AFIN 2012

The Fourth International Conference on Advances in Future Internet

ISBN: 978-1-61208-211-0

August 19-24, 2012

Rome, Italy

AFIN 2012 Editors

Alessandro Bogliolo, University of Urbino, Italy

Pascal Lorenz, University of Haute Alsace, France

AFIN 2012

Foreword

The Fourth International Conference on Advances in Future Internet [AFIN 2012], held between August 19-24, 2012 in Rome, Italy, continued a series of events dealing with advances on future Internet mechanisms and services.

We are in the early stage of a revolution on what we call Internet now. Most of the design principles and deployments, as well as originally intended services, reached some technical limits and we can see a tremendous effort to correct this. Routing must be more intelligent, with quality of service consideration and 'on-demand' flavor, while the access control schemes should allow multiple technologies yet guarantying the privacy and integrity of the data. In a heavily distributed network resources, handling asset and resource for distributing computing (autonomic, cloud, on-demand) and addressing management in the next IPv6/IPv4 mixed networks require special effort for designers, equipment vendors, developers, and service providers.

The diversity of the Internet-based offered services requires a fair handling of transactions for financial applications, scalability for smart homes and ehealth/telemedicine, openness for web-based services, and protection of the private life. Different services have been developed and are going to grow based on future Internet mechanisms. Identifying the key issues and major challenges, as well as the potential solutions and the current results paves the way for future research.

We take here the opportunity to warmly thank all the members of the AFIN 2012 Technical Program Committee, as well as the numerous reviewers. The creation of such a 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 AFIN 2012. 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 AFIN 2012 organizing committee for their help in handling the logistics and for their work to make this professional meeting a success.

We hope that AFIN 2012 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in the field of future internet.

We are convinced that the participants found the event useful and communications very open. We also hope the attendees enjoyed the historic charm Rome, Italy.

AFIN 2012 Chairs:

Jun Bi, Tsinghua University, China

Eugen Borcoci, University Politehnica of Bucharest, Romania

Petre Dini, Concordia University - Montreal, Canada / China Space Agency Center - Beijing,

China

AFIN 2012

Committee

AFIN Advisory Chairs

Petre Dini, Concordia University - Montreal, Canada / China Space Agency Center - Beijing, China
Eugen Borcoci, University Politehnica of Bucharest, Romania
Jun Bi, Tsinghua University, China

AFIN 2012 Technical Program Committee

Javier A. Barria, Imperial College London, UK
Jun Bi, Tsinghua University, China
Alessandro Bogliolo, University of Urbino, Italy
Eugen Borcoci, University Politehnica of Bucharest, Romania
Christos Bouras, University of Patras and Research Academic Computer Technology Institute, Greece
Chao-Tsun Chang, Hsiuping Institute of Technology, Taiwan
Chin-Chen Chang, Feng Chia University, Taiwan
Maurizio D'Arienzo, Seconda Università di Napoli, Italy
Sagarmay Deb, Central Queensland University, Australia
Daniel Díaz-Sánchez, University Carlos III - Madrid, Spain
Sudhir Dixit, HP Labs India - Bangalore, India
Alberto Egon Schaeffer Filho, Lancaster University, UK
Florian Fankhauser, TU-Wien, Austria
Wu-Chang Feng, Portland State University, USA
Alex Galis, University College London, UK
Ivan Ganchev, University of Limerick, Ireland
Rosario G. Garroppo, Università di Pisa, Italy
Apostolos Gkamas, Higher Eccelesiastic Academy Vellas of Ioannina, Greece
William I. Grosky, University of Michigan-Dearborn, USA
Puneet Gupta, Infosys Labs, India
Dongsoo Han, Korea Advanced Institute of Science and Technology(KAIST), Korea
Gerhard Hancke, Royal Holloway, University of London, UK
Julio Hernandez-Castro, University of Portsmouth, UK
Hiroaki Higaki, Tokyo Denki University, Japan
Pin-Han Ho, University of Waterloo, Canada
Tobias Hoßfeld, University of Würzburg, Germany
Li-Ling Hung, Aletheia University, Taiwan
Jari Kellokoski, University of Jyväskylä, Finland
Changick Kim, Korea Advanced Institute of Science and Technology (KAIST) - Daejeon, Korea
Samad S. Kolahi, Unitec Institute of Technology, New Zealand
Christian Kop, Alpen-Adria-Universitaet Klagenfurt, Austria
Yi Li, VMware, Inc., USA
Maode Ma, Nanyang Technological University, Singapore

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

Content/Location Mapping with Cache-Location Resolution for In-network Guidance

Hiroki Kawabata, Kensuke Hashimoto, Tsutomu Inamoto, Yumi Takaki, Chikara Ohta, and Hisashi Tamaki
Graduate School of System Informatics, Kobe University
1-1 Rokkodai-cho, Nada-ku, Kobe 657–8501
Email: {kawabata, hashimoto, inamoto, yumi, ohta, tamaki}@al.cs.kobe-u.ac.jp

***Abstract*—In recent years, the popularity of large contents such as high-definition video and music is increasing content server loads and the amount of traffic on the backbone networks. To tackle this problem, we propose an Mapping Server with Cache-location Resolution (MSCR), which resolves prospective cache locations (PCLs) close to the requesting user as well as content server location. Sending a query to a nearby PCL enables the user to obtain the content more efficiently. Our simulation shows that MSCR can reduce content server loads and the amount of traffic on core networks.**

Keywords-mapping server; cache location; query induction; breadcrumbs; in-network cache.

I. INTRODUCTION

Nowadays, because of the increased demand for large contents such as high-definition videos and music, content servers holding popular contents suffer from high access loads, and core networks also suffer from the massive amount of traffic thus generated. More efficient content delivery is, therefore, one of the most important issues for future as well as current networks.

One traditional solution is web caching, generally content caching. In this context, a content cache means a temporary content copy (content cache) in a user terminal (local cache), content server (web accelerator), or proxy server (cache server). In web caching, if a content query happens to find the appropriate cache on the way to the content server, the content is fetched from there, which reduces content server load and the amount of traffic on core networks. Note that only content caches on the path towards the selected content server are utilized even though other content caches exist just off the path. In this sense, content caches are not utilized efficiently.

Other approaches include the Content Delivery Network (CDN) and Peer-to-Peer (P2P), which are considered as overlay networks based on the current Internet. In recent years, attempts to fundamentally overhaul the Internet architecture have been made in order to optimize it for content-delivery based on "clean slate" approaches [1], [2], [3], [4], [5]. In such "Content-Oriented Networks (CON)," how to identify content, i.e., content naming, how to locate (or find) content, and where and how to store contents are major issues.

In this paper, we propose an mapping server, named "Mapping Server withCache-location Resolution (MSCR)"; designed to utilize distributed cache storages efficiently, it resolves the locations of prospective content caches (PCL: Prospective Cache Location) as well as original servers from content name. Here, a PCL for a certain content may be a node ID or network domain ID of a user who recently got the content.

Currently, the user on-line storage service "Pogoplug" is supported [6]. If part of such storage space is open for public access, content cache storage can become more widely deployed across the network. Further, in the future, routers might actually be equipped with content cache storages (router cache) like Transparent En-Route Caches (TERC) [7], [8] and its improved version called Breadcrumbs (BC) [2]. Based on the above considerations, in this study, we assume that content cache storages are widely distributed across the network and are publically accessible. We also assume that a unique ID (content ID) is allocated to each content. In practice, by some means or another, the user needs to acquire the ID of the content desired. Currently, in order to get the URL (Uniform Resource Locator) of what we want, we most often enter keyword(s) into search engines such as google and yahoo. Some portal sites such as yahoo provide lists of contents and redirect users to actual web sites. On this occasion, they collect users' access histories. A user who accesses a certain content via such a portal site is expected to have the content, and it is also highly possible that a corresponding content cache exists near the user for some time. By using functions similar to those of search engines and portal sites, MSCR lists candidate contents that users might want to obtain by keyword(s), resolves the content ID, original server location, and PCLs of each content, and collects users' access histories. As a result, upon sending a query toward a PCL, the user can obtain the expected content; this will lessen access loads on the corresponding content server. Further, if the PCL is close to the requester, the amount of traffic On the core networks might be also reduced. In this sense, the preferred PCL is the location of a past user who is close to the current requester and who has recently accessed the content.

A concern about privacy, however, arises since it is possible for other users to discover who obtained which content. This problem, however, can be mitigated by obscuring PCLs, that is, by using network domains instead of user locations. In particular, the BC scheme is effective even in the case of dim PCLs since a query is guided on the way to the location of the past obtainer.

In this paper, we describe MSCL and conduct simulations

 ISBN: 978-1-61208-211-0

to evaluate its effectiveness from the viewpoints of content server access load and the amount of traffic on core networks. Keyword search lies outside the scope of this paper. The remainder of the paper is organized as follows: Section II-A briefly explains the BC scheme. Section III introduce MSCR and the flow of content retrieval. Section IV conducts simulations to confirm the effectiveness of MSCR. Finally, Section V concludes this paper.

II. RREDAUXILIARY SCHEME: BREADCRUMBS

In this section, we explain the Breadcrumbs scheme[2], which mitigates the privacy problem of MSCR.

A. Breadcrumbs Scheme

The Simple Best-Effort Content Search (S-BEACONS) scheme, described below, is a traditional implementation of BC [2].

In a BC scheme, like Internet Protocol (IP) scheme, a query raised by a requester for a content is transferred toward the (original) content server. Each content is assumed to be allocated a unique content ID. In the BC scheme, routers are assumed to cache not only contents but also their corresponding BCs. Both caches are assumed to have the replacement policy of Least Recently Used (LRU), which discards the least recently used item first.

A BC contains the following information:

- Content ID.
- Node ID from which the content arrived (ID of upstream node).
- Node ID to which the content was forwarded (ID of downstream node).
- Previous content transfer time: most recent time the content passed through the node.
- Previous query transfer time: most recent time the content was requested at the node.

A BC is generated in a router when a content is transferred through the router for the first time, and it is updated every time the content or a corresponding query traverses the node.

1) Query Guidance: In the BC scheme, if a query for a content traverses a router with a BC for the content, the query is diverted to the downstream node of the content which means that it backtracks along the corresponding BC trail. Suppose that a query for a content arrived at time t at a router and found that the content was not cached at the router. Then, with timeout thresholds T_{f} and T_{q}, the router forwards the query downstream if-and-only-if

- The content was cached or refreshed (via successful query) at the router within $[t - T_{\mathrm{f}}, t]$; or
- The previous query passed through the router within $[t - T_{\mathrm{q}}, t]$ and sent downstream.

2) BC Invalidation: If the query cannot find the content on the BC trail and reaches a dead end, the BC trail is regarded as being stale, and the invalidation procedure is invoked for the trail. More precisely, when the query encounters a node with its downstream entry null (i.e., dead end) and the content is not cached there, the query turns back along the trail and deletes the corresponding BCs along the trail.

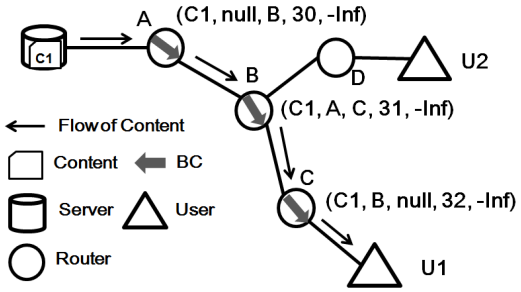


Fig. 1. BC trail and query transfer.

3) BC Update: If a content being transferred finds the corresponding BC in a router, then the BC entries, i.e., the upstream node ID, downstream node ID, and the most recent time the content passed through the node, are updated. If a query for a content finds the corresponding BC in a route, the BC entry of the previous query transfer time is updated.

4) BC Replacement: Since BC cache size is not unlimited, BCs need to have a BC cache replacement policy. In particular, core routers switch huge amounts of traffic, and their extremely rapid switching makes it difficult to provide sufficiently large BC caches. In other words, BC trails tend to frequently fail at the core routers.

5) Example of Query Guidance: Figure 1 shows an example of BC query guidance. From this figure, if content F1 is transferred via routers A, B and C and reaches user U1, BCs are newly generated on the path. Note that the entry of the previous query transfer time is set to $-\mathrm{Inf}$, and the entry of the upstream node ID in router A, to which the server is attached, and that of the downstream node in router C, to which user U1 is attached, are set to "null." The BC of each router is updated every time the content or a query traverses the router. Next, suppose that user U2 requests the same content and sends its query towards the server. It is then transferred via routers D and B and finds an available BC for the content at router B. In this case, the query is diverted downstream toward router C instead of upstream router A. If the query finds the content on the way, the content is transferred from there instead of the server. This reduces the access load of the server. On the other hand, if the query reaches router C where the downstream BC entry is "null," BCs are invalidated in the upstream direction from router C toward the server since the content is not cached on the path.

III. MAPPING SERVER WITH CACHE-LOCATION RESOLUTION

We detail MSCR in this section.

A. Basic Functions

Like search engines, MSCR resolves a list of contents by the keyword(s) that the user is interested in. The user selects one of the contents from the list, and the selection is passed to

 ISBN: 978-1-61208-211-0

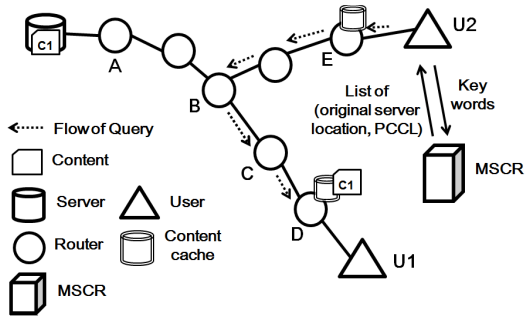


Fig. 2. Query transfer with BC and MSCR.

MSCR. MSCR then replies with the corresponding three-tuple information (content ID, original server location, PCL(s)) to the user, and, at the same time, records the user's node ID (or network domain ID) and the current time in an access history. Here, we assume that MSCR selects and replies with one (or several) proper PCL(s) although it stores multiple PCLs for each content. After getting the three-tuple information, the user sends a query towards the PCL. However, if the user fails to obtain the content desired, the user sends another query toward the original server.

In order to realize the above, MSCR stores up to N_{cont} Content/Location Mapping Information (CLMI) entries whose elements are

- Content ID,
- Original server location (Node ID),
- PCL list,
- Recent request time, and
- Access frequency,

where the PCL list consists of up to N_{PCL} two-tuple elements:

- PCL (Node IDs), and
- Access time.

Thus, MSCR stores information about N_{cont} contents, and up to $N_{\mathrm{cont}}N_{\mathrm{PCL}}$ PCLs. "Recent request time" and "access frequency" are used as the cache replacement policy as mentioned in Section III-B.

Let us explain the above procedure using Figure 2. In this figure, we consider the case that there is only one MSCR in the network, and only access routers have content cache stores.

As a precondition, it is assumed that no node has a content cache and MSCR knows only the original server location of each content, i.e., not PCLs. Furthermore, user U1 sent keyword(s) to MSCR and chose content C1. At that time, MSCR replid (C1's content ID, C1's original server location, null) to user U1 since it had no PCL for content C1. At the same time, MSCR recorded U1's node ID with the access time as a PCL for content C1, and counted up the access frequency for content C1. After getting the information, user U1 sent a query toward the server, got content C1 over path route A through D, and a copy of content C1 was newly cached at access router D.

Next, user U2 also requests content C1. At this time, since MSCR already holds the PCL for content C1 (i.e., user U1's node ID), user U2 obtains a PCL (i.e., U1 node ID) as well as the original server for content C1 from MSCR. To start with, user U2 sends a query toward the PCL (i.e., user U1), and obtains content C1 from router D. Further, a new copy of content C1 is stored at access router E.

B. PCL Replacement

In this study, we assume that an MSCR can have up to N_{cont} CLMIs, each of which can have up to N_{PCL} PCLs since MSCR cannot store unlimited quantities of CLMI. Thus, replacement policies for CLMI and PCL are necessary.

Generally speaking, more popular contents place heavier loads on the content server and core network, since they are more frequently requested. Thus it is better to store their information. In this sense, LFU (Least Frequently Used) is preferable as the CLMI replacement policy.

On the other hand, with PCL, stale information may lead to cache miss since content caches themselves are also replaced. In other words, the newer the PCL is, the better it is. Therefore, LRU (Least Recently Used) is preferable as the PCL replacement policy.

C. PCL Activation Delay

Just because a user gets a reply from MSCR does not mean that the content has already been cached anywhere. This is because there is a delay from when the user sends the query to when at least one copy of the content is cached. To make sure that a user has already obtained a content, and thus the content is cached, the user notifies the completion of content receipt to MSCR. This, however, increases control overhead and the amount of traffic. The simplest and least burdensome way is for MSCR to activate a PCL after some delay even to the cost of certainty.

D. PCL Selection

MSCR stores multiple PCLs in a CLMI for a certain content. Recall that, for a requester, a newer PCL and a closer PCL are more effective in reducing content server access load and the amount of traffic on core networks, respectively. Thus, from the requester's viewpoint, some PCLs are more effective than others. Thus, it is important which and how many PCLs should be returned to the user.

If a requester has routing information, he/she can probably decide which PCL is close to himself/herself more easily than MSCR. In this case, it is simplest for MSCR to return all PCLs to the requester. This, however, increases the amount of control traffic. If MSCR is to judge the closeness between a requester and a PCL, it needs to hold some sort of information on network topology. This is possible if network domain IDs are hierarchically allocated, as assumed in Section IV. Under this assumption, the closeness between two nodes can be roughly estimated. This approach means that the MSCR need return only a few PCLs to the requester.

 ISBN: 978-1-61208-211-0

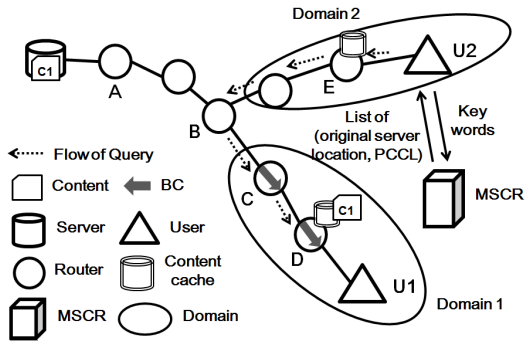


Fig. 3. Query transfer with BC and MSCR.

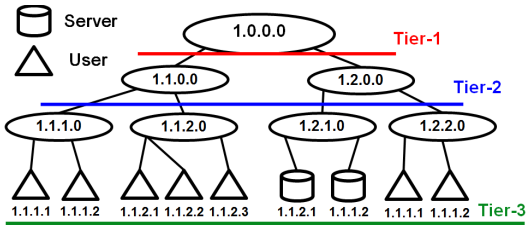


Fig. 4. Example of 3-Tier router topology.

E. Privacy

As mentioned in Section I, privacy concerns arise since other users can know who obtained which content. This concern can be mitigated if MSCR returns network domain IDs instead of user node IDs as PCLs. A query issued toward a PCL, however, may not be able to find any content cache from just the network domain ID. In such a case, in-network guidance by the BC scheme is effective, especially if network domain IDs are hierarchically allocated.

Figure 3 shows an example with in-network guidance by the BC scheme. This figure is almost the same as Figure 2 except that all routers are BC routers and network domain IDs are used as PCLs. Note that, as in Figure 2, only access routers have a content cache storage. As preconditions, we assume that just after user U1 obtained content C1 from the server, a BC trail was established from the server to user U1, and BCs on routers A through B on the trail have been pushed out due to BC cache replacement as mentioned in Section II-A4.

At this point, suppose that, for the request from user U2, MSCR returns the network domain ID of domain 1 as a PCL in addition to the original server location for content C1. Then a query is sent toward domain 1. At the entrance of domain 1, the query happens to find the fragment of the BC trail to router D which has the content cache of the content C1. Note that we assume that a query to find a corresponding BC trail is always guided along the trail. Thus, even vague information on cache location is still useful if in-network guidance by the BC scheme is applied.

F. Unique Content ID

Each content needs to be indexed uniquely, i.e., assigned a unique content ID. For example, a fixed length content ID can be generated by a hash function from the content itself or its URL. A content is at first uploaded to a particular content server and its URL is the only one piece of information related to the content at that time. So when a content is uploaded for the first time, we generate a hash from its URL which uniquely identifies the content thereafter.

G. Implementation

In the above examples, a single MSCR is used. In practice, however, such a centralized system is vulnerable and not scalable. In order to enhance dependability and scalability, we consider that MSCR should be implemented as a distributed system like Chord[9] which utilizes Distributed Hash Tables (DHTs). In our case, CLMI entries will be distributed to multiple servers, which will mitigate vulnerability and enhance scalability. Implementing MSCR in a distributed manner like Chord is left for future work, and in this paper, we evaluate the effectiveness of the basic MSCR function.

IV. Performance Evaluation

In this section, we evaluate how much MSCR can reduce the content server load and the amount of traffic on the core network. To do so, we developed an event-driven simulator in C++. In what follows, we compare four schemes from the viewpoints of cache hit ratio (ratio of the number of contents obtained from caches to that of totally obtained contents) and the amount of traffic in the tier-1 network:

- IP
- IP + Cache
- IP + Cache + MSCR
- IP + Cache + MSCR + BC

In the above, “IP” means that a user fetches a content from its content server as per the server/client model of basic IP networks. “Cache” means that access routers have content caches. If “MSCR” is stated, an mapping server resolves a PCL as well as the original server location. Otherwise, it resolves only a content server from a content name. “BC” means that every router has the BC function and only access routes have content caches.

A. Assumptions

In our simulations, we used 3-tier router topologies, which were created by combining multiple Transit-Stub (TS) topologies (i.e., 2-tier topologies), which are generated by gt-itm [10]. More precisely, in a 3-tier topology, tier-1 corresponds to a transit domain of a certain TS-topology, whose stub domains are replaced by transit domains of other distinct TS-topologies, so that their stub domains become tier-3 domains. Here, we removed links between the routers in the different tier-2 domains (originally set between the routers in different transit domains on the TS-topology). Figure 4 shows an instance of such a 3-tier topology. In this paper, a tier-1 domain is regarded as a core network in a 3-tier topology.

Each node is allocated a sixteen-digit hex node ID separated at every fourth-digit by periods, i.e., “0123.4567.89ab.cdef,” so

 ISBN: 978-1-61208-211-0

TABLE I
GENERAL PARAMETERS.

Item	Value
Link capacity	1 packet/unit time
Number of contents	10,000
Number of tier-1 domains / routers per domain	3 / 3
Number of tier-2 domains / routers per domain	9 / 8
Number of tier-3 domains / routers per domain	144 / 15
Number of servers	50
Number of users	5,000
Query size	1 packet
Content size	100 packets
Content cache size	10
Content cache replacement policy	LRU

that node ID is represented by 64 bits. Node IDs are organized hierarchically to express tier level. That is, the first four-digits express tier-1, the second tier-2, the third tier-3, and the fourth is allocated to a content server or a user. As a result, as shown in Figure 4, all tier-2s have the same first four-digits in their node IDs, and all tier-3s under a certain tier-2 have the same first eight-digits in their node IDs. This kind of address allocation can be realized by HANA (Hierarchical Automatic Locator Number Allocation Protocol) [11]. Here, let us denote the distance between two nodes whose node IDs are I_i and I_j by

$$D(I_i, I_j) = 64 - L(I_i, I_j), \quad (1)$$

where $L(I_i, I_j)$ is the size of the longest prefix match between two node IDs.

In addition to the above, we assume the following: As shown in Figure 4, content servers are located in a particular tier-3 domain, called "server domain," that is, they are connected to routers in the server domain, while users are sited randomly in the other tier-3 domains. All routers are equipped with BC caches, while only access routes that accommodate users have content caches, since routers in the backbone networks (tier-1 and 2 domains) are expected to have a paucity of high-speed memory even in the future;

The query occurrence interval of each user follows an exponential distribution; Content selection follows a Zipf-like distribution with $\alpha = 0.75$ [12]; Queries and contents are transferred without any packet loss; This time, as we focus on cache hit ratio and amount of tier-1 traffic, not the retrieval delay, each link between nodes is assumed to have capacity sufficient to transfer one packet in each unit time (including a delay for packet processing at routers). Table I summarizes the parameters used in the simulations. With regard to BC parameters, we assume that each router can store up to 50 BC entries in a BC cache, and its cache policy is LRU; the timeout thresholds of BC are set to $T_{\rm f} = 3,000$ and $T_{\rm q} = 300$. Table II summarizes the BC parameters used in the simulations. With MSCR, we assume that only one MSCR exists in a 3-tier network. In the case of content/location resolution, MSCR selects one of the nearest (and newer) PCL as well as original server location. In our simulations, PCL is specified by user node ID. MSCR holds up to 100 CLMI entries, and each has up to 30 PCLs for a certain content. In PCL entries, prospective locations are replaced as per LRU policy, and CLMI entries are replaced as per LFU policy. Table III shows the basic MSCR parameters used in the simulations.

TABLE II
BC PARAMETERS.

Item	Value
BC cache size per router	50
BC cache replacement policy	LRU
$T_{\rm f}$	3,000 unit time
$T_{\rm q}$	3,00 unit time

TABLE III
MSCR PARAMETERS.

Item	Value
PCL metric	Network distance
PCL selector	MSCR
Number of returning PCLs	1
Number of total PCLs	3,000
Max. CLMI, $N_{\rm cont}$	100
CLMI replacement policy	LFU
Max. PCL per CLMI, $N_{\rm PCL}$	30
PCL replacement policy	LRU

TABLE IV
CACHE HIT RATIO AND
RELATIVE AMOUNT OF TIER 1 TRAFFIC IN IP SCHEME.

Scheme	Cache hit ratio	Relative amount of tier 1 traffic ratio
IP	0	100
IP + Cache	1.4	98.8
IP + Cache + MSCR	7.4	94.0
IP + Cache + MSCR + BC	13.0	90.2

B. Simulation Results and Discussions

Table IV show the cache hit ratio and the amount of tier-1 traffic relative to that in IP scheme. From the table, we can see that MSCR increases the cache hit ratio (i.e., decreases content server access load) and decreases the amount of tier-1 traffic compared with the IP and IP + Cache scheme. This is because MSCR enables users to more effectively utilize content cache storages at access routers other than their own. Moreover, combining the BC scheme with MSCR increases the cache hit ratio and decreases the amount of tier-1 traffic even more. This is because the BC scheme can guide a query for a content whose PCL has not been stored yet in MSCR to a cache.

In the simulation scenario, MSCR is expected to increase the cache hit ratio and decrease the amount of tier-1 traffic by nearly 21.9%. MSCR holds one hundred CLMIs under the LFU replacement policy. That is MSCR tends to store PCLs of the first through the 100th most popular contents, which accounts for 21.6% of content requests given the Zipf-like distribution. If a content cache pointed by a PCL surely exists

 ISBN: 978-1-61208-211-0

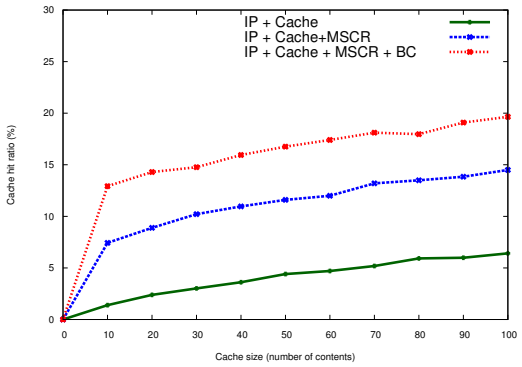


Fig. 5. Characteristics of cache hit ratio as a function of content cache size.

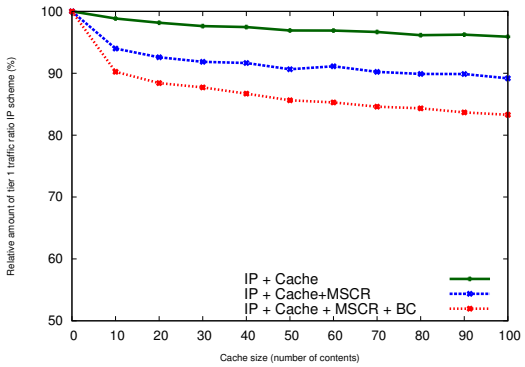


Fig. 6. Characteristics of the amount of tier 1 traffic relative to that of IP scheme as a function of contencache size.

somewhere, the cache hit ratio can be almost 21.6%, which reduces the amount of tier-1 traffic to the same degree.

The reason of relatively poor performance is explained as follows. The content cache policy is LRU, and all users demand contents according to the same, static, Zipf-like distribution. As a result, popular and similar content caches occupy the cache spaces distributed across the network, which are less diversified. This implies that the effective number of PCLs is restricted to basically the content cache size of each access router.

To verify this, we varied the content cache size of each access router from 10 to 100. Figures 5 and 6 show the cache hit ratio and the amount of tier-1 traffic, respectively. In those figures, we can see that the cache hit ratio and the relative amount of tier-1 traffic approach to the expected values as content cache size increases.

In practice, users in different domains are expected to have different preferences due to locality. In this sense, the simulation scenario that content requests must follow the same and static Zipf-like distribution is an overly-stringent condition for MSCR. This can be alleviated by increasing the diversity of content caches among content cache spaces, which could be achieved by cooperative caching between MSCR and the content cache. This is left for future work.

V. Conclusion and Future Work

In this paper, we proposed MSCR that resolves content ID, original server location, and PCL(s) in order to reduce the content server load and the amount of traffic on core networks. Simulation results showed that MSCR is effective in achieving both goals. In our simulations, all users have the same and static preference, i.e., a Zipf-like distribution, for contents, and there is no cooperation between MSCR and the content cache policy. As a result, similar contents are cached in each tier-3 domain. In this sense, it is not so significant for MSCR to guide a query to a different tier-3 domain. In practice, however, preferences will be quite different in different domains due to locality, and will vary over time. In such cases, we expect that MSCR will be even more effective. Verifying this is one of our future works. Moreover, we also investigate establishing cooperation between MSCR and content cache policy.

Acknowledgement

We would like to express our deepest gratitude to Prof. Jim Kurose and Mr. Elisha Rosensweig who provided valuable comments and suggestions. We gratefully appreciate the financial support of Information and Communications Technology (NICT), Japan.

References

[1] J. Choi, J. Han, and E. Cho, “A Survey on Content-Oriented Networking for Efficient Content Delivery,” IEEE Communications Magazine, pp. 121–127, March 2011.

[2] E. J. Rosensweig and J. Kurose, “Breadcrumbs: Efficient, Best-Effort Content Location in Cache Networks,” Proc. IEEE INFOCOM 2009, pp. 2631–2635, April 2009.

[3] I. Stoica, D. Adkins, S. Zhunang, and S. Shenker, “Internet Indirection Infrastructure,” IEEE/ACM Trans. on Networking, vol. 12, no. 2, pp. 205-218, April 2004.

[4] V. Jacobson, D. KSmetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, “Networking Named Content,” Proc. ACM CoNEXT 2009, Rome, Italy, Dec. 2009.

[5] T. Koponen, M. Chawla, B. C. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, “A Data-Oriented (and Beyond) Network Architecture,” Proc. ACM SIGCOMM 2007, Kyoto, Japan, pp. 181–192, August 2007.

[6] “Pogoplug,” https://pogoplug.com/, April 2nd, 2012 (last accessed).

[7] P. Krishnan, D. Raz, and Y. Shavit, “The Cache Location Problem,” IEEE/ACM Trans. on Networking, vol. 8, no. 5, pp. 568–582, Oct. 2000.

[8] S. Paul, R. Yates, D. Raychaudhuri, and J. Kurose, “The cache-and-forward network architecture for efficent mobile content delivery services in the future internet,” Proc. Innovations in NGN: Future Network and Services 2008, K-INGN 2008, pp. 367–374, May 2008.

[9] I. Stoica, R .Morris, D. Karger, M. F. Kaashek, and H. Balakrishnan, “Chord: A scalable peer-to-peer lookup service for internet applications,” ACM SIGCOMM Computer Communications Review, vol. 31, no. 4, pp. 149–160, Oct. 2001.

[10] “gt-itm,” http://www.cc.gatech.edu/projects/gtitm/, April 2nd, 2012 (last accessed).

[11] F. Fujikawa, H. Harai, and M. Ohta, “The basic procedures of hierarchical automatic locator number allocation protocol HANA,” Proc. the 7th Asian Internet Engineering Conference (AINTEC) 2011, pp. 121–131, Nov. 2011.

[12] L. Breslau, P. Cao, L. Fan, G. Phillips, and S. Shenker, “Web Caching and Zipf-like Distributions: Evidence and Implications,” Proc. IEEE INFOCOM 1999, pp. 126–134, March 1999.

 ISBN: 978-1-61208-211-0

The Forwarding on Gates Architecture: Merging IntServ and DiffServ

Florian Liers, Thomas Volkert, Andreas Mitschele-Thiel
Integrated Communication Systems Group
Technical University of Ilmenau
Ilmenau, Germany
e-mail: {Florian.Liers, Thomas.Volkert, Mitsch}@tu-ilmenau.de

***Abstract*—Quality of Service (QoS) will be a major enabler for Future Internet applications and services. However, today's Internet provides no suitable QoS support for end-to-end connections due to several drawbacks of IntServ and DiffServ. Therefore, this paper proposes the "Forwarding on Gates" architecture, which uses a new network protocol designed to handle IntServ and DiffServ in an integrated way. The architecture supports resource reservations for QoS guarantees, like in IntServ scenarios, and prioritized traffic, like in DiffServ scenarios. Furthermore, a combination of both is supported. This paper introduces the architecture and defines the network protocol used to implement these features. The evaluation includes theoretical descriptions of the network configuration for the different scenarios and simulation results concerning the protocol overhead in large-scale networks. Our new architecture is able to support QoS in a scalable way, since it allows a network providing QoS to move states and delegate decisions about the QoS usage to the entity using the QoS.**

***Keywords*—Future Internet; network protocol; architecture; QoS.**

I. INTRODUCTION

The Future Internet will be faced with much more applications requiring Quality of Service (QoS). Among the first, Internet video streaming is already stressing today's Internet. Forecasts predict that in 2015 about 62% of the traffic will be video [1]. For live video streams, as required for remote medical operations or for football games, QoS is required. Due to the large number of end hosts on the Internet and the large number of connections between them, scalability is a major concern of QoS provisioning.

IP only provides a best effort service. Therefore, IntServ and DiffServ were developed to handle QoS on the Internet. However, both have pros and cons. The IntServ approach [2] with its signaling protocol RSVP provides end-to-end QoS by introducing states in each intermediate router a flow passes through. According to [3], the Resource Reservation Protocol (RSVP) has to handle states for classification, scheduling and signaling. The classification states define how incoming packets are mapped to flows. With RSVP, such a state consists of a source address, a destination address and a protocol number (and optionally port numbers). Scheduling states define how flows are handled. For example, a flow can be mapped to the queue of an outgoing hardware interface with a priority for a scheduler. Finally, signaling states represent management information like authentication information and timers. For each flow, an intermediate node requires one set of these states. Due to memory limitations, such an approach causes scalability problems for scenarios with many flows [4].

DiffServ [5] aims at solving the scalability issue by introducing a small set of QoS classes used inside networks. Each QoS class defines a type of service and requires scheduling and signaling states. Thus, the number of states does not depend on the number of connections. However, DiffServ is not able to provide guarantees, since it is not aware of each individual flow. Edge routers of a network contain the classification states of a DiffServ network, in order to map incoming packets to the internal QoS classes. The classification states represent the rules for this mapping. Since most interfaces with incoming traffic will transport multiplexed flows, like multiple TCP connections over one Ethernet link, the classification is mainly done by (more or less deep) packet inspection. For example, port numbers or packet sizes can be used for classification.

IntServ and DiffServ can be combined to leverage the advantages of both approaches. IntServ provides the signaling for flows between ingress routers and DiffServ provides a set of QoS classes used inside networks [6, 7]. However, the scalability problem of IntServ now appears at the ingress routers. They have to store classification states per flow. Since the number of scheduling and signaling states remains limited due to the DiffServ classes, the classification states are the main problem. In order to maintain the states, signaling is required. The processing load of handling these messages increase the burden on a network. In the past, proposals focused on reducing the number of flows, e.g., through aggregation [3].

Our key contribution is the proposal of an orthogonal strategy: move the classification states away from ingress routers to routers handling smaller amounts of flows. Furthermore, some decision-making authority is delegated from the QoS provider to the entity using QoS in order to reduce the required signaling overhead. As discussed in more detail in Section IV, today's network protocol IP is not able to support both in all use cases. Therefore, this paper presents a new network protocol enabling the movement of classification states and the delegation of decisions between routers. Our solution is suitable for IntServ and DiffServ scenarios and is able to handle combinations of both. Its main feature is the flexible placement of the classification states according to the network graph and the load in the

 ISBN: 978-1-61208-211-0

system. It enables the handling of both QoS approaches in a single mechanism.

The remainder of this paper is structured as follows: Section II describes our system architecture. Section III introduces the protocol and how its header is processed. Afterwards, in Section IV, the implementation of the use cases based on our architecture and protocol are presented. Section V shows evaluation results from a protocol simulation. Section VI discusses related work. In the end, the main results of this work are summarized and an outlook to future work is given.

II. FORWARDING ON GATES ARCHITECTURE

The "Forwarding on Gates" (FoG) architecture splits forwarding and routing into two logical components. Both encapsulate specific tasks. The forwarding component is responsible for relaying packets between routers and hosts. It handles the resource management and enforcement of resource reservations in order to take non-functional properties such as delay and bandwidth into account. The routing component is responsible for calculating paths through the network with respect to non-functional requirements given by applications [8]. Both are linked via a route definition. The routing component specifies a route and the forwarding component forwards packets along the route. The authentication component is the third logical component of FoG. It checks the authentication of signaling messages in order to secure access to the management functions. The authentication is the basis for authorization decisions and accounting of QoS. In this paper, we use the term *flow* in a more abstract manner than *connection*. However, a flow can be a connection between end hosts.

For the following discussion, we introduce the term *QoS function*, which generalizes QoS provisioning regardless of the QoS architecture. A QoS function represents the setup required to send packets with QoS constraints. Examples of QoS functions are setups implementing a DiffServ class or an IntServ reservation. QoS functions can provide guarantees ranging from "hard" with fixed limits over "soft" with probabilistic QoS guarantees to vague goals like "optimized for delay" or "best-effort". A QoS function comprises its scheduling and signaling states. The classification states are not included.

In addition to the separation of routing and forwarding [9], our architecture has some more features. Examples are reduced forwarding table size [10], enabling routers to choose their address format [11], enabling applications to specify their requirements [8], hiding addresses from applications and support for various intra-network techniques. However, they are shared with other approaches from literature and are not the focus of this paper.

A. Forwarding Component

Today's Internet operates over interfaces of routers and hosts and links in between. FoG's forwarding component uses a virtual representation of the network, which has the form of a graph. Host and routers are represented by one or more vertices, which are called *forwarding nodes*. Edges between forwarding nodes are called *gates* and represent uni-directional links between them. In order to support QoS, multiple edges between adjacent nodes are allowed. An edge is equivalent to a link with a QoS function between two routers or hosts. Each outgoing gate of a forwarding node is assigned a *gate number*, which is unique in the scope of this forwarding node. Each FoG packet has a header, which contains the order of gates to pass through explicitly. Details about the route and how the forwarding node processes it are given in Section III.

Gates are set up with a FoG-specific management protocol. The forwarding nodes process the signaling messages of that protocol and modify the graph of forwarding nodes and gates as requested. In order to secure this management, signaling messages are signed via the authentication service by the sender. The receiver uses the authentication service to verify the signature.

The forwarding component informs the routing component about available gates and forwarding nodes to enable route calculations based on them. However, gates not intended for other flows can be hidden in order to exclude them from the routing calculations.

B. Routing Component

The routing component is responsible for route calculations based on the information received from the forwarding component. Based on a starting forwarding node and a destination address, it calculates a route through the graph of gates and forwarding nodes. QoS requirements serve as constrains for the calculation. If all gates to the destination are known, an explicit route is the result. If some gates are not known, the route is only a partial one. A partial route contains the destination address or the address of an intermediate node. During the forwarding process, the missing part of the route will be calculated based on this address.

In common scenarios, the subset known to a routing instance is a connected graph, which represents the "area" of the network itself and its surroundings. The knowledge about the parts outside of this subset is more abstract. A routing component knows about the connectivity but does not know the gate numbers required to specify the route explicitly. This is comparable with the situation known from the Border Gateway Protocol (BGP). A BGP entity knows about the existence of a route (and its cost) but does not know the outgoing ports of the intermediate routers which have to be used.

If there are insufficient gates to form an end-to-end route, a routing component can request the setup of new gates by a forwarding component. In particular, routing components can request gates with specific QoS capabilities in order to satisfy the QoS requirements of a particular route request.

 ISBN: 978-1-61208-211-0

C. Authentication Component

The authentication component is used to generate signatures for signaling messages and to check such signatures. Based on the authentication check, authorization decisions and accounting are done. It is mainly used by the forwarding component to secure gate management. Furthermore, applications can use the authentication in order to sign data packets. Thus, the authentication has an impact on the packet structure described in the next section. However, due to the QoS focus of this paper, the authentication component is not described in more detail.

III. NETWORK PROTOCOL AND ITS PROCESSING

The FoG packet structure is shown in Figure 1. It starts with a header comprising all information required to decide the next hop. This enables a router to make a forwarding decision before the packet is fully received. The packet ends with a trailer containing all information that can be added to a packet after receiving it completely. The trailer is optional and can be omitted. The header and trailer elements are defined as follows:

- Header
  - Length of the header in bytes: This field is required to access the payload as subsequent versions of the FoG protocol can add new header fields between the header fields defined in this paper and the payload.
  - Flag field which indicates
    - if the reverse route in the trailer is present,
    - if the packet is a signaling message, and
    - if the authentication information in the trailer is present.
  - Modification counter to prevent routing loops due to invalid gate setups
  - Length of the payload in bytes
  - Forward route for the packet
- Trailer
  - Length of the authentication information in bytes
  - Authentication information itself
  - Revers route for answers

Each route starts with a length field followed by a stack of route segments. There are two types of segments:

- The explicit route segment is a stack of gate numbers, defining explicitly a sequence of gates to travel through.

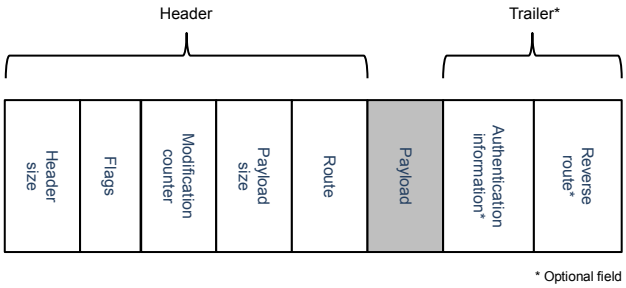


Figure 1. FoG protocol packet structure.

- The destination route segment contains a destination name or address and the requirements for the remaining route to this destination.

Each forwarding node processes the route of a packet as shown in Figure 2. If the route is empty, the packet has reached its destination. If the signaling flag is set, the packet contains signaling information dealing with the setup of gates and connection establishment between applications. The signaling message is handled by the host or router, and it updates the gate and forwarding node graph accordingly. If the signaling flag is not set and the forwarding node has a socket attached to it, it removes the FoG header and trailer and stores the payload in the receive buffer of the socket. If the route is not empty, the forwarding node processes the topmost segment. If it is an explicit route segment, it removes the topmost gate number and uses it to lookup one of its outgoing gates. If there is an outgoing gate with this gate number, the packet is handed over to this gate for further processing. If the explicit route segment is empty, it is removed from the route and the procedure restarts. If the topmost segment is a destination segment, the forwarding node has to contact the routing component in order to get the next explicit route segment.

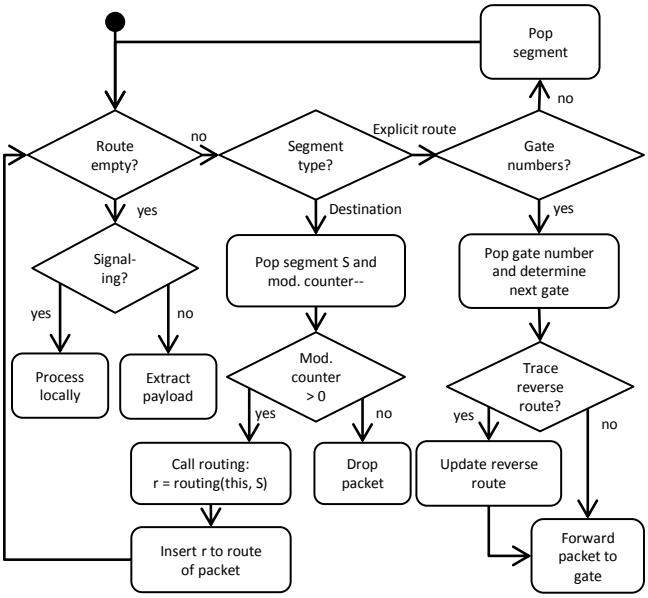


Figure 2. Forwarding node procedure without error cases.

The routing component calculates a route from the forwarding node to the destination. The requirements given in the destination segment are used as requirements for the route. The route returned by the routing component is added to the route of the packet and the procedure is restarted.

The modification counter is decremented if the route is changed in a way that loops might occur. It is used to avoid routing loops.

The reverse route of a packet is recorded if the reverse route flag in the packet header is set. A forwarding node has to derive the reverse gate number from the gate chosen for the forward direction. The reverse route does not need to be symmetric to the forward route. Furthermore, an intermediate forwarding node, which is not able or allowed to record the reverse route using explicit route segments, can insert a destination segment to the reverse route. The reverse route can be used by the receiver of a packet to reply to the sender. The main benefit of using the reverse route instead of an address is twofold. First, routing requests for reply packets are avoided and second, addresses for sending nodes are not required. The latter is useful for hosts acting only as clients. A server can reply by using the reverse route without forcing the client to have an address. If a reply with a traced backward route is received by a client, it knows the route the request packet has traveled. In most cases, this route contains less destination segments and more explicit route segments. Therefore, the client can use this route for subsequent packets in order to reduce the routing overhead and the delay for its packets.

The destination segment is not necessarily the last segment in a route. As shown by the use cases in the next section, it might define only an intermediate node of the route, due to missing knowledge about gate numbers. Theoretically, multiple destination segments in one route are possible, which would emulate loose source routing. Due to security considerations [12], policies might restrict that.

IV. USE CASES

Based on the FoG architecture and its network protocol, we will now investigate three different use cases showing the provisioning of QoS functions ranging from IntServ to DiffServ to a combination of both. For simplicity, the same example network is used in each case. Only the gate setup and the responsibility for the classification states (CS) differ.

Figure 3 and 4 show three networks with network 3 providing QoS functions in the form of gates to network 1 and 2. Gates are depicted as straight lines between the forwarding nodes (FN_i), which are shown as dots. The dotted lines represent connectivity through some other network, where the gate numbers are not known. Known gate numbers are depicted with small letters. Each network has not only the forwarding component but also the routing component as defined by the architecture. It is depicted as an extra box with its known components inside.

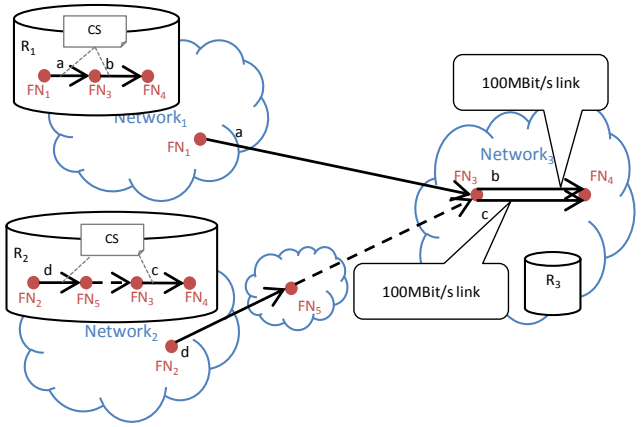


Figure 3. Gates representing IntServ reservations.

A. IntServ gates

In Figure 3, networks 1 and 2 have requested QoS functions from network 3. Network 3 has set up one gate for each request and network 1 and 2 have informed their routing component about these gates. For example, each gate represents a (virtual) link providing 100 MBit/s. The router, which is represented by FN_3, has to store the scheduling and signaling states required to provide and enforce these QoS functions. However, the classification states are not stored by FN_3 but have been moved to network 1 and 2, respectively. Their routing components know about gates *b* and *c*, respectively, and handle the decision about which flows are mapped to these gates.

If network 1 would like to establish a flow, the entity responsible for flow creation (e.g. one of the control nodes or the network edge) starts sending a signaling message with a route, which just contains a destination segment with the address of the destination and the requirements for the route, e.g., a minimum bandwidth of 10 MBit/s. In this example, the destination is FN_4. The packet with the route [[address(FN_4)]] is inserted into the forwarding component FN_1, which proceeds as described in Section III. Since the topmost segment of the route is a destination segment, it contacts the routing component R_1. In the given case, R_1 knows a route with all gate numbers to the destination. We assume that R_1 did not map too many flows on these gates and that therefore there is enough remaining capacity. R_1 maps this new flow on the gates *a* and *b* and updates its classification states. It returns the route [[*a*, *b*]] containing only one explicit route segment. FN_1 removes the destination segment from the packet and inserts this new route into the route field in the packet. FN_1 restarts the procedure with the explicit route segment as topmost segment. It pops the gate number *a* from the gate number stack and looks it up in its list of outgoing gates. Then, it hands over the packet to gate *a*. The gate transports the packet to the next hop via a link layer, e.g., Ethernet. The packet arrives at FN_3 with the route [[*b*]]. It pops *b* from the stack and hands over the packet to gate *b*. FN_4 receives the packet with an empty route and processes the packet locally.

 ISBN: 978-1-61208-211-0

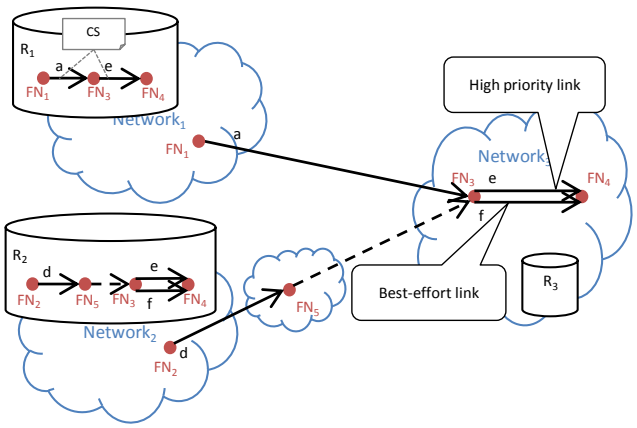


Figure 4. Gates representing DiffServ classes.

For network 2, the process is similar. However, there is a difference in the route required to reach FN_3. R_2 calculates a route with three route segments: [[*d*], [address(FN_3)], [*c*]]. In contrast to the route calculated by network 1, one more request to the routing component has to be done. FN_5 receives a packet with [address(FN_3)] as topmost segment, which triggers the remaining route request.

B. DiffServ gates

In Figure 4, network 3 provides one gate with a high priority and a best effort gate with a low priority. The latter is included in the scenario to demonstrate the integration of non-QoS links in FoG. The routing components of network 1 and 2 have slightly different views on this situation. R_1 only knows about *e* and R_2 knows about both *e* and *f*. The reason might be that R_1 decided to omit *f* or network 1 did not request a best-effort gate from network 3. Moreover, R_1 and R_2 have different strategies for tracking the flows mapped to these gates. R_1 stores the classification states as in the previous scenario. However, the criterion for using gate *e* differs. Instead of bandwidth as in the previous example, R_1 might use a cost metric (e.g. money to pay to network 3) to decide which flow is important enough to justify the usage of gate *e*. R_2 does not limit the usage of gate *e* nor *f* and does not store any classification states.

The routes calculated are similar to the previous scenario. The main difference is in the policy for selecting gates in R_1 and R_2. In addition to the previous scenario, R_2 shows the benefit of knowing a broader set of gates available for a link. Depending on the requirements for a route, R_2 can decide to use *e* or *f*. For example, it can return the route [[*d*], [address(FN3)], [*f*]] for flows with no QoS requirements. Gate *e* can be used by R_2 without having to signal to FN_3. Furthermore, FN_3 does not have to know the details about flows and can just follow the gate numbers given in a packet. This reduces the load of the router providing FN_3.

C. Combined scenario

Both gate types can be combined in a single scenario. Such a scenario can be constructed by merging the two scenarios shown before. This combined scenario has four gates between FN_3 and FN_4 representing different QoS functions. In such a scenario, R_1 would have two options (since it does not know all gates) for a route from FN_3 to FN_4:

- Gate *b*: The usage is limited by bandwidth already reserved by R_1 for other flows. Through proper management of R_1, a minimal bandwidth can be guaranteed.
- Gate *e*: The usage is limited by the cost network 1 is willing to pay for a flow (if it is charged by network 3). A certain amount of bandwidth cannot be guaranteed. However, the delay is minimized.

Which gate to choose, depends mainly on the requirements for a flow and the requesting entity.

D. Discussion

Neither network 1 nor network 2 knows about the techniques used by network 3 to provide the QoS. These implementation issues are hidden by the abstract gate description for the routing and by the gate number used for the forwarding.

In all scenarios, FN_3 does not store any classification states and does not know which flows are mapped to its gates by network 1 and 2. It delegated the decision to these networks. However, the states required to enforce the characteristics of the gates remain in network 3. Thus, even though network 3 does not know which and how many flows are mapped to a gate, it can enforce that the combined traffic does not use better QoS than requested. Another benefit of this delegation is reduced signaling overhead. In particular, no signaling messages from network 1 or 2 are required to inform FN_3 about a new mapping.

The routes calculated by network 2 show an important case, which is not supported by MPLS and IP today. While the route [[*d*], [address(FN_3)]] can be implemented with MPLS handling the explicit route segment and IP handling the destination segment, a subsequent explicit route segment ([*c*] in the example) is not directly supported. In IP, the ingress router doing the IP forwarding has to have some classification states, which link a packet to the subsequent explicit route segment. However, FoG moves this state to other routers and thus reduces the number of states to be maintained by the ingress router.

The main use case of FoG consists of a network that would like to sell some degree of QoS to its customers (its own end users and other networks). Thus, deploying FoG in order to implement a best effort network provides only limited advantages compared to IP. However, the degree of deployment is critical for QoS scenarios, too. The delegation of states and decisions cannot be done only by network 3, since it requires the support of network 1 and 2. Consequently, a partial deployment in today's Internet might not benefit from these two features. However, the more networks support FoG, the better the exploitation of the advantages. A migration strategy for introducing FoG to existing networks depends mainly on the legacy systems, which should be supported. For example, MPLS might be

 ISBN: 978-1-61208-211-0

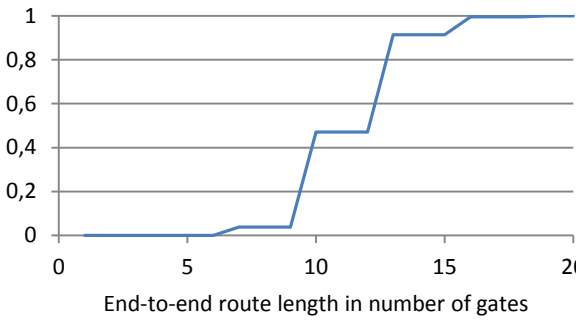


Figure 5. CDF of route lengths for scenario with 5000 nodes.

integrated by representing LSP as gates. However, suitable migration strategies are a subject for future work.

V. IMPLEMENTATION & SIMULATION RESULTS

We have implemented the FoG architecture in a Java-based discrete event simulator. It can be switched to an emulator mode that handles events in real time. The FoG emulator includes interoperability solutions combining FoG and IP based networks [13]. FoG applications specify their QoS requirements directly via an interface and FoG reacts accordingly. The interface bases on the GAPI defined in [8].

For evaluating FoG in the context of QoS management, the route length of explicit route segments is a specific concern. The more hops a packet has to travel, the more gate numbers are required and the longer the header. In order to estimate the FoG protocol overhead, the length of explicit routes for large-scale scenarios has been analyzed.

The network used for evaluation should match the characteristics of today's Internet but be smaller in size in order to reduce simulation time. Therefore, the network has been generated with the GLP algorithm implemented in BRITE [14] and the parameters derived in [15]. Therefore, the graph has similar characteristics to the real world Internet graph on the autonomous system level. The scenario consists of 5000 nodes and 12437 links between them. In addition, a different graph generated with the default parameters of BRITE (5000 nodes and 8974 links) was used for simulation. Since the results do not differ significantly, only the results from the first graph are presented.

The analysis is based on the total explicit route lengths of 6000 connections between randomly chosen FoG nodes. Figure 5 shows the cumulative distribution function of route lengths. Since each intermediate node uses three gate numbers and each end node uses two gate numbers in order to encode its routing decision, only specific route lengths such as 4 and 7 are possible. An end-to-end route contains 12.1 gate numbers in average. If each gate number is encoded in one byte, 91% of all routes remain below the size of an IPv6 address. The average number of hops between two FoG nodes $L = 3.7$ matches the expectations for the Internet [16].

VI. RELATED WORK

QoS for networks has a long research history. A survey about today's approaches is given in [17]. As discussed in the introduction, IntServ [2] and DiffServ [5] can be used to provide QoS. However, they do not support the movement of states.

MPLS uses routes comparable to the explicit route segment. In combination with IP, some use cases can be supported. However, Section IV.D points out important cases where the combination of IP and MPLS does not allow the movement of classification states. Furthermore, FoG does not require a standardization of gate numbers as required for IP's TOS field values in an inter-network scenario [18].

Other forwarding approaches using a stack of locally valid numbers to describe routes, like PARIS [19], Sirpent [20] or Pathlet [10], already introduce the split between forwarding and routing. In PFRI [9] the numbers are even globally unique in order to enable the end host to specify a loose source route based on links. An entry in a forwarding table represents virtual [10] or physical [21] next hops. Some (esp. the older) approaches are more related to intra-networks. Pathlet [10], the newest one, deals specifically with policy issues in inter-network routing. However, QoS and other application requirement aspects are not discussed in detail. Only Pathlet [10] mentions QoS but does not describe any details about how to integrate IntServ and DiffServ and a network protocol.

QoS protocols, like RSVP or NSIS [22] are able to signal QoS requirements. Either of these protocols or similar approaches are suitable to signal the setup of gates.

Other proposals for new inter-network architectures focus more on the overall architecture and do not address scalability of state information, e.g., NewArch [23], IPC [11], RNA [24].

VII. CONCLUSION AND OUTLOOK

In this paper, we have presented the Future Internet architecture "Forwarding on Gates" (FoG). It uses a network protocol, which provides the capability to explicitly define a route, use the destination address plus requirements for a route or a combination of both. This enables the movement of classification states between routers. IntServ and DiffServ are merged by introducing QoS functions, which are represented by directed gates in the FoG architecture. Routes can be defined by using the gates without knowing about their implementation. The protocol enables the flexibility to move classification states from the router implementing a QoS function to other routers, which take over the mapping of flows to QoS functions. This delegation of the mapping decisions reduces the amount of required signaling messages.

Based on three use cases, the setup of gates in IntServ, DiffServ and mixed scenarios is described. Although the route length is dynamic, the protocol overhead remains low. A protocol simulation in a large-scale network with 5000

 ISBN: 978-1-61208-211-0

nodes showed that 91% of the routes are shorter than an IPv6 address. The results presented in this paper show the flexibility of FoG in providing QoS in a scalable way. It indicates that the FoG architecture seems to be a promising basis for a Future Internet.

In the future, we plan to develop deployment and migration strategies from today's network to FoG. Furthermore, we will use route repair techniques known from MPLS to evaluate the robustness of FoG routes against link and node failures.

ACKNOWLEDGMENT

This work is funded by the German Federal Ministry of Education and Research under the project G-Lab_FoG (code 01BK0935). The project is part of the German Lab [25] research initiative.

REFERENCES

[1] Cisco Systems, "Cisco Visual Networking Index: Forecast and Methodology, 2010–2015", white paper, 2011, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf [retreived: July 2012].

[2] R. Braden, D. Clark, and S. Shenker, "Integrated Services in the Internet Architecture: an Overview," IETF, RFC 1633, June 1994.

[3] C. Deleuze and Serge Fdida, "A scalable IntServ architecture through RSVP aggregation," Networking and Information Systems Journal, vol. 2, 1999, no. 5-6, pp. 665-681.

[4] B. E. Carpenter and K. Nichols, "Differentiated service in the Internet," Proc. IEEE, vol. 90, no. 9, pp.1479-1494 , 2002.

[5] S. Blake et al., "An Architecture for Differentiated Services," IETF RFC 2475, Dec. 1998.

[6] Y. Bernet et al., "A Framework for Integrated Services Operation over DiffServ Networks," IETF RFC 2998, Nov. 2000.

[7] X. Masip-Bruin et al., "The EuQoS System: A solution for QoS Routing in Heterogeneous Networks," IEEE Communications Magazine, Vol.45 No.2, pp. 96-103, February 2007.

[8] F. Liers, et al., "GAPI: A G-Lab Application-to-Network Interface," 11th Würzburg Workshop on IP: Joint ITG and Euro-NF Workshop "Visions of Future Generation Networks" (EuroView2011) , Würzburg Germany, August 2011.

[9] K. L. Calvert, J. Griffioen, and L. Poutievski, "Separating Routing and Forwarding: A Clean-Slate Network Layer Design," In proceedings of the Broadnets 2007 Conference, pp. 261-270, September 2007.

[10] P. B. Godfey, I. Ganichev, S. Shenker, and I. Stoica, "Pathlet Routing," In proceedings of SIGCOMM 2009, pp. 111-122 August 2009.

[11] J. Day, I. Matta, and K. Mattar, "Networking is IPC: A Guiding Principle to a Better Internet," In Proceedings of ReArch'08, Article no. 67, Madrid, Spain, December 2008.

[12] A. Reitzel, "Deprecation of Source Routing Options in IPv4, IETF," Internet-Draft, August 29, 2007.

[13] F. Liers, T. Volkert, and A. Mitschele-Thiel, "Scalable Network Support for Application Requirements with Forwarding on Gates," Demo at 11th Würzburg Workshop on IP: Joint ITG and Euro-NF Workshop "Visions of Future Generation Networks" (EuroView2011) , Würzburg Germany, August 2011.

[14] A. Medina, A. Lakhina, I. Matta, and J. Byers, "BRITE: an approach to universal topology generation," In IEEE MASCOTS, pp. 346–353, Cincinnati, OH, USA, August 2001.

[15] H. Haddadi, D. Fay, S. Uhlig, A.W. Moore, R. Mortier, A. Jamakovic, and M. Rio, "Tuning Topology Generators Using Spectral Distributions," In proceedings of SIPEW, pp.154-173, 2008.

[16] CAIDA, "Comparative analysis of the Internet AS-level topologies extracted from different data sources," http://www.caida.org/~dima/pub/as-topo-comparisons.pdf [retreived: July 2012].

[17] D. Vali, S. Paskalis, L. Merakos, and A. Kaloxylos, "A Survey of Internet QoS Signaling," IEEE Communications Surveys & Tutorials, Volume 6, Fourth Quarter, pp. 32-43, 2004.

[18] Cisco Systems, "Implementing Quality of Service Policies with DSCP," http://www.cisco.com/application/pdf/paws/10103/dscpvalues.pdf [retreived: July 2012].

[19] Israel Cidon and I. S. Gopal, "PARIS: An approach to integrated high-speed private networks," International Journal of Digital ans Analog Cable Systems, pp. 77-85, 1988.

[20] D. R. Cheriton, "Sirpent: a high-performance internetworking approach," In proceedings of ACM SIGCOMM '89: Symposium proceedings on Communications architectures & protocols, pp. 158-169, 1989.

[21] H. T. Kaur, S. Kalyanaraman, A. Weiss, S. Kanwar, and A. Gandhi, "BANANAS: An evolutionary framework for explicit and multipath routing in the Internet." In Proc. ACM SIGCOMM 2003, pp. 277-288, FDNA Workshop, Aug. 2003.

[22] R. Hancock et al., "Next Steps in Signaling (NSIS): Framework," IETF, RFC4080, Jun 2005.

[23] D. Clark, K. Sollins, J. Wrolawski, D. Katabi, J. Kulik, X. Yang, R. Braden, T. Faber, A. Falk, V. Pingali, M. Handley, and N. Chiappa, "NewArch: Future Generation Internet Architecture," Technical Report, 2003, http://www.isi.edu/newarch/iDOCS/final.finalreport.pdf [retreived January 2012].

[24] J. Touch and V. Pingali, "The RNA Metaprotocol," Proc. IEEE International Conf. on Computer Comm. (ICCCN), pp. 1-6, Aug. 2008.

[25] German Lab Homepage, http://www.german-lab.de [retreived: July 2012].

 ISBN: 978-1-61208-211-0

Finding Betweenness in Dense Unweighted Graphs

Brandeis Marshall and Anuya Ghanekar
Computer and information Technology
Purdue University
West Lafayette, IN 47907 USA
{brandeis, aghanek}@purdue.edu

***Abstract*—Social network analysis (SNA) aims to identify and better determine the relationship amongst data in a graph representation.The interpretation of several core SNA measures, *degree*, *closeness* and *betweenness* centrality of a node, have been the subject of extensive research in recent years. We concentrate on the betweenness property, which seeks to determine the relatedness of more than 2 nodes. We propose our *betweenness in unweighted graph* algorithm and compare it to the k-path centrality algorithm on two image collections. By design, our proposed algorithm is less restrictive with the ability to consider any subset of nodes for betweenness. Our findings also show our proposed algorithm has a much shorter execution time as compared to the k-path centrality algorithm.**

***Keywords*-social network analysis; betweenness centrality; social networking graph model.**

I. Introduction

In an effort to deal with the large amount of data being generated in science, research and personally, data models, frameworks and algorithms are designed to reveal information connections that will result in useful knowledge. In many contexts, data remains disjointed with a one-dimensional slice of information. Data duplication and inconsistency are common concerns leading to a lack of confidence in the quality of data. A comprehensive view of information, leading to knowledge, can be obtained using a collection of semi-relevant and overlapping data slices. The ultimate aim is in providing knowledge which allows the end-user to have more confidence in making informed decisions. These measures can be applied in various fields like bioinformatics, image retrieval and supply chain management.

To achieve this goal, social network analysis (SNA) have been used in recent years to find connections amongst data using a graphical representation. Given that search and sort methods are at the center of SNA, the data quality and information flow are assessed through novel implementations of the *degree*, *closeness* and *betweenness* centrality of a node methods, which effectively navigates a social network. The degree algorithm focuses on popularity and frequency of a particular node. The closeness algorithm concentrates on pairwise relationships. The betweenness algorithm considers the relationships amongst more than two nodes.

For this paper, we examine the challenge of applying betweenness in isolating image tags' relatedness, typically used in image search. With the surge of digital photography, image search and retrieval is a complex area of research. Image search and retrieval usually fall into one of two main approaches: content-based image retrieval (CBIR) or image annotation/tagging. At the core, CBIR methods use numerical values while image tagging uses keywords and word phrases to represent an image. However, both methods have their obstacles. CBIR can be time-consuming due to the need for extensive image processing. Image tagging can be error-prone due to lack of reliable verification and validation of manual and (semi-) automated labeling.

According to the prior work on image search and retrieval, image tagging has become the popular choice due to its ease-of-use factor and reduced requirement of computing resources as compared to CBIR approaches. We therefore concentrate on the image tagging approach. We discover that image search and retrieval is a very complex in social networks. Each image is represented as a set of connected tags. When these images are transposed to a graph, we have a multigraph structure. We seek to navigate an image collection's multigraph in order to efficiently determine its betweenness connectivity. High betweenness connectivity depicts that the node has a high impact on the other nodes. We show examples of images and their associated tags in Figure 1. We make the following contributions:

- we present the *betweenness in unweighted graph* algorithm and
- we compare it to the state-of-the-art k-path centrality algorithm on 2 common image datasets, MIRFLICKR and ImageCLEF.

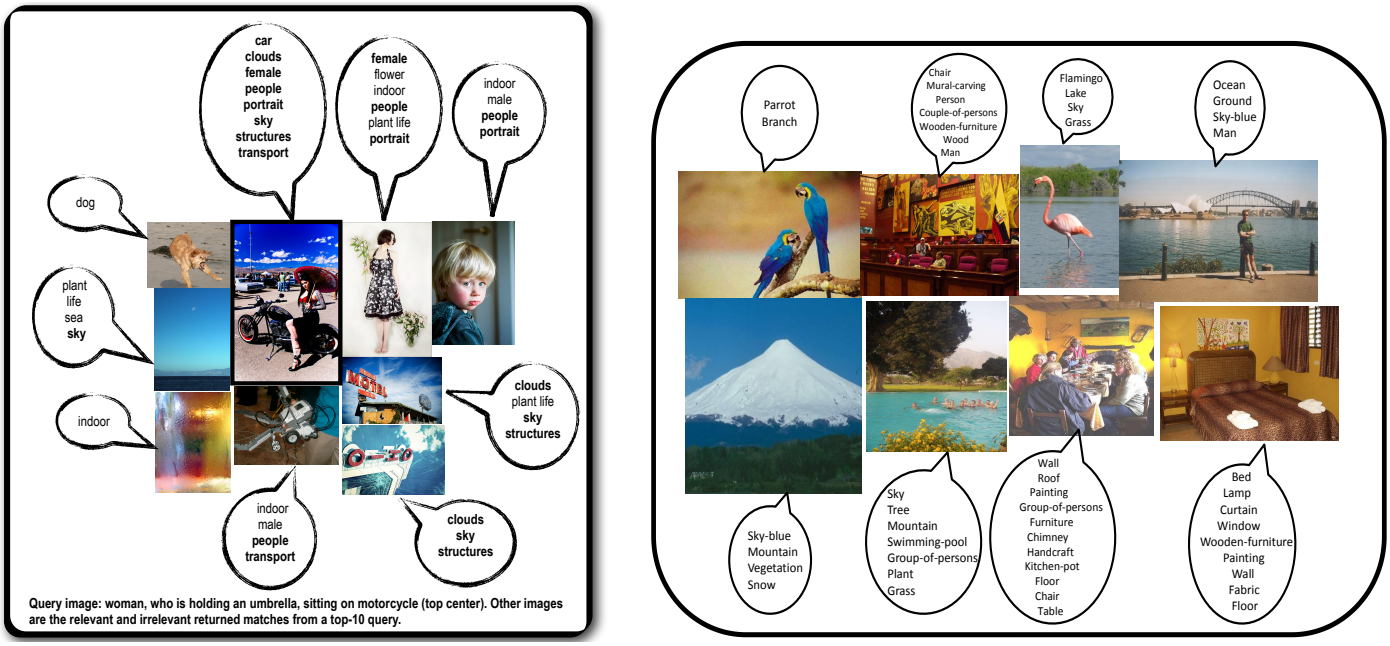
Section 2 discusses the related work for betweenness property in terms of algorithm design, experimental setup and datasets. Section 3 describes the betweenness property and proposes our algorithm for calculating betweenness in unweighted graphs. Section 4 demonstrates the experiments performed on BUG and K-path centrality algorithms. We conclude and summarize the paper in Section 5.

II. Related Work

In developing an efficient and effective betweenness algorithm, we must compare prior work [1], [2], [14] with regard to competitive algorithm design and experimental evaluation e.g., experimental setup and datasets.

a) Algorithm Design: Using the K-path centrality algorithm [1], every node selects another node to pass the information to, at random, depending on the weights of the edges and the nodes that have already been visited. It assumes message traversals only along simple paths and of a maximum

 ISBN: 978-1-61208-211-0



(a) Sample MIRFLICKR images with corresponding tags

(b) Sample ImageCLEF images with corresponding tags

Fig. 1: MIRFLICKR and ImageCLEF sample data

length k. The algorithm runs in time $O(k^3 n^{2-2\alpha} \log n)$, where k is the path length, n is the number of nodes. An adaptive sampling algorithm [2] is presented for betweenness centrality. It selects a subset of vertices and performs shortest path computations and then varies the number of samples based on the information obtained from each sample. This algorithm outputs the centrality of all vertices. Okamoto et al. [14] presents an algorithm to determine the top-k vertices by combining the exact and approximate algorithms. Hence, unlike the previous two algorithms, this algorithm is used to determine the k vertices that have the highest centrality, with some error. This algorithm takes $O((k + n^{2/3}. \log^{1/3} n)(n \log n + m))$.

b) Experimental Setup: Alakahoon et al. compare the k-path centrality algorithm with the Brandes [3], RA-Brandes [4] and AS-Brandes [2] algorithms. The experiments show that the k-path centrality algorithm can scale up easily to large networks. The near optimal performance of k-path in both correlation and speedup performance metrics can be achieved when its parameters are set to α = 0.2 and k =ln$(n + m)$, where n and m are the number of nodes and the number of edges in the network respectively.

Bader et al.'s experiments demonstrate that the estimated centrality scores are very close to the exact ones and also reduce the computation time by a factor of nearly 20. They also show that the error variance is within acceptable bounds. The experiments also show the graphs for number of samples/SSSP computations as a fraction of n to depict the amount of work done by the approximation algorithm. Since Okamoto et al. only consider the top-k elements, the computation time is considerably reduced if one is interested only in determining the highly ranked nodes instead of the actual centrality values of all the nodes.

c) Datasets: The scalability of the algorithms are a concern. Bader et al. uses 6 real world graph instances (4 undirected, 2 directed graphs) where the number of vertices varies from 2000 to 9914 and the number of edges varies from 4,435 to 41,601. On the other hand, Alakahoon et al. uses 7 real networks with the number of vertices varying from 2,424 to 82,168 and the number of edges varies from 13,354 to 948,464. Three of these networks use directed graphs while the others use undirected graphs. The edges are unweighted in all the networks except one.

III. Betweenness Property

The betweenness property has its roots in social network analysis theory [8], which considers the use of nodes on a path between a particular source and sink node. A betweenness method is usually costly, especially in complex networks [2], [6]. In addition to betweenness, social network analysis also proposes degree and closeness properties as methods to better understand how data are connected in a graph. In general, data has a semi-structured configuration, including data duplication and naming inconsistency obstacles, led to the need for explicitly and implicitly leveraging relationships within the data. Given the heterogeneous nature of today's data, the challenge is harnessing these data needs across architectures, operating systems and devices.

In prior work, the Social Network Graph (SNG) model [10], [11], [12] aims to integrate a more inclusive data model for incorporating all forms of data from multiple and diverse sources. Currently, SNG has an emphasis on representing personal images and their corresponding annotations. Tagging can be daunting; hence, semi-automated annotation approaches [5], [16] are typically employed. We make use of SNG in identifying a set of attributes, *(who, what, when, how,*

 ISBN: 978-1-61208-211-0

where), for an image. Other researchers do not consider this more comprehensive view of an image. For instance, Rattenburg et al. [15] considers "where" the photograph was taken, "what" is occasion at which it was taken and the association between objects of "how" they are related. Golder [7] focuses on images with people and, as a result, infers the picture-taker's social relationships.

SNG's construction consists of a collection of multi graphs, in which each image is represented by a clique connecting the image's tags. At the core of most betweenness algorithm implementations is a shortest path method. The methods differ with regard to graph size, number of edges and, most importantly, navigational techniques. We will describe a state-of-the-art betweenness algorithm proposed by Alakahoon et al., which we will compare to our proposed method in the Experimental Evaluation section.

A. K-Path Centrality Algorithm.

This algorithm attempts to introduce the k-path centrality, which can efficiently compute randomized centrality with accurate results even for a large network. By discovering a way to compute the centrality effectively, the various graphs can be analyzed to determine the effect of one node on another. It aims at reducing the computation time by making two assumptions - consider only simple path (no repetition of nodes) and maximum path length is k (dependent on the network). By using these assumptions, the complexity is greatly reduced as the k-path centrality gives an accurate and quick result for betweenness.

The pseudocode of this method is given as follows: it takes as input a graph G = (V,E), a non-negative weight function on the edges of G, and parameters $\alpha \in$ [-1/2,1/2] and integer κ = f(m,n) where m are the number of edges and n is the number of nodes in the graph. Lines 16-21 compute the sum count[v] that a message originating from all possible source nodes s, goes through v, assuming that message traversal are only along random simple paths of at most κ edges. To compute this, a vertex is chosen randomly such that it has not been visited and an edge exists between the vertex and s, with a probability proportional to the weight of the edge. This sum is used to calculate the centrality in lines 27-29.

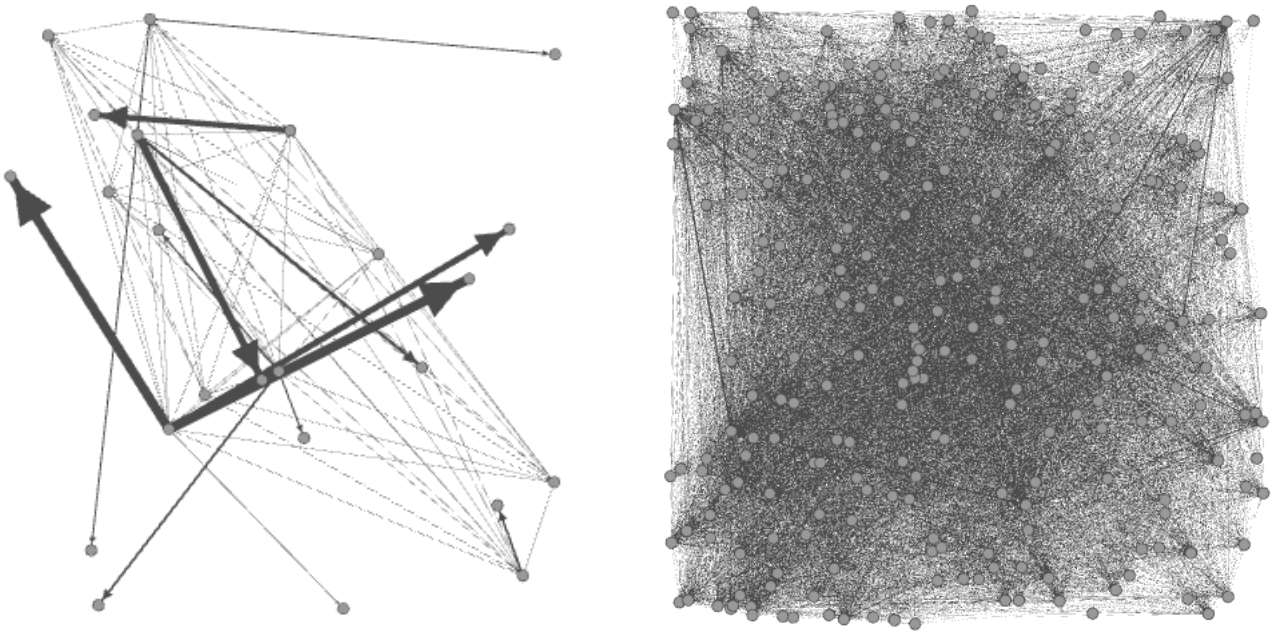
```
1: function kpathcentrality(graph:G(V, E), array:W, int:k)
2: output Array C_k of k-path centrality estimates
3: N = number of vertices
4: α ∈ [-1/2, 1/2]
5: for v = 1 to N do
6:    count[v]=0
7:    explored[v] = false
8: end
9: /* S is a stack */
10: T ← 2k^2 n^{1−2α} ln n ; S ← ∅
11: for i = 1 to T do
12:    /* simulate message traversal from s containing l edges */
13:    s ← a vertex chosen uniformly at random from V;
14:    l ← an integer chosen uniformly at random from [1,k];
15:    explored[s] ← true; push s to S; j ← 1;
16:    while j ≤ l and ∃(s, u) ∈ E s.t. !explored[u] do
17:       v ← a vertex chosen randomly from { u | (s, u) ∈ E
          and !explored[u] } with probability proportional to
          1/W (s,v);
18:       explored[v] ← true; push v to S;
19:       count[v] ← count[v] + 1;
20:       s ← v; j ← j+1;
21:    end
22:    /* reinitialize explored[v] to false */
23:    while S is nonempty do
24:       pop v ← S; explored[v] ← false
25:    end
26: end
27: for v = 1 to N do
28:    C_k[v] ← kn . (count[v]/T);
29: end
30: return C_k;
31: end
```

B. Betweenness in Unweighted Graphs (BUG) Algorithm.

We propose a betweenness method that is best-suited for unweighted dense graphs. We leverage the nearest neighbor relationship SNG nodes and edges. Below we provide our BUG pseudocode that makes execution calls to our closeness method [12]. In our closeness algorithm, we implement Dijkstra's algorithm (beginning at line 8) to find the shortest search path from source node v_i to the target node v_j. Given that our edges are not weighted, we implement a randomized K Nearest neighbor (KNN) to select the neighboring unseen node.

```
1: function closeness(graph: SNG, object: v_i, object: v_j)
2: for object v_y ∈ SNG do
3:    e(v_i, v_y) = ∞ // Unknown distance function from
      source v_i to v_y
4:    prev(v_y) = null // Previous node in optimal path from
      source
5: e(v_i, v_i) = 0
6: Q = all vertices V ∈ SNG
7: v_curr = v_i
8: while Q ≠ null OR reach v_j do
9:    object v_close = KNN(e(v_curr, v_u))
10:   if e(v_curr, v_close) = ∞ then
11:      break
12:   remove v_close from Q
13:   for each neighbor v_n of v_close do
14:      alt = e(v_curr, v_close) + e(v_close, v_n)
15:      if alt < e(v_close, v_n) then
16:         prev(v_n) = v_close
17:         v_curr = v_n
18:         break for-loop
19: return prev
```

Our BUG algorithm first computes the closeness between each node-pair and stores each path in an adjacency matrix (line 3-6). Then, we construct the final path from $v_1, \ldots, v_n$ by identifying when (or if) path overlap occurs (line 9-22). We divide the path overlap into three categories: (1) path 1



(a) MIRFLICKR dataset with 24 nodes and 31,000+ edges (b) ImageCLEF dataset with 258 nodes and 970,000+ edges

Fig. 2: Visual Representation of MIRFLICKR and ImageCLEF Datasets

and path 2 overlap in path 1 with the node at the beginning of path 2, (2) path 1 and path 2 overlap with path 1 connecting to a substring of path 2, and (3) path 1 and path 2 are disjoint, which results in a union of both paths.

1: **function** BUG(graph:SNG,objects:$\{v_1, \ldots, v_n\}$)
2: $pmatrix[n][n] = \infty$ // stores the path between each node-pair
3: **for** $i = v_1$ to v_{n-1} **do**
4: **for** $k = v_2$ to v_n **do**
5: $path_{ik}$ = closeness(i , k , SNG)
6: $pmatrix[i][k] = path_{ik}$
7: $fpath = \infty$
8: $l = v_1$
9: **while** $l \neq v_n$ **do**
10: $path_l = pmatrix[l][l+1]$
11: $path_{l+1} = pmatrix[l+1][l+2]$
12: **for** $j = 1$ to r **do**
13: **for** $m = 1$ to s **do**
14: **if** $path_l.get(j) = path_{l+1}.get(m)$ AND $m = 1$ **then**
15: $pmatrix[l][l+2] = path_l.substring(1, j) \cup pmatrix[l+1][l+2]$
16: boolean flag=true
17: break
18: **else**
19: $pmatrix[l][l+2] = pmatrix[l][l+1] \cup path_{l+1}.substring(m, end)$
20: boolean flag=true
21: break
22: **if** flag = false **then**
23: $pmatrix[l][l+2] = path_l \cup path_{l+1}$
24: $fpath.append(pmatrix[l][l+2])$
25: l+=2
26: return $fpath$

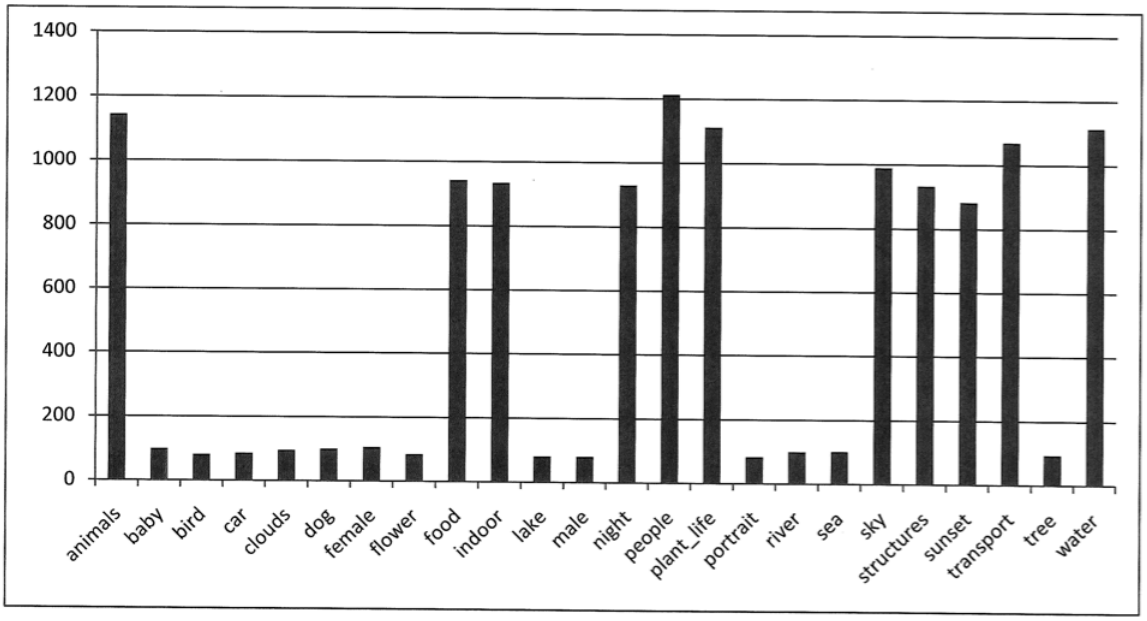
IV. Experimental Evaluation

In this section, we describe the experimental results of our BUG methods with that of the k-path centrality method. To perform a more balanced comparison, we test these methods on two datasets: MIRFLICKR-25000 [9] and ImageCLEF Segmented and Annotated IAPR TC-12 [13]. One MIRFLICKR collection consists of 25,000 images downloaded from the social photography site Flickr through its public API. With only 24 annotations, this dataset is very dense having a large number of edges between any two annotations e.g., 'baby' is labeled in 259 images and 'people' is labeled in 10,373 images. MIRFLICKR annotations are arranged in a shallow hierarchical structure of general topic and sub topic categories. The ImageCLEF SAIAPR TC-12 dataset contains segmentation masks and segmented images for 20,000 images and organized in a more complex conceptual hierarchical structure with 258 annotations.

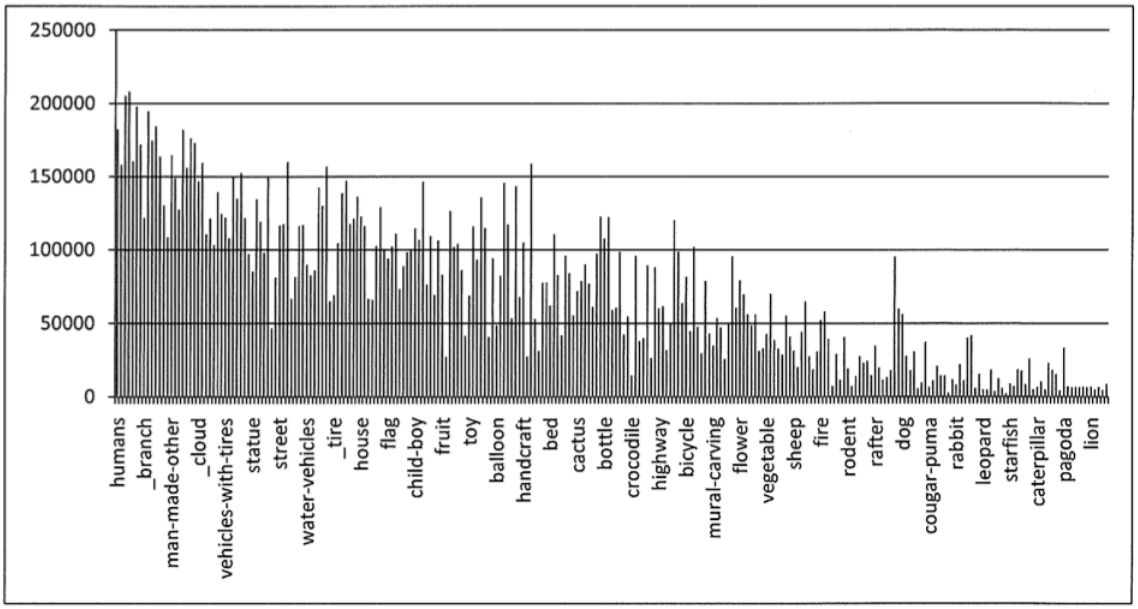
In Figure 2, we display the visual representation of both datasets using Gephi, an open source graph visualization and manipulation software (https://gephi.org). The edge thickness correlates to the frequency of connection between two nodes. We load each dataset into our SNG model, forming a clique of the tags (nodes) for each image. Our MIRFLICKR dataset has only 68 unique edges while the ImageCLEF dataset has 19,509 unique edges.

For our experiments, we execute tests which compare the run times of the k-path centrality and our proposed algorithms on both image datasets. In Figure 3, we display the run time of each tag's betweenness assessment for the MIRFLICKR

 ISBN: 978-1-61208-211-0



(a) MIRFLICKR dataset



(b) ImageCLEF dataset

Fig. 3: K-Path Centrality Results, when K=3

and ImageCLEF collections e.g., x-axis denotes the image tags and y-axis denotes the time in milliseconds. The time on y-axis indicates the average time required to find the shortest path between a node and other pairs of nodes. Each collection's hierarchical structure is revealed by the length of the run time in which image tags located at or near the tree leaves are accessed less frequently. Based on the design of the k-path centrality algorithm, the betweenness evaluation is conducted for each image tag as shown in Figure 3. Our BUG algorithm, on the other hand, first identifies which image tags are of interest and then computes their betweenness. Hence, BUG considers the binomial coefficient in which we find the betweenness of a set of nodes while the k-path centrality focuses in the information-theoretic aspect in which the information flow through a node is assessed. The k-path centrality finds a path only of length k whereas the BUG algorithm finds the shortest path between nodes without any restriction on the path length. The k path algorithm maintains a list of visited nodes and hence requires more overhead. BUG does not require such tracking of these details.

Below we show a path samples from both datasets:

- MIRFLICKR
  - BUG(baby, car, flower) has path baby $\rightarrow$ people $\rightarrow$ transport $\rightarrow$ car $\rightarrow$ plant_life $\rightarrow$ flower and takes 19 ms.
  - BUG(car, lake, tree) has path car $\rightarrow$ transport $\rightarrow$

water → lake → plant_life → tree and takes 7 ms.
  - BUG(clouds, flower, portrait) has path clouds → sky → plant_life → flower → people → portrait and takes 13 ms.
- ImageCLEF
  - BUG(fabric, cloth, _flock-of-birds) has path fabric → cloth → humans → _flock-of-birds and takes 406 ms.
  - BUG(glass, deer, hedgehog-porcupine) has path glass → _ground → deer → landscape-nature → hedgehog-porcupine and takes 558 ms.
  - BUG(diver, beetle, elephant) has path diver → beetle → animal → elephant and takes 415 ms.

These samples showcase the shortest path planning route given each collection's hierarchical structure. The betweenness assessment for the selected three image tags is not a simple and direct path. For instance, the image tags, *baby, car, flower*, are all child nodes within this MIRFLICKR collection with parent nodes *people, transport* and *plant_life*, respectively.

	K-Path Centrality	BUG
MIRFLICKR	519.39 ms	**10.55** ms
ImageCLEF	71678.87 ms	**776.93** ms

TABLE I: Run Time Averages

Table I shows the average execution times for each algorithm-dataset pair. We set k-path centrality parameter $k = 3$ denoting a 3NN information flow. We implement our BUG algorithm with $n = 3$ denoting that we are finding the relatedness of 3 image tags by not setting a restriction on K within the KNN. The BUG algorithm takes a fraction of the run time than that of k-path centrality. In addition, the BUG algorithm generates the path of any number of objects even when the objects do not have a direct edge between them.

V. Conclusion & Future Work

We propose our betweenness algorithm, that is designed for a dense multigraph environment. We performed an experimental evaluation using an MIRFLICKR 25,000 image collection and an ImageCLEF 20,000 image collection, in which we compared our proposed method to the k-path centrality method. Our findings show that the proposed algorithm executed in a fraction of the run time than the k-path centrality method. Additionally, our proposed method is designed with a less restrictive interpretation of betweenness as the shortest path including any subset of nodes is produced. In the future, we plan to work on a weighted closeness and betweenness for larger image datasets, including the MIRFLICKR 1M collection. We would like to better incorporate information theory principles in these methods and assess its impact in a large-scale data environment.

References

[1] T. Alahakoon, R. Tripathi, N. Kourtellis, R. Simha, and A. Iamnitchi. K-path centrality: A new centrality measure in social networks. In *Proceedings of the ACM Workshop on Social Network Systems*, page Article 1, 2011.

[2] D. A. Bader, S. Kintali, K. Madduri, and M. Mihail. Approximating betweenness centrality. In *Proceedings of the ACM international conference on Algorithms and models for the web-graph*, pages 124–137, 2007.

[3] U. Brandes. A faster algorithm for betweenness centrality. *The Journal of mathematical sociology*, 25(2):163–177, 2001.

[4] U. Brandes and C. Pich. Centrality estimation in large networks. *The Journal of Bifurcation and Chaos*, 17(7):2303–2318, 2007.

[5] H.-M. Chen, C. Ming-Hsiu, P.-C. Chang, M.-C. Tien, W. H. Hsu, and J.-L. Wu. Sheepdog - group and tag recommendation for flickr photos by automatic search-based learning. In *ACM Multimedia*, pages 737–740, 2008.

[6] S. Dolev, Y. Elovici, and R. Puzis. Routing betweenness centrality. *The Journal of the ACM*, 57(4), 2010.

[7] S. Golder. Measuring social networks with digital photograph collections. In *Proceedings of the ACM conference on Hypertext and hypermedia (HT)*, pages 43–48, 2008.

[8] R. A. Hanneman and M. Riddle. *Introduction to social network methods*. http://www.faculty.ucr.edu/∼hanneman/nettext/, 2005.

[9] M. J. Huiskes, B. Thomee, and M. S. Lew. New trends and ideas in visual concept detection: The mir flickr retrieval evaluation initiative. In *MIR '10: Proceedings of the 2010 ACM International Conference on Multimedia Information Retrieval*, pages 527–536, New York, NY, USA, 2010. ACM.

[10] B. Marshall. Taking the tags with you: Digital photograph provenance. In *Proceedings of the IEEE International Symposium on Data, Privacy, & E-Commerce*, pages 72–77, 2010.

[11] B. Marshall. Context seeking with social tags. In *Proceedings of the ACM International Conference on Knowledge Management Workshop Exploiting Semantic Annotations for Information Retrieval*, pages 11–12, 2011.

[12] B. Marshall and S. Pandey. Using the social networking graph for image organization. In *Proceedings of the International Conference on Advances in Future Internet*, pages 102–107, 2010.

[13] H. Mller, P. Clough, T. Deselaers, and B. Caputo. *Experimental Evaluation in Visual Information Retrieval*. The Information Retrieval Series - Springer, 2010.

[14] K. Okamoto, W. Chen, and X.-Y. Li. Ranking of closeness centrality for large-scale social networks. In *Proceedings of the ACM International Workshop on Frontiers in Algorithmics*, pages 186–195, 2008.

[15] T. Rattenburg, N. Good, and M. Naaman. Towards automatic extraction of event and place semantics from flickr tags. In *Proceedings of the ACM SIGIR Conference on Research and development in information retrieval*, pages 103–110, 2007.

[16] B. Sigurbhornsson and R. van Zwoi. Flickr tag recommendation based on collective knowledge. In *Proceedings of ACM WWW*, pages 327–226, 2008.

 ISBN: 978-1-61208-211-0

VoIP Systems Management using Internet Protocol Detail Records

Luis H. Gibeli, Gean D. Breda, Bruno B. Zarpelão, Rodrigo S. Miani, Liniquer K. Vieira, Leonardo de S. Mendes
School of Electrical and Computer Engineering
University of Campinas (UNICAMP)
Campinas – SP - Brazil
{ l044877, gean, bzarpe, rsmiani, liniquer, lmendes} @decom.fee.unicamp.br

***Abstract*—The increasing demand for latency sensitive services through the Internet imposes the development of networks capable of delivering quality of service. These networks require the use of enhanced traffic management tools. This paper performs an analysis of IP telephony or VoIP traffic considering Internet Protocol Detail Record (IPDRs). When a VoIP call occurs upon the Internet, a ticket (a file record) is generated to produce information regarding that specific call. These files are called Internet Protocol Detail Record. The IPDR, which is generated for every VoIP call, contains information related to the history of the call. The full set of information in the IPDRs carries a very comprehensive description of what happened to the call and can provide valuable information about the state of the network during the history of the call. Therefore, IPDRs can be used to establish network traffic baselines. This paper presents the development of a baseline that supports VoIP traffic management in Open Access MANs. Our main conclusion is that this method can be used to manage VoIP networks.**

Keywords-Voice Over Internet Protocol; Network Management; Open Access Metropolitan Area Networks; IPDR.

I. INTRODUCTION

As of the mid 90's, with the steady evolution of technologies, the telecommunications networks have become more and more complex, being capable of bearing multiple services. These services a

re part of a heterogeneous set of pieces of information which can be sent through the Internet, for instance, the telephone calls. In telephony companies, the voice transmission has been migrating from the classic telephony model to the IP networks, thanks to the development of VoIP technology [1][2].

In the beginning of its utilization, the VoIP technology lacked service quality and raised interest only from a specific group of users. Among VoIP technology qualities are its low cost, mobility and multiple functionalities. It, therefore, has become a challenge [3][4] to assure quality to the service within acceptable standards.

A solution which has demonstrated good results regarding to the QoS guarantee is the Open Access Metropolitan Area Networks which operate on broad bands [5]. Nevertheless, the quality of service (QoS) during the calls must be as good as possible, once, nowadays, the users have been becoming more and more impatient with the instability and unavailability of the network.

The Open Access Metropolitan Area Networks [6] are examples of high speed networks that can be utilized to transmit multimedia services, such as: voice, video and data. The Open Access MANs are models for IP network architecture whose one of the main objectives is to interconnect public buildings to the people of the municipality through a convergent multimedia network.

A solution to improve the behavior of the service in the systems is to create automation in the functions on management, aiming, mainly, to mitigate the interruption of services, to optimize the allocation of resources, to reduce costs and to, proactively, detect failures. A way to enhance and upgrade the VoIP traffic management is the utilization of tickets named IP Detail Record (IPDR) [7]. The IPDRs are tickets generated in the voice PABX(Private Automatic Branch Exchange)/gateways during the event of a VoIP call, similar to the CDRS (Call Detail Records) which are generated in the conventional telephony [8]. The IPDR function is to supply detailed information of the whole history of a call. The IPDR standard was defined by the IPDR Organization and the Telemanagement Forum [9].

Our objective in this article is to propose a new management methodology for the VoIP system through the construction of baselines based on the IPDRs analyses. In other words, we seek to offer a new approach/methodology that may contribute to increase quality of service through the characterization of the VoIP traffic. Another component is to study the feasibility of using this model in the process of detecting failures and anomalous behavior. An important factor for this study progress was the lack of an efficient monitoring/management model of the IP telephony system based on the characteristics of phone calls. We do believe in the potential of new methods that approach to the analysis of the VoIP technology behavior and see this behavior from the point of view of the events that happen in the traditional telephony: completed call, call congestion, no answer, wrong dialing, busy lines, and technical failure.

The remainder of this paper is organized as follows. Section II presents the IPDR and the Pedreira´s Open Access MAN. Section III describes the IPDR classification. Section IV presents the concepts of Baselines. Section V describes the case study conducted in Pedreira's Open Access MAN. Section VI concludes the paper and discusses future works.

II. INTERNET PROTOCOL DETAIL RECORD

As previously stated, the IPDR provides detailed information about the call. These tickets are essentially utilized in the generation of telephone accounts, that is, in the billing of calls made. There is a limited number of works

 ISBN: 978-1-61208-211-0

which focus on IPDRs. Tartarelli, et al. [10], has addressed the ticket analysis to manage the conventional telephone traffic by identifying problems and observing the utilization profile. He has analyzed a large amount of he logs and recorded all their background to help other operators with similar difficulties. A fraud management system (FMS) was developed based on the analysis of IPDRs carried out by Ruiz-Agundez and Bihina Bella [11][12]. They have proposed this system in NGN (Next Generation Network). In Proença, et al. [13], a baseline is proposed regarding to reliability and safety metrics in order to help network administrators with the system management. In Tartarelli, et al. [10], an approach is suggested in which the logs of gathered data were analyzed by a self-organized mapping system made up of neural networks capable of detecting frauds.

Another possibility is to employ the CDRs and IPDRs to run an analysis in relation to the social aspects of the users.

In Dasgupta, et al. [14], the authors analyze the CDRs to model the behavior of calls made by people who used to change operators very often. The objective of the authors in that case was to investigate the possibility of a person arbitrates to change operator led by influence of friends who had done that before. Besides, they propose an approach which aims to identify people who show bigger potential for changing operator based on their contact network. In addition to that, IPDRs and CDRs can be utilized to develop failure detection systems in communication. In Breda's and Mendes' [9] works, the performance of the algorithms was analyzed to detect failures through the CDRs analysis.

A. Creation of IPDRs

As we have already mentioned, the IPDRs are tickets generated in each call trial, no matter the call has been completed or not. Table 1 shows an example of IPDR in which some fields are shown. The most common use of the IPDR is in the pricing of subscriptions. Nevertheless, the IPDRs can also be utilized in the consumption management, traffic analysis, user profile definition, system dimensioning, among other applications.

TABLE 1. IPDR EXAMPLE

Type	Switch	Start Time	End Time	A Phone Number	...	B Phone Number
00	35	17:17:25	17:19:58	22221056		22221089
00	35	17:17:28	17:17:35	22221087		38932221
00	2	17:17:30	17:28:01	22221045		22221007
00	35	17:17:31	17:18:33	22221009		97435330
00	35	17:17:31	17:21:04	22221033		22221029

To subsidize our research along the six-month period, from January to June/2009, the IPDRs generated inside the Open Access Metropolitan Area Networks in the municipality of Pedreira were collected. This network was designed and, in part, managed by the Communications Laboratory of School of Electrical and Computer Engineering at University of Campinas (UNICAMP). The objective was to gather a real base of IPDRs, within an acceptable time interval so that the baselines developed were according to reality. One of the main reasons to take those IPDRs in consideration to generate the baselines was that such IPDR database had been already set up in the MANs PABX/gateways. It is surely a reliable source of information which portraits a real full-functioning environment.

B. Open Access Metropolitan Area Networks & VoIP

The Open Access MANs can be characterized as being an infrastructure that allows the convergence of applications and multimedia services in municipal scope [15]. Such network calls attention for its high transmission capacity and for the gathering of different kinds of information. One can say the Open Access MANs stand for the public highways of information .

A difference between the existing communication networks and the metropolitan networks is that the Open Access MAN have a universalizing character, and because they are multi-service ones, they can enable the distribution of various contents such as voice, video and data in a simple and unified way, what is currently taken in a separate way by the traditional operators.

Figure 1 shows the physical structure of the Open Access MAN of the city of Pedreira [16]. The network interconnects various public buildings, such as: city hall, board of educational, police station, hospital, municipal schools, daycare institutions, secretaries, houses, etc. The interconnection makes use of two technologies: optical enlacements and radio links. The lines in red stand for the optical fiber backbone of 1 Gigabit (1000BaseLX) connections.

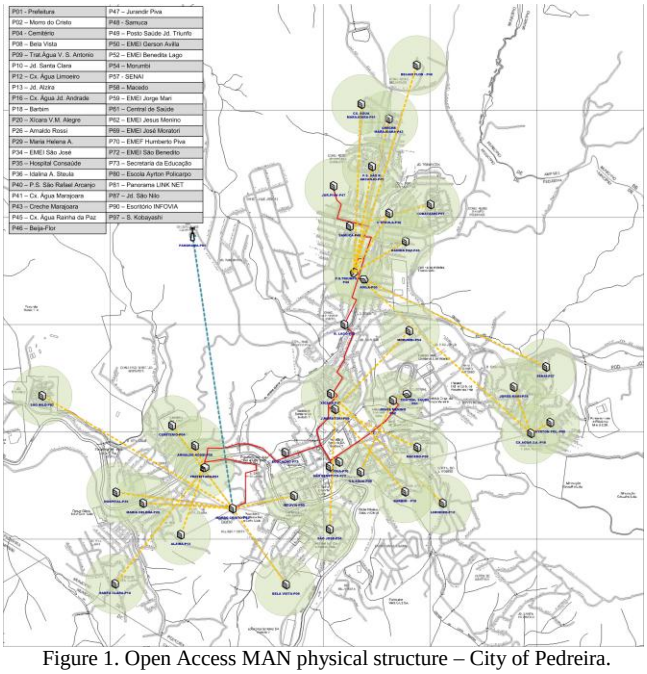


Figure 1. Open Access MAN physical structure – City of Pedreira.

The yellow dotted lines show the radio enlacements (IEEE 802.11a), where the light green circles are the wireless coverage areas for connecting the citizens to the Internet/network (IEEE802.11 b/g/n). The network is based

 ISBN: 978-1-61208-211-0

on the Ethernet standard, and the communication protocol employed is the TCP/IP.

The main objective on implementing the VoIP systems in the Open MANs is the cost reduction of calls once the voice traffic happens on the pre-existing data network. The IP connections (VoIP to VoIP) are free of charge. VoIP calls to conventional telephones will have a decrease in the billing charge. The IP telephony in the Open Access MANs can offer a residential extension through which the citizens can talk to one another at no cost.

Based on the statistics framed in [17], the utilization of VoIP extensions for intra-communication of buildings linked to public administration has generated a 76% savings in the city hall telephone bills, when compared to traditional telephony.

City Hall of Pedreira has adopted the VoIP technology to interlink all the public facilities. The configuration of the IP Telephony network follows the structure as displayed in the Figure 2.

III. IPDR CLASSIFICATION

The entire set of IPDR gathered needs to be classified. Categorizing an IPDR is basically to say what happened to it as the call went on. It is to create a taxonomy (from the Greek tassein = classify and nomos = rule, law). The taxonomy varies from system to system, that is, for mobile telephony there are events, which are different from fixed telephony and from VoIP. For instance: for a system based on VoIP it is not possible to single problems out in a given station ahead, once in an IP network the traffic may follow distinctive paths to reach their destinations. In the fixed telephony there will not be Radio Stations Bases, RF blackout, common events that usually happens in Cellular Systems. Besides all that, there are always common events among different systems, such as: completed calls, trunk congestion, busy lines, no answer, and wrong dialing.

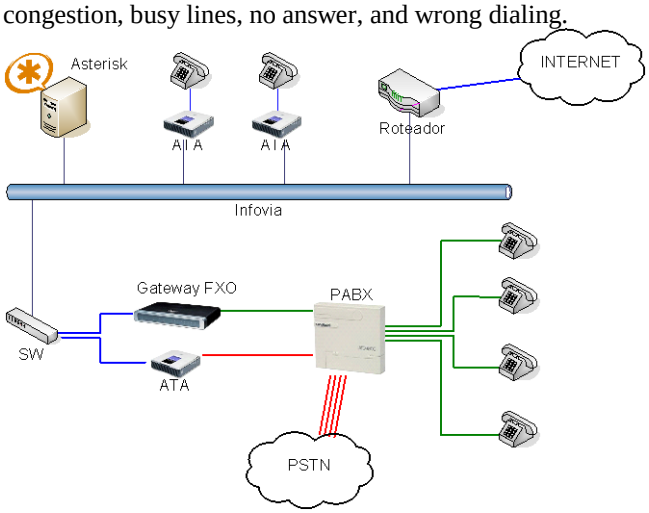


Figure 2. Basic configuration of VoIP in the Open Access MAN of Pedreira.

Every IPDR is submitted to classification which is done according to the pieces of information contained in the fields of the tickets. One of the contributions in this work was the categorization, which led to the taxonomy of IPDR tickets.

As previously mentioned, to classify a call is like attaching a label to each ticket with information about the call destination. It is possible to create a large number of events to classify the tickets. Each one can be divided into sub-events, that is, sub-divisions which reflect the peculiarities of each event. An IPDR field of outstanding relevance in the creation of taxonomy is the field related to "call status". This field reveals typically four situations:

OK: for calls successfully accomplished.

NOT OK: when the destination could not be found.

TO: when the remote terminal was busy at that time.

FAILED: when some kind of failure happened during the generation of the call.

The "call status" field is known in the conventional telephony as "ending of selection" and indicates what may have occurred to the calls as they left the PABX and were forwarded, or also, events related to the ones coming in to the PABX. This piece of information is of utmost importance in the classification of tickets. Of course, the "ending of selection" field is not the only one to be considered at the moment taxonomy is created. Most of the fields owns relevant information and must be taken in consideration as events and sub-events relative to IPDRs are developed.

Table 2 presents the taxonomy created to describe possible call records.

TABLE 2. CLASSIFICATION FOR IPDRS

Event	Description
CELE	Indicates established calls Local => External
CELI-A	Indicates established call Local => Internal (context of A call)
CELI-A1	Indicates local established calls on extensions.
CELI-A1.1	Indicates local established calls which were terminated suddenly
CELI-A1.2	Indicates local established calls with use of waiting music
CELI-A1.3	Indicates local established calls with extension transference
CELI-A1.4	Indicates local established calls with generation of voice message
CNEE	Indicates external non-established calls
CNEI-A	Indicates internal non-established calls (context of A call)
CNEI-A1	Indicates internal non-established calls, once there was no answer from destination
CNEI-A2	Indicates internal non-established calls due to junction/circuit overflow.
TO	Indicates calls whose destination telephone is busy
FCE-A	Failure occurrence when executing external call (A call context)
FCE-A1	FCE-A due to incorrect dialing
FCE-A2	FCE-A due to channel overflow without feedback of signal/message
FCE-A3	FCE-A due to channel overflow with feedback message
FCE-A4	FCE-A due to channel overflow without feedback signal
FCE-A5	FCE-A during IPDR generation

 ISBN: 978-1-61208-211-0

The classified tickes will be used to create the baselines. It is possible to create baselines for each type of event or classification. Therefore, there will be a baseline for the number of calls successfully established to an external number per hour, another baseline for the number of calls established successfully internally per hour and so on.

Table 3 contains an example of classified tickets. Comparing both Table 1 and 3 it is possible to see that the unique difference between them resides in the fact that the latter displays a new field where the classification is.

TABLE 3. CLASSIFIED IPDRS

Type	Switch	Start Time	End Time	A Phone Number	...	B Phone Number	Classification
00	35	17:17:25	17:19:58	22221056		22221089	CELE-A
00	35	17:17:28	17:17:35	22221087		38932221	FCE-A2
00	2	17:17:30	17:28:01	22221045		22221007	CELE-A
00	35	17:17:31	17:18:33	22221009		97435330	CELE-A
00	35	17:17:31	17:21:04	22221033		22221029	CELE-A

IV. BASELINES

With the continuous increase in demand for telecommunication services, more and more necessary is to automate the management of networks in order to optimize the resources, reduce costs, prevent from service unavailability, detect failures and avoid bottlenecks. Besides that, it is necessary to have a reliable network for providing latency sensitive services, as it is the case of VoIP technology. We do believe a far-reaching component for the automation of networks is the establishment of baselines. They stand for the natural behavior profile of the network. The baseline supplies subsidies for the administrator to make more accurate decision on management abnormalities or any other troubles that might be going on.

This work, as previously mentioned, proposes the building of baselines relative to VoIP calls by making use of the IPDRs. The process of generating the baselines begins when a user makes a VoIP call. This call is processed and after that an IPDR is generated. The IPDR, then, is stored in a database. Next, the tickets are classified according to this taxonomy created. Once the tickets are classified, they can be used to build the baselines.

Baselines have three dimensions: event x element x time. The baselines can reveal the various behaviors (events) of the network, such as overflowing, completed calls, transferences, busy lines, wrong dialing, etc. Beyond reflecting all these network behaviors, the baseline can be developed on the basis of all components of the network, for instance: telephone number, telephone prefixes, area codes, physical resources (extensions, junctions, PABX stations, and gateways). It is also possible to work with temporal representations like hourly, daily, weekly, monthly and annual periods.

It is meaningful to emphasize the IPDR utilization potential, for any of these three combinations can be taken to build a baseline. This leads to a very substantial flexibility which results in versatility/efficiency to manage the system.

V. CREATION OF BASELINES

This section shows some examples of baselines that were created. To create the baselines we have used IPDRs relative to the commercial time, considering that, at that time, the city hall staff was on duty and, therefore, making the large number of calls.

The Figure 3 shows the baseline created to estimate the amount of calls made throughout the day. This Figure shows the profile of telephone usage. As it can be seen, the results demonstrate a good adjustment between the baseline and the real data, which are data related to the subsequent day, at the end of the sample taken to develop the baseline. The sample to create the baseline took a four commercial-week time, that is, from Monday to Friday from 8 am to 5 pm. Also, regarding to this Figure, it is possible to see that the biggest concentration of calls occurs between 11 am and 2 pm.

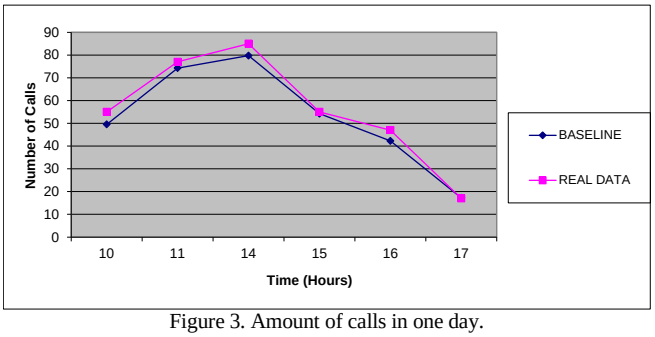


Figure 3. Amount of calls in one day.

Figure 4 shows a comparison between the baseline of local established calls, internal network (CELI-A) and its real traffic. Around 2:00 pm, there was a peak of internal calls successfully established, and not predicted by the baseline. Once they are successfully established calls, this behavior deviation is somehow beneficial to the network. It is not a problem since there was an increase in the volume of completed calls. Anyway, it is a behavior to be investigated.

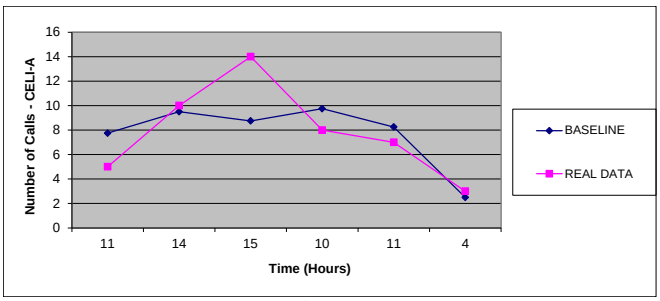


Figure 4. Baseline of established internal calls.

Figure 5 shows the baseline created to demonstrate the behavior of established calls addressed to PSTN(Public Switch Telephone Network). This type of baseline can supply interesting pieces of information relative to calls, because in any PSTN problem it will have a decline in the amount of established calls. This helps detect problems in the network operators so that it can take pro-active action in order to reestablish the service. It is important to evidence

 ISBN: 978-1-61208-211-0

that the baselines can give the possibilities to find out the problems in interconnected networks to ours, even if we do not have any management power on those networks.

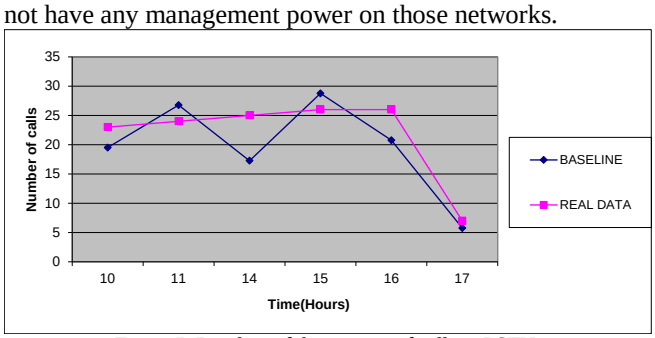


Figure 5. Baseline of the amount of calls to PSTN.

Another interesting approach to the construction of baselines is to analyze the internal telephonic traffic. In the Figure 6 the calls addressed to the Board of Educational phone extension lines were a source for the creation of this baseline. Looking at the curves it is possible to realize a good adjustment between the baseline and the curve that represents the real traffic. This baseline is shown to highlight the potential of this methodology. We can go from a specific extension to an area code (telephone number) of a municipality or state. It is possible to choose either physical elements or logical ones.

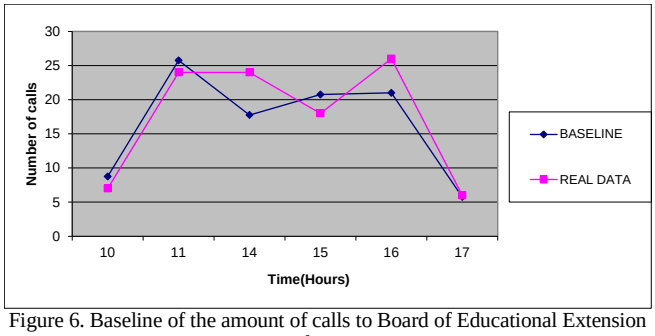


Figure 6. Baseline of the amount of calls to Board of Educational Extension lines.

The baseline in Figure 7 stands for the mapping of internal calls not established because of troubles in the exit junction (CNEI-A2). According to comparison between the baseline and the real curve, it is possible to identify a big deviation after 3 pm in the day analyzed. Such deviation means a problem, as there was excessive degradation, that is, a remarkable increase of uncompleted calls due to malfunctions in the exit junctions.

We are casting algorithms that can be used to detect possible flaws going on the network. In [9], Breda and Mendes, it was researched algorithms that were being employed in the detection of malfunctions based on the utilization of CDRs (Call Detail Records) as a source of information. As it was already explained, the CDR is for fixed/mobile telephony the same IPDR is for VoIP telephony. The advantage of using algorithms is the assurance that the indicated warnings are true. This guarantee is a probabilistic value established by the network administrator. It is reached by means of the adoption of a probabilistic model. In [9], Breda and Mendes, it is explored algorithms that make use of Binomial, Normal and Poisson distributions with guarantee of 99.99999% that the warnings generated are true, that is, they have a root cause. This guarantee means that for every million warnings generated, there is the likelihood of one false-positive warning. A false-positive warning is defined as the one that, despite having been generated, it does not end to be a problem, as it does not have a root cause in the system.

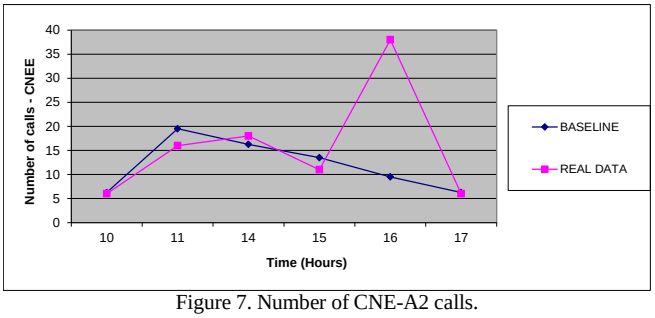


Figure 7. Number of CNE-A2 calls.

VI. CONCLUSION

Our main goal was the construction of a management model on the VoIP technology based on baselines which are put together from a database made up of IPDRs. The baselines feature the IP telephonic traffic, generating a kind of "signature" of the behavior of the system components. Such "signature" can be faced with the current behavior of the components, in a way that makes possible to infer the existence of problems affecting the network performance. Although we have taken data from a metropolitan network, this methodology can be applied to any kind of network, since it has IPDR tickets. Advancing a little bit more, we have got the conclusion that such methodology can be employed in any network, since it has logs, tickets, SNMP packs, that is, logs that portrait one or more events of the system elements.

The classification of the IPDRs has provided a vast gamut of possibilities in the creation of baselines, for instance, the amount of interurban calls made in a given sector, or the amount of international calls originated from a specific extension. This example can be employed to help with the detection of frauds in the network and also with the definition of consumption profile of users.

Another result that can be considered relevant is that the proposed model deals with VoIP systems management from the point of view of conventional telephony events. The VoIP technology is an application that runs with the TCP/IP protocol, that is, with a network of packs. The management on this network model is structured on SNMP objects and copes with some types of behavior related to those packs. The management we are proposing deals with the VoIP technology from the point of view of a regular telephonic call, that is, with all the outcomes a phone call may have. This is highly relevant as it is a change in the way of looking into the VoIP management.

 ISBN: 978-1-61208-211-0

This new approach has demonstrated to be very useful and promising, as it allowed the characterization of the traffic based on information coming from the IPDRs. The creation and analysis of the baselines complemented the network management by attributing optimization and agility to the process. The baselines generated from the IPDRs were able to demonstrate that such methodology adds efficiency in the management of the network and can be employed to detect malfunctions.

As a future work in this area, we intend to use our VoIP baseline to apply algorithms for detection of abnormal behavior and failures.

ACKNOWLEDGMENT

The work herein presented was developed under the shield of "Infovia Municipal – Uma Rede Metropolitana de Acesso Aberto", specially the Open Access MAN of City of Pedreira.

REFERENCES

[1] N.M. Markovich, and U. R. Krieger, "Statistical analysis and modeling of Skype VoIP flows," Computer Communications, vol. 33, pp. S11-S21, 2010.

[2] B. Xi, H. Chen, W.S. Cleveland, and T. Telkamp, "Statistical analysis and modeling of Internet VoIP traffic for network engineering," Electronic Journal of Statistics, vol. 4, pp. 58-116, 2010.

[3] S. Karapantazis, and F. Pavlidou, "VoIP: A comprehensive survey on a promising technology," Computer Networks, vol. 53, no. 12, pp. 2050-2090, 2009.

[4] N. Blefari-Melazzi, J.N. Daigle, and M. Feminella, "Efficient and stateless deployment of VoIP services," Computer Networks, vol. 53, no. 5, pp. 706-726, 2009.

[5] O. Dabbebi, R. Badonnel, and O. Festor, "Automated runtime risk management for voice over IP networks and services," Network Operations and Management Symposium (NOMS), 2010 IEEE , pp.57-64, 2010.

[6] L.S. Mendes, M.L. Bottoli, and G.D. Breda, "Digital Cities and Open MANs: A new communications paradigm," Latin America Transactions, IEEE (Revista IEEE America Latina), vol.8, no. 4, pp.394-402, 2010.

[7] TM Forum – IPDR norms, http://www.tmforum.org/ipdr, November 2009.

[8] G.D. Breda and L.S. Mendes, "Failures Detection in Voice Communication Systems," *In: GLOBECOM 2006*. December 2006. San Francisco/CA, USA.

[9] TM Forum – TM Forum IPDR Program, http://www.tmforum.org/BestPracticesStandards/IPDR/4501/Home.html, 2011.

[10] S. Tartarelli, N. Heureuse, and S. Niccolini, "Lessons learned on the usage of call logs for security and management in IP telephony," Communications Magazine, IEEE , vol.48, no.12, pp.76-82, December 2010

[11] I. Ruiz-Agundez, Y. Penya, and P. Garcia-Bringas, "Fraud Detection for Voice over IP Services on Next-Generation Networks," editors: P. Samarati, M. Tunstall, J. Posegga, K. Markantonakis, D. Sauveron, Information Security Theory and Practices: Security and Privacy of Pervasive Systems and Smart Devices, Lectures Notes on Computer Science, Springer Berlin / Heidelberg, vol. 6033, pp. 199-212, 2010.

[12] M.A.B. Bella, J.H.P. Eloff, and M.S. Olivier, "A fraud management system architecture for next-generation networks," Forensic Science International, Vol. 185, Issues 1-3, 2009, pp. 51-58.

[13] M.L. Proença Junior, C. Coppelmans, M. Botolli, and L. S. Mendes, "Security and reliability in information systems and networks: *Baseline* to help with network management," Ascenso, J., Vasiu, L., Belo, C. and Saramago, M. (eds), e-Business and Telecommunication Networks, Springer, Netherlands, 2006.

[14] K. Dasgupta, R. Singh, B. Viswanathan, D. Chakraborty, S. Mukherjea, A.A. Nanavati, and A. Joshi, "Social ties and their relevance to churn in mobile telecom networks," Proceedings of the 11th International Conference on Extending Database Technology: Advances in Database Technology, pp. 668-677, 2008.

[15] F. Marques and L.S. Mendes, "Proposta de uma Arquitetura Híbrida e Hierárquica de Rede de Sensores/Atuadores para Aplicação em Cenários Metropolitanos", 2010.

[16] Pedreira´s Open Access Metropolitan Area Network, http://www.pedreira.sp.gov.br/ing/index.php, July 2006.

[17] T. Porter, B. Baskin, L. Chaffin, M. Cross, J. Kanclirz Jr, A. Rosela, C. Shim, and A. Zmolek "Pratical VoIP Security", Sygress Publishing, 2006.

 ISBN: 978-1-61208-211-0

Message Scheduling and Forwarding in Congested DTNs

Ahmed Elwhishi*, Pin-Han Ho*, and Basem Shihada†
*Dept of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada
Email: { aelwhish, p4ho}@uwaterloo.ca
†MCSE Division, KAUST, Thuwal, Saudi Arabia
Email: basem.shihada@kaust.edu.sa

***Abstract*—Multi-copy utility-based routing has been considered as one of the most applicable approaches to effective message delivery in Delay Tolerant Networks (DTNs). By allowing multiple message replicas launched, the ratio of message delivery or delay can be significantly reduced compared with other counterparts. Such an advantage, nonetheless, is at the expense of taking more buffer space at each node and higher complexity in message forwarding decisions. This paper investigates an efficient message scheduling and dropping policy via analytical modeling approach, aiming to achieve optimal performance in terms of message delivery delay. Extensive simulation results, based on a synthetic mobility model and real mobility traces, show that the proposed scheduling framework can achieve superb performance against its counterparts in terms of delivery delay.**

***Index Terms*—Routing, Scheduling, Buffer management, DTN.**

I. INTRODUCTION

DTNs are characterized as sparsely connected, highly partitioned, and intermittently connected networks. In these challenging environments the end-to-end path between a given pair (source and destination) may never exist [1]. To cope with frequent, long-lived disconnections and variations in link condition over time, a node in a DTN buffers a message and waits until it finds an available link to the next hop, which in turn buffers and forwards the received message if the node is not the end destination. This process continues until the message reaches its destination. It is usually referred as *encounter-based*, *store-carry-forward*, or *mobility-assisted* routing, because it exploits the node mobility as a significant factor for the forwarding decision of each message. This model of routing constitutes a significant difference from conventional ad hoc routing strategies which assume there exists an end-to-end path between any source and destination at any time.

To improve the robustness, reduce the delivery delay, and increase the delivery ratio, extensive research efforts have been reported in design of efficient multi-copy routing algorithms [2], [4], [5], [6]. Although with excellent performance compared with single-copy routing schemes, multi-copy routing algorithms introduce additional power consumption and hardware requirement by being subject to higher computation complexity, and requiring more transmissions and buffer space. It is envisioned that the future DTNs are composed of miniature and hand-held devices (e.g., smart phones and PDAs), and could be subject to extensive congestion due to dense nodal distribution and large traffic volumes. Thus far, a few studies have considered buffer space limitation and contention of wireless links in the algorithm design [4], [10], [17], [20]. However, none of the previously reported studies provided a complete study on an efficient message scheduling and buffer management algorithm under heterogeneous DTNs.

Motivated by its importance, the paper investigates DTN routing by introducing a novel message scheduling and buffer management approach. Our goal is to come up with a solid framework which can be incorporated with many encounter-based routing schemes employing contact or inter-contact time as main factor on message forwarding decision making process. In particular, the proposed approach enables an effective buffer management policy which determines which messages should be forwarded or dropped when the buffer is full. Such a decision is made by evaluating the impact of dropping each buffered message according to collected network information. Based on the proposed buffer management policy, we analyze the message delay on a generic message forwarding scheme reported in [17], called Self Adaptive Utilty-based Routing Protocol (SAURP). The contributions of the paper are as following:

- Developing new utility-based message scheduling mechanism that incorporates with SAURP message forwarding. This new mechanism provides per-message utility values, which are calculated based on a simple theory that based on inter-contact time, and the estimation of two parameters: the number of message copies, and the number of nodes who have "*seen*" this message (*the nodes that have either carried the message or rejected the acceptance of this message*). The per-message utility values at each node are then used for the decision on whether the buffered messages should be dropped in any contact.
- Gaining understanding on the efficiency and effectiveness of the proposed approach by comparing it with counterparts using extensive simulations.

The rest of this paper is organized as follows. Section II describes the related work in terms of utility-based DTN routing, and buffer management and scheduling. Section III

 ISBN: 978-1-61208-211-0

provides the background of the study which includes the SAURP mechanism and the system model. Section IV introduces the proposed message scheduling approach. Section V provides experimental results which verify the proposed approach. Section VI concludes the paper.

II. Related work

Numerous studies have been reported to address the DTN routing issues [3], [4], [5], [6], [11], [12], [17], [18]. Yet, the impact of buffer management and scheduling policies on the performance of DTNs has only been investigated in a few studies. Zhang et al. [8] addressed this issue in the case of epidemic routing by evaluating a number of simple drop policies such as drop-front and drop-tail, and analyzed the situation where the nodal buffer has a capacity limit. The paper concluded that the drop-front policy outperforms the drop-tail. Lindgren et al. [9] evaluated a set of heuristic buffer management policies based on locally available nodal parameters and applied them to a number of DTN routing protocols. G. Fathima et al. [21] proposed a buffer management scheme based on dividing the main buffer into a number of queues, each being maintained for a class of service and scheduled accordingly. When a particular queue is full, the message is placed in the subsequent queue. When the entire buffer is full, some of the messages with least class of service should be dropped to yield room for new messages. However, it is not clear how the messages are classified. Dimitriou et al. [23] proposed a buffer management policy based on using two types of queues. A low-delay traffic (LDT) queue and a high-delay traffic (HDT) queue. Noticeably all the aforementioned policies are only based on very limited knowledge that is locally available to each node.

Dohyung et al. [20] presented a drop policy which discards a message with the largest expected number of copies first, to minimize the impact of message drop, while leaving the issue of scheduling untouched. Erramilli et al. [22] introduced a set of policies in conjunction with their forwarding algorithm. One policy is based on forwarding the message that has the highest delegation number and the other favours the smaller delegation numbers, which serve as heuristics without any optimization effort in the DTN context. Moreover, the aforementioned studies did not address issues of scheduling.

Message scheduling under heterogeneous nodal mobility was firstly addressed by Balasubramanian et al. [14], in which a resource allocation problem was formulated. The statistics of available bandwidth and the number of message replicas in the network are considered in the derivation of the routing metric to decide which message to replicate first among all the buffered messages in the custodian node. The derivation of the routing metric, nonetheless, is not related to buffer status. In the same research line, Krifa et al. [10] proposed a forwarding and dropping policies for a limited buffer capacity. The decision under these policies is made based on the value of per-message marginal utility. The parameters of the utility function are estimated under the assumption of homogeneous nodal mobility, thus the scheme could be subject to considerable performance impairment under heterogeneous nodal mobility which is considered a more practical scenario. It is clear that the aforementioned studies leave a large room to improve, where a solution for DTN buffer management and message scheduling that can well estimate and manipulate the network status is absent.

Algorithm 1 The forwarding strategy of SAURP

On contact between node A and B
Exchange summary vectors
for every message M at buffer of custodian node A *do*
  if destination node D in transmission range of B *then*
    A forwards message copy to B
  end if
  if $\triangle T^{(i)}_{(A,D)} > \triangle T^{(i)}_{(B,D)}$ *do*
    if message tokens >1 *then*
      apply weighted copy rule
    end if
    else if $\triangle T^{(i)}_{(A,D)} > \triangle T^{(i)}_{(B,D)} + \triangle T_{th}$ *then*
      A forwards message to B
    end if
  end if
end for

III. Background and System Model

This section presents the background of protocol under consideration as well as the network model for utility-based routing.

A. Self Adaptive Utility-based Routing Protocol (SAURP)

SAURP [17] is designed to solve the DTN routing problem in terms of how to select a next hop for each carried massage. Specifically, it initiates cooperation among a group of nodes in making message forwarding decision for the stored messages based on a utility function at each contact with another node. Algorithm 1 shows detailed SAURP mechanism, where the utility function value ($\triangle T$) simply represents the inter-contact time duration between a node and the destination of message i, while the routing decision for the message is made according to whether message i is in the spraying phase (i.e., the number of message i copy tokens > 1), or in the forwarding phase (i.e., the remaining number of message i copy tokens = 1). If the message is in spraying phase, a rule called weighted copy rule is applied for message forwarding decision. For more details about SAURP, the reader referred to [17].

Although SAURP can effectively select the next hop to forward a message, it lacks the ability to intelligently tell which message should be dropped when the buffer is full. This particularly becomes a problem in case of high traffic load and stringent buffer limitation, where a node has to drop some buffered messages that are less unlikely to be delivered to the destination while accommodating those with more likelihood to be successfully delivered, in order to achieve better performance. Thus, an efficient message scheduling and dropping policy should be in place as a countermeasure of the aforementioned situation. The main challenge lies on how to

 ISBN: 978-1-61208-211-0

Table I
NOTATION

Variables	Description
$Sr_j(t)$	The source of message j
$Dst_j(t)$	The destination of message j
T_j	Elapsed time since the creation of the message
R_j	Remaining lifetime of the message ($R_j = Tx_j - T_j$)
$n_j(t)$	Number of copies of message j
$m_j(t)$	Number of nodes who have "seen" message j
Tx	Message time-to-live

accurately predict the network state in a distributed manner according to the collected historical data under heterogeneous nodal mobility. The paper answers the question by investigating a novel message scheduling and dropping policy that incorporates with SAURP.

B. Network Model

For any given node A, let a number of $J_A(t)$ messages be stored in its buffer at time t. Each message j, $j \in [1, J_A(t)]$ is denoted by a tuple of variables denoted in Table 1.

The encounter (or mixing) rate between A and B, denoted as β_{AB}, is the inverse of the expected inter-encounter time for the two nodes: $\beta_{AB} = \frac{1}{\triangle T_{AB}}$. We assume that $\triangle T_{AB}$, A, $B \in [1, N]$ follows an exponential distribution (or referred to as with an exponential tail [13]). It has been shown that a number of popular mobility models have such exponential tails (e.g., Random Walk, Random Waypoint, Random Direction, Community-based Mobility [7], [15]). Recent studies based on traces collected from real-life mobility examples [16] argued that the inter-encounter period and the encounter durations in these traces demonstrate exponential tails after a specific cutoff point. The historical information becomes more accurate and the adaptation of the mobility characteristics becomes precise with a greater elapsed of time.

IV. PROPOSED MESSAGE SCHEDULING SCHEME

A. Network State Estimation

During each contact, the network information summarized as a "summary vector", is exchanged between the two nodes through an in-band control channel, which includes the following data: (1) statistics of inter-encounter time of every node pair maintained by the nodes, (2) statistics regarding the buffered messages, including their IDs, remaining time to live (R_i), destinations, the stored $n_i(T_i)$, and $m_i(T_i)$ values for each message that were estimated in the previous contact. We call the strategy of updating $n_i(T_i)$, and $m_i(T_i)$ values as Encounter History-Based Prediction (EHP).

Since it is not practical to estimate global knowledge about the network due to the heterogeneous nature of the nodal mobility, when ever two nodes encounter each other they update each other with respect to the messages they do not have in common, and the values of $m_j(T_j)$, and $n_j(T_j)$, $\{\beta_{1,d_j}, \beta_{2,d_j} ... \beta_{n,d_j}\}$, and $\{\beta_{1,d_j}, \beta_{2,d_j} ... \beta_{m,d_j}\}$ are updated accordingly, where β_{n,d_j} and β_{m,d_j} represents the encounter rate between the n^{th} custodian of the n^{th} copy of message j with the destination of message j, and the encounter rate of m^{th} node who has seen the message with the destination of message j, respectively. These parameters are further taken as inputs to calculate the proposed per-message utility function.

B. Utility Calculation

Based on the problem settings and estimated parameters, the following question should be answered at each node during every nodal contact: Given $n_j(T_j)$, $m_j(T_j)$, T_j, and limited buffer space for supporting SAURP routing, what is an appropriate decision on whether the node should drop any message in its buffer or reject any incoming message from the other node during the contact, such that the average delivery delay can be optimized?

To ansewr this quetion, let us assume that nodes A and B are in contact, and message j in A's buffer is to be forwarded to node B according to SAURP forwarding policy, while the buffer is full at node B and there is a message i with elapsed time T_i in a network that has K messages at the moment at which the decision should be made by node B with respect to dropping a message from all messages in its buffer.

To minimize the delivery delay of all messages, the decision of dropping message i should result in least increase of delivery delay of message i, while forwarding message j from node A to B should result in most decrease in the delivery delay of message j (i.e, node B should discard a message such that the expected delivery delay of all messages can be reduced the most). Since the delivery delay of the messages is mainly affected by the nodal inter-encounter time, we assume that all message have infinite or large enough Tx and derive the utility function such that it is affected by number $n_j(T_j)$, $m_j(T_j)$, $\{\beta_{1,d_j}, \beta_{2,d_j} ... \beta_{n,d_j}\}$, and $\{\beta_{1,d_j}, \beta_{2,d_j} ... \beta_{m,d_j}\}$.

To achieve the minimum average delivery delay, node B should drop the message that satisfies the following:

$$Umin_i = argmin_i \left| \left[exp(- \sum_{k \in m_i(T_i)} \beta_{k,d_i} T_i) \left(\frac{1}{\sum_{l \in n_i(T_i)} \beta_{l,d_i}} - \frac{1}{\sum_{l \in n_i(T_i) \setminus B} \beta_{l,d_i}} \right) \right] \right| \quad (1)$$

Derivation of (1): Let random variable T_d represents the delivery delay of message j. Then the expected delay in delivering a message that still has copies existing in the network can be expressed

$$D_j = P\{message\, j\, not\, deliverd\, yet\} * E[T_d \mid T_d > T_j]$$

$$D_i = exp(- \sum_{k \in m_j(T_j)} \beta_{k,d_j} T_j) * E[T_d \mid T_d > T_j] \quad (2)$$

where

$$Pr\{message\, j\, not\, delivered\, yet\} = \prod_{l=1}^{n_j(T_j)} exp - (\beta_{l,d_j} R_j) = exp(-(\sum_{l=1}^{n_j(T_j)} \beta_{l,d_j} T_j)) \quad (3)$$

,

$$E[T_d \mid T_d > T_j] = \left[T_j + \frac{1}{\sum_{l \in n_j(T_j)} \beta_{l,d_j}} \right] \quad (4)$$

 ISBN: 978-1-61208-211-0

When a node buffer is full, the node should make a drop decision that leads to the least increase in D_j. To find the local optimal decision, D_j is differentiated with respect to $n_j(T_j)$, and ∂D_j is then discretized and replaced by $\triangle D_j$:

$\triangle D_j = \frac{\partial D_j}{\partial n_j(T_j)} * \triangle n_j(T_j)$, which is equivalent to
$\triangle D_j = exp(-\sum_{k \in m_j(T_j)} \beta_{k,d_j} T_j) *$

$$\left[\frac{1}{\sum_{l \in n_j(T_j)} \beta_{l,d_j}} - \frac{1}{\sum_{l \in n_j(T_j) \setminus B} \beta_{l,d_j}} \right] \triangle n_j(T_j)$$

To reduce the delivery delay of all messages existing in the network, the best decision is to discard the message that maximizes the total delivery delay, $D = \sum_{j=1}^{K(t)} D_j$, among all $K(t)$ messages existing in the network. Therefore, the optimal buffer-dropping policy at node B that leads to minimization of the delivery delay is thus to discard the message that has the min value of $\mid \triangle D_j \mid$ (or$-\triangle D_j$), which is equivalently to choose a message with a value for $Umin_i$ that satisfies (1), which represents the marginal increase in the delivery delay of message i if its copy at node B is dropped. While the optimal buffer-forwarding policy at node A that leads to minimization of the delivery delay is thus to forward a copy of message j (or message j itself) to node B that leads to the max decrease of $\triangle D_j$, which is equivalently to choose a message with a value for $Umax_j$.

The decision of forwarding message j from node A to node B should satisfy one of two cases; based on whether message j is in spraying phase, or in forwarding phase. If message j is still in spraying phase, the decision of forwarding message j should satisfy the following:

$$Umax_j = argmax_j \left| \left[exp(-\sum_{k \in m_j(T_j)} \beta_{k,d_j} T_j) \left(\frac{1}{\sum_{l \in n_j(T_j)} \beta_{l,d_j}} - \frac{1}{\sum_{l \in n_j(T_j) \cup B} \beta_{l,d_j}} \right) \right] \right. \quad (5)$$

which represents the margin decrease in the delivery delay of message j if node A forward a copy to node B.

If message j is in forwarding phase, the decision of forwarding should satisfy the following:

$$Umax_j = argmax_j \left[exp(-\sum_{k \in m_j(T_j)} \beta_{k,d_j} T_j) \left(\frac{1}{\sum_{l \in n_j(T_j)} \beta_{l,d_j}} - \frac{1}{\sum_{l \in (n_j(T_j) \setminus A) \cup B} \beta_{l,d_j}} \right) \right] \quad (6)$$

The relation represents the marginal decrease in the delivery delay if node A hands over message j to node B.

Derivation of (5) and (6): The derivation follows same steps of deriving (1) with considering the marginal decrease of delivery delay of message j at node A if it get copied or forwarded to node B.

Algorithm 2 SAURP_based forwarding and dropping policy

On contact between node A and B
Exchange summary vectors
01: If (buffer at node B is full)
02: *for* every message j at the buffer of custodian
02: node A *do*
03: *if* (B is not source node of i) *then*
04: *if* (remaining tokens of message
04: $j \geq$ remaining tokens of i) &&
04: ($\triangle T_{B,d_i} \succ min\{\triangle T_{1,d_i}, \triangle T_{2,d_i}$..
04: .., $\triangle T_{n-1,d_i}\}$)*then*
05: *if* destination node d_j in
05: transmission range of B *then*
06: B drops message i
07: A forwards a copy of message j to B
08: *end if*
09: *else if* ($Umax_j - Umin_i > 0$) *then*
10: B drops message i
11: A forwards message j to B
12: *end else if*
13: *end if*
14: *end if*
15: *end for*
16:end if
17:else (apply SAURP)
18:end

C. SAURP_based Forwarding and Dropping Policy (SAURP_FDP)

With the per-message utility, the node firstly sorts the buffer messages accordingly from the highest to the lowest. The messages with lower utility values have higher priorities to be dropped when the node's buffer is full, while the messages with higher utility values have higher priorities to be forwarded to the encountered node. Algorithm 2 illustrates the forwarding and dropping actions which are largely based on the fact that if the utility $Umax_j$ of message j (the message with the highest utility value) buffered in A is higher than $Umin_i$ of message i (the message with the lowest utility value) at node B, then message i is dropped and replaced by message j or copy of it, if the buffer of B is full during the contact between the two nodes. To enhance the performance of the algorithm, the lowest priority of dropping is given to a message that has higher number of remaining message tokens or the inter-contact time between its current custodian and the message destination is the best one found so far.

V. Simulation Study

Simulation is conducted to examine the efficiency of the proposed scheme, namely SAURP_based Forwarding and Dropping Policy (SFDP). SFDP under EHP is denoted as SFDP_E.

 ISBN: 978-1-61208-211-0

A. Experimental Setup

To better understand the performance of the proposed strategies and their gain over SAURP without buffer management, we also implemented another estimation strategy for the values of $m_i(T_i)$, and $n_i(T_i)$, namely Global Knowledge-based Management (GKM). GKM assumes knowing the exact values of $m_i(T_i)$, and $n_i(T_i)$, and is supposed to achieve the best performance. Since such an assumption is not practical [11], the result of GKM is taken as a benchmark for the proposed scheme. We call SFDP under GKM strategy as SFDP_G.

In addition to the above prediction strategy, we compared the proposed buffer management schemes with three well-known scheduling schemes listed as follows:

- Drop oldest (DO) drops the message with shortest remaining T_x when the buffer is full. This policy obtains the best performance of all the policies used by Lindgren et al. in [9]. We call DO under SFDP as SFDP_DO.
- Delegation forwarding scheme employs a dropping policy based on drop message with highest number of forwards (DF_N) by Erramilli et al. in [22].
- RAPID scheme employs a dropping policy based on drop message that is most likely to miss the deadline [14].

We assume a message issued at a node (termed sourced messages) has the highest priority at the node. If all buffered messages and newly arrived message are from itself, the oldest is dropped.

A DTN simulator similar to that in [19] is implemented. The simulations are based on two mobility scenarios: a synthetic one on community based mobility model (CBMM) [24], and a real-world encounter traces with 98 nodes collected as part of the Infocom 2006 experiment, described in [25]. The simulation parameters are as shown in Table II. Each node has a transmission range of $D = 30$ meters to achieve a sparsely populated network, the size of all messages is same, and each message transmission takes one time unit. Euclidean distance is used to measure the proximity between two nodes and their positions. A slotted collision avoidance MAC protocol with Clear-to-Send (CTS) and Request-to-Send (RTS) features is implemented in order to arbitrate the contention on a shared channel between nodes. The message inter-arrival time at a node is uniformly distributed in such a way that the traffic can be varied from low (10 messages generated per node) to high (70 messages generated per node). The buffer size is set to 10 messages, which is quite low compared with the considered traffic arrival rates such that the network could easily go into a congestion state. Message delivery ratio and the delivery delay are taken as two performance measures. Each data is the average of the results from 30 runs.

B. Simulation Results

This section examines the proposed policy for minimizing the average delivery delay under the considered scenarios. The plots of the delivery delay obtained under CBMM and Infocom2006 traces is shown in Figure 1 and Figure 2.

As expected, the SFDP_G gives the best performance under all traffic loads for both scenarios under consideration, while

Table II
SIMULATION PARAMETERS

Mobility pattern	CBMM	Infocom06
Simulation duration (seconds)	30000	270000
Simulation area	700×700	–
No. of Nodes	110	98
Average speed (m/s)	-	-
T_x(seconds)	9000	90000

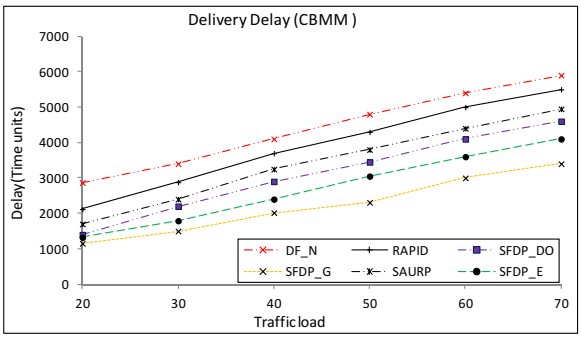


Figure 1. The effect of traffic load (CBMM scenario).

the SFDP_E is the second best and is competitive with the SFDP_G in the case of low traffic. As the traffic increases, the demand on the wireless channel and buffers increases, causing long queuing delays and substantial message loss that negatively affect the performance of all the examined policies.

Figure 1 shows the results under CBMM scenario. We have observed that the SFDP_E outperforms the SAURP, RAPID, DF_N, and SFDP_DO. SFDP_E is better than SAURP by 21%, RAPID by 35%, DF_N by 44%, SFDP_DO by 16%, and a longer delay of only 23% of that achieved by SFDP_G. Under the real trace scenario as shown in Figure 2, SFDP_E achieved delivery delay better than SAURP by 27%, RAPID by 43%, DF_N, by 56%, SFDP_DO by 20%, and a longer delay of 14% of that achieved by SFDP_G.

VI. CONCLUSION AND FUTURE WORK

This paper has investigated a novel buffer management policy for a utility-based forwarding routing in heterogeneous delay tolerant networks (DTNs), aiming to optimize the message delivery delay. The proposed framework incorporates a

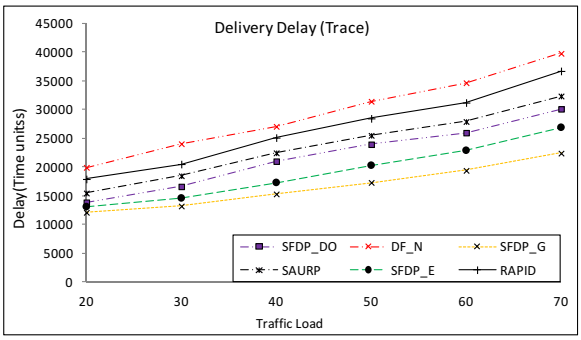


Figure 2. The effect of traffic load (real trace scenario).

suit of novel mechanisms for network state estimation and utility derivation, such that a node can obtain the priority for dropping each message in case of buffer full. Using simulations based on two mobility models; a synthetic (Community based Mobility Model) and a real trace (Infocom2006), the simulation results show that the proposed buffer management policy can significantly improve the routing performance in terms of the performance metrics of interest under limited network information.

Note that in this work, our objective was optimizing the message delivery delay. It would be interesting to introduce a utility function to optimize the delivery ratio of all messages. Also, in this study we considered relatively small network size, and all messages have the same size and same T_x value. It is important to study the performance of our proposed scheme under various network set up, and develop buffer management policies accordingly. For example, in case of larger network size under high congestion, we expect that the cost of the update of the parameters could consume larger amount of available bandwidth, which may affect the network throughput. Thus, this issue should be taken in consideration.

REFERENCES

[1] "Delay tolerant networking research group," http://www.dtnrg.org. April 12, 2012.

[2] A. Lindgren, A. Doria and O. Schelén, "Probabilistic Routing in Intermittently Connected Networks," *SIGMOBILE Mobile Computing Comm. Rev., vol. 7, no. 3, pp. 19-20, July 2003.*

[3] A. Vahdat and D. Becker, "Epidemic Routing for Partially Connected Ad Hoc Networks," *Technical Report CS-200006, Duke Univ., Apr. 2000.*

[4] A. Elwhishi and P. Ho, "SARP - a novel multi-copy routing protocol for intermittently connected mobile networks," *Proc. IEEE GLOBECOM, pp. 4482-4488, Dec. 2009.*

[5] V. Erramilli, M. Crovella, A. Chaintreau , C. Diot, " Delegation forwarding," *Proc. ACM MobiHoc, pp. 251-260, 2008.*

[6] A. Elwhishi, P. Ho, K. Naik, B. Shihada, "Self Adaptive Contention Aware Routing Protocol for Intermittently Connected Mobile Networks," *IEEE Trans. Parallel and Distributed Systems, vol.PP, no.99, pp.1, 0, Janaay 2012.*

[7] R. Groenevelt, P. Nain, and G. Koole, " The message delay in mobile ad hoc networks," *Perform. Eval. Vol.62, no.1-4, pp. 210-228, October 2005.*

[8] X. Zhang, G. Neglia, J. Kurose, and D. Towsley, "Performance modeling of epidemic routing," *Comput. Netw. 51(10), pp. 2867-2891, July 2007.*

[9] A. Lindgren and K. Phanse, "Evaluation of Queueing Policies and Forwarding Strategies for Routing in Intermittently Connected Networks," *Proc. COMSWARE, pp. 1-10, 2006.*

[10] A. Krifa, C. Barakat, and T. Spyropoulos, "Optimal buffer management policies for delay tolerant networks," *Proc. IEEE SECON, pp. 260 - 268, June 2008.*

[11] S. C Nelson, M. Bakht, R. Kravets, and Al. F. Harris, "Encounter: based routing in DTNs," *Proc. IEEE INFOCOM, pp. 846 - 854, April 2009.*

[12] T. Spyropoulos, T. Turletti, and K. Obraczka, "Routing in delay-tolerant networks comprising heterogeneous node populations," *IEEE Trans. Mobile Computing, vol. 8, no. 8, pp. 1132–1147, August 2009.*

[13] D. Aldous and J. Fill, "Reversible markov chains and random walks on graphs. (monograph in preparation.)," http://statwww. berkeley.edu/users/aldous/RWG/book.html. *April 12, 2012.*

[14] A. Balasubramanian, B. N. Levine, and A. Venkataramani, "Dtn routing as a resource allocation problem," *Proc. ACM SIGCOMM, pp. 373-384, 2007.*

[15] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Performance analysis of mobility-assisted routing," *Proc. ACM MOBIHOC, pp. 49-60 , 2006.*

[16] M. V. Thomas Karagiannis, J. Le Boudec, "Power law and exponential decay of inter contact times between mobile devices," *Proc. ACM/IEEE MobiCom, pp. 183-194, 2007.*

[17] A. Elwhishi, P. Ho, K. Naik, and Basem Shihada, "Contention Aware Routing for Intermittently Connected Mobile Networks," *The Third International Conference on Advances in Future Internet (AFIN 2011), pp. 8-18, August 2011.*

[18] A. Seth, D. Kroeker, M. Zaharia, S. Guo, and S. Keshav, "Low-cost communication for rural internet kiosks using mechanical backhaul," *Proc. MobiCom, pp. 334-345, 2006.*

[19] "DTN java simulator," http://people.ee.ethz.ch/ spyropot/dtnsim.html. *April 12, 2012*.

[20] H. P. Dohyung Kim and I. Yeom, "Minimizing the impact of buffer overflow in dtn," *Proc. International Conference on Future Internet Technologies (CFI), June 2008.*

[21] G. Fathima, and R.S.D. Wahidabanu, " A new queuing policy for delay tolerant networks," *Int. J. Computer. Application, vol. 1, no. 20, pp. 56-60, 2010.*

[22] V. Erramilli, M. Crovella, "Forwarding in opportunistic Networks with Resource constraints," *Proc. ACM CHANTS, pp. 41-48, 2008,*

[23] S. Dimitriou and V. Tsaoussidis, "Effective buffer and storage management in DTN nodes," *Proc. ICUMT, Oct. 2009, pp. 1-3.*

[24] T. Spyropoulos, K. Psounis, and C.S. Raghavendra, "Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-Copy Case," *IEEE Trans. Networking, vol. 16, no. 1, pp. 63-76, Feb. 2008.*

[25] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, "Impact of human mobility on opportunistic forwarding algorithms," *IEEE Trans. Mobile Comput., vol. 6, no. 6, pp. 606–620, Jun. 2007.*

 ISBN: 978-1-61208-211-0

Model Checking of Trust-Based User-Centric Cooperative Networks

Alessandro Aldini and Alessandro Bogliolo
University of Urbino "Carlo Bo"
Urbino, Italy
{*alessandro.aldini,alessandro.bogliolo*}*@uniurb.it*

***Abstract*—The success of user-centric networks depends on the willingness of the participants to cooperate by sharing resources and services. Reputation-based incentives and remuneration (based either on fiat money or on virtual currency) have emerged as two complementary incentive mechanisms to increase users' motivation and to discourage selfish behaviors. In this paper, we conduct a formal study of the benefits of the joint application of these two mechanisms in the context of a cooperation model recently proposed for user-centric wireless networks. To this purpose, several performance properties of cooperation incentives mechanisms are defined and analyzed through model checking of probabilistic systems with an underlying Markov process semantics.**

***Keywords*-trust, virtual currency, model checking, user-centric networks.**

I. INTRODUCTION

As more and more people get involved in any kind of online communities, ranging from social networks to sharing communities and online games, user centric networking is becoming more and more relevant for the future of the Internet. User centricity, however, entails cooperation among members of broad communities who usually do not know each other in person. Hence, cooperation incentives and trust mechanisms are essential requisites of any community, the success of which strongly depends on the willingness of its members to cooperate and can be impaired by mistrust and selfishness. This is particularly true in user-centric wireless networks (UCNs), where even the underlying communication infrastructure is dynamically built by users who share their Wi-Fi connections, and the inherent limitations of mobile devices (in terms of battery, CPU, and bandwidth) can keep users from adopting prosocial behaviors.

When *inherent* motivations (including fairness, synergy, and sense of community) provide no sufficient cooperation incentives [1], they need to be complemented by *extrinsic* motivations, such as reputation, reciprocity, and monetization. It has been recently shown that a suitable support for the implementation of extrinsic cooperation incentive mechanisms in UCNs can be provided by the joint application of *trust management* [2] and *virtual currency* [3] systems [4]. Trust and virtual currency infrastructures provide the means for implementing the so-called *soft security*, which is characterized by relaxation of the security policies and enforcement of common ethical norms for the community [5]. Such means do not rely on pervasive controls concerning, e.g., assurance of payment or service delivery, thus exposing the system to dishonest behaviors that, however, are contrasted by the adoption of cooperation incentives. Hence, it is important to verify to what extent the incentives can deal successfully with mistrust, selfishness, and cheats.

A game-theoretic analytical study [6] has recently revealed that reputation-based and price-based strategies must be integrated in order to optimize the effects of cooperation incentives. Game theory has been widely used to conduct a mathematical analysis of the complex interactions among nodes of wireless ad-hoc networks [7], [6]. The results of the analytical study are consolidated by simulation results showing the fast convergence towards cooperative behaviors in the case of mixed incentive strategies.

This work provides an orthogonal view of the benefits of mixed cooperation incentives by employing formal analysis techniques for the evaluation of quantitative properties of systems. In particular, as a real-world case study, we analyze several performance metrics of the cooperation process envisioned by Bogliolo et al. [4] for UCNs.

Formal methods provide mathematically rigorous techniques and tools for the design and verification of systems. More precisely, formal specifications are mathematical models (e.g., automata), formal verifications are based on well-formed statements (e.g., in a temporal logic), and automatic checks rely on analysis algorithms (e.g., model checking). In this paper, we evalute the cooperation model under study through the probabilistic model checker PRISM (see, e.g., [8], [9] for a survey of the approach). The modeling language of PRISM is a state-based mathematical formalism based on the Reactive Modules introduced by Alur and Henzinger [10], from which different types of probabilistic models can be derived, including discrete-time Markov chains (DTMCs) and Markov decision processes (MDPs) [11], [12]. Performance properties are expressed in a temporal logic – subsuming both probabilistic computation tree logic (PCTL) and linear time logic (LTL) – which is expressive enough to specify state-based and path-based properties, and including both probabilistic and reward operators [13].

In the remainder of the paper, we briefly introduce the cooperation model of [4] and the related modeling assumptions (Section II), we report and discuss the results of the model checking analysis (Section III), and we draw conclusions (Section IV).

 ISBN: 978-1-61208-211-0

II. COOPERATION MODEL

This section briefly outlines the cooperation model under study [4] and the modeling assumptions adopted for analysis purposes. Cooperation involves users providing services, hereafter called *requestees*, and recipients of such services, hereafter called *requesters*. According to [4], the cooperation process entails four phases, which rely on trust management and virtual currency.

In the first phase, called *discovery and request*, the requester searches for a requestee offering the required service. Reputation of the requestee is a parameter guiding the choice. If the requester is trustworthy enough to access the required service, then the issued request can be accepted. However, it may be also refused because of, e.g., lack of willingness to cooperate. In the second phase, called *negotiation*, requester and requestee establish service parameters and reward, possibly taking into account the trust of the requestee on the requester. In the third phase, called *transaction*, service is delivered and then the related payment is provided. In the fourth phase, called *evaluation and feedback*, the transaction results are used to adjust, if necessary, reputation of the involved parties.

A. Reputation System

As usual in several trust-based systems [5], we model trust (reputation) as a discrete metric. Basically, the cooperative attitude of the requestee depends on two parameters: the dispositional trust dt, representing the initial willingness to trust incoming requests, and the service trust level st, representing a threshold below which the service is not accessible. Then, given a requestee i and a requester j, the computation of the trust level of i towards j is obtained by mixing direct experience and indirect recommendations:

$$T_{ij} = \alpha \cdot trust_{ij} + (1 - \alpha) \cdot recs_{ij}$$

where $\alpha \in [0, 1]$, $trust_{ij}$ is the trust metric deriving from previous direct interactions of i with j (the initial value of $trust_{ij}$ is set to the dispositional trust of i, dt_i), and $recs_{ij}$ is the average of the trust metrics towards j of other users (different from i) that in the past negotiated directly with j. Notice that, if $T_{ij} < st_i$ then the service request of j cannot be accepted by i.

B. Virtual Currency System

Reputation-based and reward-based incentives are combined by including the trust level T of the requestee towards the requester as a parameter affecting the cost of the negotiated service. The other parameters are C_{min}, which is the minimum reward (cost) asked by the requestee regardless of his/her trust on the requester, C_{max}, which is the maximum reward asked to serve untrusted users, and T', which is the trust threshold above which the minimum cost is applied to the requester. Then, the cost function C proposed in [4] is defined as follows:

$$C(T) = \begin{cases} C_{min} + \frac{C_{max} - C_{min}}{T'} \cdot (T' - T) & T < T' \\ C_{min} & T \geq T' \end{cases} \quad (1)$$

C. Modeling Assumptions

For the sake of simplicity, here we assume that users do not play the roles of both requester and requestee. Moreover, we consider a unique type of service that is offered by each requestee in the network. Trust values range in the interval $[0, 10]$, such that $null = 0$, $low = 2$, $med = 5$, $high = 8$, and $top = 10$. Based on the system described above, the modeling assumptions concerning the four-phase cooperation process are as follows.

1) *Discovery and request.* The choice of the requestee can be nondeterministic, prioritized (precedence is given on the basis of (i) requestee's reputation and then (ii) requestee availability to negotiate; choice among requestees with the same reputation is random), or probabilistic (probabilities are weighted by requestee's reputation). By default, the chosen requestee i refuses the request of requester j if and only if $T_{ij} < st_i$. The default initial reputation is *low* for every requestee.
2) *Negotiation.* The agreement between i and j is successful. The cost C determined by i through the application of Equation (1) is accepted by j without any further negotiation. The default values are $C_{min} = 0$, $C_{max} = 10$, and $T' = high$.
3) *Transaction.* By default, the service is delivered with success. Then, j decides whether to pay or not, either nondeterministically or probabilistically with parameter $p \in [0, 1]$, namely j pays the obtained service with probability p.
4) *Evaluation and feedback.* Since the service is satisfactory, the reputation of i as perceived by j is increased by 1. On the other hand, the trust of i towards j increases (decreases) by 1 (by a factor k) in the case j pays (or not) the service. Feedback is provided by i to the other requestees.

The reader interested in the PRISM formal specifications of the cooperation model and of the logic-based properties analyzed in the following section can refer to: `http://www.sti.uniurb.it/aldini/prism_uloop/`.

III. MODEL CHECKING OF THE COOPERATION MODEL

The analysis of the cooperation process through model checking is divided into two steps. First, we study the vulnerabilities of the trust-based mechanism with respect to a possibly cheating requester that may decide not to pay the obtained services. Based on the results of such an analysis, we then verify the efficiency of the mixed cooperation incentives in discouraging selfish behaviors of the requestees and motivating honest behaviors of the requester.

 ISBN: 978-1-61208-211-0

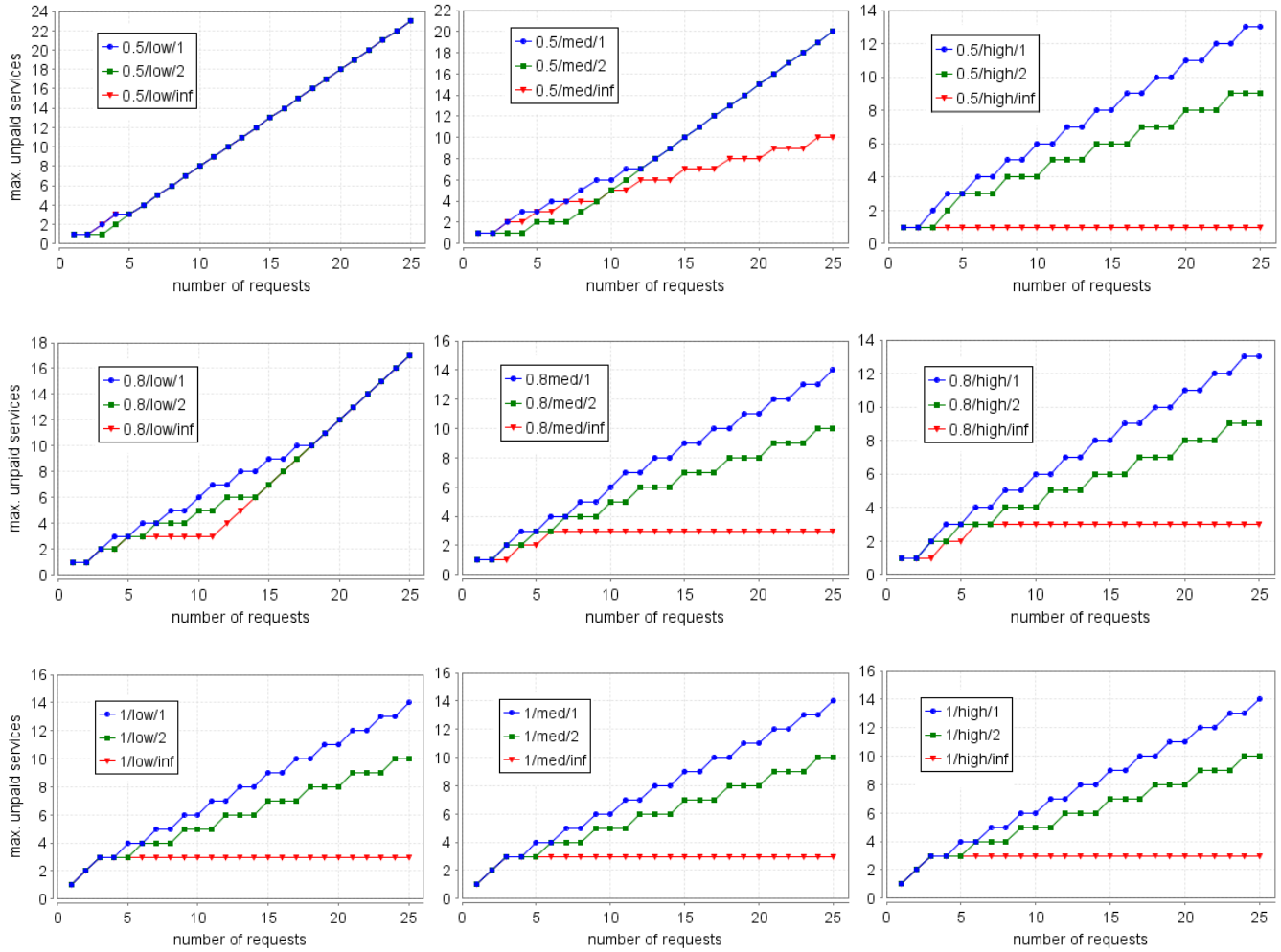


Figure 1: MDP analysis: verification of Property 1 for 27 combinations of parameters $\alpha/st/k$.

A. MDP Analysis

The effectiveness of the trust-based mechanism with respect to cheating requesters is expressed through the following property:

Property 1. What is the maximum number of services (out of nr requests) that can be obtained by a requester without honouring the payment?

This property is investigated in a scenario with a single requester and three alternative requestees. With respect to the assumptions of Section II-C, we consider requester's choices to be nondeterministic. Hence, the requester can be viewed as an adversary controlling the way in which the nondeterminism is solved adaptively. The aim of such an adversary is to find out the strategy maximizing the number of unpaid services, thus revealing the worst case from the viewpoint of the requestees.

Formally, the semantics of the model turns out to be an MDP on which Property 1 is evaluated by solving the nondeterminism in all possible ways. Then, the model checker returns the result for the *best adversary* strategy. Notice that such a strategy corresponds to the most powerful adversary, which can observe the behavior and the configuration parameters of all the requestees.

We assume three equal requestees characterized by the configuration of parameters $\alpha/st/k$, where: $\alpha \in \{0.5, 0.8, 1\}$ is the contribution of direct experience to trust, $st \in \{low, med, high\}$ is the service trust threshold, and $k \in \{1, 2, \infty\}$ denotes the rapidity with which the trust towards a cheating requester is decreased each time a payment is not honoured (∞ stands for the immediate assignment of the value *null* to the trust level). The dispositional trust is chosen to be equal to the service trust threshold in order to make it possible for a new requester to start negotiating services with the requestees.

All the 27 combinations of the parameters introduced above are analyzed, as illustrated in Fig. 1. The horizontal

 ISBN: 978-1-61208-211-0

axis denotes the total number of requests *nr*, ranging from 1 to 25, while the vertical axis reports the maximum number of unpaid services. From the analysis, we observe that for each value of α and st the success of the cheating strategy is inversely proportional to the factor k. In practice, the higher the value of k is, the faster the reaction to dishonest behaviors and, therefore, the negative effect upon trust. For the same reason, the higher the service trust level st is, the lower the number of unpaid services. When $\alpha = 1$, however, the service trust level does not affect the results because any decision depends only on previous direct experience. The analysis could be extended to values of $\alpha < 0.5$, obtaining results similar to those related to $0.5/low/\_$, regardless of the value of st. These results reveal a typical attack of a dishonest requester cheating only one requestee, which gives too much weight to the positive recommendations provided by the other requestees.

The results of Figure 1 suggest to categorize the behavior of the requestee according to two limiting profiles:

- *risky* profile, for which the unpaid services increase linearly and most of the served requests are unpaid (see, e.g., configurations $0.5/low/\_$, $0.8/low/\_$ and $\_/\_/1$).
- *cautious* profile, for which the number of unpaid services is essentially constant (see, e.g., configurations $\_/high/\infty$, $0.8/med/\infty$, and $1/\_/\infty$).

B. DTMC Analysis

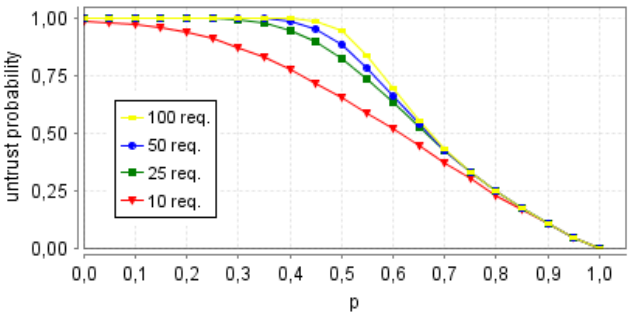
The two profiles defined above give a clear and precise perception of requestee's attitude to take prosocial decisions in an environment where requesters are possibly cheating. This subsection reports the results of further investigations conducted by considering risky requestees represented by configuration $0.5/low/1$ and cautious requestees represented by configuration $0.8/med/\infty$. Whenever the profile is not specified, configuration $0.8/low/1$ is taken as default.

In order to analyze more specific properties, we assume prioritized choice of the requestee and payment honoured probabilistically with parameter p (see Section II-C). Hence, now the semantics of the model is a DTMC, on which both *steady-state* and *transient-state* analyses can be conducted.

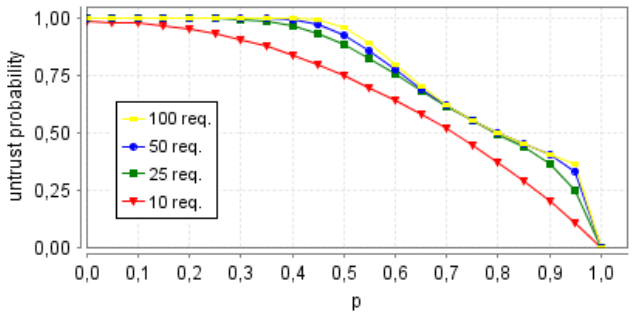
On one hand, the steady-state analysis reveals the success of the cooperation mechanism on the long run. Indeed, it turns out that at steady state for each $p < 1$ the requester becomes untrusted with probability 1 by any requestee. On the other hand, the transient analysis is important to study the convergence speed towards such a result.

Property 2. What is the probability for a cheating requester of being untrusted by each requestee after nr requests?

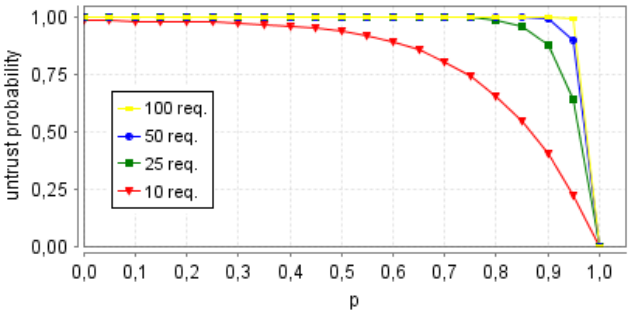
We evaluate this property by varying parameter p and by assuming $nr \in \{10, 25, 50, 100\}$. Moreover, we consider: (i) three risky requestees (see Fig. 2a), (ii) three requestees among which one is risky and one is cautious, while the default configuration is adopted for the third one (see



(a) 3 risky requestees.



(b) 1 risky, 1 cautious, and 1 default requestee.



(c) 3 cautious requestees.

Figure 2: DTMC analysis: verification of Property 2.

Fig. 2b), and (iii) three cautious requestees (see Fig. 2c). All the curves tend rapidly to 1 for $p < 0.5$ and converge to zero as p tends to 1. In particular, notice that in the case of 3 cautious requestees, for $nr \geq 25$ the curves approximate a step function, meaning that a cheating requester is almost immediately untrusted by each requestee.

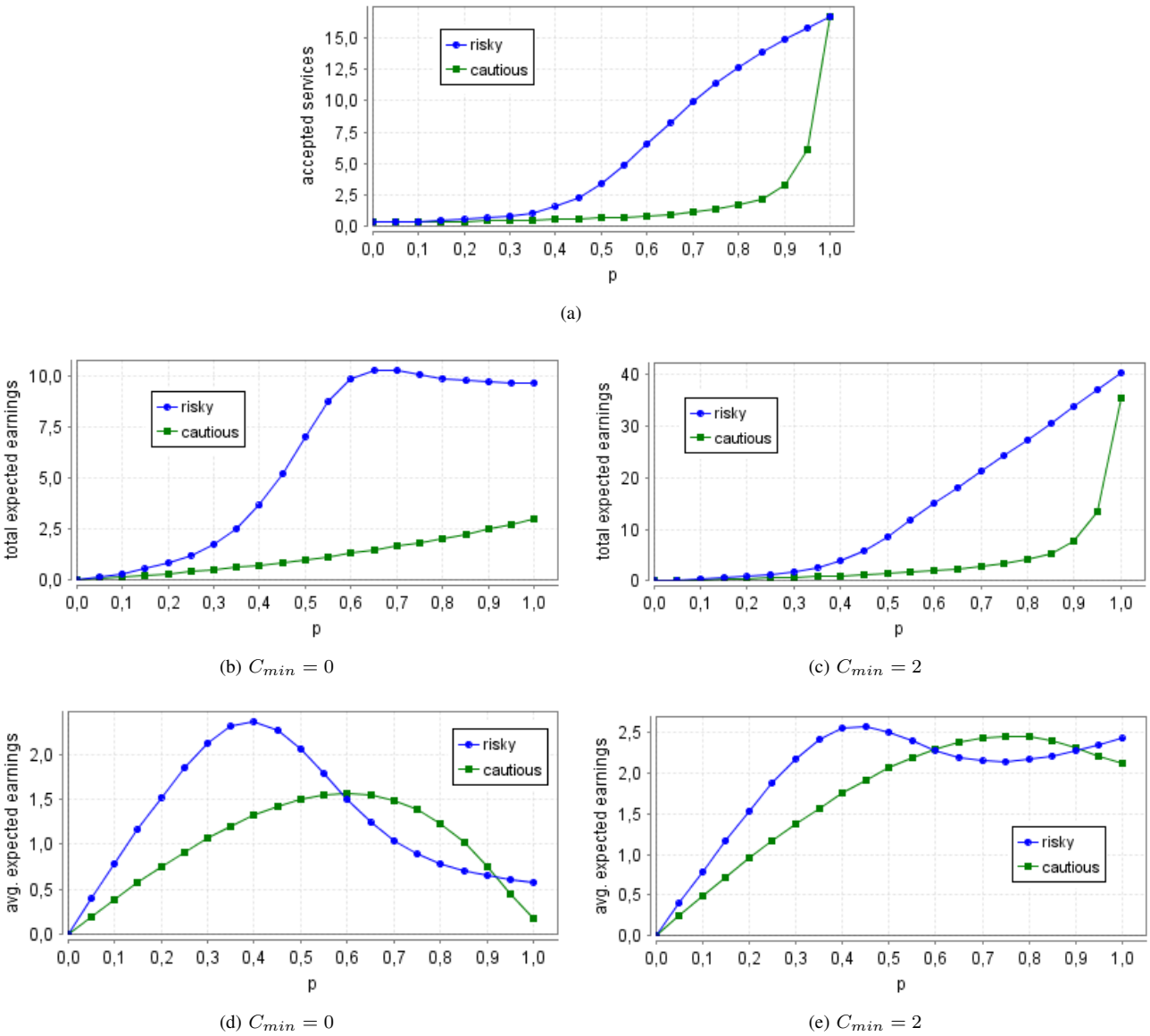
Three more properties are tested in order to investigate the economic aspects of the cooperation mechanism:

Property 3. What is the number of requests accepted by each requestee?

Property 4. What is the total expected earning for each requestee?

Property 5. What is the average earning per accepted request?

 ISBN: 978-1-61208-211-0



(a)

(b) $C_{min} = 0$

(c) $C_{min} = 2$

(d) $C_{min} = 0$

(e) $C_{min} = 2$

Figure 3: DTMC analysis: verification of Properties 3, 4, and 5.

We use these properties to compare the two profiles in a scenario with 50 requests and three requestees like those of Fig. 2b. Fig. 3 reports the performance of the risky and cautious requestees as a function of parameter p. The curves show the following results.

The number of services accepted by the risky requestee is higher than that related to the cautious requestee, see Fig. 3a. The difference is due to the relaxed conditions applied by the risky requestee, in particular the assumption $k = 1$ (resp. $k = \infty$ for the cautious requestee). In fact, by setting $k = \infty$ also for the risky requestee, its curve would collapse with that of the cautious requestee. Notice that in case of honest requester (i.e., $p = 1$), the profile of the requestees does not play any role, so that the requests are equally distributed among them, because they are assigned with the same initial reputation.

As p increases, the total expected earnings of the risky requestee become much higher than those of the cautious one, see Fig. 3b. The difference can be interpreted as a reward for taking more risk.

Similarly, Fig. 3d shows that the average expected reward/cost per service grows with the value of p up to a maximum point beyond which the expected reward/cost decreases because of the effect of the trust-based discount applied to trustworthy requesters. Such a maximum point is reached earlier by the risky requestee, thus motivating the better performance of the cautious requestee for $p \in [0.6; 0.9]$. We also observe that in such an interval the trust level of

 ISBN: 978-1-61208-211-0

the requester becomes stably high from the viewpoint of the risky requestee, as emphasized by the total earnings curve of Fig. 3b. For $p \geq 0.95$, the result is better for the risky requestee, because the requester becomes trustworthy also from the viewpoint of the cautious requestee, with a positive impact upon the number of services such a requestee accepts, see Fig. 3a.

In general, the combined effect of cost function and trust management works as an incentive to adopt a "risky" prosocial behavior. On the other hand, it is clear that the requester obtains more services at a lower average cost whenever adopting a honest behavior.

In order to show that the shape of the reward/cost curves is not purely a side effect of the assumption $C_{min} = 0$, in Figs. 3c and 3e we show the total and average expected reward/cost obtained in the case $C_{min} = 2$. The major earnings with respect to the corresponding curves of Figs. 3b and 3d reflect the difference between the minimum costs applied in the two experiments.

In order to emphasize the effect of parameter k on trust, in Fig. 4 we show the performance of the risky requestee for $k \in \{1, 2, \infty\}$ and by assuming the same scenario of Fig. 3. Observe that the curves related to number of accepted services and total earnings improve their performance as k decreases. Indeed, as we have previously seen, k and tolerance to cheating behaviors are inversely proportional. Instead, we observe the opposite result for the average earnings, because a high value of k corresponds to a fast trust decrease and, therefore, higher costs per service. Also notice that whenever the requester is honest and, as a consequence, k is never used, the three curves converge to the same values.

Similarly, we now study the impact of the dispositional trust. By varying parameter $dt \in \{low, med, high\}$, in Fig. 5 we show the performance for the risky requestee in the same scenario of Fig. 3. Increasing the dispositional trust has a twofold impact. On one hand, it works as an incentive to accept more services and augment the total earnings whenever the requester is not always honest. On the other hand, as p tends to 1, the service cost rapidly converges towards the minimum cost thus impairing the total earnings. The same considerations apply to the analysis of the relation between average reward/cost and dispositional trust.

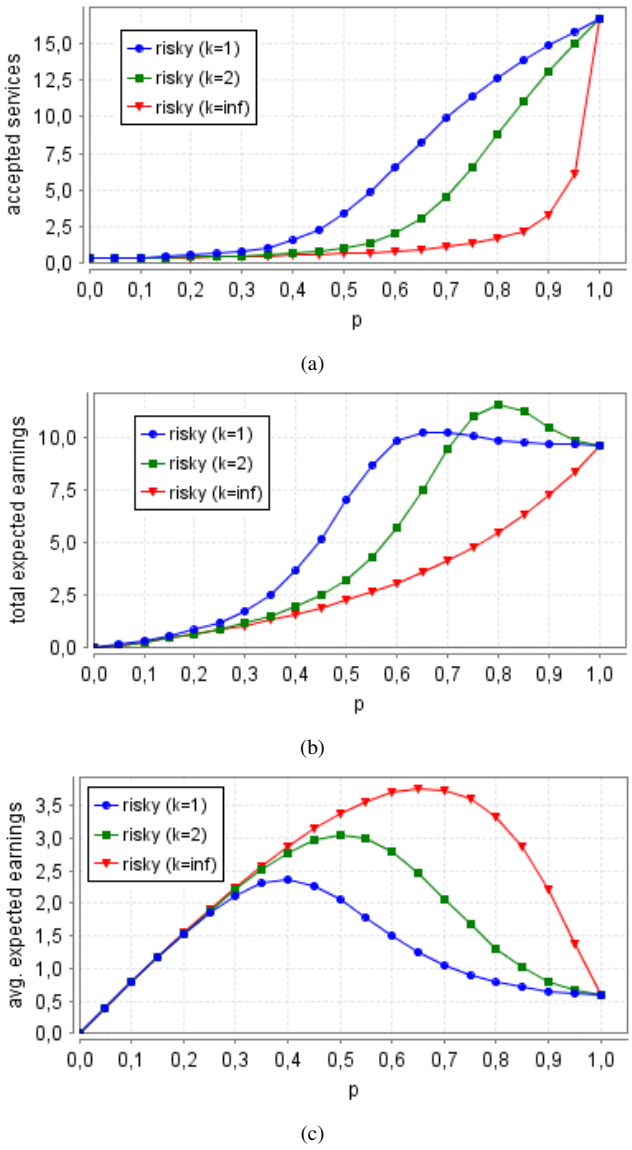


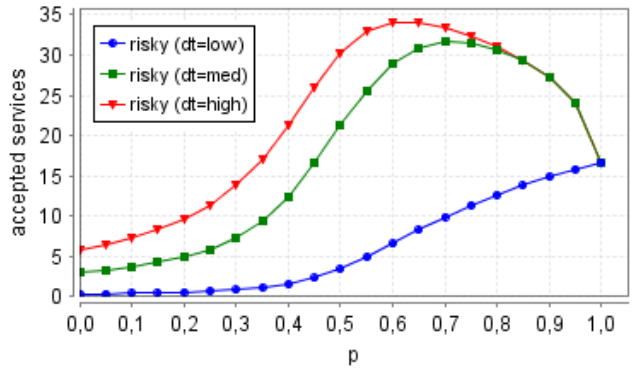
Figure 4: DTMC analysis: verification of Properties 3 to 5 for the risky requestee by varying parameter k.

C. Requestee's Reputation

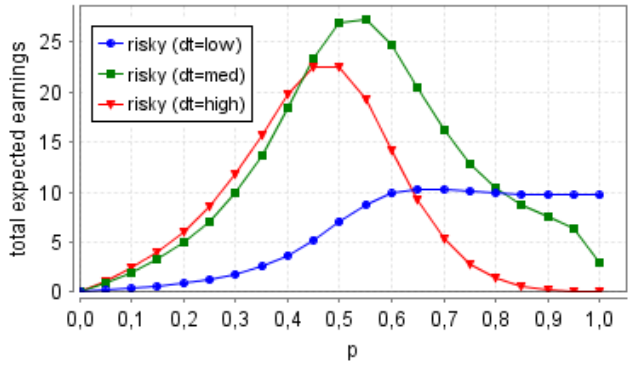
Requestee's reputation is an orthogonal aspect the effects of which are analyzed in Fig. 6. The objective is to measure the impact of requestee's reputation with respect to Property 3. In Fig. 6a we consider prioritized choice of the requestee, one risky requestee with reputation *high*, one cautious requestee with reputation *low*, while the reputation of the third requestee (with default profile) is *med*. Regardless of the profile, all the requests are served by the requestee with highest reputation, as imposed by the choice strategy followed by the requester. In fact, an analogous result would be obtained by swapping the reputations of the risky and cautious requestees. Giving less importance to reputation during the discovery phase has the effect of mitigating such a drastic behavior, as confirmed by the following experiment, in which the prioritized model of choice is replaced by the probabilistic one (see Section II-C). The results, shown in Fig. 6b, emphasize that also the cautious requestee can obtain some service. However, regardless of the value of p, it is always outperformed by the risky requestee.

The effect of requestee's reputation is investigated also by testing the performance of a paranoid requestee ($\alpha = 0.5$, $dt = low$, $st = med$, $k = \infty$) replacing the cautious requestee in the experiment of Fig. 3. In Fig. 7a we evaluate

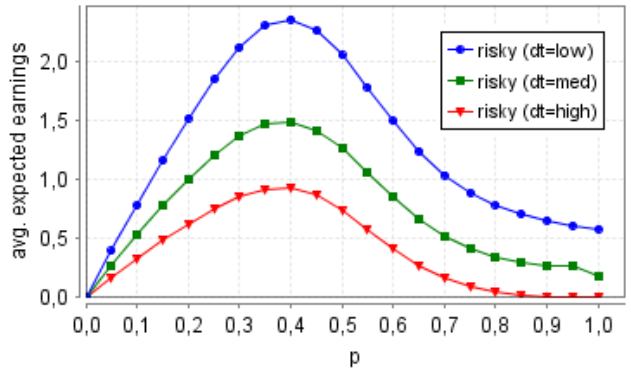
 ISBN: 978-1-61208-211-0



(a)



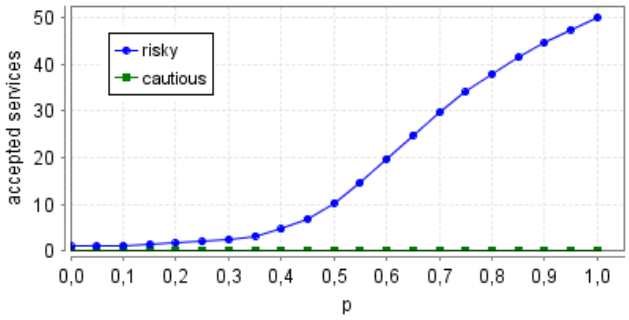
(b)



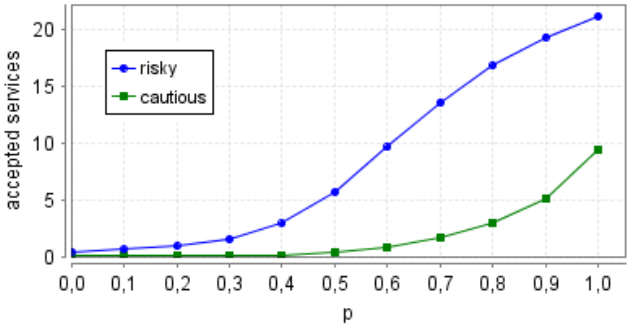
(c)

Figure 5: DTMC analysis: verification of Properties 3 to 5 for the risky requestee by varying parameter dt.

Property 5 for the paranoid requestee in two possible cases depending on its initial reputation. Apparently surprising, a paranoid requestee with reputation *med*, when put in competition with the other requestees (whose reputation is *low*), does not obtain any reward. This result is motivated by the fact that, initially, the paranoid requestee does not accept any request until a sufficiently high number of positive recommendations is received, because its service trust level is higher than its dispositional trust. Moreover, such requests are accepted by the other requestees, which gain reputation,



(a) Prioritized choice (risky rep. = *high*, cautious rep. = *low*)



(b) Probabilistic choice (risky rep. = *high*, cautious rep. = *low*)

Figure 6: DTMC analysis: verification of Property 3 with mixed reputations.

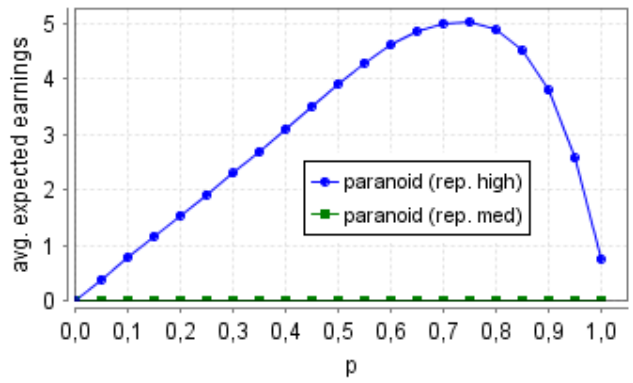
thus causing preemption over the paranoid requestee during the prioritized discovery phase. In order to observe some request served by the paranoid requestee, it is necessary to set its initial reputation to *high*. In this case, we evaluate also Property 3 (see Fig. 7b). Notice that the paranoid requestee accepts a very low number of services for $p < 0.9$, while it outperforms the risky requestee only for $p = 1$, the reason being that the honest requester becomes trustworthy rapidly enough to overcome the non-cooperative attitude of the paranoid requestee.

In a real-world setting, reputation of the requestees may also decrease, e.g., because the quality of the delivered service does not match the negotiated parameters. This aspect is not captured by the experiments reported so far. In order to analyze the importance of requester's feedback, we extend the cooperation model to represent the (possibly negative) change of requestee's reputation due to requester's evaluations. In particular, we model probabilistically with parameter $q \in [0, 1]$ the event of a service failure causing a negative evaluation.

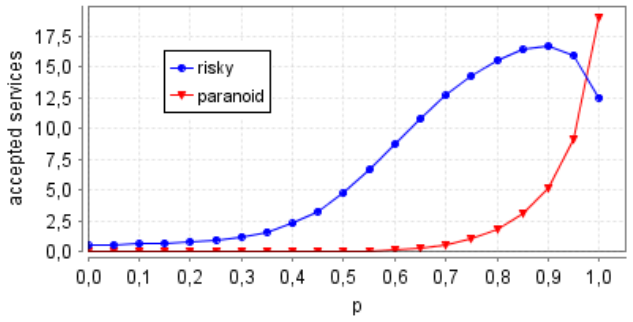
Property 6. How does requestee's reputation impact the number of accepted requests in the case of fallible services?

In a pessimistic scenario, upon each served request requestee's reputation has the same probability (namely, 0.33) of remaining unchanged, being increased by 1, or being decreased by 1. In an optimistic scenario, with probability

 ISBN: 978-1-61208-211-0



(a) risky rep. = *low*



(b) risky rep. = *low*, paranoid rep. = *high*

Figure 7: DTMC analysis: verification of Properties 5 and 3 with paranoid requestee.

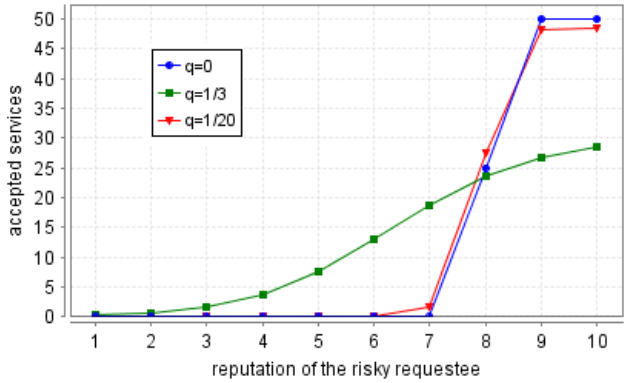


Figure 8: DTMC analysis: verification of Property 6.

0.8 requestee's reputation is increased by 1, with probability 0.15 is maintained, and with probability 0.05 it is decreased by 1. We compare these two scenarios with the original one (modeling an ideal service provider) in which requestee's reputation is always incremented. Therefore, the three scenarios are characterized by $q = 0.33$, $q = 0.05$, and $q = 0$, respectively. Moreover, for the analysis we consider a honest requester, one cautious requestee with reputation *high*, one requestee with default profile and reputation *med*, and one risky requestee. In Fig. 8 we evaluate Property 6 for the risky requestee, by varying its initial reputation from 1 to 10. For $q = 0$, the risky requestee is always outperformed by the cautious requestee in every case in which its initial reputation is less than *high*. The two requestees share the same amount of services if the initial reputation of the risky requestee is *high* as well, while the risky requestee takes all the requests in the remaining cases. These results depend on the fact that the reputation level *high* of the cautious requestee never decreases. The other curves approximate such a behavior (the lower q is, the closer the approximation becomes) and reveal that the possibly negative feedback provided by the requester affects the performance of the requestees.

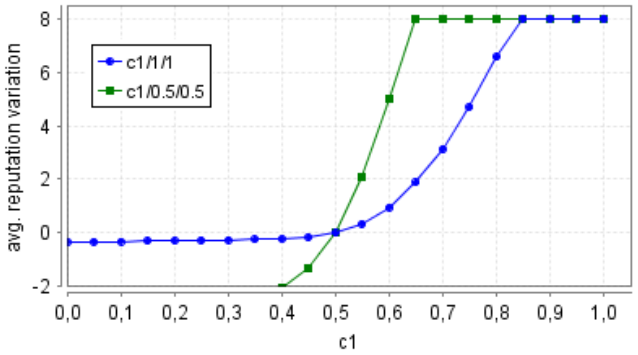
In an orthogonal way with respect to the previous experiment, we now consider the case of non-cooperative requestees, which may refuse a request even if the requester is trustworthy enough to access the service. To this aim, we model probabilistically with parameter $c_i \in [0, 1]$ the cooperative attitude of requestee i, such that i accepts a trustworthy request with probability c_i and refuses it with probability $(1-c_i)$. Obviously, refusing a trustworthy request is evaluated with a reputation decrease, as opposite to the reputation increase determined by a satisfactory service.

Property 7. How does requestee's reputation vary in the case of non-cooperative requestees?

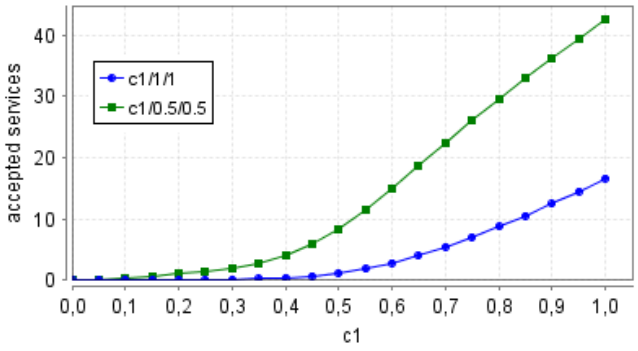
For analysis purposes, we consider a honest requester and three risky requestees with initial reputation $low = 2$. In Fig. 9a we evaluate Property 7 for the first requestee as a function of parameter c_1. In particular, we report its average relative reputation variation after 50 requests in two different cases, depending on the behavior of the other two requestees. In the first case, they are fully cooperative (i.e., $c_2 = c_3 = 1$), while in the second case they are partially cooperative (i.e., $c_2 = c_3 = 0.5$). In general, the lack of cooperation has a negative impact upon reputation of the first requestee, while it converges towards the top level as c_1 increases. We also observe that the reputation variation is slower in the first case with respect to the second case. The reason is that in the first case most of services are required to the two cooperative requestees, whose reputation increases rapidly thanks to their prosocial behavior. In order to emphasize the benefits of cooperative behaviors, in Fig. 9b we evaluate Property 3 for the first requestee in the two cases above. Notice that in the second case the number of services accepted by the first requestee increases dramatically whenever its attitude to cooperate becomes higher than that of the other two requestees.

Finally, we verify how the observed results scale by considering five requestees (four risky and one cautious with the same parameters assumed in the analysis of Fig. 3). It is worth comparing the obtained results, see Fig. 10, with those of Figs. 3a and 3b. The analogy is emphasized by the

 ISBN: 978-1-61208-211-0

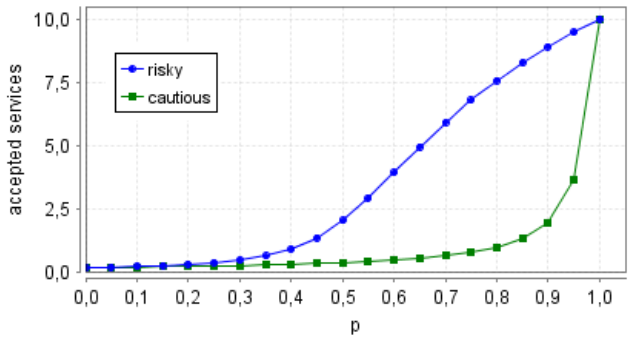


(a)



(b)

Figure 9: DTMC analysis: verification of Properties 7 and 3 with non-cooperative requestees.



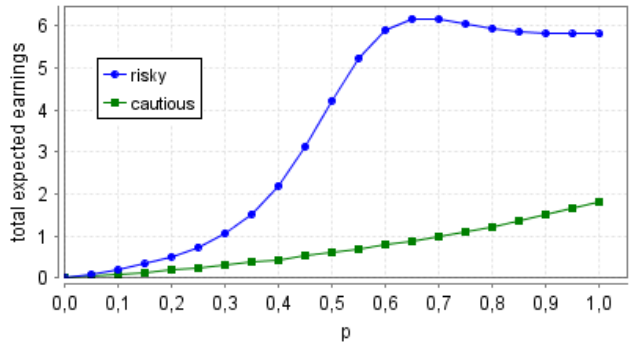


Figure 10: DTMC analysis: verification of Properties 3 and 4 with 5 requestees.

fact that the average expected earnings are exactly the same as those of Fig. 3d.

IV. Conclusion

Mixed incentive strategies, combining reputation and price-based mechanisms, have proved effective in inducing prosocial behaviors while isolating selfish or cheating nodes in a community [6]. A cooperation process entailing both trust management and virtual currency to support mixed incentive strategies has been recently proposed for user-centric wireless networks [4]. This paper has reported the results obtained by applying model checking techniques to provide formal evidence of the properties of such a process.

In summary, cooperation incentives work properly for both the requester and the requestee. On one hand, a honest behavior of the requester is motivated by a higher number of accepted services at a lower average cost with respect to the results obtained by a possibly cheating requester. On the other hand, both the reputation and the cooperative attitude of the requestee have a positive impact upon the amount of delivered services and the related earnings. This relation is exacerbated whenever the requester adopts a prioritized model for choosing the requestee during the discovery phase. Moreover, from the viewpoint of the requestee, cautious choices for the values of dispositional trust, minimum trust level required to access the service, and all the configuration parameters affecting the trust adjustment, impair directly the trading volume and indirectly the reputation if in the same network cooperative requestees are active.

The formal approach adopted in this work is currently under development in order to build a design tool to be used to assist the design and configuration of mixed incentive strategies in real-world user-centric networks. In particular, we are considering variants of the formal model taking into account more requestee's profile combinations and configuration parameter settings. This extended study is intended to integrate the overview provided in this work with a complete sensitivity analysis. We conclude by observing that the perspective provided in this paper is under consideration for being adopted by the ULOOP Consortium [14].

Acknowledgment

The research leading to these results has received funding from the EU IST Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number 257418, project ULOOP User-centric Wireless Local Loop.

References

[1] C.H. Declerck, C. Boone, and G. Emonds. *When Do People Cooperate? The Neuroeconomics of Prosocial decision Making*. Working paper of the Faculty of Applied Economics, University of Antwerp, 2011.

[2] S. Marsh. *Formalizing Trust as a Computational Concept*. PhD Thesis, Department of Mathematics and Computer Science, University of Stirling, 1994.

[3] S. Greengard. *Social Games, Virtual Goods*. Communications of the ACM, Vol. 54, No. 4, pp. 19-22, 2011.

[4] A. Bogliolo, P. Polidori, A. Aldini, W. Moreira, P. Mendes, M. Yildiz, C. Ballester, and J.-M. Seigneur. *Virtual Currency and Reputation-Based Cooperation Incentives in User-Centric Networks*. IEEE Int. Wireless Communications and Mobile Computing Conference (IWCMC-2012), Cyprus, 2012.

[5] A. Jøsang. *Trust and Reputation Systems*. In A. Aldini and R. Gorrieri, eds., Foundations of Security Analysis and Design IV (FOSAD'07), LNCS 4677:209–245, Springer, 2007.

[6] Z. Li and H. Shen. *Game-Theoretic Analysis of Cooperation Incentives Strategies in Mobile Ad Hoc Networks*. IEEE Transactions on Mobile Computing, 2012.

[7] V. Srivastava, J. Neel, A. MacKenzie, R. Menon, L. DaSilva, J. Hicks, J. Reed, and R. Gilles. *Using Game Theory to Analyze Wireless Ad Hoc Networks*. IEEE Communications Surveys and Tutorials 7(4), pp. 46–56, 2005.

[8] V. Forejt, M. Kwiatkowska, G. Norman, and D. Parker. *Automated Verification Techniques for Probabilistic Systems*. In M. Bernardo and V. Issarny, eds., Formal Methods for Eternal Networked Software Systems (SFM'11), LNCS 6659:53–113, Springer, 2011.

[9] M. Kwiatkowska, G. Norman, and D. Parker. *Stochastic Model Checking*. In M. Bernardo and J. Hillston, eds., Formal Methods for Performance Evaluation (SFM'07), LNCS 4486:220–270, Springer, 2007.

[10] R. Alur and T. Henzinger. *Reactive Modules*. Formal Methods in System Design, 15:7–48, 1999.

[11] W.-J. Stewart. *Introduction to the Numerical Solution of Markov Chains*. Princeton, 1994.

[12] R. Segala. *Modelling and Verification of Randomized Distributed Real Time Systems*. Ph.D. thesis, MIT Press, 1995.

[13] C. Baier and J.-P. Katoen. *Principles of Model Checking*. MIT Press, 2008.

[14] ULOOP. *EU IST FP7 ULOOP: User-Centric Wireless Local Loop*. http://uloop.eu, 2010-2013.

 ISBN: 978-1-61208-211-0

Store-and-Forward Protocol Advantage in a M2ANET Network

Ahmed Alghamdi, Raid Alghamdi, John DeDourek, Przemyslaw Pochec
Faculty of Computer Science
University of New Brunswick
Fredericton, Canada
E-mail: a.alghamdi, r.alghamdi, dedourek, pochec@unb.ca

***Abstract*— In this work, the performance of a store-and-forward protocol in M2ANET is investigated. The current protocols in MANETs require an end-to-end connected path between source and destination to transmit data. In a store-and-forward protocol packets are allowed to be carried at any node for a period of time until the node gets connected to another node and is able to retransmit the packets. The store-and-forward protocol is shown to maintain communication even if the end-to-end connection never occurs. Among the proposed store-and-forward protocols the GPS (Global Positioning System) enabled produce the largest throughput in the network.**

Keywords-store-and-forward protocols; disturbance–tolerant network; MANET; M2ANET; network simulation.

I. INTRODUCTION

A network is a number of computers or devices that are connected to each other through physical or wireless links. An Ad Hoc network is a type of local area network where each individual device in this network can communicate directly with any other device in a peer-to-peer style. This arrangement eliminates the involvement of a central device that acts as a base station or a router. Ad Hoc networks operate with the absence of a fixed infrastructure. The nodes in Ad Hoc networks can be hosts as well as routers which allows a message to be transmitted form node to node through the network until it reaches its final destination [1,2].

A MANET (Mobile Ad Hoc Network) is a type of Ad Hoc network with mobile nodes moving around [1,2]. The mobile nodes in a MANET change locations and re-configure connections between the nodes as needed. Due to the spontaneous and dynamic nature of a MANET, routing is a challenge. There are two aspects of MANET networking that are affected by the node movement: (i) changes in the network topology, and (ii) intermittent connectivity [3].

A response to the changes in the network topology is typically built into the MANET routing protocols. A specialized routing protocol for MANETs, like DSR (Dynamic Source Routing) [8], discovers routes dynamically when the source node attempts to send the data, and when a route is broken the protocol initiates a route discovery again.

Intermittent connectivity calls for an altogether different approach to transmitting data in a network. When a permanent path between a source and the destination cannot be maintained, the routing protocol must rely on a store-and-forward approach [4]: the data can be transferred from node to node as a set (bundle) rather than one packet at a time [5]. Such an approach to data transmission is called Delay Tolerant Networking (DTN, also known as Disturbance Tolerant Networking) [5].

We propose to use for communication such a DTN mobile network with nodes moving randomly and sending data using a store-and-forward protocol. Such a network will appear as a formless communication medium consisting of a cloud of mobile nodes. We call this scenario M2ANET for Mobile Medium Ad Hoc Network [17].

We start by presenting a literature review in Section II. We review in details the protocols used in both MANETs and DTNs respectively. In Section III, we discuss our research objective. In Section IV, we describe our proposed solutions. In Section V, we describe the simulation environment. In Section VI, we present the results. Finally, we conclude the paper and give some ideas for future work.

II. STATE OF THE ART

A. Protocols used in MANETs

Many protocols have been proposed to work in MANETs. Each one of these protocols has specific properties and structure to deliver a solution to a problem facing MANETs. A wide range of these protocols have been categorized into three major categories. These categories are Proactive Routing Protocols, Reactive Routing Protocols and Hybrid Routing Protocols [7, 8].

In proactive routing protocols, each node in the MANET network stores a table holding information about the other nodes in the network. Depending on the implementation of the protocol, the table might hold information about every other node in the network or some selective nodes [7]. These tables are updated periodically or whenever the

 ISBN: 978-1-61208-211-0

topology of the networks changes [7, 8, 9]. The protocols in this category differ in the way they update the table/s and the information kept in them. Examples of protocols that fall under this category are DSDV (Destination Sequenced Distance Vector), WRP (Wireless Routing Protocol), GSR (Global State Routing), FSR (Fisheye State Routing), STAR (Source Tree Adaptive Routing) and DREAM (Distance Routing Effect Algorithm for Mobility).

Instead of updating the tables of all the nodes in the network, in Reactive Routing Protocols, updates are only preformed on the nodes that need to send data at a specific time. This is called On-demand routing [7, 8]. This means the route from the source to the destination is determined upon sending. Usually the source floods packets into the network to determine the best route to the destination. The packets flooded are small packets known as route request packets (RREQ) [8]. Based on the acknowledgment/response/replay resulting from sending (RREQ), the best route is chosen to deliver the data. Reactive/On-demand routing is further categorized into two categories known as hop-by-hop routing and source routing [7, 8]. The difference between these two categories occurs in the header of the sent packets. In source routing, the full information of the address is stored in the packet header. In hop-by-hop routing, only the addresses carried by a packet are the final destination address and the next hop address. The source routing is reported to be inefficient due to the overhead resulting from carrying too much information in the packets headers. Reactive/On-demand protocols are reviewed in [8] and include AODV (Ad Hoc On-demand distance vector), DSR (Dynamic Source Routing), ROAM (Routing On-demand acyclic multi-path), LMR (Light-weight Mobile Routing), TORA (Temporally Ordered Routing Algorithm) and ABR (Associativity-Based Routing).

Hybrid Routing protocols adopt a mix of the first and second categories' properties. Hybrid routing protocols are reviewed in [7] and include ZRP (Zero Routing Protocol), ZHLS (Zero Based Hierarchical Link State), DST (Distributed Spanning Trees based routing protocol) and DDR (Distributed Dynamic Routing).

B. Protocols used in DTNs

Due to the repeated end-to-end connection loss, routing in DTN (Disturbance Tolerant Network) is challenging. A store-and-forward approach is used often in such networks [4]. In Store-and-forward, a message is stored in an intermediate node until the node sees an opportunity to retransmit the message. This gives the DTNs the advantage of delivering the message without the need of an end-to-end connection. The routing protocols in a DTN are designed to overcome the problem of repeated disconnections. They are two categories of DTN protocols: Deterministic Routing Protocols and Dynamic or Stochastic routing protocols [10]. In Deterministic DTNs, the future topology of the network is known or could be predicted simplifying finding a route.

In Dynamic DTNs, the topology is not known. Dynamic Routing Protocols differ in the way they make decision to which node a message is forwarded. Two routing strategies are used in DTNs; one approach is called *flooding* (replication-based) routing and the other one is called *forwarding* [12]. In flooding [11, 12, 13], multiple copies of the same message are sent to other nodes in the network. These nodes stores these multiple copies until one of them come in contact with the destination node then; the message is retransmitted and delivered to the destination. The advantage of such a strategy is to increase the probability of a message getting delivered. Different types of flooding have been investigated in the literature. These types include; Two-Hop Relay, Tree Based Flooding, Spray and Wait [14], MaxProp strategy and Epidemic Routing [12]. In Epidemic routing, each node sends the message to be delivered to each other node in range. A node accepts a message only if it does not already have another copy of the same message in its buffer. Flooding strategy suffers from bandwidth consumption due to the multiple copies of the same message circulating in the network. The multiple copies along with the repeated transmissions, lots of storage space are wasted. This raises the need of having a recovery scheme to deal with the copies of the data left in the network after a message is delivered. One solution is to introduce a life time parameter where a message is discarded if it has been carried for a period exceeding its life time. This life time scheme is optimal since the message would not reach the destination if the life time is too short. If it is too long, the storage capacity would be wasted. Another recovery scheme introduces acknowledgments that are flooded into the network once a message is received at the final destination. Each node in the network receives such acknowledgments. Then, it deletes the corresponding message stored in its buffer. These acknowledgments could be used as a way to guarantee successful delivery [10].

Forwarding strategy uses local or global knowledge to find the best path (i.e., the existing shortest path) to deliver a message without having to create multiple copies. One forwarding algorithm is the Single Hop Transmission (Direct Delivery) where the source sends a message to the destination only if the destination is in range [10, 12, 13]. This means that the message does not propagate through the network and needs not to be stored and forwarded by any intermediate node. This type of forwarding suffers from long delays [12, 13]. First Contact Routing is another type of forwarding [10, 12, 13]. In First Contact Routing, a message is forwarded to an in-range randomly chosen neighbor. The decision made to choose a random node is not efficient since this randomly-chosen node might not be moving towards the destination. The drawback in First Contact algorithm is that a message might be exchanged

 ISBN: 978-1-61208-211-0

between only two or three nodes all the time which causes transmission delay or even loss of data.

Another type of forwarding algorithm is location-based routing algorithm [12, 15]. This algorithm makes use of the physical location of the nodes. The physical location could be provided the Global Positioning System (GPS). The best path (i.e., the shortest) is determined upon the location of the source, the destination and the intermediate nodes. One location-based strategy is to forward the message to a node that is closer to the destination than the current node [16]. Another location-based algorithm is called Motion Vector (MoVe) which uses knowledge about location, velocity, and direction of a node to determine the closest and best path to the destination node [16].

C. The Mobile Medium Network Model

While a conventional view of a MANET is a (fully) connected network, we proposed in [17] to use a MANET as simply a medium for establishing a connection between two selected terminal stations. This medium is formed by the MANET nodes with forwarding capability allowing data to propagate through the medium in a way analogous to interaction between gas molecules allowing for the propagation of sound waves in a medium like air. This view differentiates explicitly between two MANET node types: (i) the terminal nodes (two communicating stations), and (ii) the mobile routing nodes (all other nodes in the MANET). We call such a network a **M**obile **M**edium MANET, or M^2ANET (pronounced "*square(d) MANET*" or "*MANET Two*") [17]. The main task of the M^2ANET is to establish communication between the terminal nodes (and not necessarily to link all the MANET nodes into a connected network). We propose to separate the network nodes into two categories: the terminal nodes and the communication nodes. A "cloud" of communication medium nodes forms a medium through which the communication channel is formed. The objective of this proposed research is to demonstrate the principles of the new M^2ANET and to establish the conditions under which a channel is established between two (fixed, or mobile) stations by means of forwarding in a mobile medium network. As opposed to a typical approach of studying MANETs, e.g. the study described in [18], in this scenario some mobile nodes may become isolated without a detrimental effect on the channel formation.

To further the idea of working with a mobile medium rather than having to deal with the individual nodes, we investigated a hypothesis that the performance of a mobile medium network depends on the characteristics of the mobile medium, rather than the performance (continuity of operation) of any one network node [19]. In a simulation experiment we switched the network nodes on and off periodically (i.e., put them to sleep) and shown that, given a sufficient number of nodes, such a network would still be able to transmit data reliably. In other words: in the experiment the performance of the network depended on the characteristics of the medium (*density*) rather than the performance of individual nodes (*on/off states*).

III. OBJECTIVES

In order to exchange messages or packets between any two nodes, the existing MANET networks require an end-to-end direct path. Without a closed path no data gets through to the destination. The same applies to the new M2ANET; the mobile medium only "conducts" the message if it is "continuous" between the source and the destination. In order to overcome this problem, a message may be carried by the intermediate nodes and may have to stay there for some time until the nodes get connected to other nodes, which essentially follows the principle of store-and-forward approach. Then, the message is retransmitted again. In other words, thanks to store-and-forward capability the mobile medium (and M2ANET) acquires some inherent storage capacity, and can breach the temporary gaps in its continuity if they occur. Our objective is to test such a scenario by simulating different versions of store–and-forward protocols for establishing communication between two selected nodes and compare them to a standard scenario when a closed path between terminal nodes is required.

IV. PROPOSED SOLUTIONS

Different versions of store-and-forward protocols are proposed in this paper. The difference between these versions is in the algorithms that are used to forward the packets. The common property which all versions share is the ability to carry/store a message for a while until a connection occurs.

These versions are; (1) First hop in the list routing (FLR), (2) closest hop routing (CHP) and (3) farthest hop routing (FHR). By introducing a GPS location (Global Positioning System), so that the distance to each node in the topology is known, (4) the closest to the destination routing (CGPS) and (5) forwarding to the hop that has the best next location to the destination (NGPS) are proposed. One last version of the store-and-forward protocol is simple flooding. In order to understand the underlying implementation of each version, a brief discussion is mandatory.

The connectivity between the nodes is stored and maintained as a matrix of 0s and 1s, which means not connected and connected respectively. In "First in the list routing", the first node spotted, by the node currently carrying a packet (the carrying hop), is the one the packet is forwarded to. In "closest hop routing", the distance between each connect node is calculated and the packet is forwarded to the one that is closest to the carrying node (in other words, the one having the strongest transmission signal). In "farthest hop routing", the packet is forwarded to the farthest node from the carrying node (in other words, the one having the weakest transmission signal).

 ISBN: 978-1-61208-211-0

In GPS-enabled routing, the current position of the destination is known to all the nodes in the network. In closest to destination routing, the distance between every connected node and the destination is calculated and sent to the carrying hop. The packet then is forwarded to the closest node to the destination. Since there is movement involved in the network, it cannot be guaranteed that the closest node to the destination is not moving away from the destination. To overcome this issue, forwarding to the closest *next location* to the destination is proposed. Rather than sending the packets to the closest current location of the node to the destination, they are forwarded to the node that has the closest next location to the destination.

V. SIMULATION ENVIRONMENT

A customized JAVA simulator was used to simulate the network and to develop the store-and-forward protocol. The JAVA simulator provides a controlled environment for testing the store-and-forward protocol and (unlike a standard off the shelf simulator, e.g., NS2 [20, 22]) provides a full control over the parameters and the algorithms used by the store-and-forward protocol. To simplify the simulation, some assumptions have been made. To be able to accurately monitor the data flow, it was decided that there was only one source sending and one destination giving only one data flow. To better visualize the network as well as to better understand how the intermediate nodes move, the source and the destination were assumed to be stationary with all other nodes mobile. Another assumption is related to the forwarding mechanism. It is assumed that packet transmission and delivery takes exactly 200 ms for every node (forwarding cycle). In 500 byte packets, this corresponds to the link transmission rate of 5kbps (assuming zero propagation time). In each forwarding cycle, only one packet is sent form each node if the node has a packet to transmit. Another assumption is regarding the type of the data flow and the data generator. The data generator is assumed to generate CBR traffic (Constant Bit Rate), with no acknowledgements required, at the source with fixed interval (one packet every 800 ms) between each packet generated. The packet is carried in the node for at most 10 seconds and then, if not retransmitted, is dropped. Buffers were introduced in each node buffering no more than 50 packets at a time. If the buffer is full, it is assumed that the node is not going to receive any more packets until the buffered packets get resent or dropped. In case of the buffers in the sending and receiving end nodes, a drop tail queue was introduce at the source which allow dropping the new generated packets if the buffer is full. At the receiving end, the buffer size is assumed to be infinity due to the fact that the receiving end is the final destination of the packets.

The movement of the nodes is random in our simulator. The way the nodes move is by generating a random X and Y coordinate (treated as the next location and bounded by the network area) and then moving at a constant speed towards this next location. After the next location is reached, it is set to be the current location and a new next location is generated. The movement pattern used in the simulation is the same pattern used by the SetDest utility supplied with NS2.

We investigated the randomness of the movement generated for our custom generator by calculating Variance to Mean Ration (VMR) and comparing it to the standard setdest movement generated in NS2 [22]. Throughout the simulation we divided the area into 64 quadrats, recorded node positions every 10 seconds and counted the nodes falling into 36 interior quadrats of the 8*8 grid. At each instance (101 samples used), the count in each of the 36 quadrats was used to calculate the mean and the variance. The VMR ratios for NS2 setdest and for our generator are plotted in Figure 1. The VMR values for our generator fall in the same range on the VMR value for setdest.

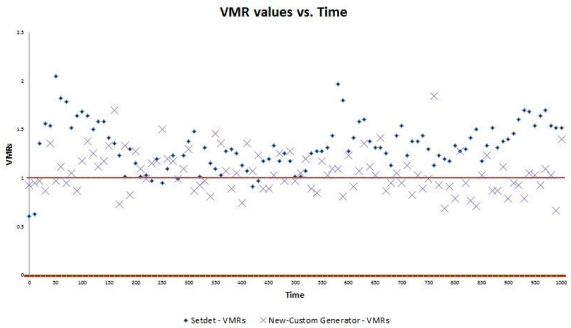


Figure 1. Comparison between setdest and our custom generator.

VI. RESULTS

We run the simulation of M2ANET using five different versions of DTN protocols proposed in Section IV. The results are compared based on the delivery ratio. We compare the number of bits received for different DTN protocols among themselves and against an idealized scenario where data would be transferred between the source and destination over a closed end-to-end path, when it exists. Two simulation scenarios were used in testing. One with N=7 mobile nodes and the other with 50.

Figure 2 shows the end-to-end connectivity between the source and destination during the simulation captured from the first simulation scenario with low density (N=7).

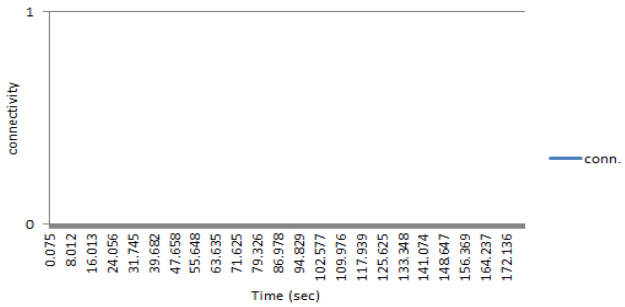


Figure 2. End-to-end connectivity for a scenario with N=7 nodes (connectivity is ZERO all the time).

 ISBN: 978-1-61208-211-0

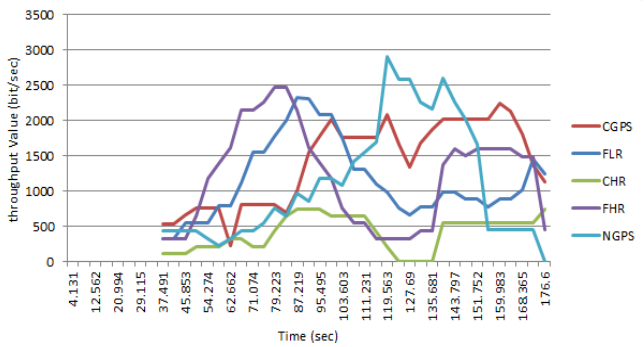


Figure 3. Instantaneous throughput for different protocols for a scenario with N=7 nodes.

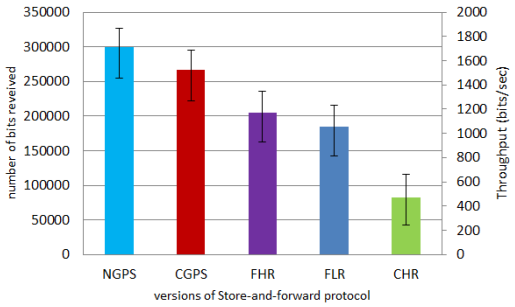


Figure 4. Total number of bits received (N=7).

The graph shows that, in this experiment, the source and the destination are never connected by a closed path. Lack of end-to-end path in conventional MANETs prevents the data from being delivered.

Figure 3 shows the throughput resulting from implementing different versions of the store-and-forward. Although, there was no end-to-end path between the source and the destination, a store-and-forward protocol allows the data to go through and be delivered to the destination. GPS-enabled versions, CGPS and NGPS, allow for the largest amount of data to be delivered.

Figure 4 shows the total number of bits received at the destination resulting from using different versions of store-and-forward protocol. Again, the graph shows that the GPS-enabled versions have the highest delivery.

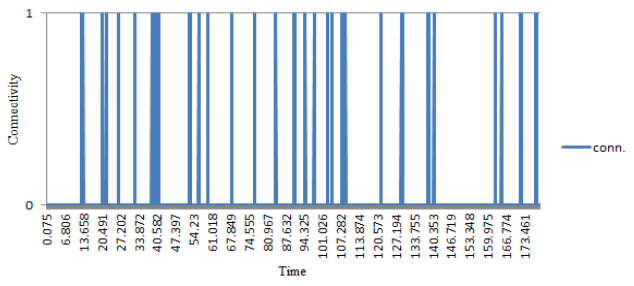


Figure 5. End-to-end connectivity for a scenario with N=50 nodes.

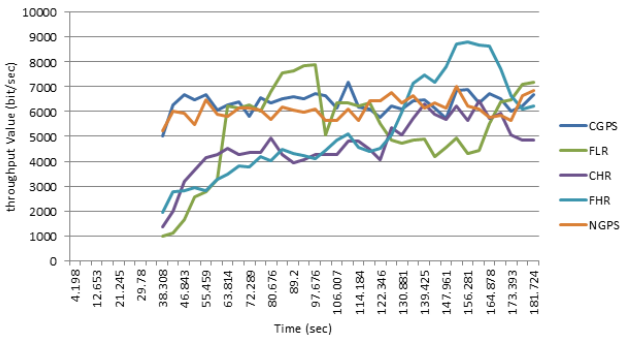


Figure 6. Instantaneous throughput for different protocols for a scenario with N=50 nodes.

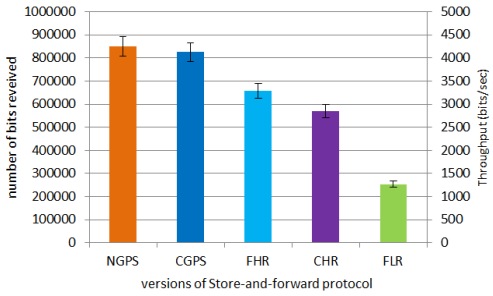


Figure 7. Total number of bits received (N=50).

Figure 5 shows the end-to-end connectivity between the source and the destination in the second experiment with high node density when the number of nodes is 50 (N=50). With more nodes used for the experiment the end-to-end connectivity occurs periodically, i.e., when the mobile nodes are positioned close one to another and forming a path from the source to the destination.

The total time of end-to-end connectivity recorded in this experiment was 6300 ms. If we use 5kbps link rate we can estimate the maximum possible number of bits delivered. The estimated number of bits delivered over the 5kbps connection is 18,000 bits. This would be the maximum throughput achievable using a conventional MANET.

The throughput for the store-and-forward protocol for N=50 is shown in Figure 6. The total number of bits delivered is in Figure 7. For NGPS protocol, we recorded 1,200,000 bits received in the course of the experiment.

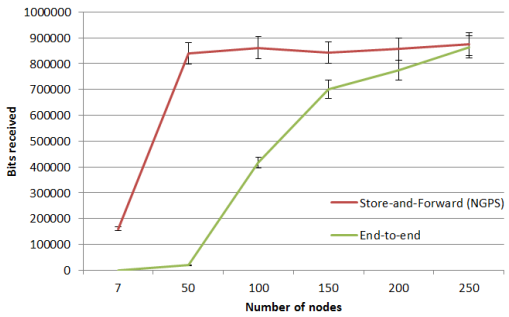


Figure 8. Store-and-forward vs. end-to-end protocols performance.

 ISBN: 978-1-61208-211-0

The clear advantage of the store-and-forward protocols over any protocol based on end-to-end connectivity only is clearly illustrated in Figure 8. The graph show the number of bits delivered from source to destination in a mobile ad hoc network for the best of the investigated store-and-forward protocols (NGPS) vs. the theoretical maximum for any end-to-end connectivity based MANET protocol all simulated at different node density (for the number of nodes ranging from 7 to 250). We observe that a store-and-forward protocol gives the top performance at N=50 nodes, while end-to-end connectivity based protocol requires at least N=250 node to achieve the same number of bits delivered.

VII. CONCLUSION AND FUTURE WORK

We used simulation to compare the number of bits delivered by a M2ANET store-and-forward protocol vs. an end-to-end connectivity based protocol. The simulation shows that, under the simulated conditions, a store-and-forward protocol offers the same throughput (i.e. bits delivered) as connectivity based protocol but with only 20% of the mobile nodes required (N=50 vs. N=250) in M2ANET.

In the future, we plan to investigate the role of mobile node characteristics in M2ANET for example the buffer size and the data retention time at the node on the throughput of M2ANET. We also plan to investigate other performance characteristics of store-and-forward protocols in M2ANET like the propagation delay.

VIII. ACKNOWLEDGMENTS

A part of this work is sponsored and funded by the Ministry of Higher Education of Saudi Arabia through the Saudi Arabian Cultural Bureau in Canada.

REFERENCES

[1] A. Seneviratn and B. Sarikaya, (1998), Cellular networks and mobile internet, *Computer Communications*, 21(14), pp. 1244-1255.

[2] S. Basagn, M. Conti, S. Gioradano and I. Stojeneoric, (2004), Mobile Ad Hoc Networking. Willy-IEEE Press.

[3] Z. Zhang, (2006), Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges, *Communications Surveys & Tutorials, IEEE* , vol.8, no.1, pp. 24-37.

[4] F. Dai, S. Yang and J. Wu, (2007), Logarithmic Store-Carry-Forward Routing in Mobile Ad Hoc Networks, Parallel and Distributed Systems, IEEE Transactions on , vol.18, no.6, pp. 735-748.

[5] S. Burleigh, et al., (2003), Delay-Tolerant Networking: An Approach to Interplanetary Internet, *IEEE Communications Magazine*, pp. 128-136.

[6] K. Fall, (2003), A Delay-Tolerant Network Architecture for Challenged Internets. Karlsruhe, Germany, *SIGCOMM'03*, pp. 27-34.

[7] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, (2003), A Review of Routing Protocols for Mobile Ad Hoc Networks. Elsevier B.V.

[8] N.S. Kulkarni, I. Gupta and B. Raman, (2009), On Demand Routing Protocols for Mobile Ad Hoc Networks: A Review, *Advance Computing Conference, 2009. IACC 2009. IEEE International* , pp. 586-591.

[9] L.A. Latiff and N. Fisal, (2003), Routing Protocols in Wireless Mobile Ad Hoc Network - a review, *Communications, 2003. APCC2003. The 9th Asia-Pacific Conference on*, pp. 600- 604.

[10] A. Socievole, F. De Rango, and C. Coscarella, (2011), Routing approaches and performance evaluation in delay tolerant networks, *Wireless Telecommunications Symposium (WTS)*, pp. 1-6.

[11] M. Balakrishnan, K. Birman, S. Pleisch, and R. Renesse, (2006), MISTRAL: Efficient Flooding in Mobile Ad-hoc Networks. [Electronic Version]. MobHoc, Florence, Italy.

[12] M. Atique and R.S. Mangrulkar, (2010), Routing Protocol for Delay Tolerant Network: A Survey and Comparison. *Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference*, pp. 210-215.

[13] A. Islam and M. Waldvogel, (2008), Reality-Check for DTN Routing Algorithms. *Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Conference*, pp. 204-209.

[14] W. Yu, C. Wu and X. Hu, (2010), Spray and Routing for Message Delivery in Challenged Networks, Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on, pp. 472-475.

[15] Y-B. Ko and N.H. Vaidya, (2000), Location-adid Routing (LAR) in mobile adhoc networks, *Wireless Networks* vol.6, pp. 307-321.

[16] J. LeBrun, C. Chuah, D. Ghosal and M. Zhang, (2005), Knowledge-Based Opportunistic Forwarding in Vehicular Wireless Ad Hoc Networks*Vehicular Technology Conference, 2005, VTC 2005-Spring. 2005 IEEE 61st*, pp. 2289-2293.

[17] J. DeDourek and P. Pochec, (2011), M^2ANET: a Mobile Medium Ad Hoc Network, Wireless Sensor Networks: Theory and Practice, WSN 2011, Paris, France, pp. 1-4.

[18] C. Bettstetter and J. Zangl, (2002) How to achieve a connected ad hoc network with homogeneous range assignment: an analytical study with consideration of border effects", 4th International Workshop on Mobile and Wireless Communications Network, pp. 125-129.

[19] K. Patel, J. DeDourek and P. Pochec, (2011), M^2ANET Performance Under Variable Node Sleep Times, The Third International Conference on Advances in Future Internet, AFIN2011, Nice, France, pp. 31-34.

[20] J. Zhang, W. Li, D. Cui, X. Zhao and Z. Yin, (2009), The NS2-Based Simulation and Research on Wireless Sensor Network Route Protocol, *Wireless Communications, Networking and Mobile Computing, 2009, WiCom '09, 5th International Conference on*, pp. 24-26.

[21] H. Ekram and T. Issariyakul, (2009), Introduction to Network Simulator NS2. Springer.

[22] J. Taylor, (1983), Quantitative Methods in Geography: An Introduction to Spatial Analysis, illustrated version, Waveland Pres.

 ISBN: 978-1-61208-211-0

Ontology-based Mobile Smart Museums Service

Approach for small & medium museums

Alexander Smirnov, Nikolay Shilov, Alexey Kashevnik
Laboratory of Computer Aided Integrated Systems
St. Petersburg Institute for Informatics and Automation of Russian Academy Science
39, 14 Line, St. Petersburg, Russia
smir@iias.spb.su, nick@iias.spb.su, alexey@iias.spb.su

***Abstract*—The proposed service suggest the visitor a museum which is currently better to attend, based on visitor preferences and current situation in the region. For this purpose, smart environments of region museums have to be organized. The smart environment is a decentralized infrastructure which allows different devices to share required information between them. Every user of the smart museum service has a mobile device connected to the smart environment. This mobile device communicates with other devices of the smart environment to suggest the best museum for attending at the moment, and prepares an excursion plan for this museum. Prepared excursion plan based on the visitor's preferences, the current amount of visitors in each museum room and other context information (closed exhibits, reconstructions, seasonal exhibitions and other) acquired from Internet and intranet services. Proposed service increases popularity of small and medium museums in the world, reduces traffic jams in museum rooms, and allow museum visitor to plan his/her time more efficiency way.**

Keywords-knowledge management; ontologies; Internet services; user profiles; smart environment; decentralized architecture; indoor positioning.

I. INTRODUCTION

The paper extends the approach to context-oriented knowledge management for supporting visitors through their mobile device in museum smart environment (presented in AFIN 2011 conference [1]) to assist visitors in an area with several museums.

Recently, the tourist business has become more and more popular. People travel around the world and visit museums and other places of interests. They have a restricted amount of time and usually would like to see many museums. Proposed service increases popularity of small and medium museums in the world. However, overwhelming majority of these museums has limited space for visitors causing accumulation of visitors and increasing waiting time for them.

In this regard an approach is needed, which allows assisting visitors (using their mobile devices), in planning their museum attending time and excursion plans depending on the context information about the current situation in the museum (amount of visitors around exhibits, closed exhibits, reconstructions and other) and visitor's preferences.

Usually, smart and medium museums have a limited amount of money and often purchasing a set of expensive audio guides is not possible for them.

The main benefit of the presented approach is assisting visitors in the museum smart environment using personal mobile devices. Such mobile devices should have Wi-Fi connection and possibility to show appropriate information to visitors.

Main problems of the approach are:

- To organize information sharing possibilities between different devices in museum;
- To determine indoor position of the visitor;
- Tto develop context driven ontology-based approach for assisting visitors in museum.

The smart environment is an aggregation of devices, which can interact with each other and use pertinent services regardless of their physical location. Such technology has a decentralized architecture and allows seamless integration with other systems, services, and program modules.

Decentralized smart environment in the proposed approach allows mobile device of every visitor acquire information from other visitor's mobile devices and services (e.g., museum services or external services) and based on this context information make own decision about the best excursion plan for this visitor taking into account visitor's preferences.

Research efforts in the area of the smart environment have become very popular recently. Such topics of research as smart home, smart car, etc. are widely discussed on research conferences (e.g., Smart Homes [2], RuSMART [3]). In such systems all elements have to interact and coordinate their behavior without any user intervention.

Modern tendencies of information & communication technologies require development of stable and reliable infrastructures to extract and keep different kinds of information and knowledge from various members of the smart environment. The smart environment assumes more than one device that uses common resources and services. One of the most appropriate approaches to implement such infrastructure is applying knowledge management systems.

There is a large amount of research works in the area of indoor positioning, e.g., Google Indoor Maps [4], Qubulus indoor positioning [5], Walkbase indoor positioning platform [6], Ericsson Labs [7], Intel Place Lab [8]. Broadcom

 ISBN: 978-1-61208-211-0

introduces new GPS chip (BCM4752), offering a platform for development of indoor positioning applications [9].

Our experiments show that it is possible to determine visitor's position in the museum using Wi-Fi with accuracy of 2-3 meters. For this purpose, a set of Wi-Fi hot spots should be placed in a certain way.

Museums of a certain area can be considered as a smart environment where each exhibit, group of exhibits, or museum is represented by a service or a set of services. Each device can interact with these services and with other devices. The visitor's mobile devices interacts with each other and with different services in museum smart environment and provides the visitor with an acceptable plan of museum attendance, excursions inside museums based on the museum context (amount of visitors at exhibits, closed exhibits, reconstructions and other) and visitor's preferences.

Visitor's mobile device can also provide textual, graphical, video and audio information about the exhibition for the visitor in his/her language.

The following scenario can be considered. A tourist arrives to St. Petersburg. He/she is going to attend the Hermitage, the Museum of Karl May Gymnasium History, Dostoevsky museum. The tourist adds his/her interests to the user profile within the intelligent museum visitor's support system. The intelligent museum guide suggests the visitor to see the St. Isaac Cathedral and Kunstkamera too. It proposes the visitor to attend at first day the Hermitage, because it is Wednesday (usually on Wednesdays the Hermitage is less crowded). When the visitor's mobile device connects to the museum smart environment, acquires current situation in preferable for the visitor museums and proposes to attend the Dostoevsky museum and Kunstkamera. When the visitor approaches the exhibit he/she gets audio, textual and video information about it from appropriate services through the Internet or intranet.

The rest of the paper is structured as follows. Section II presents an overview of mobile museum guides systems and indoor positioning systems. Section III introduces developed approach to knowledge management in museums smart environment. Information model of museum visitor's profile is given in Section IV. The case study can be found in Section V. Main results are summarized in Section VI.

II. RELATED WORK

There are several research works and projects related to assisting visitor in museum and providing information about museum exhibition. The following ones are worth to be mentioned.

Google Art Project [10] is a tool from Google that lets user visit world's most important museums of art, via a virtual tour. The Art Project is available for more than a thousand works of art.

The overall objective of the SMARTMUSEUM project [11] is to develop a platform for innovative services enhancing on-site personalized access to digital cultural heritage through adaptive and privacy preserving user profiling.

The main research activity of HIPS project [12] is development of an approach for navigating artistic physical spaces (i.e., museums, art exhibitions). The system is meant to provide the visitor with personalized information about the relevant artworks nearby. The information is mainly audio in order to let the user enjoy the artworks rather than interacting with the tool.

Bohnert et al. [13] describe a system for providing a visitor with a challenge of selecting the interesting exhibits to view within the available time. It includes the recommendation and personalization process, i.e., the prediction of the visitor's interests and locations in a museum on the basis of observed behavior.

Kuflik et al. [14] describe an approach for supporting users in their ongoing museum experience, by modeling the visitors, "remembering" their history and recommending a plan for future visits. This approach identifies some of the technical challenges for such personalization, in terms of the user modeling, ontologies, infrastructure and generation of personalized content.

Project CRUMPET [15] has realized a personalized, location-aware tourism service, implemented as a multi-agent system with a concept of service mediation and interaction facilitation. It has had two main objectives: to implement and trial tourism-related value-added services for nomadic users across mobile and fixed networks, and to evaluate agent technology in terms of user-acceptability, performance and best-practice as a suitable approach for fast creation of robust, scalable, seamlessly accessible nomadic services.

Existing systems don't take into account information about the current situation in the museum, and they are oriented to assist user only in one museum whereas the proposed approach allows monitoring the current situation in several museums and its using for visitor assistance. Also, the approach presented in the paper allows using visitor's mobile device for assisting the user. It is not needed to provide special equipment for museums.

Therefore, the indoor positioning problem needs to be considered.

F. Bohnert et al. [16] mentioned that there are two major schemes of indoor positioning: signal propagation and location fingerprinting. They have proposed several algorithms (based on both schemes) for indoor positioning and compared it. Each algorithm has advantages and drawbacks described in the paper in detail.

In [17] T. Kuflik et al. present Wi-Fi-based indoor positioning technique with position accuracy of one to three meters. The technique was tested on the Nokia 770 Internet tablet.

Place Lab [8] project's aim is to determine user location indoor and outdoor. Technically, the system is based on radio beacons, which periodically sent radio signals by Wireless LAN access points, fixed Bluetooth stations, and GSM towers. Accuracy of the presented approach is 13-30 meters.

EZ Localization algorithm is presented in [18]. It is a configuration-free indoor localization scheme that uses existing Wi-Fi infrastructure to localize mobile devices. The accuracy of EZ approach is about 2 meters.

 ISBN: 978-1-61208-211-0

The Horus [19] is a WLAN Location Determination system characterized by high accuracy: through a probabilistic location determination technique and low computational requirements: through the use of clustering techniques.

RADAR [20] is a radio-frequency based system for locating and tracking users inside buildings. RADAR is based on empirical signal strength measurements as well as a simple yet effective signal propagation model. Accuracy of the RADAR is a few meters.

In [21], an indoor localization application leveraging the sensing capabilities of the current state of the art smart phones is presented. Application is implemented for the using on smart phones and it integrates offline and online phases of fingerprinting. Accuracy of presented approach is up to 1.5 meters.

There are many systems and services which solve the problem of indoor positioning. Some considered papers propose algorithms and some propose the complete services or applications which can be used for determining indoor position.

III. ONTOLOGICAL APPROACH OF SMART MUSEUMS SERVICE

The approach presented in the paper relies on the ontological knowledge representation. The conceptual model of the proposed ontological approach is based on the earlier developed ideas of knowledge logistics [22]. In this work, the ontology is used to describe knowledge and information in the smart environment. It allows providing interoperability between different devices in smart environment.

The architecture of the approach is presented in Figure 1. Mobile devices interact with each other through the smart environment. Every visitor installs smart environment client to the mobile device. This client shares needed information with other mobile devices in the smart environment. So, each mobile device can acquire only shared information from other mobile devices. When the visitor registers in the service, his/her mobile device creates the visitor's profile (which is stored in a cloud and contains long-term context information of the visitor). This profile allows specifying and complements visitor requirements in the smart environment and personifying the information and knowledge flow from the service to the visitor. Utilizing of clouds for keeping user profiles allows visitors to change their mobile devices without loosing any settings for using the system. As clouds keep only user profiles, which consist of small amount of data, it is not needed to think about performance of this access.

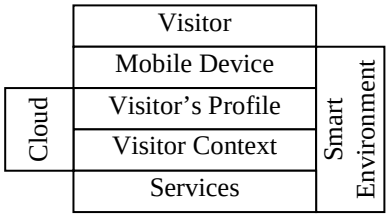


Figure 1. Architecture of the proposed approach

Each time when the visitor appears in the smart environment, the mobile device shares information from the visitor's profile with other devices.

Visitor context accumulates and stores current information about the visitor in the smart environment (current visitor context). It includes:

- Visitor location;
- Museum reaching times for the visitor;
- Current weather (in case of rain it is better to attend indoor museums);
- Visitor role (e.g., tourist, school teacher);
- Information about closed at the moment museums or exhibits;

For getting external information for different system modules, the services are used. Four types of services are proposed:

- Positioning service (calculates current indoor and outdoor positions of the visitor based on raw data provided by visitor mobile device);
- Information service (provides visitor mobile device with needed information about exhibits, e.g., Wikipedia, Google Art Project, other information services, museum internal information services);
- Current situation service (provides information about the current situation in the region, e.g., weather, GIS information, traffic information);
- Museum / exhibition (provides information related to the museum and exhibits, e.g., holidays, closed exhibits).

The proposed ontological approach to Smart Museums Service is presented in Figure 2.

Each visitor has a mobile device, which communicates with mobile devices of other visitors (shares own information to them and gets needed information), uses different services for getting and processing information, accesses and manages the visitor's profile, and processes information and knowledge stored in visitor context.

Visitor's profile and context have stored in the cloud, which allows visitors to access them from any internet enabled devices (when the visitor changes his/her mobile device it is needed only to install the appropriate software to use the new device). Also, clouds allow transferring complex calculations from mobile devices to the clouds.

The visitor context is formed based on the interaction process between the visitor's mobile device and different services through the smart environment. The context is the description of the visitor's task in terms of the ontology taking into consideration the current situation in the museum. Visitor's task in the proposed approach is a list of museums the visitor would like to attend.

Ontology in the smart environment is used for the interoperability support of different mobile devices and services. It describes the main terms used for the museum smart environment description and relationships between them. Mobile devices and services use the ontology for the information and knowledge exchange.

The following scenario for using the proposed service is considered.

 ISBN: 978-1-61208-211-0

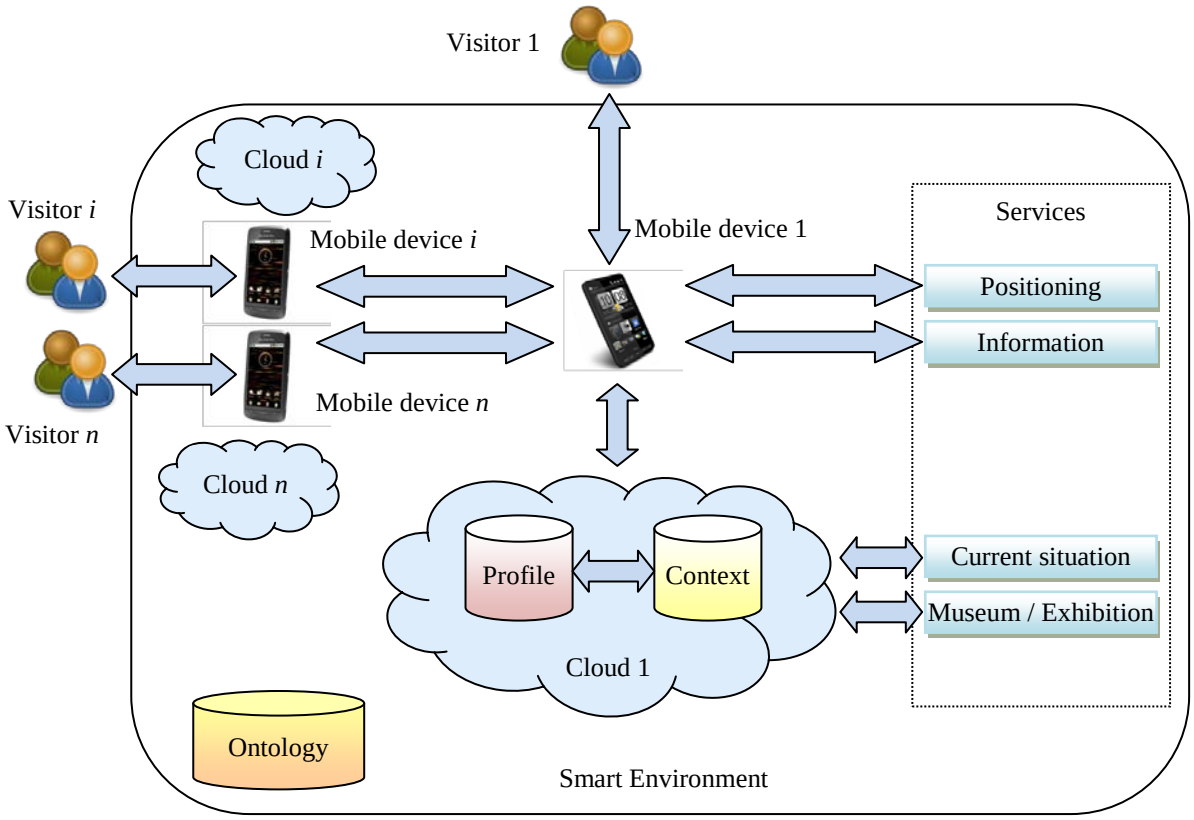


Figure 2. Ontological Approach of Smart Museums Service

A visitor arrives to a region. His/her mobile device finds the museums the visitor is going to attend in this region (stored in the visitor's profile). The mobile device generates the context, which describes the current situation of this region. It connects to different services to extract information about interesting museums (working time, closed museums, closed exhibitions, statistical occupancy of interesting museums for the next few days) and propose to the visitor preliminary interested museums attending plan.

When the visitor is going to attend the museum (next day), the mobile device updates the context by current situation in the region, e.g.: weather (in case of rain it is better to postpone attending outdoor museums), traffic situation on the roads, current museum occupancy, and expected museum occupancy (based on communicating with mobile devices of other visitors). Based on this information, the corrected museum attending plan can be proposed to the visitor.

When the visitor enters the museum an acceptable path for visiting museum rooms is built based on the museum room occupancies at the moment. Using location service and Wi-Fi infrastructure the mobile device calculates the visitor's location and shares it with other devices. Information about exhibits is acquired from the information service and displayed on the visitor's mobile device.

IV. VISITOR'S PROFILE

Most of user profile models include such information as: first name, last name, gender, date of birth, languages, and contact information and user position. This information is also important for intelligent museum visitor's support. Based on this information the service can update the excursion plan for the visitor. The visitor can hide his/her personal information from other visitors for privacy purposes. It is stored in the "Personal Information" module (Figure 3).

Museum visitors can have different roles (e.g., individual visitor, family, group of schoolchildren and other). Intelligent museum visitor support system can take into account this information for building the plan of the excursion. Some parts of the visitor's profile can be hidden from other visitors (for example, if the visitor would like to attend museum anonymously). For this purpose the visitor has to choose which information can be accessible to other devices. It is needed to provide the system with information about visitor's hardware and software capabilities, because based on this information the system suggests the visitor which types of exhibit descriptions (audio, video, textual) he/she can use. This information is stored in the "System Information" module (Figure 3).

 ISBN: 978-1-61208-211-0

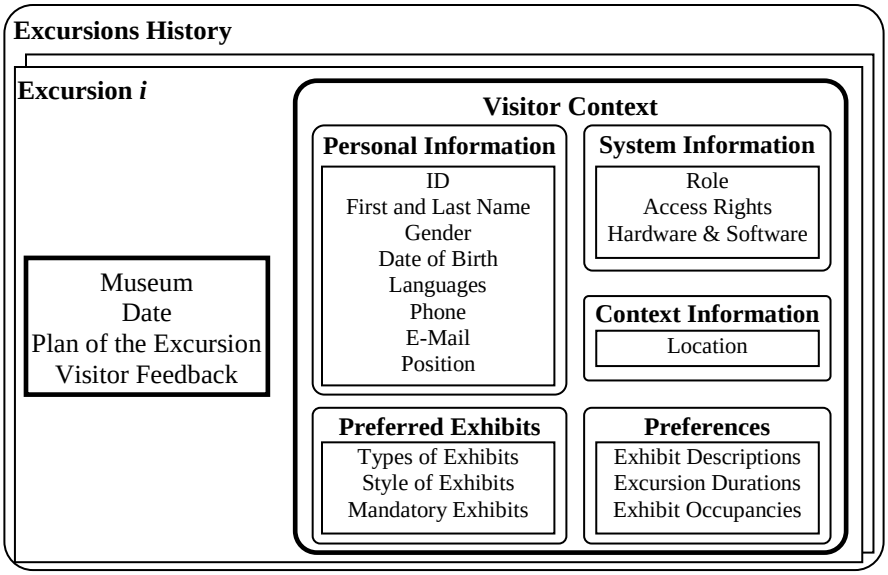


Figure 3. Model of museum visitor's profile in intelligent museum visitor's support system

Since the proposed service is context-oriented, it is necessary to determine the location of the visitor in time. For this purpose the module "Context Information" is proposed. For building an acceptable plan of the excursion the service needs information about exhibits preferred by the visitor: types of exhibits (paintings, ancient items and other), styles of exhibits (modern, impressionism and other), and mandatory exhibits the visitor has to see (e.g., Benois Madonna, the Hermitage). Also, the visitor's profile has to keep the long-term context information about preferable types of exhibit description (audio, video or/and textual), excursion duration (how much time the visitor can spend at this museum), exhibit occupancies (in case of high occupancy of an exhibit the visitor might prefer to skip this exhibit or to try to see it later).

To keep the history of interaction between the visitor's device and the museum smart environment for its further analysis, all excursions of this visitor, including the museum name, date, plan of the excursion, visitor's feedback about the excursion, and the visitor's context at the moment of excursion are stored in the visitor's profile. Based on this information, the visitor's preferences and preferred exhibits can be semi-automatically identified using ontology-based clustering mechanisms described in [23].

V. CASE STUDY

The intelligent museum visitor's support system has been implemented based on the proposed approach. Maemo 5 OS – based devices (Nokia N900) and Python language are used for implementation.

An open source software platform (Smart-M3) [26] that aims to provide a Semantic Web information sharing infrastructure between software entities and devices is used for system implementation. In this platform the ontology is represented via RDF triples. Communication between software entities is developed via Smart Space Access Protocol (SSAP) [26].

Different entities of the system are interacting with each other through the smart environment using the ontology. Each device has a part of this ontology and after connecting to smart environment it shares a part of the own ontology with the smart environment.

The system has been partly implemented in the Museum of Karl May Gymnasium History [27] located in St. Petersburg Institute for Informatics and Automation Russian Academy of Science building.

The visitor downloads software for getting intelligent museum visitors support. Installation of this software takes few minutes depending on operating system of mobile device (at the moment only Maemo 5 OS is supported). When the visitor runs the system for the first time the profile has to be completed. This procedure takes not more than 10 minutes.The visitor can fill the profile or can use a default profile. In case of default profile the system can not propose preferred exhibitions to the visitor.

Response time of the Internet services depends on the Internet connection speed in the museum, number of people connected to the network, and workload of the services. Average response time should not exceed one second.

A museum attending plan is presented in Figure 4. It consists of five museums: the Hermitage, Kunstkamera, the Museum of Karl May Gymnasium History, St. Isaac Cathedral, Dostoevsky museum.

Three top screenshots (Figure 5) present the visitor's profile. According to the model of museum visitor's profile in intelligent museum visitor's support system it consists of personal information, system information and visitor preferences (preferred exhibits and other preferences). The fourth screenshot shows an exhibit description acquired from an external Internet service (e.g., Wikipedia).

 ISBN: 978-1-61208-211-0

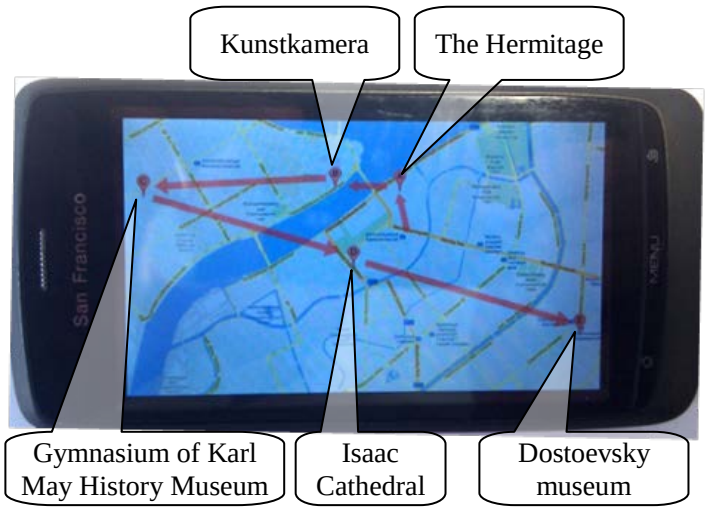


Figure 4. A smaple of museum attending plan in a visitor mobile device in the center of St. Petersburg.

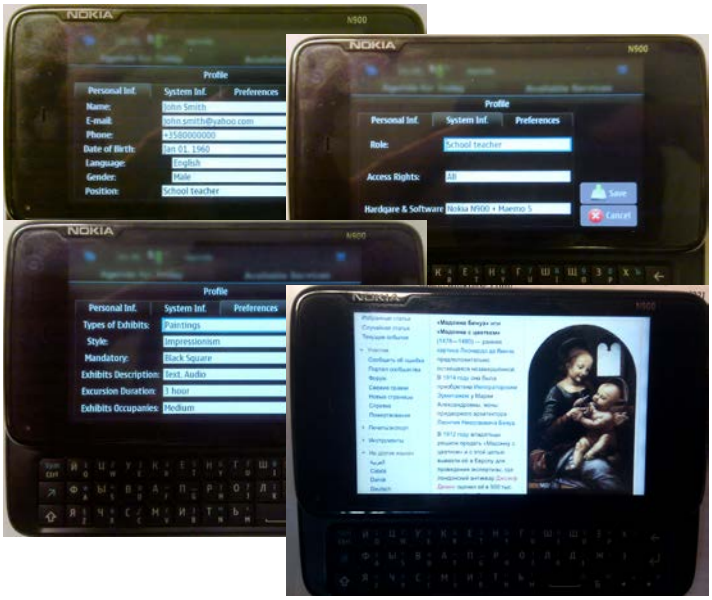


Figure 5. A sample of visitor's profile and exhibition description on the visitor mobile device.

VI. CONCLUSION

The paper presents an innovative ontology-based approach to mobile smart museums service for supporting visitors in museum smart environment in a region using their mobile devices. This approach allows devices of different visitors to interact with each other for the purpose of generating personal museums attending plan and guiding visitor in the area of museum. User profiles allow keeping important information about the visitor and using it in the smart environment.

Since there is no the centralized server in the proposed system, the performance is affected by the number of visitors indirectly. If there are many visitors using the system, the bottleneck of the system performance will be network capacity and Internet services.

ACKNOWLEDGMENT

The paper is a part of the research carried out within the ENPI project KA322 Development of cross-border e-tourism framework for the programme region (Smart e-Tourism); projects funded by grants # 12-07-00298-a, 11-07-00045-a, and 10-07-00368-a of the Russian Foundation for Basic Research; project # 213 of the research program "Intelligent information technologies, mathematical modeling, system analysis and automation" of the Russian Academy of Sciences; project 2.2 of the Nano- & Information Technologies Branch of the Russian Academy of Sciences; and contract # 14.740.11.0357 of the Russian program "Research and Research-Human Resources for Innovating Russia in 2009-2013".

 ISBN: 978-1-61208-211-0

REFERENCES

[1] A. Smirnov, N. Shilov, and A. Kashevnik, Context-Oriented Knowledge Management for Intelligent Museum Visitors Support, The Third International Conference on Advances in Future Internet (AFIN 2011), August 21-27, 2011 Saint Laurent du Var, France, pp. 120-125.

[2] Smart Homes international conference, URL: http://www.smarthomes2011.com/, last access date: 06.06.2012.

[3] RuSMART international conference, URL: http://rusmart.e-werest.org/2011.html, last access date: 06.06.2012.

[4] Google Indoor Maps, electronic resource, 2012: http://support.google.com/gmm/bin/answer.py?hl=en&answer=1685872.

[5] Qubulus indoor positioning homepage, electronic resource, 2012: http://www.qubulus.com/.

[6] Walkbase indoor positioning platform, electronic resource 2012: http://walkbase.com/.

[7] Ericsson Labs, electronic recourse, 2012: https://labs.ericsson.com/apis/indoor-maps-and-positioning/documentation.

[8] D. Kölsch, The Place Lab Project, Mobile Business Seminar, 2006.

[9] EE Dailynews, 2012, electronic resource: http://www.eedailynews.com/2012/03/broadcom-introduces-new-gps-chip.html.

[10] N. Proctor, The Google Art Project: a new generation of museums on the web?, Curator: The Museum Journal, vol. 54, Issue 2, pages 215–221, april 2011

[11] A. Kuusik, S. Roche, and F. Weis, SMARTMUSEUM: Cultural Content Recommendation System for Mobile Users, ICCIT2009 (IEEE/ACM) Int Conference on Computer Sciences and Convergence Information Technology, Seoul, Korea, Nov 2009.

[12] A. Bianchi and M. Zancanaro, "Tracking Users' Movements in an Artistic Physical Space," Proc. of the i3 Annual Conference. 1999, pp. 103–106.

[13] F. Bohnert, I. Zukerman, and S. Berkovsky, T. Baldwin, and L. Sonenberg, "Using Interest and Transition Models to Predict Visitor Locations in Museums," AI Communications, vol. 21(2-3), Apr. 2008, pp. 195–202.

[14] T. Kuflik, J. Kay, and B. Kummerfeld, "Lifelong Personalized Museum Experiences," Proc. Pervasive User Modeling and Personalization (PUMP'10), June 2010, pp. 9–16.

[15] B. Schmidt-Belz, A. Zipf, H. Laamanen, and S. Poslad, "Location-based Mobile Tourist Services: First User Experiences," International Conference for Information and Communication Technologies in Tourism, 2003, pp. 115–123.

[16] B. Li, J. Salter, A. Dempster, and C. Rizos, Indoor Positioning Techniques Based on Wireless LAN, first IEEE international conference on wireless broadband and ultra wideband communications, 2008.

[17] M. Hermersdorf, Indoor Positioning with a WLAN Access Point List on a Mobile Device, proc. Workshop on WorldSensorWeb, 2006.

[18] K. Chintalapudi, A. Iyer, and V. Padmanabhan, Indoor Localization Without the Pain, Proceedings of the sixteenth annual international conference on Mobile computing and networking, 2010.

[19] M. Youssef, and A. Agrawala, The Horus WLAN Location Determination System, Journal Wireless Networks, vol. 14 Issue 3, pp. 357-374, 2008.

[20] P. Bahl and V. Padmanabhan, RADAR: An In-Building RF-based User Location and Tracking System, Proceedings of IEEE Infocom, 2000.

[21] E. Martin, O. Vinyals, G. Friedland, and Ruzena Bajcsy, Precise Indoor Localization Using Smart Phones, Proceedings of the ACM International Conference on Multimedia, Florence, Italy, pp. 787-790, 2010.

[22] A. Smirnov, M. Pashkin, N. Chilov, T. Levashova, and A. Krizhanovsky, "Knowledge Logistics as an Intelligent Service for Healthcare," Methods of Information in Medicine, vol. 44, no 2, 2005, pp. 262–264.

[23] A. Smirnov, M. Pashkin, T. Levashova, A. Kashevnik, and N. Shilov, "Context-Driven Decision Mining," Encyclopedia of Data Warehousing and Mining, Information Science Preference, Second Edition, vol. 1, 2008, pp. 320–327.

[24] D. Signore, "Ontology Driven Access to Museum Information, "Annual Conference of the International Committee for Documentation of the International Council of Museums, May 2005.

[25] H. Mareka and W. Ron, "Ontology-based user modeling, in an augmented audio reality system for museums, " User Modeling and User-Adapted Interaction, vol. 15(3-4), 2005, pp. 339–380.

[26] J. Honkola, H. Laine, R. Brown, and O. Tyrkko, "Smart-M3 information sharing platform," The 1st Int'l Workshop on Semantic Interoperability for Smart Spaces (SISS 2010), June 2010.

[27] Gymnasium of Karl May History Museum web page: http://www.spiiras.nw.ru/modules.php?name=Content&pa=showpa&pid=8 (In Russian, last access date: 03.06.2011).

 ISBN: 978-1-61208-211-0

Internet Portal of the SEMONT Information Network for the EM Field Monitoring

Nikola Djuric
Faculty of Technical Sciences, University of Novi Sad
Trg D. Obradovica 6
21000 Novi Sad, Serbia
e-mail: ndjuric@uns.ac.rs

Nikola Kavecan
Falcon-Tech, IT Consulting, Development
Dusana Danilovica 1,
21000 Novi Sad, Serbia
e-mail: nikola@kavecan.com

***Abstract* – Recently, the electromagnetic pollution of the environment starts to be a highly important scientific and research concern. Growing number of the electromagnetic field sources have caused the increased interest of the public about potentially harmful effects of the long-term exposure to the electromagnetic radiation. As support for the efforts to inform public about the real-time and the overall level of the electromagnetic field in the environment, our team proposed wireless information network – SEMONT, intended for remote and continuous, 24 hours a day based, monitoring. This paper briefly explains the work in progress related to development of SEMONT system and dedicated Internet portal for the public presentation of the measuring results. Information network SEMONT is a unique project at national level and develops within the program of technological development of the Republic of Serbia, for the period of 2011-2014 year.**

Keywords – electromagnetic field; radiation exposure; wireless network; monitoring

I. INTRODUCTION

The electromagnetic (EM) radiation starts to be ordinary phenomenon in the last few decades. It is considered in many scientific articles, since introduction of the any modern wireless transmission technology results with a variety of the EM field sources, particularly in range of the non-ionizing radiation [1]. Their presence increases level of the EM field in the environment, since they are simultaneously present and most likely emits the EM field over the same area as sources that already exist in a power system and systems for the power transmission (transmission lines, distribution and substation equipment), together with sources from systems of radio and TV broadcasting.

Diversity of the EM field sources characteristics enforces the problem of the safety of these devices both for the human health and the environment. In the same time it gives rise in numerous research studies focused on various aspects of EM field effects on the biological systems [2].

The inevitable EM exposure of the general population in their everyday lives resulted in a necessity to keep the public informed about the real-time level of the EM fields and their distribution in the areas that are related with human activities. The necessity encourages development and utilization of some modern technologies, such as wireless sensor networks (WSN), for sophisticated EM field monitoring [3]-[4]. Such systems are to be used to get the real-time information about the current in-situ EM field strength and in addition for the exposure assessment of population in the covered area.

As a support for the Ministry of the Environment, Mining and Spatial Planning of the Republic of Serbia and the municipal Agency for non-ionizing radiation protection [5]-[6], our research team is requested to develop the EM field monitoring network – SEMONT [7]-[9]. This system employs the existing WSN technology for the area, broadband, remote, automated and permanent monitoring of the EM field level. SEMONT performs measurements of the instantaneous and the overall level in the range of non-ionizing EM radiation. The feature of this system is that results of the measurements will be publically available in a real time over dedicated Internet portal [10].

The proposed SEMONT system has been recognized by the Government of the Republic of Serbia and Ministry of Education and Science of the Republic of Serbia [11], which has approved its development within the program of technological development of the Republic of Serbia, for period of 2011–2014.

In this paper, the basic description of the partially developed SEMONT system is given in Section II, while focus of this paper is concept and several technical details about design and realization of the Internet portal, presented in Section III. The Section IV explains directions of the further development of the SEMONT Internet portal and Section V brings conclusion of this work in progress.

II. BASIC IDEA OF SEMONT SYSTEM

SEMONT is established on the well known technology of the WSN and represents implementation of the existing technology for new application. It is intended for the area supervision, introducing a new approach of the continual EM field monitoring.

SEMONT is designed as a fully automated network, offering the real-time monitoring. The utilization concept of this system is shown in Fig. 1.

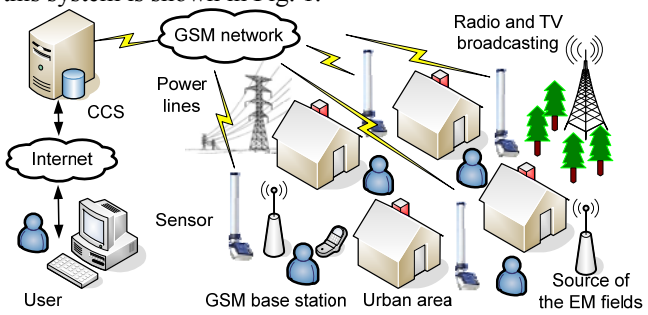


Figure 1. SEMONT utilization over urban area.

 ISBN: 978-1-61208-211-0

SEMONT system implements basic star network topology of the WSN, with all benefits and weakness of such approach, especially in case of the EM field monitoring [12].

The system is designed to consist of the following parts:

- number of autonomous and independent monitoring sensors [13]-[16], spatially distributed over the supervised area, having the task of monitoring of the EM fields from the all active sources around and in designated frequency range,
- centralized control station (CCS) with Internet portal which coordinates activities of the remote sensors, collects data, processes and stores them in centralized database,
- communication network, which provides interaction between the remote sensors and the CCS, and
- management software that supports functionality of SEMONT information network.

SEMONT is planed to implement commercially available sensors for the area EM field monitoring [13]-[16]. Those sensors have been developed in recent years and offer the long-term autonomy of the monitoring process [13]-[15].

The sensor nodes are equipped with solar panel and internal rechargeable battery, providing autonomous and continual monitoring for nearly 169 days [13]-[16], without to require the intervention of the technical personal.

Such sensors are intended to be spatially distributed over the supervised area and have to be installed on remote location without wiring to the CCS. In order to satisfy such demands the remote sensor nodes communicate with the CSS, using the Global System for Mobile Communications (GSM) standard. Both the CCS and sensor nodes are equipped with a quad-band GSM/GPRS modems for remote control and for uploading/downloading the data [17]-[18].

Moreover, the sensors are equipped with certain amount of the internal memory, storing the results of the performed measurements. Data are kept in sensor memory until the programmable time for the data download.

The sensor nodes are isolated units that are deliberately left to perform the self-alone monitoring without intention to perturb the current distribution of the EM field. Their main and only purpose is monitoring, considering that their presence must have the smallest possible influence on the original spatial distribution of the field. Thus, SEMONT system is designed so that remote sensors communicate only with CSS, without mutual communication. In addition, it is planned that once a day the data will be downloaded from sensors and stored in centralized database of the CCS. With such approach the energy of the sensors are more preserved.

Several technical details about sensors have been already presented in some previous work [13]-[18]. Unfortunately, it is not possible to repeat all of them, since the focus of this paper are on some other part of SEMONT system, the Internet portal [10].

Main idea behind SEMONT system is to employ the isotropic broadband measurements in combination with permanent daily monitoring of the EM field. Such a method provides information about the overall field level at any instant of time, without considering which of the sources are present in the observed area. Besides, the broadband measurements approach can, also, be much more convenient when it is necessary to inform the general population.

Moreover, the systems with continual monitoring provide history of the EM field changes, thus after some time we can have a so called register of the EM field, giving an overview of the daily fluctuations of the field level, as shown in Fig. 2.

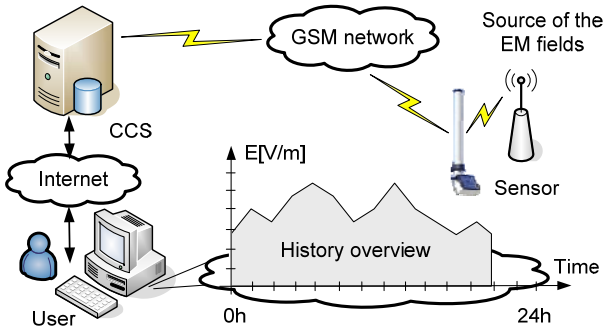


Figure 2. The long-term monitoring and history overview.

Due to the broadband measurements, where contributions of the all active EM field sources are included, SEMONT system is designed to offer a history overview of the cumulative EM field level, during the entire day [7]-[9].

Moreover, SEMONT system compares the measurement results with the Serbian prescribed limits [19]-[21] and recommendations of International commission on non-ionizing radiation protection (ICNIRP) [22].

SEMONT system has been partially developed, with full functionality only of the Internet portal [10]. At the moment, development is work in progress, where communication part of the system and implementation of ten sensors are the priority. When they finished, those tasks will result with more technical analyses and performance studies of the system.

Unfortunately, at this moment, SEMONT system can not present the real measurement results, but we expect that very soon the system will be operative.

The present development will face several challenges that are intended to be in focus of some other presentation. This paper mainly presents some details about Internet portal realization.

III. INTERNET PORTAL OF SEMONT SYSTEM

In order to transparently inform the general public about the real-time EM field level and the EM pollution of the environment, our research team developed dedicated Internet portal of SEMONT system [10].

The Internet portal is a part of the CCS of SEMONT and mainly it is intended to present the measurement results obtained from the sensor nodes, as well as related information about SEMONT system and its purpose.

The Internet web portal is publically available and it is designed to present the results of the measurements for each sensor nodes separately. The location of each sensor nodes is displayed on the electronic map of the supervised territory, while the measurements results are presented over graphs, as shown in Fig. 3.

 ISBN: 978-1-61208-211-0

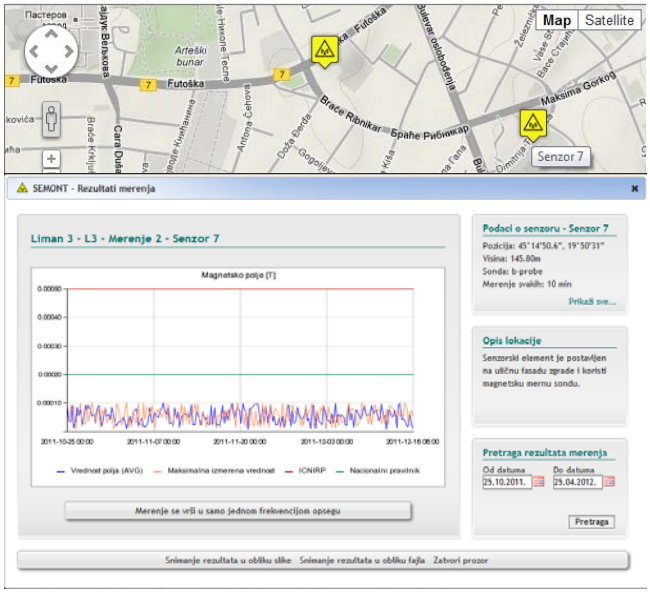


Figure 3. Example of the measurements presentation.

The electronic map will help users to analyze the cumulative level of the EM field, particularly the data from the sensor node that is closest to their location.

The sensors are able to perform measurements every six minutes, permanently and 24 hours per day. Thus, the monitoring can be considered as a continual and in combination with the history overview can offer a clear picture about the EM field fluctuation on particular location.

Comparing with the classical measurements that are performed in one moment, SEMONT system and its Internet portal possess superiority and offer significantly more information about surrounding EM fields.

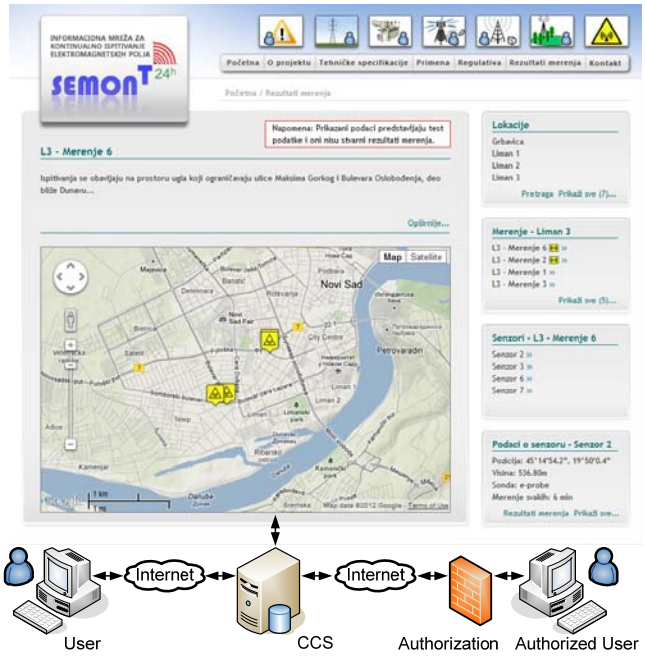


Figure 4. Access to the CCS and Internet portal.

The Internet portal consists of two separated parts: public part – available for public access and protected part – which is restricted area available only for authorized personnel, as shown in Fig. 4.

The public access is allowed only for the front-end of the portal, while for the authorized users the access is in addition granted for the back-end part, besides to the CSS.

The back-side of the portal is responsible for information upload/download and for maintenance of the CSS and Internet portal.

A. The front-end and presentation of SEMONT system

The front-end of the Internet portal presents some of the key facts about SEMONT, in addition to the results of the measurements. Portal is hierarchically organized, presenting information as shown in Fig. 5.

Figure 5. Front-end of the Internet portal.

The interested users can find basic information about SEMONT features, its technical specification, several examples of the application, some for low frequency and some for high frequency EM field monitoring, and finally, the measurement results.

Furthermore, SEMONT system is designed for monitoring according to the Serbian legislation framework [19]-[21] and recommendations of the ICNIRP [22] and EU standards [23]. That information is also present on Internet portal and can be valuable, especially for accredited laboratory that deals with the EM investigation.

B. Measurement results organization and presentation

The measurements data obtained from sensor nodes will be on automated way remotely collected and stored in a centralized database of the CSS. The Internet portal is designed to present those results respecting the hierarchy of the data, as shown in Fig. 6.

 ISBN: 978-1-61208-211-0

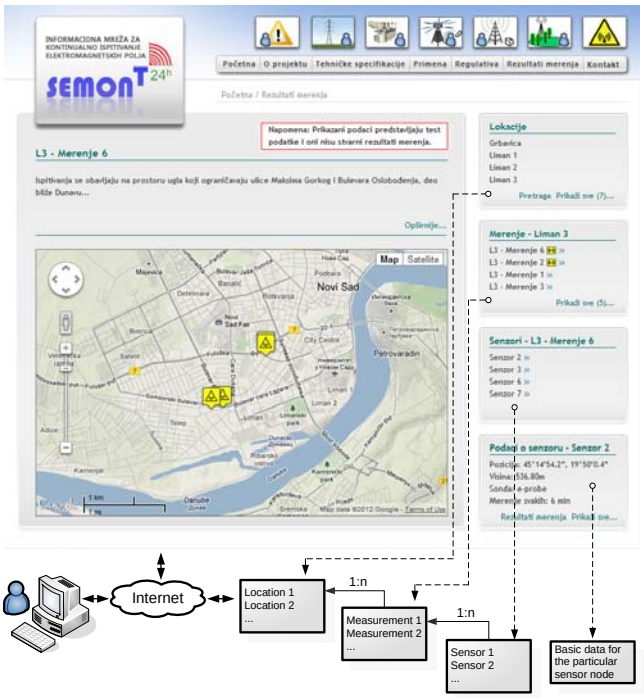


Figure 6. Hierarchy of the measurement results.

The monitoring process is intended for particular location or area and it is possible that several independent measurement campaigns can be performed during some period, using different sensor nodes.

The Internet portal is planed to show for each location which measurements are to be performed and which sensor nodes are to be used for the specific measurement. As a result, relationship between Locations, Measurements and Sensors are of the "1:n" type, which means that Location as a parent, can have several different Measurements, as children. Moreover, particular Measurement can have several associated Sensors and for each node several details are shown, as GPS coordinates, height on which sensor is installed, used field probe [13]-[16], etc.

Internet portal is designed with several search functionality allowing full history overview for a long-time period, as shown in Fig. 3. The search is available through the Locations and Measurements, over selected time period and active/inactive measurement.

C. *Employed technology for realization of the portal*

The foundation of the Internet portal is the CCS centralized database, relaying on the MySQL server, which starts to be the standard in the open source programming.

The most of the Internet portal is programmed using PHP programming language, and its special CakePHP application development framework. In addition, the Web Content Management System (WCMS) is implemented for the back-end side of the portal, providing website authoring, collaboration, and administration tools.

The web form of the portal that presents measurement results also implements the Google maps technology. It can be expected that this page will be the most visited and in order to perform the smooth change of page content, the jQuery and AJAX web development techniques are employed.

The AJAX enables that web applications can send data to and retrieve data from a server asynchronously (in the background) without interfering with the display and behavior of the existing page.

Finally, the measurement results are displayed using the charts realized with open source JpGraph library for PHP.

D. *Directions of the further Internet portal development*

The shortly presented Internet portal represents the work in progress. At this phase the most planed features are realized, but there are some that will be accomplished in the next phase. At the moment, Internet portal is able to present only results of the measurements of the existing and cumulative level of the EM filed. In next phase the portal functionality will be expanded so that it can perform the global exposure assessment, related to the increased risk of possible harmful effects of the EM radiation, according to the EN 50492:2008 standard [24].

The idea is to exploit the 24 hours a day monitoring and to calculate the daily limits of the global exposure, as shown in Fig. 7.

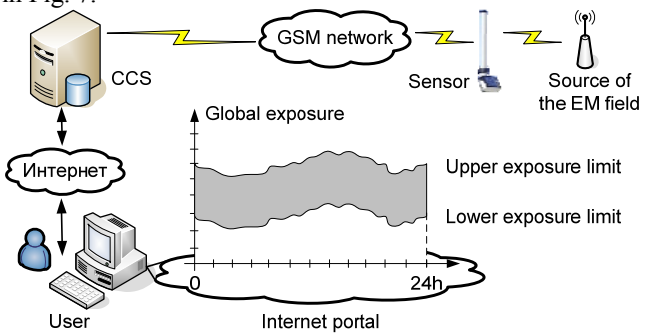


Figure 7. Daily limits of the global exposure.

SEMONT system is based on the broadband measurement approach, resulting with the unknown frequency at which the source emits the EM fields. As a result, the lowest and the highest frequency of the sensor filed probe are considered, resulting with upper and lower exposure limits.

Those daily limits can be quite valuable for the general public, because it can be unknown if some present source is active or not at the moment. Moreover, such method is a new approach that is able to inform the general public about the possible daily ranges of the exposure, something that is not possible with classical approach of the EM field measurement in the moment.

IV. CONCLUSION AND FUTURE WORK

SEMONT system introduces an advanced approach of the wireless sensor networks implemented for a daily supervision of the overall and cumulative level of the various EM field sources, over the area of interest.

The proposed SEMONT monitoring system is a unique idea at the national level and it is the most suitable solution for a constant supervision of the EM field strength, as well as for the global exposure assessment of the general population.

 ISBN: 978-1-61208-211-0

The Internet portal of this system is a significant support for the local authorities in their efforts to take a systematic care of the potential unhealthy effects of the non-ionizing radiation.

Moreover, the Internet portal and SEMONT system are a respectable answer to public concerns about the long-term exposure to the EM fields.

The potential of the proposed SEMONT system has been recognized by the Ministry of Education and Sciences of the Republic of Serbia, endorsing its development.

Currently, SEMONT system has been partially developed, but we expect that very soon this system will be operative and that will be able to offer the real-time results of the measurements. Moreover, the upcoming work will be based, also, on the Internet portal feature enhancement, especially for the global exposure assessment of the general population.

ACKNOWLEDGMENT

This work is supported by the Ministry of Education and Science of the Republic of Serbia, under the grant for project TR 32055.

REFERENCES

[1] International commission on non-ionizing radiation protection (ICNIRP) – "Exposure to high frequency electromagnetic fields, biological effects and health consequences (100 kHz-300 GHz)", http://www.icnirp.de/documents/RFReview.pdf, accessed July, 2012.

[2] EU Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR): Possible effects of Electromagnetic Fields (EMF) on Human Health, http://ec.europa.eu/health/ph_risk/committees/04_scenihr/docs/scenihr_o_007.pdf, accessed July, 2012.

[3] S. Fabbri, F. Frigo, S. Violanti, D. Andreuccetti, and M. Bini, "Electromagnetic Field Monitoring and Control Systems: State-of-the-Art and Work-in-Progress", Radiation Protection Dosimetry, vol. 97, no. 4, pp. 395-400, 2001.

[4] A. Yalofas, A. Gotsis, C. Veranopoulos, P. Constantinou, G. Belesiotis, M. Petkaris, and N. Babalis, "A fully automated and geographically distributed network for the continuous measurement of the RF radiation-"Hermes" project", 6th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Service, TELSIKS 2003, Nis, Serbia, October 1-3, vol. 2, pp. 443-448, 2003.

[5] Ministry of Environment and Spatial Planning of the Republic of Serbia – http://www.ekoplan.gov.rs, accessed July, 2012.

[6] Municipal Agency for the Environmental Protection, City of Novi Sad – http://www.environovisad.org.rs, accessed July, 2012.

[7] N. Djuric, M. Prsa, K. Kasas-Lazetic, "Serbian system for remote monitoring of electromagnetic fields", 4th International Conference on modern Power Systems MPS 2011, Cluj-Napoca, Romania, May 17-20, Acta Electrotehnica, Proceedings of papers, pp. 140-142, 2011.

[8] N. Djuric, M. Prsa, K. Kasas-Lazetic, and V. Bajovic, "Serbian remote monitoring system for electromagnetic environmental pollution", 10th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, TELSIKS 2011, Nis, Serbia, October 5-8, vol. 2, pp. 701-704, 2011.

[9] N. Djuric, M. Prsa, and K. Kasas-Lazetic, "Information network for continuous electromagnetic fields monitoring", International Journal of Emerging Sciences, Special Issue, Selected Best Papers of the PES 2011, December 2011, pp. 516-525, http://ijes.info/1/4/42541401.pdf, 2011, accessed July, 2012.

[10] SEMONT Internet portal – http://semont.ftn.uns.ac.rs, accessed July, 2012.

[11] Ministry of Education and Science of the Republic of Serbia – http://www.mpn.gov.rs, accessed July, 2012.

[12] W. Dargie and C. Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", John Wiley & Sons, 2010.

[13] M. Milutinov, N. Djuric, D. Miskovic, and D. Knezevic, "Area monitor sensor for broadband electromagnetic environmental pollution monitoring", XLVI International Scientific Conference on Information, Communication and Energy Systems and Technologies – ICEST 2011, Nis, Serbia, June 29 - July 1, vol. 1, pp. 217-220, 2011.

[14] M. Milutinov, N. Djuric, and B. Vukobratovic, "Multy-band area monitor sensor in information network for electromagnetic fields monitoring", 10th International Conference on Applied Electromagnetics, PES 2011, Nis, Serbia, September 25-29, pp. 1-4, 2011.

[15] M. Milutinov, N. Djuric, N. Pekaric-Nadj. D. Miskovic, and D. Knezevic,, "Multiband Sensors for Wireless Electromagnetic Field Monitoring System – SEMONT", submitted for the Turkish Journal of Electrical Engineering & Computer Sciences, unpublished, 2012.

[16] Narda Safety Test Solutions GmbH, AMB-8057 User's Manual, Narda, 2007.

[17] B. Vukobratovic, N. Djuric, D. Miskovic, and D. Knezevic, "Sensor communication in wireless electromagnetic field monitoring system", XLVI International Scientific Conference on Information, Communication and Energy Systems and Technologies – ICEST 2011, Nis, Serbia, June 29 - July 1, vol. 1, pp. 221-224, 2011.

[18] Narda Safety Test Solutions GmbH, AMB-8057 User's Guide to the GPRS/FTP communication, 2010.

[19] V. Bajovic, N. Djuric, and D. Herceg, "Serbian laws and regulations as foundation for electromagnetic field monitoring information network", 10th International Conference on Applied Electromagnetics, ПЕС 2011, Nis, Serbia, September 25-29, pp. 1-5, 2011.

[20] "Law on Non-Ionizing Radiation Protection", the law of Republic of Serbia, no. 36/09, 2009.

[21] "Regulation on the limits exposure of non-ionizing ra-diation", the law of the Republic of Serbia, no. 104/09, 2009.

[22] International Commission on Non-Ionizing Radiation Protection (ICNIRP) – http://www.icnirp.de, accessed July, 2012.

[23] D. Markovic and N. Djuric, "An overview of the EN standards for the electromagnetic compatibility", (Pregled EN standarda u domenu elektromagnetske kompatibilnosti), Zbornik radova FTN, Univerziteta u Novom Sadu, year 26, no. 14/2011, 2011, pp. 3500-3503, ISSN: 0350-428X, UDK: 621.37.

[24] EN 50492:2008 – Basic standard for the in-situ measurement of electromagnetic field strength related to human exposure in the vicinity of base stations, 2008.

 ISBN: 978-1-61208-211-0

MPLS-TP OAM Toolset: Interworking and Interoperability Issues

Mounir Azizi, Redouane Benaini, and Mouad Ben Mamoun
Data Mining & Network Laboratory, Department of Computer Science
Faculty of Science Mohammed V-Agdal University
Rabat, Morocco
E-mail: mounir.azizi@gmail.com, benaini@fsr.ac.ma, ben_mamoun@fsr.ac.ma

***Abstract*—The present article is aiming at presenting different Operations, Administration and Maintenance (OAM) procedures that are used for Multiprotocol Label Switching (MPLS) Transport Profile (MPLS-TP). We start by giving a quick review of what is MPLS-TP, and what makes it the solution for the Next Generation Network (NGN). This paper exposes the problem of having two standards on the MPLS-TP OAM Toolset. We highlight the difference between the two approaches and why they are not interoperable. We propose, as future work, to use a layered model solution in order to by-pass this issue.**

Keywords-mpls-tp; OAM; Y.1731; 802.ag; 802.ah; G.8113.1; G.8113.2

I. INTRODUCTION

While Time Division Multiplexing (TDM)-based technologies [1] ex. Synchronous Optical Network (SONET), and Synchronous Digital Hierarchy (SDH) has been for a long time a major player for transport, it shows weakness in the case of traffic burst such as packetized voice and video. This happens because of the fast growth of the demand for service sophistication and expansion (Triple Play, 3G / Long Term Evolution LTE, Cloud Virtualization). Carriers need to migrate from Time-Division Multiplexing (TDM) to packet in order to meet Packet Transport Network (PTN) requirements and to make efforts to minimize the cost for providing these services.

A Joint Working Team created by ITU-T and IETF is actually developing a new packet transport technology (MPLS-TP) taking benefits from existing MPLS networking infrastructure [2].

MPLS-TP is intended to provide all the advantages of the packet-based transport approach, while delivering at the same time, the reliability, availability, OAM capabilities and manageability features associated with traditional TDM transport networks. It is a subset of IP/MPLS protocol suite with new extensions which allow addressing transport network requirements. These extensions consists of adapting current MPLS to make it more "Transport like" by inheriting OAM , reliability and operational simplicity from SONET/SDH networks.

There are two approaches for MPLS-TP OAM at the standardization organizations and no industry agreement on that. The solutions are based on IETF and ITU-T recommendations. Both of OAM proposed solutions are in-band. The IETF solution is based on the existing MPLS OAM tool [3], while the ITU-T solution is based on Ethernet OAM (Y.1731) [4].

In order to best understand the impact of having two distinct standards for MPLS-TP OAM, we need to know if both of them are meeting requirements and how Carriers should take in consideration during implementation.

This paper starts by presenting fundamentals of MPLS-TP. Then we will give the actual picture of the MPLS-TP OAM toolset status and how it can be an issue. Finally, we propose a solution to overcome the problem.

II. WHAT IS MPLS-TP ?

MPLS-TP is aimed to be based on the same architectural concepts of layered network that are already used in legacy SONET/SDH [5]. IP/MPLS [6] and MPLS-TP [7] are willing to be the main packet technologies deployed in Ethernet Backhaul Access's and Aggregation's Network for the next five years. Figure 1 illustrates how MPLS-TP takes the best of two worlds: OAM performance and maturity of TDM (SONET/SDH), and Control/Data Plane efficiency of IP/MPLS.

MPLS-TP has the following key characteristics:

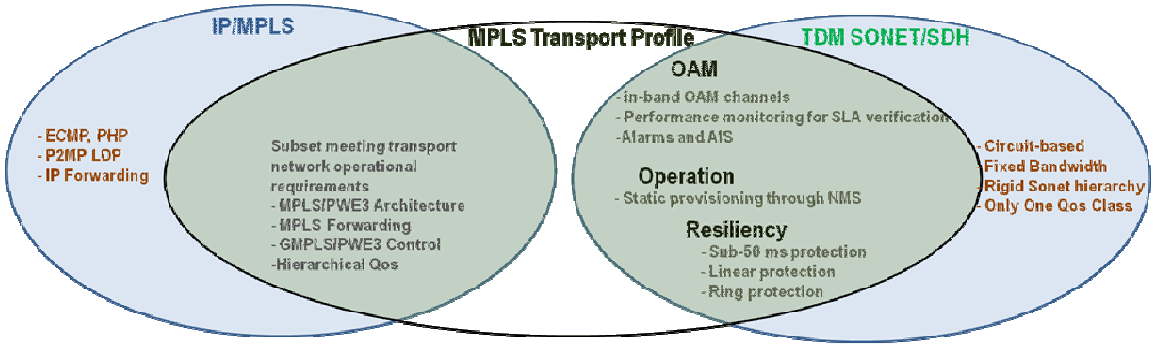


Figure 1. MPLS-TP subset of MPLS[7]

 ISBN: 978-1-61208-211-0

- Connection oriented: Equal cost Multi-Path ECMP and Multi-point to Point (MP2P) are excluded to ensure that, Penultimate Hop Popping PHP is disabled by default;
- L2/L3's client agnosticism;
- Control Plane: static or dynamic Generalized MPLS (GMPLS);
- Physical layer agnostic: allowing MPLS packets to be delivered over a variety of physical infra-structures including Ethernet, SONET/SDH and Optical Transport Network (OTN) using Generic Framing Procedure (GFP), Wavelength-Division Multiplexing (WDM), etc;

- Strong OAM functions similar to those available in legacy optical transport networks (e.g., SONET/SDH, OTN);
- Path protection mechanisms and control plane-based mechanism;
- Use of Generic Associated Channel (G-ACh) to support Fault, Configuration, Accounting, Performance and Security (FCAPS) functions;
- Network provisioning via a centralized Network management system (NMS) and/or a distributed control plane.

Based on the relative standards and recommendations, MPLS-TP is a solution based on existing Pseudo-wire (PW) and Label Switched Path (LSP). MPLS-TP supports two native service adaptation mechanisms via:

- A PW to emulate certain services, for example, Ethernet, Frame Relay, or Point-to-Point Protocol (PPP) / High-Level Data Link Control (HDLC). These adaptation functions are the payload encapsulation; see Figure 2.

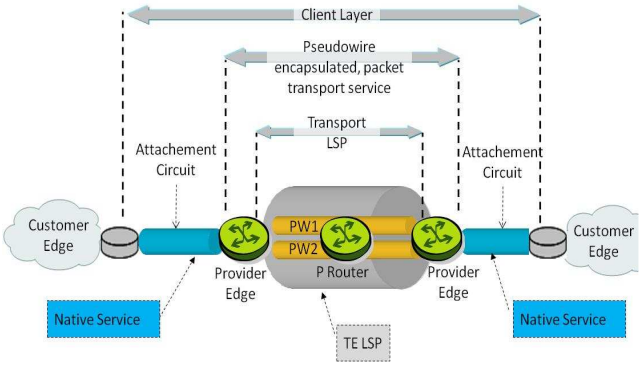


Figure 3. MPLS-TP Architecture (PW as native service)

- An LSP, to provide adaptation for any native service traffic type like IP packets and MPLS-labeled packets (i.e., PW over LSP, or IP over LSP). The adaptation function uses the MPLS encapsulation format; see Figure 3.

The major attributes of MPLS-TP protocol's suite are:

- Data Plane: remains exactly the same as MPLS to facilitate interoperability with MPLS;
- Control Plane: optional, dynamic via IP based protocols or static via management platform NMS;
- OAM: transport-like OAM;
- Protection and Resiliency: SDH-like;

In this paper, we focus on the OAM attribute in order to demystify their role and which will be the impact of having two standards options.

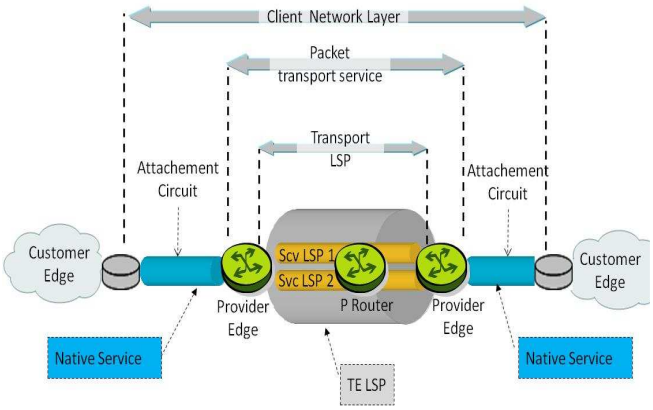


Figure 2. MPLS-TP Architecture (PW as native service)

III. OAM TOOLSET

MPLS-TP has a robust and a transport-like operations and management (OAM) capabilities. Carriers use OAM to provide reliable services with guaranteed service level agreements (SLA), while minimizing troubleshooting time and reducing operational expenses.

The general MPLS-TP OAM requirements are:

- Proactive (continuous) monitoring features, including continuity supervision, connectivity supervision, signal quality supervision (packet loss, frame delay, frame delay variation), alarm suppression, remote quality and continuity indication
- Proactive monitoring applications, including Fault management, Performance/SLA monitoring, Protection switching
- Re-active/on-demand monitoring, including fault localization, signal quality measurement (throughput, ordering and error measurement, transfer delay, delay variation and jitter measurement)
- Communication channels, including protection switching head/tail-end coordination, network management, remote node management, service management [8]:

There is three kind of OAM: Hop-by-hop (e.g., control plane based), Out-of-band OAM (e.g., User Datagram Protocol UDP return path) and In-band OAM (e.g., PW Associated Channel ACh). Within the MPLS, the ACh is known as technique for in-band Virtual Circuit Connectivity Verification (VCCV) applicable only for PW, while LSPs have no mechanism to differentiate user packets from OAM packets [9]. MPLS-TP extended the ACh to the Generic Associated Channel (G-ACh) and introduced a new label G - ACh Alert Label (GAL) to identify packets on the G-Ach. It is an in-band management channel on a PW or LSP that does not rely on routing, user traffic, or dynamic control plane functions. The OAM packets can then share the same path of user traffic, operate on a per-domain basis and/or across multiple domains, and are able to be configured in the

 ISBN: 978-1-61208-211-0

absence of a control plane. This constitutes an important toolbox which allows carriers to run OAM at each network level: LSP, PW and Section [10].

The network model of MPLS-TP OAM consists of:

- Different OAM Level (administrative domains). Each Level can be independently monitored by its own Ethernet Connectivity Fault Management (CFM) frames. The scope of OAM frames is limited to the domain in which the carried information is significant.
- Two plans; see Figure 4:
  - A "vertical plan" (red) that represents the OAM entities across different administrative domains,
  - An "horizontal plan" (blue) that represents the OAM entities within a single administrative domain.

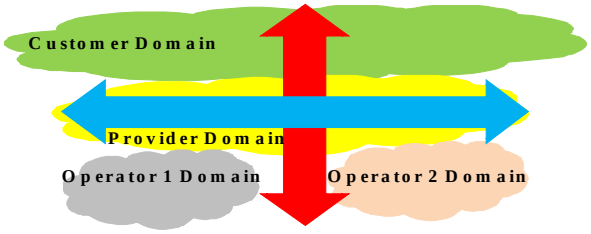


Figure 4. OAM Network Model

The Maintenance Entity Group (MEG) is the portion of the transport path that is being monitored or maintained. MEG endpoints are referred as management end points (MEPs) and intermediated nodes are referred as management intermediate points (MIPs). OAM message can be exchanged between MEPs, or from one MEP to other MIP. MEP handle OAM packet when it arrives at Label Edge Router (LER) because the label is popped and then the GAL is exposed which allow MEP to start processing by the corresponding OAM function. MIP can handle OAM packet using Time To Leave (TTL) mechanism. The TTL expiration causes the packet to be processed, and the existence of the GAL under the label for which the TTL expired causes the packet to be processed. MIPs cannot initiate OAM message, but may send an answer.

There are two proposed standards for MPLS-TP OAM and no industry agreement on that. They are based on IETF (G.8113.2) and ITU-T (G.8113.1) recommendations [11].

A. ITU-T OAM Tools G.8113.1

ITU-T suggests reuse the same OAM Protocol Data Units (PDUs) and procedures defined in Ethernet OAM ITU-T Y.1731 [12]. The presence of Y.1731 OAM PDU is identified by a single ACH channel Type (0xXXXX). Within the OAM PDU, the OpCode field allows identifying the type of OAM frame.

The ITU-T OAMs provide a set of mechanisms that meets the MPLS-TP OAM requirements. The methods and procedure supported are listed in Table. 1:

TABLE I. G.8113.1 OAM FUNCTIONS [13]

Application	OAM Function (IETF draft-bhh-mpls-tp-oam-y1731)	
Fault Management (FM)	Pro-active	Continuity check and Connectivity Verification (CC/CV)
		Remote Defect Indication (RDI)
		Alarm Indication signal (AIS)
		Client signal Fail (CSF)
	On-demand	Connectivity Verification (CV)
		Diagnostic test (DT)
		Locked Signal (LCK)
Performance Management (PM)	Pro-active	Loss Measurement (LM)
		Delay Measurement (DM)
	On-Demand	Loss Measurement (LM)
		Delay Measurement (DM)
Other Applications	Automatic Protection Switching (APS)	
	Management communication channel/ Signaling communication channel (MCC/SCC)	
	Vendor-specific (VS)	
	Experimental (EXP)	

This OAM toolset claims to be mature and widely deployed. It is still under consensus of standardization. However G.8113.1 requires a G-Ach codepoint to be assigned by IANA (IETF).

B. IETF OAM Tools G.8113.2

The IETF solution is based on the existing MPLS OAM toolset and provides the following functions: CC for proactive monitoring, CV for End-point verification, PM, FM and Diagnostics. This solution needs specifics extensions of Bidirectional Forwarding Detection (BFD) and LSP Ping and needs also to introduce new mechanisms for the function that are not available in MPLS such as loss and delay measurement. BFD and LSP should be able to run without IP (IP less). The methods and procedure supported are listed in Table. 2:

TABLE II. IETF MPLS-TP OAM FUNCTIONS/RFCS

	OAM Functions	RFC/draft
Pro-active FM OAM	MPLS-TP Identifiers	RFC6370 09/2011
	RDI – use BFD extension	RFC6428 11/2011
	AIS	RFC6427 11/2011
	Link Down Indication (LDI)	
	Lock Report (LKR)	
	Config MPLS-TP OAM using LSP Ping	draft-absw-mpls-lsp-ping-mpls-tp-oam-conf-04 April 13, 2012
On-Demand FM OAM	CV – use LSP Ping and BFD Extensions	RFC6426 11/2011
	Loopback Message/Replay (LBM/LBR)	RFC6435 11/2011
	Lock Instruct (LI)	
Proactive PM OAM Functions	Packet Loss Measurement (LM)	RFC6374 09/2011 RFC6375 09/2011
	Packet Delay Measurement (DM)	

 ISBN: 978-1-61208-211-0

	OAM Functions	RFC/draft
and On demand PM OAM	Throughput measurement (use LM)	
	Delay variation measurement (use DM)	

IETF has overcome to luck of MPLS OAM by extending BFD and LSP Ping, and also by creating new tools in order to satisfy Transport-like OAM expectations.

Since both of solutions are meeting MPLS-TP OAM requirements, the selection criteria depend on each scenario:

- Different operators have different network scenarios
- Different vendors have different implementations.

G.8113.1 is supported by Alcatel-Lucent and Huawei Technologies Co. Ltd. and by carriers China Mobile Communications Corp. and Telecom Italia SpA. The G.8113.2 camp, meanwhile, counts Cisco Systems Inc. and Ericsson AB among its supporters.

IV. INTEROPERABILITY OR INTERWORKING : ISSUES

ITU-T continues to standardize its Y.1731 based OAM solution, and is currently using an "experimental" MPLS OAM. IETF, on their side, published about many RFCs last year in order to complete their MPLS based OAM solution. Both of proposed standards claim to satisfy MPLS-TP OAM requirements. The biggest difference is the PDU format and how to identify an OAM function which makes interoperability impossible. When both solutions are present in the same network, or when interconnecting two different networks using different OAM solution, delivering end-to-end OAM become an issue.

The first option to resolve this issue is by implementing Interworking Function (IWF) at edge router to secure the mapping of different OAM message. This is also the most expensive option, since vendors have to develop IWF on their equipments.

The second one is to choose a network model in such a way to use the layered characteristics of MPLS-TP OAM: Section OAM (Link OAM), PW OAM, and LSP OAM. We suggest here, when possible, to run MPLS-TP OAM independently within each segment; see Figure 5. Maintenance Entity (ME) that exchange OAM inside the same Maintenance Domain has to use same OAM toolset. So "Operator Network 1" and "Operator Network 2" can run different OAM Toolset. Layered architecture can be based on peer or overlay model, or a mixture (hybrid).

We need to study the layered architecture to figure out how it is resolving MPLS-TP OAM interoperability issues with respect to standard requirements. An OAM discovery mechanism can be a solution where each MEP inside a maintenance domain will discover other MEPs and then exchange their capabilities.

V. CONCLUSION

It is sufficient to have only one OAM solution for MPLS-TP, however there is two standard or pre-standard toolset and both of them are supported by industry. Consequently, equipment and network deployments will be more complex and interoperability issues are becoming reality. Introduction of new interworking functions can present a solution but are cost effective and software/hardware update will be more complex. We propose to use layering model which can avoid developing IWF in a lot of cases. We suggest creating new capabilities on border Node (at layer level) which allow dynamic exchange of OAM information: Type of toolset, MEs, MEPs, MIPs, etc. the associated Channel ACh would be a good starting point of this vision.

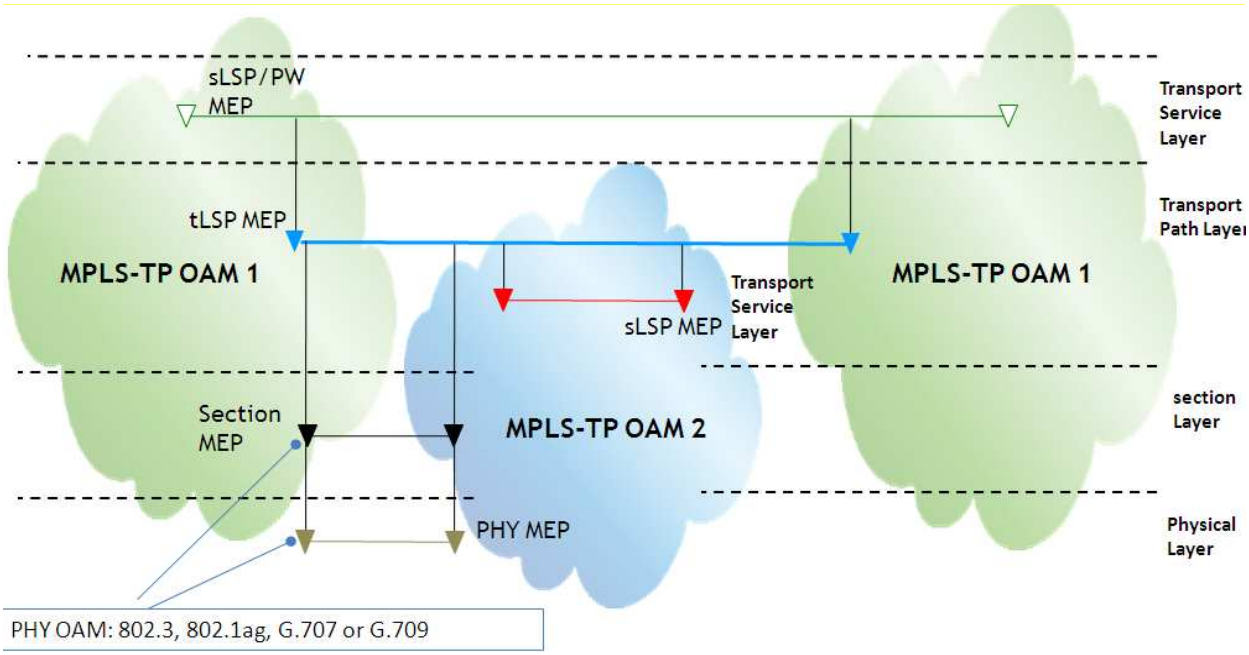


Figure 5. Layered OAM Model

 ISBN: 978-1-61208-211-0

REFERENCES

[1] ITU-T Recommendation G.704 (10/98) - Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 Kbit/s hierarchical levels.

[2] S. Bryant, and L. Andersson, "Joint Working Team (JWT) Report on MPLS Architectural Considerations for a Transport Profile", IETF RFC 5317, February 2009.

[3] K.Kompella, G.Swallow,"Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures", RFC 4379, February 2006.

[4] ITU-T Recommendation Y.1731, ”OAM functions and mechanisms for Ethernet based networks”, May 2006.

[5] D. Cavendish, K. Murakami, S. Yun, O Matsuda and M. Nishihara,”New transport services for Next-Generation SONET/SDH systems,”IEEE Commun. Mag., vol.40, no.5, pp.80-87, May 2002.

[6] E. Rosen et al, “Multiprotocol Label Switching Architecture”, RFC 3031, January 2001.

[7] M. Bocci, S. Bryant, D. Frost, L. Levrau, and L. Berger, "A Framework for MPLS in Transport Networks", IETF RFC 5921, July 2010.

[8] M. Vigoureux, D. Ward, and M. Betts, "Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks", IETF RFC 5860, May 2010.

[9] S. Bryant, G. Swallow, L. Martini, and D. McPherson, " Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN", IETF RFC 4385, February 2006.

[10] M. Bocci, M. Vigoureux, and S. Bryant, "MPLS Generic Associated Channel", IETF RFC 5586, June 2009.

[11] I.Busi, H. van Helvoort, and J. He, "MPLS-TP OAM based on Y.1731", IETF draft-bhh-mpls-tp-oam-y1731-08, Junuary 2012

[12] ITU-T Recommendation Y.1731 (02/08), "OAM functions and mechanisms for Ethernet based networks", February 2008

[13] ITU-T Recommendation G.8113.1 (05/11), "Operations, Administration and Maintenance mechanism for MPLS-TP in Packet Transport Network (PTN)", May 2011

 ISBN: 978-1-61208-211-0

Characterization and Modeling of M2M Video Surveillance Traffic

Ivo Petiz, Paulo Salvador, António Nogueira
DETI, University of Aveiro/Instituto de Telecomunicações
Campus de Santiago, 3810-193 Aveiro, Portugal
e-mail: {petiz,salvador,nogueira}@ua.pt

***Abstract*—The relevance of machine-to-machine (M2M) communications is growing significantly, largely driven by wireless networks. Internet of Things (IoT) applications will create new demands and challenges that will require high bandwidth, real-time communications or reliability in remote locations. Since M2M applications will generate traffic and transactions that compete for bandwidth and priority, network operators must be concerned of how to handle the enormous increases in their signaling traffic and, in particular, in finding new ways to meet each M2M application's requirements and service level agreements, while protecting the network and making a more efficient use of the available resources. An efficient design and control of the future Internet needs to take into account the main characteristics of the supported traffic and, therefore, accurate and detailed measurements of M2M traffic have to be carried out in order to perform a complete characterization and develop stochastic models that are able to capture the most important statistical properties of the network traffic. This paper considers a particular case of a M2M service, a video surveillance application, and proposes a general methodology that performs a detailed statistical characterization of its traffic, while addressing the main challenges that are involved in the development of an appropriate stochastic modeling approach. The M2M traffic analysis relies on the use of wavelet scalograms, which describe the signal energy on a timescale/time domain and are constructed based on the wavelet coefficients obtained from the multi-scale decomposition of the traffic process, to identify all the different traffic features. An innovative M2M modeling framework based on a multiple state machine is also proposed: its parameters should be inferred from the salient features of the traffic and it should be able to characterize both the download and upload traffic and quantify the overhead that is necessary to guarantee a secure communication.**

***Keywords* - M2M applications, wavelet transform, scalogram, traffic modeling.**

I. INTRODUCTION

Machine-to-machine (M2M) communications have emerged as a cutting edge technology for next-generation networks, undergoing a rapid development and inspiring numerous applications. Recently, this topic has attracted much attention from the industry and research communities, mainly due to the following factors: the emergence of wireless communication systems became a premise for the advance of M2M communications; (ii) the development of advanced software components that enable devices to operate intelligently and autonomously; (iii) sensors that can be used to collect information for M2M systems are being widely used and increasingly adopted. According to the Machina Research's Report "M2M Global Forecast & Analysis 2010-20" [1], global M2M connections will increase from one billion at the end of 2010 to 12 billion at the end of 2020, accounting for half of all global data connections. Connections will be dominated by two sectors: consumer electronics (including cameras, music players and TVs) and intelligent buildings (e.g. security and surveillance, HVAC systems), which will account for over 60% of the total. Over 70% of the M2M devices will be connected by short-range technologies (mostly WiFi), while of the remainder wireless cellular technologies (mostly applied to utilities and automotive applications) will dominate. At the end of 2010, M2M accounted for 2% of cellular connections and by 2020 they will reach 19%, or 2.3 billion connections.

This traffic growth will have an increasing impact in network management and dimensioning activities [2]. Mobile network providers are starting to offer M2M integrated applications, which will require the dimensioning and joint management of multiple network elements for an optimal operation. These operations will greatly benefit from the development of new mathematical tools that are able to predict network behavior under new M2M traffic scenarios. A rigorous statistical characterization of the M2M traffic is essential: in the past, several studies have shown that IP traffic properties like burstiness, self-similarity and/or long-range dependence had a significant impact on network performance and behavior and should be included in the modeling frameworks; a similar analysis should now be applied to these new applications, whose traffic should be rigorously characterized in order to design accurate and parsimonious modeling approaches.

The wavelet scalogram, which describes the signal energy on a timescale/time domain and is constructed based on the wavelet coefficients obtained from the multi-scale decomposition of the traffic process, will be used as the statistical fingerprint of each traffic trace segment. The wavelet scalogram communicates the time frequency localization property of the discrete wavelet transform, being possible to capture the correlation that exists between the time variability of the process and the different scales. Wavelet analysis allows the degree of localization to be automatically and appropriately adjusted - large window widths are used for analyzing low frequency components, whereas small window widths are used for investigating high frequency components. Thus, this methodology is able to identify different peculiar behaviors

 ISBN: 978-1-61208-211-0

even if this information is somehow hidden when performing a classical statistical analysis of the traffic. In this paper, M2M video surveillance traffic will be used to illustrate/evaluate the suitability of the proposed analysis and modeling framework: a set of traffic measurements was made in order to obtain long duration (one week) traces that allow us to identify the main characteristics and trends of this new communication paradigm and understand which features/properties should be taken into account when designing an accurate modeling framework.

The characteristics of M2M traffic are fundamentally independent from human behavior: in particular, the timings of the information exchange are no longer defined by humans [3], although many services may indirectly reflect human activities in some way (like for example M2M video surveillance and M2M car fleet telemetry services in case of non-authorized movement/entries or car accidents, whose periodicity tend to follow exponentially distributed human patterns). So, M2M traffic can no longer be modeled and predicted by traditional approaches and a new modeling paradigm should be developed. The new modeling framework must be a trade-off between generality and mathematical complexity, must be sufficiently generic to incorporate all possible M2M applications and heterogeneous characteristics, while maintaining a low mathematical complexity and high applicability. Privacy and security will be important features of any M2M service and therefore the ability to characterize the additional traffic overhead, to generate and maintain the communication keys, should also be incorporated in the M2M traffic modeling framework.

The accurate characterization and modeling of M2M traffic can be exploited to enhance different traffic engineering and management tasks. In fact, one way to improve network utilization is to mix in the same set of network resources traffic with contrasting behavior (e.g. traffic sources whose periods of higher utilization are in disjoint time intervals). In general, it is beneficial for network operators to cluster their traffic sources into groups of similar traffic profiles and to apply routing policies that are a function of the clustering solution. So, following a measurement phase, a traffic source can be classified into one of predefined groups and its routing can be adjusted accordingly; this may free some resources, which in turn, will allow additional sources to access the network. This functionality can work in pseudo real time and should be applied in a distributed way, mainly at the network traffic entry points.

The paper is organized as follows. Section II discusses the most relevant related work on M2M traffic statistical characterization and modeling; Section III proposes a new modeling framework for M2M traffic; Section IV presents a brief background on wavelet transforms and scalograms; Section V presents some traffic measurements that were made for a particular case of a M2M service, a video surveillance service, in order to illustrate the applicability/suitability of a statistical analysis methodology that is also proposed to identify the main statistical properties of the traffic; finally, Section VI presents the main conclusions.

II. Related work

IP traffic modeling has been an active research field for a long time. The growing diversity of services and applications for IP networks has been driving a strong requirement to make frequent measurements of packet flows and describe them through appropriate traffic models. Several studies have shown that IP traffic may exhibit properties of self-similarity and/or long-range dependence (LRD) [4], [5], [6], [7], [8], peculiar behaviors that have a significant impact on network performance. The heavy-tailed characteristic of the probability distributions (quite different from the simple Gaussian shape) explained network performances that were quite different from the ones predicted by traditional renewal and Markovian models. Besides, the multifractal nature of network traffic, firstly noticed by Riedi and Lévy Véhel [9], lead to the proposal of random cascades [10], [11] and L-system models [12] to describe the scaling behavior of IP traffic. However, the mathematical tractability of Markovian models lead to the development of several ingenious inference procedures that were able to account for these peculiar behaviors [13], [14], [15], [16], [17], [18], [19], [20]: these traffic models were able to match the complex statistical properties of IP traffic while maintaining an analytical simplicity that allow their use for calculating network performance metrics and predicting future traffic values.

Several reports describing the increase of machine-to-machine services, their relevance and future trends have been recently published [1], [2], [21], [22]. However, we did not find any traffic model specifically designed to describe their statistical characteristics: reference [23] is one of the few publicly available studies on this topic, proposing a theoretical model to calculate some characteristics of WPAN (Wireless Personal Area Networks) traffic, although the model still needs some modifications to account for application specific behaviors. So, it is absolutely necessary to conduct a rigorous statistical analysis of real M2M traffic applications and develop a generic analytical framework that is able to describe their relevant properties and predict future traffic values.

III. M2M Traffic Modeling Framework

The most efficient traditional traffic models usually include multiple space states where the transition dynamics are probabilistic and based on underlying exponentially distributed timings. These dynamics are frequently mapped into Markov chains that modulate the data generation process (deterministic or exponentially distributed). Examples of these processes are the Markov Modulated Deterministic Process (MMPP)[24] and the Markov Modulated Poisson Process (MMPP)[17], which assume that the time spent in each state of the space state is exponentially distributed and information objects are generated in periodic and exponentially distributed intervals, respectively.

An efficient M2M traffic model must jointly incorporate traditional deterministic characteristics of automated mechanisms and random characteristics of Artificial Intelligence, network and human processes. Therefore, we propose a modeling

 ISBN: 978-1-61208-211-0

framework based on a process ruled by a multiple space state with heterogeneous (deterministic and random) dynamics and generic information (e.g. messages, packets or bytes) generation processes. This framework model will be called Heterogeneous Chain Modulated Generic Process (HCMGP).

The HCMGP modeling framework is a multistage space state process able to model the security bi-directional traffic overhead, the M2M bi-directional communication process and admits the definition of multiple possible events that reflect different application profiles. As a result, each state will define the type of generation process (deterministic, exponential or other) and its corresponding parametrization. Moreover, the dynamics of the state transitions are heterogeneous and can be ruled by deterministic or exponential processes that define the time of permanence in each state and the destiny of the next transition.

The modeling framework parametrization will agree with the assumption that state transitions can follow a deterministic or random distribution. State transitions are ruled in parallel by two (or more) parametric matrices that define, respectively, the next transitions after a deterministic amount of time and the probabilistic transitions after a random period of time. The probabilistic/random transitions can follow an exponential distribution (analogous to Markovian models) or any other distribution. The information generation processes associated with each state will also be parametrized by two (or more) vectors defining, respectively, the deterministic values and distribution function parameters for the rates and the amount of generated information.

The chain modulated nature of the HCMGP modeling framework will allow the usage of the traditional mathematical tools (used on Markovian models) to determine the traffic model resulting from the superposition of multiple M2M sources. Existing mathematical tools allow the computation [17] and reduction [25] of the matrix form descriptors of the superposition model.

The M2M model framework is depicted in Figure 1. The underlying space state of the model comprises two base states: standby and active. The standby state models the terminal conditional upon boot, and may include specific bi-directional start-up transmissions (e.g. configuration, localization or logging messages). The active state models the non-event related operation of the terminal (e.g. localization, logging or periodic metering). The remaining states will model event driven actions of the terminal (e.g. failure report, security event report, non-scheduled metering/logging, upgrades or (re)configuration actions). Two (optional) extra states were included to model the security channel establishment and maintenance (key establishment and renegotiation). The security keys establishment actions are perform upon boot (between the standby and active states) and keys (re)negotiation actions are treated as any other event and can be periodically or protocol based deployed.

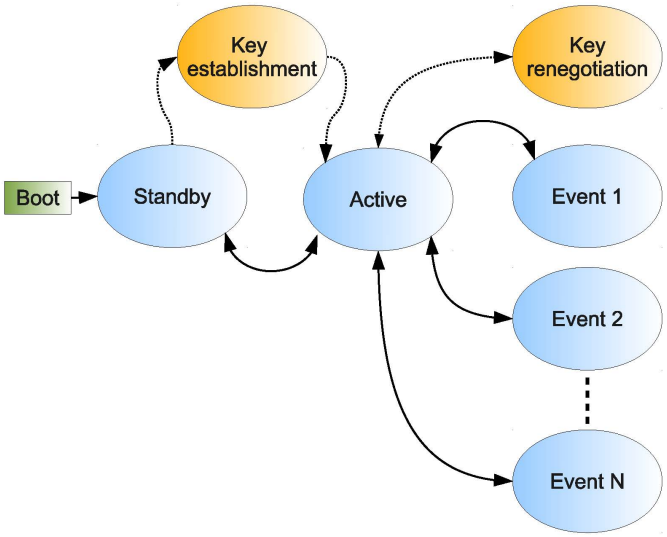


Figure 1: M2M traffic model framework

IV. Background on wavelet scalograms

The inability of conventional Fourier analysis to preserve the time dependence and describe the evolutionary spectral characteristics of non-stationary processes requires tools that allow time and frequency localization. Wavelet transforms can provide information concerning both time and frequency, which allows local, transient or intermittent components to be elucidated. Such components are often obscured due to the averaging inherent within spectral only methods, like Fast Fourier Transform (FFT) for example.

Wavelets are mathematical functions that are used to divide a given signal into its different frequency components. They consist of a short duration wave that has limited energy. Wavelets enable the analysis of each one of the signal components in an appropriate scale. Starting with a mother wavelet $\psi(t)$, a family $\psi_{\tau,s}(t)$ of "wavelet daughters" can be obtained by simply scaling and translating $\psi(t)$:

$$\psi_{\tau,s}(t) = \frac{1}{\sqrt{|s|}}\psi(\frac{t-\tau}{s}) \quad (1)$$

where s is a scaling or dilation factor that controls the width of the wavelet (the factor $\frac{1}{\sqrt{|s|}}$ being introduced to guarantee preservation of the energy, $\|\psi_{\tau,s}\| = |\psi|$) and τ is a translation parameter controlling the location of the wavelet. Scaling a wavelet simply means stretching it (if $|s| > 1$) or compressing it (if $|s| < 1$), while translating it simply means shifting its position in time.

Given a time-series $x(t) \in L^2(\Re)$ (the set of square integrable functions), its Continuous Wavelet Transform (CWT) with respect to the wavelet ψ is a function of two variables, $W_{x;\psi}(\tau, s)$, obtained by projecting $x(t)$ onto the family $\{\psi_{\tau,s}\}$ [26]:

$$W_{x;\psi}(\tau, s) =< x, \psi_{\tau,s} >= \int_{+\infty}^{-\infty} x(t)\frac{1}{\sqrt{|s|}}\psi^*(\frac{t-\tau}{s})dt \quad (2)$$

In analogy with the terminology used in the Fourier case, the (local) Wavelet Power Spectrum (sometimes called Scalogram

 ISBN: 978-1-61208-211-0

or Wavelet Periodogram) is defined in terms of normalized energy ($\hat{E}_x(\tau, s)$), for all possible translations (sub-set **S**) and a predefined sub-set of time scales (sub-set **S**), as

$$\hat{E}_x(\tau, s) = 100 \frac{|W_x(\tau, s)|^2}{\sum_{\tau' \in \mathbf{T}} \sum_{s' \in \mathbf{S}} |W_x(\tau', s')|^2} \quad (3)$$

The existence of a peak in the scalogram of a time series at a high (low) level indicates that a high (low) frequency component is present in the time series. The volume bounded by the surface of the scalogram is the mean square value of the signal.

Scalograms reveal much information about the nature of non-stationary processes that was previously hidden, so they are applied to a lot of different scientific areas: diagnosis of special events in structural behavior during earthquake excitation, ground motion analysis, transient building response to wind storms, analysis of bridge response due to vortex shedding, among others [27].

V. USE CASE - A VIDEO SURVEILLANCE SERVICE

M2M video surveillance services in public areas, buildings and transportation facilities will be very common in a near future. M2M devices will provide security by means of standard movement alarms or video surveillance cameras. Some applications transmit video continuously, while others only transmit video upon movement detection (triggered by external alarms or image analysis).

When we try to apply the general M2M modeling framework to the video surveillance service, different profiles can be identified, differing only in the amount and rate of information generated when in the active state. In this state, the M2M terminal will periodically transmit video and alarm data with a deterministic rate and size. A generic system can be modeled by a framework with two event states, one that models the alarm reporting and other that models the start/rate change of video streaming upon movement detection. Both event states, which depend on human actions, will occur according to exponential distributions, while their duration will also be exponentially distributed. However, the information generation rate will be deterministic (constant report size and average video rate).

A. Measurement setup

In order to fully characterize the traffic generated by this M2M service, we made an intensive set of traffic measurements at our networks laboratory. The experimental measurement setup is depicted in Figure 2, where two computers, a webcam and a layer 2 switch were used. Computer 1, which is responsible for creating the data stream, is a micro ITX system with an Intel Dual Core N330 processor with 1.6 GHz, a 2 GB DDR 2 memory and 120 GB of disk capacity. A generic USB 2.0 webcam, with a 640x480 pixel resolution, is attached to computer 1. Computer 2 is a common workstation built with an Intel Core 2 Duo, model E 8500, operating at 3.16 GHz, 4 GB of DDR 2 RAM and 320 GB of disk capacity. Both machines operate using a Linux Ubuntu distribution, version

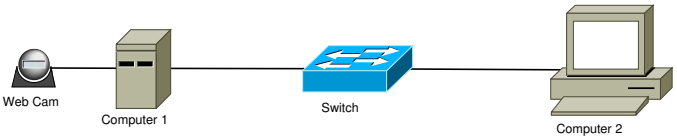


Figure 2: Video surveillance traffic measurement setup.

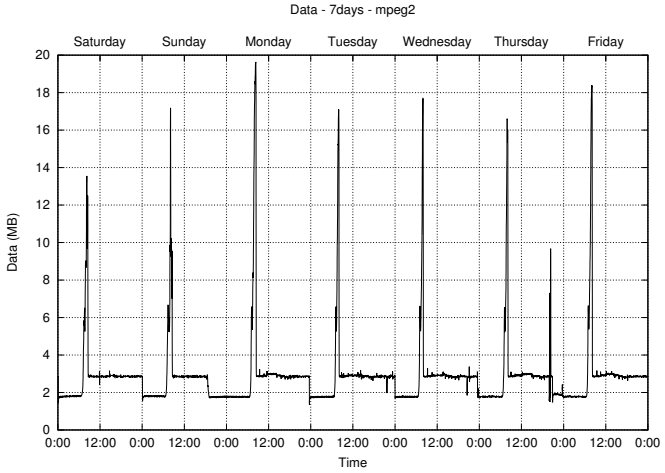


Figure 3: Amount of data over a week period.

10.10, updated and configured by default. The layer 2 switch is a common 10/100Mbps Ethernet switch.

The 'gst-launch' software was used to compose a continuous MPEG2 video stream, running over UDP, with a resolution of 640x480 pixel and 30 frames per second.

B. Traffic characterization

Figures 3 and 4 represent the number of bytes and packets, respectively, received by Computer 2 during a whole week period. As can be seen, there is a clear periodic trend in these plots, corresponding to the repetitive daily activities of the laboratory users. The first peak of these plots corresponds to Saturday, and we can see that the activity levels on Saturday and Sunday are slightly different from the levels of the remaining week days. On weekend days the movement activity is very small, so the variability of the curves is also smaller: on Saturday the laboratory is open, although with a small number of users; on Sunday, it is closed, explaining the drop of the curves in the late afternoon. In fact, on Sunday the activity level corresponds exclusively to sunlight variations (artificial lights are obviously turned off). On working days, the activity level presents some degree of variability (due to the presence of several users in the lab premises) and drops abruptly at 12:00 PM because the lab closes at this instant and lights are turned off. Finally, note that, for all days, there is a marked peak in the early morning, corresponding to the sunlight appearance.

A scalogram analysis was applied to the measured data-streams, inferring the normalized energy ($\hat{E}_x(\tau, s)$) in all time slots τ and for time-scales 1 to 64 ($s \in \mathbf{S}, \mathbf{S} = \{1, \ldots, 64\}$). The top plots of Figures 5 and 6 represent, respectively, the

 ISBN: 978-1-61208-211-0

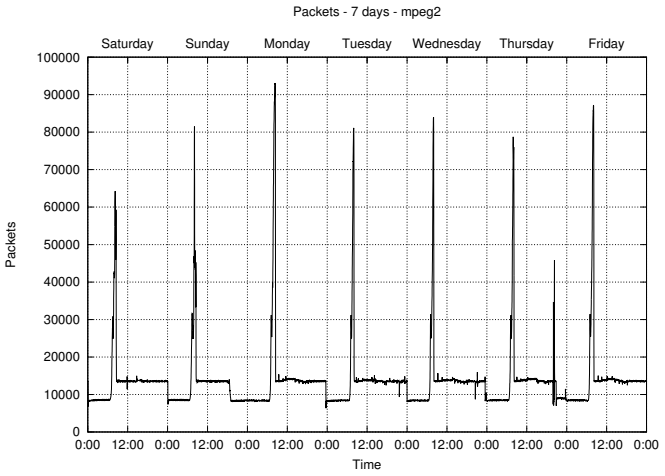


Figure 4: Number of packets over a week period.

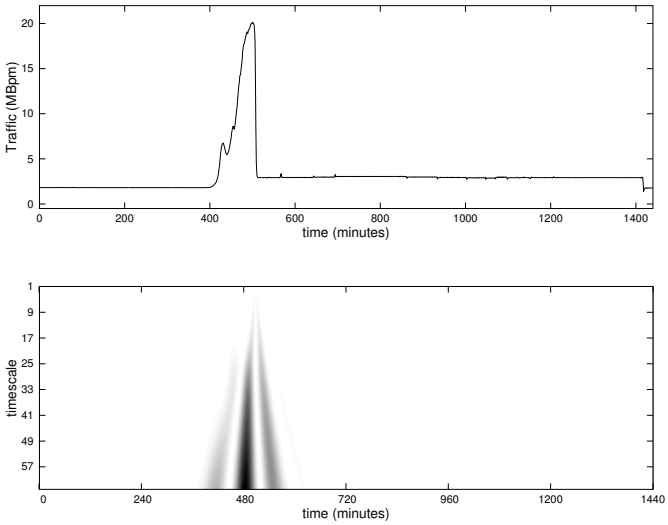


Figure 5: Traffic amount per minute (Top) and scalogram (Bottom) corresponding to a single day.

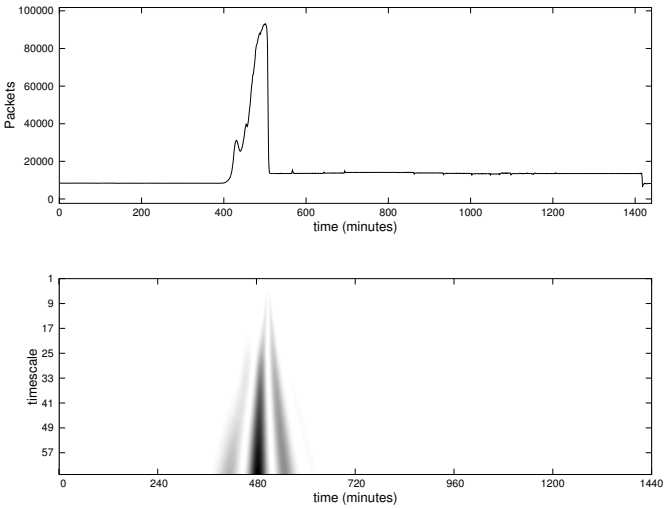


Figure 6: Number of packets per minute (Top) and scalogram (Bottom) corresponding to a single day.

traffic amount and the number of packets per minute corresponding to a single day (since their patterns are repetitive), while the bottom plots illustrate the corresponding scalograms, in terms of normalized energy over time and timescale (darker means more energy). The scalograms allow us to identify and quantify the most relevant traffic variations, knowing exactly the time instants and resolutions where they are more noticeable. If a more detailed analysis of any segment of the data trace is necessary, it is possible to calculate a new scalogram that is confined to a small portion of the signal. As an illustrative example, the top plots of Figures 7 and 8 represent the traffic amount and the number of packets per minute corresponding to a generic dawn period, respectively, while the bottom plots illustrate their corresponding scalograms. This type of detail can be used to identify important frequencies that are characteristic of some particular behaviors of a M2M service. This analysis step will have obvious consequences in the modeling phase of the M2M service: the knowledge of the different energy components and of the timescales where they are visible is an important input to the modeling effort, allowing the identification of the different model states and contributing to the inference of the various model parameters.

VI. Conclusions

This paper discussed the new paradigm that M2M traffic carries for network operators. In face of several new challenges that are imposed by M2M services, namely the periodicity of the traffic profiles and the partial/total absence of human influence, a new modeling framework able to conform with the major current and future M2M applications was presented. This approach is based on a multiple state machine and can be a valuable tool for dimensioning, optimizing and maintaining M2M services over future networks. In order to perform a complete characterization of the M2M traffic, this paper considered a particular case of a M2M service, a video surveillance application, and proposed a general methodology that is able to perform a detailed statistical characterization of the generated traffic: the traffic analysis framework relies on the use of wavelet scalograms, which describe the signal energy on a timescale/time domain and are constructed based on the wavelet coefficients obtained from the multi-scale decomposition of the traffic process.

References

[1] M. Research, “M2M global forecast & analysis 2010-20 report,” http://www.machinaresearch.com/m2mglobal2020.html.

[2] C. Wallace. (2012, March) The rise of M2M - how will the network adapt? [Online]. Available: http://kn.theiet.org/magazine/rateit/communications/internet-of-things.cfm

[3] S. Lucero, “Maximizing mobile operator opportunities in M2M, ABIresearch/Cisco,” 2012. [Online]. Available: http://www.cisco.com/go/mobile

[4] W. Leland, M. Taqqu, W. Willinger, and D. Wilson, “On the self-similar nature of Ethernet traffic (extended version),” *IEEE/ACM Transactions on Networking*, vol. 2, no. 1, pp. 1–15, Feb. 1994.

 ISBN: 978-1-61208-211-0

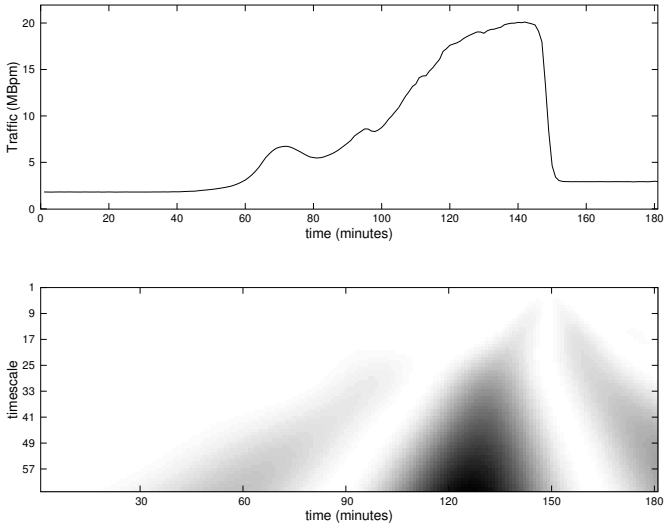


Figure 7: Traffic amount per minute (Top) and scalogram (Bottom) corresponding to the dawn period.

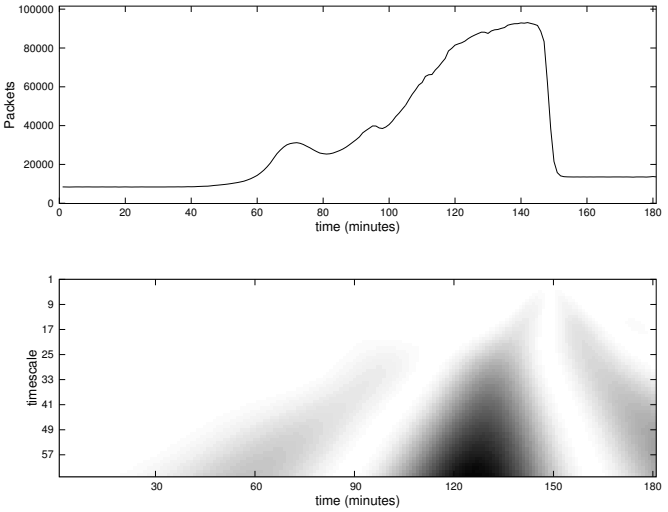


Figure 8: Number of packets per minute (Top) and scalogram (Bottom) corresponding to the dawn period.

[5] J. Beran, R. Sherman, M. Taqqu, and W. Willinger, "Long-range dependence in variable-bit rate video traffic," *IEEE Transactions on Communications*, vol. 43, no. 2/3/4, pp. 1566–1579, 1995.

[6] M. Crovella and A. Bestavros, "Self-similarity in World Wide Web traffic: Evidence and possible causes," *IEEE/ACM Transactions on Networking*, vol. 5, no. 6, pp. 835–846, Dec. 1997.

[7] V. Paxson and S. Floyd, "Wide-area traffic: The failure of Poisson modeling," *IEEE/ACM Transactions on Networking*, vol. 3, no. 3, pp. 226–244, June 1995.

[8] B. Ryu and A. Elwalid, "The importance of long-range dependence of VBR video traffic in ATM traffic engineering: Myths and realities," *ACM Computer Communication Review*, vol. 26, pp. 3–14, Oct. 1996.

[9] R. Riedi and J. Véhel, "Multifractal properties of TCP traffic: a numerical study," *Technical Report No 3129, INRIA Rocquencourt, France*, Feb 1997, available at www.dsp.rice.edu/∼riedi.

[10] A. Feldmann, A. Gilbert, and W. Willinger, "Data networks as cascades: Investigating the multifractal nature of internet WAN traffic," in *Proceedings of SIGCOMM*, 1998, pp. 42–55.

[11] R. Riedi, M. Crouse, V. Ribeiro, and R. Baraniuk, "A multifractal wavelet model with application to network traffic," *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 992–1018, April 1999.

[12] P. Salvador, A. Nogueira, and R. Valadas, "Modeling multifractal traffic with stochastic L-Systems," in *Proceedings of GLOBECOM'2002*, 2002.

[13] T. Yoshihara, S. Kasahara, and Y. Takahashi, "Practical time-scale fitting of self-similar traffic with Markov-modulated Poisson process," *Telecommunication Systems*, vol. 17, no. 1-2, pp. 185–211, 2001.

[14] P. Salvador and R. Valadas, "Framework based on markov modulated poisson processes for modeling traffic with long-range dependence," in *Internet Performance and Control of Network Systems II, Proceedings SPIE vol. 4523*, R. D. van der Mei and F. H.-S. de Bucs, Eds., August 2001, pp. 221–232.

[15] ——, "A fitting procedure for Markov modulated Poisson processes with an adaptive number of states," in *Proceedings of the 9th IFIP Working Conference on Performance Modelling and Evaluation of ATM & IP Networks*, June 2001.

[16] A. Andersen and B. Nielsen, "A Markovian approach for modeling packet traffic with long-range dependence," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 5, pp. 719–732, June 1998.

[17] P. Salvador, R. Valadas, and A. Pacheco, "Multiscale fitting procedure using Markov modulated Poisson processes," *Telecommunications Systems*, vol. 23, no. 1-2, pp. 123–148, June 2003.

[18] A. Nogueira, P. Salvador, R. Valadas, and A. Pacheco, "Fitting self-similar traffic by a superposition of mmpps modeling the distribution at multiple time scales," *IEICE Transactions on Communications*, vol. E84-B, no. 8, pp. 2134–2141, 2003.

[19] ——, "Modeling self-similar traffic through markov modulated poisson processes over multiple time scales," in *Proceedings of the 6th IEEE International Conference on High Speed Networks and Multimedia Communications*, July 2003.

[20] ——, "Hierarchical approach based on mmpps for modeling self-similar traffic over multiple time scales," in *Proceedings of the First International Working Conference on Performance Modeling and Evaluation of Heterogeneuous Networks (HET-NETs'03)*, July 2003.

[21] C. Systems. (2012, March) Cisco visual networking index: Global mobile data traffic forecast update, 2011-2016. [Online]. Available: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html

[22] d. . . m. . M. y. . . u. . h. H. Viswanathan, title = Getting Ready for M2M Traffic Growth.

[23] A. Orrevad, "M2m traffic characteristics," *Master of Science Thesis, University of Stockholm*, 2009.

[24] S. Xu and H. Hughes, "A parameterization method for markov traffic model," in *Global Telecommunications Conference (GLOBECOM '99)*, vol. 1B, 1999, pp. 1089–1093.

[25] M. Yu and M. Zhou, "A model reduction method for traffic described by MMPP with unknown rate limit," *Communications Letters, IEEE*, vol. 10, no. 4, pp. 302–304, apr. 2006.

[26] J. Slavic, I. Simonovski, and M. Boltezar, "Damping identification using a continuous wavelet transform: application to real data," *Journal of Sound and Vibration*, vol. 262, no. 2, pp. 291 – 307, 2003.

[27] K. Gurley and A. Kareem, "Applications of wavelet tran,forms in earthquake, wind, and ocean engineering." *Engineering Structures*.

 ISBN: 978-1-61208-211-0