INTERNET 2012

The Fourth International Conference on Evolving Internet

IHTIAP 2012

The First Workshop on Information Hiding Techniques for Internet Anonymity and Privacy

ISBN: 978-1-61208-204-2

June 24-29, 2012

Venice, Italy

INTERNET 2012 Editors

Massimo Villari, University of Messina, Italy

Dirceu Cavendish, Kyushu Institute of Technology, Japan

Jean-François Couchot, FEMTO-ST, University of Franche-Comté, France

INTERNET 2012

Foreword

The Fourth International Conference on Evolving Internet [INTERNET 2012], held between June 24-29, 2012 - Venice, Italy, dealt with challenges raised by evolving Internet making use of the progress in different advanced mechanisms and theoretical foundations. The gap analysis aimed at mechanisms and features concerning the Internet itself, as well as special applications for software defined radio networks, wireless networks, sensor networks, or Internet data streaming and mining.

Originally designed in the spirit of interchange between scientists, the Internet reached a status where large-scale technical limitations impose rethinking its fundamentals. This refers to design aspects (flexibility, scalability, etc.), technical aspects (networking, routing, traffic, address limitation, etc), as well as economics (new business models, cost sharing, ownership, etc.). Evolving Internet poses architectural, design, and deployment challenges in terms of performance prediction, monitoring and control, admission control, extendibility, stability, resilience, delay-tolerance, and interworking with the existing infrastructures or with specialized networks.

INTERNET 2012 also featured the following workshop:
-IHTIAP 2012, The First Workshop on Information Hiding Techniques for Internet Anonymity and Privacy

We take here the opportunity to warmly thank all the members of the INTERNET 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 INTERNET 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 INTERNET 2012 organizing committee for their help in handling the logistics and for their work to make this professional meeting a success.

We hope that INTERNET 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 the evolving internet.

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

INTERNET 2012 Chairs:
Jaime Lloret Mauri, Polytechnic University of Valencia, Spain
Eugen Borcoci, University “Politehnica” Bucharest, Romania
Abdulrahman Yarali, Murray State University, USA

INTERNET 2012

Committee

INTERNET Advisory Committee

Jaime Lloret Mauri, Polytechnic University of Valencia, Spain
Eugen Borcoci, University "Politehnica" Bucharest, Romania
Abdulrahman Yarali, Murray State University, USA

INTERNET Special Area Chairs

Routing
Mark Yampolskiy, Leibniz-Rechenzentrum (LRZ) - Garching, Germany

Traffic
Vladimir Zaborovsky, Technical University - Saint-Petersburg, Russia

Cloud and Internet
Massimo Villari, University of Messina, Italy

Security
Dirceu Cavendish, Kyushu Institute of Technology, Japan

INTERNET 2012 Technical Program Committee

Jemal Abawajy, Deakin University - Victoria, Australia
Onur Alparslan, Osaka University, Japan
Olivier Audouin, Alcatel-Lucent Bell Labs, France
Jacques Bahi, University of Franche-Comté, France
Nik Bessis, University of Derby, UK
Maumita Bhattacharya, Charles Sturt University - Albury, Australia
Jonathan Blackledge, Dublin Institute of Technology, Ireland
Eugen Borcoci, University "Politehnica" Bucharest, Romania
Christian Callegari, University of Pisa, Italy
Dirceu Cavendish, Kyushu Institute of Technology, Japan
Antonio Celesti, University of Messina, Italy
Yue-Shan Chang, National Taipei University, Taiwan
Emmanuel Chaput, IRIT-CNRS, France
Claude Chaudet, Telecom ParisTech, France
Shiping Chen, Sybase Inc., USA
Weifeng Chen, California University of Pennsylvania, USA
Young-Long Chen, National Taichung University of Science and Technology, Taiwan
Albert M. K. Cheng, Member, University of Houston, USA
Hongmei Chi, Florida A&M University, USA

Samuel Nowakovski, LORIA, France
Jeng-Shyang Pan, Harbin Institute of Technology, Taiwan
Janne Parkkila, Lappeenranta University of Technology, Finland
Marek Reformat, University of Alberta - Edmonton, Canada
Rodrigo Roman Castro, I2R, Singapore
Hamed Sadeghi Neshat, University of British Columbia
Abdel-Badeeh M. Salem, Ain Shams University Abbasia - Cairo, Egypt
Paul Sant, University of Bedfordshire, UK
Peter Schartner, University of Klagenfurt, Austria
Roman Y. Shtykh, Rakuten, Inc., Japan
Ramesh Sitaraman, University of Massachusetts - Amherst,USA
Dimitrios Serpanosm ISI/R.C. Athena & University of Patras, Greece
Adam Smutnicki, Wroclaw University of Technology, Poland
Pedro Sousa, University of Minho, Portugal
Neuman Souza, Federal University of Ceara, Brazil
Ruppa K. Thulasiram, University of Manitoba - Winnipeg, Canada
Parimala Thulasiraman, University of Manitoba - Winnipeg, Canada
Muhammad Usman, Auckland University of Technology, New Zealand
Robert van der Mei, Centrum Wiskunde & Informatica, The Netherland
Massimo Villari, University of Messina, Italy
Natalija Vlajic, York University - Toronto, Canada
Anwar Walid, Bell Labs., USA
Krzysztof Walkowiak, Wroclaw University of Technology, Poland
Junzo Watada, Waseda University - Fukuoka, Japan
Sabine Wittevrongel, Ghent University, Belgium
Kui Wu, University of Victoria, Canada
Tingyao Wu, Alcatel-Lucent/Bell Labs, USA
Mudasser F. Wyne, National University - San Diego, USA
Bin Xie, InfoBeyond Technology LLC - Louisville, USA
Mark Yampolskiy, Leibniz-Rechenzentrum (LRZ) - Garching, Germany
Zhenglu Yang, The University of Tokyo, Japan
Cliff C. Zou, University of Central Florida - Orlando, USA

IHTIAP 2012 Workshop Chairs

Jacques M. Bahi, FEMTO-ST, University of Franche-Comté, France
Christophe Guyeux, FEMTO-ST, University of Franche-Comté France
Jean-François Couchot, FEMTO-ST, University of Franche-Comté, France

IHTIAP 2012 Technical Program Committee

Gergely Acs, INRIA Rhone-Alpes, France
Jacques M. Bahi, FEMTO-ST, University of Franche-Comté, France
Thierry Berger, XLIM, University of Limoges, France
Rémi Cogranne, ICD, LM2S, University of Technology of Troyes (UTT), UMS STMR CNRS, France
Jean-François Couchot, FEMTO-ST, University of Franche-Comté, France
Eric Filiol, ESIEA Group, France
Caroline Fontaine, CNRS/Lab-STICC/CID and Télécom Bretagne/ITI, France

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

Considering Future Internet on the Basis of Smart Urban Cities A Client-City Architecture for Viable Smart Cities 1
Leonidas Anthopoulos and Panos Fitsilis

The Economic Implications of Edge-Directed Routing: A Network Operator's Perspective 5
Patrick Kwadwo Agyapong and Marvin Sirbu

On Tuning TCP for Superior Performance on High Speed Path Scenarios 11
Dirceu Cavendish, Kazumi Kumazoe, Hirofumi Ishizaki, Takeshi Ikenaga, Masato Tsuru, and Yuji Oie

Network Resources Allocation in Content-Aware Networks for Multimedia Applications 17
Eugen Borcoci, Radu Dinel Miruta, and Serban Georgica Obreja

The Super-Browser: A new Paradigm for Web Applications 24
Mark Wallis, Frans Henskens, and Michael Hannaford

An Optimization Technique on Pseudorandom Generators based on Chaotic Iterations 31
Jacques M.Bahi, Xiaole Fang, and Christophe Guyeux

Dynamic Access Control Using Virtual Multicore Firewalls 37
Alexey Lukashin and Vladimir Zaborovsky

Prototyping TCP Options to Reveal Host Identity in IP Address Sharing Environments 44
Elie Abdo, Mohamed Boucadair, and Jaqueline Queiroz

Investigation of Inadequate Multiple Account Users in a Q&A Site by Considering Deviations of Answer Submission Order 51
Kenji Umemoto, Naoki Ishikawa, Yasuhiko Watanabe, Ryo Nishimura, and Yoshihiro Okada

Electric Vehicle Charging Infrastructure – Security Considerations and Approaches 58
Steffen Fries and Rainer Falk

Man-in-the-middle Attacks Detection Scheme on Smartphone using 3G network 65
Jaemin Lee, Chaungoc Tu, and Souhwan Jung

A Robust Data Hiding Process Contributing to the Development of a Semantic Web 71
Jacques M. Bahi, Jean-Francois Couchot, Nicolas Friot, and Christophe Guyeux

Federation Between CLEVER Clouds Through SASL/Shibboleth Authentication 77
Francesco Tusa, Antonio Celesti, Massimo Villari, and Antonio Puliafito

Maximum Likelihood Decoding Algorithm for Some Goppa and BCH Codes: Application to the Matrix Encoding Method for Steganography 85
Thierry P. Berger and Mohamed Bouye Medeni

State-of-the-art in Chaotic Iterations-based Pseudorandom Numbers Generators Application in Information Hiding 90
Jacques M. Bahi, Xiaole Fang, and Christophe Guyeux

Application of Steganography for Anonymity through the Internet 96
Jacques M. Bahi, Jean-Francois Couchot, Nicolas Friot, and Christophe Guyeux

A Geometrically Resilient Digital Image Watermarking Scheme Based on SIFT and Extended Template Embedding 102
Po-Chyi Su and Yu-Chuan Chang

Formalizing and Verifying Anonymity of Crowds-based Communication Protocols with IOA 108
Yoshinobu Kawabe

Considering Future Internet on the Basis of Smart Urban Cities

A Client-City Architecture for Viable Smart Cities

Leonidas Anthopoulos and Panos Fitsilis
Project Management Department
Technological Education Institute (TEI) of Larissa
Larissa, Greece
e-mail: lanthopo@teilar.gr, fitsilis@teilar.gr

***Abstract* - The Internet has been experienced as the means for deliberation, for free social expression, for knowledge exchange, for enabling entrepreneurship. etc., while it has been capitalized by communities around the world for applications' development and for e-service deployment. In this paper Internet is considered as a supporting tool for communities' growth and wealth, and in this context the local history and experiences are viewed as the basis to focus on the future. Communities grow in organized spaces called cities. Cities did and do not emerge to the same levels, since geographic, financial, political and other variants influence this evolution. However, some cities show significant growth without meeting some of the abovementioned criteria, mainly due to the fact that some civilians present particular intelligence and enthusiasm. Various exemplars of isolated spaces were evolved due to the intelligence of some habitants, which were followed by their future generations. In this paper, this particularity structures a hypothesis, considering that the Future Internet can be based on the Smart Cities, where intelligence and experiences can be created, stored and accessed faster at a metropolitan level, limit data traffic to local areas and free significant resources of the Internet. The novel client-city architecture is proposed to support this hypothesis.**

Keywords - future Internet; smart city; internet challenges; knowledge city; networks of knowledge; smart city viability.

I. INTRODUCTION

The Internet has been dramatically evolved during the last 30 years and its evolution does not concern only technology, but all social activities. Innovative digital products that strengthen entrepreneurship, e-business, e-Government and even Internet Governance were only some of the Internet's implications. Future Internet seeks to capture Internet further evolution in more than technological aspects.

Smart cities on the other hand, appeared in late 80s and visualized urban context, while today they enhance digital content and services in urban areas, they offer sophisticated digital services, they capitalize pervasive computing and they face environmental challenges. The Smart City has an intelligent dimension [5], [7], which concerns "smart people", "smart environment", "smart economy", "smart governance", "smart mobility" and at a total "smart living". In this context, intelligence is the basis for Smart City evolution and it is measured in various ways, while commercial solutions are being offered [6] for its implementation.

This work in progress paper tries to conceptualize an architectural and algorithmic framework for the Internet of the future, which will be based on the Smart Cities for Internet future operation. More specifically, the Smart City is considered as the basis for knowledge engineering processes during e-service execution and during simple Internet processes. The produced knowledge could be captured locally and capitalized with forms similar to historical knowledge cities.

The concept of this paper is based on the following observation: cities used to evolve according to their competitive advantages and variants (e.g., habitants, physical landscape, position, facilities, access to transportation networks etc.). Knowledge cities [4] emerged as the necessity to enable urban space in order to produce and support knowledge in various ways. However, some isolated cities performed significantly in their past, growing and producing knowledge without meeting the above parameters, but due to the enthusiasm, the conceptual ability and the experiences of some habitants. Greek islands -i.e., Aegina, Spetses and Simi- and highland villages -i.e., Ferres- are representative cases, which grew impressively due to some individuals who were followed by their and by future generations.

Since isolated spaces produced knowledge that was accessed by only the local communities and supported local growth, our hypothesis concerns whether "*Smart Cities could generate and store local knowledge being produced by the local digital activities (i.e. the navigation, the discussion and the crawling of habitants) and this knowledge could be accessed at a metropolitan level by the citizens before their Internet navigation goes beyond the urban physical boundaries*". According to this hypothesis, a Smart City becomes a knowledge node –not just a proxy server-, which limits knowledge access to the civilians. Local internet users do not have to access digital resources beyond their Smart City's, and thus Internet traffic could be delimited in some scale. This conceptual model is shortly described in this paper, and this novel architecture is entitled "client-city".

Section II of this paper describes the notions of Knowledge and Smart City and determines our hypothesis. Section III describes the idea about the client-city architecture together with the potential advantages for the

 ISBN: 978-1-61208-204-2

Internet, while Section IV contains our results and future thoughts.

II. KNOWLEDGE AND SMART CITY

The city contributes to a inhabitant's everyday life in many different ways, concerning facilities and opportunities that enable citizens to live, to educate, to work, to have family, to socialize, and to perform amusing activities etc. The city provides the citizens with experiences and representations, which are influenced by the space and the place offered by the local capacity and perspectives [9]. The city offers opportunities according to its growth, and variants i.e., the position, the landscape, the population, the distance from and the position of the sea and of rivers, the accessibility to transportation networks play significant role in local growth.

Moreover, in the knowledge economy the knowledge capacity and the opportunities for knowledge production in a city matter. Various knowledge drivers have been underlined [4] such as the existence of university, the local entrepreneurship, meeting places, diversity, Information and Communications Technologies (ICT) and media. In this context, the Knowledge City could be defined as the ability of a city to enhance knowledge.

On the other hand, according to [5], the Smart City concerns the local intelligence [5], [7], which concern "smart people", "smart environment", "smart economy", "smart governance", "smart mobility" and at a total "smart living".

The term was originally met in Australian cases of Brisbane and Blacksbourg [2] where the ICT supported the social participation, the close of the digital divide, and the accessibility to public information and services. The Smart City was later evolved to (a) an urban space for business opportunities, which was followed by the network of Malta, Dubai and Kochi (India) (www.smartcity.ae); and to (b) ubiquitous technologies installed across the city, which are integrated into everyday objects and activities.

The notion of Smart City has been also approached as part of the broader term of Digital City by [1], where a generic multi-tier common architecture for digital cities was introduced, and assigned Smart City to the software and services layer. This generic architecture (Figure 4) contains the following layers:

- User layer that concerns all e-service end-users and the stakeholders of a Smart City. This layer appears both at the top and at the bottom of the generic architecture because it concerns both the local stakeholders –who supervise the Smart City, and design and offer e-services- and the end-users –who "consume" the Smart City's services and participate in dialoguing and in decision making-.
- Service layer, which incorporates all the particular e-services being offered by the Smart City.
- Infrastructure layer that contains network, information systems and other facilities, which contribute to e-Service deployment.
- Data layer that presents all the information, which is required, produced and collected in the Smart City.

III. THE CLIENT-CITY ARCHITECTURE

It is widely understood that most metropolis can be considered as Knowledge cities, while many important cities [2] are being transformed to Smart Cities. However, many small and isolated urban spaces showed crucial emergence in the past, although they did not meet some of the abovementioned drivers and characteristics of the Knowledge and Smart cities. Instead, the enthusiasm, the personality and the skills of some civilians lead to particular economic and cultural local growth, which was followed by next generations. Some representative cases come from Greece i.e., the small islands of Aegina and Simi and highland villages i.e., the village of Ferres.

This particular behavior of the urban spaces could play significant role in today's trends and in Future Internet. More specifically, the existence of a Smart City is a key driver to transform the urban space to a knowledge city. In this context, an interrelation between Smart City's architecture and knowledge city can be observed:

a) knowledge is produced on the user layer,

b) knoweledge is engineered via users' interraction with the service layer,

c) knowledge and experiences are stored in city's local resources on the data layer,

d) a knowledge mining solution could analyze these knowledge and experiences and provide them to the users in forms of organized knowledge, with a behavior much similar to knowledge cities.

Much knowledge is also produced via simple user processes (i.e. browser navigation, crawling and chatting), which enhance users' experiences. This knowledge could be also "captured" by the Smart City and stored locally, with means similar to a Proxy Server (Muller et al, 2004), but with more sophisticated mechanisms that could be called a "Smart Proxy Server". The architecture of this server is beyond the purposes of this paper.

According to this paper's approach, the entire ICT environment of the Smart City would play the role of a service provider for the local users –located at the users' architecture layer- (citizens, businesses, stakeholders). However, service provision would not be limited to the e-services -contained in the service architecture layer-, but also for trivial internet services such as Internet access, proxy services, security services (i.e., antivirus, anti-spamming, firewalls etc.), cloud services etc. In this context, the Smart City could be seen as a "metropolitan intranet".

A novel architecture can be considered, which capitalizes the Smart City's infrastructure for the execution of the previously presented knowledge management processes and for the provision of trivial Internet services. This novel architecture goes beyond cloud computing, it is entitled **client-city** architecture (Figure 1) and limits local internet activity and Internet traffic inside the city's physical boundaries. The determination of this architecture is beyond

 ISBN: 978-1-61208-204-2

the purposes of this paper and requires deeper technical analysis.

Moreover, Smart city's infrastructure could semantically describe and give logical notion to these Internet activities performed by Smart City's users, and store these "digital experiences" being gained by the civilians. For instance, consider a user who crawls for a specific issue about "*where was Alice born?*" Crawlers return various results about Alice, about her CV, about her historic profile etc., which were combined at a logical set of steps by the user, until he reaches the answer to the question. This chain of logical actions/steps that were followed by the user reflects the gained experience, while the outcome represents the gained knowledge i.e. "*Alice is born in Atlanta*" (Figure 2). Of course, alternative paths generate alternative experiences, some of which are useful, while others are meaningless.

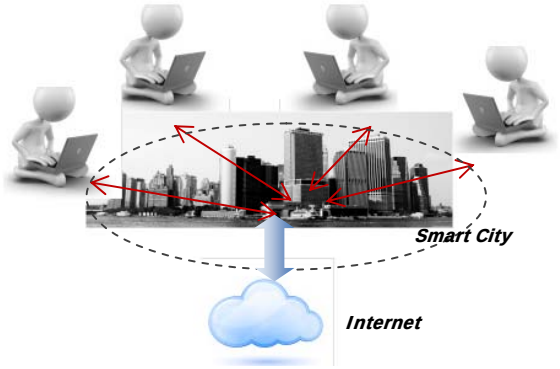


Figure 1. An initial approach to the client-city architecture: simple Internet transactions are performed via the Smart City

The Smart City could assign the successful paths to the gained answer (i.e. where the user stopped the crawling for this question), and create collections of experiences and of knowledge, in similar means such the ones that are discussed in meeting places. Consider the same procedure in a meeting place: the smart person would describe his experiences about Alice like "*Let me tell you about Alice. Alice is born in Atlanta, but … her family lives … etc.*" and a story would be created. These stories concern the local knowledge, and could be stored in the Smart City and displayed to the Smart City users automatically (Chen et al., 1995).

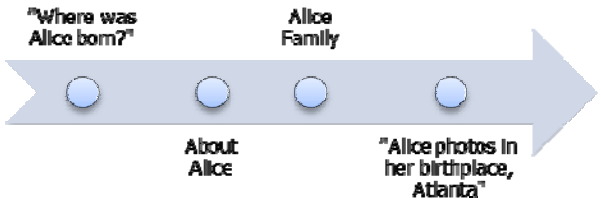


Figure 2. Experience is the path, knowledge is the reached answer

For instance, someone could read on a digital wall daily stories –like the above- created by the civilians. Furthermore, a user that would seek to answer the same question "*where was Alice born?*" would be guided by the Smart City to the locally stored answer and paths, without letting the user leave the physical boundaries of the city and charge Internet's traffic.

So the hypothesis that was defined in the beginning of this paper leads to the following potential answer: *Smart Cities can become nodes of dynamic experience and knowledge creation and storing*. Moreover, *many of local users' activities could be limited inside the Smart City, and lot of traffic can be avoided in the rest Internet*. Finally, *the client-city architecture does not influence Internet's freedom and its opportunities, since the locally stored knowledge in the Smart City can be available to all other Internet users.* According to our hypothesis, Future Internet could be based on connected Smart Cities (Figure 3).

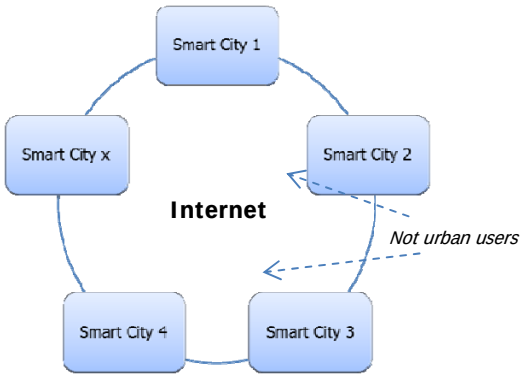


Figure 3. Future Internet can be seen as interconnected Smart Cities

IV. Results and Future Thoughts

Smart cities are being widely emerged around the world, and they enhance everyday life with the contribution of the ICT to the local needs. Various approaches to the Smart City can be faced, but all can follow the generic multi-tier architecture (Figure 4) (Anthopoulos et al., 2006). The Smart City can be seen as a driver of the Knowledge City and supports the production and storage of knowledge by its habitants.

In this paper, the capitalization of the Smart City by the Future Internet challenges is questioned. More specifically, the Smart City is considered as an isolated digital space, where knowledge is produced by the enthusiasm and by the intelligence of its civilians/end-users, with means similar to the ones observed in isolated historical villages and islands which present crucial growth.

It is hypothesized that the Smart City could support Future Internet by limiting digital traffic locally –as a metropolitan intranet-, and by lowering Internet traffic and freeing resources beyond the city area. Moreover, the Smart City can enhance knowledge production via capturing

 ISBN: 978-1-61208-204-2

citizens' digital activities and by transforming them to digital experiences and knowledge. These experiences and knowledge could be available online –e.g., in a digital wall of the Smart City-, but it could also be provided to local users who seek for similar information via local crawlers, without leaving the Smart City's resources and access the Internet.

In order for the Smart City to perform these operations it must offer typical network services –beyond its e-services-, i.e. proxy, antivirus and anti-spam, and advanced smart-proxy services. These enhanced services could also support the viability of the Smart-City, which is widely questioned and argued [2].

This paper is a work in progress, and a lot of questions need to be answered by future work. The client-city architecture must be determined in detail at a lower level, and the "smart proxy" operation needs to be specified via sophisticated algorithms. A case study would be useful and will be investigated for further research. Moreover, the transformation of the crawling process to experiences is a research challenge for the text-crawling and for the semantic web areas (i.e., the Google Knowledge Graph) and could be achieved and incorporated in a Smart City.

ACKNOWLEDGMENT

This paper is supported by the "Enterprise Architecture for Digital Cities (EADIC)" research project, which is being developed between 2012 and 2014, and funded by the Greek General Secretary for Research and Development (ARCHIMEDES III program).

REFERENCES

[1] Anthopoulos, L. and Tsoukalas, I. A., "The implementation model of a Digital City. The case study of the first Digital City in Greece: e-Trikala". Journal of e-Government (Haworth Press, Inc.), Vol.2, Issue 2, 2006.

[2] Anthopoulos, L. and Tougoutzoglou, T., "A Viability Model for Digital Cities: Economic and Acceptability Factors". In Reddick Ch. and Aikins St. (Ed) Web 2.0 Technologies and Democratic Governance: Political, Policy and Management Implications, Springer, Forth-coming, 2012.

[3] Chen, H. and Ng, T. "An Algorithmic Approach to Concept Exploration in a Large Knowledge Network (Automatic Thesaurus Consultation): Symbolic Branch-and-Bound Search vs. Connectionist Hopfield Net Activation". Journal Of The American Society For Information Science 46(5):348-369, John Wiley & Sons, Inc. 1995.

[4] Edvinsson, L., "Aspects on the city as a knowledge tool", Journal Of Knowledge Management, Vol. 10 No. 5, 2006, pp. 6-13, Emerald Group Publishing.

[5] Giffinger, R., Fertner, C., Kramar, H., Meijers, E., and Pichler-Milanovic, N., "Smart Cities: Ranking of European medium-sized cities", 2007. Retrieved, June 2012 from http://www.smart-cities.eu/download/ smartcitiesfinalreport.pdf

[6] IBM, "How Smart is your city? Helping cities measure progress", 2009. Retrieved, June 2012 from http://www-935.ibm.com/services/us/gbs/bus/html/ibv-smarter-cities-assessment.html

[7] Komninos, N., "Intelligent Cities: Innovation, Knowledge Systems and Digital Spaces", 1st. ed. London: Routledge 2002.

[8] Muller, J., Fischer, S., Gorlatch, S., and Mauve, M., "A Proxy Server-Network for Real-time Computer Games". In proceedings of Euro-Par 2004 Parallel Processing, LNCS 3149, Springer- Verlag 2004.

[9] Tuan, Yi-Fu, "Space and Place: The Perspective of Experience", 1977, University of Minnesota Press, Minneapolis, London.

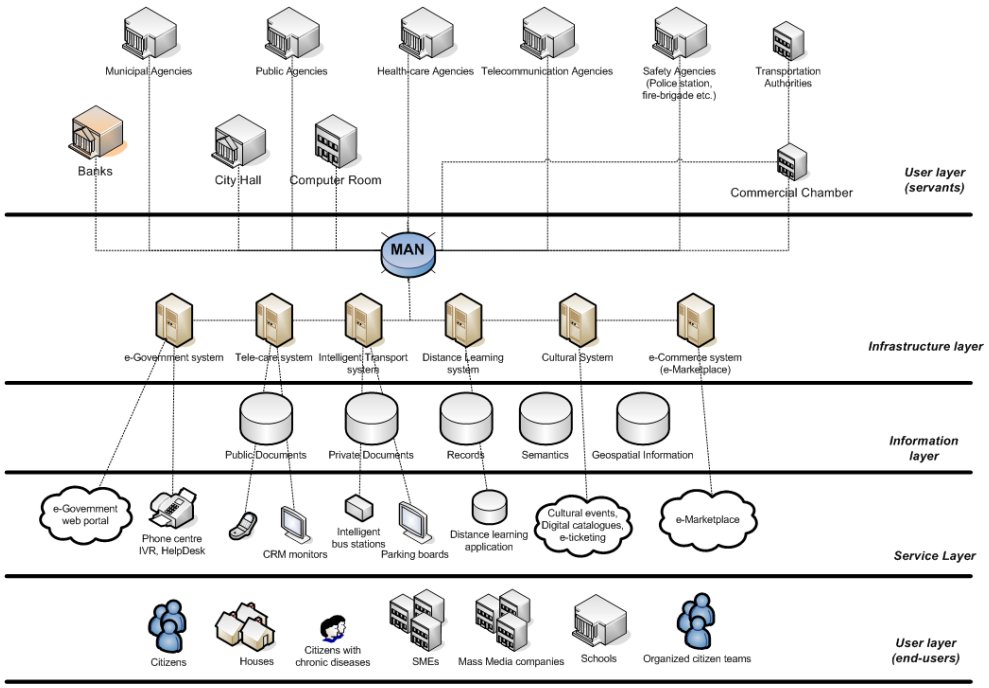


Figure 4. The multi-tier architecture of a digital city [1].

The Economic Implications of Edge-Directed Routing: A Network Operator's Perspective

Patrick Kwadwo Agyapong*†
pagyapong@cmu.edu
* Instituto Superio Técnico, Lisbon, Portugal

Marvin Sirbu †
sirbu@cmu.edu
† Carnegie Mellon University, Pittsburgh, PA 15213

***Abstract*—Edge-directed routing, a paradigm where sources and sinks of traffic, rather than the network, specify the communication path has recently gained attention as a means to deal effectively with potential conflicts that may arise between various stakeholders in the future Internet. In this paper, we use a simple economic model to show that contrary to current economic thinking, networks can deploy edge-directed routing without raising prices, provided that the service results in a relative increase in external traffic that outweighs the relative increase in costs. However, when edge-directed routing merely results in traffic shift from one path to another, then price increases are required to make it economically viable. Hence, we recommend that edge-directed routing protocols put in place payment mechanisms and support systems in their design to facilitate various pricing strategies.**

***Index Terms*—edge-directed routing; future Internet architecture; economic incentives.**

I. Introduction

Armed with lessons from almost two decades of commercial operation of the Internet, network architects realize the need to build a future Internet that is fundamentally secure and flexible enough to support diverse uses. At the same time, there is increasing awareness that, in addition to providing the right economic incentives to stimulate adoption, any new architecture must possess mechanisms to deal effectively with conflicts that may arise between various stakeholders.

It is not uncommon for an end-host's objectives to conflict with those of its provider. Unfortunately, the original architecture of the Internet lacks effective mechanisms to address such conflicts. In particular, de-facto network control over routing precludes an end-host from utilizing alternate paths to the default network-provider path. Source routing was introduced in IPv4 and IPv6 to allow sources of traffic to override default network paths. However, the majority of routers on the Internet do not support this functionality for a variety of reasons [1], [2]. Consequently, end-hosts resort to ad hoc fixes, such as overlay networks, built on top of the Internet in order to achieve performance and other security goals [3], [4].

One way to deal with conflicts between various stakeholders is to design future Internet architectures to explicitly support choice and/or competition at all levels of the architecture [5], [6]. Designing for choice implies that the architecture allows different stakeholders to express their preferences for different services [5]. On the other hand, designing for competition refers to the ability of stakeholders to "express their preferences for services by different providers" [6]. To illustrate, edge networks can currently express a preference for a first-hop network provider. Nothing prevents an edge from having multiple first-hop providers, who provide the same or different services, if desired. Hence, one can conclude that the Internet is designed for both choice and competition with regards to first-hop providers. However, an edge network has no binding input in the decisions about the intermediate networks used to transport packets, once a first-hop provider has been chosen.

Likewise, the destination or sink has no binding input in how packets are routed to it, even when it has multiple first-hop providers. In order words, the Internet is not designed for choice with regards to the nth-hop provider for both sources and sinks, when $n > 1$. This lack of nth-hop provider choice is the root cause of some of the conflicts between different stakeholders. For instance, the current Internet architecture does not support competition for the provision of intermediary services, such as filtering or virus scanning, by entities that are not first-hop providers because a sink cannot guarantee that all of its packets pass through that intermediary.

The above realization has motivated several architecture proposals that emphasize nth-hop provider choice and competition in routing [7]–[10]. It has also led to the development of a number of standalone routing protocols that provide path choice to end-hosts (e.g., [11]). We refer to these proposals collectively as edge-directed routing protocols.

Previous studies on edge-directed routing primarily focus on two main areas. The first area of work develops protocols to support edge-directed routing capabilities (e.g., [7]–[13]), whereas the second studies the equilibrium properties of networks built around edge-directed routing (e.g., [14]–[17]). Unfortunately, most studies to date have largely ignored incentive compatibility, which is vital to the successful adoption of any architecture. Specifically, previous work fail to provide any useful analysis of the economic incentives of different stakeholders to deploy and use architectures based on nth-hop provider choice.

The few studies in this area focus on understanding how network operators can maintain control over the flow of traffic through their networks when they relinquish control of path choices to the edge. For instance, Masuda and Whang use a linear programming formulation to show that networks can achieve any desirable traffic flow by using route pricing, node pricing or source-sink pricing [18]. They further show that the traffic flow that results from route or node pricing maximizes social welfare for all network participants. Kelly [19] and Laskowski *et al.* [20] obtain similar results.

However, neither of these studies addresses how such a

 ISBN: 978-1-61208-204-2

pricing mechanism is determined, the welfare effects if prices are inaccurately determined, or the information requirements needed to implement the pricing mechanism. It is very likely that the costs due to the information requirements associated with implementing elaborate pricing schemes alone will erode any benefits obtained from edge-directed routing [21]. Additionally, neither study sheds any light on whether ISPs will be better off financially from deploying edge-directed routing, even with perfectly determined route prices. Without any solid understanding of the financial risks, network operators will be reluctant to deploy edge-directed routing protocols.

In this paper, we build a simple economic model to investigate the incentives of a network operator to deploy edge-directed *inter-domain* routing. Specifically, we investigate the conditions under which network operators are better off from deploying edge-directed routing, taking into account a few pricing strategies that are relatively easy to implement. Our model shows that contrary to the arguments usually advocated in literature (e.g., [5], [20]), networks may be able to deploy edge-directed routing without increasing prices, provided that edge-directed routing results in a relative increase in external traffic that is at least equivalent to the relative increase in costs.

On the other hand, we show that if edge-directed routing merely shifts traffic from one path to another, then price increases will be required to make it economically viable. Thus, edge-directed routing protocols must incorporate payment mechanisms to support different pricing strategies. Interestingly, we also show that a flat-rate fee, with very little information requirements, will be enough to make edge-directed routing economically viable under most circumstances.

The rest of the paper is organized as follows. In Section II, we describe our network and cost model. Next, we use the model to derive the conditions that make a network operator better off from deploying edge-directed routing. We follow this with a discussion of real-world deployment issues and the implications for edge-directed routing protocol design in Section III. We conclude and discuss some future research directions in Section IV.

II. Model and Assumptions

Even though edge routing capability can be implemented at either the end-host or autonomous system (AS) level, it may be more practical to implement it at the AS level for scalability reasons. Besides, a large fraction of end-users consider the default network-selected paths sufficient for their needs and will therefore delegate path selection to the AS [11]. Moreover, it is likely that entities who are willing to pay for the capabilities of edge-directed routing consist of enterprises, educational institutions and other large organizations that can be treated as ASes. One could imagine a scenario where such an entity implements edge-directed routing on behalf of end-hosts within its control. Because of these reasons, the discussions which follow assume that edge-directed routing is implemented at the AS level.

We consider a scenario where a transit network provider, Network C, provides connectivity to N customers, who send traffic to various destinations. There exist potentially multiple paths to reach each destination outside Network C. We refer to destinations that are not customers or peers of Network C as external destinations. We consider only a single external destination for simplicity. An extension to multiple destinations is straightforward and leads to the same results. We think of each distinct path to an external destination as a different routing service (RS). We assume that Network C has the potential to offer M different routing services to reach an external destination and represent the RS set by $S = \{S^0, S^1, S^2, \ldots, S^M\}$. We illustrate this in Figure 1. In the figure, Network C has the potential to offer four routing services for its customers to reach Network L, namely $CDFIJL$, $CDFIKL$, $CEHIJL$ and $CEHIKL$.

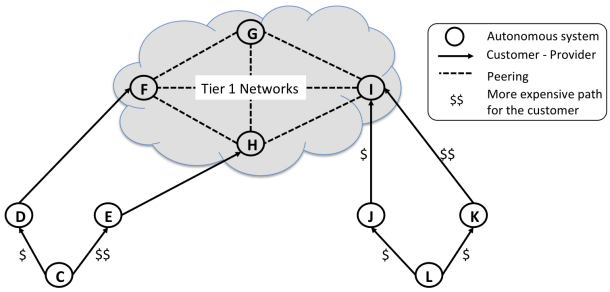


Fig. 1. Network C has the potential to offer several paths to reach a particular destination. Each different path can be considered as a routing service (RS). In the above, Network C has the potential to offer four routing services to reach Network L, namely $CDFIJL$, $CDFIKL$, $CEHIJL$ and $CEHIKL$.

Network C has two options for routing packets. It could advertise a default RS, S^0, and select the actual RS used to route packets on behalf of its customers or allow customers to specify an RS from S. For a rational network provider, S^0 is the path that minimizes its external connectivity costs. In our example in Figure 1, $CDFIKL$ is the default RS to reach Network L from Network C. This follows from the fact that Network I will only propagate path IKL in BGP because it earns more revenues when it routes traffic to L through path IK. In general, Network C can predict its own costs involved in advertising only S^0. However, the costs that Network C incurs when it allows its customers to choose from S are not well understood. In addition, it is not obvious how Network C can recover additional costs that may arise from this routing flexibility. In what follows, we provide some insights into the cost implications of allowing customers to choose from S.

Let us assume that Network C faces a total demand for external connectivity, in packets per second, given by $d = \sum_{i=1}^{N} d_i[S]$, where $d_i[S]$ is the demand for external connectivity from customer i. In the rest of the paper, we use $f[x]$ to indicate that f is a function of x. Unlike most previous work, which assumes that demand is independent of the number of available paths through the network, we explicitly make a provision for this dependency. We believe that the existence of some paths may alter traffic demand for various reasons. For instance, a customer concerned about traffic monitoring will choose to send more traffic when some perceived trustworthy paths become available. We assume that Network C has provisioned its network to support a total demand for external connectivity d.

 ISBN: 978-1-61208-204-2

In Figure 2, we show the costs that Network C incurs to route packets. In the short term, some costs such as, local loop to reach the customer, internal bandwidth within Network C and equipment, do not depend on the volume of external traffic. We denote these costs, in dollars, by K. On the other hand, external connectivity costs depend on both the volume of external traffic, d, and the path, since each path has an associated cost. Thus, we denote the external bandwidth costs, in dollars per byte transferred, by $B\left[d[S]\right]$. Additionally, Network C incurs costs, which increase with M, to distribute and manage S and to account and bill for usage. Finally, we assume that Network C faces a twice differentiable and additive cost function of the form $C\left[B[d[S]], S, K\right] = C\left[B[d[S]\right] + C\left[S, K\right]$, which satisfies $\frac{\partial C}{\partial d} = C'\left[B[d[S]]\right]|_{d=d_0}$ and $\frac{\partial^2 C}{\partial d^2} = C''\left[B[d[S]]\right]|_{d=d_0} < 0$. The latter captures economies of scale in bandwidth costs.

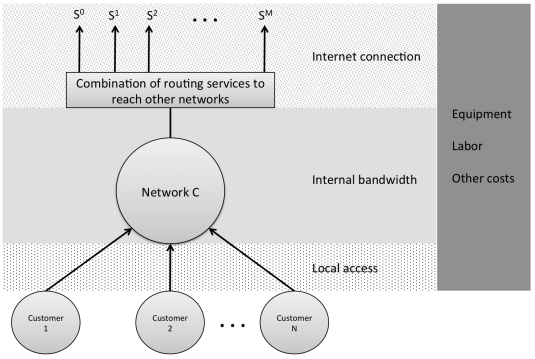


Fig. 2. Network C incurs several costs to provide both external and internal connectivity to its customers. External connectivity costs depend on the path chosen, whereas internal connectivity costs are assumed to be under Network C's control and fixed in the short-term.

A. Network-Controlled Routing

The cost to meet a total demand of d packets per second, in dollars, using S^0 is given by $\text{Cost}^{nc} = C\left[B[d[S^0]], S^0, K\right]$. Due to the presence of both fixed and variable components in the cost structure, we assume that Network C uses a two-part pricing strategy to recover its costs [22]. The choice of a two-part pricing strategy simplifies our analysis, but does not affect our results and is consistent with the interconnection scenario in the Internet [23]. The two-part price consists of a fixed access charge over period T, $E_i[S^0, K]$, in dollars, and a usage-based charge, $W_i\left[d_i[S^0]\right]$, in dollars per byte transferred by customer i. One could think of the fixed component as the flat rate fee paid for internal connectivity. Thus, over a period of T seconds, customer i pays a total of $E_i[S^0, K] + W_i\left[d_i[S^0]\right] d_i[S^0] FT$ dollars for connectivity, where F denotes the average packet size in bytes.

To reflect the situation in the current Internet peering ecosystem, we assume that the market for external connectivity is competitive. We do not make any assumptions about how Network C sets $E_i[S^0, K]$ for each customer, but we assume that $\sum_i^N E_i[S^0, K] \geq C\left[S^0, K\right]$. Given a competitive market scenario, Network C cannot set $W_i\left[d_i[S^0]\right]$ greater than the standalone costs that customer i will incur to provide the same service. Otherwise, customer i will have incentives to contract with another provider or provide the service itself. A rational cost-minimizing customer will choose S^0 when it undertakes to provide its own external connectivity. Therefore, it is reasonable for Network C to set $W_i\left[d_i[S^0]\right]$ as

$$W_i\left[d_i[S^0]\right] = \frac{C\left[B\left[d_i[S^0]\right]\right]}{d_i\left[S^0\right] FT}\ , \tag{1}$$

where $C\left[B\left[d_i[S^0]\right]\right]$ is the cost to satisfy customer i's external bandwidth demand. In order to capture the fact that Internet transit pricing exhibits economies of scale in volume, we assume that the cost function for external bandwidth is strictly sub-additive, i.e., $C\left[B\left[d[S^0]\right]\right] < \sum_i^N C\left[B\left[d_i[S^0]\right]\right]$. Sub-additivity in external bandwidth costs and $\sum_i^N E_i(S^0, K) \geq C\left[S^0, K\right]$ necessarily implies that Network C obtains a positive profit, that is, $\Pi^{nc} > 0$.

B. Edge-Directed Routing

In edge-directed routing, Network C makes S available to customers and does not impose any restrictions on the path that can be used to reach any destination. We consider a scenario where Network C has provisioned its network to support S based on some *a priori* assumptions about d. We do not address the question of how Network C selects S. Rather, we set out to find the forms that $W_i\left[d_i[S]\right]$ and $E_i[S, K]$ should take, in order to ensure that Network C is not worse off when it offers edge-directed routing based on S.

The cost and revenue for Network C when it offers edge-directed routing are given respectively by $\text{Cost}^{ec} = C\left[B[d[S]], S, K\right]$ and $\text{Revenue}^{ec} = FT\sum_i^N d_i\left[S\right] W_i\left[d_i[S]\right] + \sum_i^N E_i[S, K]$, and the resulting profit is given by Π^{ec}. In order to make edge-directed routing worthwhile, we require that $\Pi^{ec} \geq \Pi^{nc}$. If we consider the simple case where $\sum_i^N E_i[S^0, K] = C\left[S^0, K\right]$, then $\Pi^{ec} \geq \Pi^{nc}$ implies that

$$FT\sum_i^N d_i\left[S\right] W_i\left[d_i[S]\right] + \sum_i^N E_i[S, K] - C\left[B[d[S]], S, K\right]$$
$$\geq \sum_i^N C\left[B\left[d_i[S^0]\right]\right] - C\left[B\left[d[S^0]\right)\right]. \tag{2}$$

One could think of potentially infinite ways to set $W_i\left[d_i[S]\right]$ and $E_i[S, K]$ to satisfy (2). In what follows, we consider three pricing strategies and evaluate the conditions under which those strategies satisfy (2). In the first, Network C charges the same prices for both edge-directed and network-controlled routing. In the second, Network C introduces some increment on the fixed price component. In the third, the usage-based component of the price is based on the customer's standalone costs incurred to use the requested RS.

Case a : Keep same pricing as network-controlled routing: In this case, Network C sets $W_i\left[d_i[S]\right] = \frac{C\left[B\left[d_i[S^0]\right]\right]}{d_i[S^0]FT}$ and $E_i[S, K] = E_i[S^0, K]$. The constraint in (2) becomes

$$\sum_i^N C\left[B\left[d_i[S^0]\right]\right]\left(\frac{d_i[S]}{d_i[S^0]} - 1\right) \geq \Delta_B + \Delta_E\ , \tag{3}$$

where $\Delta_E = C\left[S,K\right] - \sum_i^N E_i[S^0,K]$, is the difference between the fixed costs in edge-directed and network-controlled routing and $\Delta_B = C\left[B\left[d[S]\right]\right] - C\left[B\left[d[S^0]\right]\right]$ is the difference between external bandwidth costs in edge-directed and network-controlled routing.

We see from (3) that the terms on the right side are positive. This follows from the fact that $C\left[S,K\right] > C\left[S^0,K\right]$. Also, Δ_B is zero only when all transit links are priced equally and traffic distribution is symmetric on all links with and without edge-directed routing, which is highly unlikely. Given this observation, we immediately recognize one scenario where (3) fails to hold. If the existence of a large set of path choices merely shifts demand from one path to another without increasing the total external demand, then $d_i[S] = d_i[S^0]$, which makes the term on the left side of (3) equal zero. Thus, in such a scenario, Network C is worse off when it deploys edge-directed routing without raising prices.

One could imagine that a larger set of path choices increases external traffic flowing through Network C, but does not affect total external traffic flowing through all networks. This could happen when customers move traffic away from self-provisioned (or contracted) links to Network C. If the increase in demand is large enough, then it is likely that Network C will be better off when it offers edge-directed routing without raising prices. In the short-term, Network C will obtain a competitive advantage by doing so. However, in the long-term, offering path choices will become a competitive necessity which will drive down industry-wide profits. Still, it is possible that a larger set of path choices increases external traffic flowing through the entire network. Under such a scenario, all networks will eventually find it a competitive necessity to deploy edge-directed routing without increasing prices, provided that the cost increase for doing so are smaller than the value of increased demand resulting from offering edge-directed routing. Unlike the previous case, however, it may be possible for all networks to maintain their profit margins in the long-run if external traffic increases across the entire network.

To obtain some idea about the kind of traffic increase required to make the provision of edge-directed routing justifiable without price hikes, we consider a simple case where all customers of Network C send the same volume of external traffic and pay the same prices for usage and access. Under this special case, constraint (3) can be expressed as

$$\frac{d_i[S]}{d_i[S^0]} \geq 1 + \frac{\phi C\left[B\left[d[S^0]\right],S^0,K\right]}{NC\left[B\left[d_i[S^0]\right]\right]} \ , \qquad (4)$$

where $\phi = \frac{\Delta_B+\Delta_E}{C[B[d[S^0]],S^0,K]}$ is the relative change in total costs as a result of edge-directed routing. Furthermore, we can express the total costs for Network C as

$$C\left[B\left[\cdot\right],S^0,K\right] = N\left(C\left[B\left[\cdot\right]\right] + E_i\left[S^0,K\right]\right)(1-\varsigma), \quad (5)$$

where $\varsigma = \frac{\Pi^{nc}}{\text{Revenue}^{nc}}$ is the profit margin that Network C obtains when it undertakes network-controlled routing.

Let us define $\delta = \frac{d_i[S]-d_i[S^0]}{d_i[S^0]}$ as the relative increase in external demand as a result of edge-directed routing. Based on the pricing structure assumed in our model, we can also make the approximation $\frac{C\left[B\left[d_i[S^0]\right]\right]+E_i\left[S^0,K\right]}{C[B[d_i[S^0]]]} \approx \frac{C\left[B\left[d[S^0]\right],S^0,K\right]}{C[B[d[S^0]]]}$. When changes in total costs are mostly due to changes in external bandwidth costs, which is very reasonable when $d \leq D$, then we can derive δ from (4) and (5) as

$$\delta \geq \frac{\Delta_B}{C\left[B\left[d[S^0]\right]\right]}(1-\varsigma) \ . \qquad (6)$$

Equation (6) simply states that when profit margins are close to zero, then the relative increase in external traffic must be at least equal to the relative increase in bandwidth costs in order to justify the deployment of edge-directed routing without a price increase in a well-provisioned network. For instance, when external bandwidth costs increase by 10%, then external traffic must also increase by at least 10% in order to make edge-directed routing worthwhile in the absence of a price increase. It is interesting to note that networks that only possess peering links (Tier 1 networks) do not suffer any adverse economic consequences from edge-directed routing, as long as, it does not reduce traffic flow.

Case b: Increase fixed component of price: In a scenario where the increase in external traffic from S is not large enough to overcome the additional costs associated with edge-directed routing, Network C could increase the fixed access component of the price it charges to customers. This scenario is likely to occur when edge-directed routing leads to significantly higher fixed costs (e.g. due to the need for the network to increase capacity to accommodate traffic) and/or external bandwidth costs. The idea here is that Network C sets $E_i[S,K]$ in such a way that $\sum_i^N E_i[S,K] \geq C[S,K]$, while keeping $W_i\left[d_i[S]\right] = \frac{C\left[B\left[d_i[S^0]\right]\right]}{d_i[S^0]FT}$.

In order to prevent distortion effects in pricing, we consider the case where $\sum_i^N E_i[S,K] = C[S,K]$. In setting $E_i[S,K]$, Network C could distribute the recovery burden equally among all customers or target customers who make use of edge-directed routing. It may be desirable to target the latter, in order to prevent other customers from switching to other network providers. Compared to the earlier discussion, we see that we require a smaller increase in external traffic in order to satisfy (3) when $\Delta_E = 0$.

Case c: Charge based on actual RS used: When the two pricing schemes described above fail to work, then Network C needs to charge path-based usage prices in order to make edge-directed routing economically viable. This is the conclusion reached in previous studies such as [18]–[20]. Unlike these studies, we go a step further to suggest the forms that the prices could take. For instance, the fixed access charges could be set such that $\sum_i^N E_i[S,K] = C[S,K]$, with the burden preferably shifted to customers who make use of edge-directed routing. If the network can estimate the demand from customers that will result from S, then it can set usage-based prices equal to the standalone costs for the customers to acquire the service. In other words, Network C sets $W_i\left[d[S]\right] = \frac{C[B[d_i[S]]]}{d_i[S]FT}$. Customers who obtain a utility from S will have incentives to pay the increased usage-based price, whereas other customers pay the price for using the default network path.

 ISBN: 978-1-61208-204-2

To summarize, our analysis suggests that edge-directed routing protocols that do not introduce significant fixed costs can be deployed without any increase in prices, provided that they lead to a relative increase in external traffic roughly equivalent to the relative increase in external bandwidth costs. Even when fixed costs increase, networks could recover these costs by raising fixed access charges for customers who utilize edge-directed routing. From the network provider's point of view, such pricing schemes are desirable because they incur minimum overhead to account and bill for usage. Hence, designers must minimize the fixed costs associated with edge-directed routing protocols in order to provide the maximum incentives for networks to deploy them.

Our discussion so far has focused on Network C as the provider of edge-directed routing. In truth, the arguments we have made and the pricing strategies we have discussed apply recursively from Tier 1 Networks ($F, G, H,$ and I in Figure 1) to Network C. These Tier 1 networks offer edge-directed routing to their customers based on an RS set S'. Our results suggest that Tier 1 networks can offer a large RS set, since by definition, they do not pay for transit. The customers may then act as providers to other networks and offer edge-directed routing based on an RS set S, where $S \in S'$. Thus, our model is consistent with future Internet architectures like SCION (see [10]), which relies on a top-down notion of trust (and payment) relationships among networks.

III. Real World Deployment Issues

In this section, we identify key features required to support the deployment of edge-directed routing. After this, we highlight some business opportunities enabled by edge-directed routing and the potential costs to exploit them.

A. Features Required to Support Edge-Directed Routing

We identify five features necessary for commercial deployment of any edge-directed routing protocol namely *knowledge*, *choice*, *enforcement*, *metering* and *verification*.

1) Knowledge: First, edge-directed routing protocols must provide a scalable means for edges to obtain knowledge of a set of secure and policy-complaint paths to a given destination. In particular, the process of path discovery must recognize and address the business needs of ISPs. For example, ISPs may want to control the diversity of alternative paths exposed to the edge. Even though most previous work discuss ways to provide knowledge about paths, more work is needed to design scalable and incentive-compatible knowledge dissemination mechanisms for edge-directed routing.

2) Choice: Secondly, edge-directed routing protocols must equip the source, sink or both with the capability to specify a policy-compliant path. Additionally, there must be mechanisms for intermediate networks on the path to consent to the use of the specified paths. In our model, the latter requirement was achieved by making S a subset of S', but that is not the only way one could meet this requirement.

In order to overcome some of the security issues that plagued source routing in IP networks, we note that the protocol must provide **both** the source and the sink with the joint responsibility to specify a policy compliant end-to-end path. This is the approach taken in proposals such as SCION [10] and ICING [9]. Alternatively, the protocol could insist that sinks find an independent path back to the source. It may be more desirable to give joint responsibility to the source and sink because this allows both parties to effectively deal with scenarios where they have conflicting requirements.

3) Enforcement: Thirdly, the protocol must provide a scalable means for the routers in origin and transit networks to enforce that the ASes to which they belong have approved the use of a specific network resource. This is especially important if networks charge for edge-directed routing, since the network needs to distinguish between paying and non-paying customers. This could be achieved using technical mechanisms such as cryptography embedded within the protocol or with other means outside the protocol such as admission control. This area, which was largely ignored in the past, has attracted some attention recently [9], [10]. For example, SCION uses an *opaque field* in the path construction beacon to account for the use of specific resources [10]. Similarly, ICING uses *proofs of consent* (PoCs), issued by networks on the path, as a means to enforce the use of network resources [9].

4) Metering: In addition to enforcement, the network needs to measure and track the amount of traffic that customers send in order to implement usage-based pricing. The information requirements associated with different pricing strategies will determine the viability of offering services based on that pricing model. In general, path-based pricing will require the most information to implement. Thus, ISPs will be reluctant to offer services based on this pricing model unless the information costs are negligible. However, designing metering schemes with negligible information costs poses a huge challenge. To date, most of the literature fail to address this important issue.

5) Verification: Whereas enforcement allows the network provider to account for resource use, verification enables the customer to attest that a requested edge-directed routing service was delivered. This requirement is particularly important when the customer pays for the requested service. It has been shown by Laskowski and Chuang that, at a minimum, *contractible monitors*, defined as "a distributed algorithmic mechanism that runs on the network graph, and outputs, to specific nodes, proofs about current or past network behavior that can serve as input to a contract", must be present in order to induce networks to deploy innovative technologies [24]. Most edge-directed routing protocols lack any features for verification, thereby dampening any incentives for networks to deploy and use them.

Based on the above discussion, we reckon that edge-directed routing protocols that support all the above features could lead to significant packet and communication overhead. In ICING for instance, a random packet is expected to have about 45% packet overhead [9]. Further, the designers estimate that ICING will add about 23% overhead to total traffic, which is quite significant [9]. Indeed, the extra usage cost associated with path choice may well be due to the increase in overhead, which means that the network provider has to acquire and pay more for external bandwidth, even when

 ISBN: 978-1-61208-204-2

all path choices cost the same per byte. Hence, an analysis of typical communication overhead incurred to provide the features above for proposed protocols will prove very useful to understand the viability of some business opportunities.

B. Business Opportunities

A secure and policy-compliant edge-directed routing protocol could enable providers to deploy and monetize new and enhanced routing capabilities. Business models based on charging a premium for edge-directed routing require mechanisms to distinguish between paying and non-paying customers. They also depend on the existence of verification mechanisms or other notions of trust between the network provider and the customer [24].

Unlike network-controlled routing, edge-directed routing guarantees nth-hop provider choice for $n > 1$. This capability opens up the possibility to purchase network services such as filtering, DDoS protection and virus scanning from entities other than the first-hop network provider [7], [9]. Without edge-directed routing, edges either have to purchase such services from the first-hop provider or through other providers that use BGP tricks to appear as a first-hop provider. The main limitation with purchasing middlebox services in this way is that edges are consigned to only a single middlebox service provider and cannot selectively choose which packets avoid the middlebox.

On the contrary, edge-directed routing allows a sink to simply specify a path that contains the middlebox provider for a subset of packets that requires the use of the service. The sink could even contract with multiple middlebox providers for different classes of services and dynamically decide which packets go through which middlebox service. This approach provides greater flexibility and choice to edge networks. Nonetheless, this business opportunity imposes new costs that could instigate new conflicts among Internet stakeholders and needs to be investigated further.

IV. Conclusion and Future Work

In this paper, we have shown that it may be possible for network providers to deploy edge-directed routing without raising prices, provided that it results in a relative increase in external traffic that is at least equivalent to the relative increase in costs. However, when edge-directed routing merely shifts the same external traffic from one path to another, then a price increase is required to justify its deployment. For this, we have shown that a flat-rate increase, which requires relatively little information to implement, will suffice in most cases. Nevertheless, it is important that edge-directed routing protocols provide payment mechanisms to support various pricing strategies. In addition, we have identified some essential features needed to support real-world deployment of edge-directed routing. These features include mechanisms to provide *knowledge*, *choice*, *enforcement*, *metering* and *verification*.

It will be interesting to investigate the relative magnitude of the welfare loss that results from using our simple pricing strategy, as opposed to route or node pricing. We plan to explore this area in our future work. We also hope to further explore the potential business opportunities that edge-directed routing could open up and identify the challenges that must be overcome in order to exploit these opportunities.

Acknowledgment

Support for this work was provided by the Fundação para a Ciência e a Tecnologia (FCT) through the CMU-Portugal Program under award SFRH/BD/33507/2008 and by NSF under award number CNS-1040801. The authors would like to thank the XIA Project Group at Carnegie Mellon University for providing useful feedback during the early stages of this work and the anonymous reviewers for their insightful comments, which helped to improve the clarity of the paper.

References

[1] S. M. Bellovin. Security Problems in the TCP/IP Protocol Suite. *SIGCOMM Comp. Comm. Rev.*, 19:32–48, Apr. 1989.

[2] Jake Edge. IPv6 Source Routing: History Repeats Itself. http://lwn.net/Articles/232781/, May 2007.

[3] D. Andersen, H. Balakrishnan, F. Kaashoek, and R. Morris. Resilient Overlay Networks. *SIGOPS Oper. Syst. Rev.*, 35:131–145, Oct. 2001.

[4] RFC 2547. BGP/MPLS VPNs. Technical report, Mar. 1999.

[5] D. Clark, J. Wroclawski, K. Sollins, and R. Braden. Tussle in Cyberspace: Defining Tomorrows Internet. In *Proc. of ACM SIGCOMM*, pages 347–356, Aug. 2002.

[6] J. Chuang. Loci of Competition for Future Internet Architectures. *IEEE Comm. Mag.*, 49(7):38 –43, Jul. 2011.

[7] M. Walfish, J. Stribling, M. Krohn, H. Balakrishnan, R. Morris, and S. Shenker. Middleboxes no Longer Considered Harmful. In *Proc. of the 6th Conf. on Oper. Sys. Des. & Impl. - Volume 6*, 2004.

[8] X. Yang, D. Clark, and A. Berger. NIRA: A New Inter-Domain Routing Architecture. *IEEE Trans. Net.*, 15(4):775 –788, Aug. 2007.

[9] J. Naous, A. Seehra, M. Walfish, D. Mazieres, A. Nicolosi, and S. Shenker. The Design and Implementation of a Policy Framework for the Future Internet. Technical Report TR-09-28, The University of Texas at Austin, Sep. 2009.

[10] X. Zhang, H. Hsiao, G. Hasker, H. Chan, A. Perrig, and D. Andersen. SCION: Scalability, Control, and Isolation On Next-Generation Networks. Technical Report CMU-CyLab-10-020, Mar. 2011.

[11] W. Xu and J. Rexford. MIRO: Multi-path Interdomain Routing. *SIGCOMM Comp. Comm. Rev.*, 36:171–182, Aug. 2006.

[12] B. Raghavan and A. Snoeren. A System for Authenticated Policy-Compliant Routing. *SIGCOMM Comp. Comm. Rev.*, 34:167–178, Aug. 2004.

[13] P. Godfrey, I. Ganichev, S. Shenker, and I. Stoica. Pathlet Routing. *SIGCOMM Comp. Comm. Rev.*, 39:111–122, Aug. 2009.

[14] A. Orda, R. Rom, and N. Shimkin. Competitive Routing in Multiuser Communication Networks. *IEEE Trans. Net.*, 1:510–521, Oct. 1993.

[15] K. Park, M. Sitharam, and S. Chen. Quality of Service Provision in Non-cooperative Networks with Diverse Service Requirements. *Decision Support Systems*, 28(1_-2):101 – 122, 2000.

[16] T. Roughgarden and É. Tardos. How Bad is Selfish Routing? *Journal of the ACM*, 49:236–259, Mar. 2002.

[17] L. Qiu, Y. Yang, Y. Zhang, and S. Shenker. On selfish routing in internet-like environments. *IEEE Trans. Net.*, 14(4):725 –738, Aug. 2006.

[18] Y. Masuda and S. Whang. Capacity Management in Decentralized Networks. *Manage. Sci.*, 48:1628–1634, Dec. 2002.

[19] F. P. Kelly. Charging and Rate control for Elastic Traffic. *Eur. Trans. Tel.*, 8(1):33–37, 1997.

[20] P. Laskowski, B. Johnson, and J. Chuang. User-Directed Routing: From Theory, Towards Practice. NetEcon '08, pages 1–6, 2008.

[21] D. Levinson and A. Odlyzko. Too Expensive to Meter: the Influence of Transaction Costs in Transportation and Communication. *Phil. Trans. R Soc. A*, 366(1872):2033–2046, 2008.

[22] B. M. Mitchell and I. Vogelsang. *Telecommunications Pricing: Theory and Practice*. Cambridge University Press, 1991.

[23] B. Briscoe and S. Rudkin. Commercial Models for IP Quality of Service Interconnect. *BT Technology Journal*, 23(2):171–195, Apr. 2005.

[24] P. Laskowski and J. Chuang. Network Monitors and Contracting Systems: Competition and Innovation. *SIGCOMM Comp. Comm. Rev.*, 36:183–194, Aug. 2006.

 ISBN: 978-1-61208-204-2

On Tuning TCP for Superior Performance on High Speed Path Scenarios

Kazumi Kumazoe, Hirofumi Ishizaki, Takeshi Ikenaga, Dirceu Cavendish, Masato Tsuru, Yuji Oie
Department of Computer Science and Electronics
Kyushu Institute of Technology
Fukuoka, Japan 810-0004
Email: {zaki,ike}@ecs.kyutech.ac.jp, {kuma,cavendish,tsuru,oie}@ndrc.kyutech.ac.jp

***Abstract*—Transmission control protocol performance varies considerably, depending on network and path conditions. In this paper, we discuss path conditions that affect TCP performance, from round trip delays to path capacity and buffering. We characterize throughput performance of popular TCP congestion avoidance mechanism as well as recently proposed TCP variants via open source based network experiments. We show that superior TCP performance may be achieved via careful selection of congestion avoidance mechanism, as well as parameter tuning.**

***Keywords*—high speed networks; TCP congestion avoidance; Packet retransmissions; Path capacity and buffering;**

I. INTRODUCTION

Transmission control protocol (TCP) is the dominant transport protocol of the Internet, providing reliable data transmission for the large majority of applications. User experience depends heavily on TCP performance. In the last decade, many TCP variants have been proposed, mainly motivated by performance reasons. As TCP performance depends on network characteristics, and the Internet keeps evolving, TCP variants are likely to continue being proposed. Most of the proposals deal with congestion window size adjustment mechanism, the so called congestion avoidance phase of TCP.

In prior works, we have introduced a delay based TCP window flow control mechanism that uses path capacity and storage estimation [6], [7]. The idea is to estimate bottleneck capacity and path storage space, and regulate the congestion window size using a control theoretical approach. Two versions of this mechanism were proposed: one using a proportional controlling equation [6], and another using a proportional plus derivative controller [7].

In this work, we study TCP performance of most popular TCP variants - Reno [3], Cubic (Linux) [11], Compound TCP (Windows) [12] - as well as our most recently proposed TCP variants: Capacity and Congestion Probing (CCP) [6], and Capacity Congestion Plus Derivative (CCPD) [7], under various path conditions. Our contributions are as follows. We show that most used TCP variants of today perform differently over various network scenarios. In addition, for our TCP variants, we tune their performance according to network scenarios for superior performance. Our results show that there is no single TCP variant that is able to best perform under all network scenarios. For our protocols, we investigate best protocol parameters to deliver superior performance. For other protocols, our results can be seen as a call for protocol tuning. The material is organized as follows. Related work discussion is provided on Section II. Section III introduces the TCP variants addressed in this paper, their features and differences. Section IV addresses their performance evaluation. Section VI addresses directions we are pursuing as follow up to this work.

II. RELATED WORK

Research studies of TCP performance on various network environments abound. Many of these studies, have focused on mobile wireless networks [5], [9], [13], as loss based congestion avoidance has the issue of not being able to differentiate between random packet loss and buffer overflow packet loss [4]. [5] studies throughput performance of TCP variants for various Packet Error Rates (PERs) on a mobile network via simulations. [9] also studies TCP variants performance under various PERs, but it also investigates the impact of routing protocols on TCP performance. Wireless network scenarios typically involve a low speed bottleneck link capacity, which limits the size of the congestion window to small values, masking the buffer overflow problem on routers.

On wired high speed networks, [8] has conducted a study of the impact of buffer size, packet error rate, and network delay on throughput performance of NewReno, BIC, Cubic, Highspeed, and Compound TCP variants under large bandwidth delay product and high capacity bottlenecks, via simulations. Although our work has similarities with theirs, we evaluate unique aspects of TCP such as throughput recovery upon cross traffic via open source experiments rather than simulations.

III. TRANSMISSION CONTROL PROTOCOL FRAMEWORK

TCP protocols fall into two categories, delay and loss based. Advanced loss based TCP protocols use packet loss as primary congestion indication signal, performing window regulation as $cwnd_k = f(cwnd_{k-1})$, being ack reception paced. Most f functions follow an Additive Increase Multiplicative Decrease strategy, with various increase and decrease parameters. TCP NewReno and Cubic are examples of AIMD strategies. In contrast, delay based TCP protocols use queue delay information as the congestion indication signal, increasing/decreasing the window if the delay is small/large, respectively. CCP and CCPD are examples of delay based protocols.

 ISBN: 978-1-61208-204-2

Most TCP variants follow a framework composed of few phases: slow start, congestion avoidance, fast retransmit, and fast recovery.

- **Slow Start(SS) :** This is the initial phase of a TCP session, where no information about the session path is assumed. In this phase, for each acknowledgement received, two more packets are allowed into the network. Hence, congestion window $cwnd$ is roughly doubled at each round trip time. Notice that the $cwnd$ size can only increase in this phase. In this paper, all TCP variants make use of the same slow start except Cubic [11].
- **Congestion Avoidance(CA) :** This phase is entered when the TCP sender detects a packet loss, or the $cwnd$ size reaches a target upper size called $ssthresh$ (slow start threshold). The sender understands that the $cwnd$ size needs to be controlled to avoid path congestion. Each TCP variant has a different method of $cwnd$ size adjustment.
- **Fast Retransmit and fast recovery(FR) :** The purpose of this phase is to freeze all $cwnd$ size adjustments in order to take care of retransmissions of lost packets.

Figure 1 illustrates various phases of a TCP session. A comprehensive tutorial of the evolution of TCP features can be found in [2].

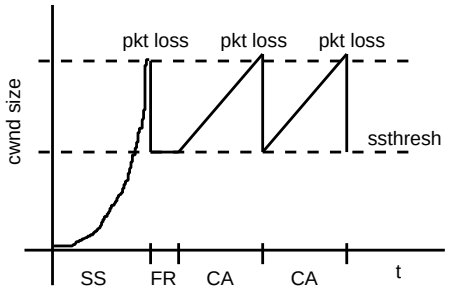


Fig. 1: TCP Congestion Window Dynamics

A. Reno TCP

Reno is a loss based TCP, and may be considered the oldest implementation of TCP to achieve widespread usage. Its congestion avoidance scheme relies on increasing the $cwnd$ by $1/cwnd$ increments, and cutting it in half on packet loss detection, as per equation 1.

$$\begin{aligned} AckRec: \quad cwnd_{k+1} &= cwnd_k + \frac{1}{cwnd_k} \\ PktLoss: \quad cwnd_{k+1} &= \frac{cwnd_k}{2} \end{aligned} \tag{1}$$

Notice that for large $cwnd$ values, the increment becomes small. So, for large bandwidth delay product paths, Reno $cwnd$ ramps up very slowly. A new version of Reno, TCP NewReno introduces an optimization of the Fast Recovery mechanism, but its congestion avoidance scheme remains the same.

B. Cubic TCP

TCP Cubic is a loss based TCP that has achieved widespread usage due to being the default TCP of the Linux operating system. Its congestion window adjustment scheme is:

$$\begin{aligned} AckRec: \quad cwnd_{k+1} &= C(t-K)^3 + Wmax \\ K &= (Wmax\frac{\beta}{C})^{1/3} \\ PktLoss: \quad cwnd_{k+1} &= \beta cwnd_k \\ Wmax &= cwnd_k \end{aligned} \tag{2}$$

where C is a scaling factor, $Wmax$ is the $cwnd$ value at time of packet loss detection, and t is the elapsed time since the last packet loss detection ($cwnd$ reduction). Although the equations look complicated, the rational is simple. Cubic remembers the $cwnd$ value at time of packet loss detection - $Wmax$, when a sharp $cwnd$ reduction is enacted, tuned by parameter β. After that, $cwnd$ is increased according to a cubic function, whose speed of increase is dictated by two factors: i) how long it has been since the previous packet loss detection, the longer the faster ramp up; ii) how large the $cwnd$ size was at time of packet loss detection, the smaller the faster ramp up. The shape of Cubic $cwnd$ dynamics is typically distinctive, clearly showing its cubic nature. Notice that upon random loss, Cubic strives to return $cwnd$ to the value it had prior to loss detection quickly, for small $cwnd$ sizes.

C. Compound TCP

Compound TCP is the TCP of choice for most Windows machines. It implements a hybrid loss/delay based congestion avoidance scheme, by adding a delay congestion window $dwnd$ to the congestion window of NewReno [12]. Compound TCP $cwnd$ adjustment is as per Equation 3:

$$\begin{aligned} AckRec: \quad cwnd_{k+1} &= cwnd_k + \frac{1}{cwnd_k + dwnd_k} \\ PktLoss: \quad cwnd_{k+1} &= cwnd_k + \frac{1}{cwnd_k} \end{aligned} \tag{3}$$

where the delay component is computed as:

$$\begin{aligned} AckRec: dwnd_{k+1} &= dwnd_k + \alpha dwnd_k^K - 1, \text{if } diff < \gamma \\ & \quad dwnd_k - \eta diff, \quad \text{if } diff \geq \gamma \\ PktLoss: dwnd_{k+1} &= dwnd_k(1-\beta) - \frac{cwnd_k}{2} \end{aligned} \tag{4}$$

where α, β, η and K parameters are chosen as a tradeoff between responsiveness, smoothness, and scalability. $diff$ is defined as the difference between an expected throughput and the actual throughput, as $diff = cwnd/minRtt - cwnd/srtt$, $minRtt$ is the minimum rtt experienced by the TCP session, and $srtt$ is a smooth round trip delay computation.

D. Capacity and Congestion Probing TCP

TCP CCP is our first attempt to design a delay based congestion avoidance scheme based on solid control theoretical approach. The $cwnd$ size is adjusted according to a proportional controller control law. The $cwnd$ adjustment scheme is called at every acknowledgement reception, and may result in either window increase and decrease. In addition, packet loss does not trigger any special $cwnd$ adjustment. CCP $cwnd$ adjustment scheme is as per Equation 5:

 ISBN: 978-1-61208-204-2

$$cwnd_k = \frac{[Kp(B - x_k) - in\_flight\_segs_k]}{2} \quad 0 \leq Kp \qquad (5)$$

where Kp is a proportional gain, B is an estimated storage capacity of the TCP session path, or virtual buffer size, x_k is the level of occupancy of the virtual buffer, or estimated packet backlog, and in_flight_segs is the number of segments in flight (unacknowledged). Typically, CCP $cwnd$ dynamics exhibit a dampened oscillation towards a given $cwnd$ size, upon cross traffic activity. Notice that $cwnd_k$ does not depend on previous $cwnd$ sizes, as with the other TCP variants.

E. Capacity and Congestion Plus Derivative TCP

TCP CCPD is our second attempt to design a delay based congestion avoidance scheme based on solid control theoretical approach, being a variant of CCP. The scheme $cwnd$ adjustment follows the same strategy of CCP. The difference is that it uses a proportional plus derivative controller as its control equation, as per Equation 6:

$$cwnd_k = Kp[B - x_k - in\_flight\_segs_k] + \frac{Kd}{t_k - t_{k-1}}[x_{k-1} + in\_flight\_segs_{k-1} + -x_k - in\_flight\_segs_k] \qquad (6)$$

where Kp is a proportional gain, Kd is a derivative gain, t_k and t_{k-1} are two consecutive ack reception epochs, and the other parameters are defined as per CCP congestion avoidance scheme. Typically, CCPD $cwnd$ dynamics present similar dampened oscillatory behavior as CCP, with a much faster period, due to its reaction to the derivative or variation of the number of packets backlogged.

IV. TCP Variants Performance Characterization

It is well known that TCP throughput performance is affected by the round trip time of the TCP session. This is a direct consequence of the congestion window mechanism of TCP, where only up to a $cwnd$ worth of bytes can be delivered without acknowledgements. Hence, for a fixed $cwnd$ size, from the sending of the first packet until the first acknowledgement arrives, a TCP session throughput is capped at $cwnd/rtt$.

As mentioned earlier, for all TCP variants, the size of the congestion window is computed by a specific algorithm at time of packet acknowledgement reception by the TCP source. In this section, we characterize TCP performance regarding data throughput in various network scenarios. For CCP, and CCPD protocols, we shall use $CCP(K_p)$ notation for CCP using proportional parameter K_p, whereas $CCPD(K_p, K_d)$ for CCPD using proportional and derivative parameters, K_p and K_d, respectively.

We evaluate the throughput performance of TCP variants in the presence of controlled cross traffic. Fig. 2 depicts the network scenario used for evaluating TCP protocols against interfering UDP and TCP types of cross traffic. One TCP session shares a 1Gbps access link with UDP cross traffic of 200Mbps intensity to a dumb-bell topology emulator highspeed network, depicted in Fig. 2 a). The PacketStorm 4XG IP Network Emulator [10] is used to vary the end-to-end round trip time of the TCP sessions. Two Alaxala switches [1] were used, AX-3630-24T2X and AX-2430-48T-B. As endpoints, Dell PowerEdge2950 Xeon 1.6GHz machines were used, running Linux 2.6.26.

Fig. 2 b) describes the timeline of the TCP and UDP sessions, with the TCP session lasting for 150 secs, and the UDP traffic starting 50 seconds after the TCP session start, and finishing 50 secs prior to the end of the TCP session. Figure 2 c) describes the timeline of a TCP and TCP two session scenario, where two TCP sessions compete for bottleneck link bandwidth.

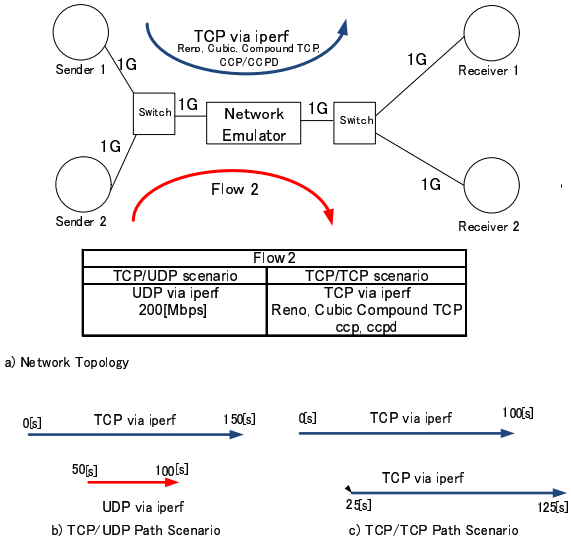


Fig. 2: TCP Coexisting Evaluation Scenarios

A. Coexisting TCP/UDP sessions

This experiment set is designed to study the performance of TCP variants on a single session, when facing cross traffic. Performance measurers of interest are throughput and throughput recovery, defined as the ratio between the throughput achieved after cross traffic exists the session path, divided by the amount of throughput achieved before the session experience any cross traffic.

1) Short round trip time paths: Figure 3 reports throughput performance of a TCP session subjected to UDP cross traffic on short rtts, similar to local or countrywide session. Overall, Compound TCP, Reno, and Cubic are best performers across all TCP variants, followed close by CCPD(4,4000), although the later is not able to reclaim as much throughput after UDP traffic goes away than the former protocols.

2) Large round trip time paths: Figure 4 reports TCP throughput performance over a session with large rtt, similar to transoceanic data transfers. Looking at the time prior to the UDP traffic injection, the outperformers are Compound TCP and Cubic, followed by CCPD(2,1000) and CCP(4). In the presence of UDP traffic, the best performers are Cubic, and most of CCPD protocols.

Figure 5 reports the throughput recovery ratio, which shows how much the TCP session is able to ramp up back after cross traffic is finished. The best performers for large rtt sessions

 ISBN: 978-1-61208-204-2

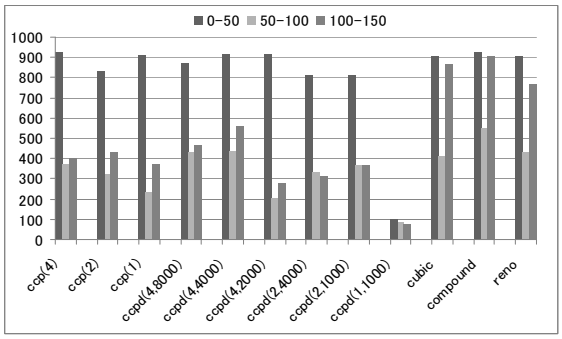


Fig. 3: TCP/UDP throughput - short rtt(20msecs)

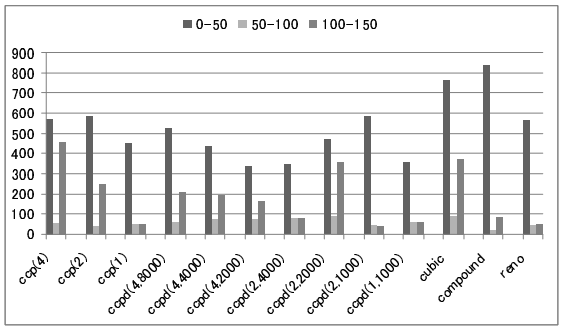


Fig. 4: TCP/UDP throughput - large rtt(200msecs)

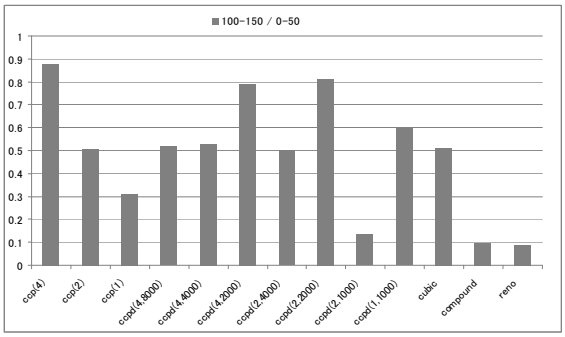


Fig. 5: TCP/UDP throughput recovery - large rtt(200msecs)

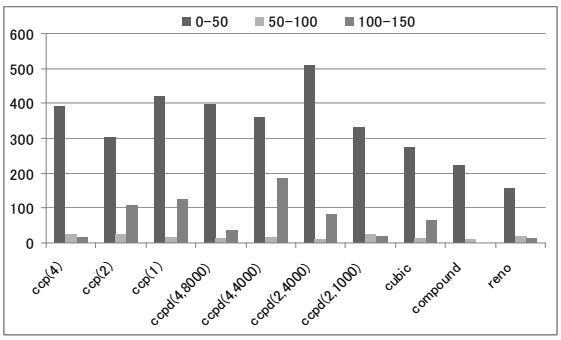


Fig. 6: TCP/UDP throughput - very large rtt(600msecs)

are CCP(4), CCPD(2,2000) and CCPD(4,2000). The worst performers are Reno and Compound TCP.

3) Very large round trip time paths: Figure 6 reports TCP throughput performance over a very large rtt, typically incurred in satellite paths. In this case, traditional TCP variants have the worst performance across all TCP variants investigated. Best performers are CCPD(2,4000), CCPD(4,4000) and CCP(1). For very large rtt paths, CCPD(2,4000) and CCPD(4,4000) seem to be the top TCP variants performers.

B. Coexisting TCP/TCP sessions

In this subsection, we investigate the throughput performance of two TCP flows sharing a single bottleneck. Two cases can be distinguished: homogeneous case, where the two TCP sessions belong to the same TCP variant; heterogeneous case, where the two TCP sessions belong to different TCP variants.

1) Small round trip time paths: Figure 7 reports throughput performance of two TCP sessions, staggered in time, over a short rtt path. For the initial period, with only a single session, all TCP variants perform similarly. During the period of the two sessions sharing a bottleneck, CCP with large alpha parameter delivers best performance. During "recovering period", where the first session leaves the system, Reno and Compound TCP present best throughput ramp up performance, followed by CCPD(4,4000) and Cubic as second best.

Figures 8 and 9 report throughput performance of CCPD(4,2000) competing with Reno, Cubic, and Compound TCP variants over a short rtt path. Figure 8 reports performance when the first flow is CCPD(4,2000), whereas Figure 9 reports the reverse scenario, when the second flow is CCPD(4,2000). In general, Flow 1 and flow 2 path bandwidth resource is shared unevenly. Comparing the two cases, throughput ramp up of flow 2 after flow 1 departs is best achieved by CCPD(4,2000), except when Compound TCP is used by flow 2, in this short rtt scenario.

Figures 10 and 11 report throughput performance of CCPD(4,4000) competing with Reno, Cubic, and Compound TCP variants over a short rtt path. In general, flow 1 and flow 2 path bandwidth resource is shared very unevenly. Comparing Figure 10 and 11, the following observations can be made. i) Throughput performance of all TCP variants are similar when there is no cross traffic; ii) CCPD(4,4000) is able to ramp up throughput to higher levels once cross traffic vanishes, except against Compound TCP ramp up performance, which again is better for this short rtt scenario. When compared with CCPD(4,2000) performance, it is clear that CCPD(4,4000) retains more throughput under TCP cross traffic for short rtt scenario.

2) Large round trip time paths: Figure 12 reports throughput performance of two TCP sessions, staggered in time, over a long rtt path. For the initial period, with only a single session, Compound TCP and Cubic deliver best throughput performance. During the period of the two sessions sharing a bottleneck, Cubic, Compound TCP and Reno present the best aggregate performance. Notice, however, that this is because the first flow retains most of its throughput prior to the sharing of bandwidth with the second flow. During "recovering period", where the first session leaves the system, Cubic and CCPD(4,2000) deliver best throughput.

 ISBN: 978-1-61208-204-2

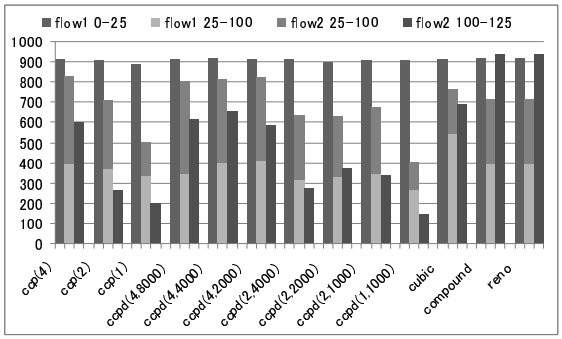


Fig. 7: TCP/TCP throughput - small rtt(20msecs)

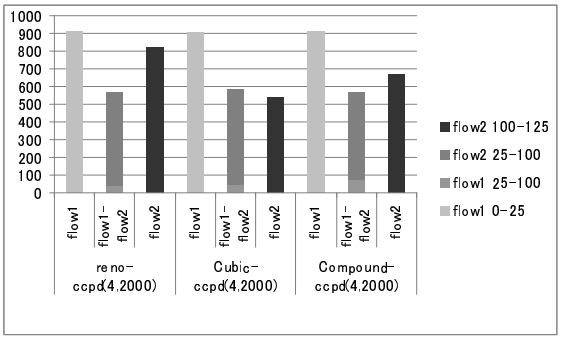


Fig. 9: TCP/CCPD(4,2000) throughput - small rtt(20msecs)

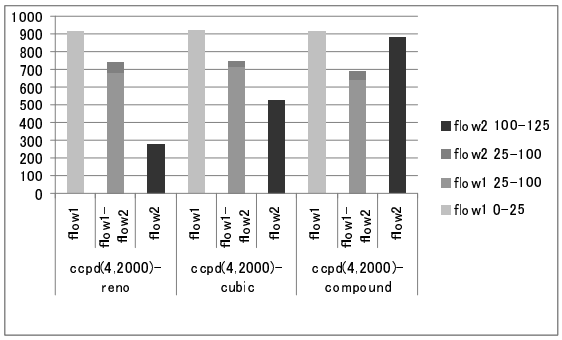


Fig. 8: CCPD(4,2000)/TCP throughput - small rtt(20msecs)

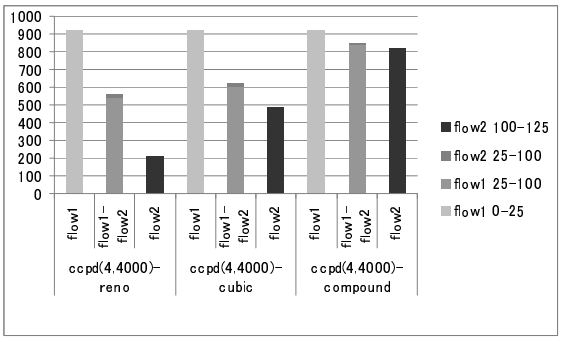


Fig. 10: CCPD(4,4000)/TCP throughput - small rtt(20msecs)

Figures 13 and 14 report throughput performance of CCPD(4,2000) competing with Reno, Cubic, and Compound TCP variants over a large rtt path. Figure 13 shows that Reno, Cubic, and Compound TCP variants deliver poor flow 2 throughput ramp up performance when both flows share path resources. In contrast, Figure 14 shows a much better flow 2 ramp up performance of CCPD(4,2000) for large rtt scenario. Moreover, CCPD(4,2000) is able to further ramp up flow 2 throughput to a highest level among all TCP variants.

Figures 15 and 16 report throughput performance of CCPD(4,4000) competing with Reno, Cubic, and Compound TCP variants over a large rtt path. TCP flow 2 throughput is low, as compared with CCPD(4,4000) flow 1, when both flows share path resources. Fig. 15 shows that Cubic TCP recovers flow 2 throughput the most, whereas Reno flow 2 has negligible throughput. Fig. 16 shows that CCPD(4,4000) flow 2 recovers the most throughput after cross traffic ends.

V. Discussions

Round trip time is used in the calculation of Retransmission Time Out (RTO). In addition, round trip time estimate may be used as an indication of path congestion in various TCP variants, such as TCP Vegas, and TCP CCP and CCPD. In these schemes, a TCP session minimum rtt, rtt_{min}, is computed, and current rtt measurement deviation from this minimum is taken as an indication of path congestion. Some TCP schemes also use an estimate of maximum rtt seen, or rtt_{max}. Care must be taken by these schemes so as to ensure robustness to path condition changes.

Firstly, an early TCP session may compute a rtt^e_{min}, whereas a late TCP session may compute a rtt^l_{min} over a same path, such that $rtt^e_{min} < rtt^l_{min}$. In this case, the early session may perceive less congestion than the late one, even though they share the same path, with the same cross traffic. Hence, an already established session may be biased to higher performance than a newly entrant one. This problem can be mitigated by having the TCP session to "release" some bandwidth once in a while. Judicious $cwnd$ variation hence is encouraged for that purpose. Another issue arises when a TCP path route changes, due to link/router failures in the network, causing path measures to become invalid. Path capacity estimates (TCP CCP and CCPD) need to be updated upon route changes.

VI. Future work

In this paper, we have characterized TCP performance over a high speed wired network scenario via open source experiments for the most widely used TCP variants, i.e., Cubic, Reno, and Compound TCP, as well as our proprietary variants, CCP and CCPD. We have shown the need to tune TCP variant parameters to network scenarios. In addition, we have selected appropriate CCP and CCPD parameters for short and long rtt paths. We are currently investigating fairness issues vis a vis TCP variants path condition estimators, such as rtt estimation for new and already established TCP sessions. We are also investigating how to make estimators more robust to sudden change of path conditions, such as re-routing.

Acknowledgment

Work supported in part by JSPS Grant-in-Aid for Scientific Research KAKENHI B (23300028).

 ISBN: 978-1-61208-204-2

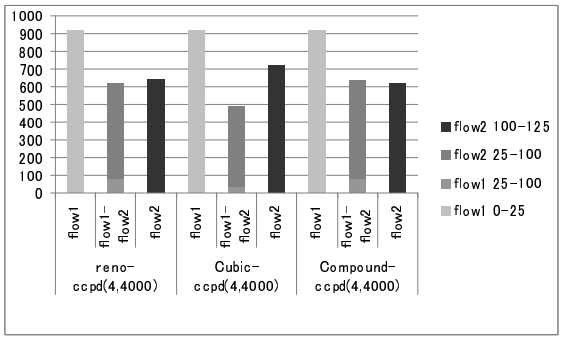


Fig. 11: TCP/CCPD(4,4000) throughput - small rtt(20msecs)

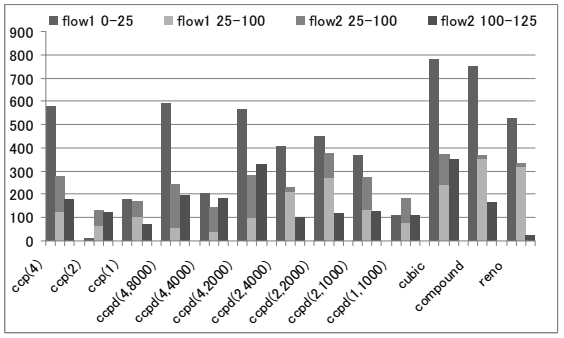


Fig. 12: TCP/TCP throughput - large rtt(200msecs)

REFERENCES

[1] Alaxala Networks Corporation, "High Performance Layer 3 Switches" *http://www.alaxala.com/en/products/index.html*, accessed Apr. 16, 2012.

[2] A. Afanasyev, N. Tilley, P. Reiher, and L. Kleinrock, "Host-to-Host Congestion Control for TCP, " *IEEE Communications Surveys & Tutorials*, Vol. 12, No. 3, pp. 304-342, Third Quarter 2010.

[3] M. Allman, V. Paxson, and W. Stevens, "TCP Congestion Control," *IETF RFC 2581*, April 1999.

[4] M. Alnuem, J. Mellor, and R. Fretwell, "New Algorithm to Control TCP Behavior over Lossy Links, " *IEEE Int. Conference on Advanced Computer Control*, pp. 236-240, Jan 2009.

[5] A. Ahmed, S.M.H. Zaidi, and N. Ahmed, "Performance evaluation of Transmission Control Protocol in mobile ad hoc networks, " *IEEE Int. Networking and Communication Conference*, pp. 13-18, June 2004.

[6] D. Cavendish, K. Kumazoe, M. Tsuru, Y. Oie, and M. Gerla, "Capacity and Congestion Probing: TCP Congestion Avoidance via Path Capacity and Storage Estimation," *Second Int. Conference on Evolving Internet*, September 2010.

[7] D. Cavendish, Hiraku Kuwahara, K. Kumazoe, M. Tsuru, and Y. Oie, "TCP Congestion Avoidance using Proportional plus Derivative Control," *Third Int. Conference on Evolving Internet*, June 2011.

[8] J. Chicco, D. Collange, and A. Blanc, "Simulation Study of TCP Variants," *IEEE Int. Symposium on Computers and Communication*, pp. 50-55, June 2010.

[9] S. Henna,"A Throughput Analysis of TCP Variants in Mobile Wireless Networks," *Third Int. Conference on Next Generation Mobile Applications, Services and Technologies - NGMAST*, pp.279-284, Sept. 2009.

[10] PacketStorm Communications, Inc., "PacketStorm 4XG Network Emulator" *http://www.packetstorm.com/psc/psc.nsf/site/4XG-software*, accessed April 16, 2012.

[11] I. Rhee, L. Xu, and S. Ha, "CUBIC for Fast Long-Distance Networks," *Internet Draft*, draft-rhee-tcpm-ctcp-02, August 20088.

[12] M. Sridharan, K. Tan, D. Bansal, and D. Thaler, "Compound TCP: A New Congestion Control for High-Speed and Long Distance Networks," *Internet Draft*, draft-sridharan-tcpm-ctcp-02, November 20088.

[13] S. Waghmare, A. Parab, P. Nikose, and S.J. Bhosale, "Comparative analysis of different TCP variants in a wireless environment," *IEEE 3rd Int. Conference on Electronics Computer Technology*, Vol.4, p.158-162, April 2011.

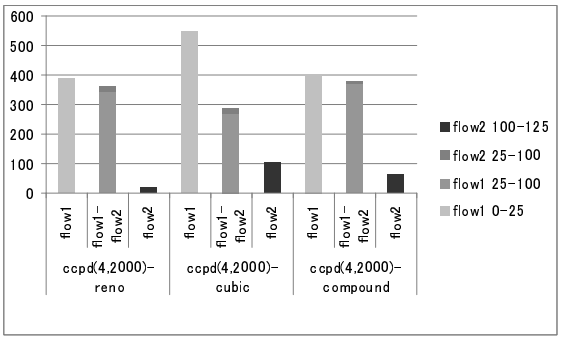


Fig. 13: CCPD(4,2000)/TCP throughput - large rtt(200msecs)

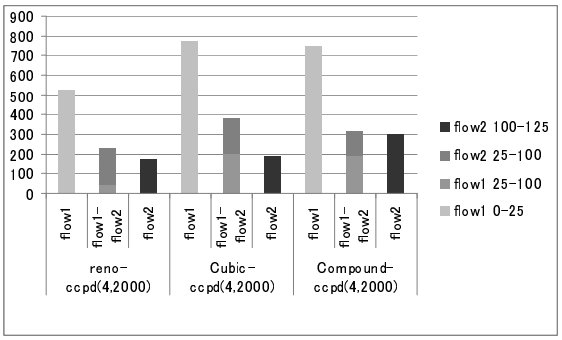


Fig. 14: TCP/CCPD(4,2000) throughput - large rtt(200msecs)

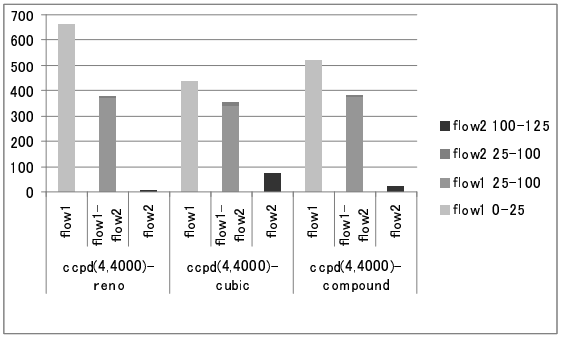


Fig. 15: CCPD(4,4000)/TCP throughput - large rtt(200msecs)

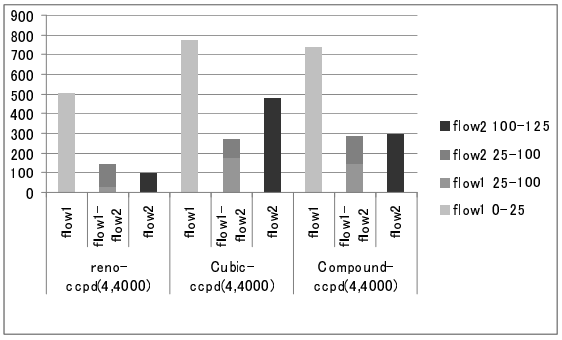


Fig. 16: TCP/CCPD(4,4000) throughput - large rtt(200msecs)

Network Resources Allocation in Content-Aware Networks for Multimedia Applications

Eugen Borcoci
Telecommunication Dept.
University POLITEHNICA of Bucharest
Bucharest, Romania
eugen.borcoci@elcom.pub.ro

Radu Dinel Miruta
Telecommunication Dept.
University POLITEHNICA of Bucharest
Bucharest, Romania
radu.miruta@elcom.pub.ro

Serban Georgica Obreja
Telecommunication Dept.
University POLITEHNICA of Bucharest
Bucharest, Romania
serban.obreja@elcom.pub.ro

***Abstract* — Virtual Content Aware Networks (VCAN) constructed as overlays over IP networks, are currently of high interest in the context of Future Internet multimedia distribution. The VCANs mapping onto real topologies while meeting some QoS properties is still an open issue and constitutes the objective of many studies. This paper continues a previous work which defined the management framework of a complex multi-domain networked media oriented system. Here it is proposed a combined set of algorithms and protocols to perform VCAN mapping on real network infrastructures both for intra and inter-domain, while meeting QoS constraints for multi-domain VCANs.**

Keywords — Content-Aware Networking; Network Aware Applications; Multi-domain; Inter-domain peering; Management; Resource allocation; Future Internet.

I. INTRODUCTION

Many research efforts are spent today to find the best solutions (evolutionary, middle-way or revolutionary) for so called Future Internet (FI), [1-5]. Content orientation of the FI is largely recognized and new solutions towards this make have been proposed, [2][6][7][8], to create virtualized *Content Aware Networks* (VCAN) and *Network Aware Applications* (NAA) on top of the IP level. Novel network nodes (routers) will process and forward the data, based on *content type* recognition or, even more, treating the data objects based on their *name* and not based on *location address*, [6][7]. The paper [6], analyses new solutions based on *Content Oriented Networking* (CON) with decoupling of contents from hosts at networking level. The VCANS can be constructed based on virtualization techniques, agreed to be used to overcome the ossification of the current Internet [3-5].

The European FP7 ICT research project, "Media Ecosystem Deployment Through Ubiquitous Content-Aware Network Environments", ALICANTE, [9-13], adopted the NAA/CAN approach. It targets to define an architecture, and then to fully specify, design and implements a Media Ecosystem, on top of multi-domain IP networks, to offer services for different business actors playing roles of consumers and/or providers. It adopted content-type recognition at network level and light virtualization (VCANs separation in the Data Plane but a single management and control – M&C plane). This approach offers seamless deployment perspectives and tries to avoid the scalability problems (still open research issues) of the full CON approaches.

The ALICANTE business entities/actors belong to Several cooperating environments: *User Environment (UE),* containing the End-Users (EU) terminal; *Service Environment (SE),* containing High Level Service Providers (SP) and Content Providers (CP); *Network Environment (NE),* where a new CAN Provider exists (CANP) to manage and offer Virtual Content Aware Networks - VCANs); traditional Network Providers (NP/ISP) - managing the network at IP level. The "environment", is here a generic grouping of functions cooperating for a common goal.

The CANP offers to the upper layers enhanced VCAN-based connectivity services, unicast and multicast (QoS enabled) over multi-domain, multi-provider IP networks. The novel CAN routers are called *Media-Aware Network Elements (MANE)* to emphasize their additional capabilities: content and context – awareness. The VCAN resources are managed quasi-statically by provisioning and also dynamically by using adaptation procedures for media flows. The management is based on vertical and horizontal Service Level Agreements (SLAs) negotiated and concluded between providers (e.g., SP-CANP). In the Data Plane, content/service description information (metadata) can also be inserted in the media flow packets by the Content Servers and treated appropriately by the intelligent routers of the VCAN.

In [12], [13] the general framework is developed, to manage connectivity services offered by the VCANs to the upper layers. This paper elaborates the mapping of the overlay VCANs (as requested by an SP) onto real network resources in a multi-domain context, while satisfying topological QoS constraints, is a challenging issue and is the main subject of this paper, thus continuing the initial work on VCAN presented in [12][13]. During this mapping the VCAN resources are logically reserved; later when the VCAN installation is requested by the SP, they will be really allocated in routers. Note that the content awareness processing is not directly discussed in this paper, but is specified in [11-13].

 ISBN: 978-1-61208-204-2

Section II presents samples of related work. Section III summarizes the overall ALICANTE architecture and VCAN general Management. Section IV describes the inter-domain peering solution. Section V is the paper core, presenting the proposal of an architecture and a joint algorithm which uses the overlay topology information and combines constrained routing and resource reservation aiming to assure the optimum VCAN virtual links mapping onto network paths. Section VI contains some conclusions and future work outline.

II. RELATED WORK

The fundamental problem for virtual networks is their instantiation and finding an optimal allocation of resources offered by a physical IP Network. In order to solve this NP-hard problem, several heuristics have been proposed in literature [4][5][24].

Our specific objective is to develop management solutions to map the QoS capable VCANs, over several independent network domains, in a scalable way to finally assure efficient transport of real-time and media traffic. The approach must take into account the ALICANTE partially decentralized architecture [9-12] : CAN Managers and Intra-domain Network Resources Managers exist – each of them being aware on the status of their resources. Therefore we should consider also the inter-domain QoS enabled domain peering problem. Basically there are two solutions: find some inter-domain paths (without checking the QoS properties mandatory), or find QoS enabled paths. Any solution applied, after paths finding, a negotiation protocol should be run, [9-11] [18][19][21], between domain managers, to establish inter-domains Service Level Specification (SLS) agreements (SLS is the SLA technical part) containing clauses for QoS guarantees. If no QoS constraints are used during routing, there are significant chances that the SLS negotiation will fail. So, it is a better solution to search for QoS enabled paths, [14][15][18][19].
In [18][19], QoS enhancements for the Border Gateway Protocol (BGP) are proposed to add QoS related information to BGP advertisements between network domains. However, the notion of parallel planes (in our case content aware) at domains level is absent there and all process are running at routing level.

Better fitted to ALICANTE needs are the solutions for inter-domain QoS peering and routing based on the overlay network idea, [14-16]. An overlay network is defined, which first, abstracts each domain with a node, represented by the domain resource manager, or more detailed with several nodes represented by the egress routers from that domain. Protocols are needed to transport QoS and other information between nodes and, based on this information, QoS routing algorithms can choose QoS capable paths. In [20] a Virtual Topology (VT) is defined by a set of virtual links that map the current link state of the domain without showing internal details of the physical network topology.

Related to management signaling for inter-domain, several solutions are examined and compared (cascade, hub, mixed-mode), [18][19][21][22]. However, neither solution considers the content awareness capabilities of the multiple domain infrastructure, nor the virtualization aspects. ALICANTE architecture realizes parallel Internet planes as in [22], but mapped onto VCANs, and additionally achieves cooperation between the network layer and applications and services layers, thus realizing a traffic optimization loop.

The solution adopted in this paper is a combined one, applicable both to inter-domain and intra-domain context: QoS enabled (constrained) routing based on overlay topology, the VCAN virtual links assignment to virtual paths, after admission control check, first at inter-domain level and then negotiation between domain mangers and running similar algorithms at intra-domain level.

III. ALICANTE SYSTEM ARCHITECTURE AND VCAN MANAGEMENT

The general ALICANTE concepts and architecture are defined in [9-11]. Figure 1 shows a mixed, simplified picture, emphasizing the actors and interactions and a multi-domain VCAN.

The network contains several Core Network Domains (CND), belonging to NPs (can be Autonomous Systems - AS) and access networks (AN). The ANs are out of scope of VCANs. The CAN layer M&C is partially distributed: one *CAN Manager* (CANMgr) belonging to CANP exists for each IP domain, doing VCAN planning, provisioning, advertisement, offering, negotiation installation and exploitation. Each domain has an *Intra-domain Network Resource Manager* (Intra-NRM), as the ultimate authority configuring the MANE and other network nodes. The EU terminals are connected to the network through Home Boxes, playing the roles of Residential Gateways. A HB can also act as a CP/SP for other HBs, on behalf of the EUs. The CAN layer cooperates with HB and SE by offering them CAN services.

The VCAN Management framework has been already defined in [12][13]. Here only a short summary is recalled for sake of clarity. A functional block at Service Manager SM@SP, performs all actions needed for VCAN support on behalf of SP (planning, provisioning, negotiation with CANP, VCAN exploitation). The CAN Manager (*CANMgr@CANP)* performs, at the CAN layer, VCAN provisioning and operation. The two entities interact based on the SLA/SLS contract initiated by the SP. The interface implementation for management is based on Simple Object Access Protocol (SOAP)/Web Services.

The main interactions in the Figure 1 are*: SP-CANP(1)*: the SP requests to CANP to provision/ modify/ terminate VCANs while CANP says yes/no; also CANP might advertise existent VCANs to SP; *CANP-CANP(2)* – negotiations are needed to extend a VCAN upon several NP domains; *CANP-NP(3)* : CANP negotiates resources with NP; *Network Interconnection Agreements (NIA) (4)* between the NPs or between NPs and CANPs; (necessary for NP cooperation). After the SP negotiates a desired VCAN with CANP, SP will issue the installation commands to CANP,

 ISBN: 978-1-61208-204-2

which in turn configures, via Intra-NRM (action 4), the MANE functional blocks.

The content awareness (CA) is realized in three ways, [11]:

(i) by concluding a SP - CANP SLA concerning different VCAN construction. The content servers are instructed by the SP to insert some special *Content Aware Transport Information (CATI*) in the data packets. This simplifies the media flow classification and treatment by the MANE; (ii) SLA is concluded, but no CATI is inserted in the data packets (legacy CSs). The MANE applies packet inspection for data flow classification and assignment to VCANs. The flows treatment is still based on VCANs characteristics defined in the SLA; (iii) no SP–CANP SLA exists and no CATI. The flows treatment can still be CA, but conforming to the local policy at CANP and IntraNRM.

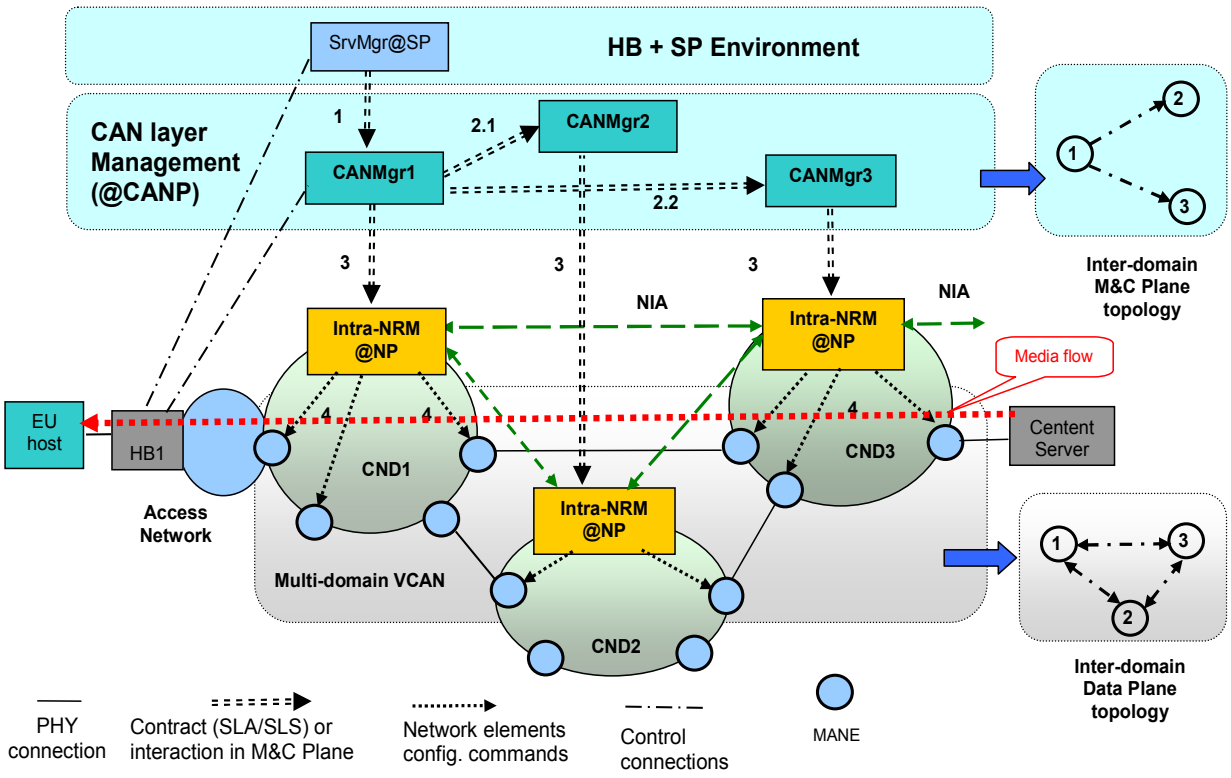


Figure 1 Example of a multi-domain VCAN. Data Plane topology and management interactions

In the CNDs DiffServ and/or MPLS technologies can support splitting the sets of flows in QoS classes (QC), with a mapping between the VCANs and the QCs with several levels of QoS granularities, [18][19]. The QoS behavior of each VCAN (seen as one of the parallel Internet planes) is established by the SP-CANP.

IV. CAN MULTI-DOMAIN PEERING

In a multi-domain context, one should distinguish between two topologies (in terms of how the domains are linked with each others): *Data plane topology* and *M&C topology*. The first can be of any kind (including the domains spanned by a given VCAN- see Figure 1- triangle). The *M&C topology* defines how the CANMgrs associated to CNDs inter-communicate for multi-domain VCANs construction. The VCAN initiating CANMgr has to negotiate with other CAN Managers. There exist two main models: *hub* model and *cascade* model, [19][21][22].

The *hub model* was selected; it has the advantage that initiating CANMgr knows, each VCAN component (network) and its status, but it must also know the inter-domain topology. Given the tiered hierarchy of the Internet, the number of CNDs involved in an E2E chain is not too high (actually is lower than 10, [8]), so, *scalability problem is not so stringent*. Two functional components are needed: (1) inter-domain topology discovery protocol; (2) overlay negotiation protocol for SLA/SLS negotiations between CAN Managers. The *cascade* model, [19][21] is better for a chain of domains topologies than for arbitrary ones.

Figure 1 shows an example of a multi-domain VCAN composed of parts of CND1, 2, 3. This VCAN is constructed in the following way. An inter-domain discovery protocol [11], has informed each CANMgr about the inter-domain graph where each CND is abstracted as a node (the inter-domain links capacities are also learned, supposing that each CANMgr knows its neighborhood). The SP asks for a

 ISBN: 978-1-61208-204-2

VCAN to a CANMgr (Initiator) – see action 1. The SP knew the edge points of this VCAN, i.e., the MANEs IDs where different sets of HB currently are, or they will be connected. The initiator *CANMgr_n* determines all CNDs involved (from the SP information and its inter-domain knowledge) and then negotiates in parallel with all other CAN Managers (actions 2.1, 2.2) to agree and reserve resources for the VCAN. The split of the SLS parameters (if it is the case) should be done at the initiator (e.g., for delay). In a successful scenario, the multi-domain VCAN is agreed and then it will be later instantiated in the network.

Each CND has complete autonomy w.r.t its network resources including network dimensioning, off-line traffic engineering (TE), and also dynamic routing. The CANMgr and Intra-NRM have together an abstract view of its CND and output links towards neighbor domains in a form of a set of virtual links (called *Traffic Trunks*). A set of such links can belong to a given QoS class. A multiple domain VCANs should also belong to some QoS class and therefore inter-domain QoS aware routing information is necessary in order to increase the chances of successful SLS establishment, between CANMgrs. The multi-domain VCANs deployment needs knowledge on a virtual multi-domain topology. Acquisition of this information is performed by an inter-domain protocol, which offers to CANMgrs an *Overlay Network Topology Discovery Service* (ONTS) similar to that described in [20]. Therefore in the following sections we suppose that this information is known by each CANMgr. Details on the protocol performing the ONTS for the benefit of given CAN managers are out of scope for this paper.

V. VCAN MAPPING AND RESOURCE RESERVATION

A. CAN Provisioning at SP

The functional block at SP for this is the CAN Provisioning Manager at SM@SP. It performs the SP-CANP SLS processing - subscription (unicast/multicast mode) in order to assure the CAN transport infrastructure for the SP. After some VCAN planning the SP requests to the CAN Manager associated with its home domain, to subscribe for a new VCAN. It negotiates the subscription and concludes an SLS denoted by: *SP-CAN_SLS-uni_sub* for unicast, or *SP-CAN_SLS-mc_sub for* multicast. The results of the contract are stored in the *CAN repository*. Note that CAN subscription only means a logical resource reservation at the CAN layer, not real resource allocation and network node configuration. The CAN subscription action may or may not be successful, depending on the amount of resources demanded by the SP and the available resources in the network. Note that at its turn the CAN Manager has to negotiate the CAN subscription with Intra-NRM, and overbooking is an option, depending on the SP policy.

B. CAN Negotiation

A negotiation protocol (SP-CANP-SLS-P) has been developed in ALICANTE (not detailed here) to support the negotiation process between several pairs of managers like *CANProvMng@SM* as a client and *CAN Manager* as a server. The main usage of this protocol is for establishing *SLS* contracts, but it should have all the necessary properties of a general negotiation protocol, and could be adapted/used to serve CAN invocation. The SP-CANP-SLS-P supports one of several negotiation actions: establishment/ modifications/ termination of SLS contracts.

C. Inter-domain CAN Planning and Resource Management

The *CAN Planning* first task is to perform the inter-domain resource management and then prepare the intra-domain similar actions. QoS capable VCANs are envisaged here. The idea of this paper is to combine the constrained QoS routing with admission control and VCAN mapping, on two levels: inter-domain and then intra-domain. This split solves partially the scalability and also administrative problems of a multi-domain environment. The planning objectives are: using the ONT information and SP request to determine the domains participating to a given VCAN requested by SP; apply a constrained routing algorithm admission control and VCAN mapping; based on routing information the SLS splitting between domains is computed.

To make the functional steps more readable, consider the Figure 2 example, containing several network domains CND1, CND2, … CND8. SP has requested a VCAN-0 construction, whose parameters are embedded in an SLS request. The CND1 is supposed to have its CAN Manager as initiator of the VCAN. The required VCAN should assure guaranteed services in a given QoS class, services, i.e. guaranteed traffic trunks (TTs) starting from the Content Servers CS1, CS2 up to different client HBs, denoted as HBc1…HBc7. SP requests the VCAN-0 and a delivers a Traffic Matrix (TM) associated to it, containing (at minimum) the requested bandwidth of the TTs.

The following actions are performed:

1. SP issues a VCAN-0 request to initiator CANMgr1 (at CND1) i.e. an SLS request (topology, traffic matrix, QoS guarantees, …etc.).
2. The CANMgr1 obtains from ONTS the inter-domain level ONT (topology graph, inter-domain link capacities, etc.). The ONT is sufficiently rich to cover the required VCAN.
3. The CANMgr1 determines the involved domains in VCAN-0 by using the border ingress-egress point's knowledge (actually MANE addresses) indicated in the SLS parameters (Figure 2.a).
4. The initiator CANMgr determines a contiguous inter-domain connectivity graph (each CND is abstracted as a node) resulting in an extended VCAN-1 (in Figure 2.a this new VCAN is represented by dotted line). In VCAN-1 graph, some new additional transit core network domains need be included, e.g., CND4, CND5 (it is supposed in the most simple version that these new core network domains added are also VCAN capable). Therefore a contiguous new VCAN-1 is defined. Optimisation techniques can be applied in this phase.
5. The initiator CAN Manager should make the first split the initial SLS among core network domains. This

means to produce the set of SLS parameters valid to be requested to each individual CND. The *inputs* are: ONT graph, abstracting each CND by a node; QoS characteristics of the inter-domain links (bandwidth, delay); Traffic Matrix (and other QoS information) of the SLS proposed by SP. The *ouputs* are the Traffic matrices for each CND composing the VCAN.

To do this, the CANMgr1 will run a constrained routing algorithm. A combined metric is proposed here for a link, similar to [14], considering the bandwidth request and the bandwidth available, targeting to choose the widest path.

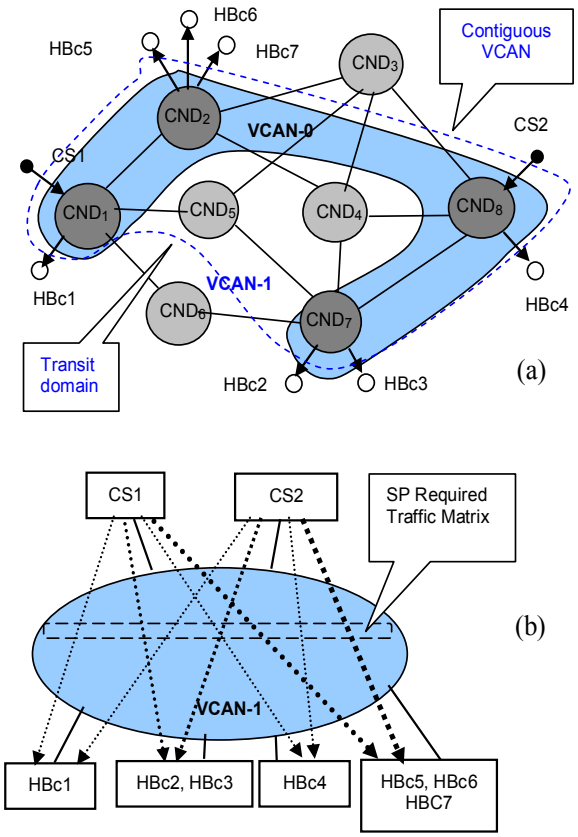


Figure 2. Example of a multi-domain requested VCAN (VCAN-0 is requested by SP).

Note that the final solution will also contain delay-constrained routing and introduce delay in the metric. This is possible, given that ALICANTE system has a powerful monitoring plane capable to perform delay measurements and compute averages both intra and inter-domain. In the example below we only consider bandwidth only in the metric defined.

The cost of a inter-domain link (i,j) in the ONT can be $C(i,j) = Breq/Bij = Breq/Bavail$, where Bij is the available bandwidth on this link and *Breq* is the bandwidth requested for that link. Another useful interpretation of this ratio is as link utilization factor ; that is we the alternative notations will be used: $C(i,j) = U_{link\_ij}$. The metric should be ≤1, this representing the bandwidth constraint applied to the algorithm. The metric is additive, so one can apply modified Dijkstra algorithm to compute the *Shortest Path Trees (SPT)* for each ingress node where the traffic flows will enter. Given that *Breq* is different for each branch of the tree the additive metric used for SPT computation is 1/Bij. The mapping is to be done jointly with the routing process.

The summary pseudo-code of the combined routing, admission control (AC) and mapping algorithm (not yet optimized) is described below. The notation ;/text after pseudo-code lines represents explanatory comments.

*1. Split the requested TM in several trees, one for each ingress node (I1, I2, ...In);/*See the Figure 2.b having two trees

2. On the current graph, repeat for 1 to n:

*{2.1. Compute the DJ_SPT (root_I1) where DJ means Dijkstra algorithm;/*Routing

*2.2. Select the TM branches that can be satisfied (i.e., Bij > Breq for that direction);/*Mapping and AC

2.3 Reserve capacities for these branches by subtracting the respective capacities from the graph;/ thus obtaining a reduced graph

2.4. *Compute the overall utilization for each path reserved as* $U_{path} = Sum_{links}$ *(Breq/Bavail) * NHF(path);*

*2.4 List the unsatisfied branches; /*it may happen to not be able to satisfy all requests of TM

}

3. Aggregate the results for all inputs, for satisfied and not satisfied branches and compute the overall VCAN utilization by summing over all paths mapped onto the real graph;

Notes:

1.The cost of a full path could be *Sum (link costs) * NHF(path)* where Number of Hops Factor NHF(path) is a weight factor approximately proportional with the number of CNDs crossed by this path. This cost will optimize the solution by reducing the number of transited domains

2.AS shown above, the ratio *Breq/Bavail* computed on a link can be interpreted as the link utilization factor $U_{link} = Breq/Bavail$ of that link. Summing for all links we can get the path utilization. Summing the utilizations for all paths one gets the overall network utilization U_{VCAN} for that VCAN.

3. We assume that only bandwidth is considered in the above metric and the procedure is: select the widest path ; however this will usually also assure the smallest transfer delay, [14].

4. In the simplest form the algorithm keeps only the best path satisfying the constraint. In an advanced version, several inter-domain paths satisfying the constraint may be retained. Knowledge of the path allows that the domains involved in this TT are determined. This solution could be useful for load balancing and it will be analysed in a future work.

5. If priorities are assigned to the TTS in the traffic matrix by SP, then these will be considered in the order of computations done in Step 2.

 ISBN: 978-1-61208-204-2

D. VCAN Mapping Optimisation and Scalability

The optimal mapping of overlay virtual networks onto real network substrate resources is shown to be a NP-hard problem, [24]. We try here to find a pragmatic solution, based on the fact VCAN construction actions have no strong real time constraints for computations. The solicitation of a CANP to construct VCANs is rather not frequent (intervals of days, weeks, etc.).

Normally the NP would like that for a given traffic matrix associated to a VCAN, the best mapping would be that one having the least overall utilization. Therefore a straightforward optimization method is to compute the step 2 of the algorithm several times, for other order of inputs given by the bijective function f(I1, ..In) -> {Ik1, Ik2, ..Ikn} which creates actually permutations of the set {I1, ..In}. The function is random. The best allocation is that one having the least overall utilization. Note that for large n, the solution is not scalable (we would need n!) computations. Therefore in practical cases one can stop repetitions of the step 2 after some computations if the overall utilization fulfill some enough good thresholds fixed by local CANP policy.

Other optimization procedure is possible if the CANP policy looks for an optimal mapping that leaves the greatest amount of resources available. Then the same algorithm can be applied, while the metric for a link will be not *U* but *1/(1-U)*.

Scalability of the solution is assured by: splitting the problem hierarchically in inter-domain and intra-domain similar problems; grouping the requests in sets of trees and avoiding of individual mapping; exploiting Internet tiered hierarchy in order to minimize the number of transit domains in a VCAN.

E. Numerical Example

Figure 3 presents a numerical example of inter-domain path computation, in order to finally determine the splitting of the overall SLS into parameters sets, each one associated to a different domain. The links are denoted with values representing the available bandwidth. Note that, depending on the policies, these bandwidth values can be used for any QoS class, based on FIFO policy of resolving the SLS requests, or might be assigned offline for given planned QoS classes.

The paths utilizations in the Figure 3 example are:

U(path_1) = (1/5 + 1/3 + 1/4) *4 = 0.78*4 = 3.12

U(path_2) = (1/2 + 1/6 + 1/3) *4 = 1.0 *4 = 4,

therefore the *path_1* is better, given that it has a lower path utilization factor.

Given the resource reservation assured by provisioning in the M&C plane (accompanied by policing in the data plane), the value of the bandwidth already booked is subtracted from the available one, on each link, before analysing other TT paths. The SLS splitting results of this computation step are:

TT(CND1) : Input_CS1---> Output_CND2, Breq= 1;
TT(CND2) : Input_CND1---> Output_CND4, Breq= 1;
TT(CND4) : Input_CND2---> Output_CND8, Breq= 1;
TT(CND8) : Input_CND4---> Output_HBc4, Breq= 1;

After splitting in this way the overall SLS, a set of parameters are available for each domain. Then, separate negotiations can be done by CANMgr1 with each other CAN Manager involved in the VCAN for that SLS.

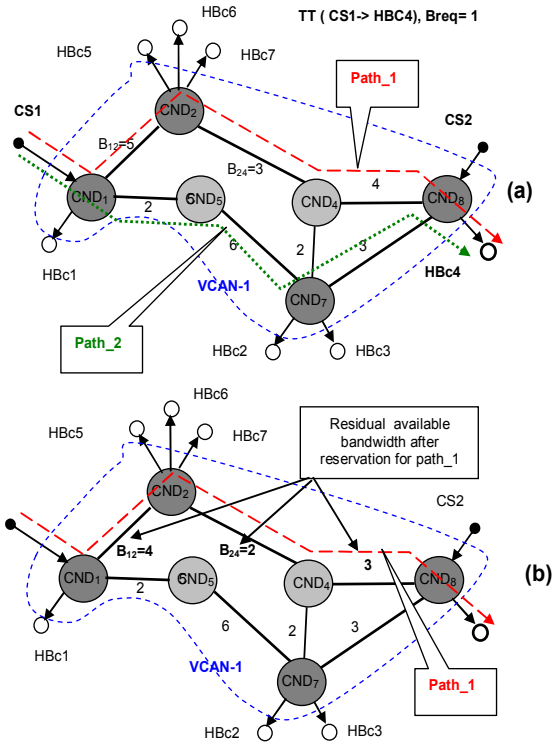


Figure 3. Connectivity graph of the extended VCAN (requested by SP SLS domains and the transit ones)

a. Inter-domain path computation (constrained routing) and implicit inter-domain resource reservation

b. Adjustment of the ONT graph after selecting *path_1* as good.

The algorithm has been preliminary implemented using Visual Studio C++ Express Edition as development environment. The hardware platform was equipped with Intel(R) Core(TM)2 CPU T5600@1.83GHz processor and 2,00 GB installed memory (RAM) on a 32-bit OS. The preliminary results have shown computation times between 10-100 ms for network graphs having 5-80 nodes. It was also observed a dependency between the number of solved requests and the number of edges in a graph with the same number of vertices. Further results will be reported in a future work.

F. Intra-domain CAN Planning and Resource Management

In ALICANTE a two level hierarchy has been selected for VCAN mapping: inter and intra-domain. Essentially, to map a VCAN portion onto a given CND network graph for the intra-domain case, *the same algorithm can be applied by the CAN Manager in cooperation with Intra-NRM.* The

 ISBN: 978-1-61208-204-2

knowledge of the intra-domain graph is obtained by Intra_NRM in the link-state style (similar to Open Shortest Path protocol- OSPF). The details will be studied in a future work. The actual placement of functions inside CAN Manager or Intra-NRM depends on policies and degree of trust between these two entities. Actual locations of mapping functions depends on relationship between CANMgr and Intra-NRM with respect to: (1) the style for Intra-NRM to upload information to CANMgr about its available resources: on demand (OD) or in proactive (P) style (at Intra-NRM initiative); (2) amount and depth of information uploaded by Intra-NRM on network resources (graph, capacities, etc.). Note that for every variant, and depending on monitoring information at network level the Resource Availability Matrix (RAM) uploaded to the CANMgr can be adjusted by Intra-NRM to improve the traffic engineering performances.

VI. CONCLUSIONS

This work proposed the architecture and a combined set of algorithms and protocols to manage network resources, in order to solve the mapping of a Virtual Content Aware Network overlay plane, onto network infrastructure resources, while respecting the QoS requirements issued by the Service Provider which is exploiting VCANs. The inter-domain part of the problem has been treated in more details, by combining an overlay topology approach with an inter-domain constrained routing and admission control. Scalability and optimization aspects have been discussed. Note that the solution discussed is currently in the phase of detailed design, evaluation and implementation inside the FP7 ALICANTE project. Consequently in the near future, complete evaluation results both formal and experimental of this solution will be published.

Acknowledgments

This work was supported partially by the EC in the context of the ALICANTE project (FP7-ICT-248652) and partially by the projects POSDRU/89/1.5/S/62557 together with POSDRU/88/1.5/S/61178.

REFERENCES

[1] J. Schönwälder, M. Fouquet, G .Dreo Rodosek, and I.C Hochstatter, "Future Internet = Content + Services + Management", IEEE Communications Magazine, vol. 47, no. 7, Jul. 2009, pp. 27-33.

[2] C. Baladrón, "User-Centric Future Internet and Telecommunication Services", in: G. Tselentis, et. al. (eds.), Towards the Future Internet, IOS Press, 2009, pp. 217-226.

[3] J. Turner and D. Taylor, "Diversifying the Internet," Proc. GLOBECOM '05, vol. 2, St. Louis, USA, Nov./Dec. 2005, pp. 760-765.

[4] T. Anderson, L. Peterson, S. Shenker, and J. Turner, "Overcoming the Internet Impasse through Virtualization", Computer, vol. 38, no. 4, Apr. 2005, pp. 34–41.

[5] 4WARD, "A clean-slate approach for Future Internet", http://www.4ward-project.eu/ (last access May 2012).

[6] J. Choi, J. Han, E. Cho, T. Kwon, and Y. Choi, A Survey on Content-Oriented Networking for Efficient Content Delivery, IEEE Communications Magazine, March 2011.

[7] V. Jacobson et al., "Networking Named Content," CoNEXT '09, New York, NY, 2009, pp. 1–12.

[8] W.K. Chai, et.al., CURLING: Content-Ubiquitous Resolution and Delivery Infrastructure for Next-Generation Services , IEEE Communications Magazine, March 2011.

[9] FP7 ICT project, "MediA Ecosystem Deployment Through Ubiquitous Content-Aware Network Environments", ALICANTE, No248652, http://www.ict-alicante.eu/ (last access May 2012)

[10] E. Borcoci, D. Negru, and C. Timmerer, "A Novel Architecture for Multimedia Distribution based on Content-Aware Networking" Proc. of. CTRQ 2010, Athens, June 2010, pp. 162-168.

[11] ALICANTE, Deliverable D2.1, ALICANTE Overall System and Components Definition and Specifications, http://www.ict-alicante.eu, Sept. 2011.

[12] E. Borcoci, M. Stanciu, D. Niculescu, D.Negru, G. Xilouris, "Connectivity Services Management in Multi-domain Content-Aware Networks for Multimedia Applications " , Proc. of. INTERNET 2011, Luxembourg, June 2011.

[13] E. Borcoci, and R. Iorga, "A Management Architecture for a Multi-domain Content-Aware Network" TEMU 2010, July 2010, Crete.

[14] Zhi Li, P. Mohapatra, "QRON: QoS-Aware Routing in Overlay Networks", IEEE Journal on Selected Areas in Communications, VOL. 22, NO. 1, January 2004, pp.29-39.

[15] Z. Wang, J. Crowcroft, "Quality-of-service routing for supporting multimedia applications", IEEE Journal on Selected Areas in Communications, vol. 14, no. 7, pp. 1228—1234, 1996.

[16] J. Galán-Jiménez and A. Gazo-Cervero, "Overview and Challenges of Overlay Networks", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.1, Feb 2011, DOI : 10.5121/ijcses.2011.2102 19

[17] Z. Li, P. Mohapatra, and C. Chuah, Virtual Multi-Homing: On the Feasibility of Combining Overlay Routing with BGP Routing, University of California at DavisTechnical Report: CSE-2005-2, 2005.

[18] P. Levis, M. Boucadair, P. Morrand, and P. Trimitzios, "The Meta-QoS-Class Concept: a Step Towards Global QoS Interdomain Services", Proc. of IEEE SoftCOM, Oct. 2004.

[19] M.P. Howarth, et. al., "Provisioning for Interdomain Quality of Service: the MESCAL Approach", IEEE Communications Magazine, June 2005, pp. 129-137.

[20] L. FabioVerdi, and F. Magalhaes "Using Virtualization to Provide Interdomain QoS-enabled Routing", Journal of Networks, April 2007, pp. 23-32.

[21] ENTHRONE, End-to-End QoS through Integrated Management of Content, Networks and Terminals, FP6 project, www.ist-enthrone.org/ (last access May 2012).

[22] M. Boucadair, et al., "A Framework for End-to-End Service Differentiation: Network Planes and Parallel Internets", IEEE Communications Magazine, Sept. 2007, pp. 134-143.

[23] Z. Wang, J. Crowcroft, "Quality-of-service routing for supporting multimedia applications", IEEE Journal on Selected Areas in Communications, vol. 14, no. 7, pp. 1228—1234, 1996.

[24] A. Haider, Richard Potter and A. Nakao, "Challenges in Resource Allocation in Network Virtualization", 20th ITC Specialist Seminar, 18.-20. May 2009, Hoi An, Vietnam, http://www.itcspecialistseminar.com/paper/itcss09Haider.pdf.

 ISBN: 978-1-61208-204-2

The Super-Browser: A new Paradigm for Web Applications

Mark Wallis, Frans Henskens, Michael Hannaford
Distributed Computing Research Group
University of Newcastle
Newcastle, Australia
Email: mark.wallis@uon.edu.au, frans.henskens@newcastle.edu.au, michael.hannaford@newcastle.edu.au

***Abstract*—The modern web browser performs a multitude of tasks, which were never contemplated in its original design. This work investigates the roles and responsibilities of the various components that comprise the web browser, and a traditional web application. We review the web browser's role in the greater architecture and propose that a "Super Browser" concept need not mean greater responsibilities for the web browser application. Instead, the solution described in this work introduces a distributed approach that is capable of executing applications composed of distinct components. The paper presents an implementation of this concept, and a comparison of this approach with a traditional web application framework.**

***Keywords*-web browser; cloud; personal data; architecture.**

I. INTRODUCTION

Web Browsers were traditionally designed to render static content sourced from remote web servers. Textual content and page format were provided as static HTML and selected multimedia types were then rendered via subsequent requests to the server. As the World Wide Web has evolved, so have the web browsers. Web Browsers today support features such as dynamic content rendering and the execution of pluggable code modules. These features have been gradually added as requirements have arisen, and were never part of the original specification of tasks a web browser was required to perform. As such, the stability and security of web browsers has been brought into question [1]. The latest attempts to address these issues have seen introduction of further features such as HTML5 [2] and execution sandboxing [3]. Simultaneously, web applications have also evolved. Various software development models now exist for the development of web applications and the increased use of Cloud Computing [4], [5] has introduced new concepts and new challenges [6].

The system presented in this work introduces a new way of designing and developing web applications. The role of the web browser is reduced to its originally intended role, that of a content renderer. Web Applications are presented as a set of inter-related components. Components may execute anywhere within the user's environment, and may be specifically tasked with such roles as content generation, data storage, and background processing. A work-in-progress implementation of this design is presented and functionally compared to existing solutions. Metrics are presented showing that this solution has performance that is comparable to existing designs. Finally, we present a summary of future work in this area.

II. PROBLEM DESCRIPTION

There is no doubt that over the past few years, web browsers have had more than their share of performance and security related issues [1]. As the user interface requirements of web applications evolved, the trend has been to push more and more features into the web browser. An alternate design approach would be to revert to traditional thick-applications hosted at the client (an appropriate way, perhaps, of describing the current 'fattening' browsers?), with the client application using network messages to interact with remote databases. It seems clear, however, that web applications do provide many advantages over client-hosted thick applications, for example, ease of deployment and centralised management. During our review of the current technologies it became apparent that each design methodology had its own positives and negatives:

1) The web application approach provides developers with positives in the areas of ease of deployment, centralised management, and standards-based development. On the negative side, web browsers are not consistent in the implementation of the 'standards', so developers are required to consider each specific web browser, making sure that the end product handles specific quirks of the browser implementations and versions. Additionally, the implementation of web applications with fully dynamic user interfaces including high-quality video and user interaction are often problematic, relying on closed-sourced web browser plugins such as Adobe Flash [7] and Microsoft Silverlight [8]. On the positive side, web application technology makes it easier to develop a program that can execute across disparate processor/operating system combinations without having to compile specifically for each environment.
2) Thick applications provide a solid means of implementing tasks (that, incidentally, have proven to require ever increasing client processing capabilities),

 ISBN: 978-1-61208-204-2

but are limited in their utilisation of distributed technology. For example, the distributed deployment scenario in which each user has their own locally installed instance of each application causes problems when it comes to patching, and deploying software updates. There are also limitations when it comes to developing an application that can execute on multiple different platforms, with compilation of a specific binary required for each platform. While languages such as Java have addressed this issue through the use of common byte-code, it locks the developer into only being able to support a single language.

3) The ”application store” concept is a newly emerging architecture that attempts to blend the ease of deployment of web applications with the stability and feature set of thick applications. Application stores provide distribution, and in some cases, patching functionality without limiting execution to within a restricted sandbox, such as the web browser.

It has become clear during this review that the ability to blend the above approaches would be beneficial to both the software developer and the end user. The design presented in the remainder of this paper provides a component-based approach to generation of an environment that takes the best features from the above architectures.

III. System Design

By using a component-based system architecture we can address many of the concerns raised in the preceding section. The design of this system can be viewed from four perspectives: component execution, component communication, user interface, and data storage.

A. Component Execution

A component-based architecture allows a developer to design and build an application using multiple, distinct, independently executing components. With the support of an appropriate runtime environment, these components can be implemented in different programming languages, and can execute in a distributed fashion with components being hosted, perhaps, by different hardware/operating system platforms. This architecture builds on that used for existing web service [9], [10] approaches, in which a web application makes use of a set of services to perform a particular task. The system we describe in this paper extends this concept to present the entire web application as an orchestrated set of components.

Components may be specified as being of the following kinds:

- Execution components present only an interface, which may be called (executed) by other components. They are generally used for processing tasks (such as encryption), and background service tasks (such as external notifications). These components execute within a runtime environment and may be physically deployed across a range of locations such as on a user’s local machine, on a specific server, or in a Cloud Computing environment.
- User interface components integrate with a web browser to generate an HTML5 [2], [11] compatible interface to the user. This provides realisation of the ”super browser” concept without the overhead (and browser ’fattening’) of code execution within the web browser itself. User interface components execute in a runtime environment that is process-separate to the web browser process. Communication between the web browser and the user interface component is performed through a strict interface, implemented in our pilot system as a set of JavaScript functions within the web browser and call-back functions in the user interface component. Security is ensured through process separation and monitors, while stability is addressed by ensuring all calls between the user interface component and the HTML realisation of the interface in the web browser are executed through well defined functions, as opposed to Domain Object Model (DOM) [12] manipulation.
- Data Storage components are similar to execution components, in that they present a callable interface, but in addition they are backed by persistent storage. The interface exposed by these components is tightly coupled to the data object(s) being persisted. Data storage components implement specific data objects, but they may share a common persistence model between them, such as a relational or NoSQL database.
- Finally, bootstrapping components provide an entry point for application orchestration. They are responsible for defining which other components are required to execute an application, and for requesting instantiation of those components. Bootstrapping components are registered in the ”application directory”, so that users can view which applications are being presented by the system.

A specific application many consist of multiple instances of each of the above kinds of component. Each component may execute within a separate execution environment, but logical groupings will be evident in most designs. For example, user interface components would typically execute on the same host as the web browser. Data storage components would often be grouped together, and execute on the same machine that hosts the related data store. It is the responsibility of the component runtime environment to select the appropriate location of execution for each component.

Figure 1 depicts the high-level system design. Component 1 (C1) is a data storage component. C2 is a user interface component and C3/C4 are execution components. The bot-

 ISBN: 978-1-61208-204-2

tom half of the figure depicts a deployment scenario of these components running in a distributed fashion across various environments, including a mobile device, a server farm and a Cloud Computing environment.

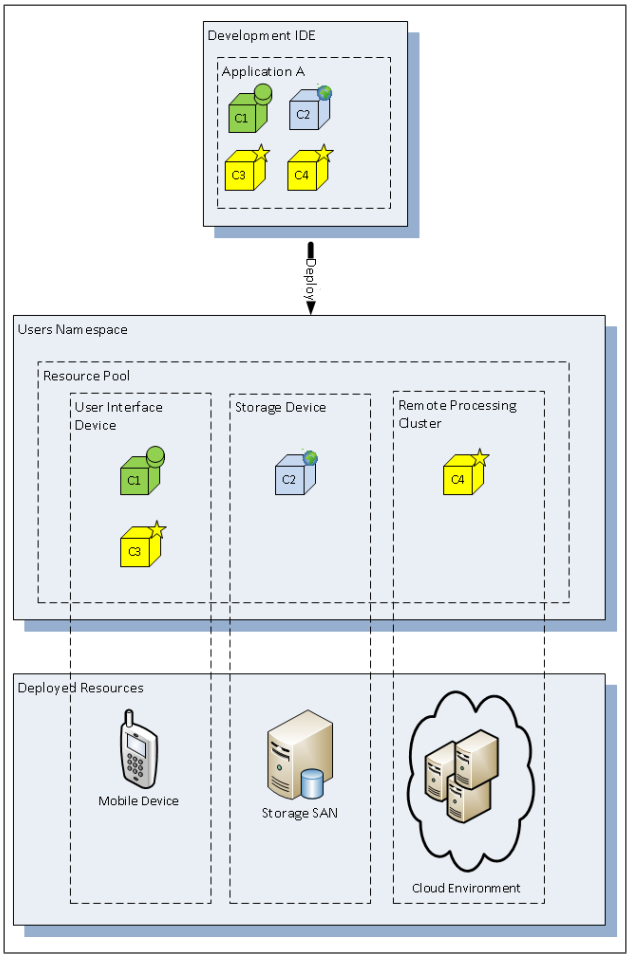


Figure 1. Distributed Component Model

B. Component Communication

Once components are instantiated across various environments, they need the ability to communicate in some fashion. Existing SOA-style architectures rely on each component establishing point-to-point channels for message passing, which provides the means for inter-component communication. While effective in dynamically orchestrated environments, the use of point-to-point channels does not typically scale well. Solutions such as Enterprise-Service-Bus architectures [13] look to address this problem by providing a common communication backbone for inter-component communication, but these buses also do not scale to Internet-wide component execution, as they typically rely on a single (non-global) bus instance. Any inter-bus communication is generally statically configured.

The bus architecture implemented in our design provides a massively distributed channel, with which multiple users can pass messages between components via the same bus, while retaining security and privacy through use of namespace techniques. Each machine that executes/hosts a component has its own local instance of the communication bus. Each bus instance is able to locate and pass messages to other buses using a logically centralised repository of end points. Each user in the environment has their own local endpoint sub-repository, which provides a way of locating specific instances of components.

The communication bus takes care of all inter-component message passing. Components are only required to correctly address and pass messages back up to the hypervisor provided by the runtime environment. Each component is only able to address components within its own application namespace, or components that have been marked as public in the component directory. The communication backbone takes care of resolving these requests to specific instances and locating the specific bus that has local addressing to the addressed component.

C. User Interface

Dynamic user interfaces in traditional web applications rely on Javascript code executing within the web browser runtime, which is capable of directly accessing and modifying the interface via the DOM. Each web browser's implementation of the DOM is known to have its own specific variations from the official specification, and as such this method of building a user interface is common seen as unstable [14].

The user interface component in our proposed design separates code execution from the web browser itself. This separation limits the web browser to simply providing a basic shim that can alter specific DOM elements. Full DOM access is not provided to the executable code, limiting the scope of potential issues caused by non-standard DOMs. The interaction between user interface components and the HTML realisation of the interface within the web browser is implemented via a strictly defined interaction interface. The actual rendering of the HTML5 content is performed by pre-existing rendering engines. This approach removes the need for complicated plugin and closed-sourced components, which can affect the stability of the web browser process.

D. Data Storage

Data Storage in the current generation of web applications is the responsibility of the web application itself. This introduces problems such as data duplication, data freshness, and data ownership [15]. The design for data persistence in our new system is tied closely to that developed in our previous research [16]. Accordingly this new system pushes the responsibility for data storage on to the end user. Data

 ISBN: 978-1-61208-204-2

Storage components will exist for each data object within an application, but the actual persistence framework will be managed by the end users, rather than by web service providers. This ensures that applications are provided a stable interface to data objects, without needing to take actual responsibility for the storage mechanism itself. Data storage components will often execute on servers, or in cloud environments, as examples of locations from which end users are able to procure storage services as required.

Figure 2 shows at a high level how the distributed data storage system works in a Web 2.0 scenario. This proven [16] approach has the data owner publishing their data to the DSS - Data Storage Service. Web Applications subscribe to this information using a publish/subscribe algorithm. Users of the Web Application access both the application itself (for HTML/framework/etc) and the DSS (for direct access to stored data). The user access to the DSS occurs using a SAML-based secure handoff technique and is key in providing a solution that performs in a way that is comparable to existing technologies.

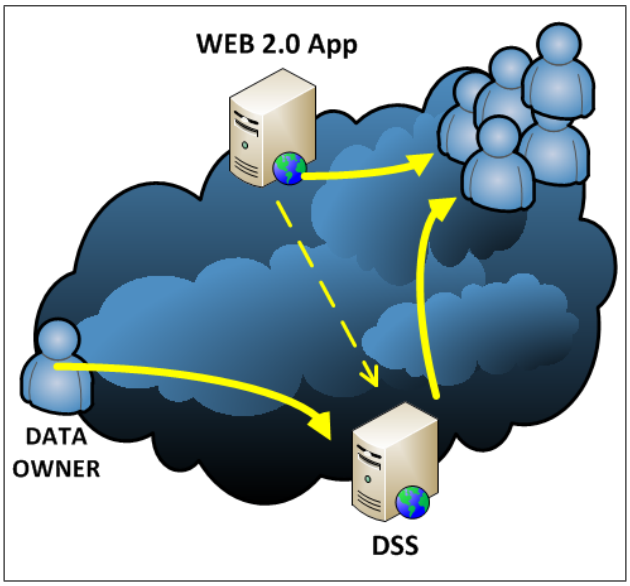


Figure 2. DSS

IV. Implementation

The authors have completed a pilot implementation of the system architecture presented in this paper. The initial deployment provides Java language support for all component types, though the communication channel is not limited to communicating only with components executing within a Java Virtual Machine. Applications can be orchestrated from the bootstrap component, and the components are instantiated in a distributed manner. Runtime support exists for the following environments:

- Microsoft Windows.
- Ubuntu Linux.
- Amazon EC2 Cloud.

User interface support is currently implemented using Gecko, the rendering engine from Mozilla Firefox [17]. The interaction between user interface components and the HTML realisation of the interface is currently implemented through the use of a TCP link with a Firefox web browser plugin. Ultimately, implementation of the rendering engine will be completely split from the traditional web browser process and wrapped in a thinner shim, thus removing much of the unnecessary plugin and sandboxing features that are made redundant by this solution. The component execution environment is implemented within a Java Application Server (Glassfish [18]) and the component communication is realised through the user of a customised Enterprise Service Bus (Glassfish ESB).

V. Evaluation

A functional evaluation has been performed of this solution in comparison to Web 2.0 technologies. Specific benefits have been identified in the following areas.

A. Application Stability

Current web technologies force the developer to implement dynamic user interface actions within complex Javascript or closed-source web browser plugins. The proposed system provides a complete runtime environment (which had historically been limited to thick applications) to the user interface component of the application. Interaction is tightly controlled via callbacks and stub functions. No direct DOM access is provided, which enforces a strict implementation strategy and good programming techniques on the developer. It also reduces overall bloat of the web browser process, and brings stability of the solution through distribution of execution. Each component implements the concept of information hiding [19] which is a proven benefit of component-based software engineering. The internal structure of the browser is hidden away from component code, while in comparison, malicious or unstable Javascript has complete access to the user interface implemented through the DOM.

B. Data Storage

The features provided by the distributed data storage model ensure that users are responsible for their own data storage. Web applications still retain full access to the data they require for execution, but this access is facilitated by remote calls to data storage components, as opposed to direct access to large silos of local storage. The issues of data freshness, data duplication, and data ownership are therefore well addressed by this model, while they remain a key issue with traditional web applications [20].

 ISBN: 978-1-61208-204-2

C. Resource utilisation

A key issue with the increased uptake of web applications is that local resources are becoming highly under-utilised. Local CPUs and data storage are only used to facilitate execution of the web browser process, while the majority of the work is performed by the server(s) hosting the web application. In comparison, the presented system performs execution in a way that allows sharing of load between any resources that a user has rights to use. A specific application may have components executing on the local machine, on a server, or in the cloud, all at the same time, in a distributed and transparent manner.

D. Transaction Support

Transaction managers in current web applications are limited to visibility of tasks executing within the web application itself. For example, if a user closes their web browser mid-transaction then often that transaction is left hanging to time-out. By moving the orchestration of the user interface out of the web browser into a specific user interface component, it becomes possible to track tasks within a transaction all the way from the user interface to the data storage system. This allows software developers to create a transaction that may involve data persistence tasks, calculation tasks, and user interaction tasks, all in the one atomic action and not wholly dependent on continued execution of the interface.

E. Cloud Computing

The proposed design also promotes extended use of Cloud Computing concepts. Currently, for a web application to execute within the cloud it is commonly seen that the complete application must be wholly encompassed in the one cloud environment. Any inter-cloud communication is restricted to application-level interactions such as web service calls and message passing. Code executing in one cloud must specifically be aware that access to code in another cloud requires a manual call over the network. The design presented in this paper abstracts component communication in such a way that building of applications out of inter-cloud components is greatly simplified. Each participating Cloud instance houses its own runtime environment with its own component communication bus. The user's namespace tracks the location of each instantiated component and abstracts the inter-cloud communication back to inter-bus communication.

F. Application Access

This design provides benefits in the area of application access and startup when compared to existing technologies. The bootstrap process is initiated when a user attempts to access an application built according to this component-based design. The bootstrapping ensures that only the initially required components are dynamically downloaded, instantiated and executed. Existing technologies such as Java Web Start [21], in comparison, must automatically download the component application bundle before execution can begin.

VI. Metrics

During the development of this system we regularly compared with current techniques to ensure that existing levels of performance and stability were maintained by our new architecture. Initial metrics have been collected on the following data points:

- Total bytes transferred per web transaction.
- Total round-trip time per web transaction.

These metrics were recorded using a user login event as an example of a typical transaction. The user login event comprised the following high-level tasks:

1) Render static login page to user.
2) Accept user input and perform basic data validation.
3) Encrypt provided user credentials.
4) Pass credentials from user interface to authentication component.
5) Decrypt provided user credentials.
6) Access a persistent data store of user credentials.
7) Authenticate the user and generate a token.
8) Pass the token back through the authentication component to the user interface.
9) Report to the user if authentication was successful.

In the traditional approach this design would be implemented using a web browser, a web application, and a relational database. In comparison, according to our new architecture the following components were generated:

- User interface in HTML5 rendered by the web browser.
- A user interface component executing on the user's local machine (that also hosts the web browser).
- An authentication component executing on a local server.
- An encryption component executing on a local server.
- A data access component for the User object executing in Amazon EC2.
- A relational database also executing within Amazon EC2.

Figure 3 compares the respective total user round-trip time experience for the traditional and proposed implementation architectures. Round-trip is measured and displayed as the number of concurrent users increases. These metrics were collected using the Grinder tool on a tuned VM that represents a typical system under load. As can be seen, the proposed new solution tracks closely in performance with existing conventional approaches. A minor constant overhead is identified, and can be explained by the increased level of internal inter-component messaging required to implement the increased level of message flow required by the new system. This constant overhead is comparable to

 ISBN: 978-1-61208-204-2

overheads observed in more complex traditional websites, where the login function is more complicated than a simple relational database lookup.

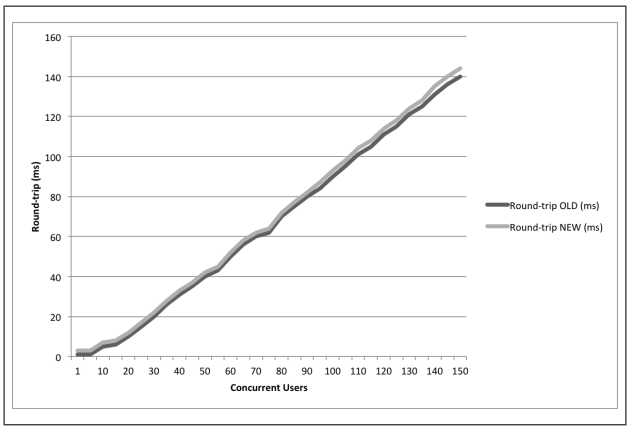


Figure 3. Round-trip comparison

Figure 4 presents comparison between the respective total bytes transferred for each architecture. Each value plotted is the sum total of all bytes transferred between all components in the experiment. Transfer of bytes is measured between the following points in the communication flow:

- Web browser and web server.
- Components and the bus.
- The bus and other components.
- Components and the data storage solution.

The comparative total bytes transferred tracks as expected when additional inter-component messaging requirements of the new solution is considered. This increase in volume of traffic is easily absorbed by the proposed new architecture because components can be distributed across multiple environments, and the additional bandwidth requirements accordingly amortised.

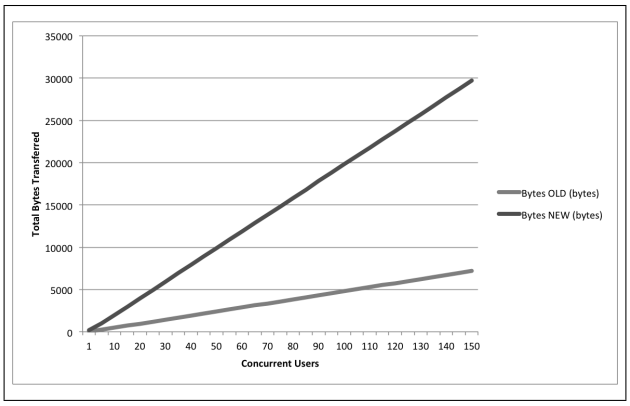


Figure 4. Total-bytes comparison

VII. Conclusion and Future Work

The system architecture presented in this paper continues to evolve as we seek to find the right mix between web application, thick application, and app-store style environments. The ”Super Browser” concept is realised as an abstraction, with the web browser becoming but one component in the overall system. To the software developer, applications are generated as a collection of inter-related components, without the need for the developer to be specifically concerned with how and where the components are executed. The full benefits of a component-based software engineering approach are realised, including the ability for systems to be designed to include off-the-shelf components. The solution presented is backwards compatible with existing web standards because the Web Browser is used as the realisation of the user interface. A Web Browser supporting the new system can seamlessly access both traditional Web 2.0 applications and applications developed using this component-based approach. The implementation is currently being finalised, with the presented metrics suggesting that performance of the new system architecture is no worse than for existing Web 2.0 technologies. The feature comparison summarised in the evaluation section shows that from a feature perspective the new model provides many benefits over existing technologies. The role of the web browser itself is simplified by distributing the hotspots such as code execution and security to a component-based design. The web browser returns to its original role of providing a user interface. This solution provides the additional benefit of allowing applications to transparently be built out of distributed components. These components can execute anywhere the user can access resources - such as on mobile devices, within server farms, or in Cloud Computing implementations.

The following items of future work have been identified:

- Further runtime environment development to cater for programming languages other than Java.
- Enhanced component locality functionality to reduce the reliance on a single component location directory.
- A comparison of security between the new user interface component design and the concept of web browser plugin process sandboxing.
- Enhancements that allow multiple users to share the same instance of a component communication bus.
- Further experimental results, specifically in comparison to existing technologies.

While the implementation of the design during this initial work is in that of middleware, the final implementation will most likely be a shared implementation across middleware and operating system. Current operating systems do not provide a component-based execution model suitable for executing the above described components, but it is envisaged that execution of these components will become a native

 ISBN: 978-1-61208-204-2

feature of the operating system in the future.

REFERENCES

[1] WebDevout. (2009, November) Web browser security statistics, http://www.webdevout.net/browser-security. [Online]. Available: http://www.webdevout.net/browser-security. (cited April 2012)

[2] D. Coursey, "Html5 could be the os killer," *PCWorld Business Centre*, 2009.

[3] C. Reis, A. Barth, and C. Pizano, "Browser security: lessons from google chrome," *Commun. ACM*, vol. 52, no. 8, pp. 45–49, 2009.

[4] G. Boss, P. Malladi, D. Quan, L. Legregni, and H. Hall. (2007, October) Cloud computing. [Online]. Available: http://download.boulder.ibm.com/ibmdl/pub/software/dw/wes/hipods/Cloud_computing_wp_final_8Oct.pdf. (cited June 2010)

[5] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599 – 616, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/B6V06-4V47C7R-1/2/d339f420c2691994442c9198e00ac87e

[6] M. Brandel, "The trouble with cloud: Vendor lock-in," *CIO.com*, 2009.

[7] Adobe Systems Incorporated. (2012) Adobe flash. [Online]. Available: http://www.adobe.com/products/flashplayer.html

[8] Microsoft. (2012) Microsoft silverlight. [Online]. Available: http://www.microsoft.com/silverlight/

[9] W3C. (2004) Web services architecture. [Online]. Available: http://www.w3.org/TR/ws-arch/

[10] M. P. Papazoglou and B. Kratz, "Web services technology in support of business transactions," *Service Oriented Computing and Applications*, vol. 1, no. 1, pp. 51–63, April 2007.

[11] I. Hickson and I. Google, *HTML 5 Specification*, editors draft ed., W3C, 2012. [Online]. Available: http://dev.w3.org/html5/spec/Overview.html

[12] D. Flanagan, *Javascript: the definitive guide*. O'Reilly, 2002.

[13] D. A. Chappell, *Enterprise Service Bus*. O'Reilly, 2004.

[14] P.-P. Koch. (2012) Quirksmode w3c dom compatability tables. [Online]. Available: http://www.quirksmode.org/compatibility.html

[15] M. Wallis, F. Henskens, and M. Hannaford, "Publish/subscribe model for personal data on the internet," in *6th International Conference on Web Information Systems and Technologies (WEBIST-2010)*. INSTICC, April 2010.

[16] ——, "Web 2.0 data: Decoupling ownership from provision," *International Journal on Advances in Internet Technology, issn 1942-2652, vol. 4, no. 1 and 2, year 2011*, pp. 47 – 59, 2011.

[17] Mozilla Foundation. (2008) Mozilla - about. [Online]. Available: http://www.mozilla.org/about/

[18] Java. (2012) Glassfish - open source application server. [Online]. Available: http://glassfish.java.net

[19] D. Parnas, "On the criteria to be used in decomposing systems into modules," *Communications of the ACM, Issue 12*, vol. 15, 1972.

[20] M. Wallis, F. Henskens, and M. Hannaford, "A distributed content storage model for web applications," in *INTERNET 2010*, 2010, pp. 98 – 103.

[21] Oracle. (2011) What is java web start and how is it launched? [Online]. Available: http://www.java.com/en/download/faq/java_webstart.xml

 ISBN: 978-1-61208-204-2

An optimization technique on pseudorandom generators based on chaotic iterations

Jacques M. Bahi, Xiaole Fang, and Christophe Guyeux*
FEMTO-ST Institute, UMR 6174 CNRS
University of Franche-Comté, Besançon, France
Email:{jacques.bahi, xiaole.fang, christophe.guyeux}@univ-fcomte.fr

***Abstract*—Internet communication systems involving cryptography and data hiding often require billions of random numbers. In addition to the speed of the algorithm, the quality of the pseudo-random number generator and the ease of its implementation are common practical aspects. In this work we will discuss how to improve the quality of random numbers independently from their generation algorithm. We propose an additional implementation technique in order to take advantage of some chaotic properties. The statistical quality of our solution stems from some well-defined discrete chaotic iterations that satisfy the reputed Devaney's definition of chaos, namely the chaotic iterations technique. Pursuing recent researches published in the previous International Conference on Evolving Internet (Internet 09, 10, and 11), three methods to build pseudorandom generators by using chaotic iterations are recalled. Using standard criteria named NIST and DieHARD (some famous batteries of tests), we will show that the proposed technique can improve the statistical properties of a large variety of defective pseudorandom generators, and that the issues raised by statistical tests decrease when the power of chaotic iterations increase.**

***Keywords*-Internet security; Pseudorandom Sequences; Statistical Tests; Discrete Chaotic Iterations; Topological Chaos.**

I. INTRODUCTION

Chaos has recently attracted more and more interests from researchers in the fields of mathematics, physics, and computer engineering, among other things due to its connection with randomness and complexity [9], [7]. In particular, various research works have recently regarded the possibility to use chaos in random number generation for Internet security. Indeed, the security of data exchanged through the Internet is highly dependent from the quality of the pseudorandom number generators (PRNGs) used into its protocols. These PRNGs are everywhere in any secure Internet communication: in the keys generation of any asymmetric cryptosystem, in the production of any keystream (symmetric cryptosystem), the generation of nonce, in the keys for keyed hash functions, and so on.

Numerous pseudorandom number generators already exist, but they are either secure but slow, or fast but insecure. This is why the idea to mix secure and fast PRNGs, to take benefits from their respective qualities, has emerged these last years [7], [1]. Chaotic dynamical systems appear as good candidates to achieve this mixture for optimization. Indeed, chaotic systems have many advantages as unpredictability or disorder-like, which are required in building complex sequences [12], [16]. This is why chaos has been applied to secure optical communications [13]. But chaotic systems of real-number or infinite bit representation realized in finite computing precision lead to short cycle length, non-ideal distribution, and other deflation of this kind. This is the reason of that chaotic systems on an infinite space of integers have been looked for these last years, leading to the proposition to use chaotic iterations (CIs) techniques to reach the desired goals. More precisely, we have proposed in INTERNET 2009 [4] to mix two given PRNGs by using chaotic iterations, being some particular kind of discrete iterations of a vectorial Boolean function. This first proposal has been improved in INTERNET 2010 [20] and INTERNET 2011 [3], to obtain a new family of statistically perfect and fast PRNGs. A short overview of these previous researches is given thereafter.

In [7], CIs have been proven to be a suitable tool for fast computing iterative algorithms on integers satisfying the topological chaotic property, as it has been defined by Devaney [10]. A first way to mix two given generators by using these chaotic iterations, called Old CIPRNGs, has been proposed in Internet 09 [4] and further investigated in [5], [2], [8]. It was chaotic and able to pass the most stringent batteries of tests, even if the inputted generators were defective. This claim has been verified experimentally, by evaluating the scores of the logistic map, XORshift, and ISAAC generators through these batteries, when considering them alone or after chaotic iterations. Then, in [20], a new version of this family has been proposed. This "New CIPRNG" family uses a decimation of strategies leading to the improvement of both speed and statistical qualities. Finally, efficient implementations on GPU using a last family called Xor CIPRNG have been designed in [6], showing that a very large quantity of pseudorandom numbers can be generated per second (about 20 Gsamples/s).

In this paper, the statistical analysis of the three methods mentioned above are carried out systematically, and the results are discussed. Indeed PRNGs are often based on modular arithmetic, logical operations like bitwise exclusive or (XOR), and on circular shifts of bit vectors. However the security level of some PRNGs of this kind has been revealed inadequate by today's standards. Since different biased generators can possibly have their own side effects when inputted into our mixed generators, it is normal to enlarge the set of tested inputted PRNGs, to determine if the observed improvement still remains. We will thus show in this research work that the intended statistical improvement is really effective for all of these most famous generators.

The remainder of this paper is organized in the following way. In Section II, some basic definitions concerning chaotic iterations are recalled. Then, four major classes of general PRNGs are presented in Section III. Section IV is devoted to two famous statistical tests suites. In Section V, various tests are passed with a goal to achieve a statistical comparison between our CIPRNGs and other existing generators. The paper ends with a conclusion and intended future work.

 ISBN: 978-1-61208-204-2

II. Chaotic Iterations Applied to PRNGs

In this section, we describe the CIPRNG implementation techniques that can improve the statistical properties of any generator. They all are based on CIs, which are defined below.

A. Notations

S^n → the n^{th} term of a sequence $S = (S^1, S^2, \ldots)$
v_i → the i^{th} component of a vector $v = (v_1, \ldots, v_n)$
f^k → k^{th} composition of a function f
strategy → a sequence which elements belong in $[\![1; \mathsf{N}]\!]$
$\mathbb{S}$ → the set of all strategies
$\mathbf{C}_n^k$ → the binomial coefficient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
$\oplus$ → bitwise exclusive or
$\ll$ and $\gg$ → the usual shift operators
$(\mathcal{X}, \mathrm{d})$ → a metric space
$LCM(a, b)$→ the least common multiple of a and b

B. Chaotic iterations

Definition 1 The set $\mathbb{B}$ denoting $\{0, 1\}$, let $f : \mathbb{B}^{\mathsf{N}} \longrightarrow \mathbb{B}^{\mathsf{N}}$ be an "iteration" function and $S \in \mathbb{S}$ be a chaotic strategy. Then, the so-called *chaotic iterations* are defined by $x^0 \in \mathbb{B}^{\mathsf{N}}$, and

$$\forall n \in \mathbb{N}^*, \forall i \in [\![1; \mathsf{N}]\!], x_i^n = \begin{cases} x_i^{n-1} & \text{if } S^n \neq i \\ f(x^{n-1})_{S^n} & \text{if } S^n = i. \end{cases} \quad (1)$$

In other words, at the n^{th} iteration, only the S^n-th cell is "iterated".

C. The CIPRNG family

1) Old CIPRNG: Let $\mathsf{N} = 4$. Some chaotic iterations are fulfilled to generate a sequence $(x^n)_{n\in\mathbb{N}} \in \left(\mathbb{B}^4\right)^{\mathbb{N}}$ of Boolean vectors: the successive states of the iterated system. Some of these vectors are randomly extracted and their components constitute our pseudorandom bit flow [4]. Chaotic iterations are realized as follows. Initial state $x^0 \in \mathbb{B}^4$ is a Boolean vector taken as a seed and chaotic strategy $(S^n)_{n\in\mathbb{N}} \in [\![1, 4]\!]^{\mathbb{N}}$ is constructed with $PRNG_2$. Lastly, iterate function f is the vectorial Boolean negation. At each iteration, only the S^n-th component of state x^n is updated. Finally, some x^n are selected by a sequence m^n, provided by a second generator $PRNG_1$, as the pseudorandom bit sequence of our generator.

The basic design procedure of the Old CI generator is summed up in Algorithm 1. The internal state is x, the output array is r. a and b are those computed by $PRNG_1$ and $PRNG_2$.

Input: the internal state x (an array of 4-bit words)
Output: an array r of 4-bit words

1: $a \leftarrow PRNG_1()$;
2: $m \leftarrow a \ mod \ 2 + 13$;
3: **while** $i = 0, \ldots, m$ **do**
4: $\quad b \leftarrow PRNG_2()$;
5: $\quad S \leftarrow b \ mod \ 4$;
6: $\quad x_S \leftarrow \overline{x_S}$;
7: **end while**
8: $r \leftarrow x$;
9: return r;

Algorithm 1: An arbitrary round of the old CI generator

2) New CIPRNG: The New CI generator is designed by the following process [11]. First of all, some chaotic iterations have to be done to generate a sequence $(x^n)_{n\in\mathbb{N}} \in \left(\mathbb{B}^{32}\right)^{\mathbb{N}}$ of Boolean vectors, which are the successive states of the iterated system. Some of these vectors will be randomly extracted and our pseudo-random bit flow will be constituted by their components. Such chaotic iterations are realized as follows. Initial state $x^0 \in \mathbb{B}^{32}$ is a Boolean vector taken as a seed and chaotic strategy $(S^n)_{n\in\mathbb{N}} \in [\![1, 32]\!]^{\mathbb{N}}$ is an *irregular decimation* of $PRNG_2$ sequence, as described in Algorithm 2.

Another time, at each iteration, only the S^n-th component of state x^n is updated, as follows: $x_i^n = x_i^{n-1}$ if $i \neq S^n$, else $x_i^n = \overline{x_i^{n-1}}$. Finally, some x^n are selected by a sequence m^n as the pseudo-random bit sequence of our generator. $(m^n)_{n\in\mathbb{N}} \in \mathcal{M}^{\mathbb{N}}$ is computed from $PRNG_1$, where $\mathcal{M} \subset \mathbb{N}^*$ is a finite nonempty set of integers.

The basic design procedure of the New CI generator is summarized in Algorithm 2. The internal state is x, the output state is r. a and b are those computed by the two input PRNGs. Lastly, the value $g_1(a)$ is an integer defined as in Eq. 2.

$$m^n = g_1(y^n) = \begin{cases} 0 \text{ if } 0 \leqslant y^n < C_{32}^0, \\ 1 \text{ if } C_{32}^0 \leqslant y^n < \sum_{i=0}^{1} C_{32}^i, \\ 2 \text{ if } \sum_{i=0}^{1} C_{32}^i \leqslant y^n < \sum_{i=0}^{2} C_{32}^i, \\ \vdots \quad \vdots \\ N \text{ if } \sum_{i=0}^{N-1} C_{32}^i \leqslant y^n < 1. \end{cases} \quad (2)$$

Input: the internal state x (32 bits)
Output: a state r of 32 bits

1: **for** $i = 0, \ldots, N$ **do**
2: $\quad d_i \leftarrow 0$;
3: **end for**
4: $a \leftarrow PRNG_1()$;
5: $m \leftarrow f(a)$;
6: $k \leftarrow m$;
7: **while** $i = 0, \ldots, k$ **do**
8: $\quad b \leftarrow PRNG_2() \ mod \ \mathsf{N}$;
9: $\quad S \leftarrow b$;
10: $\quad$ **if** $d_S = 0$ **then**
11: $\quad\quad x_S \leftarrow \overline{x_S}$;
12: $\quad\quad d_S \leftarrow 1$;
13: $\quad$ **else if** $d_S = 1$ **then**
14: $\quad\quad k \leftarrow k + 1$;
15: $\quad$ **end if**
16: **end while**
17: $r \leftarrow x$;
18: return r;

Algorithm 2: An arbitrary round of the new CI generator

3) Xor CIPRNG: Instead of updating only one cell at each iteration as Old CI and New CI, we can try to choose a subset of components and to update them together. Such an attempt leads to a kind of merger of the two random sequences. When the updating function is the vectorial negation, this algorithm can be rewritten as follows [6]:

$$\begin{cases} x^0 \in [\![0, 2^{\mathsf{N}} - 1]\!], S \in [\![0, 2^{\mathsf{N}} - 1]\!]^{\mathbb{N}} \\ \forall n \in \mathbb{N}^*, x^n = x^{n-1} \oplus S^n, \end{cases} \quad (3)$$

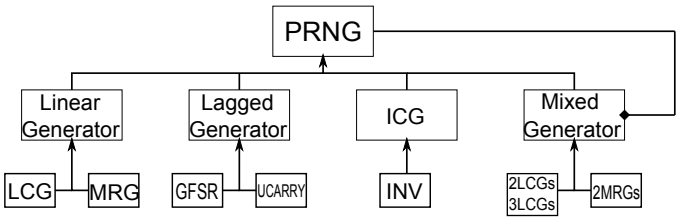


Figure 1: Ontological class hierarchy of PRNGs

The single basic component presented in Eq. 15 is of ordinary use as a good elementary brick in various PRNGs. It corresponds to the discrete dynamical system in chaotic iterations.

III. About some Well-known PRNGs

A. Introduction

Knowing that there is no universal generator, it is strongly recommended to test a stochastic application with a large set of different PRNGs [17]. They can be classified in four major classes: linear generators, lagged generators, inversive generators, and mix generators:

- **Linear generators**, defined by a linear recurrence, are the most commonly analyzed and utilized generators. The main linear generators are LCGs and MLCG.
- **Lagged generators** have a general recursive formula that use various previously computed terms in the determination of the new sequence value.
- **Inversive congruential generators** form a recent class of generators that are based on the principle of congruential inversion.
- **Mixed generators** result from the need for sequences of better and better quality, or at least longer periods. This has led to mix different types of PRNGs, as follows: $x^i = y^i \oplus z^i$

For instance, inversive generators are very interesting for verifying simulation results obtained with a linear congruential generator (LCG), because their internal structure and correlation behavior strongly differs from what LCGs produce. Since these generators have revealed several issues, some scientists refrain from using them. In what follows, chaotic properties will be added to these PRNGs, leading to noticeable improvements observed by statistical test. Let us firstly explain with more details the generators studied in this research work (for a synthetic view, see Fig. 1).

B. Details of some Existing Generators

Here are the modules of PRNGs we have chosen to experiment.

1) LCG: This PRNG implements either the simple or the combined linear congruency generator (LCGs). The simple LCG is defined by the recurrence:

$$x^n = (ax^{n-1} + c) \ mod \ m \tag{4}$$

where a, c, and x^0 must be, among other things, non-negative and less than m [19]. In what follows, 2LCGs and 3LCGs refer as two (resp. three) combinations of such LCGs. For further details, see [14].

2) MRG: This module implements multiple recursive generators (MRGs), based on a linear recurrence of order k, modulo m [19]:

$$x^n = (a^1 x^{n-1} + \ ... \ + a^k x^{n-k}) \ mod \ m \tag{5}$$

Combination of two MRGs (referred as 2MRGs) is also be used in this paper.

3) UCARRY: Generators based on linear recurrences with carry are implemented in this module. This includes the add-with-carry (AWC) generator, based on the recurrence:

$$\begin{aligned} x^n &= (x^{n-r} + x^{n-s} + c^{n-1}) \ mod \ m, \\ c^n &= (x^{n-r} + x^{n-s} + c^{n-1})/m, \end{aligned} \tag{6}$$

the SWB generator, having the recurrence:

$$\begin{aligned} x^n &= (x^{n-r} - x^{n-s} - c^{n-1}) \ mod \ m, \\ c^n &= \begin{cases} 1 & \text{if } (x^{i-r} - x^{i-s} - c^{i-1}) < 0 \\ 0 & \text{else,} \end{cases} \end{aligned} \tag{7}$$

and the SWC generator designed by R. Couture, which is based on the following recurrence:

$$\begin{aligned} x^n &= (a^1 x^{n-1} \oplus \ ... \ \oplus a^r x^{n-r} \oplus c^{n-1}) \ mod \ 2^w, \\ c^n &= (a^1 x^{n-1} \oplus \ ... \ \oplus a^r x^{n-r} \oplus c^{n-1}) \ / \ 2^w. \end{aligned} \tag{8}$$

4) GFSR: This module implements the generalized feedback shift register (GFSR) generator, that is:

$$x^n = x^{n-r} \oplus x^{n-k} \tag{9}$$

5) INV: Finally, this module implements the nonlinear inversive generator, as defined in [19], which is:

$$x^n = \begin{cases} (a^1 + a^2/z^{n-1}) \ mod \ m & \text{if } z^{n-1} \neq 0 \\ a^1 & \text{if } z^{n-1} = 0. \end{cases} \tag{10}$$

IV. Statistical tests

Considering the properties of binary random sequences, various statistical tests can be designed to evaluate the assertion that the sequence is generated by a perfectly random source. We have performed some statistical tests for the CIPRNGs proposed here. These tests include NIST suite [18] and DieHARD battery of tests [15]. For completeness and for reference, we give in the following subsection a brief description of each of the aforementioned tests.

A. NIST statistical tests suite

Among the numerous standard tests for pseudo-randomness, a convincing way to show the randomness of the produced sequences is to confront them to the NIST (National Institute of Standards and Technology) statistical tests, being an up-to-date tests suite proposed by the Information Technology Laboratory (ITL). A new version of the Statistical tests suite has been released in August 11, 2010.

The NIST tests suite SP 800-22 is a statistical package consisting of 15 tests. They were developed to test the randomness of binary sequences produced by hardware or software based cryptographic pseudorandom number generators. These tests focus on a variety of different types of non-randomness that could exist in a sequence.

For each statistical test, a set of $P-values$ (corresponding to the set of sequences) is produced. The interpretation of empirical results can be conducted in various ways. In this paper,

 ISBN: 978-1-61208-204-2

the examination of the distribution of P-values to check for uniformity ($P-value_T$) is used. The distribution of $P-values$ is examined to ensure uniformity. If $P-value_T \geqslant 0.0001$, then the sequences can be considered to be uniformly distributed.

In our experiments, 100 sequences (s = 100), each with 1,000,000-bit long, are generated and tested. If the $P-value_T$ of any test is smaller than 0.0001, the sequences are considered to be not good enough and the generating algorithm is not suitable for usage.

B. DieHARD battery of tests

The DieHARD battery of tests has been the most sophisticated standard for over a decade. Because of the stringent requirements in the DieHARD tests suite, a generator passing this battery of tests can be considered good as a rule of thumb.

The DieHARD battery of tests consists of 18 different independent statistical tests. This collection of tests is based on assessing the randomness of bits comprising 32-bit integers obtained from a random number generator. Each test requires 2^{23} 32-bit integers in order to run the full set of tests. Most of the tests in DieHARD return a $P-value$, which should be uniform on $[0, 1)$ if the input file contains truly independent random bits. These $P-values$ are obtained by $P = F(X)$, where F is the assumed distribution of the sample random variable X (often normal). But that assumed F is just an asymptotic approximation, for which the fit will be worst in the tails. Thus occasional $P-values$ near 0 or 1, such as 0.0012 or 0.9983, can occur. An individual test is considered to be failed if the $P-value$ approaches 1 closely, for example $P > 0.9999$.

V. Results and discussion

Table I shows the results on the batteries recalled above, indicating that almost all the PRNGs cannot pass all their tests. In other words, the statistical quality of these PRNGs cannot fulfill the up-to-date standards presented previously. We will show that the CIPRNG can solve this issue.

To illustrate the effects of this CIPRNG in detail, experiments will be divided in three parts:

1) **Single CIPRNG**: The PRNGs involved in CI computing are of the same category.
2) **Mixed CIPRNG**: Two different types of PRNGs are mixed during the chaotic iterations process.
3) **Multiple CIPRNG**: The generator is obtained by repeating the composition of the iteration function as follows: $x^0 \in \mathbb{B}^{\mathsf{N}}$, and $\forall n \in \mathbb{N}^*, \forall i \in [\![1; \mathsf{N}]\!]$,

$$x_i^n = \begin{cases} x_i^{n-1} & \text{if } S^n \neq i \\ \forall j \in [\![1; \mathsf{m}]\!],\ f^m(x^{n-1})_{S^{nm+j}} & \text{if } S^{nm+j} = i. \end{cases} \quad (11)$$

m is called the *functional power*.

We have performed statistical analysis of each of the aforementioned CIPRNGs. The results are reproduced in Tables I and II. The scores written in boldface indicate that all the tests have been passed successfully, whereas an asterisk "*" means that the considered passing rate has been improved.

A. Tests based on the Single CIPRNG

The statistical tests results of the PRNGs using the single CIPRNG method are given in Table II. We can observe that, except for the Xor CIPRNG, all of the CIPRNGs have passed the 15 tests of the NIST battery and the 18 tests of the DieHARD one. Moreover, considering these scores, we can deduce that both the single Old CIPRNG and the single New CIPRNG are relatively steadier than the single Xor CIPRNG approach, when applying them to different PRNGs. However, the Xor CIPRNG is obviously the fastest approach to generate a CI random sequence, and it still improves the statistical properties relative to each generator taken alone, although the test values are not as good as desired.

Therefore, all of these three ways are interesting, for different reasons, in the production of pseudorandom numbers and, on the whole, the single CIPRNG method can be considered to adapt to or improve all kinds of PRNGs.

To have a realization of the Xor CIPRNG that can pass all the tests embedded into the NIST battery, the Xor CIPRNG with multiple functional powers are investigated in Section V-C.

B. Tests based on the Mixed CIPRNG

To compare the previous approach with the CIPRNG design that uses a Mixed CIPRNG, we have taken into account the same inputted generators than in the previous section. These inputted couples $(PRNG_1, PRNG_2)$ of PRNGs are used in the Mixed approach as follows:

$$\begin{cases} x^0 \in [\![0, 2^{\mathsf{N}} - 1]\!], S \in [\![0, 2^{\mathsf{N}} - 1]\!]^{\mathbb{N}} \\ \forall n \in \mathbb{N}^*, x^n = x^{n-1} \oplus PRNG_1 \oplus PRNG_2, \end{cases} \quad (12)$$

With this Mixed CIPRNG approach, both the Old CIPRNG and New CIPRNG continue to pass all the NIST and DieHARD suites. In addition, we can see that the PRNGs using a Xor CIPRNG approach can pass more tests than previously. The main reason of this success is that the Mixed Xor CIPRNG has a longer period. Indeed, let n_P be the period of a PRNG P, then the period deduced from the single Xor CIPRNG approach is obviously equal to:

$$n_{SXORCI} = \begin{cases} n_P & \text{if } x^0 = x^{n_P} \\ 2n_P & \text{if } x^0 \neq x^{n_P}. \end{cases} \quad (13)$$

Let us now denote by n_{P1} and n_{P2} the periods of respectively the $PRNG_1$ and $PRNG_2$ generators, then the period of the Mixed Xor CIPRNG will be:

$$n_{XXORCI} = \begin{cases} LCM(n_{P1}, n_{P2}) & \text{if } x^0 = x^{LCM(n_{P1}, n_{P2})} \\ 2LCM(n_{P1}, n_{P2}) & \text{if } x^0 \neq x^{LCM(n_{P1}, n_{P2})}. \end{cases} \quad (14)$$

In Table III, we only show the results for the Mixed CIPRNGs that cannot pass all DieHARD suites (the NIST tests are all passed). It demonstrates that Mixed Xor CIPRNG involving LCG, MRG, LCG2, LCG3, MRG2, or INV cannot pass the two following tests, namely the "Matrix Rank 32x32" and the "COUNT-THE-1's" tests contained into the DieHARD battery. Let us recall their definitions:

- **Matrix Rank 32x32.** A random 32x32 binary matrix is formed, each row having a 32-bit random vector. Its rank is an integer that ranges from 0 to 32. Ranks less than 29 must be rare, and their occurences must be pooled with those of rank 29. To achieve the test, ranks of 40,000 such random matrices are obtained, and a chisquare test is performed on counts for ranks 32,31,30 and for ranks ≤ 29.
- **COUNT-THE-1's TEST** Consider the file under test as a stream of bytes (four per 2 bit integer). Each byte can contain from 0 to 8 1's, with probabilities

Table I: NIST and DieHARD tests suite passing rates for PRNGs without CI

Types of PRNGs	Linear PRNGs		Lagged PRNGs				ICG PRNGs	Mixed PRNGs		
PRNG / *Tests*	LCG	MRG	AWC	SWB	SWC	GFSR	INV	LCG2	LCG3	MRG2
NIST	11/15	14/15	**15/15**	**15/15**	14/15	14/15	14/15	14/15	14/15	14/15
DieHARD	16/18	16/18	15/18	16/18	**18/18**	16/18	16/18	16/18	16/18	16/18

Table II: NIST and DieHARD tests suite passing rates for PRNGs with CI

Types of PRNGs	Linear PRNGs		Lagged PRNGs				ICG PRNGs	Mixed PRNGs		
Single CIPRNG / *Tests*	LCG	MRG	AWC	SWB	SWC	GFSR	INV	LCG2	LCG3	MRG2
Old CIPRNG										
NIST	**15/15** *	**15/15** *	**15/15**	**15/15**	**15/15** *	**15/15** *	**15/15** *	**15/15** *	**15/15** *	**15/15**
DieHARD	**18/18** *	**18/18** *	**18/18** *	**18/18** *	**18/18**	**18/18** *	**18/18** *	**18/18** *	**18/18** *	**18/18** *
New CIPRNG										
NIST	**15/15** *	**15/15** *	**15/15**	**15/15**	**15/15** *	**15/15** *	**15/15** *	**15/15** *	**15/15** *	**15/15**
DieHARD	**18/18** *	**18/18** *	**18/18** *	**18/18** *	**18/18**	**18/18** *	**18/18** *	**18/18** *	**18/18** *	**18/18** *
Xor CIPRNG										
NIST	14/15*	**15/15** *	**15/15**	**15/15**	14/15	**15/15** *	14/15	**15/15** *	**15/15** *	**15/15**
DieHARD	16/18	16/18	17/18*	**18/18** *	**18/18**	**18/18** *	16/18	16/18	16/18	16/18

1,8,28,56,70,56,28,8,1 over 256. Now let the stream of bytes provide a string of overlapping 5-letter words, each "letter" taking values A,B,C,D,E. The letters are determined by the number of 1's in a byte: 0,1, or 2 yield A, 3 yields B, 4 yields C, 5 yields D and 6,7, or 8 yield E. Thus we have a monkey at a typewriter hitting five keys with various probabilities (37,56,70,56,37 over 256). There are 5^5 possible 5-letter words, and from a string of 256,000 (over-lapping) 5-letter words, counts are made on the frequencies for each word. The quadratic form in the weak inverse of the covariance matrix of the cell counts provides a chisquare test: Q5-Q4, the difference of the naive Pearson sums of $(OBS - EXP)^2/EXP$ on counts for 5- and 4-letter cell counts.

The reason of these fails is that the output of LCG, LCG2, LCG3, MRG, and MRG2 under the experiments are in 31-bit. Compare with the Single CIPRNG, using different PRNGs to build CIPRNG seems more efficient in improving random number quality (mixed Xor CI can 100% pass NIST, but single cannot).

C. Tests based on the Multiple CIPRNG

Until now, the combination of at most two input PRNGs has been investigated. We now regard the possibility to use a larger number of generators to improve the statistics of the generated pseudorandom numbers, leading to the multiple functional power approach. For the CIPRNGs which have already pass both the NIST and DieHARD suites with 2 inputted PRNGs (all the Old and New CIPRNGs, and some of the Xor CIPRNGs), it is not meaningful to consider their adaption of this multiple CIPRNG method, hence only the Multiple Xor CIPRNGs, having the following form, will be investigated.

$$\begin{cases} x^0 \in [\![0, 2^{\mathsf{N}} - 1]\!], S \in [\![0, 2^{\mathsf{N}} - 1]\!]^{\mathbb{N}} \\ \forall n \in \mathbb{N}^*, x^n = x^{n-1} \oplus S^{nm} \oplus S^{nm+1} \ldots \oplus S^{nm+m-1}, \end{cases} \quad (15)$$

The question is now to determine the value of the threshold m (the functional power) making the multiple CIPRNG being able to pass the whole NIST battery. Such a question is answered in Table IV.

D. Results Summary

We can summarize the obtained results as follows.

1) The CIPRNG method is able to improve the statistical properties of a large variety of PRNGs.
2) Using different PRNGs in the CIPRNG approach is better than considering several instances of one unique PRNG.
3) The statistical quality of the outputs increases with the functional power m.

VI. Conclusion and Future Work

In this paper, we first have formalized the CI methods that has been already presented in previous Internet conferences. These CI methods are based on iterations that have been topologically proven as chaotic. Then 10 usual PRNGs covering all kinds of generators have been applied, and the NIST and DieHARD batteries have been tested. Analyses show that PRNGs using the CIPRNG methods do not only inherit the chaotic properties of the CI iterations, they also have improvements of their statistics. This is why CIPRNG techniques should be considered as post-treatments on pseudorandom number generators to improve both their randomness and security.

In future work, we will try to enlarge this study, by considering a larger variety of tests. The CIPRNG's chaotic behavior will be deepened by using some specific tools provided by the mathematical theory of chaos. Finally, a large variety of Internet usages, as cryptography and data hiding, will be considered for applications.

References

[1] J. M. Bahi and C. Guyeux. A new chaos-based watermarking algorithm. In *SECRYPT 2010, International conference on security and cryptography*, pages 1–4, Athens, Greece, 2010. To appear.

 ISBN: 978-1-61208-204-2

Table III: Scores of mixed Xor CIPRNGs when considering the DieHARD battery

$PRNG_1$ \ $PRNG_0$	LCG	MRG	INV	LCG2	LCG3	MRG2
LCG		16/18	16/18	16/18	16/18	16/18
MRG	16/18		16/18	16/18	16/18	16/18
INV	16/18	16/18		16/18	16/18	16/18
LCG2	16/18	16/18	16/18		16/18	16/18
LCG3	16/18	16/18	16/18	16/18		16/18
MRG2	16/18	16/18	16/18	16/18	16/18	

Table IV: Functional power m making it possible to pass the whole NIST battery

Inputted *PRNG*	LCG	MRG	SWC	GFSR	INV	LCG2	LCG3	MRG2
Threshold value m	19	7	2	1	11	9	3	4

[2] J. M. Bahi and C. Guyeux. Topological chaos and chaotic iterations, application to hash functions. *WCCI'10: 2010 IEEE World Congress on Computational Intelligence*, Accepted paper, 2010.

[3] Jacques Bahi, Jean-François Couchot, Christophe Guyeux, and Qianxue Wang. Class of trustworthy pseudo random number generators. In *INTERNET 2011, the 3-rd Int. Conf. on Evolving Internet*, pages 72–77, Luxembourg, Luxembourg, June 2011. To appear.

[4] Jacques Bahi, Christophe Guyeux, and Qianxue Wang. A novel pseudo-random generator based on discrete chaotic iterations. In *INTERNET'09, 1-st Int. Conf. on Evolving Internet*, pages 71–76, Cannes, France, August 2009.

[5] Jacques Bahi, Christophe Guyeux, and Qianxue Wang. A pseudo random numbers generator based on chaotic iterations. application to watermarking. In *WISM 2010, Int. Conf. on Web Information Systems and Mining*, volume 6318 of *LNCS*, pages 202–211, Sanya, China, October 2010.

[6] Jacques M. Bahi, Raphael Couturier, Christophe Guyeux, and Pierre-Cyrille Heam. Efficient and cryptographically secure generation of chaotic pseudorandom numbers on gpu. *http://arxiv.org/abs/1112.5239*, December 2011. Submitted already.

[7] Jacques M. Bahi and Christophe Guyeux. Topological chaos and chaotic iterations, application to hash functions. In *WCCI'10, IEEE World Congress on Computational Intelligence*, pages 1–7, Barcelona, Spain, July 2010. Best paper award.

[8] Jacques M. Bahi, Christophe Guyeux, and Qianxue Wang. Improving random number generators by chaotic iterations. application in data hiding. In *ICCASM 2010, Int. Conf. on Computer Application and System Modeling*, pages V13–643–V13–647, Taiyuan, China, October 2010.

[9] S. Behnia, A. Akhavan, A. Akhshani, and A. Samsudin. A novel dynamic model of pseudo random number generator. *Journal of Computational and Applied Mathematics*, 235(12):3455–3463, 2011.

[10] R. L. Devaney. *An Introduction to Chaotic Dynamical Systems*. Redwood City: Addison-Wesley, 2nd edition, 1989.

[11] Christophe Guyeux and Jacques Bahi. An improved watermarking algorithm for internet applications. In *INTERNET'2010. The 2nd Int. Conf. on Evolving Internet*, pages 119–124, Valencia, Spain, September 2010.

[12] Yue Hu, Xiaofeng Liao, Kwok wo Wong, and Qing Zhou. A true random number generator based on mouse movement and chaotic cryptography. *Chaos, Solitons & Fractals*, 40(5):2286–2293, 2009.

[13] L. Larger and J.M. Dudley. Nonlinear dynamics Optoelectronic chaos. *Nature*, 465(7294):41–42, 05 2010.

[14] P. L'Ecuyer. Efficient and portable combined random number generators. *Communications of the ACM*, 31(6):742–749, 1988.

[15] George Marsaglia. Diehard: a battery of tests of randomness. *http://www.stat.fsu.edu/pub/diehard/*, 1996.

[16] L. De Micco, C.M. Gonzaez, H.A. Larrondo, M.T. Martin, A. Plastino, and O.A. Rosso. Randomizing nonlinear maps via symbolic dynamics. *Physica A: Statistical Mechanics and its Applications*, 387(14):3373–3383, 2008.

[17] David R.C. and Hill. Urng: A portable optimization technique for software applications requiring pseudo-random numbers. *Simulation Modelling Practice and Theory*, 11(7C8):643 – 654, 2003.

[18] NIST Special Publication 800-22 rev. 1. A statistical test suite for random and pseudorandom number generators for cryptographic applications. August 2008.

[19] Richard Simard and Université De Montréal. Testu01: A software library in ansi c for empirical testing of random number generators. software users guide. *ACM Transactions on Mathematical Software*, 2002.

[20] Qianxue Wang, Jacques Bahi, Christophe Guyeux, and Xiaole Fang. Randomness quality of CI chaotic generators. application to internet security. In *INTERNET'2010. The 2nd Int. Conf. on Evolving Internet*, pages 125–130, Valencia, Spain, September 2010. IEEE Computer Society Press. Best Paper award.

 ISBN: 978-1-61208-204-2

Dynamic Access Control Using Virtual Multicore Firewalls

Vladimir Zaborovsky, Alexey Lukashin
Department of Telematics
Saint-Petersburg State Polytechnical University
Saint-Petersburg, Russia
vlad@neva.ru lukash@neva.ru

Abstract—**The problems of Internet services security are becoming particularly important due to intricacy structure and dynamic nature of distributed environment, especially in a cloud and virtualized systems. The complexity of distributed platforms demands more functionality to be provided by security devices. Among these required functions is the ability to configure these devices online in accordance with the current state of the network environment through which users can gain an access to information services. The performance of security services is a major issue. This paper proposes a firewall-based solution for implementing access control using multiple cores in virtualized and pure hardware environments, and describes dynamic access control based on virtual connections management with the mechanism of traffic filtering in a transparent (also called "stealth") mode. In this mode, the firewall is not visible to other participants (components) of network interactions, and, thus, it allows implementing the access policy, but remains invulnerable for cyber crooks.**

Keywords-security; dynamic access control; firewall; virtualization; netgraph

I. INTRODUCTION

Information security solutions like firewalls are very sensitive to the level of performance. Modern information channels support huge bandwidth, 10Gbit/s is almost everywhere. In 10Gbit/s Ethernet networks firewall has to make a decision in less than 1ms for a packet. During this time it should check protocol validness and pass all filtering rules to different network layers – from the channel to applied protocols. The current work proposes to achieve this goal by using multicore capabilities of modern computing platforms. The traffic processing should be made in parallel. Concurrent programming is quite complicated, so it is necessary to provide some generic approach which allows implementing parallel data processing for different cases. The paper describes another major issue – virtualization. Today, businesses of various sizes widely use virtualization. Small companies use cloud providers like Amazon or Rackspace, medium and big businesses have its own computing infrastructure based on virtualization. The main problem is that virtual systems are hidden from hardware security devices, like hardware firewalls; thus, the necessary "virtual" communication is usually not controlled. It is very important for cloud systems to find a solution for this problem; especially, for private cloud solutions such as Eucalyptus [1], OpenStack [2], OpenNebula [3] and others. Security is a very actual problem in the cloud [5, 6]. Modern government departments build their infrastructure using cloud systems and, of course, these systems should control all information resources. So, another requirement for modern firewall is the ability to be virtual as well as high performance. Firewall virtualization gives another opportunity that allows scaling firewall resources depending of the current situation by changing number of cores or memory in runtime. Firewall performance scalability is very useful for cloud systems. The nature of cloud environments is very dynamic; the resources, which can be presented in the cloud, are extremely different. The cloud firewall should also be dynamic and flexible, by having the possibility to reconfigure itself in runtime according to the current cloud state. In this paper, we propose a solution with parallel traffic processing models and describe architecture of cloud environment secured by virtual firewalls inside hypervisors. Our firewalls manage network traffic in stealth mode; the firewall interfaces haven't any physical addresses and invisible for other network components. It increases security and allows installing these firewalls transparently to hypervisor or physical network.

The main contribution of this paper is a graph virtual connection control model, which is implemented by using Netgraph [4] network subsystem. We also present a prototype of such stealth firewall which works as a separate hardware solution and as a virtual machine in hypervisor and manages virtual traffic.

The paper is organized in six sections. Section 1 is an introduction; the second one describes virtual connections and traffic filtering as computation graph. Section 3 describes virtual connection processing models using Netgraph network subsystem. Section 4 contains description of experiments and measurements. Section 5 proposes architecture of secure cloud with stealth multicore firewalls and Section 6 is the conclusions.

II. APPROACHES FOR VIRTUAL CONNECTIONS CONTROL

Packet flow is described as a set of virtual connections between users and services [7]. Virtual connection (VC) is a logically ordered exchange of messages between the network nodes. Virtual connections are classified as technological virtual connections (TVC) and informational virtual connections (IVC). A technological virtual connection is described by network protocols, e.g., TCP session between user and database. Information virtual connection is described by applied protocols, e.g., HTTP session with a

 ISBN: 978-1-61208-204-2

web service. IVC might use multiple TVC, e.g., ftp session uses 2 TCP connections; one for data and another for control messages. And vice versa, TVC might belong to multiple IVCs, e.g., persistent connections in HTTP, as described in RFC 2616 client can reuse existing TCP connections for multiple requests, of course, resource URI might be also different.

For flexible access control and traffic management dividing TVCs into three groups was proposed:

1) Permitted important connections without additional control;
2) Prohibited connections;
3) Other connections which are not prohibited yet but need additional control.

The first group is the priority connections and the third group is background connections. All packets of virtual connections in the second group are dropped by firewall and not taken into account.

We propose the preemptive priority queuing system with two types of packets [8]. First type has priority over the second one. The packets arrive into the buffer according to the Poisson process. The service time has the exponential distribution. The buffer has a finite size m and it is shared by both types of packets. The preemptive priority in service is given to the packets of the first type. Considered system is supplied by the randomized push-out mechanism that helps precisely and accurate to manage packets of both types. If the buffer is full, a new coming packet of type 1 can push out a packet of type 2 with the probability from the buffer.

As it is shown in [8], it is possible to change the time which packets spend in the firewall buffer by choosing α parameter. That allows to limit access possibilities of background traffic and even to block a connection if it's classified as being prohibited during the data transmission. The proposed mechanism also allows controlling TVC throughput and increasing time for the access decision without interrupting the established connection.

Technical virtual connection exists in parallel to and independently from other virtual connections. Virtual connections do not share any resources. It allows parallel processing of virtual connections. The suggested approach to the network traffic filtering is based on the concept of virtual connection and allows extracting the connection context. The connection context can be described as a vector Yi, which contains a set of parameters, for example, source and destination addresses, port, connection status (for TCP protocol), etc. Virtual connection control is a computation of the indicator function F, which requires resources, such as computing processors and operating memory.

$$F(Y_i) = \{1,0,*\} \quad (1)$$

The indicator function F takes the following values: 1- if VC is allowed; 0- if VC is forbidden; *, if at the current moment it is impossible to clearly determine whether connection is prohibited or not, the decision is postponed and VC is temporarily allowed.

Calculation of the indicator function F can be decomposed into multiple computing processes; $\{F_i\}$, $i=\{1..n\}$, where n is a number of independent calculation processes, e.g., evaluation of virtual connection might consist of filtering rules check, protocol validness check, intensity check, content check, etc. In this case, the problem of VC control can be described by using the graph G(Q,X), which is called the VC control information graph. Q is a set of nodes; X is a set of edges between the nodes. The VC control information graph consists of the set of nodes; each of these nodes is attributed with the operation F_i. If two nodes q_i and q_{i+1} are connected with an arc, then the result of the operation F_i is the input for the operation F_{i+1}. Each node has an arc, which corresponds to the case when $F_i = 0$. Then VC is considered as being prohibited and no further analysis is performed.

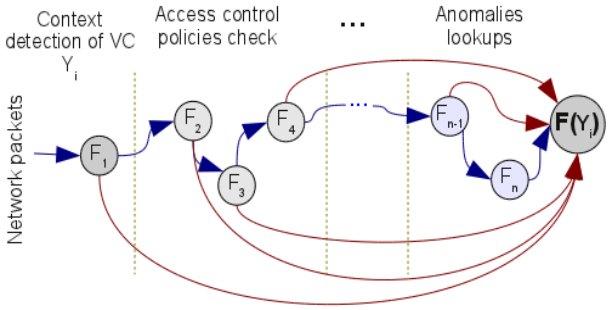


Figure 1. Virtual connection computation graph

The multiprocessor computing system which performs network traffic analyses might be described as a full mesh computation system graph with MIMD computers as its nodes. This graph is a full mesh, because the communications between CPUs are provided by hardware and operating system, and there is no predefined path between the cores; the data can pass directly from one node to another. Usually, the computation system graph and the control information graph do not match each other, because the amount of computing resources is limited and is less than the amount of computational processes. In this case, computation resources are used concurrently by information processes. It is possible to split the VC control graph in N non-crossing sub graphs and, thus, to build a VC operating pipeline. Because the virtual connections exist separately from each other, they can be processed in parallel. With the C compute nodes of MIMD type, the operating time of VC processing would be limited by (2).

$$T_{vc} = \frac{\max(z(f_i)) * \max(\tau_i)}{C} \quad (2)$$

Where $z(f_i)$ – number of CPU clocks, required for calculation of function f_i ,τ_i – average time of CPU clock in f_i calculation.

 ISBN: 978-1-61208-204-2

The given formula is an inequality because the decision on the VC classification (allowed/forbidden) can be made before passing all nodes of the graph.

Due to heterogeneity and re-configurability of the computing environments, in some cases the configuration of the firewall can be adapted to the access control tasks being solved at the current moment of time. This can be achieved by using the graph models for network traffic processing and Netgraph technology [4]. This technology allows organizing the network traffic processing in the context of the operating system [9].

Figure 1 shows an example of the virtual connections information control graph with decomposition of the indicator control function into components. The presented approach, in the combination with using the virtualization resources technology, allows improving performance of the network traffic monitoring and using only those computing components which are required for resolving the current access control problems.

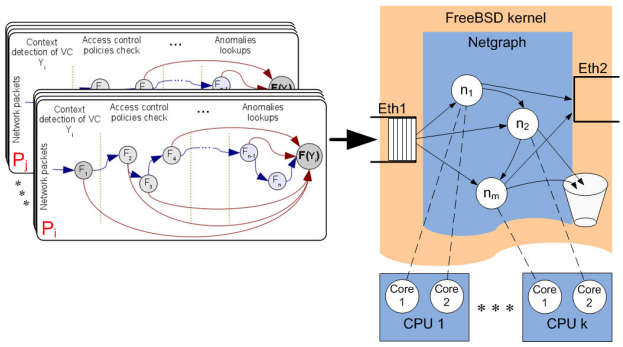


Figure 2. Information graph of the virtual connection management

Virtual connections should be processed on multiple cores. Network packets are balanced between cores using accessory to particular virtual connection. So, the order of packet flow in virtual connection is not corrupted, that allows process traffic in parallel using Netgraph network subsystem (Figure 2.).

III. VIRTUAL CONNECTIONS PROCCESING MODELS

To implement the parallel traffic processing Netgraph network subsystem, the part of FreeBSD kernel was used. This solution allows handling network connections in kernel mode and doing it using multiple cores. But the kernel mode programming produces new level of implementation complexity and delivers new behavior models which should be evaluated and carefully implemented. The cost of software bug is quite high; kernel level errors causes full system crash and reboot the firewall. But, if software stable are tested and verified, this approach will provide great performance opportunities. Well known Cisco software [10] also works in kernel mode and does it quite well. The graphs nature of Netgraph allows splitting traffic management process in independent parts logically and defining the computation process as a set of independent modules. The firewall configuration can be changed in runtime by adding and removing nodes in graph topology. It allows to extend firewall functionality and to improve performance by parallel traffic processing in separate kernel threads.

Netgraph has a complicated architecture and can operate differently, depending of the used nodes, the involved protocols and the implemented algorithms. When Netgraph starts, it creates a pool of kernel threads. The number of threads is equal to the number of available cores. These threads can be used for message processing. Network packets are presented as *mbuf* structures which are transferred between Netgraph nodes. In general, Netgraph can work in two modes – direct routine calls and queuing packets in nodes, and processing in multiple threads if possible. The operational mode depends on graph topology and node implementation. One of the reasons is function call depth. Recursive calls depth is limited by stack size. FreeBSD kernel stack is just 8K on i386 and 16K on amd64. It means that you can't pass more then 5-10 nodes without queuing (number of nodes depends on how much stack these nodes consume). There are two models which describe these Netgraph modes.

A. *Network driver based balancing and direct calls*

This solution fully depends on network interface kernel module implementation and used hardware. Not all network interfaces can handle traffic using multiple cores. Usually, it is implemented in high performance 10Gbit network interfaces. One of the possible technologies is MSI-X [11]. In this case, Netgraph uses direct calls to handle traffic. Traffic filtering works directly in network card – packet arrived event interrupts thread context. Netgraph uses the algorithm based on virtual connection attributes for balancing. For TCP connections it sends a packet of specific virtual connection to specific core. For UDP protocols it sends a packet to any available core.

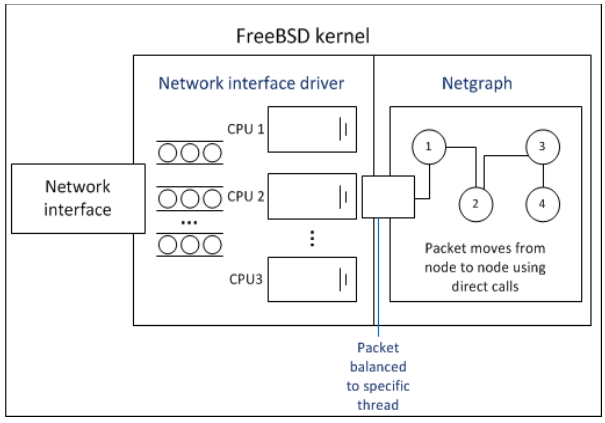


Figure 3. Load balancing in network interface driver

Figure 3 shows the structure of traffic processing in the FreeBSD kernel. A Packet arrives to network interface, then it gets processed by Netgraph Ethernet node *ng_eth* and

passes packet to the next module using direct routine call. Each next node evaluates the packet according to the filtering rules, the network protocol state model, the packet content and if the packet which belongs to some virtual connection is considered as allowed then the packet is sent to outgoing interface. If the virtual connection is prohibited, then the packet is dropped and the virtual connection is marked as prohibited. In this case, the traffic is routed through the Netgraph nodes, but it is processed in one thread. This behavior can could be presented as one process P which can be described as the process graph with the set of the states {s} and the set of the actions act(P):

$$S = \{s_i, i = 1..n\} \bigcup \{allowed, trash, wait\} \quad (3)$$

$$act(P) = \{p!.p?, d!, a!, b\} \quad (4)$$

where act(p) is the alphabet of actions, *p?* is incoming packet object, *p!* is outgoing packet object, *d!* is outgoing *drop* action (connection is prohibited), a*!* is outgoing *allowed* action – connection is allowed, no further analyses needed, b is *packet processed* action, system goes to accept the next packet. The process graph is shown on Figure 4.

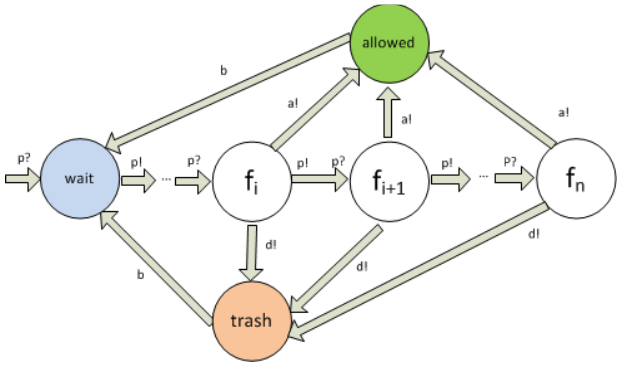


Figure 4. Connection control process graph

Process is awaiting for incoming event, when packet is scheduled to a specific thread it is evaluated by chain of Netgraph nodes, node accepts packet object, evaluates it and might generate three actions – decision is not made (to process packet on next node), connection is allowed, connection is prohibited (to move packet to trash).

B. *Queuing packets in nodes*

The second approach is to put packets in queues and process packets in Netgraph nodes in different kernel threads (Figure 5). In the described situation each Netgraph node is a separate process P_i, which can accept action messages with network packet object and produce the same messages as shown on Figure 4. But, the whole connection control process P is a parallel composition of Netgraph nodes processes:

$$P = (P_1 \mid P_2 \mid ... \mid P_n) \quad (5)$$

This solution allows to implement the parallel traffic processing using conveyers of nodes, which processes data in separate threads. The strong side of this solution is lack of hardware and network.

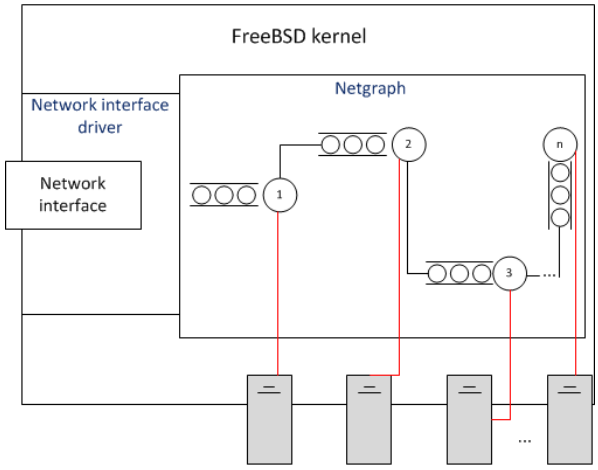


Figure 5. Netgraph nodes with queues

Figure 5 describes Netgraph behavior. Each node is processed on CPU or core in separate thread. When packet is arrived to node it put to FIFO queue.

IV. PERFORMANCE MEASUREMENT FOR NETGRAPH FIREWALL

We performed the experiments with firewall traffic control performance using Netgraph network subsystem. The first test is a scalability check. The virtualization technology was used in order to perform the experiment. The firewall was running as a virtual machine in Xen Cloud Platform hypervisor. The virtual firewall had two interfaces, which were connected to physical network using bridges in hypervisor service console. Figure 6 is the experiment schema.

 ISBN: 978-1-61208-204-2

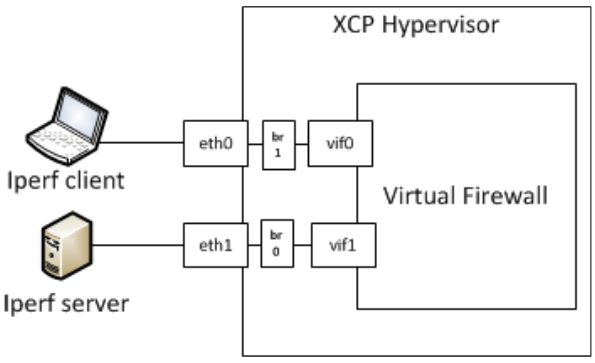


Figure 6. Scalability test experiment

We manually *slowed down* traffic filtering process in order to see how it scaled with the cores number growth. For performance measurement *iperf* tool was used in different configurations. Netgraph packet filter with packet queuing direct calls was used. Several TCP connections were created using *iperf* and this experiment was performed for one, two, and four cores configuration. Firewall performance is scaled almost linearly. The results are shown in Table 1.

TABLE I. TABLE 1. TRAFFIC CONTROL SCALABILITY TEST

	Direct calls model			**Packet queuing model**		
	1 TCP stream	2 TCP streams	4 TCP streams	1 TCP stream	2 TCP streams	4 TCP streams
1 core	1.43Mbit/s	1.43Mbit/s	1.43 Mbit/s	1.42 Mbit/s	1.44 Mbit/s	1.43 Mbit/s
2 cores	2.44 Mbit/s	2.45 Mbit/s	2.43 Mbit/s	1.52 Mbit/s	3.17 Mbit/s	3.14 Mbit/s
4 cores	2.44 Mbit/s	2.45 Mbit/s	2.44 Mbit/s	1.51 Mbit/s	3.18 Mbit/s	6.26 Mbit/s

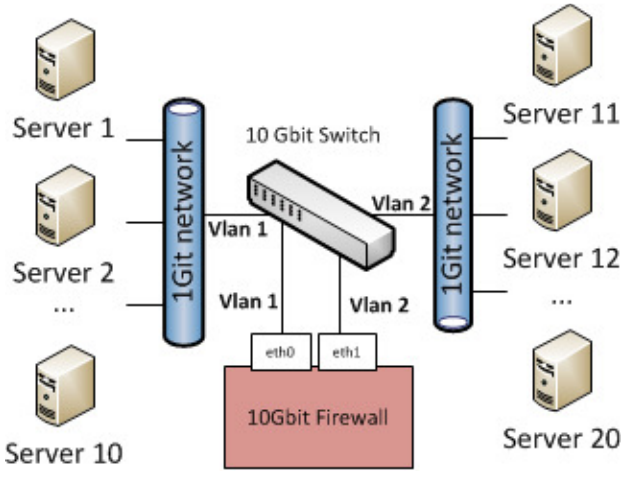


Figure 7. Performance test experiment

The second test in high performance environment was performed. Multicore system with two 10Gbit Ethernet adapters has been prepared. Firewall software has been installed on bare metal without virtualization. One gigabit Computer network with 20 hosts was separated into two segments with different VLANs and these segments were connected by stealth Netgraph firewall. Experiment schema is shown on Figure 7. Network hosts were configured to run iperf tests and generated the sufficient amount of network traffic. For this test Netgraph configuration with direct calls was selected, because hardware had 10Gbit network cards with MSI-X technology, so, traffic management was paralleled by network driver. We compared the kernel mode Netgraph firewall with the user space stealth implementation which uses Berkley Packet Filter (BPF) for traffic processing. The filtering algorithm is the same for both firewalls. The Experiment results are shown in Table 2.

TABLE II. TRAFFIC CONTROL ON MULTIPLE CORES

	Netgraph firewall	**BPF firewall**
Throughput, Gbit/s	8.3	1.2

V. VIRTUAL FIREWALL APPLIANCE IN THE CLOUD COMPUTING ENVIRONMENT

Information security in the cloud is a hot topic today [5]. There are no standards implemented in this area, but a lot of ideas were proposed. One of the major issues in virtualized systems security is an access control between virtual machines. Virtual machines communicate using network bridges in host system. Network bridge is implemented in Linux kernel and supports 802.1d standard. It can also be replaced by open vSwitch which supports more features like open flow, vlans, QoS, or proprietary bridge drivers, such as VMware vSwitch or Nexus 1000V. The paper proposes a solution which allows controlling traffic between virtual machines and having central management system. A typical distributed computing environment (cloud system) consists of the following software and hardware components:

- Virtualization nodes;
- Storage of virtual machines and user data;
- Cluster controller;
- Cloud controller.

Cloud computing systems might be used for the wide area of problems- from web services hosting government infrastructure and scientific computing. In Saint-Petersburg State Polytechnical University scientific cloud system based on OpenStack and Xen hypervisor was implemented. The distributed computing environment intended for solving scientific and engineering problems is a set of various computing resources such as virtual machines, and it has the following features [12]:

- The environment is used by a wide range of users, who are solving the problems of different classes;
- Virtual machines of different user groups can operate within one hypervisor;

 ISBN: 978-1-61208-204-2

- A wide range of software components (CAD/CAE applications, development tools) and operating systems (Linux, Windows, FreeBSD) are used;
- Different hardware configurations are used.

There is a difference in information security aspects between classic computing infrastructure, such as networks with hardware servers and user stations and virtual cloud environment where all resources are placed in the cloud, the hardware resources are shared between different users (possibly with different access rights):

- Information processing takes place on the virtual machines under full hypervisor's control; the hypervisor has access to all data processed by its virtual machines;
- Cloud software controls the resource planning and provision; it is a new entity in the information environment which has to be protected from the information security threats;
- Traditional information security components, such as hardware firewalls cannot control the internal virtual traffic between virtual machines in one hypervisor;
- In virtualized environments, files serve as virtual storage devices; these files are located in the network storages and are more exposed to threats than to hard disks;
- Transfer of instance memory occurs when virtual machines migrate between hypervisors; this memory may contain confidential information.

These features lead to the specific issues of security policy and access control in cloud systems. The environment becomes more dynamic. When the new resource (e.g. virtual machine) started in the cloud the security policy can be changed in the particular hypervisor or in the whole cloud system. For example, new virtual machine from security group "Engineering Department" was started. It changed the set of security groups in the particular hypervisor. So, the set of security policy rules was changed as well. That means, it is necessary to change the filtering rules for firewall dynamically. It controls network traffic between virtual machines, public network and other cloud components. Cloud computing system consists of virtualization nodes and cloud management services. Virtualization node is the hypervisor software which running on powerful multicore computing node. The domain level 0 (dom0 in terms of hypervisor XEN or service console in terms of other hypervisors) and virtual computing machines (domain level U, domU) operate in virtualization.

For information security and access control (AC) between the virtual machines that operate under a single hypervisor, the internal ("virtual") traffic and the external traffic (incoming from other hypervisors and from public networks) must be controlled. The solution of the access control problem could be achieved through the integration of a virtual firewall into the hypervisor; this firewall would function under the hypervisor, but separately from the user virtual machines. The virtual firewall domain can be defined as "security domain" (domS). Invisible traffic filtering is an important aspect of the network monitoring; the firewall must not change the topology of the hypervisor network subsystem. This can be achieved by using "Stealth" technology [13]; a packet traffic control is invisible to other network components**.** Virtual nature of firewall allows making hardware configuration dynamic. If security policy provides a lot of filtering rules, the number of the involved cores and memory amount can be dynamically increased. And vice versa, if the virtual firewall is not overloaded, it is possible to decrease allocated resources.

Figure 8 shows the common architecture of a distributed cloud system with integrated AC components. Abbreviations: VM – virtual machine; domS – security domain, virtual firewall; CSMS – the central security management system. The CSMS central management system generates and distributes the access control policies to all firewalls in the system. The security domain isolates virtual machines from the hypervisor, which prevents the possibility of attack against the hypervisor inside the cloud.

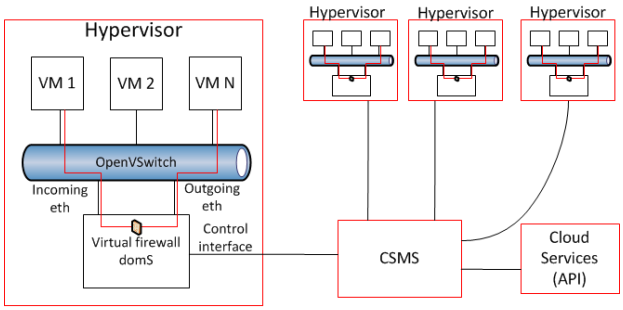


Figure 8. Secure cloud architectrure

Multicore stealth firewall based on Netgraph to implement traffic control between virtual machines was used. Virtual firewall has three network interfaces: two- for filtering and one- for management. Filtering interfaces are connected to open vSwitch bridge. Using OpenFlow technology channel level, the traffic routes were changed from the standard commutation tables – all outgoing virtual traffic routed to the incoming firewall interfaces. The firewall evaluates traffic in the stealth mode and passes it to outgoing network interface if it is allowed. From outgoing filter the interface traffic routed in a normal way by using commutation tables.

VI. CONCLUSION AND FUTURE WORK

The paper proposed the parallel traffic control model for high performance firewalls and describes firewall prototype implementation based on Netgraph network subsystem. The presented multicore firewall prototype shows good performance, up to 8.3 Gbit/s in 10Gbit networks. We also evaluated that solution based on graph model has good scalability. The firewall works in stealth mode and has not physical addresses and might be integrated to existing network topology without any changes. The firewall

 ISBN: 978-1-61208-204-2

software was tested in bare metal and virtualized environments.

The traffic management model with network card balancing requires hardware and software support side (at least, MSI-X technology), so it cannot be used in all systems. The second model (Netgraph nodes with queues) should work in all systems and we propose it as preferable. But implementation process of this model is more complicated and should be evaluated very carefully. The model with queues provides more control of traffic management. It allows performing load balancing by protocol types including nested protocols, e.g. MSI-X technology cannot perform load balancing for PPP protocol – all PPP connections are processed in single thread because it is treated as one virtual connection. Node queues also allow to override the existing Netgraph queue algorithm and to implement priority queuing as described.

Stealth mode allows implementing the information protection system for cloud computing environment in the form of a dedicated security domain (domS). The security domain can be quickly adapted to the current situation in the network and scaled if necessary because of firewall's virtual nature.

Described above architecture of secure cloud can be merged easily with low level methods of network control, for example, with flow-based traffic measurement or packet priority queuing management. The prototype of the described secure cloud environment based on OpenStack and adopted for CAD/CAE computation tasks, was created and currently in testing at the Telematics Department of the Saint-Petersburg Polytechnical University.

The future plan is to extend current virtual firewall prototype functionality. The prototype has to be adapted for work in different virtual environments such as VMware ESXi, Xen, Xen Cloud Platform, and KVM. The process models should be extended according to communicating sequential processes (CSP) theory and carefully checked because of potentially dangerous kernel operational mode.

REFERENCES

[1] Overview of Eucalyptus, 2011. URL: http://support.rightscale.com/09-Clouds/Eucalyptus/01-Overview_of_Eucalyptus 05.06.2012

[2] OpenStack: An Overview, 2012. URL: http://www.openstack.org/downloads/openstack-overview-datasheet.pdf 05.06.2012

[3] About the OpenNebula Technology, 2012. URL: http://opennebula.org/about:technology 05.06.2012

[4] Cobbs A., 2003. All about Netgraph URL: http://www.daemonnews.org/200003/netgraph.html 05.06.2012

[5] Cloud Security Alliance, Top Threats to Cloud Computing, 2010. URL: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf 05.06.2012

[6] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. 2010. A view of cloud computing. Commun. ACM 53, 4 (April 2010), pp. 50-58.

[7] A. Silinenko. Access control in IP networks based on virtual connection state models: PhD. Thesis 05.13.19: / SPbSPU, Russia, 2010

[8] V. Zaborovsky, V. Mulukha. Access Control in a Form of Active Queuing Management in Congested Network Environment // Proceedings of the Tenth International Conference on Networks, ICN 2011, pp. 12-17

[9] Zaborovsky V., Lukashin A., Kupreenko S., 2010. Multicore platform for high performance firewalls. High performance systems // Materials of VII International conference – Taganrog, Russia.

[10] Vijay Bollapragada, Russ White, and Curtis Murphy. Inside Cisco IOS Software Architecture // Cisco Press 2008. 240 pages.

[11] Improving Network Performance in Multi-Core Systems http://www.intel.com/content/www/us/en/ethernet-controllers/improving-network-performance-in-multi-core-systems-paper.html

[12] Alexey Lukashin, Vladimir Zaborovsky, and Sergey Kupreenko. Access Isolation Mechanism Based On Virtual Connection Management In Cloud Systems // 13th International Conference on Enterprise Information Systems (ICEIS 2011), pp. 371 – 375

[13] V. Zaborovsky, V. Mulukha, A. Silinenko, and S. Kupreenko. Dynamic Firewall Configuration: Security System Architecture and Algebra of the Filtering Rules // Proceedings of The Third International Conference on Evolving Internet – INTERNET 2011, June 19-24, 2011, Luxembourg City, Luxembourg, pp. 40-45

 ISBN: 978-1-61208-204-2

Prototyping TCP Options to Reveal Host Identity in IP Address Sharing Environments

Elie Abdo
France Telecom,
38, rue du General Leclerc
Issy Les Moulineaux, France
e-mails: elie.abdo@orange.com

Mohamed Boucadair
France Telecom
3, rue Clos Courtel
Rennes, France
mohamed.boucadair@orange.com

Jaqueline Queiroz
France Telecom
38, rue du General Leclerc
Issy Les Moulineaux, France
jaqueline.queiroz@orange.com

***Abstract*—Internet Service Providers must maintain the delivery of IPv4 services during the forthcoming IPv6 transition period. For this purpose, Service Providers are likely to deploy address sharing mechanisms. However, address sharing techniques raise specific issues such as the difficulty to distinguish unambiguously different hosts sharing the same public IPv4 address. To mitigate some of the encountered issues, HOST_ID TCP Option has been proposed as a means to reveal the identity of a host when address sharing is deployed by Internet service providers. If no HOST_ID is revealed to remote servers, all subscribers sharing the same IP address will be impacted by a misbehaving user. This paper documents implementation and testing results of HOST_ID TCP Option. Linux kernel and Carrier Grade NAT have been ported to support the ability to inject HOST_ID Options while iptables module has been modified to interpret the information conveyed in HOST_ID and also to enforce dedicated policies.**

Keywords- address sharing; HOST_ID; TCP Option.

I. INTRODUCTION

The explosion of the Internet in the past few years has accelerated the exhaustion of IPv4 global addresses. While only IPv6 deployment can solve IPv4 address shortage, service providers are required to maintain their IPv4 service offerings using the remaining global IPv4 addresses. To do so, large scale address sharing techniques should be implemented to serve a large number of subscribers with a limited IPv4 address space. However, when different hosts are sharing the same IPv4 address, several issues are likely to be encountered [5]. These issues impact subscribers, service providers and content providers: e.g. many services will fail to work, legitimate users will share the reputation of misbehaving users or 'spammers', etc. A use case example would be, when a user is misbehaving, the shared IPv4 address will be reported on a blacklist by the content provider; the access could be then denied for all subscribers sharing that IP address. More issues encountered with IPv4 sharing techniques are detailed in [5].

To mitigate some of these issues, [2] identifies a list of solutions aiming to reveal extra information that must be unique for each host sharing the same IPv4 address: this information is called HOST_ID.

If HOST_ID is revealed to remote servers, hosts are not identified by the sole use of IPv4 address but the identification will be based on the combination of the external IPv4 address and the HOST_ID information. To make such distinction possible, the HOST_ID must be unique to each user who shares the same global IPv4 address (no need to be globally unique). This information can be an IPv6 prefix address, the private source IPv4 address, etc.

The HOST_ID can be injected by the address sharing function (e.g., CGN (Carrier Grade NAT)) which is transparent to the host. Another alternative to reduce potential CGN performance degradation is to let the Customer Premises Equipment (CPE) or the host injecting the HOST_ID information; the CGN only verifies the content of the Option.

The HOST_ID can be leaked in multiple levels of an IP packet. The IP Identification (IP-ID) field of IP header may be used to hold HOST_ID but this will require a dedicated channel to inform servers whether this header is conveying HOST_ID or not. HOST_ID can be put at IP level as a new IP Option (e.g., [13]); however this alternative is unlikely because IP options are not processed by intermediate routers [4]. [3] defines HOST_ID solution as being a new TCP Option suitable for all TCP-based applications. Other proposals such as Proxy Protocol [12] and HIP (Host Identity Protocol [9]) require modifications at both servers and CGN; otherwise, connection could not be established. Another HOST_ID proposal consists of sending the HOST_ID information at the application level (e.g., HTTP header (XFF or Forwarded-For [10]); this proposal solves the issue for HTTP traffic only.

Defining HOST_ID as a TCP Option is superior to XFF. This paper focuses on this alternative.

This paper defines an extended HOST_ID TCP Option and provides experimentation results of this TCP Option. Linux Kernel, CGN and iptables modules have been ported to support the HOST_ID TCP Option. Appropriate validation effort has been conducted to achieve the following objectives:

 ISBN: 978-1-61208-204-2

- Assess the validity of the HOST_ID TCP Option approach.
- Evaluate the impact on the TCP stack to support the HOST_ID TCP Options.
- Improve filtering and logging capabilities based upon the contents of the HOST_ID TCP Option. This means the enforcement of various policies based upon the content of the HOST_ID TCP Option at the server side: Log, Deny, Accept, etc.
- Assess the behaviour of legacy TCP servers when receiving a HOST_ID TCP Option.
- Assess the success ratio of TCP communications when a HOST_ID TCP Option is received.
- Assess the impact of injecting a HOST_ID TCP Option on the time it takes to establish a connection.
- Assess the performance impact on the CGN device that has been configured to inject the HOST_ID Option. DS-Lite CGN is used (see Section III)

The remainder of this paper is organized as follows. An overview of the HOST_ID TCP Option is described in Section II. Then, Section III sketches at a glance an overview of DS-Lite technique. Section IV highlights the required Linux Kernel modifications to support the HOST_ID TCP Option. Section V describes the testing conducted to evaluate the behavior of legacy TCP servers and connection delays when servers receive HOST_ID Options. Section VI presents the modifications of the CGN to inject HOST_ID TCP Option. Finally, Section VII illustrates the policies to be enforced at servers' side to make use of the HOST_ID and therefore, to mitigate identification issues introduced by address sharing mechanisms.

II. FOCUS ON HOST_ID TCP OPTION

The initial idea of defining a TCP Option to convey a HOST_ID was defined in [14]. Nevertheless, the format of that Option does not allow covering various use cases (such as the load-balancer use case). A new TCP 10-byte Option is proposed to meet this requirement (Figure 1). This Option offers similar features than "Forwarded-For" HTTP header [10].

- KIND number
- Lifetime (4 bits) indicates the validity lifetime of the enclosed data, the following values are supported:
  - 0: Permanent
  - >0: Dynamic; this value indicates the validity time.
- Origin (4 bits) indicates the origin of the data conveyed in the data field. The following values are supported:
  - "0": Internal Port
  - "1": Internal IPv4 address
  - "2": Internal Port and Internal IPv4 address
  - "3": IPv6 Prefix
  - ">3": No particular semantic

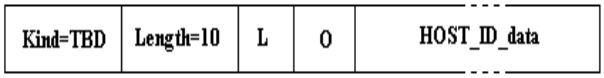


Figure 1: Format of HOST_ID TCP Option

- HOST_ID_data (7 bytes) depends on the Origin field; padding is then required as data of different length can be added.

Two modes of sending HOST_ID are supported: (1) The SYN mode in which the HOST_ID TCP Option is sent in SYN packets and (2) the ACK mode which requires to define a new 2-byte long TCP Option called HOST_ID_ENABLED and which is characterized as follows: The address sharing function injects the HOST_ID_ENABLED TCP Option in a SYN packet. If the remote server supports the HOST_ID Option, it must return the HOST_ID_ENABLED in the SYNACK packet. Then, the TCP client sends an ACK including the HOST_ID TCP Option.

III. DS-LITE AT A GLANCE

DS-Lite [3] address sharing technique is enabled in the validation platform to conducted testing on CGN (Figure 2). The DS-Lite model is composed of two components: (1) DS-Lite CPE (Customer Premises Equipment) with a B4 (Basic Bridging BroadBand) element and (2) one or several AFTR (Address Family Transition Router) elements, deployed in the network. The DS-Lite combines two techniques: IPv4-in-IPv6 tunnel encapsulation/de-capsulation that is performed at the B4 and the AFTR elements and the NAPT function [11] implemented at the AFTR (i.e., CGN).

IV. LINUX KERNEL MODIFICATIONS

The objective of Linux Kernel modifications is to support the HOST_ID Option in the SYN mode and then conduct appropriate testing to assess the behavior of top 100,000 legacy HTTP servers, a list of FTP servers, Telnet and SSH services when the HOST_ID TCP Option is conveyed to the servers. The Kernel modified machine will be used afterwards when the HOST_ID Options injection is performed by the host; the address sharing function (see Section VI) only verifies the Options' content validity. This implementation has the advantage to avoid overloading the CGN.

TCP stack of the Linux Kernel has been modified to support HOST_ID TCP Option. Subsequently, recompiling the machine allows the machine to inject the HOST_ID Options and then drive the testing. Through these modifications, we can inject the HOST_ID TCP Options in all SYN packets.

To configure the different HOST_ID Data forms, we defined new Kernel sysctl (system control) variables as HOST_ID injection impacts Kernel TCP driver which allows changing the configuration without rebooting the machine under test. Kernel modifications and recompilation have been made using Fedora and Debian Linux distributions, on

 ISBN: 978-1-61208-204-2

different Kernel versions. The following configurations options have been implemented:

- Enable/Disable injecting the TCP Options
- Support HOST_ID and HOST_ID_ENABLED
- Data form is configurable and can inject: Source IPv6 address or the first 56 bits of the IPv6 address, Source IPv4 address, Source port number, Source IPv4 address and Source port number.

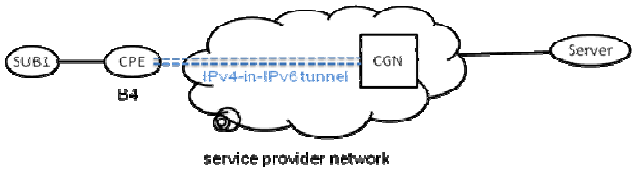


Figure 2: The DS-Lite Architecture

V. EXPERIMENTATION AND RESULTS

The testbed setup is shown in Figure 3. Two hosts are directly connected to the Internet: *Host1* is a machine which does not support HOST_ID while *Host2* is a modified machine (i.e., patched with the updated Kernel described in Section IV). We run the testing on both machines in parallel for all the HOST_ID TCP Options. The results obtained for *Host1* are used as reference for measurements. In this testing, we first connected the hosts to an enterprise network and then to two ISPs networks to make sure that HOST_ID Options are not stripped. For this purpose, we configured a local server with a public IPv4 address to make it reachable from the Internet.

This configuration is then used to assess the behavior of the top 100,000 websites when a HOST_ID Option is enabled. Also FTP, Telnet and SSH services have been tested.

We coded a Python robot as the traffic generator. The robot automates the retrieval of objects identified by URLs, and returns different connection information (different timing measures). The retrieval of pages is based upon Pycurl, a Python interface of libcurl. The robot consists of two programs. The first one takes an URL as an input parameter, performs the DNS lookup and then tries to connect to the corresponding machine and retrieves the objects identified by the URL. It returns either different time values and connection status or an error message with the source of the error in case of connection failure (e.g., DNS error).

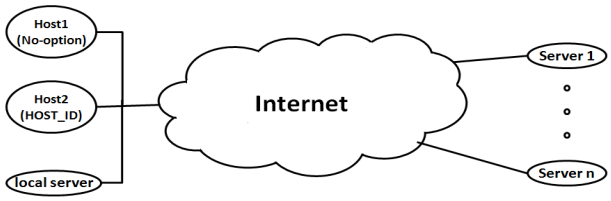


Figure 3: Machines directly connected to Internet

The TCP connection establishment time is calculated as the difference between the CONNECT_TIME and NAMELOOKUP_TIME where NAMELOOKUP_TIME is the time it took from the start until name resolution is completed and CONNECT_TIME is the time it took from the start until the connection to the remote host (or proxy) is completed. The second program prints URLs to an output file with the corresponding connection time. If connection could not be established, the program returns an error message with the corresponding error type.

We performed the testing in parallel on the two machines (Figure 3) for all the HOST_ID TCP Options. We repeated the cycle several times for each Option in different days. Then, we calculated TCP sessions establishment delays as average of testing repetitions. Also we computed sessions' success ratio and compared the results using the no-Option testing results (used as reference). The local server, shown in Figure 3, is used to verify HOST_ID TCP Options are correctly injected.

We considered various combinations of Data revealed in the HOST_ID TCP Options (see Section II): source port, IPv4 address, source port: IPv4 address, 56 bits of IPv6 Prefix and HOST_ID_ENABLED.

SSH and Telnet sessions have been successfully initiated for all HOST_ID TCP Options with the local server.

Below are reported both the success ratio and the average time to establish the TCP session a connection for HTTP and FTP services.

A. HTTP

The same results were obtained for hosts connected to an enterprise network and to networks of two ISPs. These results are synthesized in Tables 1.

TABLE I. HTTP RESULTS – CUMULATED SUCCESS RATIO

	No-Option	HOST_ID	Failures	Failure Ratio
1-1000	995	995	0	0.000%
1001-2000	992	991	1	0.101%
2001-3000	986	986	0	0.000%
3001-4000	991	990	1	0.101%
4001-5000	993	993	0	0.000%
5001-6000	996	996	0	0.000%
6001-7000	995	994	1	0.101%
7001-8000	984	983	1	0.102%
8001-9000	993	992	1	0.101%
9001-10000	991	991	0	0.000%
10001-20000	9785	9776	9	0.092%
20001-30000	9764	9746	18	0.184%
30001-40000	9778	9766	12	0.123%
40001-50000	9757	9746	11	0.113%
50001-60000	9771	9761	10	0.102%
60001-70000	9761	9751	10	0.102%
70001-80000	9744	9736	8	0.082%
80001-90000	9739	9730	9	0.092%
90001-100000	9736	9719	17	0.175%
1-100000	97751	97642	109	0.112%

For the top 100,000 websites [15], connection failures occurred for 2249 HTTP sites. These failures were reported

 ISBN: 978-1-61208-204-2

as being caused by DNS issues, connection timeouts (e.g., servers down), connection resets by peers, connection problems and empty replies from servers. The 2249 failures occur, whether HOST_ID Options are injected or not

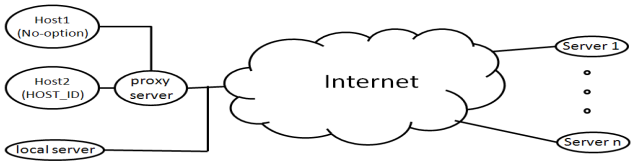


Figure 4: Proxy Server

The same results were obtained for HOST_ID and HOST_ID_ENABLED. The connection failures' ratio for HOST_ID_ENABLED is 0,105% while it is 0.112% for the HOST_ID Option in comparison with total established connections (when no HOST_ID Option is present). These results were obtained for all the HOST_ID TCP Options (source port, IPv6 prefix, etc.). When any HOST_ID TCP Option is conveyed, 103 servers did not respond; however when no Option is injected, all these servers responded normally. For six additional servers which did not respond: Three servers did not respond to the SYN packets sent by the host and three servers responded with malformed and erroneous SYN/ACK packets so connection is dropped by host when receiving the SYN/ACK packet. When HOST_ID_ENABLED is enabled, malformed SYN/ACKs were received by the host too, but these packets were error-free (a long series of NOP Options). This justifies the connection success for these two Options.

The results show that including a HOST_ID TCP Option does not systematically imply an extra delay for the establishment of the TCP session.

When an HTTP proxy is in the path (Figure 4), it strips the HOST_ID TCP Options. The testing has been conducted by verifying packets' content received by the local server: no HOST_ID Options were present in the received SYN packets at the server despite being sent by the host.

B. FTP

Two combinations of the HOST_ID TCP Option have been tested: (1) HOST_ID (source port) and (3) HOST_ID (source port: IPv4 address).

A list of 5591 FTP servers [16] has been used to conduct these tests. Among this list, only 2045 were reachable: failure to reach 942 servers due to connection timeout, failure to reach 1286 servers due to DNS errors, failure to reach 717 servers because access was denied, connection error with 500 servers, failure to reading response from 81 servers and bad response from 20 servers. When HOST_ID TCP Options are injected, 9 FTP servers did not respond to the SYN packets sent by the host. The connection failure distribution is presented in Table 2.

The results show that the sending a HOST_ID TCP Option does not systematically imply an average extra delay for the establishment of the TCP sessions with remote FTP servers. Based upon the average of the session establishment time with the 2045 FTP sites, no extra delay is observed when the HOST_ID TCP Option is injected.

TABLE II. FTP RESULTS – CUMULATED SUCCESS RATIO

	No-Option	HOST_ID	Failures	Failure Ratio
1-100	100	100	0	0,00%
101-200	100	99	1	1,00%
201-300	100	99	1	1,00%
301-400	100	100	0	0,00%
401-500	100	100	0	0,00%
501-600	100	100	0	0,00%
601-700	100	100	0	0,00%
701-800	100	100	0	0,00%
801-900	100	99	1	1,00%
901-1000	100	99	1	1,00%
1001-2000	1000	995	5	0,50%
2000-2045	45	45	0	0,00%
Total	2045	2036	9	0,44%

VI. ISC AFTR MODULE MODIFICATIONS

This section presents the modifications to support the HOST_ID functionalities by the ISC-AFTR module [7].

All privately-addressed IPv4 packets sent from DS-Lite serviced hosts are sent to an AFTR device where an isc_aftr daemon program is responsible for processing received packets. The NAPT function is performed by the AFTR. To activate/de-activate ISC-AFTR functionalities, e.g., patching TCP MSS values, fix MTU, etc, the corresponding variables must be configured in the 'aftr.conf' configuration file. We modified the ISC-AFTR code in order to support the following functionalities: (1) Inject the HOST_ID TCP Options, (2) Retrieve an existing HOST_ID TCP Option in case this Option is not configured and (3) Check the validity of the integrity of the contents of HOST_ID TCP Option in case the corresponding Option is already present in the SYN packet and at the same time the Option is enabled at the AFTR. We modified the "aftr.c" source code to support the HOST_ID Options functionalities (described above) depending on the configuration variables in "aftr.conf". Modified ISC-AFTR can be configured to inject HOST_ID TCP Option conveying: Source Port Number, Source IPv4 Address, Source IPv4 Address + Source Port Number, 56 bits of the IPv6 Source Address used by the AFTR to identify a tunnel endpoint.

The setup shown in Figure 5 is used to validate the implemented modifications in the ISC-AFTR module. We used the local server in our testing to check the contents of HOST_ID Options held in SYN packets. We also investigated the SYN packets sent by the host. Thereby, we compared the content of the packets sent by the host and those received by the server to judge if the functions implemented at the AFTR are applied properly. All possible combinations of HOST_ID Options sent by the host and HOST_ID Options configured at the AFTR. The AFTR can inject several Options, strip existing Options, check the validity of received Options. The host is a machine supporting HOST_ID TCP Option.

 ISBN: 978-1-61208-204-2

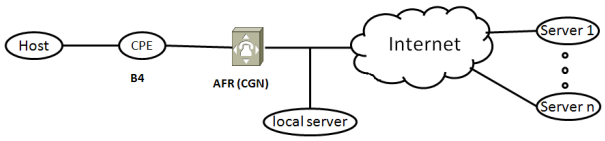


Figure 5: Testbed Setup – DS-Lite CGN environment

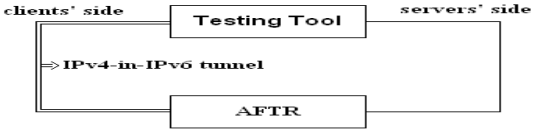


Figure 6: Platform Testbed – AFTR Performance

To conclude about the performance impact of enabling to inject HOST_ID on the CGN, we used a commercial testing product. This tool supports multiple application protocols such as HTTP and FTP for both IPv4 and IPv6 (including encapsulation). The DS-Lite model can be built directly from a port of this product: IPv4 packets are directly encapsulated in an IPv6 tunnel; the client's port emulates hosts and B4 elements at the same time. This port is directly connected to the AFTR tunnel endpoint. The AFTR's IPv4 interface is connected to the testing product server side where servers are assigned IPv4 addresses. The testbed setup of this testing is shown in Figure 6.

The testing client's port is configured with IPv6 addresses representing the B4. The testing tool also supports the DS-Lite "level" where the number of clients connected to each B4 and their addresses are configured. The AFTR address is defined at this level.

In this test group, the total number of B4 elements is 5000 behind; one client is connected to each B4 (in total, 5000 clients are configured). However, the number of active users varies from 10 to 100, 500, 1000 and 5,000 during each testing simulation. We configured five servers with IPv4 addresses. These servers support HTTP and FTP traffic. For each HOST_ID TCP Option, we repeated the testing for a different number of active users (N=10, 100, 500, 1000 and 5,000) and for HTTP and FTP traffic. The HOST_ID Options are injected by the CGN.

The testing duration was about 50 seconds during which the number of active users varies as a function of time: during the first 10s, the number of active users reaches the maximum and remains the same for the next 20 s. Then it decreases to zero during the next 20s. The same testing was also run for FTP traffic. No particular impact on the performance of the CGN (used in our testing) has been observed.

Tables 6 and 7 show some testing statistics showing details about connections' success ratio, latency and other information that can be useful to evaluate the impact of HOST_ID on the CGN (ISC-AFTR). The results clearly show that there is no impact of HOST_ID Options on session establishment success ratio, which is quite similar to the success ratio when packets do not hold Options or when HOST_ID Options are not used. Also, the number of established connections does not decrease when any HOST_ID Option is injected, so the CGN (ISC-AFTR) performance is not impacted by the fact of adding the HOST_ID Options. The HTTP connection latency does not increase when HOST_ID is present if we compare the latency measured at different times for the different Options.

VII. ENFORCE POLICIES AT THE SERVER SIDE

Internet-facing servers should be able to manipulate the HOST_ID information. For illustrating purpose, we modified *iptables* module to enforce policies based on the content of the HOST_ID. The modification of the *iptables* module aims to: strip any existing HOST_ID Option, match any HOST_ID value, log the content of TCP headers including the HOST_ID information, print the HOST_ID rules on screen, drop packets holding a HOST_ID Option and drop packets holding a specific HOST_ID value.

TABLE III. HTTP RESULTS (N=100)

		No Option	HOST_ID	O-Enabled
TCP connection established		1662	1813	1679
TCP SYN sent		1718	1819	1726
Success Ratio		96	99	97
TCP Retries		1577	1783	1576
TCP timeouts		798	934	808
Latency	**t=20s**	1,7	1,9	1,8
	t=30s	3,3	2,25	3,3
	t=50s	5	4,5	5
HTTP throughput		47,56	48,59	48,06
TCP connections Established/s		20,94	21,35	21,19

TABLE IV. HTTP RESULTS (N=5,000)

		No Option	HOST_ID	O-Enabled
TCP connection established		1576	1796	1998
TCP SYN sent		1794	2009	2262
Success Ratio		87	89	88
TCP Retries		3018	3013	3149
TCP timeouts		1167	1213	1417
Latency	**t=20s**	2,2	2,2	2,5
	t=40s	3,7	3,3	3
	t=60s	7,8	7	5,6
HTTP throughput		45	51,45	57,2
TCP connections Established/s		19,8	22,45	25,05

We built a specific Kernel module to apply HOST_ID matching rules on the packets passing through the network interfaces. This module compares the HOST_ID Options' values hold by packets with the HOST_ID values specified in the *iptables* rule table: when a packet matches the HOST_ID's range, the corresponding rule will be applied for this packet. After updating the iptables package with the required HOST_ID libraries, we enforced and tested different HOST_ID policies at the server side. Testbed

 ISBN: 978-1-61208-204-2

configuration shown in Figure 5 is used for the testing. The AFTR supports injecting HOST_ID Options and iptables modules have been patched at the local server. Logging is performed only for received SYN packets. A specific file is generated for that purpose.

To strip a given HOST_ID Option, TCPOPTSTRIP rule must be applied. The verification consists in logging and then checking the headers of the SYN packets, precisely the TCP Options: *e.g.*, the following rules must be enforced to strip HOST_ID from a received SYN packet:

```
iptables -t mangle -A INPUT -j TCPOPTSTRIP -p tcp --
    strip-options hostid
iptables -A INPUT -j LOG --log-tcp-options -p tcp --syn
```

The first rule applies for the mangle table and allows stripping HOST_ID whose role is to remove Option and replaces them by NOP Options (NOP=No Operation=0x01). The second rule enables the logging of SYN packets with the corresponding TCP Options. After applying these rules (i.e., to strip and log HOST_ID) on the local server, we tried to access the local server's pages from the host. We repeated the testing several times and a different HOST_ID Option is enabled by the AFTR each time. Then the "iptables.log" file is checked: only one SYN packet is logged with 4 bytes stripped out in the TCP Option part. All IPv4 packets going through the AFTR are also logged to compare with the server's logged stripped packets. The comparison of the SYN packets logged by the server with the SYN packets sent by the AFTR clearly shows that the stripped Option is HOST_ID. The remote server should be able to track connections coming from different clients; it should log packets headers including the HOST_ID TCP Option information. This is implemented owing to a simple command:

```
iptables -A INPUT -j LOG --log-tcp-options -p tcp --syn
```

To log packets matching a given HOST_ID value or range of values, the following rule must be enforced:

```
iptables -A INPUT -p tcp --syn -m hostid --hostid
  value[:value] -j LOG --log-tcp-options
```

This command matches the HOST_ID values conveyed in SYN packets with the specific value [or the specific range of values] determined by the configured rule. The value to match for HOST_ID is the content of HOST_ID_Data.

When the HOST_ID Option is injected by the CGN, if the data field value corresponds to the *iptables* value (or range of values), the packet header is logged. Otherwise, if the HOST_ID data is out of range or the packet does not hold the HOST_ID Option, the packet is not logged. To drop packets matching HOST_ID value (or a range of values), the following command must be executed:

```
iptables -A INPUT -p tcp --syn -m hostid --hostid value
  [:value] -j DROP
```

The HOST_ID Option is enabled at the CGN level. After applying the previous rule, hosts try to access HTTP content of the local server. A host sends SYN packets but the server does not respond. Because this packet matches the *iptables* matching value, the corresponding rule is applied to the SYN packets: a SYN packet is dropped so the host does not receive any packet in return. While the host is still trying to retrieve pages by sending SYN packets, the command '*iptables –F*' will flush all *iptables* rules. Once applied, the host establishes successfully a TCP session with the server.

VIII. CONCLUSION AND NEXT STEPS

Both implementations of HOST_ID Option at the Linux Kernel TCP stack and the CGN demonstrated that HOST_ID support is feasible and not complex. Testing, conducted using different testbed configurations, has led to: no impact is induced by injecting HOST_ID TCP Options on TCP session establishment delay, only few HTTP servers did not respond when HOST_ID Option was present. The success ratio is not significantly impacted, FTP session success ratio is slightly impacted by the presence of HOST_ID Options (0.44% of connection failures have been observed for 2045 servers), no impact of HOST_ID Options on the performance of the CGN (ISC-AFTR), SSH and Telnet sessions were established successfully, filtering and logging the incoming connections based upon the content of HOST_ID Option information were applied and tested successfully. Further work will focus on security implications of revealing a host identifier.

REFERENCES

[1] M. Bagnulo, P. Matthews and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.

[2] M. Boucadair, J. Touch, P. Levis and R. Penno, "Analysis of Solution Candidates to Reveal a Host Identifier in Shared Address Deployments", draft-ietf-intarea-nat-reveal-analysis, February 2012.

[3] A. Durand, R. Droms, J. Woodyatt and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, August 2011.

[4] R. Fonseca, G. Porter, R. Katz, S. Shenker and I. Stoica, "IP options are not an option", UCB/EECS- 2005-24, 2005.

[5] M. Ford, M. Boucadair, A. Durand, P. Levis and P. Roberts, "Issues with IP Address Sharing", RFC 6269, June 2011.

[6] M. Honda, Y. Nishida, C. Raiciu, A. Greenhalgh, M. Handley and H. Tokuda,, "Is it still possible to extend TCP?", November 2011, http://nrg.cs.ucl.ac.uk/mjh/tmp/mboxes.pdf.

[7] ISC AFTR, http://www.isc.org/software/aftr [retrieved: June, 2012].

[8] A. Medina, M. Allman and S. Floyd, "Measuring the Evolution of Transport Protocols in the Internet", ACM CCR, 35(2):37–52, 2005.

[9] R. Moskowitz, P. Nikander, P. Jokela and T. Henderson, "Host Identity Protocol", RFC 5201, April 2008.

 ISBN: 978-1-61208-204-2

[10] A. Petersson and M. Nilsson, “Forwarded HTTP Extension”, draft-ietf-appsawg-forwarded-for, January 2012.
[11] P. Srisuresh and K. Egevang, “Traditional IP Network Address Translator”, RFC 3022, January 2001.
[12] W. Tarreau, “The Proxy protocol”, November 2010, http://haproxy.1wt.eu/download/1.5/doc/proxy-protocol.txt [retrieved: June, 2012].
[13] Y. Wu, H. Ji, Q. Chen and T. Zou, “IPv4 Header Option For User Identification In CGN Scenario”, draft-chen-intarea-v4-uid-header-option, March 2011.
[14] A. Yourtchenko and D. Wing, “Revealing hosts sharing an IP address using TCP option”, draft-wing-nat-reveal-option, December 2011.
[15] Alexa, http://www.alexa.com/topsites [retrieved: June, 2012]
[16] FTP sites, ftp-sites.org [retrieved: June, 2012]

 ISBN: 978-1-61208-204-2

Investigation of Inadequate Multiple Account Users in a Q&A Site by Considering Deviations of Answer Submission Order

Kenji Umemoto, Naoki Ishikawa, Yasuhiko Watanabe, Ryo Nishimura, Yoshihiro Okada
Ryukoku University
Seta, Otsu, Shiga, 520-2194, Japan
Email: t11m074@mail.ryukoku.ac.jp, t10m096@mail.ryukoku.ac.jp,
watanabe@rins.ryukoku.ac.jp, r_nishimura@afc.ryukoku.ac.jp, okada@rins.ryukoku.ac.jp

***Abstract*—Some users in a question and answer (Q&A) site use multiple user accounts and attempt to manipulate communications in the site. In order to detect these inadequate multiple account users precisely, it is important to investigate them from various points of view. In this paper, we investigate suspicious users from the viewpoint of deviations of answer submission order and discuss the reasons why and how the deviations occurred. The results of this study will give us a chance to investigate purposes and behaviors of inadequate multiple account users in a Q&A site.**

Keywords- *multiple account; Q&A site; deviation; submission order; credibility.*

I. INTRODUCTION

In these days, many people use question and answer (Q&A) sites, where users share their information and knowledge. Q&A sites offer greater opportunities to users than search engines in the following points:

1) Users can submit questions in natural and expressive sentences, not keywords.
2) Users can submit ambiguous questions because other users give some supports to them.
3) Communications in Q&A sites are interactive. Users have chances to not only submit questions but give answers and, especially, join discussions.

As a result, Q&A sites are promising media. One of the essential factors in Q&A sites is anonymous submission. In most Q&A sites, user registrations are required for those who want to join the Q&A sites. However, registered users generally need not reveal their real names to submit messages (questions, problems, answers, comments, etc.). It is important to submit messages anonymously to a Q&A site. This is because anonymity gives users chances to submit messages without regard to shame and reputation. However, some users abuse the anonymity and attempt to manipulate communications in a Q&A site. For example, some users use multiple user accounts and submit messages to a Q&A site inadequately. Manipulated communications discourage other submitters, keep users from retrieving good communication records, and decrease the credibility of the Q&A site. As a result, it is important to detect users suspected of using multiple user accounts and manipulating communications in a Q&A site. In this case, identity tracing based on user accounts is not effective because inadequate users are likely to hide their true identity to avoid detection. A possible solution is authorship identification based on analyzing stylistic features of messages. In recent years, a large number of studies have been made on authorship identification [1] [2] [3] [4] [5], however, few researchers addressed the identification issues of authors suspected of using multiple user accounts and manipulating communications in a Q&A site. To solve this problem, we proposed methods of detecting two kinds of inadequate multiple account users:

- Multiple account users suspected of submitting questions and their answers repeatedly [6].
- Multiple account users suspected of submitting many answers to the same question repeatedly [7].

However, little is known about the purposes and methods of inadequate multiple account users. As a result, it is important to investigate these inadequate multiple account users from various points of view. One example is whether these inadequate users use multiple user accounts in different ways. Suppose that one user intends to advocate or justify his/her submitted answer and uses multiple user accounts as follows:

- A main account.
- Secondary accounts for advocating or justifying his/her answer submitted by the main account.

In this case, the deviation of answer submission order is likely to occur. As a result, we investigate user pairs who had large deviations of answer submission order and discuss the reasons why and how the deviations occurred.

By the way, we should notice that it is difficult to verify the credibility of our investigation. This is because there is no reliable information about users who used multiple user accounts and manipulated communications in Q&A sites. In order to discuss the credibility of our investigation, we show the results of our investigation in detail. The results of this study will give us a chance to investigate purposes and behaviors of users who use multiple user accounts and intend to manipulate communications in a Q&A site.

 ISBN: 978-1-61208-204-2

Table I
THE NUMBERS OF USERS AND THEIR SUBMISSIONS TO PC CATEGORY, SOCIAL ISSUES CATEGORY, AND ALL 286 CATEGORIES IN YAHOO! CHIEBUKURO (FROM APRIL/2004 TO OCTOBER/2005).

category	N_{qst}	U_{qst}	N_{ans}	U_{ans}	NP_{qst}	UP_{qst}	NP_{ans}	UP_{ans}	$UP_{userpair}$	N_{mfe}
PC	171848	43493	474687	27420	124210	36771	427049	26634	463438	67846
social issues	78777	13259	403306	25766	70886	12238	395415	25552	828812	74781
all 286 categories	3116009	165064	13477785	183242	2576718	150835	12938494	179773	23053308	–

N_{qst} and N_{ans} are the numbers of questions and answers, respectively. U_{qst} and U_{ans} are the numbers of users who submitted questions and answers, respectively. NP_{qst} is the number of questions which had two or more answers, and NP_{ans} is the number of answers submitted to questions which had two or more answers. UP_{qst} is the number of questioners who submitted questions which had two or more answers, and UP_{ans} is the number of answerers who submitted answers submitted to questions which had two or more answers. $UP_{userpair}$ is the number of user pairs who submitted answers to one or more of the same questions. N_{mfe} is the total number of each user's answers which were submitted with his/her most frequently encountered user in the category.

This paper is organized as follows. Section II describes some related works. Section III explains Yahoo! chiebukuro, the data of which we used for observation and examinations. Section IV describes submissions by using multiple user accounts in Q&A sites and deviation of answer submission order. Section V proposes a detection method of too large deviations of answer submission order. Section VI shows the experimental results and discussions. Section VII concludes this study.

II. RELATED WORKS

One of the essential factors in the Internet is anonymity. Joinson discussed the anonymity in the Internet from various points of view [8]. In these days, many users abuse the anonymity: they use multiple user accounts inadequately and submit inadequate messages, such as, deceptive opinion spams. In recent years, a large number of studies have been made on authorship identification [1] [2] [3] [4] [5], however, few researchers addressed the identification issues of authors suspected of using multiple user accounts and manipulating communications in the Internet. One of the difficulties of this problem is that we did not have sufficient number of examples of inadequate multiple account users. To solve this problem, some researchers tried to extract inadequate submissions by using heuristic methods based on text similarities and ranking results [9] [10]. On the other hand, Ott et al. pointed that these heuristic methods were insufficient to detect inadequate submissions precisely, and showed they could detect inadequate submissions precisely when they used large number of examples of inadequate submissions [11]. However, Ott et al. obtained examples of inadequate submissions by using Amazon Mechanical Turk. The examples of inadequate submissions created by workers in Amazon Mechanical Turk have the following problems.

- Little is known about the purposes and methods of inadequate submissions. As a result, it is possible that their instructions to workers in Amazon Mechanical Turk were insufficient.
- There are unreliable workers in Amazon Mechanical Turk [12].

As a result, it is important to obtain inadequate submissions from the Internet. To solve this problem, we proposed methods of detecting inadequate multiple account users and their submissions [6] [7]. However, as mentioned, little is known about the purposes and methods of inadequate multiple account users. As a result, it is important to investigate these inadequate multiple account users and their inadequate submissions from various points of view.

III. YAHOO! CHIEBUKURO

In this study, we used the data of Yahoo! chiebukuro for observation, data training, and examination. The data of Yahoo! chiebukuro was published by Yahoo! JAPAN via National Institute of Informatics in 2007 [13]. This data consists of about 3.11 million questions and 13.47 million answers which were posted on Yahoo! chiebukuro from April/2004 to October/2005. In the data, each question has at least one answer because questions with no answers were removed. In order to avoid identifying individuals, user accounts were replaced with unique ID numbers. By using these ID numbers, we can trace any user's questions and answers in the data. Table I shows the numbers of users and their submitted messages (questions and answers) to PC category, social issues category, and all 286 categories in the data. Many users have other users who submitted answers to one or more of the same questions with them. We will use the term *most frequently encountered user* of a certain user to refer to a user who submitted answers to the same questions most frequently with the user.

[most frequently encountered user] Suppose $\mathbb{U}$ is a set of users who submitted answers to the same questions with user i. The most frequently encountered user of user i, that is, $mfe(i)$ is defined as follows:

$$mfe(i) = \arg\max_{j \in \mathbb{U}} N_{ans\_together}(i, j)$$

where $N_{ans\_together}(i, j)$ is the number of questions to which user i and j submitted answers together.

N_{mfe} in Table I is the total number of each user's answers which were submitted with his/her most frequently encountered user. As a result, it is expected that, when a user

submitted 100 answers to social issues category, the user and his/her most frequently encountered user submitted

$$\frac{N_{mfe}}{N_{ans}} \times 100 = \frac{74781}{403306} \times 100 = 18.5$$

answers together to the same questions.

Furthermore, the following kinds of information are described in the data.

- Submission time of question.
- Submission time of answer.
- Problem resolution time.

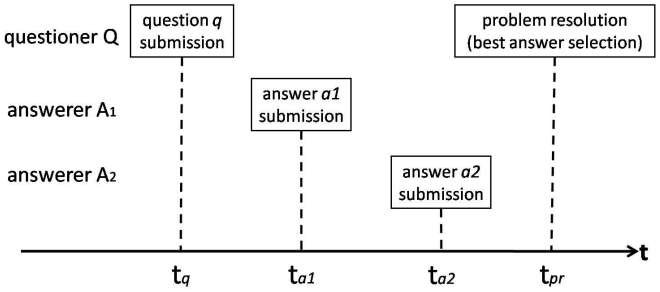
Figure 1 shows an example of a series of events that occur after a questioner submits his/her question to Yahoo! chiebukuro. In Figure 1, the submission time of question q is t_q. Also, the submission time of answer a_1 and a_2 are t_{a1} and t_{a2}, respectively. Finally, the problem resolution time of question q is t_{pr}. At the problem resolution time, questioner Q stopped accepting answers and determined which answer was the best answer. By using these kinds of time information, we measured two kinds of submission time lags:

- Submission time lags between questions and their answers (e.g., $t_{a1} - t_q$ and $t_{a2} - t_q$ in Figure 1).
- Submission time lags between answers submitted to the same question (e.g., $t_{a2} - t_{a1}$ in Figure 1).

Figure 2 shows the cumulative relative frequency of the submission time lags between questions and their answers in the data of Yahoo! chiebukuro. Also, Figure 3 shows the cumulative relative frequency of the submission time lags between answers submitted to the same question. As shown in Figure 3, the median of the submission time lags between answers submitted to the same question in social issues category was greater than those of PC category and all 286 categories. In social issues category, there were many answers criticizing or against previous answers. As a result, many answerers in this category made and submitted answers after they read other answers to the same question. We think this is one of the reasons why the median of the submission time lags between answers submitted to the same question in social issues category was greater than those of PC category and all 286 categories.

IV. Submissions by using multiple user accounts

There are many reasons why users in a Q&A site use multiple user accounts. First, we discuss a proper reason. In Yahoo! chiebukuro, users need not reveal their real names to submit their questions and answers. However, their submissions are traceable because their user accounts are attached to them. Because of this traceability, we can collect any user's submissions and some of them include clues of identifying individuals. As a result, to avoid identifying individuals, it is reasonable and proper that users change their user accounts or use multiple user accounts. However,



Questioner Q submitted question q at t_q. Also, answerer A_1 and A_2 submitted their answers at t_{a1} and t_{a2}, respectively. Finally, questioner Q stopped accepting answers and determined which answer was the best answer at t_{pr}.

Figure 1. An example of a series of events that occur after a questioner submits his/her question to Yahoo! chiebukuro.

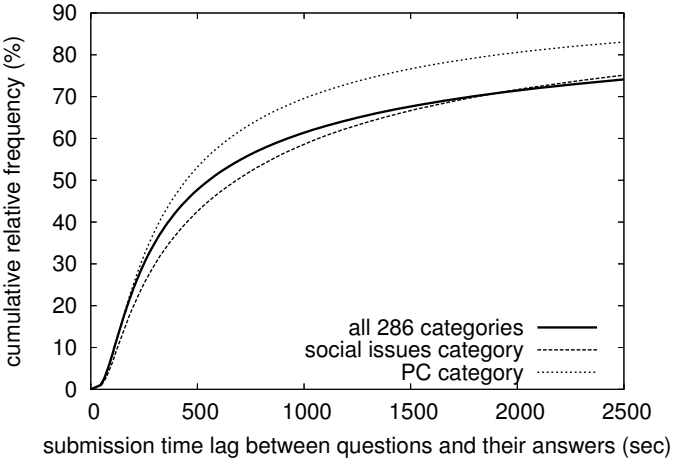


Figure 2. The cumulative relative frequency of the submission time lags between questions and their answers in social issues category, PC category, and all 286 categories of the data of Yahoo! chiebukuro.

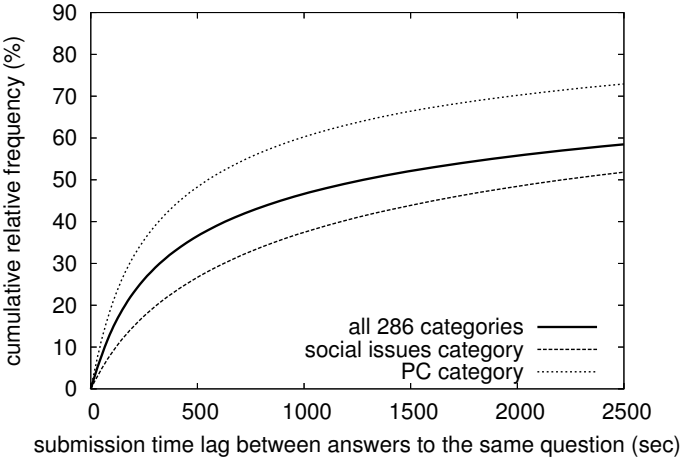


Figure 3. The cumulative relative frequency of the submission time lags between answers submitted to the same question in social issues category, PC category, and all 286 categories of the data of Yahoo! chiebukuro.

 ISBN: 978-1-61208-204-2

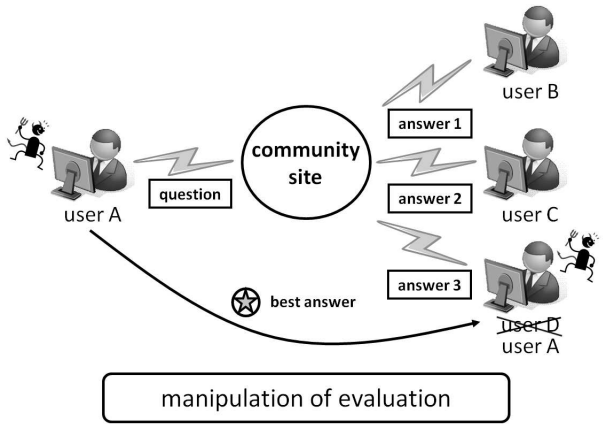


Figure 4. An example of TYPE QA submissions.

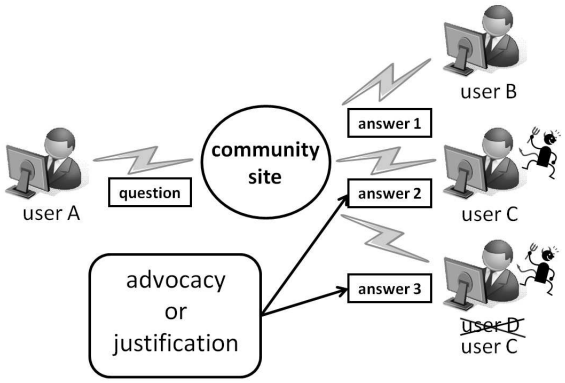


Figure 5. An example of TYPE AA submissions.

the following types of submissions by using multiple user accounts are neither reasonable nor proper.

TYPE QA One user submits a question and its answer by using multiple user accounts, as shown in Figure 4. In Figure 4, user A submits a question and its answer by using two user accounts.
We think that the user intended to manipulate the submission evaluation. For example, in Yahoo! chiebukuro, each questioner is requested to determine which answer is best and give a *best answer* label to it. These evaluations encourage answerers to submit new answers and increase the credibility of the Q&A site. We think, the user repeated this type of submissions because he/she wanted to get many best answer labels and be seen as a good answerer.

TYPE AA One user submits two or more answers to the same question by using multiple user accounts, as shown in Figure 5. In Figure 5, user C submits two answers by using two user accounts. We think that the user intended to dominate or disrupt communications in the Q&A site. To be more precise, the user intended to control communications by advocating or justifying his/her opinions, or disrupt communications by submitting two or more inappropriate messages.

These two types are not all types of inadequate submissions. However, these kinds of submissions seriously disrupt communications in a Q&A site, discourage other submitters, keep users from retrieving good communication records, and decrease the credibility of the Q&A site. As a result, it is important to detect these kinds of inadequate submissions. To solve this problem, we proposed methods of detecting multiple account users suspected of repeating TYPE QA and TYPE AA submissions [6] [7]. However, little is known about the purposes and methods of inadequate multiple account users. As a result, it is important to investigate these inadequate multiple account users from various points of view. In this study, we investigate the purposes and methods of inadequate multiple account users who use multiple user accounts in different ways.

Inadequate users repeating TYPE QA submissions are likely to use multiple user accounts as follows:

- Main accounts.
- Secondary accounts for submitting questions and manipulating evaluations of main accounts.

However, little is known whether inadequate users repeating TYPE AA submissions use multiple user accounts somehow. To solve this problem, it is important to detect inadequate multiple account users who used multiple user accounts in different ways and repeated TYPE AA submissions, and investigate the purposes and methods of them.

If one user uses multiple user accounts in different ways, some deviations are likely to occur. Suppose that one user intends to advocate or justify his/her submitted answer and uses multiple user accounts as follows:

- A main account.
- Secondary accounts for advocating or justifying his/her answer submitted by the main account.

In this case, the user is likely to submit first answers from his/her main account and other answers from their secondary accounts. In order to detect this kind of inadequate users, we introduce *deviation of answer submission order*.

[deviation of answer submission order] Suppose user i and user j submitted their answers to the same N questions, and, user i submitted N_i answers earlier than user j and user j submitted N_j answers earlier than user i. The deviations of answer submission order of this user pair is $N_i - N_j$.

As a result, in this study, we investigate user pairs who had large deviations of answer submission order and discuss the reasons why and how the deviations occurred.

In Yahoo! chiebukuro, there were many questions the purpose of which was to collect opinions. For example,

 ISBN: 978-1-61208-204-2

(Q) What do you think about Prime Minister Koizumi? He has maintained high approval ratings and does well in his work.

This kind of question often had many answers. Some of them were criticizing or against previous answers. Because of such criticizing submissions, some users were likely to use multiple user accounts and submit new answers for advocating or justifying their previous answers. We think some users used multiple user accounts as follows:

- Main accounts.
- Secondary accounts for advocating or justifying their answer submitted by the main accounts.

This is because it is easy to manage multiple user accounts. When multiple user accounts were used as above, it is easy to avoid submitting new answers which were inconsistent with the previous answers. Inconsistent answers often gave suspicious impressions to others. However, if multiple user accounts were used in this way, the deviation of answer submission order is likely to occur. As a result, in this study, we investigate user pairs who had large deviations of answer submission order and discuss the reasons why and how the deviations occurred.

V. Detection of too large deviations of answer submission order

In order to detect users who were suspected of repeating TYPE AA submissions by using multiple user accounts in different ways, we introduce two ideas. If one user repeated TYPE AA submissions too many times by using two user accounts, user i and user j, it is expected that

(idea 1) user i and user j submit too many answers to the same questions together.

Furthermore, if the user used these two user accounts in different ways, it is expected that

(idea 2) there are too large deviations of answer submission order between user i and user j.

Based on these two ideas, we determine whether users repeated TYPE AA submissions by using multiple user accounts in different ways.

A. Detection of user pairs who submitted too many answers to the same questions

As mentioned, if one person used two user accounts, user i and user j, and repeated TYPE AA submissions in a Q&A site too many times, it is expected that we observe abnormal submissions:

user i submitted abnormally too many answers to the same questions responded by j.

To detect these abnormal submissions, we test one hypothesis: Hypothesis AA.

[Hypothesis AA] If user i did not submit abnormally too many answers to the same questions with user j, we would expect that user i submitted at most $N_{AA}(i)$ answers to the same questions with user j.

$$N_{AA}(i) = \frac{N_{mfe}}{N_{ans}} \times ans(i)$$

where $ans(i)$ is the total number of answers submitted by user i. As shown in Table I, N_{ans} is the total number of answers submitted to the category, and N_{mfe} is the total number of each user's answers which were submitted with his/her most frequently encountered user.

If this hypothesis is rejected by an one-sided binomial test, we determine that user i submitted abnormally too many answers to the same questions with user j.

B. Detection of user pairs who had too large deviations of answer submission order

If one user repeated TYPE AA submissions by using two user accounts, user i and user j, in different ways, it is expected that we observe

too large deviations of answer submission order between user i and user j.

To detect too large deviations of answer submission order between user i and user j, we test one hypothesis: Hypothesis AASO.

[Hypothesis AASO] Suppose that there are $N_{AA}(i,j)$ cases where user i and user j submitted their answers to the same question. If one of these users did not submit answers too many times before the other did, we would expect that there are at most $N_{AASO}(i,j)$ cases where one user submitted his/her answer before the other did.

$$N_{AASO}(i,j) = P_{AASO}(i,j) \times N_{AA}(i,j)$$

where $P_{AASO}(i,j)$ is the probability that one user submitted an answer before the other did. In this study, $P_{AASO}(i,j)$ was set to 0.5. In other words, user i and user j have equal probability that one user submitted an answer before the other did.

If this hypothesis is rejected by a two-sided binomial test, we determine that one of these users, user i or user j, submitted answers abnormally too many times before the other did.

VI. Result of the investigation

In order to detect too large deviations of answer submission order, we test Hypothesis AA and AASO. In this study, the target user pairs are 828812 user pairs each of whom submitted answers to at least one same question in social issues category of Yahoo! chiebukuro. This is because there were many discussions between answerers in this category. As a result, it seems more likely that some multiple account users intended to advocate or justify their answers and repeated TYPE AA submissions in this category.

In this experiment, the significance level for Hypothesis AA was extremely low: 0.000005. This is because we intend

 ISBN: 978-1-61208-204-2

Table II
THE RESULT OF THE INVESTIGATION ON 7 USER PAIRS WHO HAD TOO LARGE DEVIATIONS OF ANSWER SUBMISSION ORDER.

A_1	A_2	$N_{AA}(A_1, A_2)$	$NE_{AA}(A_1, A_2)$	$T_{QA}(A_1, A_2)$	$T_{AA}(A_1, A_2)$	decision
691911	802184	47	43	5.0 min.	83 sec.	same user
267614	76731	62	44	22 min.	22 min.	same user
458523	518681	86	61	9.0 min.	26 min.	different users
414445	733881	20	18	4.0 min.	2.3 hrs.	different users
649164	622996	40	30	6.6 hrs.	30 hrs.	same user
471690	471692	12	11	16 hrs.	50 hrs.	same user
622996	471692	12	11	18 hrs.	74 hrs.	different users

User $A1$ more often submitted his/her answers before user $A2$ did. $N_{AA}(A_1, A_2)$ is the number of questions to which both user $A1$ and $A2$ submitted answers. $NE_{AA}(A_1, A_2)$ is the number of questions to which user $A1$ submitted answers before user $A2$ did. $T_{QA}(A_1, A_2)$ is the median of submission time lags between questions and the earlier of their answers of $A1$ or $A2$. $T_{AA}(A_1, A_2)$ is the median of submission time lags between answers of $A1$ and $A2$ submitted to the same question. Decision shows our judgements. By considering the similarity of writing styles and opinions, we determined whether each user pair is one and the same user or not.

to detect extreme abnormal submissions. On the other hand, the significance level for Hypothesis AASO was 0.01.

In this experiment, we first applied Hypothesis AA on 828812 user pairs in social issues category, and detected 20 user pairs who repeated submitting answers to the same question too many times. Then, we applied Hypothesis AASO on these 20 user pairs and detected 7 user pairs who had too large deviations of answer submission order. Table II shows the result of the investigation on these 7 user pairs. In Table II, user $A1$ mainly submitted answers before user $A2$ did. $N_{AA}(A_1, A_2)$ is the number of questions to which both user $A1$ and user $A2$ submitted answers. $NE_{AA}(A_1, A_2)$ is the number of questions to which user $A1$ submitted answers before user $A2$ did. $T_{QA}(A_1, A_2)$ is the median of submission time lags between questions and the earlier of their answers of $A1$ or $A2$. $T_{AA}(A_1, A_2)$ is the median of submission time lags between answers of $A1$ and $A2$ submitted to the same question. Figure 2 showed the cumulative relative frequency of submission time lags between questions and their answers. Also, Figure 3 showed the cumulative relative frequency of submission time lags between answers submitted to the same question. By considering the similarity of writing styles and opinions, we determined whether each user pair is one and the same user or not. Decision shows our judgements. We discuss the following points in detail below.

- Whether each of these seven user pairs is one and the same user or not.
- The purposes of inadequate multiple account users.
- The reasons why and how the deviations of answer submission order occurred.

User pair (267614, 76731) submitted many answers to the questions about foreign residents in Japan. We determined that user 267614 and 76731 were one and the same user. This is because their writing styles and opinions were quite similar and their answers often included special words, for example, personal HP and comic artists, which other users did not cover in this category. These accounts were likely to be used for repeating the same words. For example,

[Q: 654871] I found this exhibitor in the auction [URL]. I think it is against the rule.
[A: 76731] It is scratchbuild. Let it go. You are a snitch.
[A: 267614] You are like a snitch in North Korea. Or a hound.

We thought there were this kind of inadequate users in Yahoo! chiebukuro. However, we did not think we found them by detecting too large deviations of answer submission order. This is because we did not think of any reasons why this kind of users used their multiple user accounts in this way. We are searching more examples of this kind of inadequate users and intend to find the reasons.

Also, in case of user pair (691911, 802184), we determined these users were one and the same user. This is because the median of submission time lags between their answers was only 83 seconds although user 691911 submitted answers at different times of a day. Furthermore, when user 691911 submitted questions, user 691911 selected user 802184's answers as best answers in too many times in various categories. Like the case of user pair (267614, 76731), these accounts were likely to be used for repeating the same words.

In contrast, in cases of user pair (458523, 518681) and (414445, 733881), we determined that the users of each pair were different users. This is because we found many opinion conflict between the users of each pair. Each pair used Yahoo! chiebukuro almost at the same time of each day. For example, user 458523 and 518681 mainly used Yahoo! chiebukuro from 8:00 am to 5:00 pm. Also, user 414445 and 733881 mainly used Yahoo! chiebukuro from 8:00 pm to 1:00 am. As a result, the users of each pair read questions almost at the same time. On the other hand, the median of submission time lags from questions to user 458523's answers and user 518681's answers were 9.9 minutes and 28 minutes, respectively. Also, the median of submission time lags from questions to user 414445's answers and user 733881's answers were 7.4 minutes and 66 minutes,

 ISBN: 978-1-61208-204-2

respectively. We think, these time lags gave the deviations of answer submission order between the users of each user pair.

Both user pair (649164, 622996) and (471690, 471692) submitted answers repeatedly to questions about a certain religious group. We determined that the users of each pair were one and the same users. This is because they had similar writing styles and opinions respectively. Especially, there was only one opinion conflict between user 649164 and 622996 just after they were pointed out that they were one and the same user. These accounts were likely to be used for criticizing other users' answers, or advocating or justifying their previous answers. In these cases, user 622996 and 471692 mainly criticized other user's answers, and advocated or justified their previous answers. As shown in Table II, user 622996 and 471692 mainly submitted their answers after user 649164 and 471690 did, respectively. In both cases, two user accounts were used in different ways as follows:

- Main accounts (user 649164 and 471690).
- Secondary accounts (user 622996 and 471692) for criticizing other users' answers, or advocating or justifying answers submitted by the main accounts.

Especially, user 471692 often criticized user 622996's answers. As a result, user pair (622996, 471692) was detected although the users of this pair were different users and had different opinions.

VII. Conclusion

In this study, we investigated the user pairs who had large deviations of answer submission order and discussed the reasons why and how the deviations occurred. In social issues category of Yahoo! chiebukuro, we found four user pairs suspected of being one and the same users and submitting many answers to the same questions repeatedly by using multiple user accounts in different ways. The purposes of these users seemed to be

- To repeat the same words.
- To criticize other users' answers which were against their answers.
- To advocate or justify their previous answers.

We intend to use the results of this study for further investigation of purposes and behaviors of inadequate multiple account users in Q&A sites. Especially, we think, opinion similarity is a promising clue to the detection of inadequate users and the investigation of their purposes and behaviors.

References

[1] O. de Vel, A. Anderson, M. Corney, and G. Mohay, "Mining e-mail content for author identification forensics," ACM SIGMOD Record, Vol.30 No.4, 2001, pp. 55–64.

[2] M. Koppel, S. Argamon, and A. R. Shimoni, "Automatically Categorizing Written Text by Author Gender," Literary Linguistic and Computing, Vol.17 No.4, 2002, pp. 401–412.

[3] M. Corney, O. de Vel, A. Anderson, and G. Mohay, "Gender-Preferential Text Mining of E-mail Discourse," Proc. 18th Annual Computer Security Applications Conference (ACSAC 2002), 2002, pp. 21–27.

[4] S. Argamon, M. Saric, and S. S. Stein, "Style mining of electronic messages for multiple authorship discrimination: first results," Proc. the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, 2003, pp. 475-480.

[5] R. Zheng, J. Li, H. Chen, and Z. Huang, "A Framework of Authorship Identification for Online Messages: Writing Style Features and Classification Techniques," Journal of the American Society for Information Science and Technology, Vol.57 No.3, 2006, pp. 378-393.

[6] N. Ishikawa, Y. Watanabe, R. Nishimura, K. Umemoto, Y. Okada, and M. Murata, "Detection of users suspected of using multiple user accounts and manipulating evaluations in a community site," Proc. the 6th IEEE International Conference on Natural Language Processing and Knowledge Engineering (NLPKE 2010), 2010, pp. 600–607.

[7] N. Ishikawa, K. Umemoto, R. Nishimura, Y. Watanabe, and Y. Okada, "Detection of users in a Q&A site who suspected of submitting multiple answers to a question by using multiple user accounts," Proc. the Fourth International Conference on Internet Technologies and Applications (ITA 2011), 2011, pp. 236–244.

[8] A. N. Joinson, "Understanding the Psychology of Internet Behaviour: Virtual Worlds, Real Lives," Palgrave Macmillan, 2003.

[9] N. Jindal and B. Liu, "Opinion spam and analysis," Proc. First ACM International Conference on Web Search and Data Mining (WSDM 2008), 2008, pp. 219–230.

[10] G. Wu, D. Greene, B. Smyth, and P. Cunningham, "Distortion as a validation criterion in the identification of suspicious reviews," Technical report UCD-CSI-2010-4, University College Dublin, 2010.

[11] M. Ott, Y. Choi, C. Cardie, and J. T. Hancock, "Finding Deceptive Opinion Spam by Any Stretch of the Imagination," Proc. the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies (ACL HLT 2011), 2011, pp. 309–319.

[12] C. Akkaya, A. Conrad, J. Wiebe, and R. Mihalcea, "Amazon Mechanical Turk for Subjectivity Word Sense Disambiguation," Proc. NAACL-HLT 2010 Workshop on Creating Speech and Language Data With Amazon's Mechanical Turk, 2010, pp. 195–203.

[13] http://research.nii.ac.jp/tdc/chiebukuro.html, [retrieved: June, 2009].

 ISBN: 978-1-61208-204-2

Electric Vehicle Charging Infrastructure – Security Considerations and Approaches

Rainer Falk, Steffen Fries
Corporate Technology
Siemens AG
Munich, Germany
e-mail: [rainer.falk | steffen.fries]@siemens.com

***Abstract*—Rechargeable electric vehicles are receiving increasing attention from different stakeholders: from customers as gas prices are constantly rising, from car manufacturers to address customer, market, and environmental demands, and also from electric energy utilities for integrating them into smart electric grids. While in the first step, the emphasis is placed on electric vehicles as energy consumers, using their battery for storing energy and feeding it back to the energy network will be the consequent next step. Batteries of electric vehicles will realize a distributed energy electric storage for stabilizing the electric power grid. Thus the electric vehicle will participate as a mobile energy node within the smart grid having two types of interfaces, one for electricity and one for data communication for charging and feedback control, information exchange, and for billing. Since IT security in the smart grid is already considered as a major point to be addressed, the enhancement of the smart grid with electric mobility has to address IT security as well. This article describes example interactions of electric vehicles with the charging infrastructure and it shows which security requirements have to be fulfilled in important use cases. Moreover, security considerations of current standardization activities ISO/IEC and SAE are described.**

Keywords - eMobility security; Smart Grid security; charging infrastructure; IEC 61851; IEC 15118

I. Introduction

The Smart Grid, comprising power generation, transmission, and distribution systems, comprises two parallel infrastructures, the electrical grid carrying the energy, and the information and communication infrastructure used to automate, control, and monitor the electrical grid. The information and communication part of a Smart Grid is increasingly becoming one of the essential parts of power system operations as it is responsible not only for retrieving monitoring information from field equipment but also, more importantly, for issuing and transmitting control commands realizing intelligent control algorithms for on optimized operation of the smart grid.

The number of electric vehicles as bicycles, motorcycles, and cars is expected to increase significantly. Electric vehicles will be connected with the Smart Grid for charging or for power feedback. They connect to the Smart Grid through charging stations. Charging points in public or corporate places provide the possibility for high power AC or DC charging. Other connection points may be provided by combined service stations, e.g., for parking lots, or common home power plugs in residential areas. Closely linked with the pure flow of energy is the management and control of the energy demand for charging electric vehicles. It allows matching the energy demand with the energy available within the energy grid. A defined part of the vehicle battery's capacity can also be used as energy storage to stabilize the energy grid when needed by feeding back energy from the vehicle to the electrical grid. Besides the control of energy flow there may be a second communication channel for the billing for consumed or provided energy.

The charging infrastructure as a part of the critical infrastructure Smart Grid requires integrated protection against unintentional and intentional attacks. Safety and IT security measures, which are already being part of the Smart Grid core (e.g., defined as standard or realized in proprietary deployments), need to be enhanced to cover also the Smart Grid access infrastructure. This Smart Grid access infrastructure is provided for electric vehicles through the charging infrastructure. While current deployments do not feature an information exchange between the electric vehicle and the charging infrastructure beside a minimum local control of the charging process through pilot signals, upcoming standards and proposed scenarios provide feature rich communication options. The Smart Grid communication and control network of an energy utility is increasingly opened to various nodes not being under control of any energy network operator and thereby exposed to attacks.

Highly dependable management and operations of the information infrastructure are prerequisites for a highly reliable energy network as the power system increasingly relies on the availability of the information infrastructure. Therefore, the information infrastructure must be operated according to the same level of reliability as required for the stability of the power system infrastructure to prevent any type of outage. Especially consumers and utility companies can both benefit from managing this intelligently, and standards anticipating the new environment are emerging from many directions. The immediately apparent security needs target the prevention of financial fraud and ensure the reliable operation of the power grid. Both are complex objectives. But surely all of the security ramifications of the charging infrastructure have not been discovered yet. Especially the interaction between new market participants and value added services is currently under investigation. In any case, ensuring privacy, safety, and assuring that the

 ISBN: 978-1-61208-204-2

charging service is operating correctly are basic objectives to derive related IT security requirements. Hence, integrated information security is a central part of the charging infrastructure.

The remainder of this paper is structured as follows: Section II describes use cases around the electric vehicle charging infrastructure. Section III discusses information assets derived from the use cases, threats to these assets and also defines first security requirements. Section IV gives an overview about the security standardization for the vehicle to grid interface, while Section V concludes the document.

II. USE CASES

The electrical vehicle charging infrastructure consists of a combination of power services for electric vehicles and value-added services based on the information and communication infrastructure as illustrated in Figure 1.

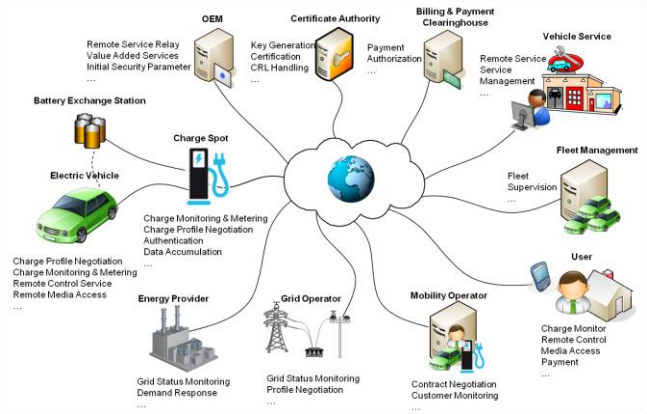


Figure 1. Communication among Actors of an Electric Vehicle Charging Infrastructure

One main goal of this information and communication infrastructure is to offer customers a choice of service options beneficial to all three, the utility company, the mobility operator as power (service) provider, and the customer. The utility can operate most efficiently when energy demand is fairly constant over time. Price incentives can be offered towards those customers having a flexible vehicle charging schedule with the objective to smooth out energy demand variations. This requires the analysis and consideration of several variables, e.g., schedule, equipment, location, payment options, and additional services.

The variety of peers in a charging infrastructure as depicted in Figure 1 shows the complexity, but also the manifold of possibilities for optimized service offerings. The following subsections provide an overview on potential use cases surrounding the charging infrastructure. Each subsection provides potential realization options for the considered use case. Note that the use case discussion stems mainly from standardization work currently done in ISO/IEC and SAE. but the use cases show the potential of a Smart Grid charging infrastructure to be a flexible platform to realize a variety of known and upcoming service offerings

A. *Control of the Electric Vehicle Charging Environment*

Connecting electric vehicles with the charging infrastructure provides flexible control of the charging process through enhanced communication between electric vehicle, charging spot, and the energy provider in the backend, e.g., to adapt the charging to the current energy provisioning situation. It also covers scenarios with limited control of the charging operation through the charging spot or backend. Charging in these scenarios may be controlled completely by the electric vehicle to the limits set by the environment. This is typically the case for AC (alternating current) charging, while in DC (direct current) charging control is being performed by the charging spot.

B. *Connecting to the Charging Infrastructure*

Connecting a vehicle to the charging infrastructure may use a portable cord set to be provided by either the electric vehicle owner or the charge spot operator. This cord set and the connectors may be different depending whether charging is being done using AC or DC , or depending on the country. An alternative is provided through wireless (inductive) charging avoiding any power cord to the car. Special consideration of the physical charging environment is necessary here, to ensure safe operation.

C. *Billing and Payment for Charging Service*

Billing and payment for consumed energy or value added services can be performed through various options:

- At the charging spot, including money, prepaid, credit cards, combination with parking ticket, etc.
- From within the vehicle (e.g., via a contract-related credential stored within the car). This option includes identification of the electric vehicle as well as charging contract verification.

Besides the direct customer interaction, there is also the interaction with clearinghouses that settle accounts between different energy providers. These become necessary when using contract based payment from within a car at a charging spot belonging to a different mobility provider.

D. *Negotiated Incentive Rate Plan*

Negotiating incentive rate plans may depend on, e.g., the contract between the customer and the mobility provider. Thus different realization options may be:

- Time of use (TOU): The utility provides a price incentive to charge a vehicle at times of lower demand typically based on time of day, day of week, and season of year. Prices are set ahead of time, in an attempt to shift load towards a more favorable time of day.
- Direct load or price control through utility: The customer receives a price incentive to give the utility direct control over the charging process. Normally, the customer is given a fixed, reduced price, and the utility has the option to interrupt or delay charging at critical times.
- Dynamic tariffs: This is a variation of time of use sometimes called real-time pricing (RTP). Price schedules vary more frequently, usually daily. Once delivered, the prices are firm and the customer, not the utility, controls the load.

 ISBN: 978-1-61208-204-2

- Critical peak pricing (CPP): This is another variation on time of use, in which the utility retains the right to override the price schedule with higher prices on a limited number of days having particularly high demand or other unusual events.
- Optimized charging: The customer gives the utility control of the charging load in turn for a price incentive. The utility may, at critical times, reduce or interrupt charging, based in part on the state of charge of the vehicle.

E. Charging Location

The charging location may vary effecting potentially also the provided service and payment options:

- Charging in private environments like the vehicle owner's home or another's home within the same utility's service area or another's home within a different utility's service area. The charging location may not be directly connected with the charging infrastructure in terms of dynamic charging control. Hence, certain options for tariffs or value added services may not always be available.
- Charging at public charge spot can also be distinguished based on the contractual relation of the vehicle owner to the charging spot operator or mobility operator like: charging spot belonging to the same utility as customer contracted, different utility (comparable to "roaming") or charging without a contractual relationship (payment based on money, pre-paid card, credit card, etc.).
- Fleet operator premises may not require a contractual relationship per vehicle directly. They may be based on the fleet operator, providing an energy "flat rate". Control of the charging process may be distinguished as described above.

F. Value Added Services

Connecting the vehicle with a charging spot featuring a communication interface provides the opportunity to leverage this communication connection also for value added services. Examples comprise:

- Software updates for ECUs or infotainment systems
- Remote diagnosis and maintenance
- Multimedia service during charging

G. Electricity Feedback

While in the first place charging is the main service provided for electric vehicles, it is also envisioned to use electric vehicles as dynamic energy storage. The electric vehicle could feed back energy into the Smart Grid upon request. Here, a distinction of the use cases can be done in a similar way as for charging:

- Based on the feedback locations, e.g., for integration within micro grids, to increase their independence from the main grid allowing the local usage of stored energy.
- Based on a local feedback plan, were the customer configures, e.g., a certain amount of energy, which is required as minimum capacity of the vehicle battery.
- Based on backend scheduling / needs.

These use cases show a variety of different services for the electric vehicle charging infrastructure. They illustrate how valuable the transmitted information is for the availability and reliable operation of the services, but also for the safety and privacy of the end user.

III. INFORMATION ASSETS, POTENTIAL THREATS, AND DERIVED SECURITY REQUIREMENTS

As just shown in the previous section, various use cases exist in which different peers exchange information to realize a dedicated service. Experience with the existing data communication infrastructure can be leveraged to analyze the charging infrastructure regarding potential threats as well as to determine suitable countermeasures. This may especially comprise security protocols or security mechanisms, which have been proven effective in the current communication infrastructures. Examples comprise security protocols like TLS (Transport Layer Security [3]) and digital signatures.

A. Information Assets in Charging-Related Communication

The information transported over the different connections is the asset that may motivate attacks against the charging infrastructure. The following table summarizes important information assets and their criticality for the system. The majority of these information assets are expected to be transmitted especially over the vehicle-to-grid interface.

TABLE I. INFORMATION ASSETS IN THE ELECTRIC VEHICLE CHARGING INFRASTRUCTURE

Information asset	Description, potential content	Security relation
Customer ID and location data	Customer name, vehicle identification number, charging location, and charging schedule	Effects customer privacy
Meter Data	Meter readings that allow calculation of the quantity of electricity consumed or supplied over a time period. These are generated by the charge spot and may be validated by the vehicle.	Effects system control and billing
Control Commands	Actions requested by one component of other components via control commands. These may also include inquiries, alarms, or Notifications.	Effects system stability and reliability and also safety
Configuration Data	Configuration data (system operational settings and security credentials, also thresholds for alarms, task schedules, policies, grouping information, etc.) influence the behavior of a component and may need to be updated remotely.	Effects system stability and reliability and also safety
Time, Clock Setting	Time is used in records sent to other entities. Phasor measurement directly relates to system control actions. Moreover, time is also needed to use tariff information optimally. It may also be used in certain security protocols.	Effects system control (stability and reliability and also safety) and billing
Access Control Policies	Determination whether a communication peer is entitled to send and receive commands and data. Such policies may consist of lists of	Effects system control system stability, reliability, and

Information asset	Description, potential content	Security relation
	permitted communication partners, their credentials, and their roles.	also safety
Firmware, Software, and Drivers	Software packages installed in components may be updated remotely. Updates may be provided by the utility (e.g., for charge spot firmware), the car manufacturer, or another OEM. Their correctness is critical for the system reliability.	Effects system stability and reliability and also safety
Tariff Data	Utilities or other energy providers may inform consumers of new or temporary tariffs as a basis for purchase decisions.	Effects customer privacy and competition

B. *Potential Threats*

Some example threats are described in the following to illustrate the need to integrate security measures into the charging infrastructure right from the beginning. These threats focus on the specifics of electric vehicle charging and connected communication.

1) *Eavesdropping / Interception*

Eavesdropping is a passive attack to intercept information, which may compromise privacy or be used to gain more information for additional, active attacks. Eavesdropping requires the adversary to have either physical or logical access to the communication connection. Both the link to the vehicle and to the backend may be intercepted (Figure 2).

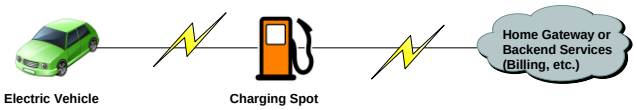


Figure 2. Potential Locations for Eavesdropping

Communication with the charging spot in general can be done using different technologies, like Wireless or Powerline Communication (PLC). Common to these technologies is that the radiation of the communication transfer (through the frequency used) is high enough that it is sufficient for an adversary to be in closer vicinity to the communication instead of having direct physical access. Missing security measures will enable an adversary to eavesdrop the communication. As shown above, charging related communication may include a variety of information being valuable for an attacker like tariff information, charging status information, or billing relevant information.

2) *Man-in-the-Middle Attack*

An attacker may intercept communication on the interface between the vehicle and the charging point and modify this information. An example may be tariff options provided by the mobility operator and send via the charging spot to the vehicle. This may be accomplished in the easiest case through a modified charging cable.

Another example is the usage of a faked charge spot as depicted in Figure 3: A potential adversary may use its own (faked) charging spot to which honest customer connect. The adversary's charge spot is connected to an official charge spot and only routes the communication between the honest customer and the original charge spot. The adversary can then consume the charging energy partially, so that the honest customer receives only a fraction of her purchased energy, but pays for the complete consumption by her vehicle plus the adversary's vehicle.

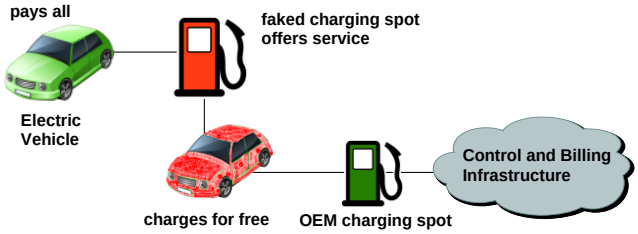


Figure 3. Man-in-the-Middle Attack to steal Energy

Interesting in this attack is that the adversary actually performs the manipulation on the energy provisioning path and not on the communication path. The latter one is untouched. This attack shows the need for connecting the flow of energy to the flow of information.

3) *Transaction Falsifying or Repudiation*

The customer himself may intentionally or unintentionally claim to have received less energy than stated on the billing record. Likewise, the utility may claim to have delivered more energy to the customer.

4) *Attack network from within vehicle (and vice versa)*

If the electric vehicle is connected to the charging infrastructure, e.g., using a value added service, an adversary (software) may inject or modify application-level traffic intentionally (as an attack) or unintentionally (faulty software component, malware).

5) *Tampered or substituted component*

A customer may manipulate a component trusted by the utility to provide accurate billing or control information. This affects both components in the charging spot and within the electric vehicle. Examples are pirated or faked replacement parts.

C. *First Set of Security Requirements*

Basic security requirements of the electric vehicle charging infrastructure have to be addressed. They target the availability and reliable energy provisioning. They also aim to limit attack effect (geographical and functional), enforce authorized control actions on the smart grid, and correct billing of energy transactions between involved peers (customer, charging sport operator, market, utility).

Based on the stated information assets and depicted threats, the basic security requirements can be more specifically addressed by requiring dedicated cryptographic measures as there are:

- Mutual authentication of end-to-end communicating entities. The authentication may be performed on different layers of the OSI reference model, e.g., on transport layer and on application layer. This is especially useful, if the peer to authenticate against is either a local communication peer or a backend peer, depending on the online state of the charging spot.

 ISBN: 978-1-61208-204-2

- Non-repudiation of billing and tariff information to ensure secure transactions.
- Protected communication between the electric vehicle and the charging spot, the electric vehicle and backend services, the charging spot and backend services, between backend services.
- Authorization, especially for control of the charging.
- Integrity-protected, authenticated and authorized software updates to avoid malfunctions through software from unauthorized sources
- Logging of security relevant events to enable auditability of the system.
- Security failure and exception handling, to support system reliability, also in case of security breaches,
- In general confidentiality and integrity of sensitive data.

These security requirements cover typically lead to technical and organizational security measures. Hence, to ensure a thorough security approach supporting the interaction of different peers using equipment from different vendors, standardization of an appropriate security approach as part of the overall system approach is necessary.

IV. STANDARDIZATION LANDSCAPE FOR THE CONNECTION TO THE CHARGING INFRASTRUCTURE

This section details the standardization activities focusing on the communication interface between the electric vehicle and the charging spot, but further connections to the backend are also considered. The main focus is placed on standardization activities from the ISO/IEC. An overview about related SAE activities is given as well.

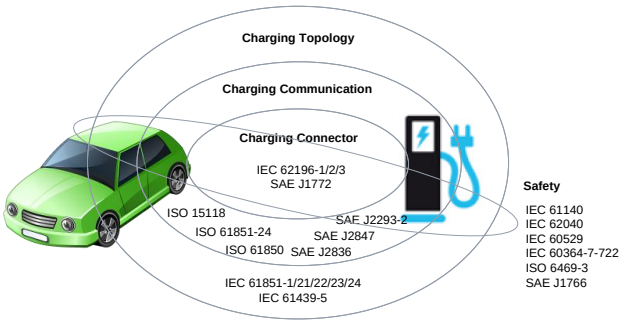


Figure 4. Communication Standards for the Electric Vehicle Charging Infrastructure [1]

As shown in Figure 4, standardization activities of ISO/IEC and SAE can be divided into four categories: charging connector, charging communication, charging topology, and safety. The following table summarizes more information about relevant standards.

TABLE II. COMMUNICATION STANDARDS AND THEIR SCOPE FOR THE ELECTRIC VEHICLE CHARGING INFRASTRUCTURE

Standard	Scope	Content
IEC 62196	Charging Connector	Plugs, socket-outlets, vehicle couplers and vehicle inlets – Conductive charging
SAE J1772	Charging Connector	Electric Vehicle Conductive Charge Coupler
ISO 15118	Charging Communication	Road vehicles - Communication protocol between electric vehicle and grid
SAE J2293	Charging Communication	Energy Transfer System for Electric Vehicles
SAE J2836	Charging Communication	Use Cases for Communication between Plug-in Vehicles and the Utility Grid (-1), Supply Equipment (EVSE) (-2), Utility Grid for Reverse Power Flow (-3)
SAE 2847	Charging Communication	Communication between Plug-in Vehicles and the Utility Grid (-1), Supply Equipment (EVSE) (-2), Utility Grid for Reverse Power Flow (-3)
IEC 61850	Power Systems Communication	Communication networks and systems in substations
IEC 61851	Charging Topology	Electric vehicle conductive charging system
IEC 61439	Charging Topology	Low-voltage switchgear and control gear assemblies

The following sections describe ISO/IEC activities related to charging communication and their IT-security considerations. This overview shows the increasing consideration of IT security requirements in the definition of evolving charging communication protocols. This is especially the case for new protocols like ISO/IEC 15118 targeting the communication for charging control and value added services between electric vehicles and charging spots.

A. IEC 61851

IEC 61851 defines a conductive charging system and was standardized in 2001. The standard addresses equipment for charging electric road vehicles at standard AC supply voltages (as per IEC 60038) up to 690 V and at DC voltages up to 1000 V, and for providing electrical power for any additional services on the vehicle if required when connected to the supply network. The standard comprises different parts addressing specific charging options:

- IEC 61851-1: Electric vehicle conductive charging system – General requirements
- IEC 61851-21: Electric vehicle conductive charging system - Electric vehicle requirements for conductive connection to an A.C./D.C. supply
- IEC 61851-22 Electric vehicle conductive charging system - A.C. electric vehicle charging station
- IEC 61851-23 Electric vehicle conductive charging system - D.C electric vehicle charging station
- IEC 61851-24 Electric vehicle conductive charging system - Control communication protocol between off-board D.C. charger and electric vehicle

IEC 61851 targets four different charging modes:

- Mode 1 (AC): slow charging from a standard household-type socket-outlet
- Mode 2 (AC): slow charging from a standard household-type socket-outlet with in-cable protection device
- Mode 3 (AC): slow or fast charging using a specific EV socket-outlet and plug with control and protection function permanently installed
- Mode 4 (DC): fast charging using an external charger

 ISBN: 978-1-61208-204-2

The communication between the vehicle and the charging spot depends on the mode applied. There is no data communication in Mode 1 and Mode 2. In Mode 3 only the control pilot communication exists, while in Mode 4 additional communication functions are available to allow battery management. Common to all modes is that IT-security is not provided. Nevertheless, for the vehicle integration into a smart-grid-connected charging infrastructure, (secure) communication is required for tariff exchange, billing, optimization of charge cost and grid load, value added services, etc. To support these functions in the future, ISO/IEC 15118 is currently being specified addressing these communications needs, including an integrated security concept (see next section).

B. ISO/IEC 15118

ISO/IEC 15118 is being standardized in an ISO/IEC joint working group. Its main focus is the interface between an electric vehicle and a charging spot interface. Communication with the backend infrastructure is not directly targeted. The specification is split into different parts, which are all still work in progress:

- ISO 15118-1: General information and use-case definition (cf. [5])
- ISO 15118-2: Technical protocol description and Open Systems Interconnections (OSI) layer requirements (cf. [6])
- ISO 15118-3: Physical layer and Data Link layer requirements (cf. [7])

Security is integral part of the standard and has been considered right from the design phase. ISO/IEC 15118-1 contains a security analysis, which investigates in specific threats, which are partly stated in section III.B above. This security analysis is the base for the security requirements and resulting security measures targeting the specified use cases.

The security measures defined in ISO/IEC 15118-2 build upon existing standards as far as possible. The access media for AC and DC charging will be powerline communication in the first step. Support of inductive charging will most likely use wireless communication. As both feature different OSI layer 1+2, security measures have not been placed here to allow an independent solution. As shown in Figure 5 ISO/IEC 15118-2 applies TCP/IP for the communication between the vehicle and the charging spot. Consequently, security is applied on transport layer using TLS (cf. [3]) ensuring a protected channel between both. Since ISO/IEC 15118 targets the communication between the vehicle and the charging spot, this might be sufficient at the first glimpse. But security measures on application layer have also been defined applying XML security (digital signatures and encryption). Application layer security became necessary, as the communication also targets billing and payment relevant information, which are exchanged with the backend in contract based payment scenarios. Moreover, to enable contract based payments, the vehicles need authentication means. To enable secure communication with the backend, the electric vehicle possesses a digital vehicle certificate and a corresponding private key. These security measures go beyond the communication hop between the electric vehicle and the charging spot. The direct data interaction of the electric vehicle with the backend is shown in Figure 5 in the charging cycle loop. Here, charging spot meter readings are signed by the vehicle and forwarded by the charging spot to the backend. They build the base for the billing process later on. Note that the general data exchange in Figure 5 has been simplified and mainly security related exchanges are shown.

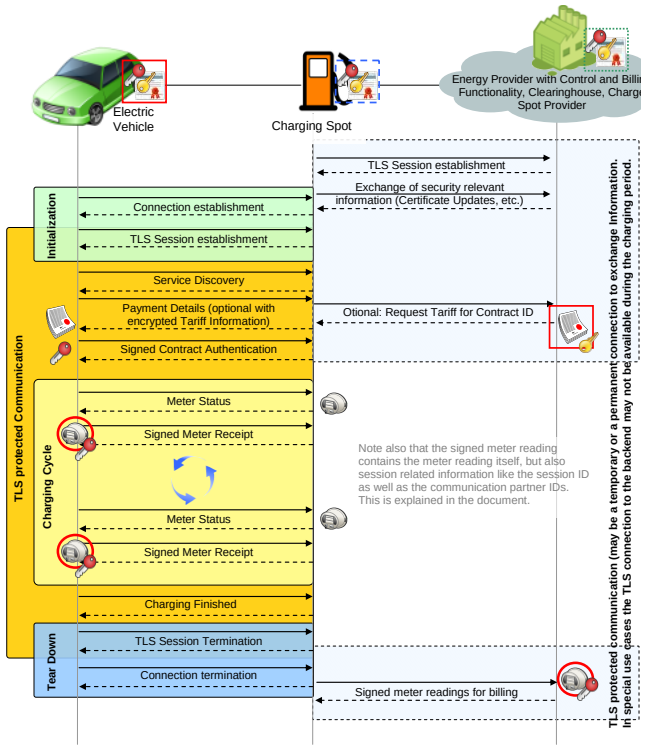


Figure 5. Information Exchange for Electric Vehicle Charging

The proposed security solution takes the connection state of a charging spot into account to support charging spots that have very limited or even no online connectivity. In general, the charging spot is assumed to be online at least once a day. This online period may coincide with the charging period of an electric vehicle. Therefore, explicit precautions have to be given to the exchanged data, especially, if the backend depends on these.

To enable secure transmission of data from the backend to the vehicle (e.g., credential updates or tariff information) a secret needs to be established between the vehicle and the backend allowing an end-to-end encrypted transfer. The vehicle certificate contains static Diffie-Hellman parameters to enable an easy setup of a session based encryption key. Only the backend needs to generate fresh per-session Diffie-Hellman parameters that are used to calculate a fresh Diffie Hellman secret, which can then be used as session secret. This has the advantage, that the backend can pre-calculate session keys for vehicle communication, once the vehicle's certificate is known at the backend. This approach is known from many of today's web server applications, which use the same technique.

For the normal operation the vehicle certificate will be a contract-based credential. Thus the backend already

 ISBN: 978-1-61208-204-2

possesses the certificate information, once the customer enrolled for a contract. For setup operation, the vehicle may possess an OEM credential installed during manufacturing of the car and used for bootstrapping the contact based credential.

Notably, the used security mechanisms target elliptic curve cryptography (ECC) for authentication (during key management phases) and for digital signatures. The digital signature standard ECDSA based on ECC provide comparable security to RSA but uses significantly shorter cryptographic key sizes. As the certificates support ECDSA, the Diffie-Hellman key agreement is performed in its elliptic curve variant ECDH. Moreover, elliptic curves can be implemented efficiently in hardware. As ISO/IEC 15118 targets especially electronic control units (ECU) in vehicles and charging sports, memory and calculation constraints are evident and pose further implementation requirements.

As described above, digital certificates for the charging spot, and, depending on the use cases, also a vehicle certificate are the basis for protecting the charging control communication. This requires a dedicated credential management infrastructure (Public Key Infrastructure – PKI) handling the initial provisioning, but also the revocation and update of certificates and cryptographic keys. The call flow as depicted in Figure 5 is based on the application of unilateral authenticated TLS, where the electric vehicle implements the client part. Hence, the client is required to check the certificate validity including the issuer. The standard ISO/IEC 15118 requires vehicles to store only a fixed, limited number of root certificates to enable issuer verification. Moreover, it also restricts the number of supported intermediate certification authorities. Besides the validity and issuer, the client also needs to check the certificate revocation status. One option to avoid the handling of certificate revocation lists is the usage of short term certificates from the server side. Another option is the provisioning of the revocation state by the server itself, e.g., by attaching a fresh Online Certificate Status Protocol (OCSP) response to the certificate during the authentication phase. To keep a balance regarding the implementation and operational effort, the current ISO/IEC 15118 proposal features both, short term certificates for the server side certificates and OCSP responses for intermediate CAs.

V. CONCLUSION

The focus of this paper has been the discussion of security requirements and solution approaches for the interface between an electric vehicle and a charging spot. Especially the standard ISO/IEC 15118 was in focus here addressing a variety of use cases while considering security right from the beginning. Nevertheless, to enable online control of the charging operation and also value added services, at least the charging spot needs to be connected to the Smart Grid core.

One standard, which can be directly applied for the energy automation communication is IEC 61850 [9], already applied in substation automation. This communication can be protected by security measures according to IEC62351 [8]. The security in IEC 62351 features similar protection means for TCP/IP based communication also based on TLS. This eases the secure interworking between the Smart Grid communication core and the access via the charging infrastructure. Moreover besides pure charging control, there may be also value-added services provided through the charging spot like multimedia services, software or firmware updates, remote diagnosis, and so on. All of these services have to be protected appropriately. The intrinsic complexity of this overall Smart Grid vehicle charging system requires a systematic approach to include required security measures right from the beginning that can be used and managed efficiently. It is expected that new use cases will enhance the existing security requirements and also influence the further development of communication standards.

VI. ACKNOWLEDGEMENT

The base version of this report (see [11]) compiled in June 2011 has been supported by the German Federal Ministry for the Environment, Nature Conservation and Nuclear Safety within the Harz.EEmobility project under contract 03KP623 (see [2] for more information). The further research and investigation leading to this update of the initial report is part of the FINSENY (Future INternet for Smart ENergY) project (see [3] for more information). The authors gratefully acknowledge the contributions of all FINSENY project partners. FINSENY is partly funded by the European Commission within the FI-PPP, which is part of the Framework Program FP7 ICT.

References

[1] The German Standardization Roadmap for Electromobility, http://www.elektromobilitaet.din.de/sixcms_upload/media/3310/Normung-Roadmap_Elektromobilit%E4t_en.pdf, last access April 2012

[2] HarzEE-mobility, https://www.harzee-mobility.de/, last access April 2012

[3] FINSENY – Future Internet for Smart Energy: http://www.fi-ppp-finseny.eu/

[4] T. Dierks and E. Rescorla: "The Transport Layer Security (TLS) Protocol Version 1.2", RFC5246, IETF, 2008.

[5] ISO/IEC 15118-1: Road vehicles — Vehicle-to-Grid Communication Interface — Part 1: General information and use-case definition, Work in Progress

[6] ISO/IEC 15118-2: Road vehicles — Vehicle-to-Grid Communication Interface — Part 2: Technical protocol description and Open Systems Interconnections (OSI) layer requirements, Work in Progress

[7] ISO/IEC 15118-2: Road vehicles — Vehicle-to-Grid Communication Interface — Part 3: Physical layer and Data Link layer requirements, Work in Progress

[8] ISO-IEC 62351, Part 1-8, http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=sea22.p&search=iecnumber&header=IEC&pubno=62351, last access April 2012

[9] ISO-IEC 61850, Part 1-9, http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=sea22.p&search=iecnumber&header=IEC&pubno=61850 , last access April 2012

[10] IEC 61851, Part 1, 21-24, www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=sea22.p&search=iecnumber&header=IEC&pubno=61851, last access April 2012

[11] R. Falk and S. Fries: Securing the Electric Vehicle Charging Infrastructure – Current status and potential next steps, Oct 2011, Berlin, VDI-Berichte 2131, VDI-Verlag Düsseldorf. ISBN 978-3-18-092131-0.

 ISBN: 978-1-61208-204-2

Man-in-the-middle Attacks Detection Scheme on Smartphone using 3G network

Jaemin Lee
School of Electronic Engineering
Soongsil University
Seoul, Korea
dlwoas@ssu.ac.kr

Chaungoc Tu
School of Electronic Engineering
Soongsil University
Seoul, Korea
chaungoctu@ssu.ac.kr

Souhwan Jung
School of Electronic Engineering
Soongsil University
Seoul, Korea
souhwanj@ssu.ac.kr

Abstract— **In this paper, we propose a scheme to detect the man-in-the-middle attacks occurring when user accesses to the Web server with SSL using smart-phones. Normally, server verification process under smart-phone environment does not properly work in computer environment. Because Mobile Web Server usually uses server-side certificate, and smart-phone cannot correctly validate server certificate, this could cause the risk of man-in-the-middle attack. This vulnerability allows a rouge AP to carry out a man-in-the-middle attack easily every time user connect to the secure website using his smart-phone via WLAN. To solve the problem in an effective way, we first make use of the dual interfaces network (3G and WiFi) in smart-phone to communicate with server in order to get certificates from both interfaces. The certificates are then compared to determine whether there is a man-in-the-middle attack or not. Our scheme not only offers a realistic countermeasure to prevent man-in-the-middle attack but also does not require a complex procedure or changes in HTTPs protocol.**

Keywords -- MITM; Rogue AP; Smart Phone.

I. INTRODUCTION

Nowadays, the developing of WiFi service has brought the increasing of smart-phone users who get benefit from its features. However, WiFi users still suffer from the risk of man-in-the-middle (MITM) attack. Based on users' habit of familiar SSIDs connect to an AP, a rouge AP can trick user to connect to its network by creating a WLAN with the same SSID with legitimate AP. By successfully luring users into its network, rouge AP can sniff and steal user packets through various types of attacks and modify those packets into various forms. One of the typical examples for those attacks is SSL interception. SSL interception can be implemented when user request to access secure Web server (which use the HTTPs protocol). By capturing and replacing the certificate with its own, a rouge AP can provide user with a fake certificate, thus can create shared session keys with user and server. With those session keys, a rouge AP can easily catch all the packets that contains personal information like user ID and password. This type of attack can be more easily applied to the mobile web environment where certificate verification process is not properly executed. To solve this problem, the proposed scheme takes advantage of the 3G network combining with existing WiFi network in user's smart-phone to provide a proper authentication method. To immediately detect the sign of MITM attack under secure connection, our scheme provides a method to verify the server's certificate in user terminal.

This paper is organized as follows. In Section II, we present various types of MITM attacks and current solutions for preventing the attacks. Section III describes the procedure and features of proposed scheme. The implementation of proposed scheme will be presented in Section IV. The experiments and results as well as comparison with other schemes are presented in Section V. Finally, Section VI provides concluding remarks.

II. RELATED RESEARCH

The phrase "man-in-the-middle" is used to describe the attack which occurs during communication between a consumer and a legitimate organization. The most dangerous part of man-in-the-middle attack is the ability to perform packet sniffing through encrypted communications between two sides [1] [2] [3] [4]. Recently, with the grown of smart-phone users, the risks for them to become victim of MITM attack have also become an issue in online communities.

In this section, we present different approaches of MITM attacks which are usually carried out by attacker before implementing SSL interception procedure and the solutions for defending against those attacks.

A. MITM attack types

1) MITM attack through the rogue AP

This is a kind of MITM attack which known as "session hijacking attacks" [5] [6] [7]. In this attack, the intruder aims to tamper the legitimate user's session by gaining access to it. The attacker usually start an attack by sniffing and eavesdropping techniques on a network stream, and ends with altering, forging or rerouting the intercepted data. This MITM attack is usually chosen by attacker to attack against public-key cryptosystems by substituting the intercepted public key with their forged public keys. In this case, the victim parties are made to believe that they are still under safe communication with each other. In common

 ISBN: 978-1-61208-204-2

MITM attack scenario, attacker often insinuates into the communication between a client and a server and transmits deceitful messages between them to make them feel safe in communicating with each other. Technically, attacker usually uses a program which appears like a server to the client or vice versa. Figure 1 illustrates that client/server scenario:

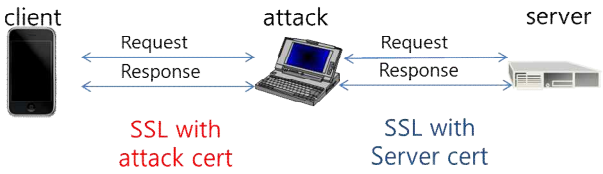


Figure 1 Client/server scenario

In MITM attacks, the attacker first aims to interfere the two sides of communications, and captures all communication between them. After successfully implementing the first step, attacker can launch other attacks like sniffing the packet, hijacking authenticated sessions, injecting packets or commands to the server, and sending the forged to the victim client. Main target of MITM attack is to get sensitive and valuable information, so MITM attacker frequently choose to intercept both HTTP and HTTPs communication. A MITM attack which can deceitfully direct the target endpoint (like the victim) to the attacker's proxy server instead of the real server can be considered as a successful attack. Objectives for MITM attacks include gaining access to the client's message and modifying it before forwarding to the server. The consequences for a successful MITM attack are misleading the communication, or getting confidential information like identity, address, password for malicious purposes.

With those potential threats, MITM attacks is a common risk to web-based financial transaction system. For example: e-business websites, payment gateways, and online banking, insurance and credit card servicing platforms. MITM attacks may lead to identity thefts and financial frauds.

2) MITM attack through the Evil Twin

This MITM attack is mainly based on the use of scanning and interfering methods [8]. By detecting the user connection with legitimate AP, the attacker can determine and create an AP with the same MAC address as legitimate AP. The attacker then tries to interfere with the connection between user and his current AP by sending the Disassociation frame. Using stronger of signal, the fake AP can successfully attract user to connect to it. The MITM attack is successful after user connects to the fake AP.

3) MITM through the ARP Spoofing

An attacker repeatedly send ARP reply messages to both sides of communication (user side and the legitimate AP side) attempt to associate his MAC address with the IP address of a target host, so that any traffic meant for the target host is redirected to the attacker's MAC instead [9].

4) DNS spoofing

In this attack, the ID of any DNS request is sniffed and target request is replied by attacker with the incorrect ID before the real DNS server. There are many existing tools for implementing this kind of attack. For example: "ADM DNS spoofing tools" which can spoof DNS packet actively and passively. Others knowable tools are "ettercap","Dsniff", DNS local spoofing, DNS jizz spoofing and DNS ID Spoofing also can be used for DNS spoofing.

5) IP address spoofing

In order to conceal the identity of the packet sender or to impersonate another computer system, the attacker creates IP packets with a forged source IP address. Although using this method on remote system can be very difficult because it requires the modification of thousands of packets at a time, it is still effective where trust relationships exist between endpoints. A typical tool for spoofing IP datagrams is "Hping" which only with one-line of command, this tool can send spoofed datagram to almost any target victim.

In such scenarios, a MITM attacker usually intercepts the communication to get exchanged public keys between client and server, so that he can modify those keys. The attacker also intercepts the relevant encrypted messages and responses, then uses the correct public keys to decrypt and re-encrypt them for all communication segments in every moment to successfully avoid any suspicion from either relevant party. Although such attacking seem too tough to accomplish, it can pose a real risk to insecure networks (e.g., the Internet, and wireless networks)

B. MITM defense techniques

1) Detecting Rogue AP using Client-side bottleneck bandwidth analysis

This method determines whether the network packets of an IP address are routed from APs, according to client-side bottleneck bandwidth [10]. The inter-arrival of Packet is derived from bandwidth. This value can be used to detect the difference between wired and wireless bandwidths. However, as this method has large window size problem and bandwidth measurement technique, it is not easy to be used in real environment.

2) A Passive Approach to Rogue AP detection

The main idea of this approach is based on the use of RTT to detect rouge AP and legitimate AP [11]. The characteristics of lower capacity and the higher variability between wired and wireless networks can be used for distinguishing between those networks. However, in different conditions, normal user can be accidently classified into an attacker.

 ISBN: 978-1-61208-204-2

3) Using radius authentication server for prevent Rogue AP

This method uses the radius authentication server which is made from 4 parts: Wireless security management interface, database, radius authentication server, and rogue AP detection module [12]. Radius authentication server is used for device authentication. The problem of this method is the need for ISP (Internet Service Provider) to install the Radius authentication server, which causes inconvenience. This method cannot detect the rouge AP coming from an ISP which does not install the Radius authentication server.

III. DETECTION SCHEME

With the information provided in section II, we can easily see that user's privacy is still at risk even if they access through a secure service like SSL-based HTTPS secure connection service [5][6][7].

To solve this problem, many techniques have been proposed, however because of the cost, space limitations, facilities and feasibility, we cannot provide safe services to users [10][11][12]. The proposed technique provides a simple, user-side verification without significant cost increase for detecting the man-in-the-middle attack based on SSL interception. In order to find the attacker, we also do not need to install additional equipment and modify the existing protocol. This method is also likely to detect the attacker with no space limitations, which means we can detect the rouge AP anywhere.

In the proposed scheme, user terminal (like smart-phone...) requests the server certificate via 3G and WiFi networks simultaneously. Smartphones usually have 3G interface and 3G network is more security than WiFI [13]. After receiving the certificates, the user terminal verifies whether they are the same. If an attacker modified their server certificate through WiFi that will be detected in user terminal. This procedure is illustrated in Figure 2 below:

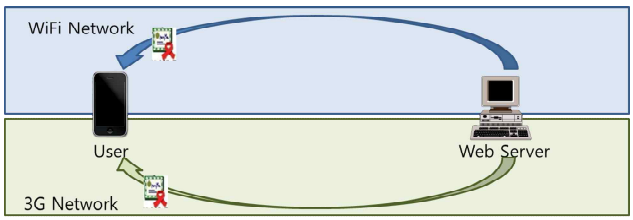


Figure 2 certificate transport using 3G network and WiFi network

The certificate of the web server where user frequently connects can be downloaded in advance via 3G networks and stored in user terminal.

Table 1 describes the structure for storing certificate value

TABLE I. TABLE FOR STORED CERTIFICATE VALUE

Web Site name	Certificate value	Save Date
paypal	b01aefc4c…..	2011.10.5
google	a330f91a1s…..	2011.6.20

Certificate values can be stored in PEM format or DER format. With PEM format, certificate values are stored in the form of base-64 encoding (base64 encoding) like numbers, letters and symbols etc …. With DER format, certificate values are stored in binary value form.

Figure 3 illustrates the comparison between certificate values in PEM format

Figure 3 Certificate value verify in PEM format

In case two values are different, current AP will be considered as rouge AP and will be disconnected. The application will try to connect to other AP and restart the verification procedure. If there is no safe AP around, only the 3G network is used.

Figure 4 illustrates the verification procedure of our scheme.

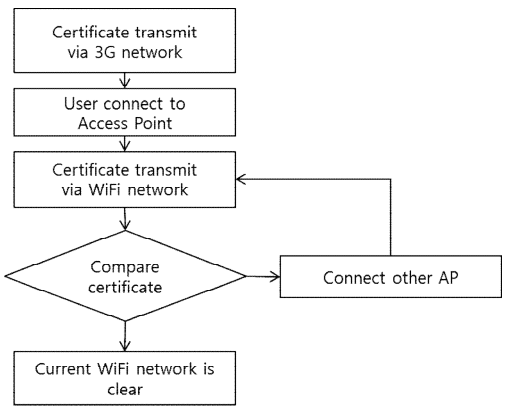


Figure 4. Compare certificates received by 3G and WiFi

The verification procedure only runs at the first time when user connects to an AP. After the first verification to

determine whether the AP is a safe one to use or not, if the AP is safe, all checked AP in the future don't have to repeat this procedure. Even connection another Web server service. This purpose is detect MITM AP.

IV. IMPLEMENTATION

In this paper, we implement the actual experiment for the proposed design techniques to defend against man-in-the-middle attacks to analyze the effective of our scheme. The architecture of our implement is illustrated by Figure 5 as follow

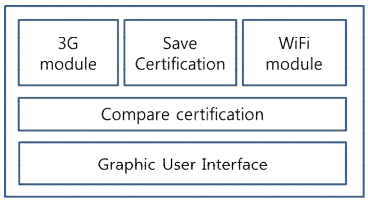


Figure 5 Application architecture of detect MITM attack

The implementation of our propose techniques is based on Android-based smart phones. An application is installed in Android phone to test the detection applications. The smart-phone device uses API 10 version 2.3.7, below are details of our experiment device:

- OS : Android 2.3.7 API 10
- Phone name: HTC Desire
- CPU: Qualcomm Snapdragon, 1000 MHz
- RAM: 576MB
- ROM: 512MB Flash
- WiFi: 802.11a/b/g/n
- Main Screen Resolution: 480 x 800
- 3G Network: GSM, CDMA

A. Working procedures

1) The user terminal which uses the 3G network or a WiFI network, checks whether it can connect to the 3G network or not. After checking, it sends the value of 3G networks in order to receive certificate from HTTPS sites (such as. Gmail.com).

2) The certificate value that received by 3G network will be stored and will be used as a cache when the 3G network is used to access to same site again, thus reduce unnecessary operation.

3) WiFi interface is activated and connect to available AP's. After that a request is sent to the same HTTPs site to receive authentication value. Those authentication value will be stored in memory in order to compare the two certificates.

4) The authentication value transmitted though 3G networks are used for verification with the values sent via WiFi network. Certificate value is sent in hexadecimal, so the site certificate values can be seen through a string comparison. If there is any different of authentication value between WiFi network and 3G network, it will be considered as man-in-the-middle attack, in this case, user can connect to other AP and redo the verification process. If two certificates are same, that mean AP is safe and secure.

B. Application GUI

The user application has been designed for easily detecting the man-in-the-middle attack. The user interface has been designed so that in order to verify the certificate in a website, user only need to enter website domain and click the search buttons. The authentication value received from both 3G and WiFi networks are shown in Log screen. Log screen includes operating hours, SSID of current connection AP, BSSID and warning message if there is a man-in-the-middle attack occurs. Application GUI is illustrated by Figure 6 below:

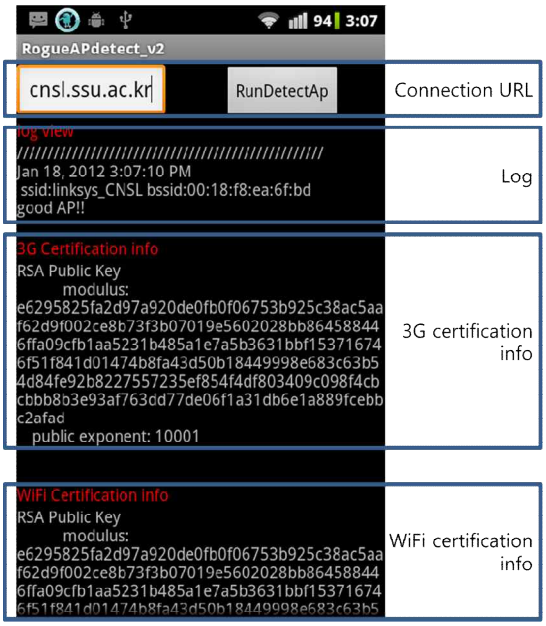


Figure 6 Application GUI

V. EXPERIMENTS AND RESULTS

In this paper, we design the environment where MITM occurs in order to test the effective of our scheme. We use Backtrack 5 OS to implement the MITM attack. The webmitm uses for fake certificate generation and ssldump is used for checking the log. We also created a wireless AP with airmon-ng and airbase-ng.

In order to create rogue AP, the following steps are implemented:

Firstly, airmon-ng is run for creating new wireless AP.

```
airmon-ng start wlan0
airbase-ng –c 6 –e "SSID" mon0&
```

 ISBN: 978-1-61208-204-2

After that, we configure iptables, create air-interface, setting DHCP server and set https port forward.

```
#Clear out iptables
    iptables --flush
    iptables --table nat --flush
    iptables --delete-chain
#Create a simple masquerade rule, routing all data of wlan1
    iptables --table nat --delete-chain
    iptables --table nat --append POSTROUTING --out-interface wlan2 -j
MASQUERADE
#Accept anything coming in interface at0
    iptables --append FORWARD --in-interface at0 -j ACCEPT

#Make sure forwarding is enabled
    echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
    ifconfig at0 up
    ifconfig at0 192.168.0.254 netmask 255.255.255.0
    route add -net 192.168.0.0 netmask 255.255.255.0 gw 192.168.0.254
    /etc/init.d/dhcp3-server start
    dhcpd3 -cf /etc/dhcp3/dhcpd.conf -pf /var/run/dhcp3-server/dhcpd.pid
at0

    iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT
    iptables -A FORWARD -j ACCEPT

    iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT
    iptables -A FORWARD -j ACCEPT
```

Next step, we run webmitm tool so that we can change the certificate, and ssldump for saving user information on log.txt

```
    webmitm –d
    ssldump –i at0 –n –d –k webmitm.crt | tee log.txt
```

Result of MITM attack experiment has shown user's id and password even under secure environment (like gmail). Figure 7 illustrates the result of our MITM attack.

```
    User-Agent: Mozilla/5.0 (Linux; U; Android 2.3.7; (
AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobi
    Origin: https://accounts.google.com
    Accept: application/xml,application/xhtml+xml,text,
    Content-Type: application/x-www-form-urlencoded
    Content-Length: 190

    continue=http%3A%2F%2Fmail.google.com%
2F&service=mail&dsh=-7303616239754199511&timeStmp=&sec
PQ&Email=dlwoas&Passwd=198[redacted]PersistentCookie=yes
+in-----------------------------------------------
New TCP connection #192: 192.168.1.106(54874) <-> 74.1
192 1  0.0859 (0.0859)  C>S SSLv2 compatible client he
  Version 3.1
```

Figure 7 Result of the attack

From the result of MITM attack, we can prove that MITM attack is possible and attacker can get user information from secure website. We also implemented our detection scheme against Man-in-the-middle attacks. Figure 8 and Figure 9 illustrate two results between normal AP and rogue AP situations. Figure 8 shows result when user connects to a normal AP "linksys_CNSL" and Figure 9 illustrates result with rouge AP "CNSL_TestAP" situation. The experimental results are as follows: In normal AP situation, the certified values transmitted via WiFi and 3G are the same. On the other hand, the authentication values are different in the AP "CNSL_TestAP" which is the man-in-the-middle.

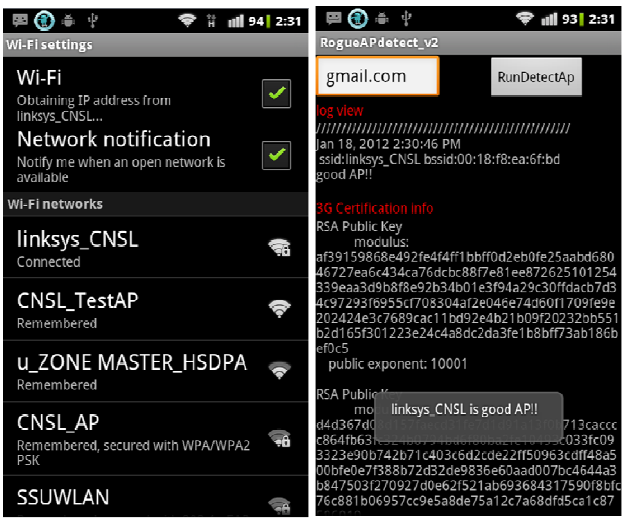


Figure 8 Result of the normal AP situation.

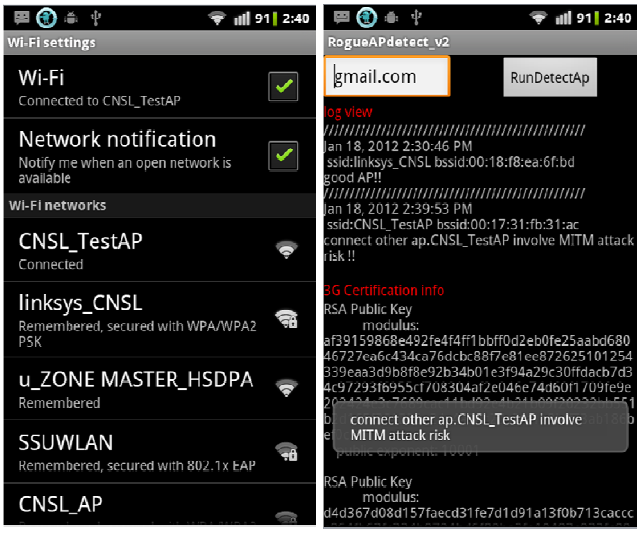


Figure 9 Result of the MITM attack situation

VI. A COMPARISON OF DEFENSE TECHNIQUES

MITM attack detection techniques have already been proposed through the use of additional equipment or the use of wireless sensors. Another approach like radius authentication server which uses a wired or wireless network

with prevention techniques and detection methods that are managed by the operator to detect man-in-the-middle attack techniques in same network also need separate equipment required to install and operate, and must be regularly monitored by the administrator. Table II shows the comparison between various defense techniques

TABLE II. A COMPARISON TABLE OF DEFENSE TECHNIQUES

Techniques	Cost	Features	Requirements
Detect rogues AP with sensor	High cost to install a wide range	Detect man-in-the-middle attacks by analyzing packets	Requires a large number of sensors
Rogue AP Protection System Based On Radius Authentication Server	High cost to installation and maintenance costs	Radius authentication server can communicate with the AP through a secure	Difficulties detect rogue AP on open environment
Detection technique using wired and wireless networks	High cost to installation and maintenance costs	Get information from wired and wireless network	Difficulties detect rogue AP on open environment
Detect rogue AP Using 3G network	None	User terminal can be detected n the man-in-the-middle attacks	Install application

However, the proposed technique without modification to an existing protocol from the user terminal and no additional equipment needed, is available in any location and environment, man-in-the-middle attacks can be detected directly from your handset, so users can apply in every situation, because what they are compared to existing techniques it can be called a practical and effective.

VII. CONCLUSIONS

As the WiFi smart phone users increase, security threats also increase. To protect user privacy at the Web server, a secure SSL authentication technique is applied against man-in-the-middle attacks, but the risk of hacking still exists. To prevent this attack, many techniques and services have been proposed to be applied to all users, but the implementation cost is a limit. Proposed scheme is very simple and effective for detecting man-in-the-middle attacks because it does not require huge implementation cost or expensive security sensors. The other advantage of our system is that users can directly determine man-in-the-middle attack at any time and any place. Our scheme does not need any modification in current protocol or developing a new protocol, so it is a practical and effective technique. The disadvantage of proposed method is that it can only detect an attack which attempts to modify the certificate. We will further study other types of attacks to make our solution to be more applicable.

ACKNOWLEDGMENT

"This research was supported by the KCC (Korea Communications Commission), Korea, under the R&D program supervised by the KCA (Korea Communications Agency)" (KCA-2012- 08-911-05-001)

REFERENCES

[1] K. Cheng, M. Gao, and R. Guo, "Analysis and Research on HTTPS Hijacking Attacks," 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, IEEE, pp. 223-226, Apr. 2010.

[2] M. Moixe, "New Tricks For Defeating SSL in Practice", BlackHat Conference, USA. Feb. 2009.

[3] T. Koutny, "Detecting Unauthorized Modification of HTTP Communication with Steganography," 2010 Fifth International Conference on Internet and Web Applications and Services, IEEE, pp. 26-31, May. 2010.

[4] Internet Incident Response Support Center, " Internet Attack Trends and Analysis," Korea Information Security Agency, pp. 22-37, Jun. 2007

[5] D. Jiang, L. Xinghui, and H. Hua, "A Study of Man-in-the-Middle Attack Based on SSL Certificate Interaction," 2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp. 445-448, Oct. 2011.

[6] F. Callegati, W. Cerroni, and M. Ramilli,, "Man-in-the-Middle Attack to the HTTPS Protocol," Security & Privacy, IEEE, pp. 78-81, 2009.

[7] R. Meyer, "Secure Authentication on the Internet, " SANS InfoSec Reading Room - Securing Code, Feb. 2008.

[8] S. Yimin, Y. Chao, and G. Guofei, "Who Is Peeping at Your Passwords at Starbucks? - To Catch an Evil Twin Access Point," International Conference on Dependable Systems & Networks (DSN), IEEE, June. 2010.

[9] T. Chomsiri, "HTTPS Hacking Protection, " 21st International Conference on Advanced Information Networking and Applications Workshops, IEEE, May. 2007.

[10] K. kuofong, L .ien, and L. Yuehchia, "Detecting rogue access points using client-side bottleneck bandwidth analysis," Computers & Security, vol. 24(3-4), ELSEVIER, pp. 144-152, May. 2009.

[11] L. Watkins, R. Beyah, C. Corbett, "A Passive Approach to Rogue Access Point Detection," Global Telecommunications Conference, 2007. IEEE. pp. 355-360, Nov.2007

[12] K. DongPhil, K. chulbum, and K. Sangwook, "Rogue AP Protection System Based On Radius Authentication Server," Korean Institute of Information Scientists and Engineers, vol. 31(1), April, 2004.

[13] 3GPP TS 33.102, "3G security; Security architecture," 3GPP, Rel-11, version11.1.0, Dec. 2012.

[14] K. Kuofong, Y.Taoheng, Y.waishuoen, and C.Huihsuan, "A location-aware rogue AP detection system based on wireless packet sniffing of sensor APs," SAC '11 Proceedings of the 2011 ACM Symposium on Applied Computing, ACM, 2011.

[15] B. Yan, G. Chen, J. Wang, and H. Yin, "Robust Detection of Unauthorized Wireless Access Points," Mobile Networks and Applications Journal, vol. 14(4), pp. 508-522, Aug. 2009.

[16] R. Beyah, "Rogue access point detection_challenges, solutions, and future directions," IEEE Security and Privacy Article, vol. 9(5), IEEE, pp. 56-61, 2011.

 ISBN: 978-1-61208-204-2

A Robust Data Hiding Process Contributing to the Development of a Semantic Web

Jacques M. Bahi, Jean-François Couchot, Nicolas Friot, and Christophe Guyeux
FEMTO-ST Institute, UMR 6174 CNRS
Computer Science Laboratory DISC
University of Franche-Comté
Besançon, France
{jacques.bahi, jean-francois.couchot, nicolas.friot, christophe.guyeux}@femto-st.fr

***Abstract*—In this paper, a novel steganographic scheme based on chaotic iterations is proposed. This research work takes place into the information hiding framework, and focus more specifically on robust steganography. Steganographic algorithms can participate in the development of a semantic web: medias being on the Internet can be enriched by information related to their contents, authors, etc., leading to better results for the search engines that can deal with such tags. As media can be modified by users for various reasons, it is preferable that these embedding tags can resist to changes resulting from some classical transformations as for example cropping, rotation, image conversion, and so on. This is why a new robust watermarking scheme for semantic search engines is proposed in this document. For the sake of completeness, the robustness of this scheme is finally compared to existing established algorithms.**

***Keywords*-*Semantic Web*; *Information Hiding*; *Steganography*; *Robustness*; *Chaotic Iterations*.**

I. Introduction

Social search engines are frequently presented as a next generation approach to query the world wide web. In this conception, contents like pictures or movies are tagged with descriptive labels by contributors, and search results are enriched with these descriptions. These collaborative taggings, used for example in Flickr [2] and Delicious [1] websites, can participate to the development of a Semantic Web, in which every Web page contains machine-readable metadata that describe its content. To achieve this goal by embedding such metadata, information hiding technologies can be useful. Indeed, the interest to use such technologies lays on the possibility to realize social search without websites and databases: descriptions are directly embedded into media, whatever their formats.

In the context of this article, the problem consists in embedding tags into internet medias, such that these tags persist even after user transformations. Robustness of the chosen watermarking scheme is thus required in this situation, as descriptions should resist to user modifications like resizing, compression, and format conversion or other classical user transformations in the field. Indeed, quoting Kalker in [11], "Robust watermarking is a mechanism to create a communication channel that is multiplexed into original content [...] It is required that, firstly, the perceptual degradation of the marked content [...] is minimal and, secondly, that the capacity of the watermark channel degrades as a smooth function of the degradation of the marked content". The development of social web search engines can thus be strengthened by the design of robust information hiding schemes. Having this goal in mind, we explain in this article how to set up a secret communication channel using a new robust steganographic process called $\mathcal{DI}_3$. This new scheme has been theoretically presented in [4] with an evaluation of its security. So, the main objective of this work is to focus on robustness aspects presenting firstly other known schemes in the literature, and presenting secondly this new scheme and and evaluate its robustness. This article is thus a first work on the subject, and the comparison with other schemes concerning the robustness will be realized in future work.

The remainder of this document is organized as follows. In Section II, some basic reminders concerning the notion of Most and Least Significant Coefficients are given. In Section III, some well-known steganographic schemes are recalled, namely the YASS [17], nsF5 [8], MMx [12], and HUGO [15] algorithms. In the next section the implementation of the steganographic process $\mathcal{DI}_3$ is detailed, and its robustness study is exposed in Section V. This research work ends by a conclusion section, where our contribution is summarized and intended future researches are presented.

II. Most and Least Significant Coefficients

We first notice that terms of the original content x that may be replaced by terms issued from the watermark y are less important than others: they could be changed without be perceived as such. More generally, a *signification function* attaches a weight to each term defining a digital media, depending on its position t.

Definition 1: *A* signification function *is a real sequence* $(u^k)^{k\in\mathbb{N}}$. □

Example 1: *Let us consider a set of grayscale images stored into portable graymap format (P3-PGM): each pixel ranges between 256 gray levels, i.e., is memorized with eight bits. In that context, we consider* $u^k = 8-(k \mod 8)$ *to be*

 ISBN: 978-1-61208-204-2

the k-th term of a signification function $(u^k)^{k\in\mathbb{N}}$. Intuitively, in each group of eight bits (i.e., for each pixel) the first bit has an importance equal to 8, whereas the last bit has an importance equal to 1. This is compliant with the idea that changing the first bit affects more the image than changing the last one. □

Definition 2: *Let $(u^k)^{k\in\mathbb{N}}$ be a signification function, m and M be two reals s.t. $m < M$.*

- *The* most significant coefficients (MSCs) *of x is the finite vector*

$$u_M = \left(k \mid k \in \mathbb{N} \text{ and } u^k \geqslant M \text{ and } k \leq \mid x \mid\right);$$

- *The* least significant coefficients (LSCs) *of x is the finite vector*

$$u_m = \left(k \mid k \in \mathbb{N} \text{ and } u^k \leq m \text{ and } k \leq \mid x \mid\right);$$

- *The* passive coefficients *of x is the finite vector*

$$u_p = \left(k \mid k \in \mathbb{N} \text{ and } u^k \in]m; M[\text{ and } k \leq \mid x \mid\right).$$

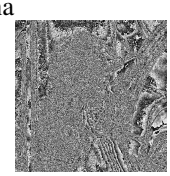
For a given host content x, MSCs are then ranks of x that describe the relevant part of the image, whereas LSCs translate its less significant parts.

Remark 1: *When MSCs and LSCs represent a sequence of bits, they are also called Most Significant Bits (MSBs) and Least Significant Bits (LSBs). In the rest of this article, the two notations will be used depending on the context.* □

Example 2: *These two definitions are illustrated on Figure 1, where the significance function (u^k) is defined as in Example 1, $m = 5$, and $M = 6$.*

(a) Original Lena

(b) MSCs of Lena



(c) LSCs of Lena ($\times$17)

Figure 1. Most and least significant coefficients of Lena

III. STEGANOGRAPHIC SCHEMES

To compare the approach with other schemes, we now present recent steganographic approaches, namely YASS (Cf setc. III-A), nsF5 (Cf setc. III-B), MMx (Cf setc. III-C), and HUGO (Cf setc. III-D). One should find more details in [7].

A. YASS

YASS (*Yet Another Steganographic Scheme*) [17] is a steganographic approach dedicated to JPEG cover. The main idea of this algorithm is to hide data into 8×8 randomly chosen inside $B \times B$ blocks (where B is greater than 8) instead of choosing standard 8×8 grids used by JPEG compression. The self-calibration process commonly embedded into blind steganalysis schemes is then confused by the approach. In the paper [16], further variants of YASS have been proposed simultaneously to enlarge the embedding rate and to improve the randomization step of block selecting. More precisely, let be given a message m to hide, a size B, $B \geq 8$, of blocks. The YASS algorithm follows.

1) Computation of m', which is the Repeat-Accumulate error correction code of m.
2) In each big block of size $B \times B$ of cover, successively do:
   a) Random selection of an 8×8 block b using w.r.t. a secret key.
   b) Two-dimensional DCT transformation of b and normalisation of coefficient w.r.t a predefined quantization table. Matrix is further referred to as b'.
   c) A fragment of m' is embedded into some LSB of b'. Let b'' be the resulting matrix.
   d) The matrix b'' is decompressed back to the spatial domain leading to a new $B \times B$ block.

B. nsF5

The nsF5 algorithm [8] extends the F5 algorithm [18]. Let us first have a closer look on this latter.

First of all, as far as we know, F5 is the first steganographic approach that solves the problem of remaining unchanged a part (often the end) of the file. To achieve this, a subset of all the LSB is computed thanks to a pseudo random number generator seeded with a user defined key. Next, this subset is split into blocks of x bits. The algorithm takes benefit of binary matrix embedding to increase it efficiency. Let us explain this embedding on a small illustrative example where a part m of the message has to be embedded into this x LSB of pixels which are respectively a 3 bits column vector and a 7 bits column vector. Let then H be the binary Hamming matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

The objective is to modify x to get y s.t. $m = Hy$. In this algebra, the sum and the product respectively correspond to the exclusive *or* and to the *and* Boolean operators. If Hx is already equal to m, nothing has to be changed and x can be sent. Otherwise we consider the difference $\delta = d(m, Hx)$

 ISBN: 978-1-61208-204-2

which is expressed as a vector :

$$\delta = \begin{pmatrix} \delta_1 \\ \delta_2 \\ \delta_3 \end{pmatrix} \text{ where } \delta_i \text{ is 0 if } m_i = Hx_i \text{ and 1 otherwise.}$$

Let us thus consider the jth column of H which is equal to δ. We denote by $\overline{x}^j$ the vector we obtain by switching the jth component of x, that is, $\overline{x}^j = (x_1, \ldots, \overline{x_j}, \ldots, x_n)$. It is not hard to see that if y is $\overline{x}^j$, then $m = Hy$. It is then possible to embed 3 bits in only 7 LSB of pixels by modifying on average $1 - 2^3$ changes. More generally, the F5 embedding efficiency should theoretically be $\frac{p}{1-2^p}$.

However, the event when the coefficient resulting from this LSB switch becomes zero (usually referred to as *shrinkage*) may occur. In that case, the recipient cannot determine whether the coefficient was -1, +1 and has changed to 0 due to the algorithm or was initially 0. The F5 scheme solves this problem first by defining a LSB with the following (not even) function:

$$LSB(x) = \begin{cases} 1 - x \mod 2 \text{ if } x < 0 \\ x \mod 2 \text{ otherwise.} \end{cases} .$$

Next, if the coefficient has to be changed to 0, the same bit message is re-embedded in the next group of x coefficient LSB.

The scheme nsF5 focuses on steps of Hamming coding and ad'hoc shrinkage removing. It replaces them with a *wet paper code* approach that is based on a random binary matrix. More precisely, let D be a random binary matrix of size $x \times n$ without replicate nor null columns: consider for instance a subset of $\{1, 2^x\}$ of cardinality n and write them as binary numbers. The subset is generated thanks to a PRNG seeded with a shared key. In this block of size x, one choose to embed only k elements of the message m. By abuse, the restriction of the message is again called m. It thus remains $x - k$ (wet) indexes/places where the information shouldn't be stored. Such indexes are generated too with the keyed PRNG. Let v be defined by the following equation:

$$Dv = \delta(m, Dx). \quad (1)$$

This equation may be solved by Gaussian reduction or other more efficient algorithms. If there is a solution, one have the list of indexes to modify into the cover. The nsF5 scheme implements such a optimized algorithm that is to say the LT codes.

C. MMx

Basically, the MMx algorithm [12] embeds message in a selected set of LSB cover coefficients using Hamming codes as the F5 scheme. However, instead of reducing as many as possible the number of modified elements, this scheme aims at reducing the embedding impact. To achieve this it allows to modify more than one element if this leads to decrease distortion.

Let us start again with an example with a $[7, 4]$ Hamming codes, *i.e*, let us embed 3 bits into 7 DCT coefficients, $D_1, \ldots, D_7$. Without details, let $\rho_1, \ldots, \rho_7$ be the embedding impact whilst modifying coefficients $D_1, \ldots, D_7$ (see [12] for a formal definition of ρ). Modifying element at index j leads to a distortion equal to ρ_j. However, instead of switching the value at index j, one should consider to find all other columns of H, j_1, j_2 for instances, s.t. the sum of them is equal to the jth column and to compare ρ_j with $\rho_{j_1} + \rho_{j_2}$. If one of these sums is less than ρ_j, the sender has to change these coefficients instead of the j one. The number of searched indexes (2 for the previous example) gives the name of the algorithm. For instance in MM3, one check whether the message can be embedded by modifying 3 pixel or less each time.

D. HUGO

The HUGO [15] steganographic scheme is mainly designed to minimize distortion caused by embedding. To achieve this, it is firstly based on an image model given as SPAM [14] features and next integrates image correction to reduce much more distortion. What follows refers to these two steps.

The former first computes the SPAM features. Such calculi synthesize the probabilities that the difference between consecutive horizontal (resp. vertical, diagonal) pixels belongs in a set of pixel values which are closed to the current pixel value and whose radius is a parameter of the approach. Thus, a fisher linear discriminant method defines the radius and chooses between directions (horizontal, vertical, etc.) of analyzed pixels that gives the best separator for detecting embedding changes. With such instantiated coefficients, HUGO can synthesize the embedding cost as a function $D(X, Y)$ that evaluates distortions between X and Y. Then HUGO computes the matrices of $\rho_{i,j} = \max(D(X, X^{(i,j)+})_{i,j}, D(X, X^{(i,j)-})_{i,j})$ such that $X^{(i,j)+}$ (resp. $X^{(i,j)-}$) is the cover image X where the the (i, j)th pixel has been increased (resp. has been decreased) of 1.

The order of modifying pixel is critical: HUGO surprisingly modifies pixels in decreasing order of $\rho_{i,j}$. Starting with $Y = X$, it increases or decreases its (i, j)th pixel to get the minimal value of $D(Y, Y^{(i,j)+})_{i,j}$ and $D(Y, Y^{(i,j)-})_{i,j}$. The matrix Y is thus updated at each round.

IV. The new steganographic process $\mathcal{DI}_3$

A. Implementation

In this section, a new algorithm which is inspired from the schemes $\mathcal{CIW}_1$ and $\mathcal{CIS}_2$ respectively described in [9] and [10] is presented. Compare to the first one, it is a steganographic scheme, not just a watermarking technique. Unlike $\mathcal{CIS}_2$ which require embedding keys with three strategies, only one is required for $\mathcal{DI}_3$. So compare to

 ISBN: 978-1-61208-204-2

$\mathcal{CIS}_2$ which is also a steganographic process, it is easier to implement for Internet applications especially in order to contribute to a semantic web. Moreover, since $\mathcal{DI}_3$ is a particular instance of $\mathcal{CIS}_2$, it is clearly faster than this one because in $\mathcal{DI}_3$ there is no operation to mix the message on the contrary on the initial scheme. The fast execution of such an algorithm is critical for internet applications.

In the following algorithms, the following notations are used:

Notation 1: *S denotes the embedding and extraction strategy, H the host content or the stego-content depending of the context. LSC denotes the old or new LSCs of the host or stego-content H depending of the context too. N denotes the number of LSCs, λ the number of iterations to realize, M the secret message, and P the width of the message (number of bits).* □

Our new scheme theoretically presented in [4] is here described by three main algorithms:

1) The first one, detailed in Algorithm 1 allows to generate the embedding strategy of the system which is a part of the embedding key in addition with the choice of the LSCs and the number of iterations to realize.
2) The second one, detailed in Algorithm 2 allows to embed the message into the LSCs of the cover media using the strategy. The strategy has been generated by the first algorithm and the same number of iterations is used.
3) The last one, detailed in Algorithm 3 allows to extract the secret message from the LSCs of the media (the stego-content) using the strategy wich is a part of the extraction key in addition with the width of the message.

In adjunction of these three functions, two other complementary functions have to be used:

1) The first one, detailed in Algorithm 4, allow to extract MSCs, LSCs, and passive coefficients from the host content. Its implementation is based on the concept of signification function described in Definition 2.
2) The last one, detailed in Algorithm 5, allow to rebuild the new host content (the stego-content) from the corresponding MSCs, LSCs, and passive coefficients. Its implementation is also based on the concept of signification function described in Definition 2. This function realize the invert operation of the previous one.

Remark 2: *The two previous algorithms have to be implemented by the user depending on each application context should be adjusted accordingly: either in spatial description, in frequency description, or in other description. They correspond to the theoretical concept described in Definition 2. Their implementation depends on the application context.* □

Example 3: *For example the algorithm 4 in spatial domain can correspond to the extraction of the 3 last bits of each pixel as LSCs, the 3 first bits as MSCs, and the 2 center bits as passive coefficients.* □

Algorithm 1: $strategy(N, P, \lambda)$

```
/* S is a sequence of integers into
   [[0, P-1]], such that (S_{n_0}, ..., S_{n_0+P-1})
   is injective on [[0, P-1]].                    */
Result: S: The strategy, integer sequence (S_0, S_1, ...).
begin
    n_0 ⟵ L - P + 1;
    if P > N OR n_0 < 0 then
        return ERROR
    S ⟵ Array of width λ, all values initialized to 0;
    cpt ⟵ 0;
    while cpt < n_0 do
        S_cpt ⟵Random integer in [[0, P-1]].;
        cpt ⟵ cpt + 1;
    A ⟵ We generate an arrangement of [[0, P-1]];
    for k ∈ [[0, P-1]] do
        S_{n_0+k} ⟵ A_k;
    return S
end
```

Algorithm 2: $embed(LSC, M, S, \lambda)$

```
Result: New LSCs with embedded message.
begin
    N ⟵ Number of LSCs in LSC;
    P ⟵ Width of the message M;
    for k ∈ [[0, λ]] do
        i ⟵ S_k;
        LSC_i ⟵ M_i;
    return LSC
end
```

Algorithm 3: $extract(LSC, S, \lambda, P)$

```
Result: The message to extract from LSC.
begin
    RS ⟵ The strategy S written in reverse order.;
    M ⟵ Array of width P, all values initialized to 0;
    for k ∈ [[0, λ]] do
        i ⟵ RS_k;
        M_i ⟵ LSC_i;
    return M
end
```

B. Discussion

We first notice that our $\mathcal{DI}_3$ scheme embeds the message in LSB as all the other approaches. Furthermore, among all

Algorithm 4: $significationFunction(H)$

Data: H: The original host content.
Result: MSC: MSCs of the host content H.
Result: PC: Passive coefficients of the host content H.
Result: LSC: LSCs of the host content H.
begin
  /* Implemented by the user. */
  return (MSC, PC, LSC)
end

Algorithm 5: $buildFunction(MSC, PC, LSC)$)

Result: H: The new rebuilt host content.
begin
  /* Implemented by the user. */
  return (MSC, PC, LSC)
end

the LSB, the choice of those which are modified according to the message is based on a secured PRNG whereas F5, and thus nsF5 only require a PRNG. Finally in this scheme, we have postponed the optimization of considering again a subset of them according to the distortion their modification may induce. According to us, further theoretical study are necessary to take this feature into consideration. In future work, it is planed to compare the robustness and efficiency of all the schemes in the context of semantic web. To initiate this study in this first article, the robustness of $\mathcal{DI}_3$ is detailled in the next section.

V. Robustness Study

This section evaluates the robustness of our approach [5].

Each experiment is build on a set of 50 images which are randomly selected among database taken from the BOSS contest [6]. Each cover is a 512×512 greyscale digital image. The relative payload is always set with 0.1 bit per pixel. Under that constrain, the embedded message m is a sequence of 26214 randomly generated bits.

Following the same model of robustness studies in previous similar work in the field of information hiding, we choose some classical attacks like cropping, compression, and rotation studied in this research work. Other attacks and geometric transformations will be explore in a complementary study. Testing the robustness of the approach is achieved by successively applying on stego content images attacks. Differences between the message that is extracted from the attacked image and the original one are computed and expressed as percentage.

To deal with cropping attack, different percentage of cropping (from 1% to 81%) are applied on the stego content image. Fig. 2 (c) presents effects of such an attack.

We address robustness against JPEG an JPEG 2000 compression. Results are respectively presented in Fig. 2 (a) and in Fig. 2 (b).

Attacked based on geometric transformations are addressed through rotation attacks: two opposite rotations of angle θ are successively applied around the center of the image. In these geometric transformations, angles range from 2 to 20 degrees. Results effects of such an attack are also presented in Fig. 2 (d).

From all these experiments, one firstly can conclude that the steganographic scheme does not present obvious drawback and resists to all the attacks: all the percentage differences are so far less than 50%.

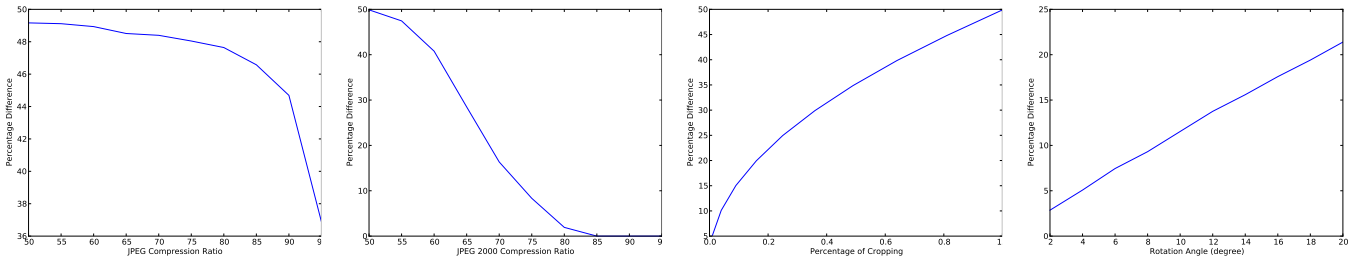
The comparison with robustness of other steganographic schemes exposed in the work will be realize in a complementary study, and the best utilization of each one in several context will be discuss.

VI. Conclusion and future work

In this research work, a new information hiding algorithm has been introduced to contribute to the semantic web. We have focused our work on the robustness aspect. The security has been studied in an other work [4]. Even if this new scheme $\mathcal{DI}_3$ does not possess topological properties (unlike the $\mathcal{CIS}_2$ [9]), its level of security seems to be sufficient for Internet applications. Particularly in the framework of the semantic web it is required to have robust steganographic processes. The security aspects is less important in this context. Indeed, it is important that the enrichment information persist after an attack. Especially for JPEG 2000 attacks, which are the two major attacks used in an internet framework. Additionally, this new scheme is faster than $\mathcal{CIS}_2$. This is a major advantage for an utilization through the Internet, to respect response times of web sites.

In a future work we intend to prove rigorously that $\mathcal{DI}_3$ is not topologically secure. The tests of robustness will be realized on a larger set of images of different types and sizes, using resources of the *Mésocentre de calcul de Franche-Comté [13] (an High-Performance Computing (HPC) center)* and using Jace environment [3], to take benefits of parallelism. So, the robustness and efficiency of our scheme $\mathcal{DI}_3$ will be compared to other schemes in order to show the best utilization in several contexts. Other kinds of attacks will be explored to evaluate more completely the robustness of the proposed scheme. For instance, robustness of the $\mathcal{DI}_3$ against Gaussian blur, rotation, contrast, and zeroing attacks will be regarded, and compared with a larger set of existing steganographic schemes as those described in this article. Unfortunately these academic algorithms are mainly designed to show their ability in embedding. Decoding aspect is rarely treated, and rarely implemented at all. Finally, a first web search engine compatible with the proposed robust watermarking scheme will be written, and

 ISBN: 978-1-61208-204-2



(a) JPEG effect. (b) JPEG 2000 effect. (c) Cropping attack. (d) Rotation attack.

Figure 2. Robustness of $\mathcal{DI}_3$ scheme facing several attacks (50 images from the BOSS repository)

automatic tagging of materials found on the Internet will be realized, to show the effectiveness of the approach.

REFERENCES

[1] Delicious social bookmarking, http://delicious.com/. Retrieved June, 2012 from http://delicious.com/.

[2] The frick collection, http://www.frick.org/. Retrieved June, 2012 from http://www.frick.org/.

[3] Jacques Bahi, Mourad Hakem, and Kamel Mazouzi. Reliable parallel programming model for distributed computing environments. In *HeteroPar'09*, volume 6043 of *LNCS*, pages 162–171, Delft, Netherlands, 2009. Springer.

[4] Jacques M. Bahi, François Couchot, Nicolas Friot, and Christophe Guyeux. Application of steganography for anonymity through the internet. In *IHTIAP'2012, The First Workshop on Information Hiding Techniques for Internet Anonymity and Privacy*, pages ***–***, Venice, Italy, June 2012. To appear.

[5] Jacques M. Bahi, Jean-François Couchot, and Christophe Guyeux. Steganography: A class of secure and robust algorithms. *The Computer Journal*, 55(6):653–666, 2012.

[6] P. Bas, T. Filler, and T. Pevný. Break our steganographic system — the ins and outs of organizing boss. In T. Filler, editor, *Information Hiding, 13th International Workshop*, Lecture Notes in Computer Science, Prague, Czech Republic, May 18–20, 2011. Springer-Verlag, New York.

[7] Jessica Fridrich. *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press, New York, NY, USA, 1st edition, 2009.

[8] Jessica J. Fridrich, Tomás Pevný, and Jan Kodovský. Statistically undetectable jpeg steganography: dead ends challenges, and opportunities. In Deepa Kundur, Balakrishnan Prabhakaran, Jana Dittmann, and Jessica J. Fridrich, editors, *MM&Sec*, pages 3–14. ACM, 2007.

[9] Nicolas Friot, Christophe Guyeux, and Jacques M. Bahi. Chaotic iterations for steganography - stego-security and chaos-security. In Javier Lopez and Pierangela Samarati, editors, *SECRYPT*, pages 218–227. SciTePress, 2011.

[10] Christophe Guyeux, Nicolas Friot, and Jacques Bahi. Chaotic iterations versus spread-spectrum: chaos and stego security. In *IIH-MSP'10, 6-th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, pages 208–211, Darmstadt, Germany, October 2010.

[11] T. Kalker. Considerations on watermarking security. In *Multimedia Signal Processing, 2001 IEEE Fourth Workshop on*, pages 201–206, 2001.

[12] Younhee Kim, Zoran Duric, and Dana Richards. Modified matrix encoding technique for minimal distortion steganography. In Jan Camenisch, Christian S. Collberg, Neil F. Johnson, and Phil Sallee, editors, *Information Hiding*, volume 4437 of *Lecture Notes in Computer Science*, pages 314–327. Springer, 2006.

[13] University of Franche-Comté. Le mésocentre de calcul de franche-comté, an high-performance computing (hpc) center. Retrieved June, 2012 from http://meso.univ-fcomte.fr/, 2012.

[14] Tomás Pevný, Patrick Bas, and Jessica J. Fridrich. Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on Information Forensics and Security*, 5(2):215–224, 2010.

[15] Tomás Pevný, Tomás Filler, and Patrick Bas. Using high-dimensional image models to perform highly undetectable steganography. In Rainer Böhme, Philip W. L. Fong, and Reihaneh Safavi-Naini, editors, *Information Hiding*, volume 6387 of *Lecture Notes in Computer Science*, pages 161–177. Springer, 2010.

[16] Anindya Sarkar, Kaushal Solanki, and B. S. Manjunath. Further study on yass: Steganography based on randomized embedding to resist blind steganalysis. In *Security, forensics, steganography, and watermarking of multimedia contents X, San Jose CA , USA*, pages 1–11, 2008.

[17] Kaushal Solanki, Anindya Sarkar, and B. S. Manjunath. Yass: Yet another steganographic scheme that resists blind steganalysis. In Teddy Furon, François Cayre, Gwenaël J. Doërr, and Patrick Bas, editors, *Information Hiding*, volume 4567 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2007.

[18] Andreas Westfeld. F5-a steganographic algorithm. In Ira S. Moskowitz, editor, *Information Hiding*, volume 2137 of *Lecture Notes in Computer Science*, pages 289–302. Springer, 2001.

 ISBN: 978-1-61208-204-2

Federation Between CLEVER Clouds Through SASL/Shibboleth Authentication

Francesco Tusa, Antonio Celesti, Massimo Villari and Antonio Puliafito
Dept. of Mathematics, Faculty of Engineering, University of Messina
Contrada di Dio, S. Agata, 98166 Messina, Italy.
e-mail: {ftusa, acelesti, mvillari, apuliafito}@unime.it

***Abstract*—Several ICT operators are realizing the advantages of federating cloud providers in order to carry out new business benefits, hence increasing their revenues. Nevertheless, how to achieve a cloud architecture able to perform authentication with other installations is not fully clear. CLEVER is a cloud IaaS middleware conceived with federation in mind. In this paper, we discuss an approach to perform SSO authentication based on an integration between SASL and SAML in a CLEVER environment. More specifically, we describe how to federated the Ejabberd servers, on which the communication of each CLEVER cloud is based, through a Shibboleth authentication.**

Keywords-Cloud Computing; CLEVER; Federation; Security; SASL; SSO Authentication; SAML; Shibboleth.

I. INTRODUCTION

Nowadays, most of Cloud providers can be considered as "islands in the ocean of the Cloud computing" and do not present any form of federation. At the same time, a few Clouds are beginning to use the Cloud-based services of other Clouds, but there is still a long way to go toward the establishment of a worldwide Cloud ecosystem including thousands of cooperating Clouds. In such a perspective, the latest trend toward Cloud computing is dominated by the idea to federate heterogeneous Clouds, as it is highlighted in [1]. This means not to think about independent private Clouds anymore, but to consider a new Cloud federation scenario where different Clouds, belonging to different administrative domains, interact each other, sharing and gaining access to physical resources. Cloud Federation is a concept that goes beyond the simple achievements falling into Hybrid Clouds (Private + Public, see [2]).

The US Department of NIST, after the well-known definition of *SaaS, PaaS and IaaS*, is actively working for accelerating Standards to foster the Adoption of Cloud Computing [3]. *Interoperability, Portability and Security* are the main aims of their enforcement. Our work tries to find a solution for the first and third of these aspects seen for federated Cloud scenarios, exploiting CLEVER (see [4]). It is an IaaS Cloud middleware, conceived having in mind federation. The innovation of CLEVER is that its communication system has been designed with the public-subscribe philosophy using the Extensible Messaging and Presence Protocol (XMPP) [5] (see also RFC 6120 [6]). XMPP is an open-standard communications protocol for message-oriented middleware based on XML (Extensible Markup Language). Thus, in CLEVER, each Cloud belongs to a domain managed by an XMPP server. In CLEVER, the way to federate two Clouds is to establish a server-to-server inter-domain communication between the XMPP servers of the involved Clouds.

Cloud federation raises many issues especially in the field of security and privacy. Single Sign On (SSO) authentication is fundamental for achieving security in a scalable scenario such as Cloud federation. However, the Simple Authentication and Security Layer (SASL) [7], i.e., a framework for authentication and data security in Internet protocols, supported by XMPP does not support any SSO authentication mechanism.

In this paper, integrating the SASL with the Security Assertion Markup Language (SAML) protocol [8], we describe an approach to authenticate two or more CLEVER Clouds, discussing an implementation based on Ejabberd [9] and Shibboleth [10]. The paper is organized as follows. Section II describes the state of the art of Cloud middlewares dealing with federation. Section III introduces the CLEVER Cloud middleware, discussing how it supports federation. Section IV describes the technological issues for the SSO authentication achievement during the process of federation establishment. More specifically, a solution based on SASL and SAML is discussed. Section V describes an implementation practice of SSO authentication between CLEVER Clouds using Ejabberd servers and Shibboleth. Section VI concludes the paper.

II. RELATED WORKS

Hereby, we describe the current state-of-the-art in Cloud computing analyzing the main existing middleware implementations, emphasizing the federation aspects they attempt to address. Before such a description, it is interesting to point out the results of Sempolinski and Thain work published in 2010 [11]. They provided a comparison among three widely used architectures: Nimbus, Eucalyptus and OpenNebula. They remarked how the projects are aimed at different goals, but a clear convergence is recognizable. The authors posed three main questions, one about who has a complete Cloud computing software stack. It is common in the three architectures that the actual Cloud controller is only a small part of the overall system. The second one is who is really

 ISBN: 978-1-61208-204-2

customizable. These are open-source projects, and the appeal of setting up a private Cloud, as opposed to using a commercial one, is that the administrator can have more control over the system. They support standard API interfaces (i.e., front-end that uses a subset of the EC2 interface), and they are often one of these customizable components. The last one is about the degree of transparency in the user interface. One of the main shared opinions in the commercial Cloud setting is the black-box nature of the system. The individual user, is not aware where, physically, his VMs are running. In a more customizable open-source setting, however, opportunities exist for a greater degree of explicit management with regard to the underlying configuration of physical machine and the location of the VMs. We remark that the authors of such a work have not recognized any features suitable for the cross Cloud management.

Nimbus [12] is an open source toolkit that allows to turn a set of computing resources into an Iaas Cloud. It was conceived from designers originally coming from the GRID world. Nimbus comes with a component called workspace-control, installed on each node, used to start, stop and pause VMs, implements VM image reconstruction and management, securely connects the VMs to the network, and delivers contextualization. Nimbus's workspace-control tools work with Xen and KVM but only the Xen version is distributed. Nimbus provides interfaces to VM management functions based on the WSRF set of protocols. There is also an alternative implementation exploiting Amazon EC2 WSDL. Its Federation system exploits the GRID-like existing functionalities. It leverages Virtual Organization (VOs) of GRID for controlling the access on virtual resources.

Eucalyptus [13] is an open-source Cloud-computing framework that uses the computational and storage infrastructures commonly available at academic research groups to provide a platform that is modular and open to experimental instrumentation and study. Eucalyptus addresses several crucial Cloud computing questions, including VM instance scheduling, Cloud computing administrative interfaces, construction of virtual networks, definition and execution of service level agreements (Cloud/user and Cloud/Cloud), and Cloud computing user interfaces. Not far past Eucalyptus was adopted as Virtualization Manager in the Ubuntu Core, but recently there is not longer support (Canonical switches to OpenStack for Ubuntu Linux Cloud [14]). The federation is out of the scope for them.

OpenNebula [15] is a virtualization tool to manage virtual infrastructures in a data-center or cluster, which is usually referred as private Cloud. Only the more recent versions of OpenNebula are trying to supports Hybrid Cloud to combine local infrastructure with public Cloud-based infrastructure, enabling highly scalable hosting environments. OpenNebula also supports Public Clouds by providing Cloud interfaces to expose its functionalities for virtual machine, storage and network management. The middleware tries to manage the federated resources but, considering the approach they use for interacting with physical servers (SSH remote shell commands), it is quite hard to accomplish real federation achievements. OpenNebula is mainly aimed at interoperability through OCCI interface.

A separated analysis has to be faced with the OpenStack [16] middleware because it operates in the direction of an open middleware for Clouds. The National Aeronautics and Space Administration (NASA) leads the project aiming to allow any organization to create and offer Cloud computing capabilities using open source software running on standard hardware. Openstack has three sub-projects that is OpenStack Compute, OpenStack Object Store and OpenStack Imaging Service. In particular OpenStack Compute is a software for automatically creating and managing large groups of virtual private servers. Open-Stack Storage is a software for creating redundant, scalable object storage using clusters of commodity servers to store terabytes or even petabytes of data. It adopts the Shared Nothing (SN), an architectural philosophy in which the platform is fully distributed and each node is independent and self-sufficient, and there is no single point of contention across the system. OpenStack Image Service is necessary for discovering, registering, and retrieving virtual machine images. The federation is not addressed at all in Openstack, the concepts Shared Nothing guarantees a high level of scalability and reliability, but at the same time the federation needs to be accomplished out of the architecture, at least as a *Federation Broker* that solves some of the federation issues. The SSO is only aimed at the dashboard web access, that is for the end-user.

III. THE CLEVER IAAS CLOUD

A. Overview

The CLEVER middleware is based on the architecture schema depicted in Figure 1, which shows a cluster of n nodes (also an interconnection of clusters could be analyzed) each containing a host level management module (Host Manager). A single node may also include a cluster level management module (Cluster Manager). All the entities interact exchanging information by mean of the Communication System based on the XMPP. The set of data necessary to enable the middleware functioning is stored within a specific Database deployed in a distributed fashion.

Figure 1 shows the main components of the CLEVER architecture, which can be split into two logical categories: the software agents (typical of the architecture itself) and the tools they exploit. To the former set belong both the Host Manager and the Cluster Manager:

- The Host manager (HM) performs the operations needed to monitor the physical resources and the instantiated VMs; moreover, it runs the VMs on the physical hosts (downloading the VM image) and performs the migration of VMs (more precisely, it performs the low

 ISBN: 978-1-61208-204-2

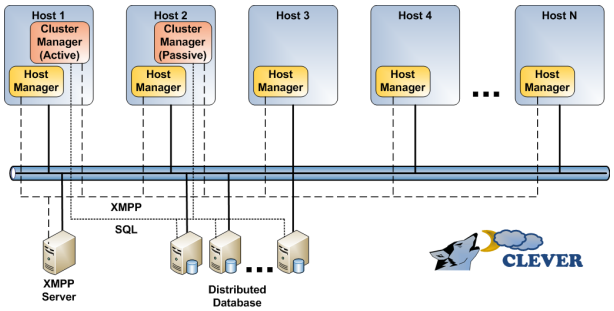


Figure 1. CLEVER architecture.

level aspects of this operation). To carry out these functions it must communicate with the hypervisor, hosts' OS and distributed file-system on which the VM images are stored. This interaction must be performed using a plug-ins paradigm.

- The Cluster Manager (CM) acts as an interface between the clients (software entities, which can exploit the Cloud) and the HM agents. CM receives commands from the clients, performs operations on the HM agents (or on the database) and finally sends information to the clients. It also performs the management of VM images (uploading, discovering, etc.) and the monitoring of the overall state of the cluster (resource usage, VMs state, etc.). At least one CM has to be deployed on each cluster but, in order to ensure higher fault tolerance, many of them should exist. A master CM will exist in active state while the other ones will remain in a monitoring state.

Regarding the tools such middleware components exploit, we can identify the Distributed Database and the XMPP Server.

B. Internal/External Communication

The main CLEVER entities, as already stated, are the Cluster Manager and the Host Manager modules, which include several sub-components, each designed to perform a specific task. In order to ensure as much as possible the middleware modularity, these sub-components are mapped on different processes within the Operating System of the same host, and communicate each other exchanging messages. CLEVER has been designed for supporting two different types of communication: intra-module (internal) communication and inter-module (external) communication.

1) Intra-module (Internal Communication): The intra-module communication involves sub-components of the same module. Since they essentially are separated processes, a specific Inter Process Communication (IPC) has to be employed for allowing their interaction. In order to guarantee the maximum flexibility, the communication has been designed employing two different modules: a low level one implementing the IPC, and an high-level one instead acting as interface with the CLEVER components, which allows access to the services they expose.

For implementing the communication mechanism, each module virtually exchanges messages (horizontally) with the corresponding peer exploiting a specific protocol (as the horizontal arrows indicate in Figure). However, the real message flow is the one indicated by the vertical arrows: when the Component Communication Module (CCM) of the Component A aims to send a message to its peer on a different Component B, it will exploit the services offered by the underlying IPC module. Obviously, in order to correctly communicate, the CCM must be aware of the interface by means of these services are accessible. If all the IPC were designed according to the same interface, the CCM will be able to interact with them regardless both their technology and implementation.

Looking into the above mentioned mechanism, when the Component A needs to access a service made available from the Component B, it performs a request through its CCM. This latter creates a message which describes the request, then formats the message according to the selected communication protocol and sends it to its peer on the Component B by means of the underlying IPC module. This latter in fact, once received the message, forwards it to its peer using a specific container and a specific protocol. The IPC module on the Component B, after that such a container is received, extracts the encapsulated message and forwards it to the overlying CCM. This latter interprets the request and starts the execution of the associated operation instead of the Component A.

2) Inter-module (External Communication): When two different hosts have to interact each other, the inter-module communication has to be exploited. The typical use cases refer to:

- Communication between CM and HM for exchanging information on the cluster state and sending specific commands;
- Communication between the administrators and CM using the ad-hoc client interface.

As previously discussed, in order to implement the inter-module communication mechanism, an XMPP server must exist within the CLEVER domain and all its entities must be connected to the same XMPP room.

When a message has to be transmitted from the CM to an HM, as represented in Figure 2, it is formatted and then sent using the XMPP. Once received, the message is checked from the HM, for verifying if the requested operation can be performed.

As the figure shows, two different situations could lay before: if the request can be handled, it is performed sending eventually an answer to the CM (if a return value is expected), otherwise an error message will be sent specifying an error code. The "Execution Operation" is a sub-activity

 ISBN: 978-1-61208-204-2

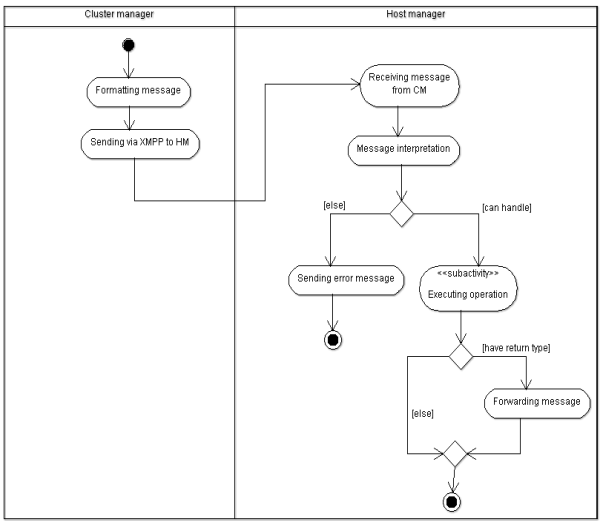


Figure 2. Activity diagram of the external communication.

whose description is pointed out in Figure 3. When the sub-activity is performed, if any return value is expected the procedure terminates, else this value has to be forwarded to the CM in the same way has been done previously with the request.

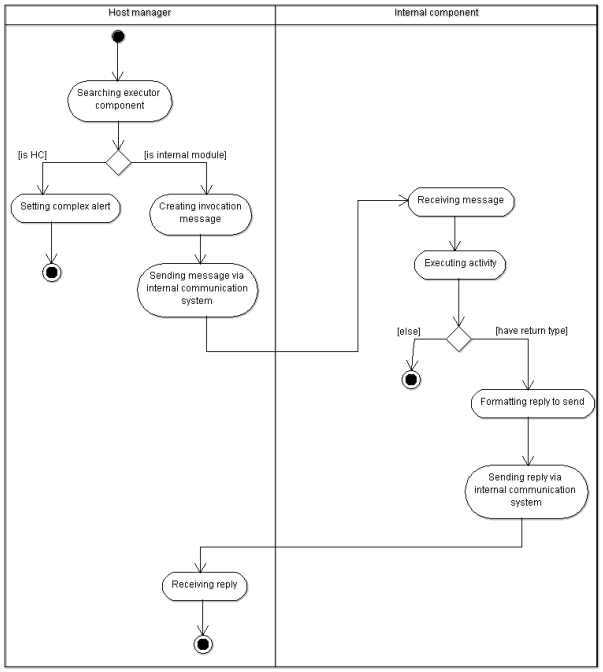


Figure 3. Activity Diagram of the sub-activity Executing Operation.

The sequence of steps involved in the sub-activity is represented in Figure 3. If the operation that has to be executed involves a component different from the Host Coordinator, the already described intra-module communication has to be employed. Once the selected component receives the message using this mechanism, if no problem occurs, the associated activity will be performed, else an error will be generated. If the operation is executed correctly and a return value has to be generated, the component will be responsible of generating the response message which will be forwarded to the HM, and thus, to the CM.

C. Federation Features

CLEVER has been designed with an eye toward federation. In fact, the choice of using XMPP for the CLEVER module communication (i.e., external communication XMPP room) has been made thinking about the possibility to support in the future also interdomain communication between different CLEVER administrative domains. Federation allows Clouds to “lend” and “borrow” computing and storage resources to/from other Clouds. In the case of CLEVER, this means that a CM of an administrative domain is able to control one or more HMs belonging other administrative domains. For example, if a CLEVER domain A runs out of resources of its own HMs, it can establish a federation with a CLEVER domain B, in order to allow the CM of the domain A to use one or more HMs of the domain B. This enables the CM of domain A to allocate VMs both in its own HMs and in the rented HMs of domain B. In this way, on one hand the CLEVER Cloud of domain A can continue to allocate services for its clients (e.g., IT companies, organization, desktop end-users, etcetera), whereas on the other hand the CLEVER Cloud of domain A earns money from the CLEVER Cloud of domain B for the renting of its HMs.

As anyone may run its own XMPP server on its own domain, it is the interconnection among these servers that exploits the interdomain communication. Usually, every user on the XMPP network has an unique Jabber ID (JID). To avoid requiring a central server to maintain a list of IDs, the JID is structured similarly to an e-mail address with an user name and a domain name for the server where that user resides, separated by an at sign (@). For example, considering the CLEVER scenario, a CM could be identified by a JID bach@domainB.net, whereas a HM could be identified by a JID liszt@domainA.net: bach and liszt respectively represent the host names of the CM and the HM, instead domainB.net and domainA.net represent respectively the domains of the Cloud which “borrows” its HMs and of the Cloud which “lends” HMs. Let us suppose that bach@domainB.net wants to communicate with liszt@domainA.net, bach and liszt, each respectively, have accounts on domainB.net and domain A XMPP servers.

The idea of CLEVER federation is straightforward by means of the built-in XMPP features. Figure 4 depicts an example of interdomain communication between two CLEVER administrative domains for the renting of two HMs from a domain A to domain B.

 ISBN: 978-1-61208-204-2

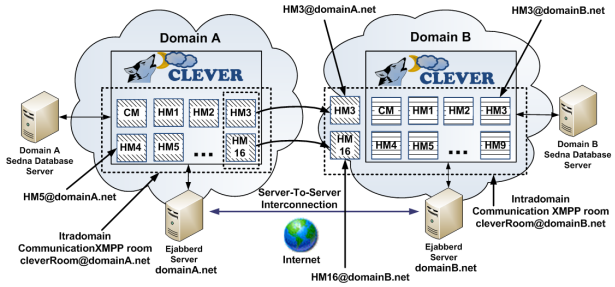


Figure 4. Example of CLEVER in horizontal federation.

Considering the aforementioned domains, i.e., domainA.net and domainB.net, in scenarios without federation, they respectively include different XMPP rooms for intradomain communication (i.e., cleverRoom@domainA.net and cleverRoom@domainB.net) on which a single CM, responsible for the administration of the domain, communicates with several HMs, typically placed within the physical cluster of the CLEVER domain. Considering a federation scenario between the two domains, if the CM the domainB.net domain needs of external resources, after a priori agreements, it can invite within its cleverRoom@domainB.net room one or more HMs of the domainA.net domain. For example, as depicted in Figure 4, the CLEVER Cloud of domainB.net rents from the CLEVER Cloud of domainA.net, HM6 and HM16. Thus, the two rented HMs will be physically placed in domainA.net, but they will be logically included in domainB.net. As previously stated, in order to accomplish such a task a trust relationship between the domainA.net and the domainB.net XMPP servers has to be established in order to enable a Server-to-Server communication allowing to HMs of domain A to join the external communication XMPP room of domain B.

IV. Authentication Issues in CLEVER Federation

Federation between CLEVER Clouds implies the establishment of a secure inter-domain communication between their own XMPP servers. This raises several issues regarding the management of authentication between the XMPP servers of different CLEVER Clouds. In this section, after a discussion of the authentication mechanisms supported by XMPP for the establishment of a server-to-server federation, we describe the authentication issues in a scalable scenario of federated CLEVER Clouds, proposing a solution based on the IdP/SP model.

A. Concerns about XMPP Server-to-Server Federation

Considering that the communication in each CLEVER Cloud is achieved through XMPP or Jabber messages by means of an Ejabberd server, the federation establishment between two or more CLEVER Clouds implies a secure inter-domain communication between their respective Ejabberd servers. In fact, in the XMPP terminology, the term "federation" is commonly used to describe communication between two servers.

The public-subscribe technology is reemerging for enabling real-time communication within Cloud infrastructure, nevertheless its major protocol XMPP is somewhat dated from the point of view of security.

In order to enable federation between servers, it is needed to carry out a strong security to ensure both authentication and confidentiality thanks to encryption. According to the IETF 6120, compliant implementations of servers should support Dialback or SASL EXTERNAL protocol for authentication and the TLS protocol for encryption.

The basic idea behind Server Dialback [17] is that a receiving server does not accept XMPP traffic from a sending server until it has (i) "called back" the authoritative server for the domain asserted by the sending server and (ii) verified that the sending server is truly authorized to generate XMPP traffic for that domain. The basic flow of events in Server Dialback consists of the following four steps:

1) The Originating Server generates a dialback key and sends that value over its XML stream with the Receiving Server. (If the Originating Server does not yet have an XML stream to the Receiving Server, it will first need to perform a DNS lookup on the Target Domain and thus discover the Receiving Server, open a TCP connection to the discovered IP address and port, and establish an XML stream with the Receiving Server.)
2) Instead of immediately accepting XML stanzas on the connection from the Originating Server, the Receiving Server sends the same dialback key over its XML stream with the Authoritative Server for verification. (If the Receiving Server does not yet have an XML stream to the Authoritative Server, it will first need to perform a DNS lookup on the Sender Domain and thus discover the Authoritative Server, open a TCP connection to the discovered IP address and port, and establish an XML stream with the Authoritative Server).
3) The Authoritative Server informs the Receiving Server whether the key is valid or invalid.
4) The Receiving Server informs the Originating Server whether its identity has been verified or not.

SASL is a framework for providing authentication and data security services in connection-oriented protocols via replaceable mechanisms. It provides a structured interface between protocols and mechanisms. The resulting framework allows new protocols to reuse existing mechanisms and allows old protocols to make use of new mechanisms. SASL is used in various application protocols (e.g., XMPP, IMAP, LDAP, SMTP, POP, etc.) and support many mechanisms including:

- **PLAIN**, a simple clear text password mechanism. PLAIN obsoleted the LOGIN mechanism.

 ISBN: 978-1-61208-204-2

- **SKEY**, an S/KEY mechanism.
- **CRAM-MD5**, a simple challenge-response scheme based on HMAC-MD5.
- **DIGEST-MD5**, HTTP Digest compatible challenge-response scheme based upon MD5. DIGEST-MD5 offers a data security layer.
- **GSSAPI**, for Kerberos V5 authentication via the GSS-API. GSSAPI offers a data-security layer.
- **GateKeeper**, a challenge-response mechanism developed by Microsoft for MSN Chat

At the time of writing of the IETF 6120, in March 2011, most server implementations still use the Dialback protocol to provide weak identity verification instead of using SASL to provide strong authentication, especially in cases where SASL negotiation would not result in strong authentication anyway (e.g., because TLS negotiation was not mandated by the peer server, or because the PKIX certificate presented by the peer server during TLS negotiation is self-signed and has not been previously accepted). The solutions is to offer a significantly stronger level of security through SASL and TLS.

B. SASL and SAML for Secure CLEVER Federation

In a scalable scenario of federation each CLEVER Cloud can require to frequently establish/break partnerships with other CLEVER Clouds. This implies that each Cloud should manage a huge number of credentials in order to authenticate itself in other Clouds. In a federated CLEVER environment, this means that the XMPP server of the Cloud requiring federation has to be authenticated by the XMPP server of the Cloud accepting the federation request. If we consider thousand of Clouds, each Cloud should manage one credential for accessing to each federated Cloud. This is problem is commonly known as Single-Sign-One (SSO), i.e., considering an inter-domain environment, performing the authentication once, gaining the access to the resources supplied by different Service Provider, each one belonging to a specific domain. A model addressing the SSO problem is the Identity Provider/Service Provider Model (IdP/SP). Typically, a client who wants to access to the resources provided by a SP, perform the authentication once on the IdP (asserting party), which asserts to the SP (relaying party) the validity of the authentication of the client. Considering many SPs relaying on the IdP if the client wants to access another SP, as this latter will be trusted with the IdP, no further authentication will be required. This model is widely known on the Web with the term "Web Browser SSO", in which the client is commonly an user who perform an authentication fill in an HTML form with his user name and password. Nowadays, the major standard implementing defining the IdP/SP model is the Security Assertion Markup Language (SAML) [8], developed by OASIS.

The scenario of CLEVER federation is quite similar. In this case, the client who wants to perform the authentication is the XMPP server of the CLEVER Cloud requiring federation, instead the role of the SP is played by the XMPP server of the Cloud accepting the federation request. As the XMPP server support authentication through SASL a concern raises: the RFC 4422 does not support any security mechanism implementing the IdP/SP model.

Therefore, in order to achieve such a scenario, we followed the Internet-Draft entitled "A SASL Mechanism for SAML", defined by CISCO TF-Mobility Vienna, describing the applicability and integration between the two protocols for non-HTTP use cases. According to such a draft, the authentication should occur as follows:

1) The server MAY advertise the SAML20 capability.
2) The client initiates a SASL authentication with SAML20
3) The server sends the client one of two responses:
   a) a redirect to an IdP discovery service; or
   b) a redirect to the IdP with a complete authentication request.
4) In either case, the client MUST send an empty response.
5) The SASL client hands the redirect to either a browser or an appropriate handler (either external or internal to the client),and the SAML authentication proceeds externally and opaquely from the SASL process.
6) The SASL Server indicates success or failure, along with an optional list of attributes

In this way, thanks to SASL and SAML, for each CLEVER Cloud it is possible to perform the authentication once gaining the access to all the other Clouds relying on the IdP, thence, lending and/or borrowing HMs according to agreements.

V. SECURE CLEVER INTERDOMAIN COMMUNICATION THROUGH SHIBBOLETH FEDERATION

In the previous section, we have analyzed different technologies able to address authentication issues in distributed environments, where users need to prove their identities. As we introduced earlier, some specific scenarios, such as Cloud Federation, may require that systems belonging to different administrative domains interact each other to cooperate. In this section, we try to extend the mechanisms regarding authentication in distributed environment toward Cloud systems, proposing our idea for implementing Single Sign On among different XMPP servers, in order to grant either scalability and flexibility while the authentication process is accomplished.

In a Cloud Federated scenario, where each Cloud refers to CLEVER as Virtual Infrastructure Manager, and the communication among its entities is thus based on XMPP, the most convenient and easy way to build a Cloud federation should rely on the employment of the federation features made available by the XMPP protocol itself. This latter

 ISBN: 978-1-61208-204-2

assumes a XMPP server can be configured for accepting external connections from other servers for creating server-to-server interactions (server federation).

According to the XMPP specifications, this mechanism is quite easy to implement and the result will be the ability for two XMPP servers in different domains to exchange XML stanzas. There are different levels of federation:

- Permissive Federation, a server accepts a connection from any other peer on the network, even without verifying the identity of the peer based on DNS lookups.
- Verified Federation, a server accepts a connection from a peer only after the identity of the peer has been weakly verified via Server Dialback, based on information obtained via the Domain Name System (DNS) and verification keys exchanged in-band over XMPP.
- Encrypted Federation, a server accepts a connection from a peer only if the peer supports Transport Layer Security (TLS) and the client authenticates itself using a SASL mechanisms.

On one hand, Permissive and Verified Federation are the simplest federation approaches: as discussed in the previous Section, they lack some security aspects since they are not based on any password exchange procedure and, in order to implement domain filtering (in the second case), a list of allowed sites has to be compiled preemptively. On the other hand, the Encrypted Federation level relies on a more secure way to perform the authentication, based on challenge-response authentication protocols relaying on passphrase.

This standard authentication mechanisms are enough when you want to enable the communication among a limited endpoint number but, in a scenario where several XMPP servers might exist, it could be a difficult task to statically pre-configure the binding among all the involved entities and manage credentials for authenticating a given server to each other. Our idea aims to address these issues and propose the integration of a new SASL security mechanism for allowing a more scalable management of the authentication process exploiting the well-known concept of SSO. The integration we are talking about refers to the use of SAML 2.0.

In ordeer to implement the above mentioned scenario, we arranged a distributed Cloud environment composed of two CLEVER sites relying on the Ejabberd XMPP server [9] to allow communication within each domain. Furthermore, in order to verify the server-to-server federation we configured each server to listen for incoming connection on a given port. This task is usually accomplished by an Ejabberd module that manages incoming and outcoming connections from/to external servers. According to the XMPP core specification, this module is able to establish server federation according to the three different levels pointed out above. In our work we considered more specifically the Encrypted Federation case and we have modified the Ejabberd module performing SASL to add in the list of the supported security mechanism also SAML 2.0. This latter has been introduced relying on an external software module based on Shibboleth named Authentication Agent (AA).

The Authentication Agent acts as user when it is contacted from the Source Ejabberd Server for starting the Federation, whereas represents the Relying Party when it is contacted from the Destination Ejabberd Server.

In the following, we present the sequence of steps performed by two servers (for simplicity Source Server and Destination Server) that aim to build the federation. As Figure 5 depicts, the involved actors in the process are the s2s_Manager(s) of both the Ejabberd servers, the two authentication agents acting as User and Relying Party (User, the one interacting with the Source Server; Relying Party the one interacting with the Destination Server) and the Identity Provider (also implemented using Shibboleth).

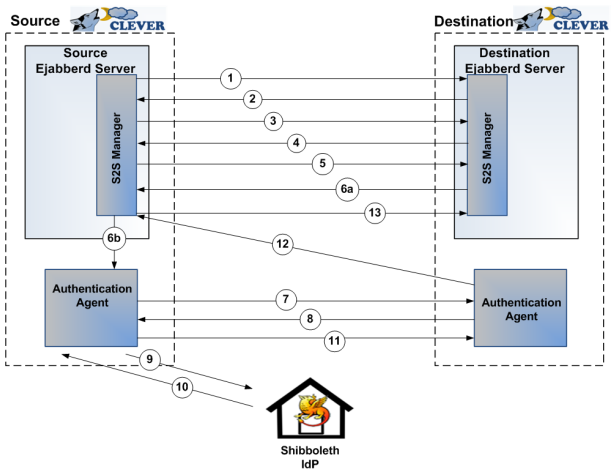


Figure 5. Step performed by two XMPP servers aiming to build Federation: the authentication process is executed using SAML 2.0 as external SASL mechanism

- Step 1: s2s_Manager of Source Server initiates stream to the s2s_Manager of the Destination server.
- Step 2: s2s_Manager of the Destination Server responds with a stream tag sent to the s2s_Manager of the Source Server.
- Step 3: s2s_Manager of the Destination Server informs the s2s_Manager of the Source Server of available authentication mechanisms.
- Step 4: s2s_Manager of the Source Server selects SAML as an authentication mechanism.
- Step 5: s2s_Manager of Destination Server sends a BASE64 encoded challenge to the s2s_Manager of the Source Server in the form of an HTTP Redirect to the Destination AA (acting as Relying Party).
- Step 6: a) s2s_Manager of Source Server sends a BASE64 encoded empty response to the challenge and b) forward to the Source AA the URL of the Relying Party.

 ISBN: 978-1-61208-204-2

- Step 7: The Source AA (User) engages the SAML authentication flow (external to SASL) contacting the Destination AA (Relying Party).
- Step 8: Destination AA redirect Source AA to the IdP.
- Step 9: Source AA contacts IdP and performs Authentication
- Step 10: IdP responds with Authentication Assertion
- Step 11: Source AA contacts Destination AA for gaining access to the resource.
- Step 12: Destination AA contacts the s2s_Manager of the Destination Server informing it about the authentication result.
- Step 13: if the authentication is successful the s2s_Manager of the Source Server initiates a new stream to the s2s_Manager of Destination Server.

The advantage of performing the authentication among servers in such a way mainly consists in the higher security level achieved than the traditional Dialback/SASL mechanisms and in the possibility of exploiting the SSO authentication. Looking at Figure 5, after that the federation has been achieved with the depicted server, if the same Source Cloud aims to perform server-to-server federation with a new XMPP server that relies on the same IdP as trusted third-party, such a process would be straightforward. Since the Source Server already has an established security context with the IdP, once the SASL process starts and the SAML mechanism is selected, no further authentication will be required.

VI. Conclusions and Remarks

In this paper, we discussed how to perform the authentication among CLEVER Clouds in order to establish federation. CLEVER is an IaaS Cloud middleware designed according to the public-subscribe technology and implementing the XMPP protocol. The federation establishment involves the federation among their own XMPP servers. Considering the current implementation of XMPP servers, server-to-server federation implies security issues due to authentication. In particular the SASL framework used in XMPP server does not provide any SSO authentication mechanism, a mandatory requirement for a scalable federated Cloud environment. In order to address this issue, in this work, we used an integration of SASL and SAML implementing a testbed including Ejabberd as XMPP server and Shibboleth as SAML implementation. Experiments have proved that such a solution can be a valid approach for a federation-enabled Cloud infrastructure using a public-subscribe technology, such as CLEVER.

References

[1] B. Rochwerger, D. Breitgand, A. Epstein, D. Hadas, I. Loy, K. Nagin, J. Tordsson, C. Ragusa, M. Villari, S. Clayman, E. Levy, A. Maraschini, P. Massonet, H. Munoz, and G. Toffetti, "Reservoir - when one cloud is not enough," *Computer*, vol. 44, pp. 44–51, 2011.

[2] B. Sotomayor, R. Montero, I. Llorente, and I. Foster, "Virtual Infrastructure Management in Private and Hybrid Clouds," *Internet Computing, IEEE*, vol. 13, pp. 14–22, Sept.-Oct. 2009.

[3] National Institute of Science and Technology. Standards Acceleration to Jumpstart Adoption of Cloud Computing; http://csrc.nist.gov/groups/SNS/cloud-computing/ July 2011.

[4] F. Tusa, M. Paone, M. Villari, and A. Puliafito., "CLEVER: A CLoud-Enabled Virtual EnviRonment," in *15th IEEE Symposium on Computers and CommunicationsS Computing and Communications, 2010. ISCC '10. Riccione*, June 2010.

[5] Extensible Messaging and Presence Protocol (XMPP), http://xmpp.org/, Jan 2012.

[6] RFC 6120, Extensible Messaging and Presence Protocol (XMPP): Core, http://tools.ietf.org/rfc/rfc6120.

[7] RFC 4422, Simple Authentication and Security Layer (SASL), http://www.ietf.org/rfc/rfc4422.

[8] SAML V2.0 Technical Overview, OASIS, http://www.oasis-open.org/specs/index.php#saml, Jan 2012.

[9] Ejabberd, the Erlang Jabber/XMPP daemon: http://www.ejabberd.im/, Jan 2012.

[10] The Shibboleth system standards, Available: http://shibboleth. internet2.edu/, Jan 2012.

[11] P. Sempolinski and D. Thain, "A Comparison and Critique of Eucalyptus, OpenNebula and Nimbus," in *The 2nd IEEE International Conference on Cloud Computing Technology and Science*, July 2010.

[12] C. Hoffa, G. Mehta, T. Freeman, E. Deelman, K. Keahey, B. Berriman, and J. Good, "On the Use of Cloud Computing for Scientific Workflows," in *SWBES 2008, Indianapolis*, December 2008.

[13] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus Open-Source Cloud-Computing System," in *IEEE/ACM CCGRID*, pp. 124–131, May 2009.

[14] Canonical switches to OpenStack for Ubuntu Linux cloud. http://www.zdnet.com/blog/open-source/canonical-switches-to-openstack-for-ubuntu-linux-cloud/8875, Jan 2012.

[15] B. Sotomayor, R. Montero, I. Llorente, and I. Foster, "Resource Leasing and the Art of Suspending Virtual Machines," in *HPCC*, pp. 59–68, June 2009.

[16] OpenStack: Open source software for building private and public clouds. http://www.openstack.org/, Jan 2012.

[17] XEP-0220: Server Dialback, http://xmpp.org/extensions/xep-0220.html.

 ISBN: 978-1-61208-204-2

Maximum likelihood decoding algorithm for some Goppa and BCH Codes: Application to the matrix encoding method for steganography

Thierry P. Berger
XLIM (UMR CNRS 7252), Université de Limoges
Limoges, France
Email: thierry.berger@unilim.fr

Mohamed Bouye Ould Medeni
LMIA, Université Mohammed V- Agdal
Rabat, Morocco
Email: sbaimedeni@yahoo.fr

***Abstract*—The idea of "Matrix encoding" was introduced in steganography by Crandall in 1998. The implementation was then proposed by Westfeld with steganography algorithm F5. Matrix encoding using linear codes (syndrome coding) is a general approach to improving embedding efficiency of steganographic schemes. The covering radius of the code corresponds to the maximal number of embedding changes needed to embed any message. Steganographers, however, are more interested in the average number of embedding changes rather than the worst case. In fact, the concept of embedding efficiency - the average number of bits embedded per embedding change - has been frequently used in steganography to compare and evaluate performance of steganographic schemes. The aim of this paper is to transform some algebraic decoding algorithms up to the error correcting capacity into a maximum likelihood decoder by the use of a limited exhaustive search. This algorithm is directly inspired from those proposed by N. Courtois, M. Finiasz, and N. Sendrier in the context of electronic signature. It remains exponential, however it becomes practicable for for some small BCH and Goppa codes (typically, with an error correcting capacity until 4).**

Keywords - Steganography; Error-correcting Codes; Complete Decoding; Goppa Codes; Embedding Efficient.

I. INTRODUCTION

Research on hiding data into digital multimedia objects, such as images, audios, and videos, has advanced considerably over the past decade. Steganography refers to the science of covert communication, and steganalysis is the opposite of steganography. Nowadays, a large number of steganography tools have been developed based on replacement of the least significant bit (LSB) with secret message because of its extreme simplicity.

An interesting steganographic method is known as matrix encoding, introduced by Crandall [4]. Matrix encoding requires the sender and the recipient to agree in advance on a parity check matrix H, and the secret message is then extracted by the recipient as the syndrome (with respect to H) of the received cover object. This method was made popular by Westfeld [17], who incorporated a specific implementation using Hamming codes in his F5 algorithm. This steganographic scheme can embed m bits of message in 2^m-1 cover symbols by changing at most one of them.

There are three parameters to evaluate the performance of a steganographic method over a cover vector of n symbols. The first one is average distortion $D = \frac{r_a}{n}$, where r_a is the expected number of changes over uniformly distributed messages. The second one is the embedding rate $\epsilon_r = \frac{k}{n}$, which is the amount of bits that can be hidden in a cover vector [2] (k is the number of bits of the hidden message). The third one is the embedding efficiency $\epsilon_{\mathit{eff}} = \frac{k}{r_a}$, which is the average number of hidden bits per changed bit. So, we have the relation $D\epsilon_{\mathit{eff}} = \epsilon_r$. In general, for the same embedding rate a method is better when the average distortion is smaller. As usually, we denote by (n, k, r_a) the parameters of a steganographic protocols. the reader must be careful not to confuse with the parameters $[n, k, d]$ of a code, in particular the number of bits of a steganographic scheme is generally the co-dimension $n - k$ of a code of dimension k.

The matrix encoding technique is a well-studied method to insert a hidden message into a cover message, for example into an image *cf* [6], [14], [15], [18]. It is assumed that a strategy of insertion has been previously defined, therefore in this paper we will not discuss the security of any stegosystem, which is directly dependent on the chosen strategy. The main objective of the matrix encoding is to minimize the number of modified bits during the insertion of a given message. One of the limitations of this method is the fact that a maximum likelihood decoding algorithm is required. Unfortunately, maximum-likelihood decoding of general linear codes is NP-hard [1]. Some family of codes, such as BCH codes or Goppa codes, have a decoding algorithm up to a correction capacity t. The purpose of this paper is to transform these algorithms into maximum likelihood decoding algorithms. This decoding algorithm is a kind of exhaustive search aided by an algebraic decoding algorithm. It is derived from that presented in [3], which is used to provide a short signature based on the McEliece Public key Cryptosystem. We present specific applications to some binary Goppa codes and BCH codes and show that these codes are new candidates for practical implementation of the matrix encoding technique.

This paper is organized as follows. In Section 2, we review the basic application of coding theory in steganography. In

 ISBN: 978-1-61208-204-2

Section 3, we recall the complete decoding technique. Section 4 presents the experimental results on some classical binary Goppa and BCH codes.

II. Error-correcting Codes in Steganography

An important kind of steganographic protocols can be defined from coding theory. Error-correcting codes are commonly used for detecting and correcting errors, or erasures, in data transmission. An explicit description of the relations between error-correcting codes and steganographic systems was presented in [14], [15], [18]. The most commonly used codes in steganography are linear. The existence of a parity check matrix helps on designing good steganographic protocols. Crandall [4] introduced the matrix encoding idea to improve the embedding efficiency for steganography. F5 proposed by Westfeld [17] is the first implementation of the matrix encoding concept to reduce modification of the quantized DCT coefficients. Basically, the matrix encoding technique in F5 modifies at most 1 coefficient among n coefficients to hide k bits. For example, if we use the $[7, 4]$ Hamming code, we obtain a $(7, 3)$ steganographic *i.e.*, one can insert 3 bits into a cover of length 7 by changing one bit of the cover. Modified matrix encoding (MME) [11] uses a $(n, k, 2)$ code where one more coefficient may be changed in each group compared with the matrix encoding. Main concept of the matrix encoding technique is "the less number of modification to the DCT coefficients, the less amount of distortion in the image".

Later, several efficient codes have been proposed to realize the matrix encoding: BCH error-correcting code [19], [16], Reed-Solomon (RS) [5], product perfect codes [15]. Error-correcting codes and steganographic systems were presented by Zhang [14], Munuera, Galand [18], [10]. It is shown in [14] that there is a corresponding relation between the maximum length embeddable (MLE) codes and perfect error correcting codes.

Let n and k be positive integers, $k \leq n$, and let B be a finite set. An embedding/retrieval steganographic protocol of type (n, k) over B is a pair of maps $e : B^k \times B^n \to B^n$ and $r : B^n \to B^k$ such that $r(e(s, v)) = s$ for all $s \in B^k$ and $v \in B^n$. Maps e and r are respectively the embedding and the retrieval map. The number $\rho = max\{d(v, e(s, v)); s \in B^k, v \in B^n\}$, d being the Hamming distance, is the radius of the protocol. The embedding map of a (n, k) embedding/retrieval steganographic protocol [8], [7], [20] with radius ρ allows us to hide k information symbols into a string of n cover symbols, by changing at most ρ symbols of the cover.

A linear code of length n over the finite field $GF(q)$ is a subspace C of the $GF(q)$-linear space $GF(q)^n$. The Hamming distance $d(v, w)$ between two vectors v and w of $GF(q)^n$ is the number of distinct coefficients between v and w. The support of a vector $v = (v_1, v_2, ..., v_n) \in GF(q)^n$ is the set $Supp(v) = \{i | v_i \neq 0\}$. So, $d(v, w)$ is also the number of elements of $Supp(v - w)$. The minimum distance d of a code C is the minimum distance between any pair of codewords (*i.e.* elements of C). The covering radius ρ of the code C is defined as $\rho = max_{v \in GF(q)^n}\{d(v, C)\}$, where $d(v, C)$ means the minimum Hamming distance from vector v to the code C. The parameters $[n, k', d]$ (or $[n, k']$ as d is not known) are respectively the length, the dimension and the minimum distance of the code. In the sequel, for steganographic application, we are interested in the co-dimension $k = n - k'$ of the code, which is the size of the hidden message.

Let $B = GF(q)$. A a parity check matrix H of C is a $(n - k') \times n$ full rank matrix such that $v \in C$ if and only if $H \times v^t = 0$, where v^t means the vector v as a column vector. The syndrome of any $v \in B^n$ is the vector $r(v) = H \times v^t$. A coset $C + v$ is the set of all vectors in B^n with the same syndrome. A vector $l_{r(v)}$ of minimum weight in $C+v$ is called a coset leader. Note that this coset leader is not necessarily unique.

The matrix encoding steganographic protocol is defined as follows. The syndrome map $r : B^n \to B^k$ defined by $r(v) = H \times v^t$ is the retrieval map of the (n, k, r_a) steganographic protocol, which will be called linear to emphasize that the retrieval map r is a linear map. The embedding algorithm $e(s, v)$ requires the classical coset leader decoding algorithm, which return the coset leader of $v + C$. The embedding algorithm is described in Algorithm 1.

Algorithm 1: Coset steganographic algorithm.

Required : a coset decoding algorithm: input a syndrome u, output: a coset leader l_u
Input : a cover v of size n and a message s of size k.
Output : $v' = e(s, v)$, a steganographic cover of s with distortion $d(v, v')$ as small as possible.

1: **Compute** $u := r(v) - s$,
2: **set** $c := v - l_u$,
3: **return** $e(s, v) := c$.

The maximum weight of a coset leader is the covering radius ρ of the code, so the embedding efficiency is upper bounded by ρ: $r_a \leq \rho$, with equality if and only if the code is perfect.

III. Complete Decoding Algorithm

For practical implementation of the matrix embedding technique, the crucial point is the fact that it requires a complete decoding algorithm. In this section, we will present a more efficient decoding algorithm than those used previously, under the restriction that the chosen code must posses a non-complete) algebraic decoding algorithm. A complete decoding algorithm takes in input any word of the space and return a nearest codeword in C. It performs a maximum likelihood decoding. This problem is equivalent to be able to find an error pattern of minimal weight corresponding to any given syndrome. This problem is known to be NP-hard [1], [3]. Clearly, such an algorithm will be able to correct errors of weight greater than the error-correcting capacity t of the code. The weight of correctable errors is upper-bounded by the covering radius ρ. Unfortunately, for steganographic applications,

 ISBN: 978-1-61208-204-2

the determination of the covering radius value of a code is also a hard problem. More precisely, the determination of the covering radius of a linear code was proved Π2-hard by McLoughlin [12]. In practice, the determination of the covering radius needs the enumeration of the coset leaders (minimum weight words) of any coset of the code. Roughly speaking, it requires $\binom{n}{\rho}$ operations.

A complete decoding algorithm can be performed by an exhaustive search on codewords. It can also be performed by an exhaustive search on errors of increasing weight.

In the sequel, following the idea developed in [3] in the context of digital signature, we propose to extend any classical algebraic decoding algorithm up to the error correcting capacity t into a complete decoding algorithm. If the error is of weight $w = t + i$, this algorithm performs an exhaustive search on the first i bits, the remaining t bits are corrected by the algebraic decoder.

The principle is as follows: First, we try to decode the received word x with the algebraic algorithm. If this attempt succeeds, we return the corrected codeword. If not, we enumerate all the possible errors following their increasing weight, we add this error to the received word and try to decode it again. If the distance between x and the code C is w, this algorithm succeeds with an additional error e of weight $w - t$, so the algorithm is upper-bounded by a maximal weight of additional error $\rho - t$. Clearly, this modified decoding algorithm remains exponential in the weight of the errors, however, in practice, it is efficient to decode more than t errors (typically, until $t + 4$ for practical applications).

Algorithm 2: Complete decoding [3].

Required : a decoding algorithm dec of error capacity t. For an entry v it returns a boolean value $\mathrm{dec}\,1(v)$ and a vector $\mathrm{dec}\,2(v)$: "true" and $c \in C$ with $d(c, v) \leq t$ if it succeed, "false" and v if not.
Input : a cover v of size n and a message s of size k.
Output : $v' = e(s, v)$, a steganographic cover of s with distortion $d(v, v')$ as small as possible.

if $\mathrm{dec}_1(v)$ = true **then**
  return $\mathrm{dec}_2(v)$
end if
$i := 1$
$x := v$
while $\mathrm{dec}_1(x)$ = false **do**
  Enumerate all the errors vectors e of weight $w(e) = i$
  $x := v + e$
  if $\mathrm{dec}_1(x)$ = true **then**
    return $\mathrm{dec}_2(x)$
  end if
  $i := i + 1$
end while

It is possible to derive a non-complete polynomial decoding algorithm up to a fixed error-correction capacity $c < \rho$ by limiting the exhaustive search on the i-th first errors to whose of weight less than or equal to $\delta = c - t$.

Combining Algorithm 2 with Algorithm 1, we can derive an efficient steganographic protocol as described in Algorithm 3.

Algorithm 3: Steganographic scheme.

Required : a decoding algorithm dec of error capacity t. For an entry v it returns a boolean value $\mathrm{dec}\,1(v)$ and a vector $\mathrm{dec}\,2(v)$: "true" and $c \in C$ with $d(c, v) \leq t$ if it succeed, "false" and v if not.
Input : a cover v of size n and a message s of size k.
Output : $v' = e(s, v)$, a steganographic cover of s with distortion $d(v, v')$ as small as possible.

1: **Compute** $u := r(v) - s$,
2: **Compute** x such that $r(x) = u$
3: **Decode** x with Algorithm 2. Set $c \in C$ the output of the decoding algorithm.
4: **Set** $e = x - c$ the error vector
5: **return** $e(s, v) = v + e$

IV. Application to binary BCH codes and Goppa Codes

As a concrete example of application of our method, we tested it on binary BCH codes and binary Goppa codes, with a prescribed minimum distance of 7 or 9, *i.e.*, with a decoding algorithm of error correcting capability 3 or 4. The decoding algorithm is completed with an exhaustive search until 4 additional errors. We choose these two classes of codes because they have an algebraic decoding algorithm up to the error correcting capacity, and parameters suitable for practical applications.

From a theoretical point of view on the parameters of the corresponding stegosystem, we are able to determine the true covering radius only for codes with small length and small covering radius. The following tables present the results obtained from BCH codes and Goppa codes with constructed error-correcting capability $t = 3$ and $t = 4$. We compare these values with whose obtained from known constructions.

Table I compares the theoretical parameters of steganographic protocols based on Hamming codes (F5 [17]), 2 errors correcting BCH codes [19], [16], and 3 or 4 errors correcting BCH and Goppa codes. The third value is not the embedding efficiency in average as usual, but the upper-bound given by covering radius. This value was computed using Magma Computer Algebra system [13]. For large codes, we were not able to achieve this computation. An estimation of the true embedding efficiency will be given in the next tables. It is not easy to directly compare results with distinct values of n and k. The comparison will be clearer in Figure 1. The main interest of our method is to reach new parameter values for steganographic protocols.

Tables II and III present the experimental results of simulations on BCH and Goppa codes of minimum distance 7 and

 ISBN: 978-1-61208-204-2

BCH $t = 2$ [16], [19]	Hamming $t = 1$ [17]
$(15, 8, 3)$	$(15, 4, 1)$
$(31, 10, 3)$	$(31, 5, 1)$
$(63, 12, 3)$	$(63, 6, 1)$
$(127, 14, 3)$	$(127, 7, 1)$
$(255, 16, 3)$	$(255, 8, 1)$
$(511, 18, 3)$	$(511, 9, 1)$
$(1023, 20, 3)$	$(1023, 10, 1)$

BCH $t = 3$	Goppa $t = 3$	BCH $t = 4$	Goppa $t = 4$
$(15, 10, 5)$	$(15, 10, 6)$	$(15, 14, 7)$	
$(31, 15, 6)$	$(31, 15, 6)$	$(31, 20, 7)$	$(30, 19, 8)$
$(63, 18, 5)$	$(63, 18, 6)$	$(63, 24, 7)$	$(63, 24, 8)$
$(127, 21, 5)$	$(127, 21, 6)$	$(127, 28, ?)$	$(127, 28, ?)$
$(255, 24, ?)$	$(255, 24, ?)$	$(255, 32, ?)$	$(255, 32, ?)$
$(511, 27, ?)$	$(511, 27, ?)$	$(511, 36, ?)$	$(511, 36, ?)$
$(1023, 30, ?)$	$(1023, 30, ?)$	$(1023, 40, ?)$	$(1023, 40, ?)$

TABLE I: Parameters (n, k, ρ), n: length of the cover, k: length of the hidden message,ρ: covering radius. t: error-correcting capacity.
First table: known results on 2-ECC BCH codes and Hamming codes.
Second table: our results on 3-ECC and 4-ECC on binary Goppa codes and BCH codes.

code	n	k	r_a	$r_{\max}$	it_a	$it_{\max}$	ϵ_{eff}	ϵ_r
BCH	15	10	$3,3$	5	$2,15$	19	3	$0,67$
Goppa	15	12	$4,52$	6	$43,6$	527	$2,7$	$0,8$
BCH	31	15	$4,28$	5	$30,5$	227	$3,5$	$0,48$
Goppa	31	15	$4,08$	6	$16,9$	502	$3,7$	$0,48$
BCH	63	18	$4,06$	5	27	648	$4,4$	$0,28$
Goppa	63	18	$3,87$	6	$10,7$	2041		$0,28$
BCH	127	21	$3,85$	5	9	276	$5,5$	$0,16$
Goppa	127	21	$3,85$	5	$7,5$	169	$5,5$	$0,16$
BCH	255	24	$3,83$	5	8	524	$6,3$	$0,095$
Goppa	255	24	$3,83$	5	$6,9$	307	$6,3$	$0,095$
BCH	511	27	$3,83$	5	$7,5$	1027	$7,05$	$0,05$
Goppa	511	27	$3,83$	5	$6,7$	540	$7,05$	$0,05$
BCH	1023	30	$3,83$	5	$7,5$	1074	$7,8$	$0,03$
Goppa	1023	30	$3,83$	5	$6,4$	1044	$7,8$	$0,03$

TABLE II: BCH and Goppa, $\delta = 7$, $t = 3$.

code	n	k	r_a	$r_{\max}$	it_a	$it_{\max}$	ϵ_{eff}	ϵ_r
BCH	15	14	$5,93$	7	96	542	$5,9$	$0,93$
BCH	31	20	$6,06$	7	340	4643	$6,06$	$0,645$
Goppa	30	19	$5,79$	7	250	2192	$5,79$	$0,63$
BCH	63	24	$5,59$	7	159	4998	$5,6$	$0,38$
Goppa	63	24	$5,58$	7	145	4362	$5,6$	$0,38$
BCH	127	28	$5,28$	7	81	8134	$5,3$	$0,22$
Goppa	127	28	$5,3$	7	$89,3$	8534	$5,3$	$0,22$
BCH	255	32	$5,06$	6	56	1281	$6,3$	$0,12$
Goppa	255	32	$5,06$	6	$57,5$	307	$6,3$	$0,12$
BCH	511	36	$4,97$	6	$35,5$	1281	$7,2$	$0,07$
Goppa	511	36	$4,97$	6	$35,5$	540	$7,2$	$0,07$
BCH	1023	40	$4,95$	6	$27,5$	1157	$8,1$	$0,039$
Goppa	1023	40	$4,95$	6	$27,5$	1044	$8,1$	$0,039$

TABLE III: BCH and Goppa, $\delta = 9$, $t = 4$.

9 respectively. These results were obtained by testing 100000 inputs (random covers and random messages) for each code.

The different values given in these tables are:
• n: the length of the code (*i.e.*, of the length of the steganographic cover),
• k: the co-dimension of the code, (*i.e.*, the length of the steganographic message),
• r_a: the average of the number of modified symbols,
• $r_{\max}$: the maximum number of modified symbols,
• it_a: the average of the number of iterations of the decoding algorithm,
• $it_{\max}$: the maximum number of iterations of the decoding algorithm,
• ϵ_{eff}: the embedding efficiency (*i.e.*, the number of embedded bits per unit bit of distortion)
• ϵ_r: the average of embedding rate.

Goppa codes are known to be asymptotically good (in term of ratio between the minimum distance and the dimension of the codes), contrary to t BCH codes. However, for our range use, it turns out that there is no significative difference between the parameters of these two families of codes. So, it is not surprising that the experimental results are similar for these two classes of codes.

The specificity of these families of codes come only from the existence of an algebraic decoding algorithm.

An iteration of our algorithm consists essentially to decode a BCH code or a Goppa code of small error correcting capacity (until $t = 4$). These decoders are implemented in many hardware and software applications. We use the function "Decode" of the Magma Computer Algebra system, which is a not optimized implementation, but a generic implementation of a decoder for GRS / Alternant codes. Depending on the parameters of the code, the encoding map needs between 1.5 and 20 seconds. An optimized C implementation will take less than one second in any case. The retrieval map is just the computation of a syndrome, as usually for the matrix encoding.

The graph in Figure 1 represents the embedding efficiency given as a function of embedding rate. We compare our results to those obtained from previous works based on: Hamming codes (F5) [17], BCH 2-errors correcting codes [19], [16] and Golay codes [11]. These results show that 3-correcting BCH codes improves the results of existing implementations. The 4-correcting BCH give poorer results, probably because the number of changes to make is too great.

In this paper, we deliberately limited our study to the binary case. So, we limit our comparisons to other binary codes with a computationally effective implementation. Fridrich et al. [8] explain how the use of non-binary codes will increase the embedding efficiency, in particular for large payload (*i.e.*, embedding rate). A natural extension of our work will be to test ternary BCH and Goppa codes in order to compare with the results presented in [9]. However, in the ternary case, the enumeration of supplementary errors is more complex.

V. CONCLUSION

In this paper, we have presented a new method for steganography. This method is based on a complete decoding algorithm,

 ISBN: 978-1-61208-204-2

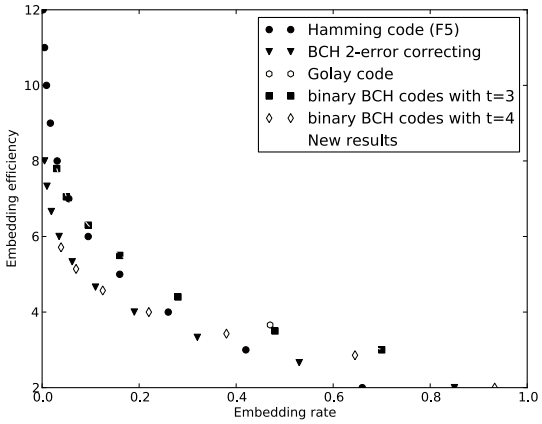


Fig. 1: Performance comparison.

which uses an exhaustive search aided by an algebraic decoding algorithm. This method is practicable for codes with small minimum distance (typically, d less than 10).

Our examples, based on Goppa codes and BCH codes, show that we are able to improve some previous results and to propose new sets of parameters for matrix encoding based on binary codes, especially for high embedding rates.

REFERENCES

[1] E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems", *IEEE Transactions on Information Theory*, vol. 24 (3), pp. 384-386, 1978.

[2] J. Bierbrauer and J. Fridrich, "Constructing good covering codes for applications in steganography", in Transactions on Data Hiding and Multimedia Security III, LNCS vol. 4920 , pp. 1-22, Springer, 2008.

[3] N. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a McEliece based digital signature scheme", Asiacrypt 2001, LNCS vol. 2248, pp. 157-174. Springer, 2011.

[4] R. Crandall, "Some notes on steganography", available at http://os.inf.tu-dresden.de/ west- feld/crandall.pdf, 1998.

[5] C. Fontaine and F. Galand, "How Reed-Solomon Codes Can Improve Steganographic Schemes", EURASIP Journal on Information Security Vol. 2009, Article ID 274845, special issue "Secure Steganography in Multimedia Content" 2009.

[6] J. Fridrich, "Steganography in Digital Media: Principles, Algorithms, and Applications", Cambridge University Press, 2009.

[7] J. Fridrich and P. Lisonek, "Grid colorings in steganography", IEEE Transactions on Information Theory, vol. 53, (4), pp. 1547-1549, 2007.

[8] J. Fridrich, P. Lisonek, D. Soukal, "On steganographic embedding efficiency", Information Hiding 2006, LNCS vol. 4437, pp. 282-296, Springer, 2007.

[9] J. Fridrich and D. Soukal, "Matrix embedding for large payloads", IEEE Transactions on Information Forensics and Security, vol. 1 (3), pp. 390-395, 2006.

[10] F. Galand and G. Kabatiansky, "Information hiding by coverings", in Proceedings of IEEE Information Theory Workshop (ITW '03), pp. 151-154, Paris, France, 2003.

[11] Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique for minimal distortion steganography", Information Hiding 2006, LNCS vol. 4437, pp. 314-327, Springer 2007.

[12] A. McLoughlin, "The complexity of computing the covering radius of a code", IEEE Transactions on Information Theory, vol. 30 (6), pp. 800-804, 1984.

[13] Magma Computer Algebra. http://magma.maths.usyd.edu.au/magma/

[14] C. Munuera, "Steganography and error-correcting codes", Signal Process. 87 (2007) pp. 1528-1533, available online at http://www.sciencedirect.com.

[15] H. Rifà-Pous and J. Rifà, "Product perfect codes and steganography", Digtal Signal Processing, vol. 19 (4), pp. 764-769, July, 2009.

[16] D. Schönfeld and A. Winkler, "Embedding with syndrome coding based on BCH codes", In: Proceedings of the 8th ACM Workshop on Multimedia and Security, pp. 214-223, 2006.

[17] A. Westfeld, "High capacity despite better steganalysis (F5 steganographic algorithm)", Information Hiding 2001, LNCS vol. 2137, pp. 289-302, Springer, 2001.

[18] W. Zhang and S. Li, "A coding problem in steganography", Designs, Codes and Cryptography, vol. 46 (1), pp. 67-81, 2008.

[19] R. Zhang, V. Sanchev and H. J. Kim, "Fast BCH Syndrome Coding for Steganography", Information Hiding 2009, LNCS vol. 5806, pp. 48- 58, 2009.

[20] X. Zhang and S.Wang, "Stego-encoding with error correction capability", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E88-A, (12), pp. 3663-3667, 2005.

 ISBN: 978-1-61208-204-2

State-of-the-art in Chaotic Iterations-based Pseudorandom Numbers Generators Application in Information Hiding

Jacques M. Bahi, Xiaole Fang, and Christophe Guyeux
FEMTO-ST Institute, UMR 6174 CNRS
University of Franche-Comté, Besançon, France
Email:{jacques.bahi, xiaole.fang, christophe.guyeux}@univ-fcomte.fr

***Abstract*—The confidentiality of information transmitted through the Internet requires an intensive use of pseudorandom number generators having strong security properties. For instance, these generators are used to produce encryption keys, to encrypt data with a one-time pad process, or to dissimulate information into cover media. In our previous work, we have proposed the use of discrete chaotic iterations to build pseudorandom number generators that receive two inputted possibly deficient generators, and mix them to produce pseudorandom numbers with high statistical qualities. In this article, we summarize these contributions and we propose simple applications of these generators for encryption and information hiding. For each application, first experimental evaluations are given, showing that an attacker using these statistics as detection tools cannot infer the presence of an hidden message into given cover documents.**

***Keywords*-Internet Security; Pseudorandom Number Generators; Information Hiding; Discrete Chaotic Iterations.**

I. Introduction

Since pseudorandom sequences are easy to be generated and processed, and due to their need in almost all cryptographic protocols and information hiding schemes, PRNGs (Pseudo Random Number Generators) are widely used for a secure Internet use. Among other things, they are part of the keys generation of any asymmetric cryptosystem, they produce keystreams in symmetric cryptosystems, they determine which bits will receive the secret message in information hiding, and so on. However, a lot of existing pseudorandom number generators (PRNGs) used in numerical simulations are eliminated for such applications, due to the requirements of speed, statistical quality, and security in that context.

Recent years, some researchers have investigated with success the use of chaotic dynamical systems to generate pseudorandom sequences [1], [2]. Indeed, chaotic systems have many advantages as unpredictability or disorder-like, which are needed when producing complex sequences. They are extremely sensitive to the initial states too: a minute difference can cause a significant change in output. All these features fit well the requirements of PRNGs, thus explaining the proposal of such dynamics to secure exchanges. However, chaotic systems using real numbers on infinite bit representation, realized in finite computing precision, lead to short cycle length, non-ideal distribution, and other deflation of this kind. This is why chaotic systems on a infinite space of integers have been dig for these years, leading to the proposition to use chaotic iterations (CIs) techniques to reach the desired goals [3].

Having these goals in mind, we have investigated the proposition to mix secure and fast PRNGs, to take benefits from their respective qualities [4], [5]. In [5], CIs have been proven to be a suitable tool for fast computing iterative algorithms on integers satisfying the topological chaotic property, as it has been defined by Devaney [6]. The way that mix two given generators by using these chaotic iterations has been firstly presented in Internet 2009 [3]. It was called "Old CIPRNG". Then, further investigations have been proposed in [7], [5], [8]. These generators were chaotic and able to pass the most stringent batteries of tests, even if the inputted PRNGs were defective. This claim has been verified experimentally, by evaluating the scores of the logistic map, XORshift, and ISAAC generators through these batteries, when considering them alone or after chaotic iterations. Then, in [9], a new version of this family has been expressed. This so-called "New CIPRNG" family uses a decimation of strategies leading to the improvement of both speed and statistical qualities. Finally, most recently, efficient implementations on GPU (Graphics Processing Unit) using a last family named XOR CIPRNG, have been designed in [10], showing that a very large quantity of pseudorandom numbers can be generated per second (about 20 Gsamples/s).

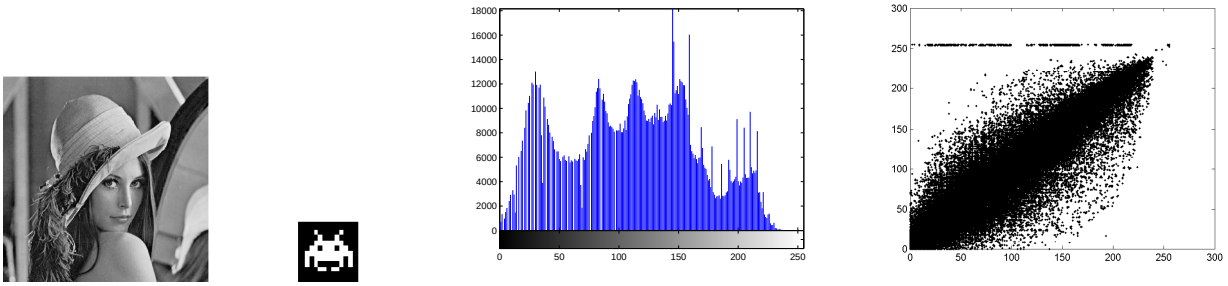
The objective of this article is to make a state-of-the-art of chaotic iterations-based PRNGs, and to propose a possible use of them in the field of secrecy preservation through the Internet, by using information hiding techniques. Random binary sequences will be generated by the three methods mentioned above and a XORshift generator. The application of these pseudorandom bits for information hiding will be carried out systematically, and results will be discussed in order to verify that an attacker, who has only access to some elementary statistical tests, cannot determine whether hidden information are embedded into cover documents or not.

The remainder of this paper is organized in the following way. In Section II, some basic definitions concerning chaotic iterations and XORshift are recalled. Their use to produce three new families of generators is recalled in the next section. Section IV contains the proposed applications of the PRNGs for information hiding. This summary of our previous works in the field of PRNGs and their applications ends by a conclusion section, where our contribution is summarized and intended future work is presented.

II. Basic Remainders

In this section, notations used in this document are introduced, chaotic iterations embedded in the proposed pseudorandom number generators (PRNGs) are defined, and the well-known XORshift generator is recalled.

 ISBN: 978-1-61208-204-2



(a) (b) (c) (d)

Figure 1: (a) The original image. (b) The hidden image. (c) Correlation distribution of the original image. (d) Histogram of the original image.

A. Notations

S^n $\rightarrow$ the n^{th} term of a sequence $S = (S^1, S^2, \ldots)$
v_i $\rightarrow$ the i^{th} component of a vector $v = (v_1, \ldots, v_n)$
f^k $\rightarrow$ k^{th} composition of a function f
$[\![a; b]\!]$ $\rightarrow$ the interval $\{a, a+1, \ldots b\}$ of integers
$X^{\mathbb{N}}$ $\rightarrow$ the set of sequences belonging into X
strategy $\rightarrow$ a sequence of $[\![1; \mathsf{N}]\!]^{\mathbb{N}}$
$\mathbb{S}$ $\rightarrow$ the set of all strategies
$\mathbf{C}_n^k$ $\rightarrow$ the binomial coefficient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
$\oplus$ $\rightarrow$ bitwise exclusive or
$\ll$ and $\gg$ $\rightarrow$ the usual shift operators

B. Chaotic iterations

Definition 1 The set $\mathbb{B}$ denoting $\{0, 1\}$, let $f : \mathbb{B}^{\mathsf{N}} \longrightarrow \mathbb{B}^{\mathsf{N}}$ be an "iteration" function and $S \in \mathbb{S}$ be a chaotic strategy. Then, the so-called *chaotic iterations* are defined by $x^0 \in \mathbb{B}^{\mathsf{N}}$, and

$$\forall n \in \mathbb{N}^*, \forall i \in [\![1; \mathsf{N}]\!], x_i^n = \begin{cases} x_i^{n-1} & \text{if } S^n \neq i \\ f(x^{n-1})_{S^n} & \text{if } S^n = i. \end{cases}$$

In other words, at the n^{th} iteration, only the S^n-th cell is "iterated".

C. XORshift

XORshift is a category of very fast PRNGs designed by George Marsaglia [11]. It repeatedly uses the transform of exclusive or (XOR) on a number with a bit shifted version of it. The state of a XORshift generator is a vector of bits. At each step, the next state is obtained by applying a given number of XORshift operations to w-bit blocks in the current state, where $w = 32$ or 64. A XORshift operation is defined as follows. Replace the w-bit block by a bitwise XOR of the original block, with a shifted copy of itself by a positions either to the right or to the left, where $0 < a < w$. This Algorithm 1 has a period of $2^{32} - 1 = 4.29 \times 10^9$.

Input: the internal state z (a 32-bit word)
Output: y (a 32-bit word)

1: $z \leftarrow z \oplus (z \ll 13)$;
2: $z \leftarrow z \oplus (z \gg 17)$;
3: $z \leftarrow z \oplus (z \ll 5)$;
4: $y \leftarrow z$;
5: return y;

Algorithm 1: An arbitrary round of XORshift algorithm

III. Chaotic Iterations applied to PRNGs

In this section, we describe the CIPRNG implementation techniques that can improve the statistical properties of a large variety of defective generators. They all are based on chaotic iterations (CIs), which have been defined in the previous section.

A. The Old CIPRNG

Let $\mathsf{N} = 4$. Some chaotic iterations are fulfilled to generate a sequence $(x^n)_{n\in\mathbb{N}} \in \left(\mathbb{B}^4\right)^{\mathbb{N}}$ of Boolean vectors: the successive states of the iterated system. Some of these vectors are randomly extracted and their components constitute our pseudorandom bit flow [3]. Chaotic iterations are realized as follows. Initial state $x^0 \in \mathbb{B}^4$ is a Boolean vector taken as a seed and chaotic strategy $(S^n)_{n\in\mathbb{N}} \in [\![1, 4]\!]^{\mathbb{N}}$ is constructed with $PRNG_2$. Lastly, iterate function f is the vectorial Boolean negation. At each iteration, only the S^n-th component of state x^n is updated. Finally, some x^n are selected by a sequence m^n, provided by a second generator $PRNG_1$, as the pseudorandom bit sequence of our generator.

The basic design procedure of the Old CI generator is summed up in Algorithm 2. The internal state is x, the output array is r. a and b are those computed by $PRNG_1$ and $PRNG_2$.

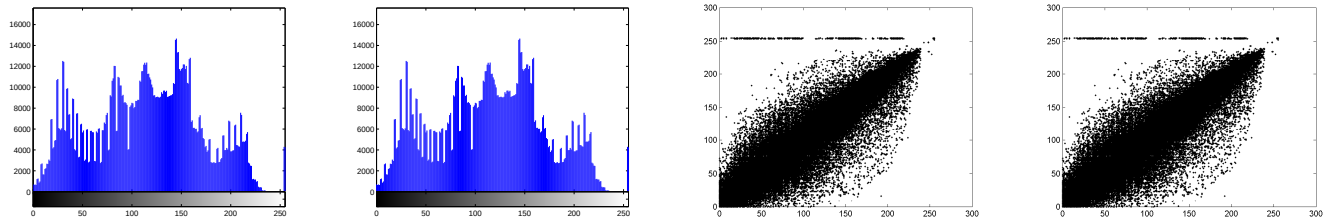
Input: the internal state x (an array of 4-bit words)
Output: an array r of 4-bit words

1: $a \leftarrow PRNG_1()$;
2: $m \leftarrow a \ mod \ 2 + 13$;
3: **while** $i = 0, \ldots, m$ **do**
4: $\quad b \leftarrow PRNG_2()$;
5: $\quad S \leftarrow b \ mod \ 4$;
6: $\quad x_S \leftarrow \overline{x_S}$;
7: **end while**
8: $r \leftarrow x$;
9: return r;

Algorithm 2: An arbitrary round of the Old CI generator

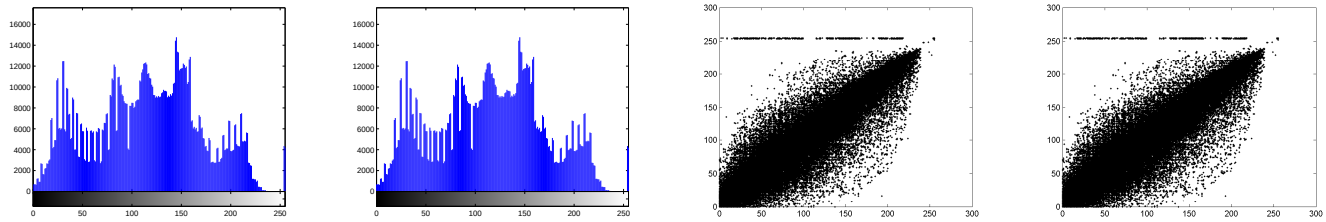
In the paper [3] presented at Internet 2009, the chaotic behavior of CIs is exploited in order to obtain an unpredictable PRNG constituted by two logistic maps. This novel generator has successfully passed the NIST [12]. Then, in [7], we have achieved to improve the speed of the former PRNG, by using two XORshifts in place of the logistic map. In addition,

 ISBN: 978-1-61208-204-2



(a) (b) (c) (d)

Figure 2: (a) Histogram of pixel values when LSBs are replaced by Old CI. (b) Histogram of pixel values when LBSs are an hidden message xored with Old CI. (c) Correlation distribution of two adjacent pixels in Fig.(a). (d) Correlation distribution of two adjacent pixels in Fig.(b).



(a) (b) (c) (d)

Figure 3: (a) Histogram of pixel values when LSBs are replaced by New CI. (b) Histogram of pixel values when LBSs are an hidden message xored with New CI. (c) Correlation distribution of two adjacent pixels in Fig.(a). (d) Correlation distribution of two adjacent pixels in Fig.(b).

this new version of our PRNG is able to pass the famous DieHARD statistical battery of tests [13]. Its security has been improved compared to XORshift alone, and to our former PRNG. However, this latter cannot pass the TestU01 [14] battery, widely considered as the most comprehensive and stringent battery of tests. This goal is achieved by using XORshift and ISAAC as $PRNG_1$ and $PRNG_2$ in [8].

B. New CIPRNG

The New CI generator is designed by the following process [9]. First of all, some chaotic iterations have to be done to generate a sequence $(x^n)_{n\in\mathbb{N}} \in \left(\mathbb{B}^{32}\right)^{\mathbb{N}}$ of Boolean vectors, which are the successive states of the iterated system. Some of these vectors will be randomly extracted and our pseudorandom bit flow will be constituted by their components. Such chaotic iterations are realized as follows. Initial state $x^0 \in \mathbb{B}^{32}$ is a Boolean vector taken as a seed and chaotic strategy $(S^n)_{n\in\mathbb{N}} \in [\![1, 32]\!]^{\mathbb{N}}$ is an *irregular decimation* of $PRNG_2$ sequence, as described in Algorithm 3.

Another time, at each iteration, only the S^n-th component of state x^n is updated, as follows: $x_i^n = x_i^{n-1}$ if $i \neq S^n$, else $x_i^n = \overline{x_i^{n-1}}$. Finally, some x^n are selected by a sequence m^n as the pseudorandom bit sequence of our generator. $(m^n)_{n\in\mathbb{N}} \in \mathcal{M}^{\mathbb{N}}$ is computed from $PRNG_1$, where $\mathcal{M} \subset \mathbb{N}^*$ is a finite nonempty set of integers.

The basic design procedure of the New CI generator is summarized in Algorithm 3. The internal state is x, the output state is r. a and b are those computed by the two input PRNGs. Lastly, the value $g_1(a)$ is an integer defined as in Eq. 1.

$$m^n = g_1(y^n) = \begin{cases} 0 \text{ if } 0 \leqslant y^n < C_{32}^0, \\ 1 \text{ if } C_{32}^0 \leqslant y^n < \sum_{i=0}^{1} C_{32}^i, \\ 2 \text{ if } \sum_{i=0}^{1} C_{32}^i \leqslant y^n < \sum_{i=0}^{2} C_{32}^i, \\ \vdots \qquad \vdots \\ N \text{ if } \sum_{i=0}^{N-1} C_{32}^i \leqslant y^n < 1. \end{cases} \tag{1}$$

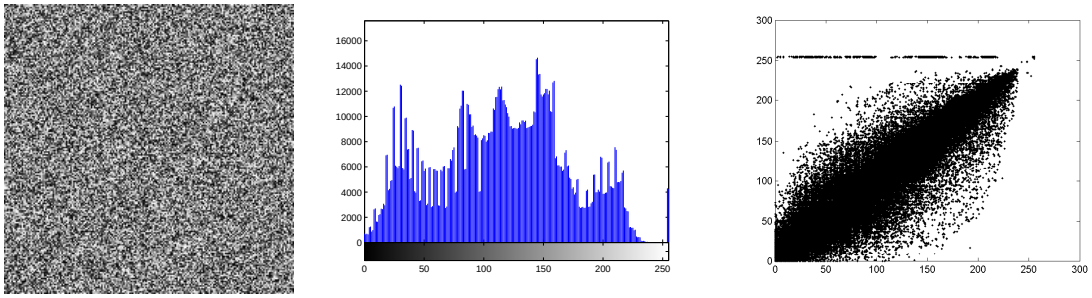
Input: the internal state x (32 bits)
Output: a state r of 32 bits

1: **for** $i = 0, \ldots, N$ **do**
2: $d_i \leftarrow 0$;
3: **end for**
4: $a \leftarrow PRNG_1()$;
5: $m \leftarrow f(a)$;
6: $k \leftarrow m$;
7: **while** $i = 0, \ldots, k$ **do**
8: $b \leftarrow PRNG_2()\ mod\ \mathsf{N}$;
9: $S \leftarrow b$;
10: **if** $d_S = 0$ **then**
11: $x_S \leftarrow \overline{x_S}$;
12: $d_S \leftarrow 1$;
13: **else if** $d_S = 1$ **then**
14: $k \leftarrow k + 1$;
15: **end if**
16: **end while**$r \leftarrow x$;
return r;

Algorithm 3: An arbitrary round of the New CI generator

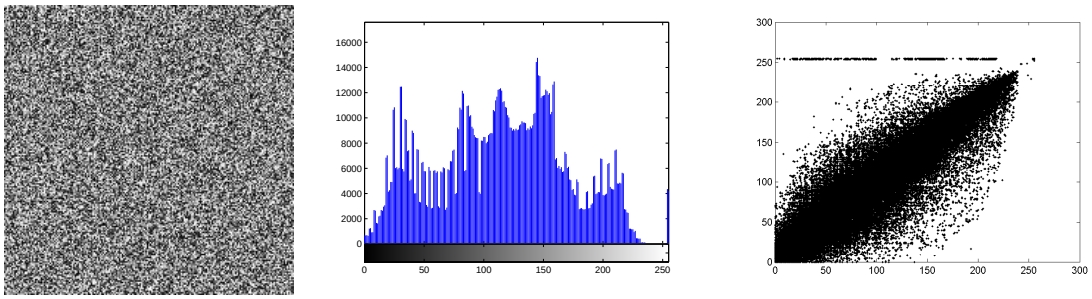
This New CI method presented at Internet 2010 has been

 ISBN: 978-1-61208-204-2



(a) (b) (c)

Figure 4: (a) The encrypted Lena (one-time pad using Old CI). (b) Histogram of Fig.(a). (c) Correlation distribution of two adjacent pixels in Fig.(a)



(a) (b) (c)

Figure 5: (a) The encrypted Lena (one-time pad using New CI). (b) Histogram of Fig.(a). (c) Correlation distribution of two adjacent pixels in Fig.(a)

published in [9]. It was initially using two XORshifts, showing better speed and statistical performance while preserving chaotic properties of the Old CIPRNG. For more information, the reader is referred to [9].

C. XOR CIPRNG

Instead of updating only one cell at each iteration as Old CI and New CI, we can try to choose a subset of components and to update them together. Such an attempt leads to a kind of merger of the two random sequences. When the updating function is the vectorial negation, this algorithm can be simply rewritten as follows [10]:

$$\begin{cases} x^0 \in [\![0, 2^{\mathsf{N}} - 1]\!], S \in [\![0, 2^{\mathsf{N}} - 1]\!]^{\mathbb{N}} \\ \forall n \in \mathbb{N}^*, x^n = x^{n-1} \oplus S^n, \end{cases} \quad (2)$$

The single basic component presented in Eq. 2 is of ordinary use as a good elementary brick in various PRNGs. It corresponds to the discrete dynamical system in chaotic iterations.

IV. Application Evaluation

In this section, the application of PRNGs using CI methods for information hiding is given.

A. The Proposed Information Hiding Method

Suppose that the size of the image is $M \times N$. The steps of the proposed information hiding algorithm using the CIPRNG family are summed up below.

1) Generate a pseudorandom sequence S of length $M \times N$ using the above CI methods respectively.
2) Transform the image into a $M \times N$ integer sequence.
3) The LSBs (Least Significant Bits) of the image integer sequence are replaced by the generated random bits S. These random LSBs will be treated as a keystream.
4) The information (text or picture) to hide is transformed into a binary sequence.
5) The binary message is hiding into the random LSBs of the image sequence, by using the bitwise exclusive or operation between the two sequences, starting from a selected position acting as part of the secret key.

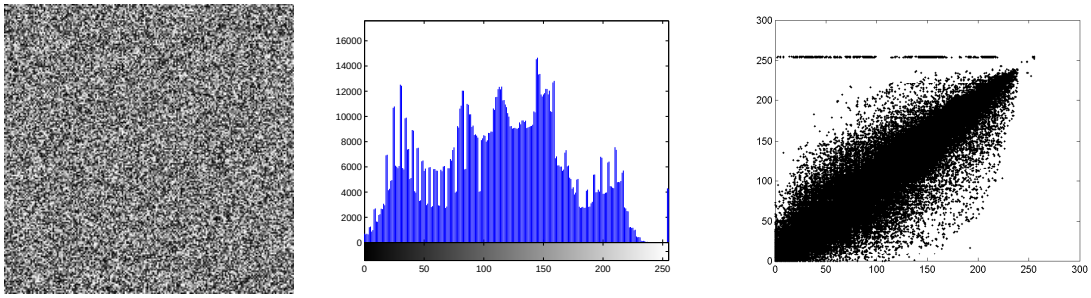
Pseudorandom sequences generated by the three CI methods mentioned in the previous section, with two XORshift generators and a given image, are used in this application to process to an evaluation of the scheme.

B. First Experimental Evaluation of the Proposed Scheme

1) The context: The original image of size 713×713, probably the most widely used test image for all kind of processing algorithms (such as compression and encryption), is depicted in Fig. 1-a. Fig. 1-c presents its histogram, and Fig. 1-d shows the correlation distribution of two horizontal adjacent pixels in this original image. Finally, information that must be hidden into it is the picture of Fig. 1-b, which has 89×89 pixels.

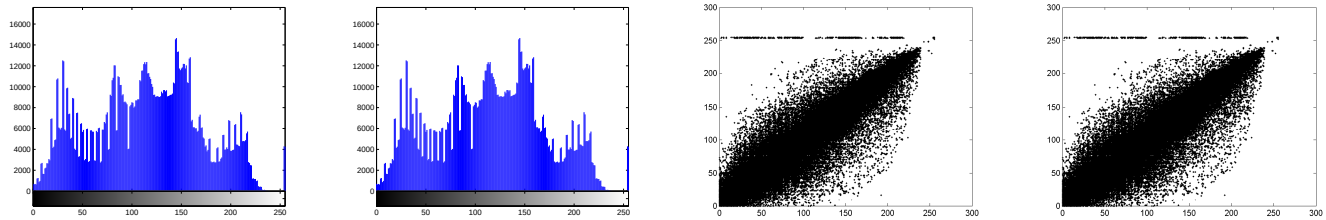
2) Histogram and Horizontal Correlation: Two XORshift generators are used to generate a random sequence based on the old CI method. Results are shown in Fig. 2. Histograms and correlation distributions (Fig. 2-a,b,c,d) are very closed to each other, leading to the assumption that such a method can well protect the hidden information when facing statistical attacks. The same experimental validation has been applied to the New CI method using two XORshift generators. Such

 ISBN: 978-1-61208-204-2



(a) (b) (c)

Figure 6: (a) The encrypted Lena (one-time pad using XOR CI). (b) Histogram of Fig.(a). (c) Correlation distribution of two adjacent pixels in Fig.(a)



(a) (b) (c) (d)

Figure 7: (a) Histogram of pixel values when LSBs are replaced by XOR CI. (b) Histogram of pixel values when LBSs are a hidden message xored with XOR CI. (c) Correlation distribution of two adjacent pixels in Fig.(a). (d) Correlation distribution of two adjacent pixels in Fig.(b).

experiments lead to results that are shown in Fig. 3. These first results are encouraging and confirm that simple histogram and correlation evaluations cannot detect the presence of hidden messages. The same conclusion can be claimed when using the XOR CI generator, as it is depicted in Fig. 7.

3) All directions correlation coefficients analysis: Using an identical experimental evaluation than in [15], the correlation coefficients of the horizontal, vertical, and diagonal directions of all the concerned images (original, with random as LSBs, and with secret information in these LSBs) are shown in Table I. It can be experimentally deduced that the correlation properties of these images are very similar to each other. So an attacker, whose intention is to analyze these coefficients in order to detect possible information hiding, cannot attain his/her goal by such a simple experiment.

4) Initial condition sensitivity: One of the most important properties of the chaotic sequences is that they are very sensitive to their initial conditions. This property can help to face an attacker who has access to the whole algorithm and to an approximation of the secret key. His/her intention, in this attack scenario, is to find the exact secret key (the seed of the keystream and the position of the message), by making small changes on this key. If the keystream and the position do not change a lot when the key is slightly updated, then the attacker can converge by small changes to the used secret key. In the experiments of Figure 8, we slightly alter the keys and try to extract the hidden information from the image. We can conclude that such optimistic attempts always fail in recovering the message.

C. A small evaluation of Encryption

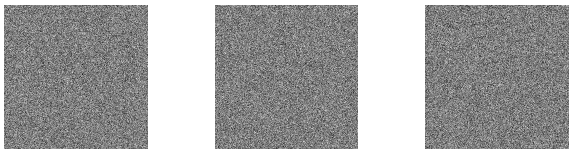
The dissimulation has been obtained in this paper by using the CIPRNGs recalled previously as stream cyphers: encryption is the result of the use of the bitwise exclusive or (XOR) between the given message and pseudorandom sequences generated from various CIPRNGs. We can wonder whether an attacker, who has access to the histogram of LSBs, can infer what can of CIPRNG has been used as keystream. For obvious reasons, these histograms should at least be uniform for each PRNG.

For illustration purpose, Lena has been encrypted by such method using each of the three kind of CIPRNGs, and histogram and correlation distribution of the encrypted image have been computed. The resulting images are depicted in Fig. 4 when using the Old CI method, in Fig. 5 for the New CI one, and in Fig. 6 for the last PRNG recalled here. We can show that this first reasonable requirement seems to be respected, even if this illustration is not a proof.

V. Conclusion

We have summarized in this paper our previous contributions in the field of pseudorandom generators, and we have proposed simple illustrative examples of use for information hiding. The three family of CIPRNGs recalled here are namely the Old CI, the New CI, and the XOR CI PRNGs. For each generator, firsts experimental evaluations of a simple information hiding scheme have been realized, to illustrate that that an attacker using simple statistics cannot determine easily, only by regarding the form of histograms or correlation distributions, the presence of an hidden message into a given document. No evidence of dissimulation appears at first glance, when comparing histograms, correlation distribution, or all

 ISBN: 978-1-61208-204-2



(a) (b) (c)

Figure 8: (a) The difference of two random LSBs image using Old CI PRNG with slight change in initial condition. (b) The difference of two random LSBs image using New CI PRNG with slight change in initial condition (c) The difference of two random LSBs image using XOR CI PRNG with slight change in initial condition

Table I: Correlation coefficients of two adjacent pixels in all directions in the original image, random LSBs images and infomation intergraded random LSBs images

Image \ Direction	Horizontal	Vertical	Diagonal
Original image	0.9793	0.9686	0.9488
Old CI			
no info	0.9792	0.9686	0.9488
intergrading info	0.9792	0.9686	0.9488
New CI			
no info	0.9793	0.9686	0.9488
intergrading info	0.9793	0.9686	0.9488
XOR CI			
no info	0.9793	0.9686	0.9487
intergrading info	0.9793	0.9686	0.9487

directions' correlation coefficients. Furthermore, experiments have illustrated high sensitivity to the secret parameters. These simple evaluations do not imply the security of the proposed scheme, they only illustrate that the use of the recalled PRNGs for information hiding can be further investigated by more stringent tools as steganalyzers and mathematical proofs.

REFERENCES

[1] Y. Hu, X. Liao, K. wo Wong, and Q. Zhou, "A true random number generator based on mouse movement and chaotic cryptography," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2286–2293, 2009.

[2] L. D. Micco, C. Gonzaez, H. Larrondo, M. Martin, A. Plastino, and O. Rosso, "Randomizing nonlinear maps via symbolic dynamics," *Physica A: Statistical Mechanics and its Applications*, vol. 387, no. 14, pp. 3373–3383, 2008.

[3] Q. Wang, C. Guyeux, and J. M. Bahi, "A novel pseudo-random generator based on discrete chaotic iterations for cryptographic applications," *INTERNET '09*, pp. 71–76, 2009.

[4] J. M. Bahi and C. Guyeux, "A new chaos-based watermarking algorithm," in *SECRYPT 2010, International conference on security and cryptography*, (Athens, Greece), pp. 1–4, July 2010.

[5] J. M. Bahi and C. Guyeux, "Topological chaos and chaotic iterations, application to hash functions," in *WCCI'10, IEEE World Congress on Computational Intelligence*, (Barcelona, Spain), pp. 1–7, July 2010. Best paper award.

[6] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*. Redwood City: Addison-Wesley, 2nd ed., 1989.

[7] J. Bahi, C. Guyeux, and Q. Wang, "A pseudo random numbers generator based on chaotic iterations. application to watermarking," in *WISM 2010, Int. Conf. on Web Information Systems and Mining*, vol. 6318 of *LNCS*, (Sanya, China), pp. 202–211, Oct. 2010.

[8] J. M. Bahi, C. Guyeux, and Q. Wang, "Improving random number generators by chaotic iterations. application in data hiding," in *ICCASM 2010, Int. Conf. on Computer Application and System Modeling*, (Taiyuan, China), pp. V13–643 – V13–647, Oct. 2010.

[9] Q. Wang, J. Bahi, C. Guyeux, and X. Fang, "Randomness quality of CI chaotic generators. application to internet security," in *INTERNET'2010. The 2nd Int. Conf. on Evolving Internet*, (Valencia, Spain), pp. 125–130, IEEE Computer Society Press, Sept. 2010. Best Paper award.

[10] J. M. Bahi, R. Couturier, C. Guyeux, and P.-C. Héam, "Efficient and cryptographically secure generation of chaotic pseudorandom numbers on gpu," *CoRR*, vol. abs/1112.5239, 2011.

[11] G. Marsaglia, "Xorshift rngs," *Journal of Statistical Software*, vol. 8(14), pp. 1–6, 2003.

[12] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications," *NIST Special Publication 800-22*, 2010.

[13] G. Marsaglia, "Diehard: a battery of tests of randomness." http://www.stat.fsu.edu/pub/diehard/ [retrieved: July,2011].

[14] P. L'ecuyer and R. Simard, "Testu01: A software library in ansi c for empirical testing of random number generators," *Laboratoire de simulation et doptimisation. Universit de Montral IRO*, 2009.

[15] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749 – 761, 2004.

 ISBN: 978-1-61208-204-2

Application of Steganography for Anonymity through the Internet

Jacques M. Bahi, Jean-François Couchot, Nicolas Friot, and Christophe Guyeux
FEMTO-ST Institute, UMR 6174 CNRS
Computer Science Laboratory DISC
University of Franche-Comté
Besançon, France
{jacques.bahi, jean-francois.couchot, nicolas.friot, christophe.guyeux}@femto-st.fr

***Abstract*—In this paper, a novel steganographic scheme based on chaotic iterations is proposed. This research work takes place into the information hiding security framework. The applications for anonymity and privacy through the Internet are regarded too. To guarantee such an anonymity, it should be possible to set up a secret communication channel into a web page, being secure. To achieve this goal, we propose an information hiding scheme being stego-secure, which is the highest level of security in a well defined and studied category of attacks called "watermark-only attack". This category of attacks is the best context to study steganography-based anonymity through the Internet. The steganalysis of our steganographic process is also studied in order to show its security in a real test framework.**

***Keywords-Privacy*; *Internet*; *Steganography*; *Security*; *Chaotic iterations*.**

I. INTRODUCTION

In common opinion or for non specialists, anonymity through the Internet is only desirable for malicious use. A frequent thought is that individuals who search or use anonymity tools have something wrong or shameful to hide. Thus, as privacy and anonymity software as proxy or Tor [1] are only used by terrorists, pedophiles, weapon merchants, and so on, such tools should be forbidden. However, terrorism or pedophilia existed in the absence of the Internet. Furthermore, recent actualities recall to us that, in numerous places around the world, to have an opinion that diverges from the one imposed by political or religious leaders is something considered as negative, suspicious, or illegal. For instance, Saudi blogger Hamza Kashgari jailed, may face execution after tweets about Muhammad [2]. Generally speaking, the so-called Arab Spring, and current fighting and uncertainty in Syria, have taught to us the following facts. First, the Internet is a media of major importance, which is difficult to arrest or to silence, bearing witness to the need for democracy, transparency, and efforts to combat corruption. Second, claiming his/her opinions, making journalism or politics, is dangerous in various states, and can lead to the death penalty (as for numerous Iranian bloggers: Hossein Derakhshan [3], Vahid Asghari, etc.).

Considering that the freedom of expression is a fundamental right that must be protected, that journalists must be able to inform the community without risking their own lives, and that to be a defender of human rights can be dangerous, various software have emerged these last decades to preserve anonymity or privacy through the Internet. Excepting of the Mix-Network principle [4], the most famous tool of this kind is probably Tor, the onion router. Tor client software routes Internet traffic through a worldwide volunteer network of servers, in order to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis. Another example of this kind is given by Perseus [5], a firefox plugin that protect personal data, without infringing any national crypto regulations, and that preserve the true needs of national security. Perseus replaces cryptography by coding theory techniques, such that only agencies with a strong enough computer power can eavesdrop traffic in an acceptable amount of time. Finally, anonymous proxy servers around the world can help to keep machines behind them anonymous: the destination server (the server that ultimately satisfies the web request) receives requests from the anonymizing proxy server, and thus does not receive information about the end user's address.

These three solutions are not without flaws. For instance, when considering anonymizers, the requests are not anonymous to the anonymizing proxy server, which simply moves the problem on: are these proxy servers worthy of trust? Perseus can be broken with enough computer power. And due to its central position and particular conception, Tor is targeted by numerous attacks and presents various weaknesses (bad apple attack, or the fact that Tor cannot protect against monitoring of traffic at the boundaries of the Tor network).

Considering these flaws, and because having a variety of solutions to provide anonymity is a good rule of thumb, a steganographic approach is often regarded in that context [6]. Steganography can be applied in several ways to preserve anonymity through the Internet, encompassing the creation of secret channels through background images of websites, into Facebook photo galleries, on audio or video streams, or

 ISBN: 978-1-61208-204-2

in non-interpreted characters in HTML source codes. The authors' intention is not to describe precisely these well-known techniques, but to explain how to evaluate their security. They applied it on a new algorithm of steganography based on chaotic iterations and data embedding in least significant coefficients. This state-of-the-art in information hiding security is organized as follows.

In Section II, some basic reminders concerning both mathematical notions and notations, and the Most and Least Significant Coefficients are given. Our new steganographic process called $\mathcal{DI}_3$ which is suitable to guarantee anonymity of data for privacy on the Internet is presented in Section III. In Section IV, a reminder about information hiding security is realized. The attacks classification in a steganographic framework are given, and the level of security of $\mathcal{DI}_3$ is studied. In the next section the security of our new scheme is evaluated. Then, in Section- VI, the steganalysis of the proposed process is realized, and it is compared with other steganographic schemes in the literature. This research work ends by a conclusion section, where our contribution is summarized and intended future researches are presented.

II. Basic Reminders

A. Mathematical definitions and notations

Let S^n denotes the n^{th} term of a sequence S, and V_i the i^{th} component of a vector V. For $a, b \in \mathbb{N}$, we use the following notation: $[\![a; b]\!] = \{a, a+1, a+2, \ldots, b\}$.

Definition 1: *Let* $\mathsf{k} \in \mathbb{N}^*$. *The set of all sequences which elements belong into* $[\![1; \mathsf{k}]\!]$, *called* strategy adapters *on* $[\![1; \mathsf{k}]\!]$, *is denoted by* $\mathbb{S}_{\mathsf{k}}$. □

Definition 2: *The* support of a finite sequence S *of* n *terms is the finite set* $\mathscr{S}(S) = \left\{S^k, k < n\right\}$ *containing all the distinct values of* S. *Its cardinality is s.t.* $\#\mathscr{S}(S) \leqslant n$. □

Definition 3: *A finite sequence* $S \in \mathbb{S}_{\mathsf{N}}$ *of* n *terms is* injective *if* $n = \#\mathscr{S}(S)$. *It is* onto *if* $N = \#\mathscr{S}(S)$. *Finally, it is bijective if and only if it is both injective and onto, so* $n = N = \#\mathscr{S}(S)$. □

Remark 1: *On the one hand, "*S *is injective" reflects the fact that all the* n *terms of the sequence* S *are distinct. On the other hand, "*S *is onto" means that all the values of the set* $[\![1; \mathsf{N}]\!]$ *are reached at least once.* □

B. The Most and Least Significant Coefficients

We first notice that terms of the original content x that may be replaced by terms issued from the watermark y are less important than other; they could be changed without be perceived as such. More generally, a *signification function* attaches a weight to each term defining a digital media, depending on its position t.

Definition 4: *A* signification function *is a real sequence* $(u^k)^{k \in \mathbb{N}}$. □

Example 1: *Let us consider a set of grayscale images stored into portable graymap format (P3-PGM): each pixel ranges between 256 gray levels, i.e., is memorized with eight bits. In that context, we consider* $u^k = 8 - (k \mod 8)$ *to be the* k*-th term of a signification function* $(u^k)^{k \in \mathbb{N}}$. *Intuitively, in each group of eight bits (i.e., for each pixel) the first bit has an importance equal to 8, whereas the last bit has an importance equal to 1. This is compliant with the idea that changing the first bit affects more the image than changing the last one.* □

Definition 5: *Let* $(u^k)^{k \in \mathbb{N}}$ *be a signification function,* m *and* M *be two reals s.t.* $m < M$.

- *The* most significant coefficients (MSCs) *of* x *is the finite vector*

$$u_M = \left(k \;\middle|\; k \in \mathbb{N} \text{ and } u^k \geqslant M \text{ and } k \leq |\, x \,|\right);$$

- *The* least significant coefficients (LSCs) *of* x *is the finite vector*

$$u_m = \left(k \;\middle|\; k \in \mathbb{N} \text{ and } u^k \leq m \text{ and } k \leq |\, x \,|\right);$$

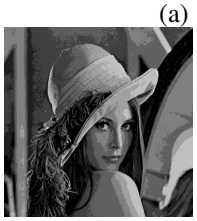
- *The* passive coefficients *of* x *is the finite vector*

$$u_p = \left(k \;\middle|\; k \in \mathbb{N} \text{ and } u^k \in]m; M[\text{ and } k \leq |\, x \,|\right).$$

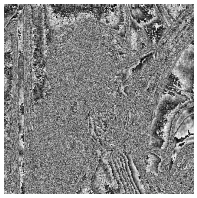
For a given host content x, MSCs are then ranks of x that describe the relevant part of the image, whereas LSCs translate its less significant parts.

Example 2: *These two definitions are illustrated on Figure 1, where the significance function* (u^k) *is defined as in Example 1,* $m = 5$, *and* $M = 6$.

(a) Original Lena.



(b) MSCs of Lena.



(c) LSCs of Lena ($\times$17).

Figure 1. Most and least significant coefficients of Lena.

Using the concept described in this section, it is now possible to expose our new steganographic scheme.

III. The new Process: $\mathcal{DI}_3$

In this section, a new algorithm, which is inspired from the scheme $\mathcal{CIS}_2$ described in [7], is presented. Unlike $\mathcal{CIS}_2$ which require embedding keys with three strategies, only one is required for $\mathcal{DI}_3$. Thus it is easyer to implement for Internet applications, especially in order to guarantee anonymization. Moreover, because in $\mathcal{DI}_3$ there is no operation to mix the message, this new scheme seems to be faster than $\mathcal{CIS}_2$, which is a major advantage to have fast response times on the Internet.

Let us firstly introduce the following notations. $\mathsf{P} \in \mathbb{N}^*$ is the width, in term of bits, of the message to embed into the cover media. $\lambda \in \mathbb{N}^*$ is the number of iterations to realize, which is s.t. $\lambda > \mathsf{P}$. The initial state $x^0 \in \mathbb{B}^{\mathsf{N}}$ is for the N LSCs of a given cover media C supposed to be uniformly distributed. $m \in \mathbb{B}^{\mathsf{P}}$ is the message to hide into x^0. Finally, $S \in \mathbb{S}_{\mathsf{P}}$ is a strategy such that the finite sequence $\left\{S^k, k \in [\![\lambda - \mathsf{P} + 1; \lambda]\!]\right\}$ is injective.

Remark 2: *The width P of the message to hide into the LSCs of the cover media x^0 has to be far smaller than the number of LSCs.* □

The proposed information hiding scheme is defined by an iterative process applied on LSCs of the cover media as follow:

Definition 6 ($\mathcal{DI}_3$ Data hiding scheme):
$\forall (n, i) \in \mathbb{N}^* \times [\![0; \mathsf{N} - 1]\!]$:

$$x_i^n = \begin{cases} x_i^{n-1} & \text{if } S^n \neq i \\ m_{S^n} & \text{if } S^n = i. \end{cases}$$ □

The stego-content is the Boolean vector $y = x^\lambda \in \mathbb{B}^{\mathsf{N}}$, which will replace the former LSCs (LSCs of the cover media are replaced by the vector y).

Remark 3: *The implementation of this data hiding scheme is exposed in a complementary work [8].* □

IV. Data Hiding Security and Robustness

A. Security and robustness

Even if security and robustness are neighboring concepts without clearly established definitions [9], robustness is often considered to be mostly concerned with blind elementary attacks, whereas security is not limited to certain specific attacks. Indeed, security encompasses robustness and intentional attacks [10], [11]. The best attempt to give an elegant and concise definition for each of these two terms was proposed in [10]. Following Kalker [10], we will consider in this research work the two following definitions:

Definition 7 (Security [10]): *Watermarking security refers to the inability by unauthorized users to have access to the raw watermarking channel [...] to remove, detect and estimate, write or modify the raw watermarking bits.* □

Figure 2. Simmons' prisoner problem [12]

Definition 8 (Robustness [10]): *Robust watermarking is a mechanism to create a communication channel that is multiplexed into original content [...] It is required that, firstly, the perceptual degradation of the marked content [...] is minimal and, secondly, that the capacity of the watermark channel degrades as a smooth function of the degradation of the marked content.* □

In this article, we will focus more specifically on the security aspects, which have been formalized in the Simmons' prisoner problem.

B. The prisoner problem

In the prisoner problem of Simmons [12], Alice and Bob are in jail, and they want to, possibly, devise an escape plan by exchanging hidden messages in innocent-looking cover contents (Fig. 2). These messages are to be conveyed to one another by a common warden, Eve, who over-drops all contents and can choose to interrupt the communication if they appear to be stego-contents.

C. Classification of Attacks

In the steganography framework, in the Simmons' prisoner problem context, attacks have been classified in [13] as follows.

Definition 9 (Classes of attacks):

WOA: *A* Watermark-Only Attack *occurs when an attacker has only access to several watermarked contents.*

KMA: *A* Known-Message Attack *occurs when an attacker has access to several pairs of watermarked contents and corresponding hidden messages.*

KOA: *A* Known-Original Attack *is when an attacker has access to several pairs of watermarked contents and their corresponding original versions.*

CMA: *A* Constant-Message Attack *occurs when the attacker observes several watermarked contents and only knows that the unknown hidden message is the same in all contents.* □

A synthesis of this classification is given in Table I.

In this article, we will focus more specifically on the "Watermark-Only Attack" situation, which is the most relevant category when considering anonymity and privacy protection through the Internet.

 ISBN: 978-1-61208-204-2

Class	Original content	Stego content	Hidden message
WOA		×	
KMA		×	×
KOA	×	×	
CMA			×

Table I
WATERMARKING ATTACKS CLASSIFICATION IN CONTEXT OF [10]

D. Reminder about Stego-Security

The stego-security, defined in the *Watermark-Only Attack* (WOA) framework, is the highest security level that can be defined in this setup [13].

Definition 10 (Stego-Security): *Let $\mathbb{K}$ be the set of embedding keys, $p(X)$ the probabilistic model of N_0 initial host contents, and $p(Y|K_1)$ the probabilistic model of N_0 watermarked contents. Moreover, each host content has been watermarked with the same secret key K_1 and the same embedding function e. Then e is said* stego-secure *if:*

$$\forall K_1 \in \mathbb{K}, p(Y|K_1) = p(X).$$

Until now, only three schemes have been proven stego-secure. On the one hand, the authors of [13] have established that the spread spectrum technique called Natural Watermarking is stego-secure when its distortion parameter η is equal to 1. On the other hand, we have proposed in [14] and [7] two other data hiding schemes satisfying this security property.

V. SECURITY STUDY

Let us prove that,

Proposition 1: *$\mathcal{DI}_3$ is stego-secure.* □

Proof: Let us suppose that $x^0 \sim \mathbf{U}\left(\mathbb{B}^{\mathsf{N}}\right)$, $m \sim \mathbf{U}\left(\mathbb{B}^{\mathsf{P}}\right)$, and $S \sim \mathbf{U}\left(\mathbb{S}_{\mathsf{P}}\right)$ in a $\mathcal{DI}_3$ setup, where $\mathbf{U}(X)$ describes the uniform distribution on X. We will prove by a mathematical induction that $\forall n \in \mathbb{N}, x^n \sim \mathbf{U}\left(\mathbb{B}^{\mathsf{N}}\right)$. The base case is obvious according to the uniform repartition hypothesis.

Let us now suppose that the statement $x^n \sim \mathbf{U}\left(\mathbb{B}^{\mathsf{N}}\right)$ holds for some n ($P\left(x^n = k\right) = \frac{1}{2^N}$).

For a given $k \in \mathbb{B}^N$, we denote by $\tilde{k_i} \in \mathbb{B}^N$ the vector defined by:
$\forall i \in [\![0; \mathsf{N}-1]\!]$, if $k = (k_0, k_1, \ldots, k_i, \ldots, k_{\mathsf{N}-2}, k_{\mathsf{N}-1})$, then $\tilde{k_i} = \left(k_0, k_1, \ldots, \overline{k_i}, \ldots, k_{\mathsf{N}-2}, k_{\mathsf{N}-1}\right)$, where $\overline{x}$ is the negation of the bit x.

Let p be defined by: $p = P\left(x^{n+1} = k\right)$. Let E_j and E be the events defined by: $\forall j \in [\![0; \mathsf{P}-1]\!], E_j = (x^n = \tilde{k_j}) \wedge (S^n = j) \wedge (m_{S^n} = k_j)$, $E = (x^n = k) \wedge (m_{S^n} = x_{S^n})$. So, $p = P\left(E \vee \bigvee_{j=0}^{\mathsf{N}-1} E_j\right)$.

On the one hand, $\forall j \in [\![0; \mathsf{P}-1]\!]$, the event E_j is a conjunction of the sub-events $(S^n = j)$ and other sub-events. $\forall j \in [\![0; \mathsf{P}-1]\!]$, all the sub-events $(S^n = j)$ are clearly pairwise disjoints, so all the evente E_j are pairwise disjoints too.

On the other hand, $\forall j \in [\![0; \mathsf{P}-1]\!]$, the events E_j and E are disjoints, because in E_j, a conjunction of the sub-event $(x^n = \tilde{k_j})$ with other sub-events appears, whereas in E a conjunction of the sub-event $(x^n = k)$ with other sub-events appears, and the two sub-events $(x^n = \tilde{k_j})$ and $(x^n = k)$ are clearly disjoints.

As a consequence, using the probability law concerning the reunion of disjoint events we can claim that: $p = P(E) + \sum_{j=0}^{N} P(E_j)$.

Now we evaluate both $P(E)$ and $P(E_j)$.

1) *The case of $P(E)$*: As the two events $(x^n = k)$ and $(m_{S^n} = x_{S^n})$ concern two different sequences, they are clearly independent.
Then, by using the inductive hypothesis: $P(x^n = k) = \frac{1}{2^N}$. So,

$$\begin{aligned} p(E) &= P(x^n = k) \times P(m_{S^n} = x_{S^n}) \\ &= \tfrac{1}{2^{\mathsf{N}}} \times [P(m_{S^n} = 0)P(x_{S^n} = 0) \\ &\quad + P(m_{S^n} = 1)P(x_{S^n} = 1)] \\ &= \tfrac{1}{2^{\mathsf{N}}} \times [P(m_{S^n} = 0)P(x_{S^n} = 0) \\ &\quad + P(m_{S^n} = 1)(1 - P(x_{S^n} = 0))] \\ &= \tfrac{1}{2^{\mathsf{N}}} \times \left[\tfrac{1}{2}P(x_{S^n} = 0) + \tfrac{1}{2}(1 - P(x_{S^n} = 0))\right] \\ &= \tfrac{1}{2^{\mathsf{N}+1}}. \end{aligned}$$

2) *Evaluation of $P(E_j)$*: As the three events $(x^n = \tilde{k_j})$, $(S^n = j)$, and $(m_n = k_j)$ deal with three different sequences, they are clearly independent. So

$$\begin{aligned} P(E_j) &= P(x^n = \tilde{k_j}) \times P(S^n = j) \times P(m_{S^n} = k_j) \\ &= \tfrac{1}{2^{\mathsf{N}}} \times \tfrac{1}{\mathsf{P}} \times \tfrac{1}{2} \\ &= \tfrac{1}{\mathsf{P}} \times \tfrac{1}{2^{\mathsf{N}+1}}, \end{aligned}$$

due to the hypothesis of uniform repartition of S and m.

$$\begin{aligned} \text{Consequently, } p &= P(E) + \sum_{j=0}^{\mathsf{P}} P(E_j) \\ &= \tfrac{1}{2^{\mathsf{N}+1}} + \sum_{j=0}^{\mathsf{P}} \left(\tfrac{1}{\mathsf{P}} \times \tfrac{1}{2^{\mathsf{N}+1}}\right) \\ &= \tfrac{1}{2^{\mathsf{N}}}. \end{aligned}$$

Finally, $P\left(x^{n+1} = k\right) = \frac{1}{2^N}$, which leads to $x^{n+1} \sim \mathbf{U}\left(\mathbb{B}^{\mathsf{N}}\right)$. This result is true $\forall n \in \mathbb{N}$, we thus have proven that the stego-content y is uniformly distributed in the set of possible stego-contents: $y \sim \mathbf{U}\left(\mathbb{B}^{\mathsf{N}}\right)$ when $x \sim \mathbf{U}\left(\mathbb{B}^{\mathsf{N}}\right)$. ■

Remark 4 (Distribution of LSCs): *We have supposed that $x^0 \sim \mathbf{U}\left(\mathbb{B}^{\mathsf{N}}\right)$ to prove the stego-security of the data hiding process $\mathcal{DI}_3$. This hypothesis is the most restrictive one, but it can be obtained at least partially in two possible manners. Either a channel that appears to be random (for instance, when applying a chi squared test) can be found in the media. Or a systematic process can be applied on the images to obtain this uniformity, as follows. Before embedding the hidden message, all the original LSCs must be replaced by randomly generated ones, hoping so that*

such cover media will be considered to be noisy by any given attacker.

Let us remark that, in the field of data anonymity for privacy on the Internet, we are in the "watermark-only attack" framework. As it has been recalled in Table I, in that framework, the attacker has only access to stego-contents, having so no knowledge of the original media, before introducing the message in the random channel (LSCs). However, this assumption of the existence of a random channel, natural or artificial, into the cover images, is clearly the most disputable one of this research work. The authors' intention is to investigate such hypothesis more largely in future works, by investigation the distribution of several LSCs contained in a large variety of images chosen randomly on the Internet. Among other things, we will check if some well-defined LSCs are naturally uniformly distributed in most cases. To conduct such studies, we intend to use the well-known NIST (National Institute of Standards and Technology of the U.S. Government) tests suite, the DieHARD battery, or the stringent TestU01 [15]. Depending on the results of this search for randomness in natural images, the need to introduce an artificial random channel could be possibly removed. □

Remark 5 (Distribution of the messages m): *In order to prove the stego-security of the data hiding process $\mathcal{DI}_3$, we have supposed that $m \sim \mathbf{U}\left(\mathbb{B}^{\mathsf{P}}\right)$. This hypothesis is not really restrictive. Indeed, to encrypt the message before its embedding into the LSCs of cover media if sufficient to achieve this goal. To say it different, in order to be in the conditions of applications of the process $\mathcal{DI}_3$, the hidden message must be encrypted.* □

Remark 6 (Distribution of the strategies S): *To prove the stego-security of the data hiding process $\mathcal{DI}_3$, we have finally supposed that $S \sim \mathbf{U}\left(\mathbb{S}_{\mathsf{P}}\right)$. This hypothesis is not restrictive too, as any cryptographically secure pseudorandom generator (PRNG) satisfies this property. With such PRNGs, it is impossible in polynomial time, to make the distinction between random numbers and numbers provided by these generators. For instance,* Blum Blum Shub (BBS) *[16],* Blum Goldwasser (BG)*, or* ISAAC*, are convenient here.* □

VI. Steganalysis

The steganographic scheme detailed along these lines has been compared to state of the art steganographic approaches, namely YASS [17], HUGO [18], and nsF5 [19].

The steganalysis is based on the BOSS image database [20] which consists in a set of 10 000 512x512 greyscale images. We randomly selected 50 of them to compute the cover set. Since YASS and nsF5 are dedicated to JPEG support, all these images have been firstly translated into JPEG format thanks to the `mogrify` command line. To allow the comparison between steganographic schemes, the relative payload is always set with 0.1 bit per pixel. Under that constrain, the embedded message m is a sequence of 26214 randomly generated bits. This step has led to distinguish four sets of stego contents, one for each steganographic approach.

Next we use the steganalysis tool developed by the HugoBreakers team [21] based on AI classifier and which won the BOSS competition [20]. Table II summarizes these steganalysis results expressed as the error probabilities of the steganalyser. The errors are the mean of the false alarms and of the missed detections. An error that is closed to 0.5 signifies that deciding whether an image contains a stego content is a random choice for the steganalyser. Conversely, a tiny error denotes that the steganalyser can easily classify stego content and non stego content.

Steganographic Tool	$\mathcal{DI}_3$	YASS	HUGO	NsF5
Error Probability	0.4133	0.0067	0.495	0.47

Table II
Steganalysis results of HugoBreakers steganalyser

The best result is obtained by HUGO, which is closed to the perfect steganographic approach to the considered steganalyser, since the error is about 0.5. However, even if the approach detailed along these lines has not any optimization, these first experiments show promising results. We finally notice that the HugoBreakers's steganalyser should outperform these results on larger image databases, *e.g.*, when applied on the whole BOSS image database.

VII. Conclusion and Future Work

Steganography is a real alternative to guarantee anonymity through the Internet. Unlike the principle of onion routers or Mix-networks, such a protocol using steganography doesn't require any third party potentially corrupted. Only the two parties who want to anonymously communicate are involved in the protocol. Each one holds a secret key for embedding and extraction of the message in the cover media. So to guaranty the anonymity of the communication, only the stealth and the undetectability of the message is required. It is assured by the security of the steganographic process. For instance, the scheme presented in this article offers a secure solution to achieve this goal, thanks to its stego-security. Even if this new scheme $\mathcal{DI}_3$ does not possess topological properties (unlike the $\mathcal{CIS}_2$), its level of security seems to be sufficient for Internet applications. Indeed, we take place into the *Watermark Only Attack (WOA)* framework, where stego-security is the highest level of security. Additionally, this new scheme is faster than $\mathcal{CIS}_2$. This is a major advantage for an utilization through the Internet, to respect response times of web sites. Moreover, for this first version of the process, the steganalysis results are promising.

In future work, various improvements of this scheme are planed to obtain better scores against steganalysers. For

 ISBN: 978-1-61208-204-2

instance, LSCs will be embedded into various frequency domains. The robustness of the proposed scheme will be evaluated too [22], to determine whether this information hiding algorithm can be relevant in other Internet domains interesting by data hiding techniques, as the semantic web. Finally a cryptographic approach of information hiding security is currently investigated, enlarging the Simmons' prisoner problem [23], and we intend to evaluate the proposed scheme in this framework.

REFERENCES

[1] www, "Tor: Anonymity online - protect your privacy. defend yourself against network surveillance and traffic analysis." 02 2012, [On line - 2012.02.22]. [Online]. Available: https://www.torproject.org/

[2] A. Wordsworth, News in National Post.com, Feb. 2012, availlable at http://news.nationalpost.com/2012/02/13/hamza-kashgari/.

[3] Wikipedia, "Hossein derakhshan — wikipedia, the free encyclopedia," 2012, [Online; accessed 1-May-2012]. [Online]. Available: http://en.wikipedia.org/w/index.php?title=Hossein_Derakhshan&oldid=488149891

[4] ——, "Mix network — wikipedia, the free encyclopedia," 2012, [Online; accessed 2-May-2012]. [Online]. Available: http://en.wikipedia.org/w/index.php?title=Mix_network&oldid=478408804

[5] ESIEA, "Perseus technology for anonymity through the internet," 02 2012, [On line - 2012.02.22]. [Online]. Available: http://www.esiea-recherche.eu/perseus.html

[6] C. Guyeux and J. Bahi, "An improved watermarking algorithm for internet applications," in *INTERNET'2010. The 2nd Int. Conf. on Evolving Internet*, Valencia, Spain, Sep. 2010, pp. 119–124.

[7] N. Friot, C. Guyeux, and J. M. Bahi, "Chaotic iterations for steganography - stego-security and chaos-security," in *SECRYPT*, J. Lopez and P. Samarati, Eds. SciTePress, 2011, pp. 218–227.

[8] J. M. Bahi, F. Couchot, N. Friot, and C. Guyeux, "A robust data hiding process contributing to the development of a semantic web," in *INTERNET'2012, The Fourth International Conference on Evolving Internet*, Venice, Italy, Jun. 2012, pp. ***–***, to appear.

[9] L. Perez-Freire, P. Comesanñ, J. R. Troncoso-Pastoriza, and F. Perez-Gonzalez, "Watermarking security: a survey," in *LNCS Transactions on Data Hiding and Multimedia Security*, 2006.

[10] T. Kalker, "Considerations on watermarking security," in *Multimedia Signal Processing, 2001 IEEE Fourth Workshop on*, 2001, pp. 201–206.

[11] P. Comesaña, L. Pérez-Freire, and F. Pérez-González, "Fundamentals of data hiding security and their application to spread-spectrum analysis," in *IH'05: Information Hiding Workshop*, ser. Lecture Notes in Computer Science, M. Barni, J. Herrera-Joancomartí, S. Katzenbeisser, and F. Pérez-González, Eds., vol. 3727. Lectures Notes in Computer Science, Springer-Verlag, 2005, pp. 146–160.

[12] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Advances in Cryptology, Proc. CRYPTO'83*, 1984, pp. 51–67.

[13] F. Cayre, C. Fontaine, and T. Furon, "Kerckhoffs-based embedding security classes for woa data hiding," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 1–15, 2008.

[14] C. Guyeux, N. Friot, and J. Bahi, "Chaotic iterations versus spread-spectrum: chaos and stego security," in *IIH-MSP'10, 6-th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, Darmstadt, Germany, October 2010, pp. 208–211.

[15] P. L'Ecuyer and R. Simard, "Testu01: A software library in ansi c for empirical testing of random number generators," *Laboratoire de simulation et d'optimisation. Université de Montréal IRO*, 2009.

[16] P. Junod, *Cryptographic secure pseudo-random bits generation: The Blum-Blum-Shub generator*. August, 1999.

[17] K. Solanki, A. Sarkar, and B. S. Manjunath, "Yass: Yet another steganographic scheme that resists blind steganalysis," in *Information Hiding*, ser. Lecture Notes in Computer Science, T. Furon, F. Cayre, G. J. Doërr, and P. Bas, Eds., vol. 4567. Springer, 2007, pp. 16–31.

[18] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Information Hiding*, ser. Lecture Notes in Computer Science, R. Böhme, P. W. L. Fong, and R. Safavi-Naini, Eds., vol. 6387. Springer, 2010, pp. 161–177.

[19] J. J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable jpeg steganography: dead ends challenges, and opportunities," in *MM&Sec*, D. Kundur, B. Prabhakaran, J. Dittmann, and J. J. Fridrich, Eds. ACM, 2007, pp. 3–14.

[20] P. Bas, T. Filler, and T. Pevný, "Break our steganographic system — the ins and outs of organizing boss," in *Information Hiding, 13th International Workshop*, ser. Lecture Notes in Computer Science, T. Filler, Ed. Prague, Czech Republic: Springer-Verlag, New York, May 18–20, 2011.

[21] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Transactions on Information Forensics and Security*, vol. PP Issue:99, pp. 1 – 1, 2011, to appear.

[22] J. Bahi, J.-F. Couchot, and C. Guyeux, "Steganography: a class of secure and robust algorithms," *The Computer Journal*, pp. ***–***, 2011, available online. Paper version to appear. [Online]. Available: http://dx.doi.org/10.1093/comjnl/bxr116

[23] J. M. Bahi, C. Guyeux, and P.-C. Héam, "A complexity approach for steganalysis," *CoRR*, vol. abs/1112.5245, 2011.

 ISBN: 978-1-61208-204-2

A Geometrically Resilient Digital Image Watermarking Scheme Based on SIFT and Extended Template Embedding

Po-Chyi Su
Dept. of Computer Science and Information Engineering
National Central University, Jhongli, Taiwan
Email: pochyisu@csie.ncu.edu.tw

Yu-Chuan Chang
Dept. of Computer Science and Information Engineering
National Central University, Jhongli, Taiwan
Email: 995202026@cc.ncu.edu.tw

***Abstract*—This research presents a feature-based still image watermarking approach. Scale-Invariant Feature Transform (SIFT) is first applied to locate the interest points, from which we form the invariant regions for watermark embedding. To resist geometrical transformations, the extended synchronization templates, which help to ensure that reasonably large invariant regions will be available for carrying the watermark payload and/or for increasing the confidence of watermark detection, will also be embedded. In the detection phase, after SIFT, the template is first determined locally by adjusting the related affine parameters of the grid to match with the possible hidden template signal so that the watermark can be retrieved afterwards. Experimental results show the feasibility of the proposed method.**

***Keywords*—digital watermark; geometrical transformations; SIFT; StirMark.**

I. INTRODUCTION

Digital watermarking has been considered as a potential solution to providing further protection of digital content. The close integration of the hidden signal, *i.e.*, digital watermark, with the host media can be used for declaring/verifying the ownership of the content, controlling the software/hardware operations or for the trailer tracking purposes. In most of the related applications, the digital watermark signal has to be robust against the "watermark attacks," including lossy compression, signal processing procedures and even malicious watermark-removal operations, etc. For still images, the watermark surviving geometrical transformations is always required since such manipulations as cropping, rotation and scaling are so common. Nevertheless, these procedures cause challenging synchronization problems for watermark detection and special care must be taken such that the watermark can resist such attacks to meet the requirements of applications.

Existing methods to resist geometrical transformations can be classified into four types, *i.e.*, the exhaustive search [1], embedding the watermark in invariant domains [2], [3], embedding synchronization templates [4], [5], [6] and employing feature detections for locating the watermark [7]. In our opinions, exhaustive search has to be coupled with certain side information to reduce its computational load. The algorithms of watermarking in invariant domains seem elegant but they may not perform well under all kinds of possible geometrical attacks. Employing synchronization templates may be a more flexible method to deal with attacks. However, the so-called "template attack" [8] may detect and remove the template if it is used repeatedly. The feature-based approaches thus gain more and more attention. Kutter *et al.* [7] first claimed that the feature-based approaches are the second-generation watermarking schemes. They illustrated this concept by applying the Mexican-hat wavelet to extract features and the Voronoi diagram to define the local characteristic regions for watermarking. Several methods have been proposed in recent years [9], [10], [11], [12], [13]. The basic idea of these approaches is applying such feature-point extraction as Harris corner detection [14] or Scale-Invariant Feature Transform (SIFT) [15], etc. to determine the interest areas, which are then transformed into the regions with known shape, size and orientation for the subsequent watermark embedding and detection. Since the interest points are extracted according to the content, the process of locating the embedded areas can be facilitated. Nevertheless, according to our observation, the feature-based watermarking may encountered some problems. First, in order to detect one watermark in a small invariant area, such transforms as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) or Discrete Fourier Transform (DFT) are usually applied and the middle-frequency components may be modified considerably to achieve the robustness and/or payload. Compared with the neighboring areas without watermarks, the quality of embedded area may be affected a lot, especially when the perceptual model is not employed. Second, deviations of the position, scale and/or orientation of the watermarked regions may appear under attacks, or even right after the watermark embedding without any attack. Therefore, almost all the schemes have to try a few different shapes of their invariant regions for the watermark detection. Then, the watermark here looks more like a template or pilot signal, instead of a watermark signal carrying the necessary hidden information. The false positive rate of watermark detection may also become higher. Furthermore, if image transforms are used, they have to be applied several times and the computational load will be increased. Third, there are

 ISBN: 978-1-61208-204-2

usually many feature points extracted from an image. We thus have to make sure that the watermark embedder and detect choose the same ones for processing and this is not a trivial issue. In our opinions, certain searching should be applied to make the feature-based approaches more practical.

In this research, we propose a feature-based still image watermarking approach based on SIFT and the extended template embedding to alleviate the above-mentioned problems. The spatial template signal will be embedded for achieving the synchronization. The template detection is based on the local search of the hidden templates to recover the regions for the subsequent watermark detection. The rest of the paper is organized as follows. The proposed scheme is detailed in Section II, including the reasons of such design, the determination of the invariant areas, the signal embedding and detection processes. Section III shows some experimental results and Section IV presents the conclusion and future work.

II. The Proposed Watermarking Approach

Fig. 1 illustrates the flowchart of the proposed scheme. To begin with, the image is applied with SIFT to extract the feature points, which help to determine the invariant regions by their descriptors, including location, scale, and orientation. Some inappropriate feature points are removed in the preprocessing step. The invariant regions for signal embedding will be formed around the remaining points. Basically, we segment the image into areas associated with different feature points and each invariant region extends to a large area for the signal embedding. We choose to embed the watermark that contains the necessary hidden information in DCT coefficients as an illustration while the template signal will be embedded in the spatial/pixel domain. Both signals will be weighted according to the perceptual model for guaranteeing the image quality. In other words, the template will serve as the pilot signal for synchronization. In the signal detection, SIFT is applied and the local searching will be performed around the extracted feature points to determine the possible areas with watermark. The preprocessing step may be omitted if the detection efficiency is not the major issue. Through the template detection, we can roughly locate the target areas and then perform the watermark detection. This design may look a bit strange to many people since the feature-point extraction should have solved the synchronization problem and the template or pilot signals seem unnecessary. However, the watermark detection usually requires pretty strict synchronization for signal matching. As mentioned before, the feature detection will be affected by geometrical attacks more or less and the accuracy may not be enough. The use of template will help to not only ensure the synchronization but speed up the detection process. Therefore, the major contribution of our research is to combine the different types of watermarking approaches in a reasonable way to achieve the feasibility. In other words, local searching will be applied to accommodate the possible deviations of extracted features. The searching is based on template matching but different (known) templates can be used to avoid the "template attacks." As the template or pilot signals may not carry enough information for the target applications, we only use them for synchronization and the watermark carrying the information can thus be embedded and detected successfully. Furthermore, compared with the existing methods, our algorithm demonstrates better performances against the random bending attack in StirMark [16], which applies different affine transformations on different areas. Next, we will detail each step in the following.

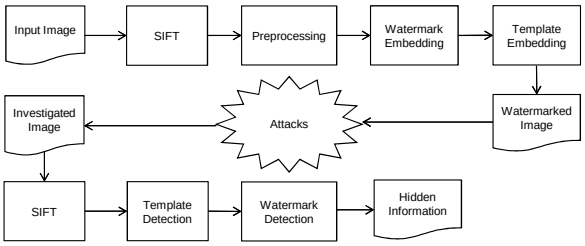


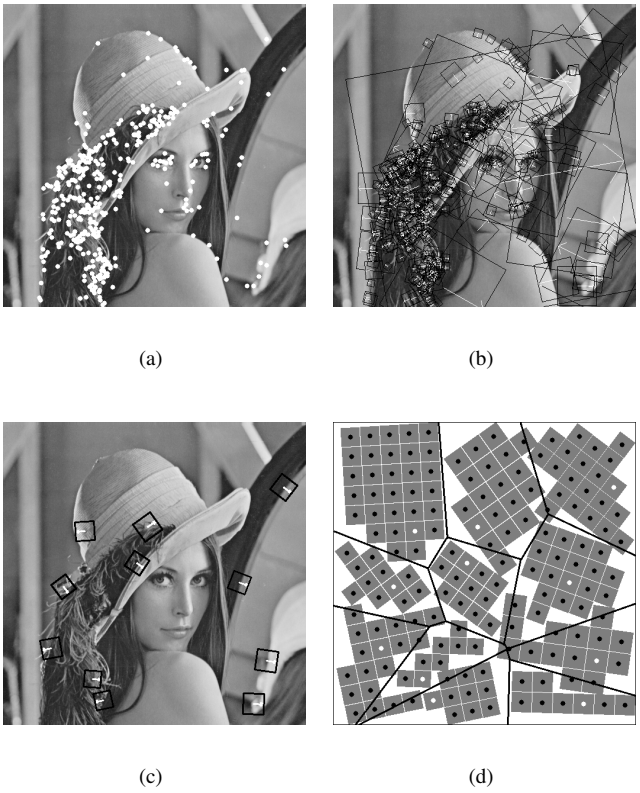
Fig. 1. The flowchart of the proposed watermarking approach.

A. Invariant Area Determination

The first step is to determine the areas for signal embedding/detection so that the synchronized detection can be achieved. Here, we use the Lena image to explain the procedures. Fig. 2(a) illustrates the interest or feature points extracted by SIFT and marked with white dots. Fig. 2(b) shows the invariant areas associated with all the feature points in Lena. The invariant regions are squares centered at the interest points. The square shape is chosen since the watermark will be embedded after a block transform. Besides, we will try to embed the signal in larger areas and these squares can help to cover a broader portion of an image by tiling. The length of one side of this square is determined by the multiplication of the characteristic scale of the corresponding SIFT feature point, λ, and a predefined positive value, τ. The orientation of the invariant area is also decided by the gradient information of the SIFT interest point. Since SIFT usually generates a large number of interest points and certain invariant regions are even overlapped, we choose to reject some interest points from signal embedding. First, we check the robustness of interest points and delete weaker ones. We apply JPEG compression with quality factor equal to 30, followed by Gaussian filtering, and pick those interest points that are still matched between the original image and attacked image. Some points are further eliminated according to their characteristic scales. It should be noted that the extracted invariant area will be embedded with the signal with a fixed size so the scaling/normalization of either our hidden signal pattern or the image content is inevitable. If the size of invariant area is too different from the size of the hidden pattern, the scaling itself may affect the embedded signal severely. For example, if the fixed size is 32×32, we will pick the feature point with its $\lambda \times \tau$ within the range of $[28, 36]$. Furthermore, we expect that the selected points should be separated from each other by a reasonable distance so we adopt the maximum distance algorithm to

 ISBN: 978-1-61208-204-2

disperse the feature points. To be more specific, the location of interest points can be seen as a set of 2-dimensional vectors, $\mathcal{V} = \{\mathbf{v_i}\}$. We calculate the centroid of the $|\mathcal{V}|$ vectors and choose the one closest to the centroid as our first feature point, $\mathbf{fp_1}$. From the $|\mathcal{V}| - 1$ vectors, choose the one that has the largest distance from the first feature point as the second feature point, $\mathbf{fp_2}$. To find the third feature point from the remaining $|\mathcal{V}| - 2$ vectors, we calculate the distance $Dist_i$ of each vector, $\mathbf{v_i}$, and the already chosen feature points, (*i.e.*, $Dist_i = Min(Dist(\mathbf{fp_1}, \mathbf{v_i}), Dist(\mathbf{fp_2}, \mathbf{v_i}))$). Again, we will find the one with the largest distance as $\mathbf{fp_3}$. Repeat the process to increase the number of feature points until the additional feature point will yield the distance from the selected points smaller than a distance threshold, T_{Dist}. These feature points will then be used to form the grids for the signal embedding. Fig. 2(c) illustrates the chosen invariant regions. Some existing schemes may only employ these regions for the watermark embedding/detection. However, if the regions are small, the payload or the detection confidence will be affected. On the other hand, if a larger size is used, the embedded watermark may be affected by the local distortion easily. In our scheme, the invariant areas or grids will be extended to cover a larger area for signal embedding. The major advantages of expanding are enhancing the detection confidence, even though weak signals are embedded, and the increased robustness against the random bending by StirMark. Before expanding, we use Voronoi diagram to set up the boundaries for separating the image into subregions and each subregion belongs to one selected feature point. The expansion of invariant area can then be applied. For an invariant grid, four extended grids are generated. The grids associated with the same feature point will thus have the same size and orientation. The same process will be applied on each extended grid too and the expansion from one initial grid will be limited in the Voronoi subregion. A few grids can still be added on the boundaries of Voronoi subregions as long as the added ones will not overlap others. The grids for signal embedding can then be generated almost all over the host image as illustrated in Fig. 2(d).



(a) (b) (c) (d)

Fig. 2. (a) The extracted feature points by SIFT on Lena and (b) the associated invariant areas. (c) The chosen invariant regions and (d) the extended grids.

B. Signal Embedding

It should be noted that the signals will be embedded into almost all the grids but the grids that cover the initially selected feature points as shown in Fig. 2(c). The reason of such omission is to avoid the embedded signals from modifying the descriptors of interest points and from making these points undetectable. According to our observation, the signal embedding will change the image data more or less and we cannot fully prevent the feature-point extraction from being affected. Although we may apply SIFT on the embedded area right after the embedding to see whether the selected feature point is reliable or not, we choose not to take this risk so that the embedding process can be simplified. In other words, the signals will only be embedded into the extended grids. Therefore, each extended grid will be embedded with the watermark first and then with the template signal. For the watermark embedding, we employ a pretty traditional spread spectrum approach in DCT as an example. A pseudo-random sequence W taking two values, *i.e.*, ± 1, is generated as the watermark signal and embedded into the middle-low frequency DCT coefficients. To be more specific, we randomize Hadamard sequences to generate the watermark sequences since they are mutually orthogonal. This bipolar watermark signal is then weighted according to Watson's perceptual model [17]. Although Watson's model should be able to be applied on blocks with variable sizes, some questioned that it can only ensure the invisibility of the noises within blocks. We thus choose small blocks for the watermark embedding. A grid with its side length equal to $\lambda \times \tau$ will be rotated and scaled into a 32×32 block, which will be divided into 8×8 subblocks for the watermark embedding. According to the zig-zag scan, the lowest three DCT coefficients are skipped and the next three coefficients are chosen as an illustration for watermark embedding/detection. The lowest frequency components are excluded to maintain the high image quality while the high-frequency components are not chosen to reduce the interference from the template signals. It should be noted that other methods, such as quantization index modulation, may also work under our framework since the synchronization issue will be settled. The Watson's model basically takes two masking effects into account, *i.e.*, the luminance masking

 ISBN: 978-1-61208-204-2

and contrast masking. The luminance masking refers to the dependency of the visual threshold and the mean luminance of the local image region while the contrast masking indicates that the threshold for a visual pattern would be reduced in the presence of other patterns. The Just Noticeable Difference (*JND*) of a DCT coefficient, $m_{i,j,h}$, is computed as

$$m_{i,j,h} = Max[a_{i,j,h}, |c_{i,j,h}|^{s_{i,j}} \times a_{i,j,h}^{(1-s_{i,j})}], \quad (1)$$

where $a_{i,j,h}$ is the luminance-adjusted threshold related to the global display and perceptual parameters, such as the viewing distance, display resolution and luminance. $c_{i,j,h}$ is the DCT coefficient and $s_{i,j}$ is the exponent that typically is set as 0.7.

As mentioned before, for a given grid, $\mathbf{G}$, we will transfer it to a 32×32 square $\hat{\mathbf{G}}$ and the watermark signals will be embedded into its 8×8 DCT coefficients $c_{i,j,h}$ by

$$c'_{i,j,h} = \begin{cases} c_{i,j,h} + w_{i,j,h} \cdot m_{i,j,h}, \\ \quad \text{if } sgn(c'_{i,j,h}) = sgn(c_{i,j,h}) \\ 0, \quad \text{otherwise,} \end{cases} \quad (2)$$

where $c'_{i,j,h}$ is the watermarked coefficient and the watermarked grid, $\mathbf{G}'$, is formed by the inverse DCT. We calculate the difference grid $\bar{\mathbf{G}} = \mathbf{G}' - \hat{\mathbf{G}}$. For each pixel in the grid, $\mathbf{G}$, we determine its deviation by checking $\bar{\mathbf{G}}$ with the inverse mapping. Since the watermark sequence is long, we will embed it into several grids. A selected feature point will serve as an anchor point and the watermark sequence will be embedded into the corresponding locations.

Then, each pixel in an extended grid will be embedded with the component of a 32×32 template taking ± 1. Since the template signal can be viewed as a spatial-domain watermark, to maintain the quality of the image, we employ the noise visibility function (*NVF*) [18] to determine the embedded energy. For each pixel, $I(i,j)$, its *NVF* is derived from:

$$NVF(I(i,j)) = \frac{1}{1 + \sigma_I^2(i,j)}, \quad (3)$$

where $\sigma_I^2(i,j)$ denotes the local variance in a window centered on the pixel. The template embedding is applied by

$$I^t(i,j) = I^r(i,j) + (1 - NVF(I(i,j))) \cdot \alpha_s \cdot W_t(i,j), \quad (4)$$

where $I^r(i,j)$ denotes the DCT watermarked pixel and $\alpha_s = 3$ is a predefined embedding strength. $W_t(i,j)$ is the template component and $I^t(i,j)$ is the resulting pixel.

C. Signal Detection

For the signal detection, an investigated image will be applied with SIFT to extract the feature points to locate the areas for the hidden signal detection. The correlation between the retrieved signal and the host template/watermark will be computed to verify whether the hidden signal exists. If the template is found, the watermark will be extracted and the expanding procedure will be performed to find other areas for detections. Since the grid covering the initial feature point is not embedded with any signal, we adopt a strategy of "delayed detection." Given a selected interest point, we use its characteristic orientation and scale to help extract the four adjacent grids for template detection. For each extended grid, we slightly adjust the parameters to form various affine matrices and grid centers. A set of compensative grids, $\hat{\mathbf{G}}_\mathbf{u}$, are generated for tests. The positions do not need to be integers so that the accuracy can be further achieved. Then we apply the interpolation to form a 32×32 block for the template detection. Since the detection in the extended grids around the feature point is very important, we test 3×3 positions (± 1 pixels in horizontal and vertical directions), $\pm 6^\circ, \pm 4^\circ, \pm 2^\circ$ rotations, and $\pm 6, \pm 4, \pm 2$ pixel differences of the grid side. Totally 441 detections will be applied for each grid. The detection is based on the correlation coefficient of the template $\mathbf{W_t}$ and the filtered grid by

$$\rho_u = \frac{\mathbf{W_t} \cdot \tilde{\mathbf{G}}_\mathbf{u}}{\sqrt{\mathbf{W_t} \cdot \mathbf{W_t}} \sqrt{\tilde{\mathbf{G}}_\mathbf{u} \cdot \tilde{\mathbf{G}}_\mathbf{u}}}, \quad (5)$$

where $\tilde{\mathbf{G}}_\mathbf{u}$ is obtained by filtering $\hat{\mathbf{G}}_\mathbf{u}$ with

$$\mathbf{H} = \begin{bmatrix} 0 & 1 & -2 & 1 & 0 \\ 1 & 2 & -6 & 2 & 1 \\ -2 & -6 & 16 & -6 & -2 \\ 1 & 2 & -6 & 2 & 1 \\ 0 & 1 & -2 & 1 & 0 \end{bmatrix}. \quad (6)$$

The largest response, ρ_u^{max}, in an extended grid is compared with a threshold, T_1, to determine if the template exists. The sphere model [19] is used to evaluate the false positive rate. For a single detection, the false positive rate is estimated by

$$P_{fp}^{single}(\rho) = \frac{\int_0^{\cos(\rho)} \sin^{N-2}(x) dx}{2 \int_0^{\pi/2} \sin^{N-2}(x) dx}, \quad (7)$$

where ρ is the response of a single detection and $N = 32 \times 32$. The false positive rate of a grid is

$$P_{fp}^{grid}(\rho) = 1 - (1 - P_{fp}^{single}(\rho))^K, \quad (8)$$

where $K = 411$ is the number of detections in a grid. We can thus set T_1 according to the target false alarm rate.

Once the first extended grid associated with a selected feature point is marked as being embedded with the template pattern, we can proceed to expand the invariant area by the similar method. Again, the delayed detection will be applied. That is, we employ/adjust the determined affine matrix and grid center that result in the largest response in the already detected grid for testing the current extended grid. The slight difference is that less trials are used in the extended grids to speed up the process. To be more specific, we check 3×3 positions and ± 2 degrees so totally $K = 27$ compensated grids will be tested. If the largest response among the K trials is not large enough, the expanding procedure from this grid will be stopped. The unique idea in our approach is that we do not use a single fixed threshold for determining the existence of a template. Since we adopt the strategy of extended grids, after we find a large response, it is quite possible that the adjacent grids will be embedded with the signal. We thus adopt a lower threshold T_2 for the further extended grids and this trick is quite helpful in correctly finding more grids for the

 ISBN: 978-1-61208-204-2

subsequent watermark detection. However, a lower threshold may introduce a higher false alarm rate. Our strategy is to set up another adaptive threshold, T_3. From our observations, the responses in grids of a subregion are usually related as they are similarly large or small, T_3 is designed as $\rho_m - 2 \times \rho_\sigma$, where ρ_m is the mean of detected template responses in a subregion so far, and ρ_σ is the standard deviation. The rule of template detection is thus as follows. If ρ_u^{max} of a grid is larger than T_1, the template is ruled as being detected. If ρ_u^{max} is smaller than T_1 but larger than $\max\{T_2, T_3\}$, the responses of its neighbors will be checked. If there is at least one neighbor with its ρ_u^{max} larger than T_1 or there are at least two neighbors with their ρ_u^{max} larger than T_2, the template will also be ruled as being detected. For the grids around the selected feature point, $T_1 = 0.1425$ and $T_2 = 0.1089$. For other extended grids, $T_1 = 0.1233$ and $T_2 = 0.0937$. The corresponding false alarm rates of T_1 and T_2 are 0.001 and 0.033 respectively. Basically, the expansion is applied in a recursive way but we always check whether a response of a grid has been computed before to speed up the process.

After the template detection helps to achieve the synchronization, the detection of watermark can be executed in a straightforward manner. The 32×32 affine-transformed grid will be divided into sixteen 8×8 subblocks for calculating DCT. The same coefficients will be considered for the watermark detection. Similarly, the response, ρ_b, is calculated by

$$\rho_b = \frac{\sum_h \sum_{(i,j)\in B} c^*_{i,j,h} \times w^b_{i,j,h}}{\sqrt{\sum_h \sum_{(i,j)\in B} (c^*_{i,j,h})^2} \sqrt{\sum_h \sum_{(i,j)\in B} (w^b_{i,j,h})^2}}, \quad (9)$$

where $c^*_{i,j,h}$ is the DCT coefficient and B is the set of selected DCT coefficients and $w^b_{i,j,h} = \pm 1$ is the component of tested watermark sequence. After all the grids are detected, the existence of watermark is claimed if ρ_b is larger than a threshold, T_{nc}, which is also set according to a pre-determined false positive rate by Eq. (7) with N equal to the number of considered DCT coefficients. Large ρ_b indicates the existence of a certain watermark signal. To embed more information, we may simply divide the DCT coefficients into m parts and each part is embedded with one of 2^n watermark sequences so that $m \times n$ bits are embedded.

III. Experimental Results

We demonstrate some results to show the feasibility of the proposed approach by using 512×512 Lena image. The size of a template pattern is set to be 32×32 as mentioned before. The marked image is shown in Fig. 3 with Peak Signal to Noise Ratio (PSNR) equal to 36.43 dB. Then we test several kinds of attacks on the proposed watermarking scheme. We use StirMark benchmark 4.0 to generate the attacked images, including rotating $1°$, $2°$, $5°$, $10°$, $15°$, $30°$, $45°$, $90°$, scaling to 50%, 60%, 70%, 75%, 80%, 90%, 110%, 120% of the size, cropping off 15%, 25%, 50%, 75% of the size, horizontally/vertically shearing by 5%, JPEG with quality factor equal to 90, 70, 50, Gaussian filtering, sharpening, and rotating with cropping by $15°$ and $45°$. Table I shows the results of the attacked Lena images. The second column shows the number of detected SIFT interest points. The two values shown in the third column are the numbers of correctly determined interest points for watermarking and those should be detected. The fourth column lists the numbers of detected grids, followed by the numbers of false positive detections. The fifth column shows the responses of watermark detections. The sixth column shows the threshold T_{nc}, which corresponds to the false alarm rate equal to 10^{-8}. The execution time evaluated in seconds is listed in the seventh column as the reference. The first row shows the results of marked image without any attack for comparison. All the embedded grids can be correctly determined. As we can see, the watermarks are detected in almost all the cases except the attack of scaling by 50% and cropping by 75%. Cropping by a large scale may result in fewer feature points left and the number of DCT coefficients may not be large enough to generate a higher response than the adaptive threshold.

Compared with the existing works, such as [9] and [10], our method demonstrates more consistent performances under various attacks. We can compare the numbers of detected regions, as shown in the third column of Table I, with those listed in the tables of [10]. The values in their five methods vary in different cases. If we use the ratio, *i.e.*, the number of detected areas divided by the number of embedded areas, as an indication, the ratios of five approaches in [10] are $71/168 = 0.42$, $20/132 = 0.15$, $84/276 = 0.30$, $53/324 = 0.16$ and $52/156 = 0.33$. The ratio of [9] is $73/468 = 0.16$ and ours is $68/132 = 0.52$, which is the highest. In addition, our approach has reasonable performances in all the attack cases except the aspect-ratio changes, from which no template can be determined. This problem may be solved by employing more flexible templates, instead of squares only. It is worth noting that our scheme may outperform others under the random bending attack by StirMark. Since this attack is applied in a random way, each time a different outcome appears. Table II illustrates the performances of our scheme against such attack. We employ two parameters, weaker (1.0) and stronger (2.0) geometrical modifications. The tests are run six times in each case. We can see that our scheme has no problem dealing with the random bending on the Lena image. In fact, according to our experiments, strong attacks sometimes cause misses of detections in other images. For stronger random bending attacks, two challenges may appear. The first challenge is the stability of SIFT interest points. It seems that either the descriptors or positions of interest points are changed. The same problem may happen when sharpening is applied. We think that developing a more suitable feature extraction method for digital watermarking may be an interesting research topic. The second challenge is that using only square grids for matching may not be enough, as mentioned before. Further adjusting the parameters of grids, such as modifying the positions of four corners in different ways, may provide more diverse forms of grids for detection. However, heavier computational load will be expected and may hinder the feasibility.

 ISBN: 978-1-61208-204-2

Fig. 3. The watermarked Lena with PSNR equal to 36.43 dB.

TABLE I
RESULTS OF ATTACKED LENA IMAGES

Attacks	Pts.	Regions	Grids	Response	T_{nc}	Time
NoAttack	77	11/11	161(0)	0.36	0.06	116
Rot. 1	97	10/11	143(0)	0.34	0.07	151
Rot. 2	82	10/11	124(2)	0.32	0.07	126
Rot. 5	90	10/11	143(1)	0.33	0.07	142
Rot. 10	94	8/11	112(1)	0.31	0.08	166
Rot. 15	79	9/11	124(0)	0.32	0.07	126
Rot. 30	95	10/11	119(1)	0.32	0.07	169
Rot. 45	91	7/11	85(0)	0.34	0.09	181
Rot. 90	81	11/11	161(0)	0.36	0.06	116
Scale 0.5	137	3/11	38(0)	0.06	0.13	252
Scale 0.6	167	7/11	32(1)	0.25	0.14	301
Scale 0.7	114	6/11	49(0)	0.31	0.12	206
Scale 0.75	104	8/11	111(2)	0.26	0.08	187
Scale 0.8	94	11/11	146(1)	0.32	0.07	156
Scale 0.9	70	8/11	95(0)	0.33	0.08	125
Scale 1.1	102	9/11	98(1)	0.32	0.08	175
Scale 1.2	136	8/11	107(1)	0.30	0.08	234
Crop 15%	73	8/ 8	92(0)	0.36	0.08	108
Crop 25%	60	7/ 7	65(0)	0.35	0.10	78
Crop 50%	29	3/ 3	19(0)	0.36	0.18	32
Crop 75%	6	1/ 1	4(0)	0.33	0.39	5
ShearX 5%	82	10/11	151(2)	0.30	0.07	116
ShearY 5%	92	9/11	131(1)	0.32	0.07	141
JPEG 90	80	11/11	161(0)	0.35	0.06	118
JPEG 70	88	10/11	131(1)	0.33	0.07	141
JPEG 50	95	7/11	49(0)	0.31	0.12	179
Gaussian	93	8/11	95(0)	0.35	0.08	137
Sharpen	75	4/11	57(0)	0.44	0.11	126
Rot.Crop15	76	8/8	81(0)	0.33	0.09	99
Rot.Crop45	61	5/5	54(1)	0.31	0.11	101

TABLE II
RANDOM GEOMETRICAL ATTACKS FROM STIRMARK

Attacks	Pts.	Regions	Grids	Response	T_{nc}	Time
Lena/1.0/(1)	98	10/11	124(2)	0.32	0.07	147
Lena/1.0/(2)	102	7/11	93(0)	0.33	0.11	159
Lena/1.0/(3)	97	10/11	138(0)	0.30	0.08	151
Lena/1.0/(4)	100	10/11	150(0)	0.37	0.11	142
Lena/1.0/(5)	97	8/11	109(1)	0.29	0.07	138
Lena/1.0/(6)	90	11/11	134(0)	0.31	0.11	137
Lena/2.0/(1)	107	8/11	52(0)	0.36	0.07	183
Lena/2.0/(2)	97	8/11	55(1)	0.29	0.07	166
Lena/2.0/(3)	108	8/11	59(1)	0.28	0.08	192
Lena/2.0/(4)	99	10/11	132(3)	0.28	0.09	147
Lena/2.0/(5)	111	8/11	85(0)	0.34	0.07	181
Lena/2.0/(6)	101	8/11	66(0)	0.21	0.10	170

IV. CONCLUSION

We developed a feature based image watermarking method enabling the spread spectrum based schemes to resist geometric distortions. SIFT is used to help solve the synchronization problem. The embedding regions are extended to increase the detection confidence. The experimental results show that the scheme is effective against rotation, scaling, cropping, shearing, and random bending. The current version mainly illustrates the feasibility and novel ideas of combining SIFT and extended template embedding. We may integrate this idea with the parallel computing to speed up the processing.

REFERENCES

[1] M. Barni, "Effectiveness of exhaustive search and template matching against watermark desynchrnizaion," *IEEE Signal Processing Letters*, vol. 12, no. 2, pp. 158–161, 2005.

[2] J. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal processing*, vol. 66, no. 3, pp. 303–317, 1998.

[3] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Trans. on Image Processing*, vol. 10, no. 5, pp. 767–782, 2001.

[4] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," *IEEE Trans. on Image Processing*, vol. 9, no. 6, pp. 1123–1129, 2000.

[5] M. Kutter, "Watermarking resisting to translation, rotation and scaling," in *Proc. of SPIE: Multimedia systems and applications*, Boston, MA, Nov. 1998, pp. 423–431.

[6] P.-C. Su and C.-C. J. Kuo, "Synchronized detection of the block-based watermark with invisible grid embedding," in *SPIE Photonics West*, San Jose, CA, Jan. 2001, pp. 423–431.

[7] M. Kutter, S. Bhattacharjee, and T. Ebrahimi, "Towards second generation watermarking schemes," in *IEEE International Confernece on Image Process*, vol. 1, 1999, pp. 320–323.

[8] A. Herrigel, S. Voloshynovsky, and Y. Rytsar, "The watermark template attack," in *SPIE Photonics West*, San Jose, CA, Jan. 2008, pp. 394–405.

[9] P. Bas, J. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Trans. on Image Processing*, vol. 11, no. 9, pp. 1014–1028, 2002.

[10] J. Seo and C. Yoo, "Image watermarking based on invariant regions of scale-space representation," *IEEE Trans. on Signal Processing*, vol. 54, no. 4, pp. 1537–1549, 2006.

[11] X. Gao, C. Deng, X. Li, and D. Tao, "Geometric Distortion Insensitive Image Watermarking in Affine Covariant Regions," *IEEE Trans. on Systems, Man and Cybernetics. Part C, Applications and reviews*, vol. 40, no. 3, pp. 278–286, 2010.

[12] X. Wang, J. Wu, and P. Niu, "A new digital image watermarking algorithm resilient to desynchronization attacks," *IEEE Trans. on Information Forensics and Security*, vol. 2, no. 4, pp. 655–663, 2007.

[13] D. Zheng, S. Wang, and J. Zhao, "RST invariant image watermarking algorithm with mathematical modeling and analysis of the watermarking processes," *IEEE Trans. on Image Processing*, vol. 18, no. 5, pp. 1055–1068, 2009.

[14] C. Harris and M. Stephens, "A combined corner and edge detector," in *Alvey vision conference*, vol. 15. Manchester, UK, 1988, p. 50.

[15] D. Lowe, "Distinctive image features from scale-invariant keypoints," *Int. journal of computer vision*, vol. 60, no. 2, pp. 91–110, 2004.

[16] F. Petitcolas, M. Steinebach, F. Raynal, J. Dittmann, C. Fontaine, and N. Fates, "A public automated web-based evaluation service for watermarking schemes: StirMark benchmark," in *Proc. SPIE*, 2001, pp. 575–584.

[17] A. Watson, "Visually optimal DCT quantization matrices for individual images," in *Data Compression Conference*, 1993, pp. 178–187.

[18] S. Voloshynovskiy, A. Herrigel, N. Baumgaertner, and T. Pun, "A stochastic approach to content adaptive digital image watermarking," in *Information Hiding*. Springer, 1999, pp. 211–236.

[19] M. Miller and J. Bloom, "Computing the probability of false watermark detection," in *The Third International Workshop on Information Hiding*, Dresden, Germany, Sep. 1999, pp. 146–158.

 ISBN: 978-1-61208-204-2

Formalizing and Verifying Anonymity of Crowds-Based Communication Protocols with IOA

Yoshinobu KAWABE
Department of Information Science, Aichi Institute of Technology
1247 Yachigusa Yakusa-cho, Toyota, Aichi, Japan
kawabe@aitech.ac.jp

***Abstract*—Crowds is a communication protocol that guarantees sender's anonymity. As a case study, this paper provides a computer-assisted anonymity proof for Crowds. To prove anonymity, we first describe a simple specification of Crowds with an I/O-automaton-based formal specification language. Then, the specification is translated into first-order logic formulae with a formal verification tool. Finally, by showing the existence of an anonymous simulation, the anonymity of Crowds is proved. In this proof, a theorem proving tool is employed. Also, in this study, we formalize an extension of Crowds that guarantees the anonymity with regard to a recipient.**

***Keywords*-anonymity; formal verification; Crowds; theorem-proving**

I. INTRODUCTION

On the Internet, there are many services and protocols where anonymity should be provided. For example, an electronic voting system should guarantee anonymity to prevent the disclosure of who voted for which candidate. When such services and protocols are developed, an anonymous communication system, such as Crowds [8], is often employed as a sub-protocol.

It is important to prove the correctness of anonymous communication systems. In the field of software engineering, there are formal method studies that have analyzed distributed systems. There are also formal method studies for anonymity, e.g. [4][9]; the method in [9] is a model-checking approach, and the method in [4] incorporates theorem-proving. In this study, based on the proof method in [4] we verify that a Crowds-based communication protocol is anonymous. To prove the anonymity, this study describes a simple specification of the protocol with a formal specification language. The specification is translated into first-order predicate logic's formulae with a verification tool, and the anonymity of Crowds is proved with a theorem prover. This paper also specifies an extension [5][6] of Crowds that guarantees recipient's anonymity as well as sender's anonymity.

There are already studies [5][6][10] that analyzed Crowds-based communication protocols. To analyze a Crowds-based protocol, in this study we employ I/O-automaton and a theorem proving tool; especially, the author believes that this is the first attempt to describe [5]'s protocol with I/O-automaton.

This paper is organized as follows. Section II illustrates the notion of anonymity and its formalization. In Section III, a formal specification of Crowds is described. In Section IV, the specification is translated into first-order predicate logic's formulae, and the anonymity is verified with a theorem proving tool. Section V formalizes an extension of Crowds that guarantees the anonymity of a recipient. We have discussions in Section VI.

II. PRELIMINARIES

This section first describes notations in I/O-automaton theory [7]. Then, we explain the notion of anonymity and its I/O-automaton-based formalization.

A. I/O-automaton

I/O-Automaton X has a set of actions $sig(X)$, a set of states $states(X)$, a set of initial states $start(X) \subset states(X)$ and a set of transitions $trans(X) \subset states(X) \times sig(X) \times states(X)$. We use $in(X)$, $out(X)$ and $int(X)$ as sets of input, output and internal actions, respectively; that is, $sig(X) = in(X) \cup out(X) \cup int(X)$. We assume that $in(X)$, $out(X)$ and $int(X)$ are disjoint. We define $ext(X) = out(X) \cup in(X)$ whose element is called an external action. For simplicity, this paper only deals with I/O-automaton X satisfying $in(X) = \emptyset$; that is, we assume that $ext(X) = out(X)$.

To formalize anonymity, this paper employs a family of actor action sets $act(X)$ with the following conditions:

- $\bigcup_{A \in act(X)} A \subset ext(X)$
- A and A' are disjoint for any distinct $A, A' \in act(X)$.

Transition $(s, a, s') \in trans(X)$ is written as $s \xrightarrow{a}_X s'$; we also write $s \rightarrow_X s'$ if a is internal. We define a relation $\twoheadrightarrow_X$ as the reflexive transitive closure of $\rightarrow_X$. For any $a \in sig(X)$ and $s, s' \in states(X)$, we write $s \stackrel{a}{\Longrightarrow}_X s'$ for $s \twoheadrightarrow_X s_1 \xrightarrow{a}_X s_2 \twoheadrightarrow_X s'$ with some $s_1, s_2 \in states(X)$ if a is external, or for $s \twoheadrightarrow_X s'$ if a is internal. For any $s_0 \in start(X)$ and transition sequence $\alpha = s_0 \xrightarrow{a_1}_X s_1 \xrightarrow{a_2}_X \cdots \xrightarrow{a_n}_X s_n$, the trace of α is the sub-sequence of $a_1 a_2 \cdots a_n$ consisting of all the external actions. In addition, we write $traces(X)$ for the entire set of X's traces.

 ISBN: 978-1-61208-204-2

B. Basic notion of anonymity

We explain the basic notion of anonymity with the following example.

Example 1 (Donating anonymously): There are two people, Alice and Bob, and we assume that only one of them has made an anonymous donation. Alice was going to contribute \$5, while Bob was going to contribute \$10.

I/O-automaton D1 in Fig. 1 describes the above situation. Actions $5 and $10 of D1 are external actions to represent a donation. I/O-automaton D1 has an initial state, and only one of I'm(Alice) or I'm(Bob) is possible at the initial state. Here, I'm(Alice) and I'm(Bob) are special actions that specify the donor. For convenience, we call I'm(Alice) and I'm(Bob) *actor actions*. We can see that D1 is anonymous if an adversary who observed all the occurrences of the non-actor actions cannot determine which actor action of D1 occurred.

Q1: Suppose an adversary observed that \$5 was posted. Can the adversary deduce who is the donor?

In D1, action $5 can occur only when actor action I'm(Alice) occurs. Thus, the adversary can deduce that Alice made a donation. That is, D1 is not anonymous.

One reason for D1 not being anonymous is that an adversary can know how much money was posted. To discuss this aspect, the next question is considered.

Q2: A donation was posted in an envelope. Is this donation anonymous?

We consider an operation to replace external actions $5 and $10 of D1 with a fresh external action env, and the resulting automaton is called D2 (see Fig. 1). This operation hides information on how much money was posted, so we can see that this operation formalizes the encryption of messages. With D2, an adversary who can detect the occurrence of env cannot deduce which actor action is possible. Hence, D2 is anonymous.

There are cases where we can establish the anonymity by encrypting messages. But, there are cases where we cannot establish the anonymity even though all the messages are encrypted. To explain this, our final question is introduced.

Q3: Bob was going to post \$10 in two envelopes each containing \$5. Is this donation anonymous?

Figure 1 also shows I/O-automaton D3, which describes the above setup. In this case, an adversary can determine the identity of a donor by counting the number of time that env occurs. Therefore, D3 is not anonymous. This example shows that a system might not be anonymous even though all the messages are encrypted. Hence, to establish anonymity, we should deal with patterns of communication such as the number of messages or the existence/nonexistence of a message.

C. Formalization of anonymity

If an eavesdropper cannot distinguish the trace set of system X and that of X's "anonymized" version, then we can see that X is anonymous. The anonymized system is formalized as follows.

Definition 1: Let X be an I/O-automaton. We define I/O-automaton $anonym(X)$ as follows:

- $states(anonym(X)) = states(X)$,
- $start(anonym(X)) = start(X)$,
- $ext(anonym(X)) = ext(X)$,
- $int(anonym(X)) = int(X)$,
- $act(anonym(X)) = act(X)$,
- $trans(anonym(X)) = trans(X)$
  $\cup \{(s_1, a, s_2) \mid (s_1, a', s_2) \in trans(X) \wedge A \in act(X) \wedge a' \in A \wedge a \in A\}$.

Definition 2: I/O-automaton X is trace anonymous if $traces(anonym(X)) = traces(X)$ holds.

For I/O-automata D1, D2 and D3 in Fig. 1, we can see that

$$\begin{cases} traces(anonym(\texttt{D1})) \neq traces(\texttt{D1}) \\ traces(anonym(\texttt{D2})) = traces(\texttt{D2}) \\ traces(anonym(\texttt{D3})) \neq traces(\texttt{D3}) \end{cases}$$

if we define $act(\texttt{D1})$, $act(\texttt{D2})$ and $act(\texttt{D3})$ as $act(\texttt{D1}) = act(\texttt{D2}) = act(\texttt{D3}) = \{\{\texttt{I'm(Alice)}, \texttt{I'm(Bob)}\}\}$. This follows Section II-B's result.

A simulation-based proof method for trace anonymity was introduced in [4].

Definition 3 ([4]): Assume X is an I/O-automaton. An anonymous simulation as of X is a binary relation on $states(X)$ that satisfies the following conditions:

1) $as(s, s)$ holds for any initial state $s \in start(X)$;
2) For any states $s_1, s_2, s_1' \in states(X)$ and action $a \in sig(X)$, $as(s_1, s_1')$ and $s_1 \xrightarrow{a}_X s_2$ implies the following:
   a) If $a \in A$ for some $A \in act(X)$ holds, for all $a' \in A$ there is a state s_2' such that $as(s_2, s_2')$ and $s_1' \overset{a'}{\Longrightarrow}_X s_2'$;
   b) If $a \notin \bigcup_{A \in act(X)} A$, there is a state s_2' such that $as(s_2, s_2')$ and $s_1' \overset{a}{\Longrightarrow}_X s_2'$.

Intuitively, for any states $s_1, s_2 \in states(X)$ and anonymous simulation as, $as(s_1, s_2)$ iff s_1 and s_2 are indistinguishable to an observer. The trace anonymity of an automaton can be proved by finding an anonymous simulation.

Theorem 1 ([4]): If automaton X has an anonymous simulation, X is trace anonymous. □

III. Crowds and its formalization

In this section, an overview of Crowds is described, and we formalize Crowds with an I/O-automaton.

A. Overview of Crowds

Crowds consists of a collection of agents that can communicate with each other (see Fig. 2). To set up a communication path to a website, agents employ the following protocol:

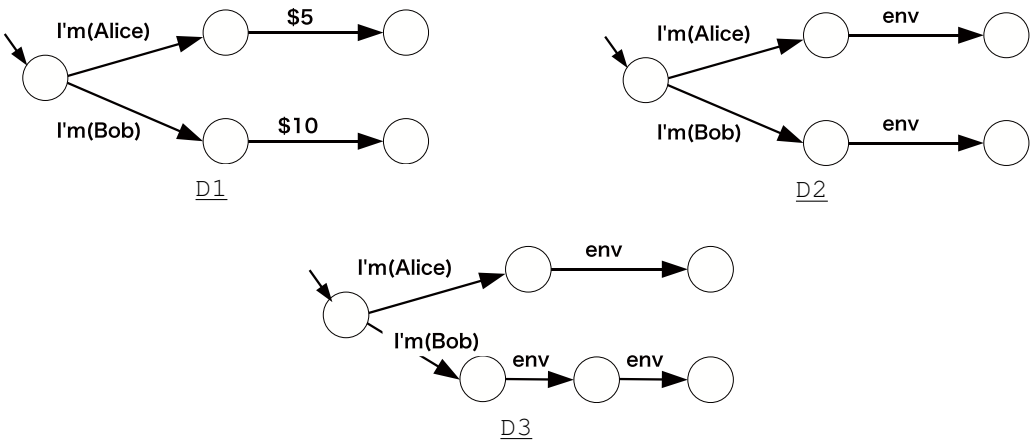


Figure 1. Formalizing Anonymous Donation

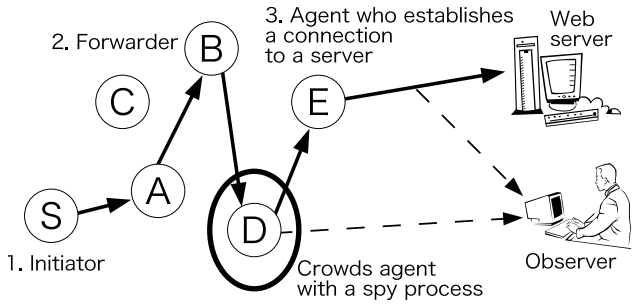


Figure 2. Crowds

The protocol of Crowds

phase 1	An initiator agent first generates a new request;
phase 2	If an agent i has a request, then the agent chooses another agent j randomly and forwards the request to j. By forwarding a request, agents i and j establish a link with regard to the request;
phase 3	After the request has been forwarded several times, some agent establishes a connection to a website.

After making a communication path with the above protocol, the initiator agent connects to a website. We assume that an observer (i.e. an eavesdropper) can observe a connection from a final agent to a website but the observer cannot observe a connection among Crowds agents.

This paper introduces a spy process, which is a computer virus that can read a message from the memory of a Crowds agent and broadcast the message to the public. We say a Crowds agent is 'corrupt' if the agent has a spy process. That is, a corrupt Crowds agent can:

- forward a request to another Crowds agent;
- establish a connection to a website; and
- reveal from which agent a request comes.

We say the Crowds system is anonymous if an observer cannot know which agent is the initiator agent. If there is no spy process then the Crowds system is clearly anonymous. However, it is not trivial in case of allowing spy processes.

B. Formalizing Crowds with IOA

Automaton `crowds` in Fig. 3 is a formal specification for Crowds. This is written in IOA, which is an I/O-automaton-based formal specification language. An IOA specification has three portions:

- `signature` declares sorts and actions;
- `states` declares variables and initial values;
- `transitions` defines the body of actions, where each action consists of a precondition (`pre`-part) and an effect (`eff`-part).

A state of automaton `crowds` is a tuple of values `pc`, `mesIsAt`, `mesIsFrom` and `corrp`. These values are as follows:

- `pc` is a program counter of the Crowds system. The value of `pc` ranges over:
  - `init`: Crowds agents waiting for a new request created,
  - `shuffle`: Crowds agents making a communication path, and
  - `terminate`: a communication path to a website established;
- `mesIsAt` is an ID of an agent that has a request;
- `mesIsFrom` is an ID of an agent that had a request in the previous step;
- `corrp` is an array of Boolean values. If `corrp[i]` is true, then agent `i` is corrupt.

Automaton `crowds` has four actions `start(i)`, `pass(i, j)`, `out(i)` and `reveal(i, j)`. Specifically, these actions are as follows:

```
automaton crowds
  signature
    output   start(i:ID)
    internal pass(i:ID, j:ID)
    output   out(i:ID)
    output   reveal(i:ID, j:ID)

  states
    pc:        PC := init,
    mesIsAt:   ID,
    mesIsFrom: ID,
    corrp:     Array[ID, Bool]

  transitions
    output start(i)  % actor action
      pre pc = init
      eff pc := shuffle;
          mesIsAt := i;
          mesIsFrom := i

    internal pass(i, j)
      pre pc = shuffle /\ i = mesIsAt
      eff mesIsFrom := i;
          mesIsAt := j

    output out(i)
      pre pc = shuffle /\ i = mesIsAt
      eff pc := terminate

    output reveal(i, j)
      pre    pc = shuffle
          /\ i = mesIsFrom
          /\ j = mesIsAt
          /\ corrp[j]
      eff do nothing
```

Figure 3. IOA specification for Crowds

- `start(i)` is an actor action, which represents that agent `i` creates a new request;
- `pass(i, j)` represents that a request is forwarded from agent `i` to agent `j`. This action is introduced as internal, since we assume that the observer cannot observe a connection between Crowds agents;
- `out(i)` represents that a final agent `i` establishes a connection to the website. Since a connection to a website is observable, `out(i)` is defined as an external action.
- `reveal(i, j)` is an action for a spy process.

We can see that actions `start(i)`, `pass(i, j)` and `out(i)` formalize phases 1, 2 and 3 of the Crowds protocol, respectively.

IV. Theorem-proving anonymity of Crowds

This section shows that `crowds` is trace anonymous. In this proof, a theorem proving tool is employed.

A. Translating IOA into first-order logic

Larch [2] is a theorem prover based on first-order predicate logic. I/O-automaton `crowds` is translated into Larch's language by IOA-Toolkit [1]. For example, the following is the result of translation with regard to action `start(i)`:

```
enabled(s, start(i)) <=> (s.pc = init)
effect(s, start(i)).pc = shuffle
effect(s, start(i)).mesIsAt = i
effect(s, start(i)).mesIsFrom = i
effect(s, start(i)).corrp = s.corrp
```

where

- `s.`α is the value of α at state `s`;
- `enabled(s, a)` is true iff action `a` is executable at state `s`; and
- `effect(s, a)` is the successor state of `s` for action `a`.

The first formula is for a precondition of action `start(i)`, and four equations are for a state change by `start(i)`.

B. Computer-assisted anonymity proof for Crowds

Below is a binary relation over *states*(`crowds`):

```
as(s, s')
  <=> (s.pc = s'.pc
       /\ (s.corrp[s.mesIsAt]
           <=> s'.corrp[s'.mesIsAt])).
```

This means that states `s` and `s'` are indistinguishable to an observer iff:

- `s.pc` and `s'.pc` are the same; and
- A corrupt agent has a request at state `s` iff a corrupt agent has a request at state `s'`.

We prove that `as` is an anonymous simulation. At first, the condition 1 of Definition 3 is proved. Specifically, we prove the following:

```
% --- Initial state condition
start(s:States[crowds]) => as(s, s)
```

where `start(s)` is true iff state `s` is an initial state. We can easily prove this with the Larch prover.

Then, the step correspondence for actions `pass(i, j)`, `out(i)` and `reveal(i, j)` is proved; that is, we prove condition 2-b in Definition 3. It suffices to show

```
% --- step correspondence condition
% --- for internal action pass(i, j)
(reachable(s1)
 /\ reachable(s1')
 /\ as(s1, s1')
 /\ enabled(s1, a)
 /\ effect(s1, a) = s2
 /\ ~anonymp(a)
 /\ internal(a))
 => (\E s2':States[crowds] (\E a':Actions[crowds]
       (   as(s2, s2')
        /\ enabled(s1', a')
        /\ effect(s1', a') = s2'
        /\ internal(a'))))
```

and

```
% --- step correspondence condition
% --- for output actions (except start(i))
(reachable(s1)
```

```
 /\ reachable(s1')
 /\ as(s1, s1')
 /\ enabled(s1, a)
 /\ effect(s1, a) = s2
 /\ ~anonymp(a)
 /\ output(a))
 => (\E s2':States[crowds]
       (   enabled(s1',
                   pass(s1'.mesIsAt,
                        s1.mesIsFrom))
        /\ enabled(effect(s1',
                          pass(s1'.mesIsAt,
                               s1.mesIsFrom)),
                   pass(s1.mesIsFrom, s1.mesIsAt))
        /\ effect(effect(
                  effect(s1', pass(s1'.mesIsAt,
                                   s1.mesIsFrom)),
                               pass(s1.mesIsFrom,
                                    s1.mesIsAt)), a)
            = s2'
        /\ as(s2, s2')))
```

where

- `reachable(s)` is true iff state `s` is reachable from an initial state;
- `anonym(a)` is true iff `a` is an actor action;
- `internal(a)` is true iff `a` is an internal action; and
- `output(a)` is true iff `a` is an output action.

Finally, we prove the step correspondence for actor action `start(i)`. It suffices to show

```
% --- step correspondence condition
% --- for actor action start(i)
(reachable(s1)
 /\ reachable(s1')
 /\ as(s1, s1')
 /\ enabled(s1, a)
 /\ effect(s1, a) = s2
 /\ a = start(i))
 => (\A i':ID (\E s':States[crowds]
    (\E i'':ID (\E s2':States[crowds]
        (   enabled(s1', start(i'))
         /\ effect(s1', start(i')) = s'
         /\ enabled(s', pass(i', i''))
         /\ effect(s', pass(i', i'')) = s2'
         /\ as(s2, s2'))))))
```

and this is to prove condition 2-a in Definition 3.

All the conditions in this section can be proved with the Larch theorem prover. Consequently, from Theorem 1, we obtain the following result.

Theorem 2: `crowds` is trace anonymous. □

V. FORMALIZING 3-MODE CROWDS

Kono et al. introduced an extension [5][6] of Crowds that guarantees recipient's anonymity as well as sender's anonymity. In Crowds, an agent can either:

1) forward a request to another agent; or
2) establish a connection to a website.

We call the former action *mode 1*, and the latter is called *mode 2*. In the extended version, a Crowds agent has another mode, called *mode 3*, where an agent (say, `i`) can change the destination of a request temporarily; the new destination is `i`. By this change, the proper destination is hidden.

```
automaton crowds3mode
  signature
    output   start(i:ID, j:ID)
    internal pass(i:ID, j:ID)
    internal loop(i:ID, j:ID)
    internal out(i:ID)
    output   reveal(i:ID, j:ID)

  states
    pc:        PC := init,
    mesIsAt:   ID,
    mesIsFrom: ID,
    mesIsTo:   ID,
    corrp:     Array[ID, Bool],
    lst:       Array[ID, List[ID]]
                  := constant(empty)

  transitions
    output start(i, j)
      pre pc = init
      eff pc := shuffle;
          mesIsAt := i;
          mesIsFrom := i;
          mesIsTo := j

    internal pass(i, j)
      pre pc = shuffle /\ i = mesIsAt
      eff mesIsFrom := i;
          mesIsAt := j

    internal loop(i, j)
      pre    pc = shuffle
          /\ i = mesIsAt
          /\ lst[i] = empty
      eff lst[i] := mesIsTo -| empty;
          mesIsTo := i;
          mesIsFrom := i;
          mesIsAt := j

    output reveal(i, j)
      pre    pc = shuffle
          /\ i = mesIsFrom
          /\ j = mesIsAt
          /\ corrp[j]
      eff do nothing

    internal out(i)
      pre    pc = shuffle
          /\ i = mesIsAt
          /\ i = mesIsTo
      eff if lst[i] = empty then
            pc := terminate
          else
            mesIsTo := head(lst[i]);
            lst[i] := empty
          fi
```

Figure 4. Formalization of Crowds with 3 modes

I/O-automaton `crowds3mode` in Fig. 4, which is a modified version of `crowds`, formalizes this extension. For `crowds3mode`, we introduced new variables:

- `mesIsTo`: ID of the destination of a request, and
- `lst`: list of an ID.

Variable `lst` is to store a destination of request and it is used when a Crowds agent changes the destination. For mode 3, automaton `crowds3mode` has action `loop(i, j)`, and

 ISBN: 978-1-61208-204-2

actions `start` and `out` are modified.

Verifying the anonymity of `crowds3mode` with a theorem prover is an interesting future work.

VI. Discussions

This section discusses the strength of an adversary and a probabilistic aspect of anonymity.

A. Introducing too strong adversaries cannot establish anonymity

In `crowds`, transition $s_1 \xrightarrow{\texttt{start(i)}} s_2$ by initiator `i` can be simulated by an initiator `j`'s transition sequence

$$s_1 \xrightarrow{\texttt{start(j)}} p \xrightarrow{\texttt{pass(j, i)}} q \xrightarrow{\texttt{pass(i, i)}} s_2.$$

This is essential for the anonymity of `crowds`. In order to construct the transition sequence by `j`, we need the following two conditions:

1) Action `pass` is internal;
2) We can construct a transition sequence that does not contain action `reveal`.

The first condition guarantees that a communication packet is invisible to an observer. We can easily see that system `crowds` may not be anonymous if this requirement is not satisfied; that is, if the occurrences of packets are visible to an observer, then the Crowds system is not anonymous. The second condition is with regard to the timing of attacker's execution. In this paper's example, an agent and its spy process run concurrently, and the spy process may miss to read the agent's memory. If we employ a stronger attacker such that the attacker can execute `reveal(j, j)` immediately after the occurrence of `start(j)`, then an observer knows the identity of the initiator agent.

If an attacker is too strong, we cannot establish the anonymity of a security protocol. This study employed an attacker that was modeled with action `reveal`, and the anonymity of `crowds` was confirmed with a theorem-proving tool.

B. Probabilistic anonymity

This study analyzed Crowds in a nondeterministic setting, since we employed a nondeterministic version of I/O-automaton and a theorem proving tool. However, it is important to deal with probabilities, and Crowds-based protocols are actually analyzed in a probabilistic setting [5][6][8][10]; the original version of Crowds in [8] has a probabilistic anonymity called "probable innocence".

A probabilistic version of anonymous simulation technique is introduced in [3], and probable innocence is proved with this technique for the original version of Crowds. This proof is by induction on the length of execution sequences, and the proof is done by hand; that is, it is not a computer-assisted proof. It is an interesting future work to provide a computer-assisted proof for probable innocence in a probabilistic setting.

VII. Conclusion

This paper presented a computer-assisted anonymity proof of Crowds. Specifically, to enable us to prove the anonymity, we described Crowds with an I/O-automaton, and verified the existence of an anonymous simulation. In this verification, a theorem proving tool based on first-order predicate logic was employed.

This paper also formalized an extended version of Crowds with an I/O-automaton. The extended version `crowds3mode` guarantees the anonymity with regard to the proper recipient. As future work, we are planning to verify the anonymity of `crowds3mode` with a theorem proving tool.

Acknowledgment

This study is supported by the Grant-in-Aid for Young Scientists (B), No.23700024, of the Ministry of Education, Culture, Sports, Science and Technology, Japan.

References

[1] A. Bogdanov, Formal verification of simulations between I/O-automata, Master's thesis, MIT (2000).

[2] S. J. Garland, J. V. Guttag, J. J. Horning: An overview of Larch, LNCS 693, pp. 329–348. Springer (1993).

[3] I. Hasuo, Y. Kawabe, H. Sakurada, Probabilistic anomymity via coalgebraic simulations, Theoretical Computer Science, Vol. 411, No. 22-24, pp. 2239-2259 (2010).

[4] Y. Kawabe, K. Mano, H. Sakurada, Y. Tsukada: Theorem-proving anonymity of infinite-state systems, Information Processing Letters, vol. 101, no. 1, pp. 46–51 (2007).

[5] K. Kono, Y. Ito, N. Babaguchi: Anonymous communication system using probabilistic choice of actions and multiple loopbacks, Proc. Information Assurance and Security (IAS), pp. 210-215 (2010).

[6] K. Kono, Y. Ito, N. Babaguchi: Anonymous communication system based on multiple loopbacks, Journal of Information Assurance and Security, vol. 6, no. 2, pp. 124-131 (2011).

[7] N. A. Lynch: Distributed algorithms, Morgan Kaufmann Publishers (1996).

[8] M. K. Reiter, A. D. Rubin: Crowds: anonymity for Web transactions, ACM Trans. on Information and System Security, vol. 1, no.1, pp. 66-92 (1998).

[9] S. Schneider, A. Sidiropoulos: CSP and anonymity, Proc. ESORICS '96, LNCS 1146, pp. 198–218, Springer (1996).

[10] V. Shmatikov: Probabilistic model checking of an anonymity system, Journal of Computer Security, vol. 12, no. 3/4, pp. 355-377 (2004).

 ISBN: 978-1-61208-204-2