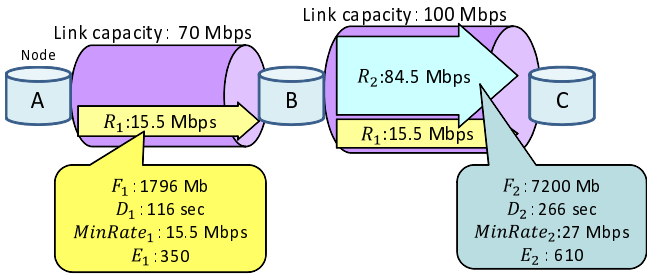


Figure 3. Execution example (2/4)

Next, at 10 sec after A_1, Fig. 3 shows the arrival of R_2, which has an F_2 of 7200 Mb and a D_2 of 266 sec. Because R_1 has consumed 70 Mbps for 10 sec, F_1 and $MinRate_1$ are recalculated as follows:

$$F_1 = 2496 - 70 \times 10 = 1796\text{Mb}. \quad (7)$$

$$MinRate_1 = \frac{1796}{116} \fallingdotseq 15.5\text{Mbps}. \quad (8)$$

Here, E_1 and E_2 are calculated as follows:

$$E_1 = 1796 \times 2 \times (1 - \frac{15.5}{70}) \fallingdotseq 350. \quad (9)$$

$$E_2 = 7200 \times 1 \times (1 - \frac{27}{84.5}) \fallingdotseq 610. \quad (10)$$

Therefore, 84.5 Mbps of $MaxRate_2$ has to be assigned to R_2, with the remaining bandwidth of 15.5 Mbps being assigned to R_1.

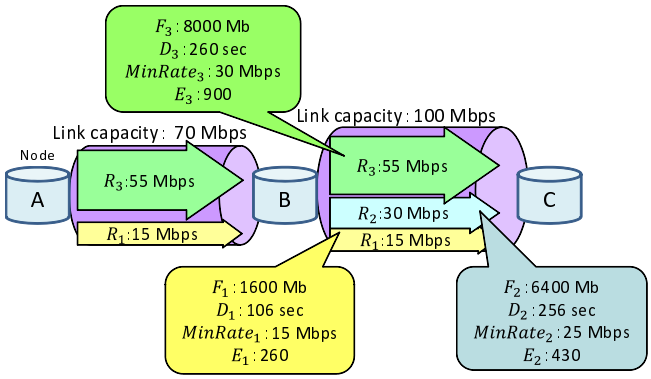


Figure 4. Execution example (3/4)

Next, at 10 sec after A_2, Fig. 4 shows the arrival of R_3, which has an F_3 of 8000 Mb and a D_3 of 260 sec. R_1 and R_2 have consumed 15.5 Mbps and 84.5 Mbps for 10 sec, respectively. F_1 and F_2 are recalculated as follows:

$$F_1 = 1796 - 15.5 \times 10 \fallingdotseq 1600\text{Mb}. \quad (11)$$

$$F_2 = 7200 - 84.5 \times 10 \fallingdotseq 6400\text{Mb}. \quad (12)$$

In the same way, the E_i value for each request is calculated as follows:

$$E_1 = 1600 \times 2 \times (1 - \frac{15}{45}) \fallingdotseq 260. \quad (13)$$

$$E_2 = 6400 \times 1 \times (1 - \frac{25}{55}) \fallingdotseq 430. \quad (14)$$

$$E_3 = 8000 \times 2 \times (1 - \frac{30}{55}) \fallingdotseq 900. \quad (15)$$

At this stage, an assigned bandwidth for R_3 that has the highest evaluation value is considered. For R_3, 60 Mbps (100 Mbps of link capacity minus $MinRate_1$ and $MinRate_2$) can be assigned to the link B–C. However, only 55 Mbps (70 Mbps of link capacity minus $MinRate_1$) can be assigned to the link A–B. Therefore, 55 Mbps is assigned to R_3. Next, E_1 and E_2 are recalculated as follows:

$$E_1 = 1600 \times 2 \times (1 - \frac{15}{15}) = 0. \quad (16)$$

$$E_2 = 6400 \times 1 \times (1 - \frac{25}{30}) \fallingdotseq 130. \quad (17)$$

Therefore, 30 Mbps is assigned to R_2, which has the larger evaluation value, and the remaining bandwidth of 15 Mbps is assigned to R_1.

 ISBN: 978-1-61208-292-9

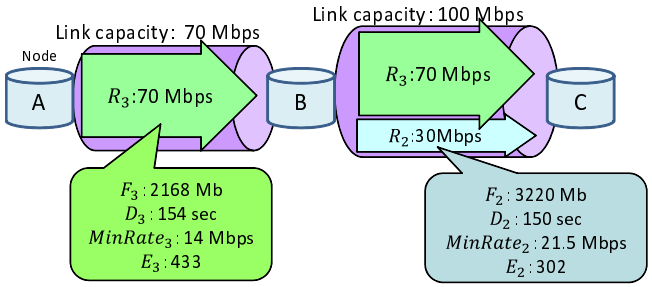


Figure 5. Execution example (4/4)

With no additional requests arriving, R_1 completes at 106 sec after A_3, as shown in Fig. 5. Here, F_2 is $6400-30\times106 = 3220$Mb and F_3 is $8000 - 55 \times 106 = 2168$Mb. E_2 and E_3 are calculated as follows:

$$E_2 = 3220 \times 1 \times (1 - \frac{21.5}{86}) \fallingdotseq 302. \quad (18)$$

$$E_3 = 2168 \times 2 \times (1 - \frac{14}{70}) \fallingdotseq 433. \quad (19)$$

Therefore, 70 Mbps is assigned to R_3, with R_2 receiving the remaining bandwidth of 30 Mbps.

IV. Performance Evaluation

A. Simulation Model

We evaluated the performance of the proposed method by experimental simulation. In the simulation, the network had Waxman's random topology [13], with 100 nodes and about 300 links. Each link in the network had a uniform capacity of 1 Gbps. The download requests were generated via a Poisson arrival process, with an average arrival rate of λ. The source and destination nodes for each request were selected randomly. The blocking probability was used as the performance measure and the existing $ChangeRates$ method was used as a method for comparison.

B. Simulation Results

The proposed method was evaluated for the scenarios described below.

1) Scenario 1: This scenario enabled the basic performance of the proposed method to be evaluated. In this scenario, all requests involved a file size of 5 GB and a deadline of 200 sec. Fig. 6 shows the results, where the proposed method outperforms the existing method for any average arrival rate.

2) Scenario 2: This scenario was used to evaluate the performance in a situation where three requests with equal $MinRate$ arrive, having file sizes of 2.5 GB, 5 GB, and 7.5 GB, and deadlines of 100 sec, 200 sec, and 300 sec, respectively. The total blocking probability for this scenario is shown in Fig. 7. This graph is similar to that for Scenario 1. Furthermore, as shown in Fig. 8, when the $MinRate$ at each request's arrival was the same, we can note that the number of rejected requests is almost the same regardless of the request's file size and deadline.

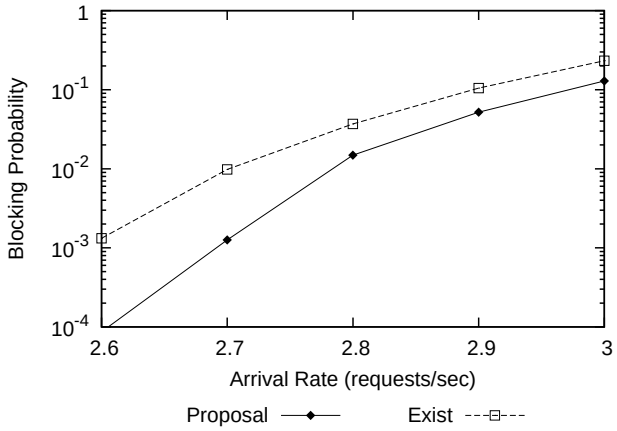


Figure 6. Scenario 1

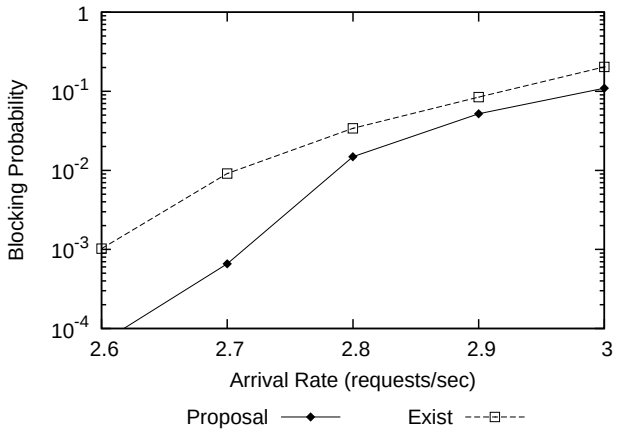


Figure 7. Scenario 2 : total

3) Scenario 3: The final scenario aimed to evaluate the effect of differences in the requests' deadlines. We assume the arrival of three requests that have the same file size of 5 GB but different deadlines of 100 sec, 200 sec, and 300 sec. As shown in Fig. 9, we can note the reduction in the blocking probability for the proposed method in this scenario. Fig. 10 shows that the proposed method has a low blocking probability for requests of 100 sec at an high arrival rate, but the existing method is low for requests of 200 sec and 300 sec. This indicates that the existing method could reduce the blocking probability by handle many requests which would load to the network more lightly, and it has no room for the network than the proposed method. Therefore, it is considered that the proposed method to be more effective for requests of the short deadline.

V. Conclusion

This paper has focused on downloading large files with time constraints. We have proposed a dynamic bandwidth assignment method for reducing the call-blocking probability and have evaluated its performance by experimental simulations. The simulation results show that our proposed method is effective.

In future work, we will enhance the proposed method to enable it to work with distributed management. In addition,

 ISBN: 978-1-61208-292-9

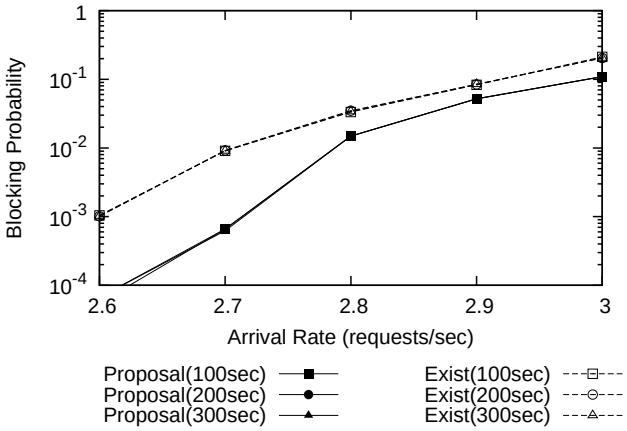


Figure 8. Scenario 2 : each request

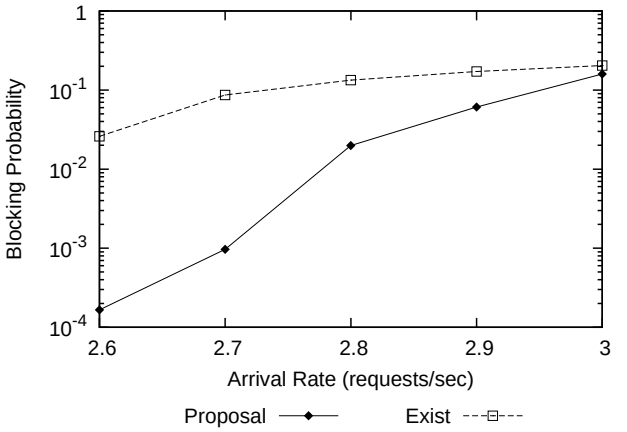


Figure 9. Scenario 3 : total

we will investigate routing methods that are better suited to the proposed bandwidth assignment method.

ACKNOWLEDGMENT

This research was partly supported by the National Institute of Information and Communications Technology (NICT).

REFERENCES

[1] A. S. Tanenbaum, "Computer Networks Fourth Edition," Prentice-Hall, New Jersey, 2003.

[2] H. Okada, T. N. Trung, K. Kinoshita, N. Yamai, and K. Murakami, "A Cooperative Routing Method for Multiple Overlay Networks," Proceedings of the 6th Annual IEEE Consumer Communications and Networking Conference (CCNC 2009), pp. 1–2, Jan. 2009.

[3] L. Toka, M. Dell'Amico, and P. Michiardi, "Data Transfer Scheduling for P2P Storage," IEEE P2P, pp. 132–141, Sept. 2011.

[4] Y. M. Chiu and D. Y. Eun, "Minimizing File Download Time in Stochastic Peer-to-Peer Networks," IEEE/ACM Trans. Networking, vol. 16, no. 2, pp. 253–266, Apr. 2008.

[5] S. Kamei, "Status and Traffic Issues of Peer-to-Peer Technology," Computer Software, vol.22, no.3, pp. 8–18, 2005.

[6] S. Gorinsky and N. Rao, "Dedicated Channels as an Optimal Network Support for Effective Transfer of Massive Data," Proceedings of 25th IEEE International Conference on Computer Communications, pp. 1–5 Apr. 2006.

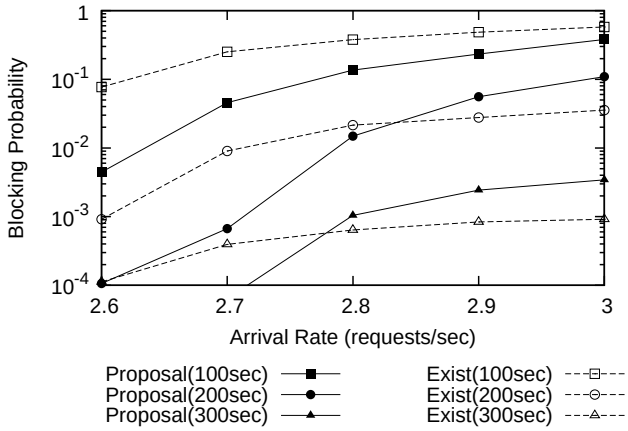


Figure 10. Scenario 3 : each request

[7] B. Chen and P. Primet, "Scheduling deadline-constrained bulk data transfers to minimize network congestion," Proceedings of 7th IEEE International Symposium Cluster Computing and the Grid (CCGRID), pp. 410–417, May 2007.

[8] D. Andrei, M. Batayneh, S. Sarkar, C. Martel, and B. Mukherjee, "Deadline-Driven Bandwidth Allocation with Flexible Transmission Rates in WDM Networks," Proceedings of the IEEE International Conference on Communications 2008 (ICC 2008), pp. 5354–5358, May 2008.

[9] D. Andrei, "Efficient Provisioning of Data-Intensive Applications over Optical Networks," Ph.D. thesis, UC.Davis, 2009.

[10] R. S. Prasad, M. Murray, C. Dovrolis, and K. Claffy, "Bandwidth Estimation: Metrics, Measurement Techniques, and Tools," IEEE Network, Vol. 17, No. 6, pp. 27–35, Nov.–Dec. 2003.

[11] M. Yamazaki, Y. Hirota, K. Kinoshita, H. Tode, and K. Murakami, "A Service Provision Method for Service Platform Unified with Network Control," IEICE technical report, ICM2011-43, pp. 67–72, Jan. 2012.

[12] D. Andrei, M. Tornatore, M. Batayneh, C. U. Martel, and B. Mukherjee, "Provisioning of Deadline-Driven Requests With Flexible Transmission Rates in WDM Mesh Networks," IEEE/ACM Transactions on Networking, Vol. 18, No. 2, pp. 353–366, Apr. 2010.

[13] B. M. Waxman, "Routing of multipoint connections," IEEE Journal of Selected Areas in Communications, Vol. 6, No. 9, pp. 1617–1622, Dec. 1988.

 ISBN: 978-1-61208-292-9

Key Performance Indicators for Cloud Computing SLAs

Stefan Frey, Claudia Lüthje, Christoph Reich
Furtwangen University
Cloud Research Lab
Furtwangen, Germany
{stefan.frey, claudia.luethje, christoph.reich}@hs-furtwangen.de

***Abstract*—Reducing IT costs by using cloud computing is tempting for many companies. As cloud rapidly is gaining momentum as alternative mean of providing IT ressources, the need for regulated service qualities increases. To attract companies to outsource their services to clouds, providers need to offer Service Level Objectives specified in SLAs for their customers. The content of such Service Level Objectives is a key reason for the successful usage of cloud computing and consists of Key Performance Indicators. Due to the dynamic character and complex nature of the cloud environment, creating SLAs for the cloud can be very difficult. This paper proposes selected KPIs for cloud SLAs and describes possible Service Level Objectives, as well as how they should be monitored.**

Keywords*—*Cloud Computing; KPI; SLA; QoS

I. INTRODUCTION

After an initial hype, cloud computing has established itself as adequate means of providing resources on demand. By now cloud computing provides a practical alternative to, locally hosted resources for companies. The main benefits of cloud computing are the cost savings through its "pay-per-use" model, low investment costs and its rapid implementation of innovations. According to a market analysis by the Gartner Group [1], the IT budgets of german companies has been reduced by 2.7% in 2011. The study also shows that companies will increasingly rely on outsourcing their IT to the cloud to save costs in the future. At present, most cloud computing providers only offer generic Service Level Agreements (SLA). Thereby guarantees for QoS characteristics like, bandwidth, data backup, etc. are given on the best-effort principal. Companies require QoS, monitoring and control of the cloud services at any time, as stated in the "Architecture of Managing Clouds" [2], Study Group Report of Cloud Computing [3], and others.

For cloud computing, the quality and reliability of the services become an important aspect, as customers have no direct influence on the services. Therefore Service Level Agreements are fundamental to an effective cloud utilization and especially business customers need them to ensure risks and service qualities are prevented respectively provided in the way they want. For this purpose, the expected service qualities are documented legally binding in contracts between provider and customer. Due to significant variation in consumer needs, SLAs have to be created individually by a negotiation process. The confirmed SLAs serve as a basis for compliance and monitoring of the QoS. Due to the dynamic cloud character, the QoS attributes must be monitored and managed consistently [4].

In order to describe the QoS, metrics and key performance indicators (KPI) are used. These must exactly represent the actual service expectations and requirements, and correspond to both customer as well as provider. In addition to this QoS attributes representation, an SLA includes a general section, in which roles and responsibilities, costs, etc. are listed. The aim of this paper is to propose various possible KPIs for cloud SLAs to facilitate an assist customers in the negotiation and generation of SLAs for cloud services. In addition, a general insight on SLA content and structure as well as monitoring and management is given. After discussing related work in Section II, Section III will give a brief introduction into SLA content und management. Following Section IV presents the Service Level Objectives for cloud computing and the corresponding KPIs. The conclusion is drawn in Section V.

II. RELATED WORK

As the usage of cloud service by companies continues to grow, the need for SLAs is increasing. NIST [5] has pointed out the necessity of SLAs, SLA management, definition of contracts, orientation of monitoring on Service Level Objects (SLOs) and how to enforce them. A basic discussion of SLA management and cloud architectures can be found in Service Level Agreements for Cloud Computing [6], but it is mainly concerned about SLA definitions and negotiations.

In recent years, a significant amount of research has been performed on the standardization and creation of machine-readable formats. There are two major specification for describing SLAs, WSAL [7] and WS-A [8]. The Web Service Agreement Language (WSAL) [7] was developed by IBM with the focus on performance and availability metrics. It has been mainly developed for Web services and the usage in other fields is questionable. It shows significant shortcomings regarding content as it was focused mainly on technical properties. WS-Agreement (WS-A) [8]. was developed by the Open Grid Forum in 2007. The newest update, which is based on the work of the European SLA@SOI project, was done in 2011. Although it has been enhanced within the SLA@SOI project [9], the development is unclear, because the SLA@SOI project developed its own format SLA(T), which is supported by the European IT industry.

Although much research has been done in the direction of SLA formats, the contents of SLAs remain a further field for investigations. The fact that SLAs are always very scenario specific makes it difficult to generalize their contents. KPIs,

 ISBN: 978-1-61208-292-9

as a central component of service level objectives, are increasingly offered in KPI libraries [10]. However, these are mosty of rudimentary content and are not suitable for implementation.

III. SLA

Service Level Agreements (SLAs) specify the promised respectively the expected performance characteristics between service providers and customers. Thereby, all legally relevant information and services are established. The most important part of a SLA is the exact description of the service quality (service level). The following section illustrates the prerequisites, content and structure of Service Level Agreements.

The creation of Service Level Agreements provides certain requirements to customers and providers. Customers need to be able to meet certain requirements in order to successfully define SLAs, which are listed briefly here. A customer must:

- Understand the roles and responsibilities that are regulated by the SLA.
- Be able to describe precisely and specific the service to be controlled by the SLA.
- Know the requirements of the controlled services, and define the matching key figures.
- Specify service levels based on the critical performance characteristics of the service.
- Understand the process and procedures of regulated service.

These requirements are necessary so that the customer is able to put in the correct SLAs values, and to understand implications of his decisions. Furthermore, a SLA should fulfill the following tasks:

- Describe the services accurately.
- Specify the service quality to be provided in detail.
- Describe detailed the key performance indicators, metrics and service levels.
- Breakdown transparently all the costs.

A. SLA Life Cycle

The life cycle of a service level agreement involves several steps for a successful use of SLAs [11]. There are different views on whether the definition phase of the SLA is one of its life cycle or not, since this can also be counted among the preconditions (see [12] and [13]). Figure 1 shows the SLA life cycle. The individual phases are briefly described:

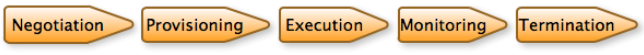


Fig. 1: SLA Life Cycle

The preconditions for this life cycle is the definition of an initial SLA template based on which the negotiation phase is started. In the negotiation phase, the deliverable and service levels and the costs are negotiated with the provider. While in the provisioning phase, the entry into force of the agreement is marked by the signatures of both partners. Here, the provided services are provisioned and the agreements are communicated and fitted into the organizations. During the execution phase the customer uses the service according to his notions. Parallel to this, the monitoring phase the runtime data is checked and assessed against the service levels. If needed, corrective actions are executed and reports and documentation are created for the partners. The final termination phase marks the end of the usage by the customer and initiates the decommission of the service.

B. SLA Content

The structure of service level agreements are generally very scenario specific and can not be easily generalized. However, there are some basic elements that should be present in every SLA. The following remarks are not intended to be used to create an universal pattern for SLAs, but rather give a guideline for most current contents of SLAs.

The contents of a SLA can be divided into the following four categories: (see [14]) *agreement-related elements, service-related elements, document-related elements and management-related elements.*

The agreement-related elements contain the basic rules of the agreement and include, among others, the subject of SLAs, objectives, partners, as well as the scope, entry into force, duration and termination of SLAs. Often these elements are shown in practice in the form of a preamble or introduction. The subject of SLAs introduction here describes the content and context as well as a description and demarcation of the services being controlled by the SLA. The objectives of the SLAs reflect the specific objectives of both parties and serve, among other things, as a basis for future success control.

The service-related elements represent those elements which describe the regulation of a service. These must be specified individually for each service. The content is basically to describe who, when, where, and what services are provided. The description of the service should be generally understandable. The description of the quality of a service is the central role of the SLA. The negotiated quality of service is defined by Key Performance Indicators (KPIs), which is the basis for the Service Level Objectives" (SLOs). These indicators include a label next to the calculation or metric, and a reference area and measurement point. Similarly here, the cost of services to be provided are defined.

Document-related elements include administrative and editorial elements, which play a minor role inside a SLA and are mainly there to improve the handling, understanding and readability. These elements are, e.g., version, the date of last modification, revision history, table of contents, the index or glossary. These elements increase the readability by underpinning the context and explain the background.

The management-related elements include the aspects that have to do with the administration and control of SLAs. These represent a very important section of the contents of a SLA, since both the customer notification and the procedure in case of problems or failures to meet the service levels are regulated.

 ISBN: 978-1-61208-292-9

Furthermore, penalties and compensation in case of damage which may occur due to deviations from service levels are regulated.

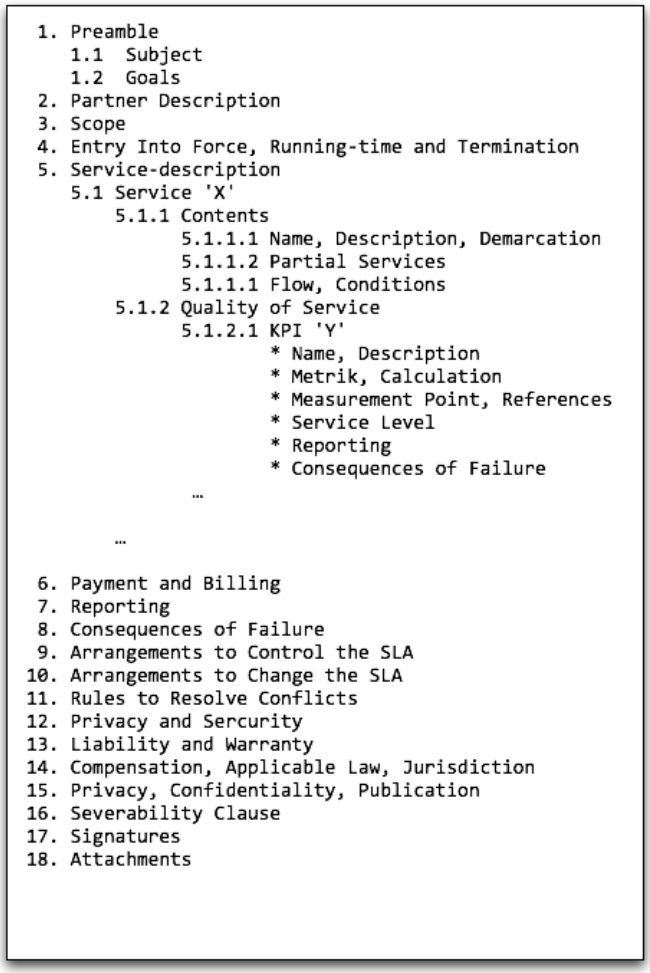


Fig. 2: SLA Structure

Based on the presented elements, an exemplary structure of an SLA can be created. This can be seen in Figure 2 above. Here, it is clear that the service descriptions, or service level objectives are the central aspect of each SLA. These and their contents are described in more detail in the following sections. Likewise, it comes clear that even small SLAs mean large administrative overhead and the creation is a lot of work.

IV. Service Level Objectives

Service Level Objectives (SLOs) are a central element of every service level agreements (SLA), which include the negotiated service qualities (service level) and the corresponding Key Performance Indicators. SLOs contain the specific and measurable properties of the service, such as availability, throughput or response time and often consist of combined or composed attributes. SLOs should thereby have the following characteristics: [15]

- Achievable / attainable
- Repeatable
- Measurable
- Understandable
- Significant
- Controllable
- Affordable
- Mutually acceptable
- Influential

A SLOs should always contain a target value or service level, a metric and corresponding measurement period, as well as the type and location of the measurement. For this purpose, KPIs with associated service level values are stated. The KPIs contain information about the measurement process, place and unit as well. A valid SLO specification might, for instance, look like this: *The IT system should achieve an availability of 98% over the measurement period of one month. The availability represents thereby the ratio of the time in which the service works with a response time of less than 100ms plus the planned downtime to the total service time, measured at the server itself.* From such a description, the actual performance values can be compared with the reference values of the SLOs and the achievement is calculated. Based on this, further measures can carried out to for correction if necessary.

To choose the correct KPIs for a service a wide knowledge of the service and its usage is required. To give an insight into possible cloud-specific KPIs, the most common ones are listed briefly below without going into much detail. The following KPIs provide specifically for cloud computing selected guarantees but also may overlap in part with traditional KPIs, as the essential services requirements do not differ from other general services [16].

A. General Service KPIs

Service Level Agreements must always be tailored to the service to be controlled. Nevertheless, there are some KPIs, which rules can be used in various SLA. These KPIs represent the basic needs of each service to run efficiently. These include, for example the availability, security aspects, service times and helpdesk, as well as monitoring and reporting. These are basic requirements for every purchased service.

1) Basic Services: The basic services include the availability which is defined at the time the service is usable + the maintenance time relative to total time. Deemed usable here is if the system can handle request within a specified response time. Also included are the KPIs Mean Time Between Failure and Mean Time To Repair, which specify the time intervals at which to expect failures and how long it takes to repair them.

2) Security: Security KPIs regulate for example which software version levels shall be used, how long it should take until an update is implemented, as well as the scope and frequency of security audits. Other important KPIs control the encryption of data, the use and timeliness of anti virus software and the isolation and logging.

 ISBN: 978-1-61208-292-9

3) Service and Helpdesk: Service and Helpdesk KPI control including the times at which assistance is provided, which support methods are applied or how many calls are received per week. Similarly, the qualification of the support personnel and the duration is given to problem solving.

4) Monitoring: Monitoring KPIs to define in which values are determined intervals to monitor and how to handle the resulting reports. The arrangements of these KPIs can be reused in the other categories.

B. Network Service KPIs

Particularly for cloud computing, the network has a strong meaning, as all provided resources and services are available through a network. Here, the network has to be considered both as pure transmission medium for other services as well as independent service itself. For the KPIs described here, the entry point of the provider network is usually chosen as measured point, as the guarantees of the provider refer only to this area.

Round Trip Time: Time of a network packet to travel from sender to receiver and back. Specifies how long the transmission of one packet needs within the network limits. Usually measured in milliseconds.

Response Time: Time taken by a request until the arrival of the response at the requesting interface. Here the time for the processing of the request is included as opposed to the pure orbital period of the round trip time. The type of the request and the behavior of the processing has to be concretely defined for this.

Packet Loss: Percentage of lost packets in the total of transmissions. Formula:

$$\frac{Number \quad of \quad lost \quad packets}{Number \quad of \quad total \quad packets \quad * \quad 100} \tag{1}$$

The value of this indicator should kept as low as possible since for example an a loss rate of 5% to 10% significantly affects the quality of VoIP applications [17]

Bandwidth: Gross capacity of the connection. Amount of data which cloud be transmitted within a time unit. Here, not the actual capacity is specified but the rated maximum capacity.

Throughput: Number of transmitted data per time unit. Only the pure transmitted data is taken into account, thus the capacity available to the user is specified. Measured in Mbit/s or / Gbit/s

Network Utilization: Proportion of the throughput to the bandwidth. Here, it can be seen how busy the connection is. Formula:

$$\frac{Throughput}{Bandwidth \quad * \quad 100} \tag{2}$$

Latency: Time interval between submitting a packet and arrival at its destination. Is usually considered together with *Jitter:* The difference in the latency of a packet and the average / minimum / maximum run time. The run time variations are problematic especially in real-time applications, since packages may arrive too late or too early.

C. Cloud Storage KPIs

The term storage can be distinguished within cloud computing in two basic types. First, Storage as a service itself, that is obtained as a memory for preexisting infrastructures. On the other hand storage can be used as part of another service such as a backup or data storage for cloud services.

Response Time: Time interval between sending a request to the storage and the arrival of the response at the output interface. Usually measured in milliseconds.

Throughput: Number of transmitted data per time unit. Here, a specified amount of data is transferred to the storage and measured the needed time from a given point. The size of the data set and package sizes are important factors for the validity of this measure. Furthermore, the network and its utilization must be considered.

Average Read Speed: In contrast to the throughput, the average reading speed usually refers to an individual hard drive. This value indicates how fast data can be read from the hardware. In RAID systems or virtual storage solutions, this figure is expected to interconnected hard drives.

Average Write Speed: Just like the reading speed it refers to the write speed to the hard drive. This value thus indicates how quickly data can be written from a source to the hardware.

Random Input / Outputs per second (IOPS): Number of possible random input / output operations per second for different block sizes. The higher the IOPS value, the faster the disk. This value is also important to measure how many concurrent accesses can be handled by the system.

Sequential Input / Outputs per second (IOPS): Number of possible sequential input / output operations per second for different block sizes.

Free Disk Space Usable free capacity in % of the total capacity or remaining free space in MB, GB, or TB. This indicator can be very useful since thus it can be defined how much memory must always be at minimum available on the system.

Provisioning Type Type of provisioning where at "thin provisioning" the client gets the storage not permanently assigned but it is dynamically allocated at runtime. In contrast, the thick-provisioned storage is allocated to the customer immediately.

Average Provisioning Time Time, the provider needs to provide a defined amount of data volume growth.

D. Backup and Restore KPIs

Backup and Restore KPIs refer to both the storage, i.e., the stored data, as well as services, for example, VMs or SaaS services. Below, important KPIs are presented.

Backup Interval The time interval in which a backup is performed. Here, an exact specification is given to the provider along with the backup type and a description of the scoop.

Backup Type Definition of the backup type, e.g., full backup or incremental backup. Backup types ca relate to individual systems or whole service alliances.

 ISBN: 978-1-61208-292-9

Time To Recovery Specification of the minimum and maximum time from the failure of a storage, to the successful restore from an existing backup.

Backup Media Specifying the media where the backups are stored, such as magnetic tapes. Indication of media breaks to store backups on different media types.

Backup Archive Interval and number of archived backups. Specification of when backups are archived and how long they are kept and how these are to be terminated.

E. Infrastructure as a Service KPIs

Infrastructure as a Service refers not only to the service itself but also to the virtual machines used. For this, additional VM KPIs are specified in this section.

VM CPUs Number and type of CPUs used by the virtual machine. Additionally information about the overbooking of the provided CPU resources shall be given. Here the shared resources are allocated with more capacity than is physically available. Thus, no real physical allocation of resources takes place. Actual performance is dependent on the overall consumption of the system.

CPU Utilization Proportion of CPU resources in use to the total number of resources provided per time unit. Also the CPU queue, which indicates the number of open requests to the CPU should be considered.

VM Memory Amount and type of the provided memory. This may relate to physical memory or virtual memory. Information about the overbooking of allocated memory resources should be stated.

Memory Utilization Proportion of the memory resources used to the total amount of memory made available to the VM.

Minimum Number of VMs Guaranteed number of the provided VMs with the specified specs stated in the previous points.

Migration Time Time that is needed to move a VM from two predefined resources.

Migration Interruption Time Maximum time in which a customer has no access to migration to the resource.

Logging Retention of log data. Specifies how long log data to be stored by the provider and specification of what level to be logged. (e.g., INFO, DEBUG, etc.)

V. Conclusion

The paper pointed out both the general content and specific KPIs for the creation of cloud SLAs. Thus, cloud user have now th basis for the creation of cloud SLAs. Since this is only a general overview of the contents of cloud SLAs the details and designs have to be discussed further. Particularly, in the area of measurement of the KPIs further research is needed.

Acknowledgment

This research is supported by the German Federal Ministry of Education and Research (BMBF) through the research grant number 03FH046PX2.

References

[1] Gartner Group, “Cio-prioritäten und budgets 2011.” [Online]. Available: http://www.cio.de/strategien/analysen/2262709/ [retrirved: june, 2013].

[2] Distributed Management Task Force, “Architecture for managing clouds.” [Online]. Available: http://dmtf.org [retrieved: june, 2013].

[3] ISO/IEC SC 38 Study Group, “Jtc 1/sc 38 study group report on cloud computing,” International Organization for Standardization, Tech. Rep., 2011. [Online]. Available: http://isotc.iso.org [retrirved: june, 2013].

[4] A. Keller and H. Ludwig, “The wsla framework: Specifying and monitoring service level agreements for web services,” Journal of Network and Systems Management, vol. 11, no. 1, pp. 57–81, Mar. 2003.

[5] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, “Nist cloud computing reference architecture,” NIST special publication, vol. 500, p. 292, 2011.

[6] J. Happe, W. Theilmann, A. Edmonds, and K. Kearney, Service Level Agreements for Cloud Computing. Springer-Verlag, 2011, ch. A Reference Architecture for Multi-Level SLA Management, pp. 13–26.

[7] H. Ludwig, A. Keller, A. Dan, R. P. King, and R. Franck, “Web Service Level Agreement (WSLA) Language Specification, v1.0,” Jan. 2003. [Online]. Available: http://www.research.ibm.com/wsla/WSLASpecV1-20030128.pdf [retrirved: may, 2013].

[8] K. T. Kearney, F. Torelli, and C. Kotsokalis, “Sla*: An abstract syntax for service level agreements,” 11th IEEE/ACM International Conference on Grid Computing, pp. 217–224, 2011.

[9] SLA@SOI. SLA@SOI projekt website. http://sla-at-soi.eu/. [retrirved: june, 2013].

[10] MIRROR-42, “Kpi library.” [Online]. Available: http://mirror42.com [retrieved: june, 2013].

[11] W. Sun, Y. Xu, and F. Liu, “The role of xml in service level agreements management,” in Services Systems and Services Management, 2005. Proceedings of ICSSSM ’05. 2005 International Conference on, vol. 2, 2005, pp. 1118–1120.

[12] P. Hasselmeyer, B. Koller, I. Kotsiopoulos, D. Kuo, and M. Parkin, “Negotiating slas with dynamic pricing policies,” Proceedings of the SOC@ Inside07, 2007.

[13] G. R. Gangadharan, G. Frankova, and V. D’Andrea, “Service license life cycle,” in Collaborative Technologies and Systems, 2007. CTS 2007. International Symposium on, 2007, pp. 150–158.

[14] T. G. Berger, Konzeption und Management von Service-Level-Agreements fur IT-Dienstleistungen. TU Darmstadt, 2005.

[15] R. Sturm, W. Morris, and M. Jander, Foundations of Service Level Management, ser. Sams Professionals. Pearson Sams, 2000, iSBN: 978-0-6723-1743-9.

[16] S. Ran, “A model for web services discovery with qos,” SIGecom Exch., vol. 4, no. 1, pp. 1–10, Mar. 2003.

[17] K. C. Mansfield and J. L. Antonakos, Computer Networking from LANs to WANs: Hardware, Software, and Security. Boston: Course Technology, Cengage Learning, 2010, iSBN: 9781743044544.

 ISBN: 978-1-61208-292-9

Performance Improvement of Heterogeneous Wireless Sensor Networks Using a New Clustering Algorithm

Magdy A. Ahmed
Computer and Systems Engineering Department
Faculty of Engineering, Alexandria University
Alexandria, Egypt
magdy@alexu.edu.eg

***Abstract*—This paper proposes and evaluates a new clustering algorithm: Weighted Election Probabilities Clustering Scheme (WEPCS) for Heterogeneous Wireless Sensor Networks (HWSNs). WEPCS is an improvement of the Energy Efficient Heterogeneous Clustered (EEHC) protocol. The modification proposed allows the election of Cluster Heads (CHs) using different weighted probabilities. The WEPCS algorithm aims mainly to improve network stability period and the network throughput. An Experimental evaluation is presented and the results show that the WEPCS achieves longer life time and more throughput than the existing clustering protocols in heterogeneous environments.**

Keywords-Wireless Sensor Network; Heterogeneous; Clustering; Energy Consumption; Network Stability Period.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are an example of the paradigm shift-taking place in wireless network architectures. Recent advances in computing and communication have caused a significant shift in sensor network research.

WSN is composed of a Base Station (BS) and a number of wireless Sensor Nodes (SNs). These SNs are characterized as low-cost and low-power entities and are capable of communication at very short distances, also, they perform limited computation. All SNs, communicate wirelessly, and form a sensor field [1,2]. Typically, BS serves as an access point for the user, or as a gateway to another network.

The main task of the SN is to sense and collect data from a certain region, process it, and transmit it to the BS, where further processing on the collected data can be performed. So, WSN can be used in a wide variety of civilian and military applications, e.g., environmental monitoring, battlefield surveillance, industry process control, and health.

Depending on the application of WSNs, certain routing protocols are required in order to establish the communication among SNs and the BS [3]. WSNs consume their limited energy while collecting data, performing calculations, and routing the received data. Nevertheless, in most applications, each SN is expected to last for a long time. For these reasons, both efficient routing schemes and efficient use of energy are highly important in WSNs.

Different techniques have already been proposed to improve energy consumption rate and network's lifetime, such as: clustering and data aggregation.

Clustering is a key technique used to extend the lifetime of WSN by organizing SNs into clusters. Each cluster has a leader called Cluster Head (CH). Each SN transmits its data to the closest CH to minimize energy consumption. Then the CH manages communication within a cluster, and forwards collected data from its Cluster Members (CMs) to the BS.

In clustered WSNs, CH has a higher burden than its CMs The CH drains its energy much more quickly than the CMs. Rotating the CH's role distributes this higher burden among SNs, thereby preventing CH from dying prematurely [4,5]. Hence, an important design issue in WSNs is to lessen the energy consumption in WSN for sake of the network lifetime.

One of the ways for saving energy is to insert a percentage of SNs equipped with additional energy resources in the sensing field, i.e., making WSN heterogeneous in terms of energy.

Many existing schemes for Heterogeneous Wireless Sensor Networks (HWSNs), such as SEP [6], DEEC [7], and EEHC [8], demonstrate that HWSNs are supposed to survive for a longer time compared to homogeneous WSNs.

This paper proposes and evaluates a new clustering algorithm: Weighted Election Probabilities Clustering Scheme (WEPCS) for HWSNs. It takes advantages from previous developed algorithms and studies the impact of heterogeneity of SNs on the network performance, based on their energy levels. The main issue of our interest is to maximize the lifetime of HWSN and throughput.

The rest of this paper is organized as follows. Section II discusses the related work. Section III presents the proposed algorithm. Section IV provides the experimental results. Section V concludes the paper and discusses the future work.

II. RELATED WORK

Most of the clustering algorithms, e.g., LEACH [9], assume WSNs are homogeneous, where all SNs have the same initial energy. These algorithms perform poorly in heterogeneous environments, where all SNs of WSN are equipped with different amounts of energy. HWSNs are very much useful in real deployments because they are more close to real life situations; so the work presented in this paper emphasizes upon HWSNs where two or more types of SNs are considered [10,11,12,13].

Low-Energy Adaptive Clustering Hierarchy (LEACH) [9] is one of the most simple and effective widely deployed clustering solutions for WSN. In LEACH, each SN is given equal chance to be a CH. The clusters are re-established and new CHs are elected in each "round", so that the load is distributed and balanced among SNs of the network.

Distributed Energy-Efficient Clustering (DEEC) [7] is a cluster-based scheme for two level and multilevel

 ISBN: 978-1-61208-292-9

energy HWSNs. DEEC is based on LEACH. In this scheme, CHs are selected using the probability based on the ratio between the residual energy of each SN and the average energy of the network. Thus, DEEC can prolong the stability period. SNs with high initial and residual energy will have more chances to be CHs than low energy SNs. However, this choice penalizes always advanced SNs, because these SNs will be continuously CHs. In this situation, the advanced SNs die quickly than the others.

Energy Efficient Heterogeneous Clustered (EEHC) [8] is developed for the 3-level heterogeneous networks, which include three types of nodes according to the initial energy, i.e., the super nodes, the advance nodes and the normal nodes. The rotating epoch and election probability is directly correlated with only the initial energy of nodes. EEHC performs poorly when heterogeneity is a result of operation of the sensor network.

III. THE WEIGHTED ELECTION PROBABILITIES CLUSTERING SCHEME (WEPCS)

After studying the operation of LEACH [9], DEEC [7], and EEHC [8], the following facts were noticed:

First, SN nearer to BS than to any CH may send its data to far CH, as shown in Fig. 1. As a result, it will lose more energy compared to the case of sending its data directly to BS, as shown in Fig. 2.

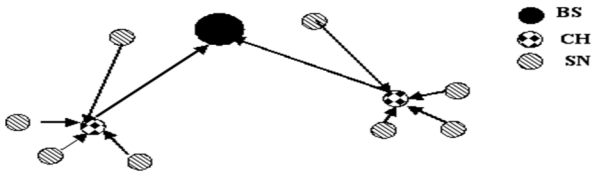


Figure 1. The Network Model for the General Clustering Algorithms.

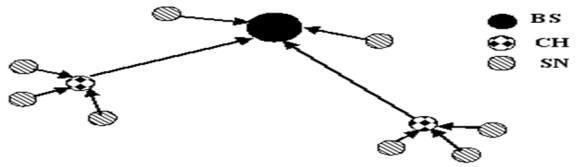


Figure 2. The Network Model for the WEPCS Algorithm.

Second, when no SN elects itself as CH, and at the same time there are some SNs still alive and has enough energy to send data to BS, then SNs usually will turn off to sleep mode. In turn, the packets of these live SNs will not be sent to BS. This great disadvantage influences the transmission reliability in the networks, especially for some important real-time tasks, e.g., fires and volcanoes.

Third, in EEHC, the "CH weighted election probability" equation does not consider the residual energy of the SNs, the residual energy of the network, and the number of live SNs, i.e., EEHC depends only on the initial parameters of the network. In addition, EEHC considers three types of SNs only (normal, advanced, and super) instead of Multi-Level type that can be encountered in HWSN after a significant amount of time of operation.

Thus, in this paper, we will consider the previous notes in the proposed algorithm.

A. Goals of WEPCS

- Improving network stability period in terms of the Death of First SN (FND), by increasing the time until a SN breaks down
- Increasing HWSN lifetime in terms of the Death of Half SNs (HND), by increasing the half-life period of the network
- Increasing total throughput, by increasing the total number of packets that sent to BS.

To achieve these goals, WEPCS includes the following modifications:

BS will act as if it is one of CHs thus,

- Non CH (NCH) is allowed to send its packets directly to BS when it has no CH, i.e., when no SN elects itself as CH and there are some SNs still alive. Hence, in WEPCS, loss of data due to inability to reach BS is avoided. This enhances WSN efficiency.
- NCH is allowed to choose its nearest leader (CH or BS), i.e., if any NCH is nearer to BS than any CHs, it will contact directly to BS. Moreover, accordingly, the power dissipation due to the distance will be decreased, and more communication energy will be saved.

CH selection will depend on three basics:

- The weighted election probability equation, which is used in threshold and epoch calculations, is based on the residual energy of SNs, the actual residual energy of the network, and the number of alive SNs.
- The scheme of WEPCS is implemented along three scenarios for sending the remaining energy information of SN to BS along three different rates: none in implementation-a (Impl-a), every round in implementation-b (Impl-b), and every epoch in implementation-c (Impl-c).

We consider different models of HWSN, which are Two Level, Three-Level, and Multi-Level in terms of the SN initial energy.

B. Phases of the WEPCS Algorithm

The operation of each round of WEPCS is divided into three phases, as shown in Fig.3.

Set-Up Phase: SNs will organize themselves into local clusters, with one SN acts as CH. SNs elect themselves as CHs with respect to their energy levels, autonomously. Then, BS selects CHs based on suggestions of requesting SNs to be CHs, i.e., the proposed algorithm is a combination between distributed and centralized clustering algorithms. Fig. 4 gives an overview of the formal description of the Set-Up phase.

Steady-State Phase: The sensed data packet will be collected from all CMs by its leader (CHs or BS). CHs

 ISBN: 978-1-61208-292-9

perform processing functions on the received data (e.g., data aggregation and compression). Then CHs send the compressed data to BS.

BS has two types of data: one from CHs, and another from SNs that sent directly to BS. BS performs another data aggregation function, which aggregates both types of data.

Maintenance phase: The "*network status*" information, which contains the real number of live SNs and the total remaining energy of the network, will be updated for all SNs.

CMs send their "*remaining energy*" information to their leaders (CH or BS). The leaders aggregate remaining energies and calculate the real number of live SNs in their clusters, and then CHs send this "*energy level*" information to BS.

After that, BS aggregates the real number of live SNs and the total remaining energy of the network. Then, BS broadcasts "*network status*" to all SNs in the network. Finally, SNs receive this information, and update their stored "network status".

This "*network status*" will be used in three different ways, according to the implementation scenarios of WEPCS: Impl-a, Impl-b, or Impl-c.

After this phase, the next round begins, and the algorithm reforms the CH selection process.

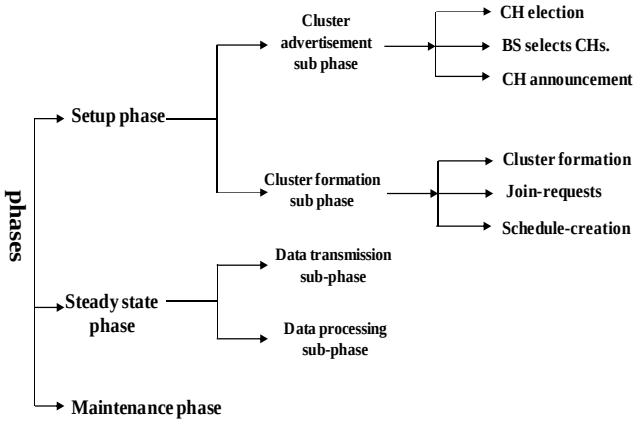


Figure 3. Phases of the Proposed Algorithm

C. Cluster Head Selection for WEPCS

When a new round begins, each SN decides whether to become CH or not. This decision is made by SN choosing a random number between 0 and 1.

SN becomes a CH for the current round, if the number is less than the following threshold [8]:

$$T(s_i) = \begin{cases} \dfrac{P_{s_i}}{1 - P_{s_i} * r \bmod \left(\frac{1}{P_{s_i}}\right)}, & \text{If } s_i \in G \\ 0, & \text{Otherwise} \end{cases} \quad (1)$$

where P_{s_i} is the weighted election probabilities of SN in the current round r, and G is the set of SNs that are eligible to be CHs at round r.

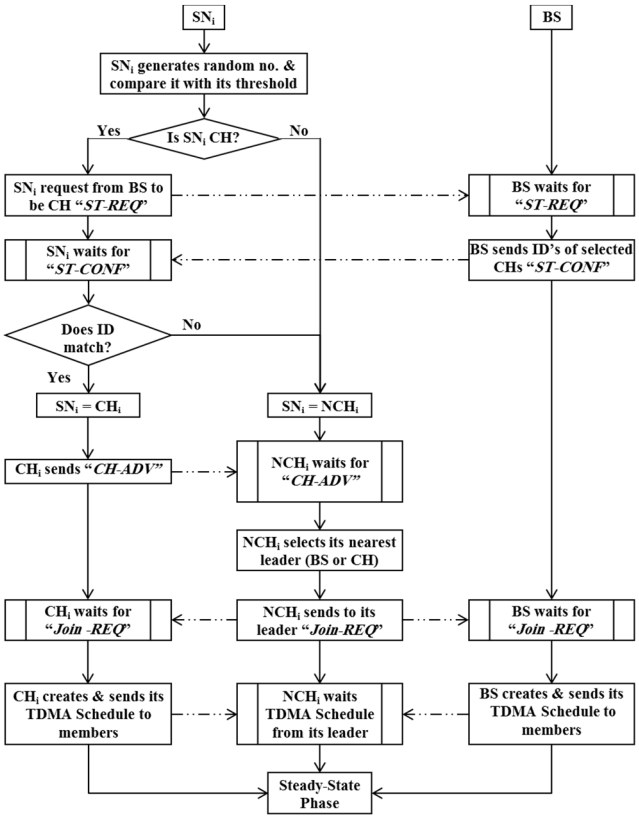


Figure 4. Formal Description of the Set-Up phase

After SN works as CH in current round, it will not belong to the set G, i.e., it will be prevented from being elected again during next rounds until it passes its individual rotating epoch ($m_{Si} = 1/P_{s_i}$). After a new epoch starts, SN will belong again to the set G.

Weighted Election Probabilities: WEPCS makes more control on the threshold. This control is achieved based on the weighted election probability, $\mathbf{P_{s_i}}$. According to the implementation scenarios of WEPCS, $\mathbf{P_{s_i}}$ is computed as follows:

a) Implementation-a of WEPCS (Impl-a)

The weighted probability for Impl-a scenario is:

$$P_{s_i} = \frac{n_{initial} \times P_{opt} \times E_{s_i}(r)}{E_{total-initial}} \quad (2)$$

where P_{opt} is optimal percentage of SNs to become CHs, $E_{s_i}(r)$ is current energy of SN per round, $n_{initial}$ is the total number of SNs at the start of the network operation, and $E_{total-initial}$ is the total initial energy of HWSN.

b) Implementation-b of WEPCS (Impl-b)

The weighted probability for Impl-b scenario is:

$$P_{s_i} = \frac{n(r) \times P_{opt} \times E_{s_i}(r)}{E_{total}(r)} \quad (3)$$

 ISBN: 978-1-61208-292-9

where n(r) is total number of SNs in the network at the start of each round and $E_{total}(r)$ is total energy of HWSN at the start of each round. These two values are updated every round by using network status information.

c) *Implementation-c of WEPCS (Impl-c)*

The weighted probability for Impl-c scenario is:

$$P_{s_i} = \frac{n(m) \times P_{opt} \times E_{s_i}(r)}{E_{total}(m)} \quad (4)$$

where n(m) is total number of SNs at start of each optimal epoch and $E_{total}(m)$ is total energy of HWSN at the start of each optimal epoch. These two values are updated every optimal epoch ($m_{opt}=1/P_{opt}$).

D. Network Model

We have considered the following assumptions:

- All SNs are randomly distributed in a (M * M) square sensing field.
- All SNs and BS are stationary, after deployment.
- All SNs have unique IDs and they are location-unaware.
- BS is located at the center of the square field.
- BS location is known by each SN in the network.
- Type of communication is single hop.
- Communication is symmetric and SN can compute the approximate distance based on the received signal strength.
- The communication environment is contention and error free. Hence, SNs do not have to retransmit any data.

In the work presented in this paper, WEPCS is applied on several types of HWSN, including Two-Level, Three-Level, and Multi-Level in terms of the SN initial energy. Next, the total initial energy of each network level is calculated. This total energy is used in computing P_{s_i} in Eq. (2), (3) and (4) to elect CH at the start of WEPCS within the three scenarios of implementation.

Two-Level HWSN

There are two types of SNs : advanced and normal SNs. Let's assume that E_0 is the initial energy of normal SNs, and m is the fraction of advanced SNs, which own α times more energy than the normal ones.

Thus there are n*m advanced SNs equipped with initial energy of $(1+\alpha)*E_0$, and n*(1-m) normal SNs equipped with initial energy of E_0. The total initial energy of the Two-Level HWSN [6,7,12] is:

$$E_{total} = n*(1-m)*E_0+n* m*(1+ \alpha) *E_0= n* E_0*(1+ \alpha m) \quad (5)$$

Three-Level Network

There are three types of SNs: super, advanced, and normal SNs. Assuming that E_0 is the initial energy of normal SNs, m is the fraction of advanced SNs, which own α times more energy than the normal ones, and m_0 is the fraction of super SNs, which own β times more energy than the normal ones.

Thus there are $n*m*m_0$ super SNs equipped with initial energy of $(1 + \beta)*E_0$, $n*m*(1-m_0)$ advanced SNs equipped with initial energy of $(1 + \alpha)*E_0$, and n*(1 – m) normal SNs equipped with initial energy of E_0. The total initial energy of the Three-Level HWSNs [8,10,11] is :

$$E_{total} = n *m*m_0*(1+ \beta) E_0 + n*m*(1-m_0)*(1+ \alpha) E_0 +n*(1-m)*E_0$$
$$E_{total} = n*E_0*(1+ m*(\alpha -a*m_0+m_0* \beta)) \quad (6)$$

Multi-Level Network

There are many different types of SNs. Let assume the initial energy E_0 is randomly distributed over the close set $[E_0 , E_0*(1 + \alpha_{max})]$, where E_0 is the lower bound and α_{max} determines the value of the maximal energy. Initially, the node s_i is equipped with initial energy of $E_0*(1 + \alpha_i)$, which is α_i times more energy than the lower bound E_0. The total initial energy of Multi-Level HWSNs [7] is:

$$E_{total} = E_0 (1+ \alpha_1) + E_0 (1+ \alpha_2) + ...+ E_0 (1+ \alpha_n)$$
$$E_{total} = \sum_{i=1}^{n} E_0 * (1+ \alpha_i) = E_0 (n + \sum_{i=1}^{n} \alpha_i) \quad (7)$$

E. Energy Model

The work presented in this paper adopts the same energy model proposed in [9,14]. The free space energy model used because SNs are randomly distributed over the sensing field and BS is at the center, as a result, the distance from any SN to the BS or its CH is small. Table 1 describes the energy dissipation in CHs during each phase and Table 2 describes the energy dissipation in NCHs (CMs) during each phase.

TABLE 1. ENERGY DISSIPATION IN CHS

Operation	Energy Dissipated
Set-Up Phase	
When CH sends its status "ST-REQ" request to BS	$L_1 E_{elec}+ L_1 e_{fs} d^2_{to\ BS}$
When CH receives its confirmation "ST-CONF" message from BS	$L_1 E_{elec}$
When CH broadcasts "CH-ADV" message to all SNs	$L_1 E_{elec}+ L_1 e_{fs} d^2_{range}$
When CH receives "Join-REQ" messages from CMs.	$N_c L_1 E_{elec}$
When CH transmits its TDMA schedule to CMs.	$L_1 E_{elec}+ L_1 d^2 e_{fs}$
Steady-State Phase	
When CH receives sensed data packet from its CMs (E_{Rx})	$L_2 E_{elec}$
When CH aggregates the sensed data packet of its CMs (E_{DA})	$L_2 E_{aggr}$
When CH transmits aggregated data to BS (E_{Tx})	$L_2 (E_{elec} + e_{fs} d^2_{to\ BS})$
Maintenance Phase	
When CH receives "remaining energy" information from its CMs	$N_c L_3 E_{elec}$
When CH aggregates this information	$(N_c + 1) L_3 E_{elec}$
When CH transmits this "energy level" information to BS	$L_3 (E_{elec} + e_{fs} d^2_{to\ BS})$
When CH receives the "network status" information from BS	$L_4 E_{elec}$

 ISBN: 978-1-61208-292-9

TABLE 2. ENERGY DISSIPATION IN NCHS

Operation	Energy Dissipated
Set-Up Phase	
When NCH receives "CH-ADV" message from CHs	$L_1 E_{elec}$
When NCH transmits "Join-REQ" message to its leader	$L_1 E_{elec} + L_1 e_{fs} d^2$
When NCH receives TDMA schedule from its leader	$L_1 E_{elec}$
Steady-State Phase	
When NCH (CM) transmits sensed data packet to its leader (E_{Tx})	$L_2 E_{elec} + L_2 e_{fs} d^2_{to\ CH}$
Maintenance Phase	
When NCH transmits "remaining energy" information to its leader	$L_3 (E_{elec} + e_{fs} d^2_{to\ leader})$
When NCH receives the "network status" information from BS	$L_4 . E_{elec}$

where, E_{elec} is the energy dissipated per bit to run the transmitter or the receiver circuit, d is the distance between CM and its leader, d_{toBS} is the distance between CH and BS, d_{range} is the CH radio range distance, N_c is the number of CMs in each cluster, L_1 is the number of bits in each set up message, L_2 is the number of bits in each data message, L_3 is the number of bits of "energy level" information and "remaining energy" information, L_4 is the number of bits of "network status" information, e_{fs} depends on the transmitter amplifier of the free space model, and E_{aggr} is the processing energy cost of a reported bit to BS.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

A. Simulation Environment and settings

The simulation has been done using MATLAB. The parameters used in our simulation are shown in Table 3.

The SN is considered dead when it has energy less than the energy needed for transmitting L_1-bit packets to its leader. In addition, the optimal percentage of SNs that will be CHs P_{opt} is equal to 5% of the total number of SNs in the network as in [9, 14].

B. Simulation Metrics

- *Overall network performance view:* The lifetime of HWSN is defined by three metrics [15]:

TABLE 3. SIMULATION PARAMETERS

Parameter	Value
Square Sensing field.	(100,100)
n: total number of SNs in the network.	Init.: 100
E_{elec}: energy dissipated per bit to run the transmitter or receiver circuit.	50 nJ/bit/ packet
e_{fs}: energy consumed by the amplifier to transmit at a short distance.	10 pJ/bit/m2
E_0: initial energy of normal SN	0.5 J
E_{DA}: data aggregation energy is the processing cost of a bit report to BS.	5 nJ/bit/ report
L_1: number of bits in each set up packet	200 bits
L_2: number of bits in each data packet	4000 bits
L_3: number of bits in each network status packet	200 bits
P_{opt}: optimal probability of SN to become CH.	Init:0.05
BS Location	(50,50)

  - First Node Died (FND), which indicates the period from the start of the network operation and the first dead SN (stability period).
  - Half Nodes Died (HND), which indicates an estimated value for the half-life period of HWSN.
  - Last Node Died (LND), which indicates an estimated value for the overall lifetime of HWSN. This research finds LND when all nodes die-if possible; but this measure is not of interest here.

  In this paper, we limit the discussion of algorithms to the metrics FND and HND.
- *Overall network status*: These metrics reflect the total number of alive SNs per round and the total number of dead SNs per round.
- *Throughput:* This metric reflects the total number of data packets sent over the network to BS per round.
- *Improvements along the metrics*: The improvement of FND, HND, and Throughput will be calculated by:

$$\text{Improvement} = \frac{\text{Value of WEPCS metric} - \text{Value of other algorithm metric}}{\text{Value of other algorithm metric}} \quad (8)$$

C. Simulation Results

This section provides a limited set of results, obtained using simulation. The simulation results compare the performance of WEPCS to the three previously developed algorithms: LEACH (Homogeneous LEACH, and heterogeneous LEACH), DEEC, and EEHC. Homogeneous LEACH schemes are obtained assuming that the SNs of WSN are equipped with the same amount of energy. Also, heterogeneous LEACH schemes are considered assuming that a percentage of the SNs' population is equipped with more energy than the rest of SNs in the same network. We extended LEACH, DEEC, and EEHC to be tested under Two-level, Three-level, and Multi-level HWSNs.

1) Results Under Two-Level HWSN

For two-level heterogeneous networks, Fig. 5 and Table 4 show the results of the case with *m=0.3*, and *a=1.5*. This mean that the total number of normal SNs (N_n) is equal to 70, initial energy of normal SNs (E_{in}) is equal to 0.5 J, total number of advanced SNs (N_a) is equal to 30, initial energy of advanced SNs (E_{ia}) is equal to 1.25 J, and total initial energy of network (E_{total}) is equal to 72.5 J.

TABLE 4. PERCENTAGE OF IMPROVEMENT BETWEEN THE PROPOSED ALGORITHM AND OTHER ALGORITHMS FOR TWO-LEVEL HWSN

	Metrics	Hetero. LEACH	DEEC	EEHC
Impl-a	Stability period (FND)	66.7%	4%	39%
	HND	47%	5%	26.6%
	Throughput	41%	40%	38%
Impl-b	Stability period (FND)	62.8%	1.7%	36%
	HND	31.6%	-6%	12.7%
	Throughput	19%	18.5%	16.5%
Impl-c	Stability period (FND)	72.8%	8%	44%
	HND	42.9%	1.68%	22%
	Throughput	28%	27.5%	25%

 ISBN: 978-1-61208-292-9

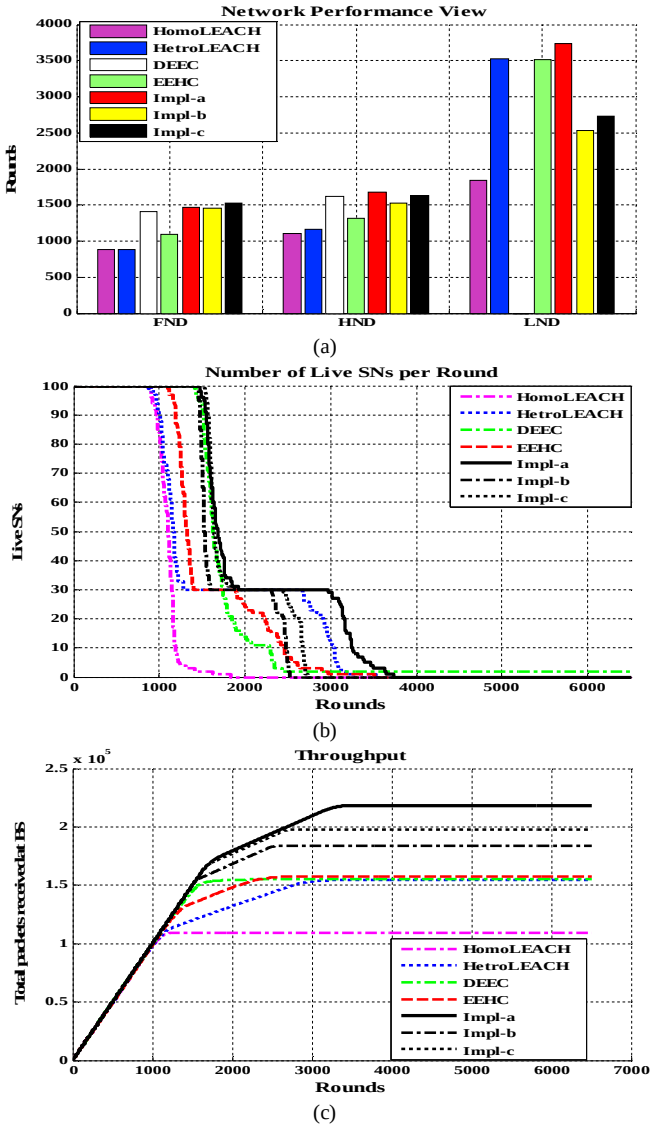


Figure 5. Results for Two-level HWSN.

2) Results Under Three-Level HWSN

For three-level heterogeneous networks, Fig. 6 and Table 5 show the results of the case of $m=0.2$, $m_0=0.5$, $\alpha=2$, and $\beta=1$. This means that 10% of SNs are advanced which are equipped with 200% more energy than normal SNs, and 10% of SNs are super which are equipped with 100% more energy than normal SNs.

3) Results Under Multi-Level HWSN

In this case, we consider that the initial energies of SNs are randomly distributed in [E_0,=0.5 $2E_0$=1]. The results are in Fig. 7 and Table 6. In addition, Figs. 8, 9, and 10 show the effect of changing initial energy of SN, packet size of SN, and number of SNs.

From our simulations, we observed the followings:

1. The stability period of WEPCS is prolonged compared to that of LEACH, DEEC, and EEHC in heterogeneous settings.
2. The instability period was shortened for WEPCS compared to that of LEACH, DEEC, and EEHC.
3. The number of packets received by BS (Throughput) during the lifetime of the network are more than that of LEACH, DEEC, and EEHC. This is because WEPCS has more number of alive SNs as shown in Figs. 5(b), 6(b), 7(b).

TABLE 5. PERCENTAGE OF IMPROVEMENT BETWEEN THE PROPOSED ALGORITHM AND OTHER ALGORITHMS FOR THREE-LEVEL HWSN

	Metric	Hetero. LEACH	DEEC	EEHC
Impl-a	Stability period (FND)	60.%	9.5%	35.5%
	HND	40.5%	3.5%	25%
	Throughput	38.9%	40%	37%
Impl-b	Stability period (FND)	50.9%	3.%	27.6%
	HND	24.8%	-8%	11%
	Throughput	14%	15%	12.7%
Impl-c	Stability period (FND)	63.9%1	12%	38.6%
	HND	34.9%	-0.5%	20%
	Throughput	22.7%	23.9%	21%

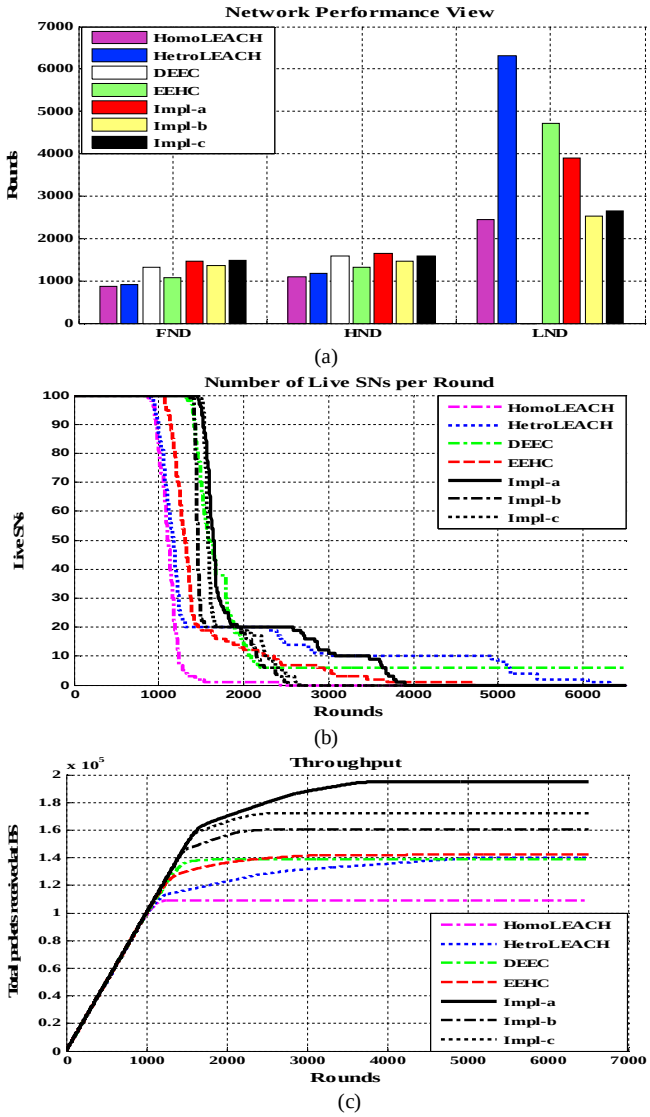
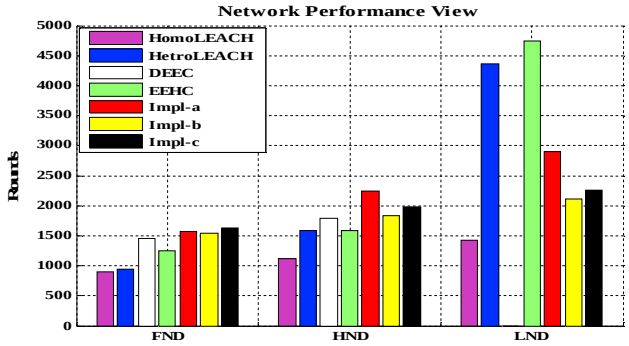


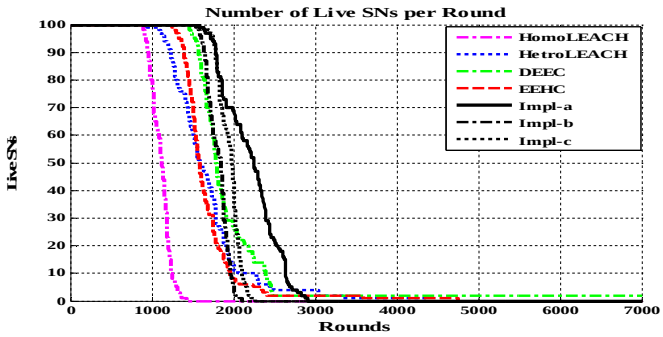
Figure 6. Results for Three-Level HWSN

TABLE 6. PERCENTAGE OF IMPROVEMENT BETWEEN THE PROPOSED ALGORITHM AND OTHER ALGORITHMS FOR MULTI-LEVEL HWSN

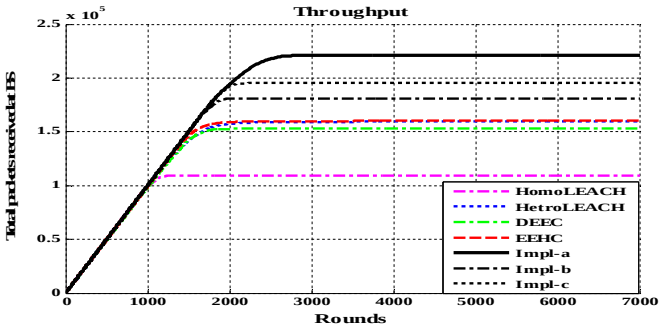
	Metrics	Hetero. LEACH	DEEC	EEHC
Impl-a	Stability period (FND)	68%	7.7%	26%
	HND	42%	25.6%	42%
	Throughput	38.7%	44%	38%
Impl-b	Stability period (FND)	64%	5%	23%
	HND	16%	2.9%	16.5%
	Throughput	13.6%	18%	13%
Impl-c	Stability period (FND)	73.6%	11%	30%
	HND	25%	10.6%	25%
	Throughput	22%	27%	21.8%



(a)

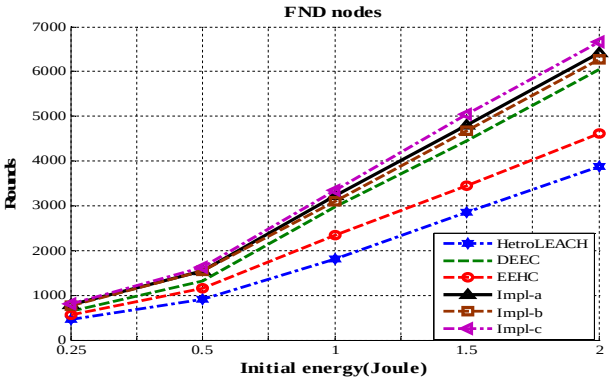


(b)

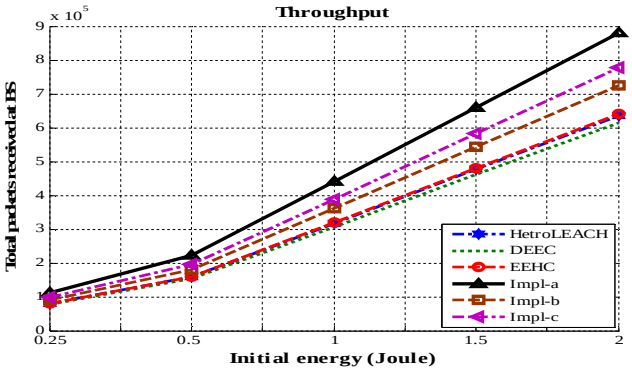


(c)

Figure 7. Results for Multi-Level HWSN [E_0, $2E_0$]

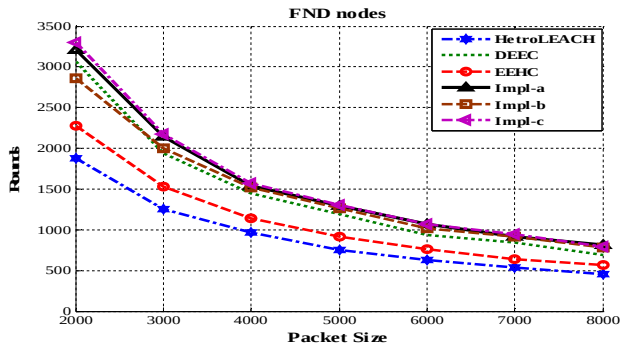


(a)

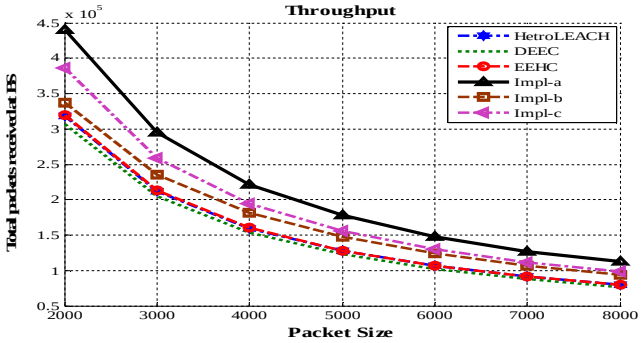


(b)

Figure 8. Performance results for Multi-Level HWSN with different ***initial energies:*** (a) FND and (b) Throughput.



(a)



(b)

Figure 9. Performance results for Multi-Level HWSN with different ***data packet sizes:*** (a) FND and (b) Throughput.

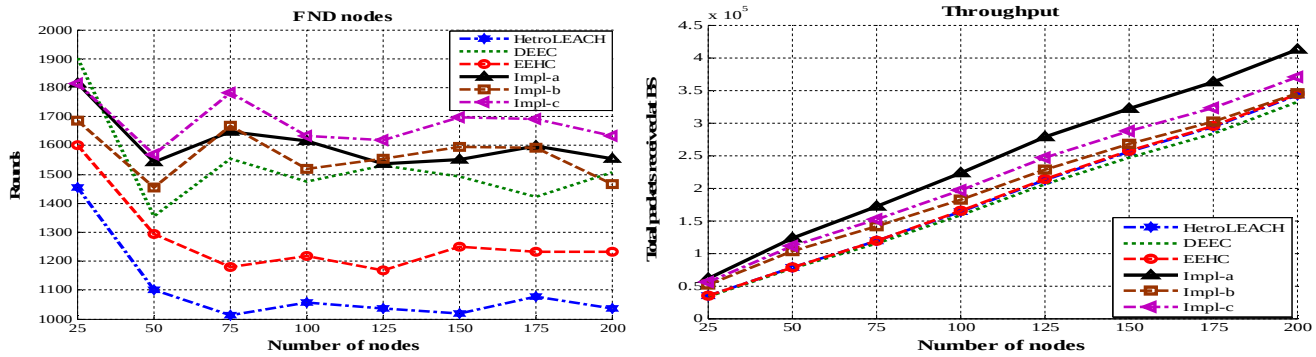


Figure 10. Performance results for Multi-Level HWSN with different ***numbers of SNs:*** (a) FND and (b) Throughput.

V. CONCLUSION AND FUTURE WORKS

In this paper, we proposed and evaluate WEPCS; a new clustering scheme for heterogeneous wireless sensor networks. WEPCS is an extension of the EEHC. In WEPCS, the election of cluster-heads is based on different weighted probabilities. The epochs of being cluster-heads for nodes are different according to their initial and residual energy. Finally, the simulation results show that WEPCS achieves longer lifetime and more throughput than current important clustering protocols in two-level, three-level, and multi-level heterogeneous environments.

The work done in this paper is based on the assumption that the communication environment is contention and error free.

A future extension of the work may consider the effect of the underlying medium access protocol. Also, the work can be extended by applying the algorithm to multi-hop HWSN.

REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks,” IEEE Communications Magazine, vol. 40, no. 8, August 2002, pp. 102–114.

[2] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless Sensor Network Survey,” Computer Networks 52, 2008, pp. 2292–2330.

[3] L. Villalba,, A. Orozco, A. Barenco, and C. Abbas, ”Routing Protocols in Wireless Sensor Networks,” Sensors, *9*(11), Oct. 2009, pp. 8399-8421, doi:10.3390/s91108399.

[4] A. Abbasi and M. Younis, “A Survey on Clustering Algorithms for Wireless Sensor Networks,” Computer Communications vol. 30, 2007, pp. 2826-2841.

[5] V. Katiyar, N. Chand, and S. Soni, “A Survey on Clustering Algorithms for Heterogeneous Wireless Sensor Networks,” Int. Journal of Advanced Networking and Applications vol. 2, no. 4, 2011, pp. 745-754.

[6] G. Smaragdakis, I. Matta, and A. Bestavros, “SEP: A Stable Election Protocol for clustered heterogeneous wireless sensor networks,” Second International Workshop on Sensor and Actor Network Protocols and Applications (SANPA 2004), 2004.

[7] L. Qing, Q. Zhu, and M. Wang, “Design of a distributed energy efficient clustering algorithm for heterogeneous wireless sensor networks,” Computer Communications, vol. 29, no. 12, August 2006, pp. 2230-2237.

[8] D. Kumar, T. Aseri, and R. Patel, “EEHC: Energy Efficient Heterogeneous Clustered Scheme for Wireless Sensor Networks,” Computer Communications, vol. 32, 2009, pp. 662-667.

[9] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-Efficient Communication Protocol for Wireless Microsensor Networks,” Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS 33), January 2000.

[10] D. Kumar, T. Aseri, and R. Patel, “Prolonging Network Lifetime and Data Accumulation in Heterogeneous Sensor Networks,” The International Arab Journal of Information Technology, vol. 7, no. 3, July 2010.

[11] D. Kumar, T. C. Aseri, and R. Patel, “Distributed Cluster Head Election (DCHE) Scheme for Improving Lifetime of Heterogeneous Sensor Networks,” Tamkang Journal of Science and Engineering, vol. 13, no. 3, 2010, pp. 337-348.

[12] Ben Alla Said et al., “Improved and Balanced LEACH for heterogeneous wireless sensor networks,” (IJCSE) International Journal on Computer Science and Engineering, vol. 02, no. 08, 2010, pp. 2633-2640.

[13] E. Brahim, S. Rachid, A. Zamora, and D. Aboutajdine, “Stochastic and Balanced Distributed Energy-Efficient Clustering (SBDEEC) for Heterogeneous Wireless Sensor Networks,” Infocomp: journal of computer science, vol. 8, no. 3, 2009, pp. 11-20.

[14] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “An application-specific protocol architecture for wireless microsensor networks,” IEEE Transactions on Wireless Communications, vol. 1, no. 4, October 2002, pp. 660-670.

[15] M. Handy, M. Haase, and D. Timmermann, “Low energy adaptive clustering hierarchy with deterministic cluster-head selection,” Proceeding of the 4th IEEE Conf. on Mobile and Wireless Communications Networks, Sept. 2002, pp. 368-372.

 ISBN: 978-1-61208-292-9

Analysing Impact of Mobility Dynamics on Multicast Routing in Vehicular Networks

Ines Ben Jemaa and Oyunchimeg Shagdar
IMARA project team
INRIA Rocquencourt
Rocquencourt, France
e-mail:{ines.benjemaa,oyunchimeg.shagdar}@inria.fr

Paul Muhlethaler
HIPERCOM2 project team
INRIA Rocquencourt
Rocquencourt, France
e-mail:paul.muhlethaler@inria.fr

Arnaud de la Fortelle
CAOR Lab
Mines ParisTech
Paris, France
e-mail:arnaud.de_la_fortelle@inria.fr

***Abstract*—Enabling Internet to Vehicular multicast communication is fraught with challenges due to the heterogeneous nature of the two networks. While the conventional multicasting in the Internet relies on "structured" multicast routing, it is not clear how robust can be such routing structure in vehicular networks. We study the robustness of the multicast routing structure in vehicular networks for data flow from the Internet to a set of vehicles. In this paper, we investigate the impact of the urban traffic dynamics on the link stability of the multicast tree. Our study shows that in an intersection scenario, the link can be sufficiently stable without depending much on the relative direction of the vehicles, while on straight roads, the link stability is largely affected by the relative direction.**

***Keywords*—Multicast routing; vehicular networks; urban traffic dynamics; link stability**

I. INTRODUCTION

A number of Intelligent Transportation System (ITS) applications, including the vehicular fleet management and publish/subscribe geo-scoped services, requires multicast communications from the Internet to Vehicular networks. Enabling such application is challenging due to the hybrid communications path (the Internet and wireless media) and the highly mobile nature of the destination nodes, which are the members of the multicast group.

The conventional multicast routing in the Internet is based on protocols such as Protocol Independent Multicast (PIM) [1], which relies on a tree structure to deliver packets form the source to the destinations. Due to the fixed topology of the Internet, the size of the multicast tree can be very large. On the other hand, due to the highly mobile nature of vehicular networks, it can be difficult to maintain a large tree in vehicular networks. Indeed, there is tendency to prefer structureless routing, e.g., opportunistic routing, for vehicular communications. However, it is not clear how such a structureless routing can be used for multicasting and how it can be combined with the structured multicast routing, which is used for the Internet, for Internet-to-Vehicular multicast communications.

To the best of our knowledge, very few studies are made on pure multicasting for Internet to vehicular communications for different road environments. The analysis made by Karaoglu and Heinzelman [2] shows that multicasting is preferable to broadcasting when the number of nodes in the network or the size of the area increase. Most of the existing works on multicasting for vehicular networks including [3] assume that the multicast members are all the nodes that belong to a specific geographic area and tackle the problems of geographic broadcasting (geocast) among the vehicles. On the other hand, some other works focus on vehicular group clustering organization and management. Although promising solutions are proposed (e.g., [4]), the proposals lack a deeper analysis of the impact of realistic road traffic on the communication between vehicles.

In this paper, we study multicasting for vehicular networks for data flow between Internet and vehicles. Since the tree-based multicast routing is the *de-facto* scheme in the Internet, we first investigate the stability and robustness of the tree structure in realistic road environments. This paper reports our preliminary analysis, which is carried out using the SUMO traffic simulator [5] targeting a realistic intersection road scenario. The simulations show the impact of some parameters such as velocity on maintaining stable links in urban scenarios including intersections.

This paper proceeds as follows. The related works are introduced in Section II. In Section III, we present our preliminary study concerning the impact of traffic dynamics on neighbor link stability. Finally, we conclude the paper in Section IV.

II. RELATED WORK

A number of efforts are made for multicasting in ad hoc networks. Feng et al. [6] showed the feasibility of maintaining a multicast delivery tree for vehicular ad hoc networks (VANET) in straight roads environments. The scheme identifies the multicast members as the set of vehicles, which are concerned by the road warning message, and builds a delay-constrained minimum Steiner tree and optimize it by using a specific cost function. Unlike our work, the intersection road scenarios, which create more complex traffic dynamics, are not considered in this study. Chandra et al. [4] propose a multicast mechanism that enables communication in the context of an architecture which integrates the Long Term Evolution (LTE) technology and the IEEE 802.11p in VANET. In what they call "low-level multicasting" (group communication in a cluster), they build a two-hops shared tree to disseminate the message from the Cluster Head to the members of the group. In their analysis, the authors claim that the use of the multicast tree provides efficiency and low control overhead. However, the authors didn't justify the chosen size of the tree and they did not analyze the effects of the vehicular moility characteristics on the tree's stability.

 ISBN: 978-1-61208-292-9

In [7], Badessari et al. propose an approach to deliver multicast packets from the Internet to the vehicles which are located in a specific geographical area. In this approach, the packets are first forwarded to the access router, whose IP address is matched with the destination geographic area, and then the access router broadcasts the packets over one or more number of hops. Tonguz et al. [3] present a broadcasting protocol named DV-CAST that addresses the problem of dealing with the extreme situations of dense and sparse vehicular traffic. The design of the protocol strongly relies on the one-hop neighborhood informations and shows a certain reliability in each road traffic situation. Although the approaches based on geobraodcast ensure robustness in some situations, it is not clear yet how efficient and scalable they are, especially in situations when the vehicular density is high or when the multicast group size is small as read in [2].

In [8], a study of the impact of the spatio-temporal traffic density variation in highway scenario is presented. The authors use in their study both empirical and analytical data to analyze and report the impact of different traffic situations on the communication performance. Although this work is similar to ours, it considers only simple dissemination mechanisms based on multi-hop geocast and single-hop broadcast.

III. Impact of Traffic Dynamics on Neighbor Link Stability

In our simulations, we consider an urban area with an intersection as illustrated in Fig. 1. The size of the overall area is $4000m \times 4000m$. Each road has a single forward and backward lanes. Vehicles are generated at the edge of each lane (the points A, B, C and D in Fig. 1) following the Poisson process at the average rate λ Hz (car/second). The maximum speed, acceleration and deceleration are 50 km/h, 0.8 m/s^2 and 4.5 m/s^2 respectively. The minimum inter-vehicle distance is 2.5 m. The velocity of the vehicles is limited to 50 Km/h. Their acceleration ability is set to 0.8 m/s^2 and their deceleration ability is set to 4.5 m/s^2. The intersection is equipped with traffic lights and so that, the vehicles stop at the intersection if necessary. At the intersection, vehicles select randomly their destination and follow the route to their destination. Consequently, vehicles dynamically control their mobility following the traffic rule as well as to avoid collisions. The total simulation time is 15 minutes.

The aim of the simulations is to evaluate the number of K-hops neighbors of randomly chosen ego nodes (vehicles), the neighborhood lifetimes, the relative directions and velocities. We define a node as a neighbor of the ego node, if the distance between the node and the ego is less than the communication range R. R is set to 300 m, with the IEEE 802.11p technology [9], in mind. The neighborhood lifetime is the period of time during which the nodes stay as neighbors. The relative direction is the angle difference between the moving directions of the neighbors.

Fig. 2 illustrates the maximum, the minimum and the average values of lifetimes for 10 randomly chosen ego vehicles. The horizontal axis is the road density, more specifically λ (the average vehicle generation rate). For each simulation, we change the value of the density, λ. As shown is the figure, the neighborhood lifetime linearly increases with the increase

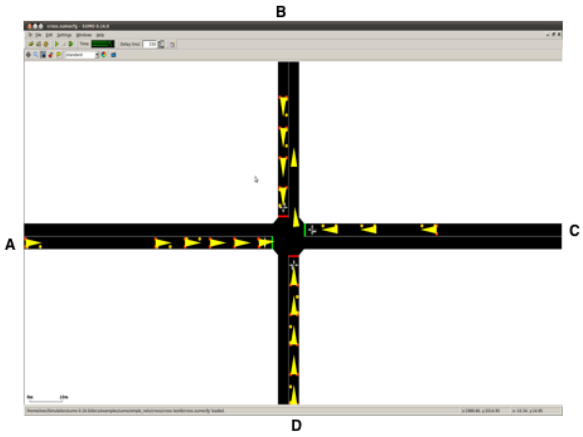


Figure 1: Intersection scenario set up

of the density. When the vehicular density on the road is low (λ=0.04 Hz), the maximum lifetime that we obtain is about 150 seconds, resulting in shorter neighborhood lifetimes with individual neighbors compared to those when density is higher (e.g., 650 seconds expressed by λ=0.2 Hz). The minimum neighborhood lifetime remains the same for all densities. This value is obtained when both the ego vehicle and its neighbors are moving at the maximum velocity and in opposite directions. As in the scenario, assuming that the maximum velocity is 50 km/h and the range R is 300 meters, the minimum neighborhood lifetime value can be obtained in this scenario as following:

$$\Delta t = \frac{R}{|v_{ego} - v_{neighbor}|} = \frac{0,3km}{100km/h} = 10,79sec$$

The average neighborhood lifetime drops notably compared to the maximum value of the neighborhood lifetime. The range of the average neighborhood lifetime varies from 30 seconds for a density λ of 0.04 Hz to 170 seconds for a density λ of 0.2 Hz. Those values explain that only few neighbors are kept for a long period (maximum lifetime) and that most of the contacts' durations belong to the interval [30sec,170sec]. Thus, vehicles are able to share common links with their neighbors during relatively long periods of time (i.e., neighborhood lifetime) in intersection scenarios.

In the following, Fig. 3, Fig. 4 and Fig. 5 show, respectively, the number of the neighbors, the relative direction and the relative velocity measured (w.r.t ego node) when λ is 0.1 Hz. The horizontal axis of Fig. 3 and Fig. 4 (corresponding to the vertical axis of Fig. 5) is the normalized neighborhood lifetime. Based on our analysis, we used different markers; both rectangular and cross markers correspond to the results obtained for straight roads whereas triangular markers correspond to the results obtained in the intersection area.

Fig. 3 shows that a great number of neighbors, between 35 and 15 (expressed with rectangular markers), kept less than 0.07 of the total lifetime (more precisely between 4% and 7% of the total lifetime). This explains why the average lifetime is much lower compared to the maximum lifetime in Fig. 2. The relative direction of these neighbors, as shown in Fig.

 ISBN: 978-1-61208-292-9

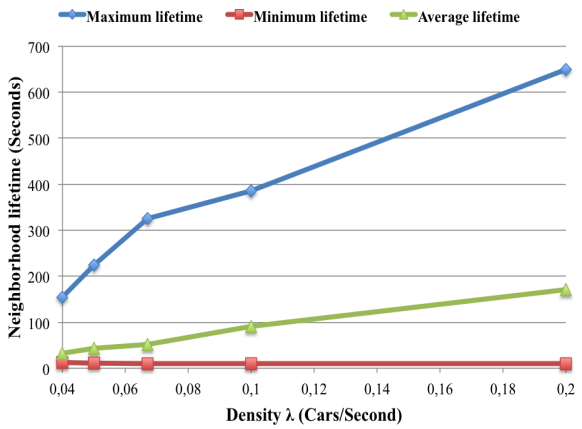


Figure 2: Variation of the maximum neighborhood lifetime with the road density

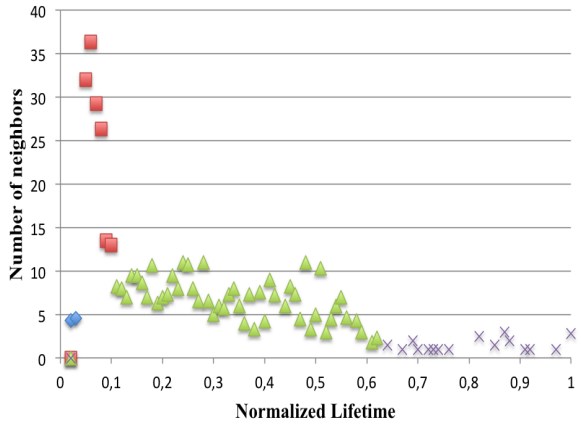


Figure 3: Average number of neighbors

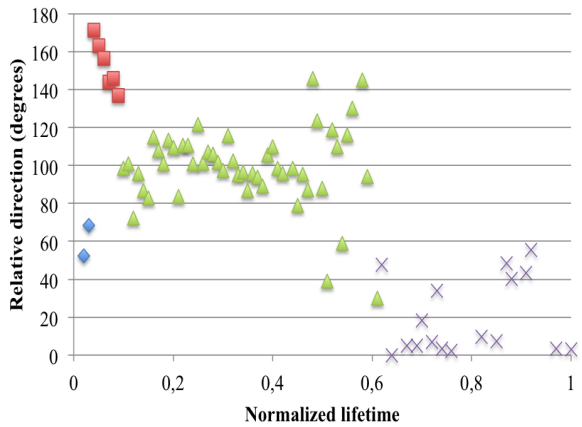


Figure 4: Neighbors' relative direction w.r.t the ego vehicle.

4 is as high as close to 180 degrees (i.e., opposite direction with the ego vehicle). Fig. 3 also shows that the lifetime of very few neighbors (1 to 3 neighbors) is longer than 50% of

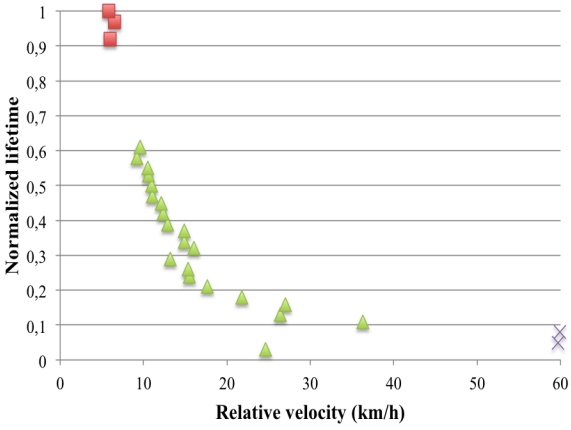


Figure 5: Neighbors' relative velocity w.r.t the ego vehicle

the maximum neighborhood lifetime and the corresponding relative direction is at most 40 degrees (expressed with cross markers in the figures).

Our investigation shows that such extremely short or long lifetime values reflect the situations where the ego vehicle is driving on the straight road. This implies that on the straight road, the relative direction provides a major impact on the link stability. While the ego node meets a larger number of nodes, which are moving to the opposite direction, the neighborhood lifetime can be short and thus unreliable. On the other hand, while the number can be few, the neighbors, which are following the same direction as the ego node even after the intersection area, can provide stable links, and the lifetime can be especially long. Those situations correspond to a normalized lifetime of 1.

Furthermore, the neighbors which start their journey on the same road segment as the ego node but take a different direction at the intersection, gives slightly shorter lifetime (between 0.5 to 0.8) and the relative direction is higher than 0. The lifetime in the range of [0.05, 0.08[(expressed with rectangular markers in the figures) corresponds to the neighbors which meet the ego node at the intersection. The relative directions of those nodes are relatively high; 80 to 160. It is interesting to observe that for those neighbors, the relative direction takes a high value for a long lifetime. Specifically, the neighbor with the relative direction [80, 120] had the neighborhood lifetime of [0.1, 0.3], whereas the neighbors with the relative direction 160 has neighborhood lifetime of 0.47. Finally, attention should be made to the case of lifetime neighborhood of less than 0.02 (expressed with diamond marker) that corresponds to the neighbors, which did not stop at the intersection and with whom the ego meets at the intersection. Because the neighborhood lifetime of such nodes is even shorter than those of the neighbors, which move on the opposite direction at the straight road), such nodes should be distinguished from nodes which stop at the intersection.

As a consequence, it should be mentioned that we could not find a clear relationship between the neighborhood lifetime and the direction. For this reason, we investigated the impact of the velocity (Fig. 5) on the neighborhood lifetime duration of an ego vehicle.

 ISBN: 978-1-61208-292-9

Fig. 5 illustrates the variation of the neighborhood lifetime with the neighbors' relative velocity. From the figure, we can notice that long neighborhood lifetimes (almost 100% of the lifetime) are obtained when the relative velocity is low (i.e., between 0 to 10 km/h). In contrast, it is almost less than 10% of of the neighborhood lifetime when the relative velocity is 60 km/h. Those situations correspond to the scenarios where vehicles are either driving on the same direction or on opposite direction but in the same road. On the other hand, the lifetime considerably decreases and becomes almost constant for the highest relative velocity which reflects the situation where the neighborhood contact duration is low when the vehicles are moving in opposite directions. Following the observation of Fig. 5 and Fig. 4, it seems that keeping relatively long neighborhood lifetime does not depend much on the moving direction but more on the relative velocity. indeed, as can be seen from Fig. 4, at intersection, while vehicles can have large relative direction, the lifetime's duration is short.

Consequently, our current investigation of the parameters that may have impacts on the neighborhood lifetime duration in the intersection scenario leads to the conclusion that the velocity seems to have the major influence on the neighborhood link duration. Our next step will be the investigation of such parameter in n-hop neighborhood.

IV. Conclusion and future work

We studied the traffic road impact on the stability of multicast routing for data flows from Internet to Vehicular networks. In this paper, we reported our preliminary study of the traffic dynamics impact on link stability for a realistic intersection road scenario. The study is carried out using the SUMO traffic simulator under different road traffic settings. Simulation results show that in an intersection scenario, the link can be sufficiently stable without depending much on the relative direction of vehicles. On the other hand, on straight roads, the link stability is largely affected by the relative direction. Specifically, for the target scenario, only 2 neighbors are kept for more than 80% of the total ego trip time, whereas 35 neighbors keep a link with the ego for 5%of the total travel time. Our study shows also the impact of the relative velocity on the stability of the links between vehicles as it is clearly shown that a low relative velocity with neighbors ensures long neighborhood lifetimes and vice versa.

As a future work, we study the impact of vehicles' velocity and density on the neighborhood lifetime for K-hop neighbors under more complex urban scenarios. Based on our studies, we plan to seek a multicast routing approach that is more adapted to Internet to vehicular communications scenarios.

References

[1] B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas. Protocol independent multicast - sparse mode (pim-sm), August 2006.

[2] B. Karaoglu and W. Heinzelman. Multicasting vs. broadcasting: What are the trade-offs? *GLOBECOM*, pages 1–5, December 2010.

[3] O. K. Tonguz, N. Wisitpongphan, and F. Bai. Dv-cast: a distributed vehicular broadcast protocol for vehicular ad hoc networks. *Wireless Commun.*, 17(2):47–56, April 2010.

[4] R. Sivaraj, A. K. Gopalakrishna, M. G. Chandra, and P. Balamuralidhar. QoS-enabled group communication in integrated VANET-LTE heterogeneous wireless networks. *WiMob*, pages 17–24, October 2011.

[5] SUMO http://sumo.sourceforge.net/.

[6] A. Sebastian, M. Tang, Y. Feng, and M. Looi. A Multicast Routing Scheme for Efficient Safety Message Dissemination in VANET. *WCNC*, pages 1–6, April 2010.

[7] R. Baldessari, C. J. Bernardos, and M. Calderon. Geosac - scalable address autoconfiguration for vanet using geographic networking concepts. In *PIMRC*, pages 1–7, September 2008.

[8] F. Bai and B. Krishnamachari. Spatio-temporal variations of vehicle traffic in vanets: facts and implications. In *VANET*, pages 43–52, 2009.

[9] S. Graing, P. Mahonen, and J Riihijarvi. Performance evaluation of ieee 1609 wave and ieee 802.11p for vehicular communications. In *Second International Conference on Ubiquitous and Future Networks (ICUFN)*, pages 344–348, June 2010.

 ISBN: 978-1-61208-292-9

Dynamic Reorganization of P2P Networks Based on Content Similarity

Takuya Yamaguchi
Graduate School of Science and Engineering, Saitama University
Saitama, Japan
takuya@ss.ics.saitama-u.ac.jp

Noriko Matsumoto
Graduate School of Science and Engineering, Saitama University
Saitama, Japan
noriko@ss.ics.saitama-u.ac.jp

Norihiko Yoshida
Graduate School of Science and Engineering, Saitama University
Saitama, Japan
yoshida@ss.ics.saitama-u.ac.jp

***Abstract*—A unstructured P2P network does searching by packet forwarding which has some problems: hit ratios are low, and the network is filled with packets. A structured P2P network based on the distributed hash table (DHT) solves these problems. However, it is restricted to keyword search. This paper proposes a P2P network which reorganizes itself dynamically, aiming at search efficiency of the structured P2P and the search flexibility of the unstructured P2P at the same time. We define similarity of contents based on the folksonomy in social networks, and make the network update its links dynamically based on the content similarities. By simulation-based experiments, we confirmed improvements of query hits in this P2P network.**

Keywords-P2P; content-based reorganization; folksonomy

I. INTRODUCTION

P2P networks have some categories according to content search methods. An unstructured (pure) P2P such as Gnutella, which uses flooding-based search, has advantages in regards to network flexibility and robustness. However, flooding causes network congestion. Some techniques have been proposed to suppress the congestion such as Expanding Ring [1] and Random Walks [1]. However, they have no concern with the properties of contents.

Usually, the time-to-live (TTL) parameter is used to control flooding. It specifies the maximum number of forwarding hops of search queries. The smaller the TTL is, the less the congestion is. However, the smaller TTL leads to the lower hit ratio (or success ratio) as well. A peer node which emits a search query (searcher) is assumed to have a similar interest to a peer which has the target content. This means that peers with similar interests are better located nearer in order to suppress network congestion and to assure hit ratio at the same time.

The Distributed Hash Table (DHT) is another category of P2P, which suffers no network congestion. However, a DHT-based P2P network must have a strictly structured topology, and consequently is prone to failure, costful in dynamic restructuring, and also search in the DHT is limited to exact matching in principle.

This paper proposes a P2P network with a restructuring function similar to a consensus formation theory [2]. The function simulates a group formation in social networks, and is to make groups of nodes with similar contents dynamically.

We begin with our observation on P2P content search.

- It is likely that the searcher has already some contents similar to the one being searched.
- It is likely that the searcher is always interested in the search keyword.
- It is likely that the searcher will be interested in related keywords in the future.

The interest of a peer must be inferred from the set of its contents. Our P2P network restructures itself based on the peers' similarity.

Hereafter, we introduce related works regarding network reconstruction in Section 2, and propose a reconstruction method based on similarity in Section 3. The simulation and consideration in a P2P network using our technique are shown in Section 4. Section 5 includes some concluding remarks.

II. RELATED WORKS

From the early days of P2P networks, there were some attempts to content-based retrieval and peer clustering. Lu and Callan (2003) [3] and Wang and Yang (2006) [4] proposed such mechanisms on top of a super-peer-based hybrid P2P network, in which a super peer acts as an index server for contents. On the other hand, Tang, et al. (2003) [5], Kacimi and Yetongnon (2008) [6], and Tirado, et al. (2010) [7] proposed a semantic overlay network over a DHT-based structured P2P network. We have taken an alternative approach. A P2P network itself is an overlay on top of a physical network. Therefore, instead of constructing a content-based overlay on top of a P2P overlay, we reorganize a P2P overlay to be a content-based overlay as well. Vazirgiannis, et al. (2006) [8] proposed an approach similar to ours. However, their work stayed at a preliminary stage.

Sripanidkulchai, et al. (2003) [9] proposed a content allocation scheme based on interest proximity (or similarity), and Voulgaris, et al. (2004) [10] extended it towards a semantic overlay. Our originality lies in aggregation of content similarities to get node similarities, reducing the network traffic.

Below are some topics related to P2P network reorganization.

A. Reorganization for Reliability Improvement

Simple Trust Exchange Protocol (STEP) [11] is a protocol for P2P reorganization to improve network reliability. STEP aims at taking care of a normal peer by eliminating free riders, which do not provide contents, but only consume, and malicious peers which distribute inaccurate contents.

A receiver evaluates service provided by a sender, and issues a "token" with rating of the service. Each node exchanges

 ISBN: 978-1-61208-292-9

the tokens by messages called "knowledge" with its neighbors periodically, and sums up single evaluations to make a more precise evaluation. Then, each node decides how tightly it keeps its link with the evaluated node, and any node with a "bad" evaluation is eliminated from the network in this manner.

B. Network Reorganization by Consensus Building

A social network consists of various groups. People in a group usually share the same interest and/or opinion. Holme and Newman [2] tried to model this group formation under agreement and opinion adjustment.

The initial network has N nodes and M random links. Each node has one out of G opinions. This network repeats the below every unit time.

1) Choose one node i at random.
2) If the node i does not have a link, do nothing. Otherwise, choose one link at random, which is to connect to the node j.
   - Upon probability of ϕ, reconnect the link to a node with the same opinion as i.
   - Upon probability of $1-\phi$, change i's opinion to the same as j's.

They simulated the model and confirmed that clusters emerged in the network according to the opinions.

III. METHOD

Our proposed method is divided into the similarity calculation method and the network reconstruction method. Below we present them respectively.

A. Similarity Calculation Method

Network reconstruction is done based on the peer similarity. Each peer calculates the peer similarity value based on the content similarity value of the peer's contents. The content similarity value is calculated based on the content information exchanged between peers. If a peer must exchange and calculate the similarity value for all the contents it contains, it would cause severe network traffic and overhead. Therefore, we introduce "Virtual Typical Content" (VTC) for each peer, whose similarity value is an aggregation of the values of all the contents of the peer. A peer's VTC represents the tendency of the content which the peer has. We may say, looking at the VTC, we can get the "taste" of the peer.

The purpose of VTCs is to reduce network traffic and overhead drastically. It causes significantly lower traffic to exchange only VTCs between peers than to exchange all the contents on peers. Each peer has the predefined number of VTCs (not necessarily one) regardless of the number of the contents it really has. This method is particularly effective in a network composed of poor performance peers and narrow band communication.

The similarity value of the VTC is calculated from the similarity of contents. It is difficult and resource consuming to get the similarity of contents by analyzing the contents. Therefore, we use folksonomy [12] instead.

1) Folksonomy: Folksonomy is a sort of information classification. Users attach tags to contents. A tag is typically a keyword which the users think represents the meaning or nature of the contents. Then the contents are classified based on a collection of tags (Fig. 1).

Recently, this method is getting widely used on the Internet, for example, as social bookmarks. Although having some problems, i.e. tags cannot handle synonyms, and tags may be unsuitable intentionally, folksonomy is promising because of its significantly lower cost compared to automatic keyword distillery using "TF-IDF" for example.

In our method, content suppliers give tags to each content, and the system calculates similarity values from tags.

2) Making Virtual Typical Content: Virtual typical contents are created as follows:

Let C, T be sets, and (M, m) be a multiplex set. The number of VTCs is N, and the max number of tags assigned to VTC is M.

1) Let a peer have contents $C = \{c_1, c_2, \ldots, c_n\}$, and let each content c_x have tags T_{c_x}.
2) Calculate $M_1 = \bigcup_{c_k \in C} T_{c_k}$.
3) Calculate the most common tag t_{max} that is $m_1(t_{max}) = max(\{m_1(x) \mid x \in M_1\})$ (Fig. 2).
4) Find a content having the most common tag $C_{max} = \{c_x \mid t_{max} \in T_{c_x}\}$ (Fig. 3).
5) Calculate $M_2 = \bigcup_{c_k \in C_{max}} T_{c_k}$.
6) Calculate $T_{VTC} = \{t \mid t \in M_2, m_2(t) \geq \alpha\}$. But, α is decided suitably about $n(T_{VTC}) = M$ (Fig. 4).
7) Making VTC which assigned T_{VTC} (Fig. 4).
8) Calculate $C = C - C_{max}$.
9) If $C = \emptyset$ or the number of VTC is N, the loop terminates. Otherwise, the loop goes back to 2) and continues.

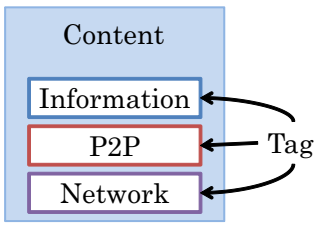


Figure 1. Assignment of tags.

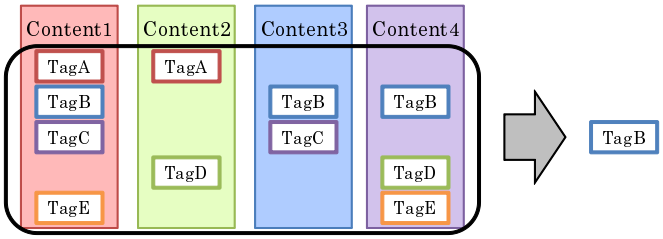


Figure 2. Selection of the most common tag.

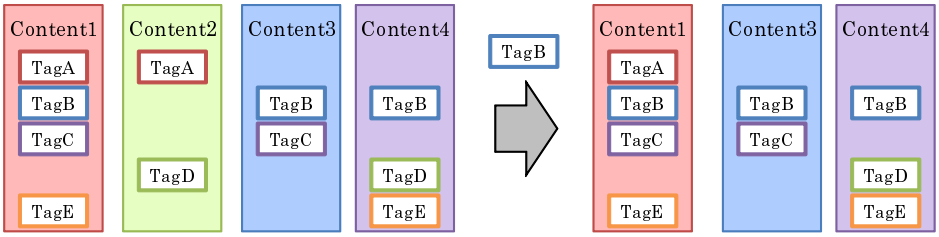


Figure 3. Selection of contents with the most common tag.

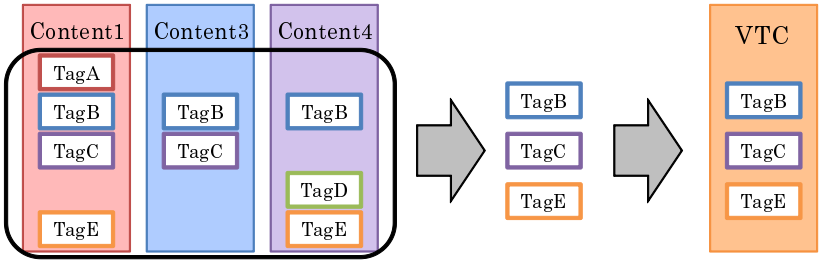


Figure 4. Making of a virtual typical content.

3) Content Similarities: Content suppliers attach tags to each content. The content similarity is calculated from an agreement ratio of these tags.

Let content A be assigned tags $T_A = \{T_{A1}, \ldots, T_{AN}\}$, and content B be assigned tags $T_B = \{T_{B1}, \ldots, T_{BM}\}$. The similarity value R_C between content A and B is defined as follows:

1) If $T_A = \emptyset$ or $T_B = \emptyset$, then $R_C = 0$
2) Otherwise, (i.e. $T_A \neq \emptyset$ and $T_B \neq \emptyset$),

$$R_C = \frac{n(T_A \cap T_B)}{min(n(T_A), n(T_B))} \quad (1)$$

where $n(X)$ means the number of elements in the set X.

Therefore, the content similarity satisfies the below properties:

1) If $T_A \cap T_B = \emptyset$ then $R_C = 0$.
2) If $T_A \subseteq T_B$ or $T_A \supseteq T_B$ then $R_C = 1$.
3) The domain of R_C is $0 \leq R_C \leq 1$.

4) Peer Similarities: We calculate the peer similarity value R_P from the content similarity value as follows. We specify the number of VTCs and the number of tags attached to each VTC, given a set of contents on a peer, and create VTCs. Then, the peer calculates content similarity values for all the VTCs, and make the maximum value of the outcome R_C as the peer similarity value R_P.

B. Reconstruction Method

Network reconstruction is done by reconnecting network links, using a technique similar to the neighbor peer replacement technique in STEP.

Two peers connected by a link are called neighbor peers. For each peer, let there be the predefined maximum number of neighbor peers. Each peer can have this number of links at the most.

If a peer $P1$ receives a new connection request from a peer $P2$ which is not a neighbor peer, $P1$ approves or denies the request as follows:

1) If $P1$ does not have the maximum number of neighbor peers, the request from $P2$ is approved and a link between $P1$ and $P2$ is created.
2) If $P1$ already has the maximum number of neighbor peers, similarities to all neighbor peers as well as $P2$ are calculated.
   a) If the similarity to $P2$ is lower than any of the similarities to all the neighbor peers, the request is denied (Fig. 5).
   b) Otherwise, a link to a peer whose similarity is the lowest among the neighbor peers is discarded, and the request to create a link to $P2$ is approved (Fig. 6).

Each peer does the above, and some cluster of peers with the high similarities emerges in the network autonomously.

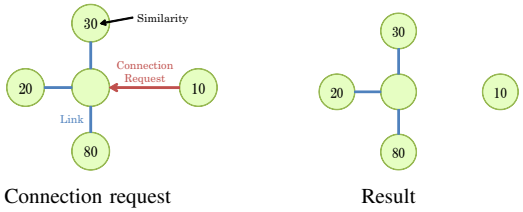


Figure 5. Connection denial.

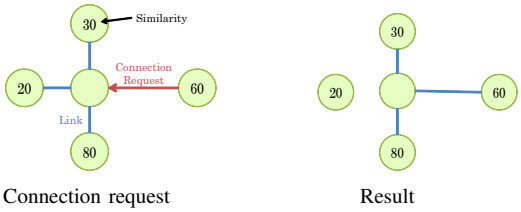


Figure 6. Connection approval.

IV. SIMULATION

We built a simulator which constructs virtual P2P networks on a single computer, and performed some experiments and evaluation.

A. Simulation Model

As described in Section 1, each peer is supposed to have some tendency, or deviation, in its interests. The simulator reflects this as follows.

Each peer is assigned an unique integer of 1 or more, PID, as its identification number. A tag is assigned also an integer of 1 or more, although a tag in the real world would be some keyword. Peers in the network are grouped in the manner that a peer having such a PID that $(k-1)\times M+1 \leq \mathrm{PID} \leq k\times M$ belongs to the group G_k. Peers in a group G_k has an interest in such a tag t that $(k-1)\times M+1 \leq t \leq k\times M$. Let p be a search deviation ratio. With the probability p, a peer searches a tag within the interests of G_k. Otherwise (with the probability $1-p$), a peer searches a random tag. Likewise, Let $p\prime$ be a content deviation ratio. With the probability $p\prime$, each content on a peer within G_k has a tag within the interests of G_k. Otherwise, a content has a random tag.

Some major parameters in the simulation are summarized in Table I. We performed simulations for networks in which the number of peers are 100, 200, and 300, and for a case with network reconstruction and a case without reconstruction. We repeated simulations five times.

We define a unit time of the simulation as a period necessary to forward a message from a peer to its neighbor peer. Each peer does all the necessary computation and this one hop communication within the unit time. We call the unit time "second" in this simulation, and one simulation lasted for ten hours.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Max number of neighbor peers	4
Time-to-Live (TTL)	4
Number of VTC	10
Max number of tags assigned to VTC	6
Number of peers in a group	10 (20 in case of 300 peers)
Search deviation ratio	80%
Content deviation ratio	80%
Minimum connection time	3 second
Disconnection Probability	0.2%
Disconnection interval	60 second

B. Simulation Results

1) The Number of Search Hits: The number of average hits (QueryHit) to one query is shown in Fig. 7, Fig. 8, and Fig. 9 for the cases of 100, 200, and 300 peers respectively. The number of hits in search is shown to be improved in the network with reconstruction compared to the network without reconstruction under the same small value of TTL.

2) Overhead of Similarity Calculation: Table II shows the average number of VTCs transfer per peer per one hour during similarity calculation. It must cause message overhead to the network by the proposed method. Real overhead to an actual

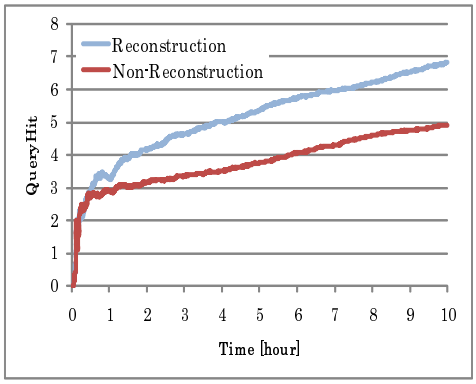


Figure 7. Averages of QueryHits (100 Peers).

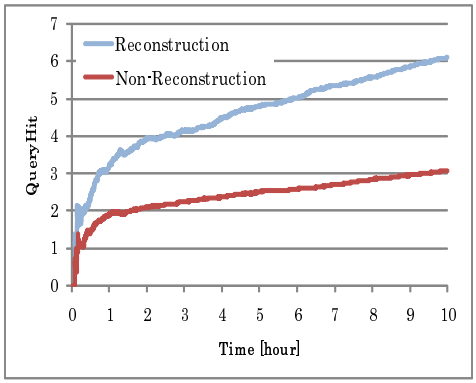


Figure 8. Averages of QueryHits (200 Peers).

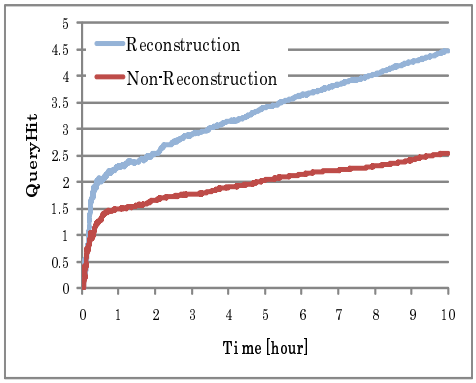


Figure 9. Averages of QueryHits (300 Peers).

 ISBN: 978-1-61208-292-9

TABLE II. THE NUMBERS OF VTCS

	100	200	300
First	157.22	204.24	184.58
Second	188.04	177.68	175.96
Third	196.21	191.04	201.41
Fourth	154.32	195.68	168.34
Fifth	167.45	200.40	184.09
Average	172.65	193.81	182.88

Table III. COMPARISON OF VTCS AND QUERIES

	VTC	Query
First	157.22	3211.68
Second	188.04	3356.04
Third	196.21	3240.48
Fourth	154.32	3152.99
Fifth	167.45	3275.56
Average	172.65	3247.35

network would be a product of this average number and the size of a VTC message. However, this size must be small, because a VTC message only contains tag information, and comparable to the size of a search query message, and much smaller than the size of a content.

Table III shows comparisons of the number of VTCs and the number of queries per peer per hour in the 100 peer network. The number of VTCs is about $1/20$ of the number of queries. This 5% overhead of VTC messages added to query messages in the network traffic is supposed to be acceptable compared to the traffic for content delivery.

We suppose this overhead of VTC messages could be reduced. These results shown here are obtained out of the worst cases in the sense that the numbers of VTCs are the largest in these networks. More than one VTC messages from the same peer could be aggregated into a single message. Also, caching of VTC messages could reduce the network traffic.

V. CONCLUSION AND FUTURE WORK

In this paper, we proposed a reconstruction method of P2P networks based on content similarity. The proposed method uses tags to each content in a peer, makes virtual typical contents (VTCs) representing interests of the peer from the tags assigned to the contents, calculates similarity values from VTCs, and updates links between peers according to similarity values. This reorganization improves success ratios of queries even if the time-to-live (TTL) value is unchanged. In other words, we could make the time-to-live value smaller to achieve the same success ratios, which leads to lower network traffic.

We are still at the starting point toward practical implementation and deployment of this design. Future work includes some improvement for selecting a peer to whom a connection request is sent using the similarity values. In the current design, a connection request is sent to an arbitrary peer. This improvement must bring more efficient clustering. Another work would be aggregation of VTC messages to query messages to reduce the overhead of VTC messages to the network traffic as well as to convey the VTC messages farther than its neighbors.

REFERENCES

[1] Q. Lv, P. Cao, E. Cohen, K. Li, and S. Shenker, “Search and Replication in Unstructured Peer-to-Peer Networks”, Proc. ACM 16th Int. Conf. on Supercomputing, 2002, pp. 84–95.

[2] P. Holme and M. E. J. Newman, “Nonequilibrium Phase Transition in the Coevolution of Networks and Opinions”, Physical Review E, Vol. 74, 056108, November, 2006, 5 pages.

[3] J. Lu and J. Callan, “Content-Based Retrieval in Hybrid Peer-to-Peer Networks”, Proc. ACM 12th Int. Conf. on Information and Knowledge Management, 2003, pp. 199–206.

[4] J. Wang and S. Yang, “Content-based Clustered P2P Search Model Depending on Set Distance”, Proc. 2006 IEEE/WIC/ACM Int. Conf. on Web Intelligence and Intelligent Agent Technology, 2006, pp. 471–476.

[5] C. Tang, Z. Xu, and S. Dwarkadas, “Peer-to-Peer Information Retrieval Using Self-Organizing Semantic Overlay Networks”, Proc. ACM SIGCOMM, 2003, pp. 175–186.

[6] M. Kacimi and K. Yetongnon, “Content-Based Information Routing and Retrieval in Cluster-based P2P Overlay networks”, Proc. 2008 IEEE Int. Conf. on Signal Image Technology and Internet Based Systems, 2008, pp. 70–77.

[7] J. M. Tirado, D. Higuero, F. Isaila, J. Carretero, and A. Iamnitchi, “Affinity P2P: A Self-Organizing Content-Based Locality-Aware Collaborative Peer-to-Peer Network”, Computer Networks No. 54, 2010, pp. 2056–2070.

[8] M. Vazirgiannis, K. Norvag, and C. Doulkeridis, “Peer-to-Peer Clustering for Semantic Overlay Network Generation”, Proc. 6th Int. Workshop on Pattern Recognition in Information Systems, 2006, 10 pages.

[9] K. Sripanidkulchai, B. Maggs, and H. Zhang, “Efficient Content Location Using Interest-Based Locality in Peer-to-Peer Systems”, Proc. IEEE INFOCOM, 2003, pp. 2166–2176.

[10] S. Voulgaris, A.-M. Kermarrec, L. Massoulie, and M. v. Steen, “Exploiting Semantic Proximity in Peer-to-Peer Content Searching”, Proc. 10th IEEE Int. Workshop on Future Trends of Distributed Computing Systems, 2004, pp. 238–243.

[11] I. Martinovic, C. Leng, F. A. Zdarsky, A. Mauthe, R. Steinmetz, and J. B. Schmitt, “Self-Protection in P2P Networks: Choosing the Right Neighbourhood”, Proc. 1st Int. Workshop on Self-Organizing System, 2006, pp. 23–33.

[12] A. Mathes, “Folksonomies - Cooperative Classification and Communication Through Shared Metadata”, LIS590CMC, University of Illinois Urbana-Champaign, December, 2004, 13 pages.

 ISBN: 978-1-61208-292-9