INTERNET 2013

The Fifth International Conference on Evolving Internet

ISBN: 978-1-61208-285-1

July 21 - 26, 2013

Nice, France

INTERNET 2013 Editors

Dirceu Cavendish, Kyushu Institute of Technology, Japan

Abdulrahman Yarali, Murray State University

INTERNET 2013

Foreword

The Fifth International Conference on Evolving Internet (INTERNET 2013), held between July 21 and July 26, 2013 in Nice, France, dealt with challenges raised by the 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.

We take here the opportunity to warmly thank all the members of the INTERNET 2013 Technical Program Committee, as well as the numerous reviewers. The creation of such a broad and high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and efforts to contribute to INTERNET 2013. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

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

We hope that INTERNET 2013 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in the field of the evolving Internet.

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

INTERNET 2013 Chairs:

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 2013

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 2013 Technical Program Committee

Jemal Abawajy, Deakin University - Victoria, Australia
Onur Alparslan, Osaka University, Japan
Mercedes Amor, University of Malaga, Spain
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
Bruno Bogaz Zarpelão, State University of Londrina (UEL), Brazil
Eugen Borcoci, University "Politehnica" Bucharest, Romania
Christian Callegari, University of Pisa, Italy
Maya Carrillo Ruiz, Benemérita Universidad Autónoma de Puebla (BUAP), Mexico
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

Zhenglu Yang, The University of Tokyo, Japan
Habib Zaidi, Geneva University Hospital, Switzerland
Zhao Zhang, Iowa State University, USA
Cliff C. Zou, University of Central Florida - Orlando, USA

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

Direct Routing for Mobile Multicasting in Distributed Mobility Management Domain

Yongwon Kim, Truong-Xuan Do, Younghan Kim
School of Electronic Engineering, Soongsil University
Seoul, Korea
{crimson_88, xuan}@dcn.ssu.ac.kr, younghak@ssu.ac.kr

***Abstract*— Distributed mobility management is the newly emerging research trend replacing the current centralized ones. So far, no complete solution has been found for integrating IP multicast into the DMM domain. In one recent research, some use cases for multicast support in the DMM environment showed some problems such as traffic duplication and non-optimal routing. In this paper, we propose a new scheme to support the multicast listener in the DMM domain, which overcomes the above mentioned problems. Our scheme uses a direct routing concept that makes use of the current multicast infrastructure. Each access router in our scheme has both mobility management and MLD proxy functions. Numerical analysis shows that our proposal improves the other schemes in terms of packet loss rate.**

Keywords-Mobile Multicast; Multicast Listener Support; Distributed Mobility Management; multimedia; handover.

I. INTRODUCTION

Current centralized mobility management schemes suffer major issues such as single point of failure and sub-optimal routing. To solve these issues, several Distributed Mobility Management (DMM) approaches are discussed in [1]. The popularity of live multimedia services makes IP multicast [o] a very important technique in reducing redundant traffic in the Internet network. The integration of IP multicast and mobility management brings new user experiences for delay-sensitive applications and optimizes network bandwidth. A base deployment for supporting mobile multicast listener in a PMIPv6 domain is standardized [2]. Additionally, some use cases for supporting multicast in DMM presented issues, such as duplicated traffic and non-optimal routing [3].

In our previous work [4], we discussed the concept of direct routing which utilizes the existing multicast infrastructure and separates multicast function from Local Mobility Anchor (LMA). This concept helps us avoid problems, such as duplicated traffic and tunnel convergence when combining multicast with mobility management. However, our work did not show the details of protocol operation. It only supported multicast in the centralized domain.

In this paper, we apply this concept into a new environment, i.e., DMM environment. In our scheme, each access router has functions of mobility management and MLD proxy. Moreover, the central database is extended to store multicast context information with mobility session information. By numerical analysis, our proposal's packet loss rate will be improved over the other schemes [2] [3].

The paper is organized as follows: Section II presents our scheme for multicast support in the DMM domain. Section III analyzes our scheme performance. Section IV shows a result of numerical analysis. The paper ends with conclusion and future researches.

II. MULTICAST LISTENER SUPPORT IN DISTRIBUTED MOBILITY MANAGEMENT DOMAIN

Figure 1 shows network architecture for multicast support in the DMM domain. Both mobility management functions of LMA (e.g., prefix allocation, location management) and Mobile Access Gateways (location update) are embedded in each distributed access router (DAR). Additionally, these DARs have MLD proxy function and are connected to the multicast infrastructure.

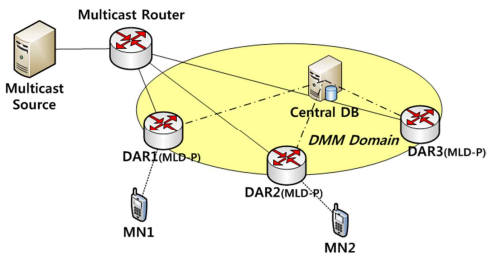


Figure 1. Architecture for multicast support in the DMM domain

Our scheme also introduces a new extension for the central database (CDB). Thus, the CDB will contain the multicast context information (e.g., multicast source, group address) beside the mobility session information of MN. The content of CDB is shown in Table I.

TABLE I. BINGDIND TABLE IN CDB

MN-ID	Prefix	Anchor	MC?	S	G
MN1	MN1-HNP1	pDAR	No	-	-
MN2	MN2-HNP1 MN2-HNP2	pDAR nDAR	Yes	S1	G1

Figure 2 shows the handover procedure of the MN. In this case, we consider that the MLD proxy function is installed in each DAR. When the MN attaches to the previous DAR (pDAR), it will send a MLD report to the pDAR to join the multicast channel.

 ISBN: 978-1-61208-285-1

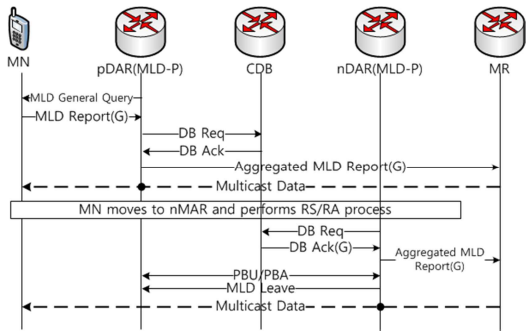


Figure 2. Initiated Attach and Handover Procedure

This multicast context information of the MN will be registered in the central database through the DB Req/DB Ack process. Then, the pDAR sends the aggregated MLD report to join the multicast tree, so the multicast data will be routed to the pDAR, finally to the MN. When the MN performs handover to new DAR (nDAR), the MN performs an attachment procedure using RS/RA messages. The nDAR immediately queries to the CDB to get the mobility session information of the MN (previous anchor points) and the multicast context information of the MN (content source and multicast group address). Then, the MN performs a location update procedure to the pDAR via PBU/PBA messages and sends an aggregated MLD report to the multicast tree. From that point on, the multicast data can flow from the multicast tree to nDAR, finally to the MN.

III. PERFORMANCE ANALYSIS

In this section, our scheme and three others: 1) Base deployment for multicast listener support in PMIPv6 domain scheme; 2) Tunnel-Based Reactive Scheme; and 3) Tunnel-Based Proactive Scheme will be evaluated and compared in terms of packet loss rate. The analytical model is referred from [3], [5], [6].

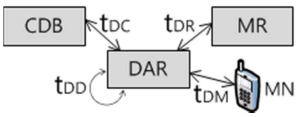


Figure 3. Reference Topology

Figure 3 shows the network topology used for performance evaluation. D_{scheme} is defined as the total latency for completing all signaling procedures plus the time for sending the first multicast data packet to the MN. In our analysis, we only take into account the signaling procedures used for receiving the multicast data. The formula for calculating each component delay $t_{entities}$ is referred from [5].

- *Base deployment for multicast listener support in PMIPv6 domain (BDMP)*

$$D_{BDMP} = 4t_{DC} + 3t_{DM} \quad (1)$$

- *Tunnel-Based Reactive Scheme (TBRS) [3]*

$$D_{TBRS} = 4t_{DC} + 2t_{DD} + 3t_{DM} \quad (2)$$

- *Tunnel-Based Proactive Scheme (TBPS) [3]*

$$D_{TBPS} = 4t_{DC} + 2t_{DD} + t_{DM} \quad (3)$$

- *Our scheme without tunnel when deploying MLD-Proxy (MPWT)*

$$D_{MPWT} = 2t_{DC} + 2t_{DR} + t_{DM} \quad (4)$$

We assume the coverage area of each DAR has the diameter *l,* the velocity of the MN is *v,* and the density of the MN in one coverage area α. The subnet crossing rate is given as follows:

$$r_c = \alpha v l / \pi \quad (5)$$

We suppose the packet arrival rate follows the Poisson distribution and has the average value λ. Thus, the packet loss rate is calculated as:

$$L_{scheme} = \lambda \times r_c \times D_{Scheme} \quad (6)$$

IV. NUMERICAL RESULTS

The numerical values for performance analysis are referred from [5] [6]. Figure 4 shows the multicast packet loss rate variation with the mobility rate of the MN. The multicast packet loss rate of our scheme increases at a much lower rate than two other tunnel-based schemes. Additionally, our scheme has a bit lower packet loss rate than the BDMP. This low packet loss rate is resulted from the low handover latency of our scheme. This low latency of our scheme is due to optimized signaling operation (one CDB query/response for getting both the mobility session and the multicast context information). By separating multicast and unicast routing, we can receive the multicast data without waiting for signaling procedures of unicast traffic to finish.

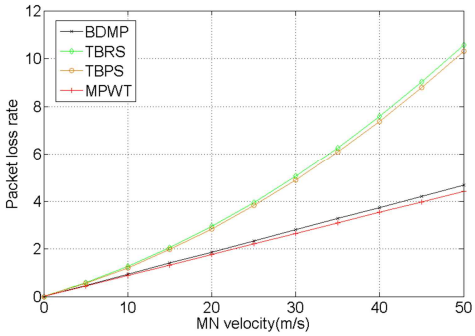


Figure 4. Packet Loss rate

V. CONCLUSION AND FUTURE WORK

In this paper, we proposed a scheme to support multicast listener in the DMM domain. Our scheme uses a direct routing concept which utilizes the existing multicast infrastructure and separates multicast function from LMA, so existing problems, such as traffic duplication and non-

 ISBN: 978-1-61208-285-1

optimal routing, have been solved. By numerical analysis, our scheme achieves the lowest packet loss rate, when the handoff rate increases. Therefore, our scheme will provide a better user of experience. Our future work will include the simulation of our scheme to get the exact packet loss rate. In addition, we will extend to support multicast sender in DMM domain, in other words, the mobility of multicast content source.

ACKNOWLEDGMENT

This research was supported by the MSIP(Ministry of Science, ICT & Future Planning), Korea, under the Convergence-ITRC(Convergence Information Technology Research Center) support program (NIPA-2013-H0401-13-1004) supervised by the NIPA

REFERENCES

[1] IETF DMM WG, http://datatracker.ietf.org/wg/dmm/ [retrieved: April, 2013].

[2] T. Schmidt, M. Waehlisch, and S. Krishnan, "Base Deployment for Multicast Listener Support in PMIPv6 Domains," IETF RFC 6224, April 2011.

[3] S. Figueiredo, S. Jeon, and R. L. Aguiar, "Use-cases Analysis for Multicast Listener Support in Network-based Distributed Mobility Management," Proc. IEEE Symp. Personal Indoor and Mobile Radio Communications (PIMRC 2012), Sep. 2012, pp. 1478-1483, doi: 10.1109/PIMRC.2012.6362581.

[4] S. Jeon, N. Kang, and Y. Kim, "Mobility Management Based on Proxy Mobile IPv6 for Multicasting Services in Home Networks," IEEE Transactions on Consumer Electronics (TCE), vol. 55, no. 3, Aug. 2009, pp. 1227-1232.

[5] C. Makaya and S. Pierre, "An Analytical Framework for Performance Evaluation of IPv6 based mobility management protocols," IEEE Transaction on Wireless Communication (TWC), Vol. 7, No. 3, Mar. 2008, pp. 972-983.

[6] S. Jeon, N. Kang, Y. Kim, and W. Yoon, "Enhanced PMIPv6 Route Optimization Handover," IEICE Transactions on Communications vol. E91-B, no.11, Nov. 2008, pp. 3715-3718.

 ISBN: 978-1-61208-285-1

An Efficient Query Scheme for Semantic Web on Mobile P2P Network

Jun-Li Kuo, Chen-Hua Shih and Yaw-Chung Chen
Department of Computer Science
National Chiao Tung University
Hsinchu, Taiwan
estar.cs95g@nctu.edu.tw, shihch@nctu.edu.tw, ycchen@cs.nctu.edu.tw

***Abstract*—Service orientation and decentralization are characteristics in both semantic web and peer-to-peer (P2P) networks. In P2P networks, we can take the advantages of scalability and flexibility to improve semantic web services with lower cost. With IPv6, the P2P network can be extended to mobile network to support anycast delivery. This article proposes a novel semantic web service (SWS) integrated with mobile P2P network, called Mobile P2P Semantic Web, which combines extensibility of SWS, scalability of P2P, mobility of mobile network to enhance interactivity and interoperability of query service for semantic web. The simulation results demonstrated that our proposed scheme shortens the query response delay and reduces the number of duplications of query significantly.**

Index Terms—Semantic web; peer-to-peer; mobile network; IPv6; anycast.

I. INTRODUCTION

Semantic web has been proposed to provide comprehensive and triple-play web data. It enables users to create and share web content that features awareness and definition for computers or devices. Semantic Web Service (SWS) is gradually evolving into a worldwide network of semantic and statistical information, which can be accessed by users via hyperlink operations or database management [1]. SWS maintains the associations of meaningful content, which can be located and retrieved from any site of the Internet. SWS is also integrated with Service-Oriented Architectures (SOA) to create the web systems with high interactivity and interoperability. The meaningful content with high interoperability can be available via informative query that includes the queries of reasoning semantics, sentence parser, and string prefix.

SWS should be constructed with the decentralized scheme due to the high dynamics of information explosion and the high scalability of Internet development. Peer-to-peer (P2P) is a solution to cope with the characteristics of SWS. P2P systems can minimize server load and reduce bandwidth requirement of the servers by using forwarding query without flooding. A P2P system not only features the service-oriented cooperation but also utilizes the decentralized overlay. The integration of SWS and P2P provides the diversified sharing and querying solutions [2]. A P2P overlay can support a SWS framework, which allows data to be shared and reused across multiple applications.

With the development of Web 2.0 [27] and evolution of Web 3.0 [28], the novel vision of SWS has been created in the mobile network. An online semantic web not only needs the real-time management of rich semantic information about all digital resources (i.e., machine readability or content awareness), but also extends the management of dynamic location information (i.e., overlay locality and proximity) [3]. Both SWS and P2P have been developed in wired networks, so there are several challenges in the mobility extension.

In summary, SWS provides high flexibility, P2P offers high scalability, and mobile network supports high mobility. The mobile P2P environment can extend the applications of SWS for high accessibility and availability surely. Although P2P and mobile issues have been addressed in SWS individually, the combination of mobile network and P2P cooperative network has never been applied in SWS so far. The successful semantic query across mobile P2P network must bring rich and useful information and the importance of extended SWS, but the issue has never been discussed yet.

In this paper, we propose an extended query for semantic web and it can be applied to P2P and wireless mobile networks. The proposed Mobile P2P Semantic Web (MP2PSW) uses an informative query across IPv6-based network[22] to retrieve data from P2P system. The informative query is delivered via anycast forwarding. Due to the advantages of anycast and P2P, it can be shown that MP2PSW significantly reduces the traffic overhead and the response delay of query in the semantic web service.

The rest of this paper is organized as follows. Section II addresses the related works. In Section III, we discuss the proposed scheme. In Section IV, the simulation experiment and results are illustrated. Section V concludes the work.

II. RELATED WORKS

Since MP2PSW involves P2P overlay, mobile network, and anycast scheme, we discuss the terms one by one and survey the existed works.

 ISBN: 978-1-61208-285-1

A. P2P

P2P [23] network is a popular and interesting development, it is widely used for file sharing, voice communications and video streaming nowadays. Distributed Hash Table (DHT) is commonly used in P2P network to hasten the query process and heighten the content availability. For example, Chord [4] uses DHT as its core algorithm that has been used successfully in P2P networks; such method has been proven to be an efficient overlay for a variety of scalable and robust distributed applications.

Chord uses a ring-based DHT to index files and peers. Every peer has a unique identification with n bits, so there are 2^n peers on Chord overlay with scalability. Every file can be identified and mapped via the hash key, which is derived from DHT to bind some peer. Every peer only maintains a finger table to forward any message or data to its successor, so the one-dimensional lookup in Chord is hop-by-hop and its complexity is O(n). Other popular P2P systems can be found in [19 – 21].

B. Mobile Network

Wireless network provides Internet accessibility for mobile devices. Nowadays, popular WiFi [29], WiMax [30], 3G [31] and LTE [32] can support network access with or without infrastructure. Both WiFi and WiMax have access-point mode with infrastructure and ad-hoc mode without infrastructure, and the latter mode is generally known as Mobile Ad hoc NETwork (MANET). The performance of ad hoc routing protocols is similar with P2P forwarding process; so, the integration of MANET and P2P is efficient for mobile SWS [5].

There is a large amount of personal information and potential knowledge, including geographical features, topological information, and social relationships, in WiFi and MANET. Through informative query, the personal and potential knowledge is searchable via SWS, and knowledge data such as files and streams is available via P2P content sharing.

C. Anycast

Anycast is an addressing/routing mechanism based on IP network [6]. In essence, data or packets can be delivered through any network via one-to-one unicast, one-to-all broadcast, or one-to-many multicast. In unicast, a sender clearly queries or sends data to only one receiver; in broadcast, a sender floods data to all nodes, and some nodes drop such data that is not interested by the node; in multicast, a sender queries or sends data to multiple receivers, which forms a multicast group in advance. However, anycast is a new concept; it adopts the one-to-one-of-many delivery. A sender queries or sends data to an unspecified receiver, which forwards such data to other receivers in the anycast group.

Anycast originates from IPv6 [22] for service-orientated applications to reduce the network traffic and shorten the response delay. An anycast address can be assigned to an anycast group, in which the receivers with the same anycast address should receive the same packets. For example, MP2PSW sends an informative query through anycast to a group providing service-oriented application in semantic web, such that the nodes in the group should receive the same query.

Although the source should send a query to the nearest destination among an anycast group of multiple receivers, the nearest destination is not consistent with different routing principles and arbitrary routing paths. Therefore, anycast is suitable for connectionless protocols, generally built on UDP [24].

D. Query Service

The query service is a function of SWS; it provides a solution to the search engine or social network. The combination of Web Service Description Language (WSDL) [25] and Web Ontology Language (OWL) [26] provides a standard to develop the query service. The query can be developed from the string manipulation to the informative query with reasoning ontology. The informative query can integrate with SOA to improve interactivity and interoperability, Figure 1 illustrates the general module of informative query and the components of semantic web query service.

Enhanced-Chord Web Service [7] also uses P2P overlay with Chord to efficiently discover web services in a fully decentralized network. Chord is modified to a two-level hierarchy overlay, which is built by single super ring and multiple sub rings. Enhanced-Chord Web Service uses WSDL and OWL in semantic web, and it uses the super-peer solution in P2P overlay. A convergence of semantic web also uses the super-peer solution to achieve the P2P groupware [8], and the hierarchical overlay uses the computational model and distributed replication model to manage P2P framework. P2P Model for Semantic Web Service (PM4SWS) [9] is based on P2P network to discover SWS for the high scalability and avoid single point of failure. PM4SWS clearly defines the maintenance of P2P network and the process of WSDL and OWL. Semantic Overlay Network (SON) [10] presents a distributed and semantic matching-based approach for SWS publication and discovery by leveraging P2P technology. SON not only sorts the relevant concepts for service matching but also publishes ontology mapping on P2P network.

Context-Aware Semantic-Based Access Control (CASBAC) [11] follows OWL to build a model for mobile web services. Semantic COntext-aware Ubiquitous scouT (SCOUT) [12] is a mobile application framework, which supports online semantic sources to improve personalization. It not only provides the mobile query but also manages the detection and location of user profile. Semantic Mobile Service Discovery (SeMoSD) [13] is a mechanism to discover mobile web services. It can query, reason, and make result for the accurate search. Semantic Web mobile Learning Object Repository (SWmLOR) [14] develops a

 ISBN: 978-1-61208-285-1

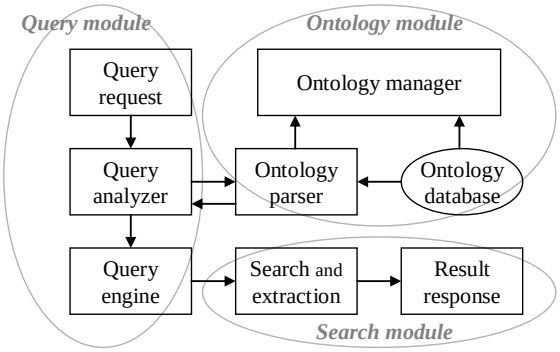
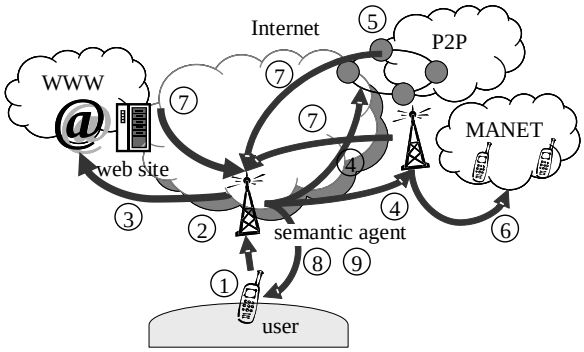
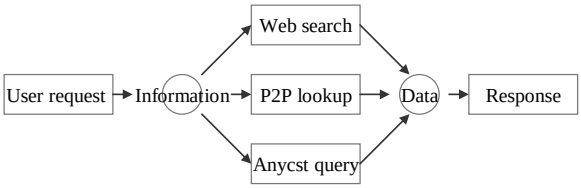


Figure 1. The components of semantic web query service.



(a) The network architecture and query process.



(b) Informative query

Figure 2. The system overview and query process.

mobile e-learning repository via semantic web technology and ontology.

Although P2P issues [7 – 10] or mobility issues [11 – 14] have been taken account in SWS, we must emphasize again that, to our best knowledge, there is no functional combination of SWS with P2P and mobile networks so far; MP2PSW is the first trial to integrate SWS with P2P and mobile networks.

III. Proposed Scheme

The proposed MP2PSW focuses on informative query rather than semantic design or analysis. The proposed design focuses on network performance rather than web or database design. We focus on the promotion of P2P scheme for SWS, and the anycast delivery is adopted for mobility improvement.

A. System Overview

A user may use a wired personal computer or a wireless handheld device to request or access the SWS by initiating an informative query, which should be forwarded to a semantic agent through the Internet. The agent handles the basic ontology extraction, data mining, or reasoning management to parse the query to the semantic web site, or a P2P overlay which can be formed either on a social network or on a mobile network. The query arrives at the semantic web site or P2P overlay and the returned result contains the information that is very likely a list of hyperlinks for real data. If the query is matched, the real data will be downloaded or responded via P2P file sharing or live streaming. The query process is summarized and illustrated in Figure 2 (a).

1. A user sends a query for a file.
2. The query is parsed by a semantic agent.
3. The query is sent to web site, which may be a search engine.
4. The query is sent to P2P network and mobile network simultaneously.
5. The query is forwarded via DHT lookup in P2P network.
6. The query is forwarded via anycast in mobile network.
7. The semantic agent receives the results of query from multiple networks as Figure 2 (b) illustrated.
8. The semantic agent ranks the results and sends them back to the user.
9. The result indicates a document or multimedia content, and the user can download it via P2P network.

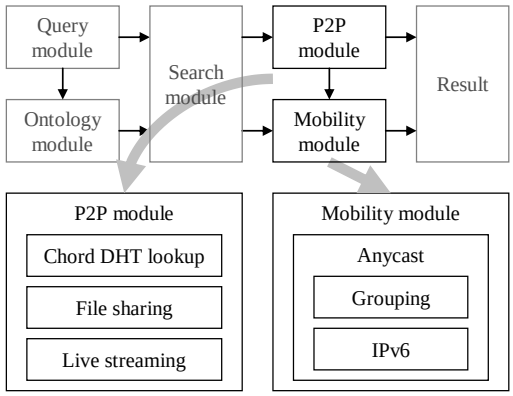


Figure 3. The proposed system modules.

The system overview is illustrated in Figure 3. Compared to Figure 1, besides the general query service, MP2PSW proposes two special modules, P2P module and mobility module.

In P2P module, DHT locates the peers and indexes the files. An informative query is looked up via Chord protocol. If a lookup is matched with returned content, which then can be available for file sharing or live streaming. For example, a movie on PPLive [15, 19] is responded, such that it can be delivered via live streaming on demand through P2P network.

```
while an informative query is received do
    let q = informative query;
    let req = getRequest(q);
    let sem[ ] = parseSemantics(req);
    while sem[ ] ≠ Φ do
        sends sem as a data query;
        delete sem;
    end while
end while
while a data query is received do
    let q = data query;
    let meta = extractData(q);
    sends meta as a web query;
    sends meta as a P2P query;
end while
while a web query is received do
    let result[ ] = searchResult(web query);
    let link[ ] = getHyperlink(result);
    sends link;
end while
while a link is received do
    let response = shareP2P(link);
    sends response;
end while
```

```
while a P2P query is received do
    let key = hashChord(P2P query);
    let peer = forwardChord(key);
    let result[ ] = Φ;
    while peer ≠ null do
        if peer is a mobile node then
          sends such P2P query as a mobility
          query to peer;
        else
          result[ ] = result[ ] + searchResult(peer);
            peer = peer → next;
    end while
    let link[ ] = getHyperlink(result);
    sends link;
end while
while a mobility query is received do
    let peer = anycastDelivery(mobile query);
    let result[ ] = Φ;
    while peer ≠ null do
        result[ ] = result[ ] + searchResult(peer);
        peer = peer → next;
    end while
    let link[ ] = getHyperlink(result);
    sends link;
end while
```

Figure 4. The algorithm of MP2PSW.

In MP2PSW, Chord not only indexes peers, but also forwards informative query for P2P overlay (called P2P query). Therefore, Chord is modified to forward query efficiently. Every P2P network owns an individual P2P ID, which is linked to a unique ring-based DHT inherited from Chord. Every peer is identified by a peer ID, which is ranging from 0 to $2^n - 1$ like Chord, but a peer can own multiple peer IDs unlike Chord due to the consideration for multidimensional query. When a peer has higher availability and its files have higher level of ontology, its peer ID will be smaller to reduce the forward steps.

In mobility module, anycast protocol is used to deliver an informative query. The anycast address of IPv6 is defined as the ID of P2P group to integrate P2P solution, such that every mobile node is seen as a peer in WLAN or MANET. We adopt IPv6 to implement anycast delivery, because IPv6 features higher extensibility, scalability, and mobility than that in IPv4 .

Since the cooperative network is formed in WLAN or MANET, the communication between mobile nodes is similar to the communication between peers. However, anycast delivery is forwarded in IP layer, while P2P delivery is forwarded in application layer. In order to allow informative queries for mobile network, anycast address in IPv6 is set to a P2P ID. Therefore, an informative query can be translated to a P2P query and mobility query for an integration of P2P and mobile network.

B. Algorithm

In MP2PSW, SWS must handle the messages of query process, as illustrated in Figure 4. Every informative query should be parsed to generate multiple data queries via either the query module or ontology module. Such data query is translated to P2P query or mobility query, which is forwarded via Chord forwarding or anycast routing, respectively. Through P2P and mobile network, the results are responded with hyperlinks. We discuss the steps necessary to implement MP2PSW as followings:

1. The query module is implemented in the semantic agent, which supports the network socket.
2. The socket may need multiple network interfaces to support some relay nodes.
3. The relay node is bound to single or multiple P2P network or mobile network to handle query.
4. The result of query may be generic. The ontology principle let the result specific.
5. Because every mobile node need a public IP to route informative query through Internet and supports anycast query, IPv6 is required.

C. Advantages

First, MP2PSW can avoid the single-point-of-failure problem because MP2PSW is based on P2P scheme. Although the semantic agent is used in MP2PSW, it is still

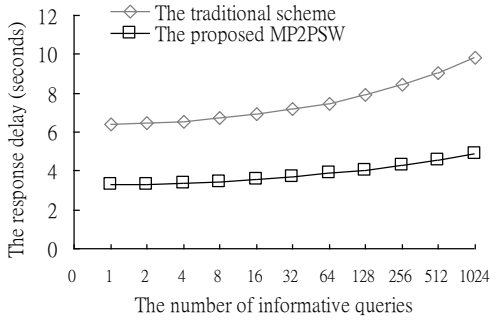


Figure 5. The response delay of informative query.

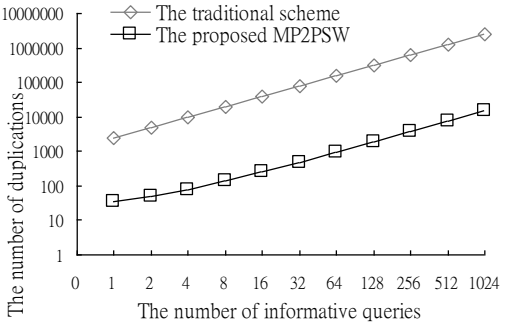


Figure 6. The duplications of informative query.

workable even if a semantic agent is failed. An information query is still forwarded to P2P and mobile network without a semantic agent, but the query results will be multifarious and the response delay will be long due to the lack of ontology parser and extraction.

Second, the combination of P2P and wireless mobile network heightens the interoperability of SWS, because such combination extends the scalability and heterogeneity of the network. The advantage of interoperability brings the rich information. In addition, P2P solution provides file streaming and video streaming services, and mobility solution provides geographic information in SWS.

Third, the network overhead can be reduced. P2P minimizes server load and anycast reduces traffic load when processing informative query. P2P solution also balances network overhead when downloading or sharing content.

IV. Performance Evaluation

We focus on the network performance of MP2PSW, which is evaluated through system simulation. We use OMNet++ [16] to construct a simulation environment as Fig. 2 illustrates. Under OMNet++, OverSim [17] is used for P2P core, i.e., Chord, and INET/ xMIPV6 [18] is used for anycast delivery. The simulation is based on IPv6, with 10000 peers given in a P2P network, in which there are 20 WLANs, with 100 mobile nodes in each WiFi. We compare MP2PSW with the traditional scheme, which adopts the server-client model. Every user as a client sends the query to the server, and waits for the response from server. The server uses the flooding query to all network nodes. The experiment repeats 20 simulations and the result represents an average.

During a given interval, a user continuously sends a large number of informative queries to the semantic agent. More queries lead to longer response delay and higher overhead. As Figure 5 illustrated, MP2PSW outperforms the traditional scheme. Based on the DHT query of Chord, the response delay is slightly long with the increasing queries. Since MP2PSW handles the variants of informative query (i.e., web query, P2P query, and mobile query) in parallel, the search process can be fastened. Via the proposed P2P module and mobility module, the modified Chord can perform query for the peers with high level of ontology, so the steps can be reduced with hop-by-hop query.

The number of duplications is used to measure the network overhead. The more the duplications are, the higher the overhead will be. As Figure 6 illustrated, MP2PSW adopts DHT-based P2P search to forward informative query in P2P network, such that the number of duplications of MP2PSW is much smaller than that of the server-client model. Although the number of duplications increases exponentially, unlike the traditional scheme, the network overhead is limited within a reasonable bound in MP2PSW. Since the anycast delivery is more efficient than the flooding delivery, the query duplications are not only reduced in wired P2P network but also minimized in wireless mobile network. However, the admission of multiple peer IDs for multidimensional query cannot alleviate the duplicated load.

V. Conclusions

In this paper, we proposed a novel scheme, which not only enables the informative query across P2P and mobile networks for SWS, but also retrieves the responded context via P2P file sharing or live streaming. The proposed MP2PSW orientates SWS to the cooperative and wireless network to obtain the potential demand and information. The proposed P2P module and mobility module parallelize the informative query via Chord and anycast protocols individually. We modified Chord and anycast to support SWS. MP2PSW not only accomplishes the pioneer and practicable design, but also considers the network performance. Therefore, MP2PSW can be demonstrated to achieve the high interoperability, scalability, and flexibility. Although MP2PSW must work in IPv6 with low popularity now, MP2PSW follows the current trend and takes advantage of P2P socialization and mobile personalization.

References

[1] V. Ermolayev, N. Keberle, S. Plaksin, O. Kononenko, and V. Terziyan, “Towards a framework for agent-enabled semantic web service composition,” International Journal of Web Services Research, vol. 1, iss. 3, July–September 2004, pp. 63-87.

[2] D. Skoutas, D. Sacharidis, V. Kantere, and T. Sellis, “Efficient semantic web service discovery in centralized and

P2P environments," ISWC '08 Proceedings of the 7th International Conference on the Semantic Web, October 2008, pp. 583-598.

[3] J. Veijalainen, S. Nikitin, and V. Tormala, "Ontology-based semantic web service platform in mobile environments," Proc. 7th International Conference on Mobile Data Management, Nara, Japan, May 2006.

[4] I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, August 2001, pp. 149-160.

[5] J. L. Kuo, C. H. Shih, C. Y. Ho, and Y. C. Chen, "A cross-layer approach for real-time multimedia streaming on wireless peer-to-peer ad hoc network," Ad Hoc Networks, vol. 11, iss. 1, January 2013, pp. 339-354.

[6] S. Weber and L. Cheng, "A survey of anycast in IPv6 networks," IEEE Communications Magazine, vol. 42, iss. 1, August 2004, pp. 127-142.

[7] A. Adala and N. Tabbane, "Discovery of semantic Web Services with an enhanced-Chord-based P2P network," International Journal of Communication Systems, vol. 23, iss. 11, November 2010, pp. 1353-1365.

[8] F. Xhafa and A. Poulovassilis, "Awareness in P2P groupware systems: a convergence of contextual computing, social media and semantic web," Proc. International Conference on Emerging Intelligent Data and Web Technologies, September 2011, pp. 14-21.

[9] M. Gharzouli and M. Boufaida. "PM4SWS: a P2P model for semantic web services discovery and composition," Journal of Advances in Information Technology, vol. 2, no. 1, February 2011, pp. 15-26.

[10] H. Si, Z. Chen, Y. Deng, and L. Yu, "Semantic web services publication and OCT-based discovery in structured P2P network," Service Oriented Computing and Applications, January 2012, DOI 10.1007/s11761-011-0097-4.

[11] H. B. Shen and Y. Cheng, "A context-aware semantic-based access control model for mobile web services," Advanced Research on Computer Science and Information Engineering, 2011, pp. 132-139.

[12] W. V. Woensel, S. Casteleyn, E. Paret, and O.D. Troyer, "Mobile querying of online semantic web data for context-aware applications," IEEE Internet Computing, vol. 15, iss. 6, November–December 2011, pp. 32-39.

[13] R. Besen and F. Siqueira, "A mechanism for semantic web services discovery in mobile environments," Proc. 10th International Conference on Networks, January 2011, pp. 329-334.

[14] R. Pathmeswaran and V. Ahmed, "SWmLOR: technologies for developing Semantic Web based mobile Learning Object Repository," The Built & Human Environment Review, vol. 2, special iss. 1, 2009.

[15] X. Hei, C. Liang, J. Liang, Y. Liu, and K. W. Ross, "A measurement study of a large-scale P2P IPTV system," IEEE Transaction on Multimedia, vol. 9, iss. 8, December 2007, pp. 1672-1687.

[16] A. Varga, "Using the OMNeT++ discrete event simulation system in education," IEEE Transactions on Education, vol. 42, iss. 4, November 1999.

[17] I. Baumgart, B. Heep, and S. Krause, "OverSim: a flexible overlay network simulation framework," Proc. IEEE Global Internet Symposium, May 2007, pp. 79-84.

[18] F. Z. Yousaf, C. Bauer, and C. Wietfeld, "An accurate and extensible mobile IPv6 (xMIPV6) simulation model for OMNeT++," Proc. International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops, March 2008, Article No. 88.

[19] "PPLive," http://www.pplive.com/ [Retrieved: April, 2013]

[20] "PPStream,"http://www.ppstream.com/[Retrieved:April, 2013]

[21] "BitTorrent,"http://www.bittorrent.com/[Retrieved:May, 2013]

[22] http://ipv6.com/articles/general/Next-Generation-Networking. Htm[Retrived: May, 2013]

[23] https://www.hpl.hp.com/techreports/2002/HPL- 2002-57R1.pdf [Retrieved: March, 2013]

[24] http://www.ietf.org/rfc/rfc768.txt [Retrieved: March, 2013]

[25] http://www.w3.org/TR/wsdl [Retrieved: March, 2013]

[26] G. Antoniou and F. van Harmelen, "Web Ontology Language: OWL," International Handbooks on Information Systems 2004, pp. 67-92.

[27] http://oreilly.com/web2/archive/what-is-web-20.html [Retrieved: May, 2013]

[28] Victoria Shannon, "A 'more revolutionary' Web," International Herald Tribune [Retrieved: May, 2013]

[29] http://www.wi-fi.org/ [Retrieved: May, 2013]

[30] http://www.wimaxforum.org/[Retrieved: May, 2013]

[31] ITU (4 July 2002), "IMT-2000 Project - ITU" [Retrieved: April, 2013]

[32] E. Dahlman, H. Ekström, A. Furuskär, J. Karlsson, M. Meyer, S. Parkvall, J. Torsner and M. Wahlqvist, "The long-term evolution of 3G," Ericsson Review, no. 02, 2005.

 ISBN: 978-1-61208-285-1

Generating Web Traffic based on User Behavioral Model

Guo-feng Zhao
Institute of Future Internet Technology
Chongqing University of Posts and Telecommunications
Chongqing, P. R. China
zhaogf@cqupt.edu.cn

Min-chang Yu,
Institute of Future Internet Technology
Chongqing University of Posts and Telecommunications
Chongqing, P. R. China
615176114@qq.com

Chuan Xu,
Institute of Future Internet Technology
Chongqing University of Posts and Telecommunications
Chongqing, P. R. China
xuchuan@cqupt.edu.cn

Hong Tang
Institute of Future Internet Technology
Chongqing University of Posts and Telecommunications
Chongqing, P. R. China
tanghong@cqupt.edu.cn

***Abstract*— Generating Web traffic is of great importance to analyse performance of new designed network, test new equipment, and verify new protocols, etc. Most existing traffic generation systems tend to simulate the overall characteristics of network traffic, while neglecting of the behavior of the individual users. However, in principle, the emerged characteristics of overall traffic originate from the aggregation of individual users' access behavior. In this paper, we propose an innovative web traffic generating method based on user browsing behavior. Our method simulates the real users' accessing behavior, and visits the real web servers. Then, we design and develop a web traffic generating system. Because our system accesses the real web, it can produce almost the real network traffic. The test results show that the traffic generated by our system has characteristics of burstiness and self-similarity, which are widely exposed characteristics in real networks; meanwhile, our system better reflects real user's web browsing behavior.**

Keywords-Traffic generation; Pareto Distribution; Markov Model;

I. INTRODUCTION

The Web traffic generating system are widely used in many aspects, such as network performance test, new network protocol test, and site security assessment, etc. The traffic generated by such systems will directly determine the accuracy of experimental test results. So, how to generate the similar traffic as the real network is of great importance.

Currently, the methods of generating Web traffic can broadly be classified into two kinds: 1) traffic playback, and 2) traffic model simulation. 1) Traffic playback uses the network tools, e.g., sniffer, to capture packets and record them in a log file, then new simulating traffic can be generated based on the log file. This method can generate real network traffic captured by network tools. However, the result is time and scope limited, and cannot reflect the changing characteristics of network traffic. 2) Based on mathematical traffic models, many tools can generate network traffic. Leland [1] analyzed the real network traffic and pointed out that it had self-similarity and burstiness, and it proved to be true in many different networks. Using this method, we can produce changing network traffic similar to real network, but the traffic cannot reflect individual users' browsing behavior, such as the law of users' jump relation among different Uniform Resource Locators (URLs), users' preferences on different pages. However, many research tasks hunt for network traffic with users' behavior revealed, to test the particular network technology, such as service migration in Service-Oriented Future Internet [2].

The main work of this paper is as follows. 1) We propose a web traffic generating method based on web users' access behavior model. According to the method, first, we choose the first webpage of a real Web for a web user to visit; next, we calculate a page viewing time for the user; and then, we forecast the next page to access. 2) We present the design of the web traffic generating system, which consists of management module, preprocessing module and traffic generating module. 3) We develop a prototype using Python [3] and test the system. Results show that traffic generated by our system has similar characteristics as the real web traffic, such as self-similarity and burstiness characteristics; however, it takes users' behavior into consideration.

The remaining of the paper is organized as follows. After discussing related work in Section II, we describe our traffic generating method based on user behavior in Section III. We present the details of system design in Section IV and show test results in Section V. In Section VI, we conclude and outline future work.

II. RELATED WORK

The experimental verification of network testbed is critical for Future Internet research. Traffic generator being a key part of the network testbed is widely used in the evaluation of website and network performance. With the development of Future Internet research, traffic generator based on user behavior characteristic validates and evaluates the performance of the key technologies more effectively.

A number of successful application-specific traffic generators have been developed. Tcpreplay is a typical flow playback tool, which can replay directly packets captured by a 3rd part network data catching software such as Tcpdump [4]. Tcpreplay also supports replay packets

 ISBN: 978-1-61208-285-1

with appropriate modifications in the headers of link layer, network layer and transport layer, but such tools only mechanically replay the captured data packets at a regular rate. SPECweb, a tool of evaluating the performance of web servers, generate network traffic by sending HTTP Get requests to web server [5]. User can send requests separated by a constant interval. As a result of neglecting the real web user's behavior, traffic flow generated by SPECweb is deviant from the real network.

Alessio Botta et al. present a tool for the generation of realistic network workload that can be used for the study of emerging networking scenarios. However, it also did not take the user behavior into consideration [6].

Above analyses show that current traffic generators are developed based on part of traffic characteristics. However, they did not consider individual user browsing behavior, such as the law of users' jump relation between different URLs, users' preferences on different pages.

III. TRAFFIC GENERATING METHOD BASED ON USER BEHAVIORAL MODEL

Our web traffic generator can simulate normal access behavior of web users, and generate accurate and real network traffic. The procedure on how it works can be divided into the following steps:

Step 1: choose the first page of a real Web to visit. For example, when web users first browse a comprehensive portal website, they will choose the first page to visit, whatever it belongs to news section, sports section, or entertainment section, etc.

Step 2: spend a period of time on reading the content of the webpage. It is an interval between the accesses of two consecutive pages (viewing time).

Step 3: choose a new page for the next visit. Briefly, we extract and log the hyperlink URLs embedded in pages, and choose the next page URL based on Markov model.

In a web user's session, the Step 2 and Step 3 are running repeatedly until it logs out. In short, we need determine the first page, viewing time and the next page.

A. How to choose the first page

For a given real website, the web pages can be sorted to different ranks based on their popularity. All the ranks can be defined as follows: w_1, $w_2 \ldots$ w_n. The bigger n is, the more popular the web page is. We use random variable W to represent a web page, and w_i represent the probability of the web page accessed. It is well-known that the page popularity has the law of the Zipf-Mandelbrot distribution as in Equation (1) [7].

$$P(W = i) = \frac{\Omega}{(i+q)^{\alpha}} \tag{1}$$

We denote α ($\alpha > 0$) as the skewness coefficient, which determines the skewness of the Zipf-Mandelbrot distribution, and q ($q \geq 0$) as the plateau coefficient. The plateau coefficient means the most popular web page is more likely. When $\alpha = 1$, the Zipf-Mandelbrot distribution becomes the Zipf distribution. When q=0, the distribution becomes Zipf-like distribution.

$$\sum_{i=1}^{N} P(W = i) = 1 \tag{2}$$

$$\Omega = \sum_{i=1}^{N} \left(\frac{1}{(i+q)^{\alpha}} \right)^{-1} \tag{3}$$

According to [7], Equation (3) can be inferred from Equations (1) and (2). We denote P(W=i) as the probability of accessing page i, and P_{max}=Max{P(W=1), P(W=2), …, P(W=n)} as the most popular web page, which means this page is more likely to become first page selected by web users. In other words, the popularity of web pages shows high degree of asymmetry. Most of the requests access a few hot pages.

B. How to calculate the viewing time

Viewing time refers to the interval bewtween two consecutive Web page requests and shows how long a user spends on a given Web page. We use the traditional ON/OFF model to describe the users' viewing behavior, as shown in Figure 1.

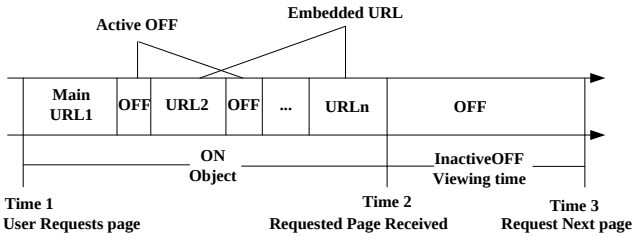


Figure 1. ON/OFF model of user browsing behavior

Figure 1 illustrates the behavior of web users. The horizontal axis represents time. On the first time slot, the client sends HTTP Get to URL1. The response message contains n embedded URL. Then, the client sends HTTP Get every OFF time, until the web browser receives all the data on the second time pot. Subsequently, the inactive OFF time means viewing time. On the third time pot, the client sends HTTP Get to request for next page.

Since the active OFF time is very short (less than 1 second) in actual development, we can ignore it relative to the web user's viewing time. According to all kinds of web browsers, we send HTTP Get requests for embedded URLs as soon as possible. Therefore, the active OFF time is influenced by the performance of client machine and network latency, and the inactive OFF time follows Pareto Distribution [8].

We denote W as the page viewing time and k=Min{wi}($1 \leqslant i \leqslant n$) as the minimum viewing time and

then the probability density function of the viewing time distribution is denoted as in Equation (4) [7].

$$P(W = w_i) = \alpha k^{\alpha} w_i^{-(\alpha+1)} \quad (4)$$

From the Equation (4), we can get cumulative distribution function, as in Equation (5).

$$F(w_i) = 1 - (k / w_i)^{\alpha} \quad (5)$$

We can get the random variable α following Pareto Distribution with the inverse function, as in Equation (6).

$$w_i = k / U^{1/\alpha} \quad (6)$$

The random parameter U follows Uniform Distribution within the range of (0, 1]. We figure out the viewing time of different Web requests, and it follows Pareto Distribution. Therefore, we can use Kolmogorov-Smirnov (KS) to compute parameter α [9].

Let X_1, X_2, …, X_n be independent identically distributed observation samples, Kolmogorov-Smirnov(KS) test of this distribution is based on D_n which is the absolute value of the maximum vertical distance between the assumed distribution function F_n (x) and the empirical distribution function F(x).

$$D_n = \sup_x | F_n(x) - F(x) | \quad (7)$$

We assume that the null hypothesis H_0 represents the hypothesis distribution function $F_n(x)$ follows the empirical distribution F(x). If the inequality (8) is satisfied, the nul hypothesis H_0 is invalid; otherwise, the distribution follows empirical distribution F(x).

$$(\sqrt{n} + 0.12 + 0.11/\sqrt{n}) D_n > c(\alpha) \quad (8)$$

where the critical value of c(α) depends on the significant level a. Since we assume a=0.05, the value of c (α) is 1.358 [10]. In (8), the smaller D_n is, the more the distribution anatomized with empirical distribution. We use a smaller D_n to figure out the parameters of hypothesis distribution, so that we can get the parameter of Pareto Distribution.

C. How to forecast next page

We forecast the browsing pattern of web users using Markov model. Markov model can be represented as a triplet MK = {W, A, π } as in Equations (9) and (10), where we denote W as a discrete random variable, its range is [w_1, w_2,…, w_n], where w_i represents one web page as model's state. Matrix A is denoted as the transition probability. Let p_{ij}=P {W_t=w_j|W_{t-1}=w_i} indicate the probability of requesting for page W_j at time t, when the web user request web page W_i at t-1 time. π represents the initial state.

$$A = (p_{ij}) = \begin{bmatrix} p_{11}\ p_{12} \cdots p_{1n} \\ p_{21}\ p_{22} \cdots p_{2n} \\ \vdots \ddots \\ p_{n1}\ p_{n2} \cdots p_{nn} \end{bmatrix} \quad (9)$$

$$\pi = (p_i) = (p_1, p_2, p_3, \cdots p_n) \quad (10)$$

The transition matrix A and the initial state matrix π can be predefined by user or computed by web log. The method can be explained as follows. First, aggregate the web log based on IP address. Second, random extract N users' web log to constitute a learning data set U= {u_1, u_2… u_n}. Taking advantage of the learning data, we can estimate all the parameters of Markov model with maximum likelihood estimation.

$$p_{ij} = \frac{S_{ij}}{\sum_{j=1}^{n} S_{ij}}, \quad p_i = \frac{\sum_{j=1}^{n} S_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{n} S_{ij}} \quad (11)$$

According to current page and the transition matrix of Markov model, we can predict the next web page user will browse. Let vector V(T)= (0, 0, 1, …, 0, 0) represent the page k at time t, and the next page location is $\max(\mathrm{V(t)} \cdot \mathrm{A})$ at time t+1.

IV. SYSTEM DESIGN

A. Design Considerations

When designing the traffic generating system, we take the following characteristics into consideration.

Accuracy. It means the system should produce traffic which fits well in two aspects: (1) The authenticity of the network traffic, such as burstiness and self-similar. (2) the authenticity of web user browsing behavior, such as page popularity and jumping.

Concurrency. The system should simulate many web users' browsing behavior simultaneously. However, the scale of the traffic generated can be controlled and adjusted by client for different test goals.

Platform-independence. The system can be applied to as many platforms, such as Linux and Windows, to satisfy client's demand.

B. System Components

The system is composed of four key modules (management module, web log preprocessing module,

database module and traffic generating module). This modular combination of system can build new generator to meet multiple requirements. Different functional model can be assigned to several develop team, which can simplify the software development, shorten the development cycle and enhance its scalability.

The system design is shown in Figure 2, and the four key functional modules are as follows:

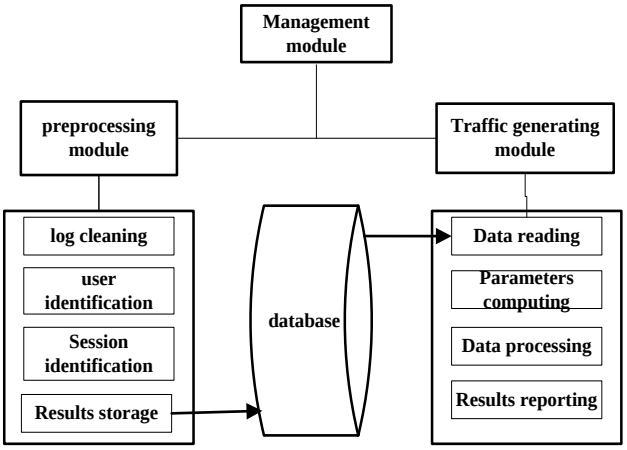


Figure 2. System design of the traffic generator

Management module. As the intermediate layer between the user and system, it takes charge of the system, distributes task，gather results, and handle bugs.

Preprocessing module. When web users access a real Web server, it returns corresponding web pages. Since a web page may contain a number of hyperlinks, we extract the hyperlink URLs embedded in such pages, and log them in a pool for next page candidate selection.

Database module. It stores the results of the web log process module, which can be used in the following traffic generating module.

Traffic generating module. As the core module in the system, its functions are as follows: (1) read the results of the log cleaning in Web log process model; (2) calculate the system's parameters, such as the Pareto Distribution parameter and Markov transition matrix; (3) interact with remote web server based on the access model, such as sending HTTP Get requests and receiving the responses.

V. TEST RESULTS

A prototype system has been developed and programmed in Python, which owns a number of complied and portable function modules. The system was implemented in a server with AMD Sempron 3800+ CPU, 2GB RAM, and running Fedora8 operating system. This server is a key part of Ocean, which is a network testbed used to evaluate research results of new protocols in Future Internet study, mainly address lacking of network background traffic generated by real user. Sixty threads were implemented concurrently, and each thread is corresponding to a Web user. We make the viewing time following Pareto Distribution (α=1.5) and extract about 100 pages to build a Markova transition matrix. We choose three time units, one second, 10 seconds and 30 seconds as sampling period for statistical analyses. This way, the test lasts about ten hours, and the results show that the traffic generated by the system has good burstiness and self-similarity.

A. *Burstiness test*

For self-similar traffic, burstiness remains regardless of the level of the aggregation because of the infinite variance of the source [11]. One way to observe this effect is by visually inspecting the time series plot vs such traffic with varying levels of aggregation [12]. In Figure 3, we show the traffic variations collected under different statistical period, respectively as 1 second (shown in Figure 3.a), 10 seconds (shown in Figure 3.b), and 30 seconds (shown in Figure 3.c). As in Figure 3, where the red line represents mean number of transmitted bytes under different statistical period, the traffic generated by our presented traffic generating system shows obvious burstiness. Moreover, the traffic burst does not significantly decrease as the time scale increased, which is consistent with the intrinsic characteristic of self-similar traffic flow.

B. *Self-similarity test*

Mathematically, a process X is called exactly (second-order) self-similar, if the aggregate process of X has the same correlation structure as X. The degree of self-similarity can be measured with Hurst parameter (H) [1]. Process X is self-similar when the value of H ranges from 0.5 to 1, and the more the Hurst parameter close to 1, the more self-similar the process is. We have applied two methods to compute the Hurst parameter, and the results are shown respectively in Figure 4.a and 4.b. When using R/S plot method, it is 0.73, and 0.72 when using variance-time plot method. The two Hurst parameters both reveal the self-similar nature of traffic generated by the system.

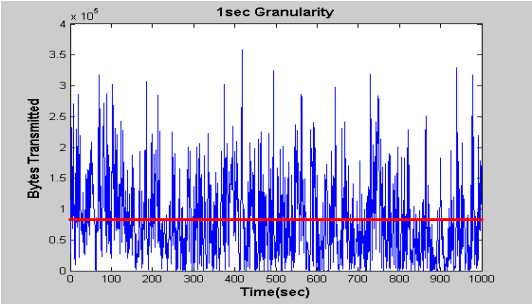


Figure 3.a. Traffic collected vs Time.
(Statistical period=1 Second)

 ISBN: 978-1-61208-285-1

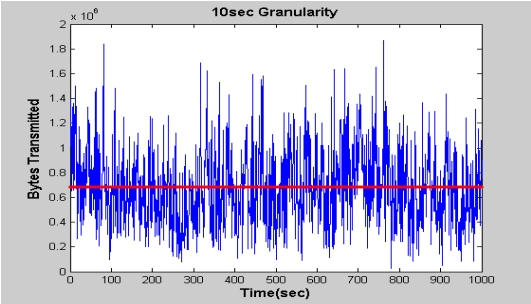


Figure 3.b. Traffic collected vs Time.
(Statistical period=10 Seconds)

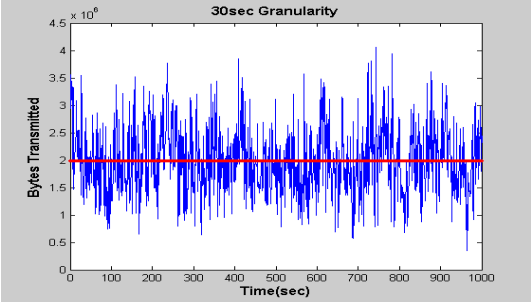


Figure 3.c. Traffic collected vs Time.
(Statistical period=30Second)

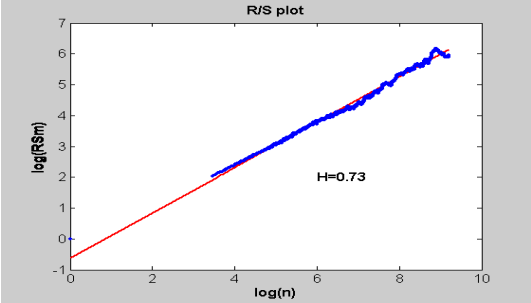


Figure 4.a. R/S plot of the traffic.
(H=0.73)

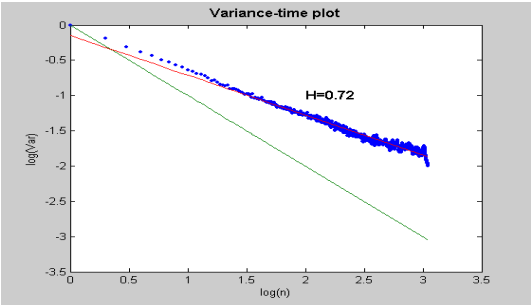


Figure 4.b. Variance-time plot of the traffic.
(H=0.72)

C. *Analysis of traffic self-similarity*

In our approach, On/Off model is used as a key part of user behavior model; we send page request to Web server according to the interval between ON state and OFF state. Threads in the system simulate ON or OFF sources, and the aggregation of them derives self-similar network traffic. However, why such approach makes our system generate self-similar traffic?

ON/OFF model has clear physical meaning. The data source is divided into two states, ON time and OFF time. Data source sends data in ON time, rather than OFF time. Take web user browsing as an example, a user sends Get requests and receives response from web server in the ON state, but there is no data transmit between the user and the server in the OFF state, which is regard as the user's thinking time.

It is assumed that the ON time and OFF time are independent and identically distribution. Suppose the duration of the ON state for the N (T), the duration of the OFF time for F(t), and the random variable N(t), F(t) for independent and identically Pareto distribution, then when aggregating enough ON/OFF sources, the generated network traffic is self-similar [13].

VI. CONCLUSION AND FUTURE WORK

In this paper, we proposed a web traffic generating method based on web users' access behavior model, and develop a traffic generating system. Compared to current traffic playback and traffic model based methods, our approach can simulate the real web users' accessing to real web servers, which are not pre-defined but determined by system clients, and generate almost the real network traffic. Test results show that traffic generated by our system has similar characteristics as the real web traffic, such as self-similarity and burstiness characteristics.

In future work, in order to improve the accuracy in simulating web users' behavior, we will polish the user behavior model, and make it more adapt the self-similarity nature of traffic. Moreover, we will extend this system so that it can generate other kinds of traffic, such as FTP, P2P, to meet different requirements.

ACKNOWLEDGMENT

This work is supported by the National Basic Research Program of China (2012CB315806) and the Natural Science Foundation of Chongqing (CSTC.2012JJB40008).

REFERENCES

[1] W. E. Leland, M. S. Taqqu, W. Willinger, and D.V. Wilson. "On the self-similar Nature of ethernet traffic(extended version)", Networking, IEEE/ACM Transactions on, vol. 2, no. 1, Feb 1994, pp. 1-15, doi: 10.1109/90.282603

[2] G. Xie, Y. Sun, Y. Zhang, Z. Li, H. Zheng, and X. Zheng. "Demo Abstract: Service-Oriented Future Internet Architecture (SOFIA)", IEEE Infocom/Poster, Shanghai, China, April 2011.

[3] Python, http://www.python.org/download/releases/2.6.8/, [retrieved:08.2012].

[4] Tcpreplay, http://tcpreplay.synfin.net/, [retrieved: 01.2013].

 ISBN: 978-1-61208-285-1

[5] SPEC, http://www.spec.org/osg/web99/, [retrieved: 01.2013].

[6] A Botta, A Dainotti, A Pescap é A tool for the generation of realistic network workload for emerging networking scenarios, Computer Networks, vol. 56, iss. 15, October 2012, pp. 3531-3547, ISSN 1389-1286, 10.1016/j.comnet.2012.02.019.

[7] S. Yu, G. Zhao, S. Guo, Y. Xiang, and A.V. Vasilakos. "Browsing behavior mimicking attacks on popular web sites for large botnets". Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on, April 2011, pp. 947-951, doi: 10.1109/INFCOMW.2011.5928949.

[8] P. Barford and M. Crovella. "Generating representative Web workloads for network and sever performance evaluation"[C]. ACM SIGMETRICS Performance Evaluation Review, pp. 151-160.

[9] P. Stuckmann, H. Finck, and T. Bahls. "A WAP Traffic Model and its Appliance for the Performance Analysis of WAP over GPRS". In Proc. of the IEEE International Conference on Third Generation Wireless and Beyond(3Gwireless '01) USA: San Francisco, 2001

[10] R. B. D' Agostino and M. A. Stephens. "Goodness-of-Fit Techniques"[M], Marcel Dekker, 1986.

[11] L.D. Catledge and J. E. Pitkow. "Characterizing browsing strategies in the World-Wide web"(J). Computer Networks and ISDN Systems. vol. 27, iss. 6, April 1995, pp. 1065–1073.

[12] H. Choi and J. Limb. "A behavioral model of Web traffic. Network Protocols", 1999. (ICNP '99) Proceedings. Seventh International Conference on, 31 Oct.-3 Nov. 1999, pp. 327-334.

[13] W. Willinger, M. S. Taqqu, R. Sherman, and D. V. Wilson. 1995. Self-similarity through high-variability: statistical analysis of ethernet LAN traffic at the source level. SIGCOMM Comput. Commun. Rev. vol. 25, no. 4, October 1995, pp. 100-113.

 ISBN: 978-1-61208-285-1

Performance Characterization of Streaming Video over TCP Variants

Gaku Watanabe, Kazumi Kumazoe, Dirceu Cavendish, Daiki Nobayashi, Takeshi Ikenaga, Yuji Oie
Department of Computer Science and Electronics
Kyushu Institute of Technology
Fukuoka, Japan
e-mail: {i108132g@tobata.isc, kuma@ndrc, cavendish@ndrc, nova@ecs, ike@ecs, oie@ndrc}.kyutech.ac.jp

***Abstract*—Video streaming has become the major source of Internet traffic. In addition, content delivery network providers have adopted Video over HTTP/TCP as the preferred protocol stack for video streaming. In this paper, we characterize the performance of various TCP variants when transporting video traffic over various network scenarios. We utilize network performance measurers, as well as video quality metrics, to characterize the performance and interaction between network and application layers of video streams for various network scenarios. We show that no widely deployed TCP variant is able to deliver best performance across all scenarios evaluated.**

***Keywords*—Video streaming; high speed networks; TCP congestion control; Packet retransmissions; Packet loss.**

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. TCP protocol interacts with video application in non trivial ways. Widely used video codecs, such as H-264, use compression algorithms that result in variable bit rates along the playout time. In addition, TCP has to cope with variable network bandwidth along the transmission path. Network bandwidth variability is particularly wide over paths with wireless access links of today, where multiple transmission modes are used to maintain steady packet error rate under varying interference conditions. As these two bit rates are independent, it is the task of the transport protocol to provide a timely delivery of video data so as to support a smooth playout experience.

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 to be proposed. Most of the proposals deal with congestion window size adjustment mechanism, which is called congestion avoidance phase of TCP, since congestion window size controls the amount of data injected into the network at a given time. In prior work, 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 [2], Cubic (Linux) [11], Compound (Windows) [12] - as well as our most recently proposed TCP variants: Capacity and Congestion Probing (CCP) [6], and Capacity Congestion Plus Derivative (CCPD) [7], in transmitting video streaming data over wireless path conditions. The motivation for including our proposed TCP variants is that CCP and CCPD utilize delay based congestion control mechanism, and hence are resistant to random packet losses experienced in wireless links.

Our contributions are as follows. We show that most used TCP variants of today affect video quality differently over various network scenarios. Our results show that there is no single TCP variant that is able to best deliver video streams under all network scenarios. The material is organized as follows. Related work discussion is provided on Section II. Section III describes video streaming over TCP system. Section IV introduces the TCP variants addressed in this paper, their features and differences. Section V addresses video delivery performance evaluation for each TCP protocol. Section VI addresses directions we are pursuing as follow up to this work.

II. RELATED WORK

Research studies of TCP performance on wireless network environments abound. Many of these studies [4], [9], [13] focus on the issue of loss based TCP not being able to differentiate between random packet loss and buffer overflow packet loss [3]. In [4], throughput performance of TCP variants for various Packet Error Rates (PERs) on a mobile network is studied via simulations. In [9], TCP variants performance under various PERs is also studied, including investigation of 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. In our work, we study the impact of network random losses on video streaming.

Recently, the impact of wide variability of TCP throughput caused by network packet losses on video streaming has been addressed [5], [10]. In [10], variable rate video encoders are considered, where video source adjusts its encoding rate according with network available bandwidth in the streaming path. In [5], a TCP Reno delay model is used by the video encoder to change encoding mode according with network conditions. Both approaches require a tight coupling between application and transport protocol. In contrast, our client video source and client are “loosely” coupled with TCP stack.

Another distinct aspect of our current work is that we analyze performance of widely used TCP variants, as well as our proposed delay based TCPs, CCP and CCPD, on real client

 ISBN: 978-1-61208-285-1

and server network stacks that are widely deployed for video streaming, via VLC open source video client, and standard HTTP server. As TCP variants have different dynamics when facing random losses, we seek to understand whether there are better TCP variants for video streaming, without having to tightly couple transport layer with video server/client.

III. Anatomy of Video Streaming over TCP

Video streaming over HTTP/TCP involves an HTTP server side, where video files are made available for streaming upon HTTP requests, and a video client, which places HTTP requests to the server over the Internet, for video streaming. Fig. 1 illustrates video streaming components.

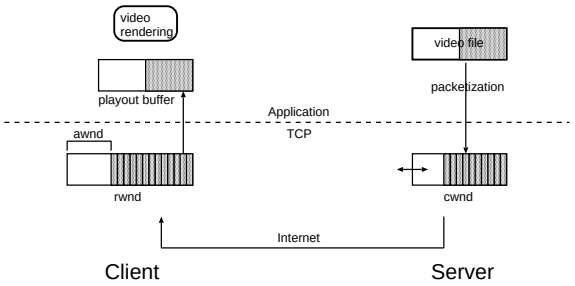


Fig. 1: Video Streaming over TCP

An HTTP server stores encoded video files, available upon HTTP request. Once a request is placed, a TCP sender is instantiated to transmit packetized data to the client machine. At TCP transport layer, a congestion window is used for flow controlling the amount of data injected into the network. The size of the congestion window, $cwnd$, is adjusted dynamically, according to the level of congestion in the network, as well as the space available for data storage, $awnd$ at the TCP client receiver buffer. Congestion window space is freed only when data packets are acknowledged by the receiver, so that lost packets are retransmitted by the TCP layer. At the client side, in addition to acknowledging arriving packets, TCP receiver sends back its current available space $awnd$, so that $cwnd \leq awnd$ at all times. At the client application layer, a video player extracts data from TCP receiver buffer into a playout buffer, used to smooth out variable data arrival rate.

A. Interaction between Video streaming and TCP

At the server side, HTTP server retrieves data into the TCP sender buffer according with the $cwnd$ size. Hence, in case of HTTP server, the injection of video data into the TCP buffer is unrelated to the video variable encoding rate. In addition, 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 $cwnd/rtt$. For each TCP variant, to be described shortly, the size of the congestion window is computed by a specific algorithm at time of packet acknowledgement reception by the TCP source. However, for all TCP variants, the size of the congestion window is capped by the available TCP receiver space $awnd$ sent back from the TCP client.

At the client side, the video data is pulled by the video player into a playout buffer, and delivered to the video renderer. Playout buffer may underflow, if TCP receiver window empties out. On the other hand, playout buffer overflow does not occur, since the player will not pull more data into the playout buffer than it can handle.

In summary, video data packets are injected into the network only if space is available at the TCP congestion window. Arriving packets at the client are stored at the TCP receiver buffer, and extracted by the video playout client at the video nominal playout rate.

IV. Transmission control protocol variants

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. Delay based TCP protocols, on the other hand, use queue delay information as the congestion indication signal, increasing/decreasing the window if the delay is small/large, respectively. Vegas, CCP and CCPD are examples of delay based protocols. We have not included Vegas on our study because Vegas performance is not competitive against well established TCP variants [6].

Most TCP variants follow TCP Reno phase framework: 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 controls the $cwnd$ size 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 2 illustrates various phases of a TCP session. A comprehensive tutorial of TCP features can be found in [1].

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 its current size in half on packet loss detection, as per equation 1.

 ISBN: 978-1-61208-285-1

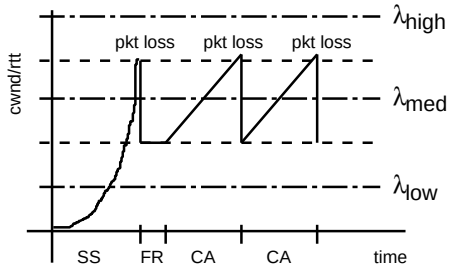


Fig. 2: TCP Congestion Window Dynamics vs Video Playout

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

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 as 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). The rational for these equations 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 Wintel 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.

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:

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

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. CCPD cwnd adjustment scheme is as per Equation 6:

$$\begin{aligned} cwnd_k = Kp[B - x_k - in\_flight\_segs_k] + \\ \frac{Kd}{t_k - t_{k-1}}[x_{k-1} + in\_flight\_segs_{k-1} + \\ -x_k - in\_flight\_segs_k] \end{aligned} \tag{6}$$

(7)

where Kp is a proportional gain, Kd is a derivative gain, 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.

Let λ be the video average bit rate across its entire playout time. That is, $\lambda = VideoSize/TotalPlayoutTime$. Fig. 2 illustrates three video playout rate cases: $\lambda_{high}, \lambda_{med}, \lambda_{low}$:

 ISBN: 978-1-61208-285-1

λ_{high} The average playout rate is higher than the transmission rate. In this case, playout buffer is likely to empty out, causing buffer underflow condition.

λ_{med} The average playout rate is close to the average transmission rate. In this case, buffer underflow is not likely to occur, affording a smooth video rendering at the client.

λ_{low} The average playout rate is lower than the transmission rate. In this case, playout buffer may overflow, causing picture discards due to overflow condition. In practice, this case does not happen if video client pulls data from the TCP socket, as it is commonly the case. In addition, TCP receiver buffer will not overflow either, because $cwnd$ at the sender side is capped by the available TCP receiver buffer space $awnd$ reported by the receiver.

V. Video Streaming Performance Characterization over TCP Variants

Figure 3 describes the network testbed used for emulating a network path with wireless access link. An HTTP video server and a VLC client machine are connected to two access switches, which are connected to a link emulator, used to adjust path delay and inject controlled random packet loss. All links are 1Gbps, ensuring plenty of network capacity for many video streams between client and server. No cross traffic is considered, as this would make it difficult to isolate the impact of TCP variants on video streaming performance. An extended version of this paper is planned to include multiple video stream experiments.

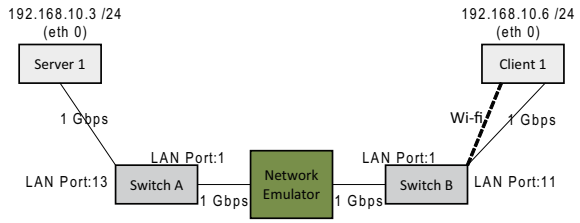


Fig. 3: Video Streaming Emulation Network

Video and network settings are as follows: video file size: $409Mbytes$; Playback time: $10min24sec$; Average playback rate: $5.24Mbps$; Encoding: MPEG-4;[1] video codec: H.264/AVC; frame rate: 30fps; audio codec: MPEG-4 AAC; playout buffer size: $656Kbytes$. TCP sender and receiver maximum buffer size: $256Mbytes$.

Performance measurers adopted, in order of priority, are:

- **Picture discards:** number of frames discarded by the video decoder. This measurer defines the number of frames skipped by the video rendered at the client side.
- **Buffer underflow:** number of buffer underflow events at video client buffer. This measurer defines the number of "catch up" events, where the video freezes and then resumes at a faster rate until all late frames have been played out.
- **Packet retransmissions:** number of packets retransmitted by TCP. This is a measure of how efficient the TCP variant is in transporting the video stream data. It is likely to impact video quality in large round trip time path conditions, where a retransmission doubles network latency of packet data from an application perspective.

In the TCP variant performance comparison study that follows, no attempt was made to tune TCP parameters to best video streaming performance. In particular, for CCP(x), where x is Kp parameter of Eq. 5, and CCPD(x,y), where x and y are Kp and Kd parameters of Eq. 6, the parameters used were derived from [8], tuned to provide best file transfer performance, not video streaming, for a fair comparison with the other TCP variants.

We organize our test cases into the following categories:

- Network bandwidth smaller than video playout rate
- Network bandwidth larger than video playout rate
- Network bandwidth much larger than video playout rate
- Wifi access link scenario

For each of these categories, we have run ten trial experiments for each TCP variant with and without random packet losses, and various round trip times. Results are reported as average and standard deviation bars.

A. Network bandwidth smaller than video playout rate

Fig. 4 summarizes performance measurers when the network emulator is set to throttle network bandwidth to a value slightly lower than video nominal playout rate, when the video server and client are far apart (100msec rtt). In this case, Cubic is the TCP variant with least picture discards and playout buffer underflow events, event though it presents the largest number of packet retransmits. The high number of packet retransmits attests the aggressive behavior of Cubic in ramping up its congestion window, as illustrated in Fig. 5. A side effect of this aggressiveness is a lower number of playout buffer underflow events. Reno and Compound present the largest number of picture discards, which can be traced to their lack of aggressiveness, attested by their low number of packet retransmissions. Reno is the least aggressive TCP variant in ramping up $cwnd$ size, as illustrated in Fig. 5. The trade-off is the number of playout buffer underflow events, higher than Cubic.

Comparing $cwnd$ dynamics in Fig. 5 (X-axis in units of 100msec), one can see how slower to react to network packet loss Reno and Compound TCP variants are. Cubic reacts faster, but not as fast as CCP(1). CCPD(1,4000) has the highest range of variation; notice how steady CCPD(1,2000) $cwnd$ dynamic is, even in the presence of dropped packets due to network congestion. A large $cwnd$ size range makes more difficult to achieve a smooth video rendering experience.

We have also run the same scenario, but injecting a 0.01% packet loss. Comparative results are similar to the ones just presented, and are omitted for sake of space.

B. Network bandwidth larger than video playout rate

In this experiment, network available bandwidth is set to a value slightly larger than the average video playout rate, and video server and client are far apart (100msec rtt). Performance results are shown in Fig. 6. In this case, the number of picture discards and playout buffer underflow events is negligible

 ISBN: 978-1-61208-285-1

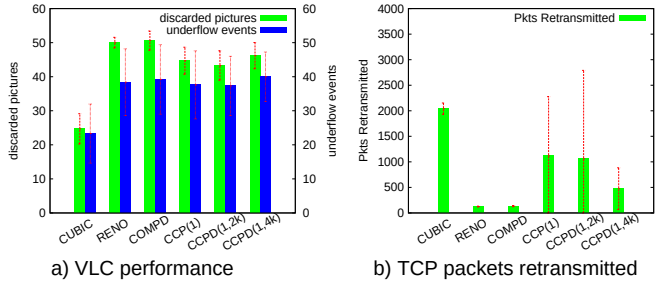


Fig. 4: Perf: AvgVR>NetBW; NoRanLoss; rtt=100msec

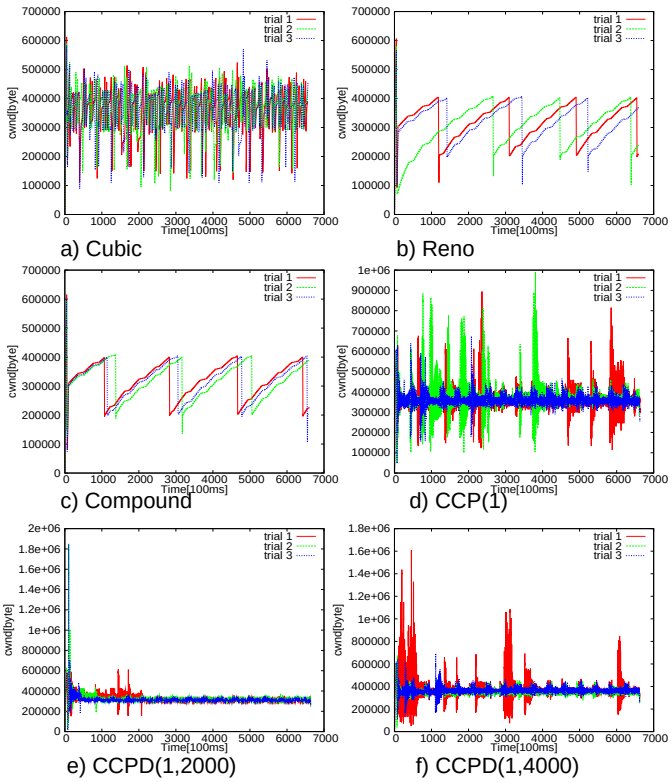


Fig. 5: Cwnd: AvgVR>NetBW; NoRanLoss; rtt=100msec

across all TCP variants. However, the least number of packet retransmits is presented by Reno and Compound, the least aggressive TCP variants. Cubic presents the largest number of packet retransmits. In contrast, in a similar lossless scenario, but with server and client close to each other (10msec rtt), is presented in Fig. 7. In this case, picture discards are again not significant for all TCP variants, even though packet retransmits are about the same for most variants, except Cubic. In general, the longer the path between video source and client, the more picture discards the streaming session will experience. This is because the client needs to render 30 frames/sec, which means a frame being rendered every 33msecs. If network latency is large and the buffer playout is not deep enough, retransmitted packets with additional rtt delay will likely arrive too late for the frame to be rendered.

When we introduce a 0.01% packet loss in the long (100msec rtt) path (Fig. 8), Reno and Compound performance

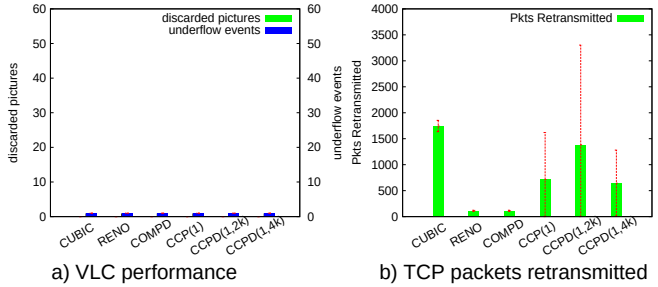


Fig. 6: Perf: AvgVR<NetBW; NoRanLoss; rtt=100msec

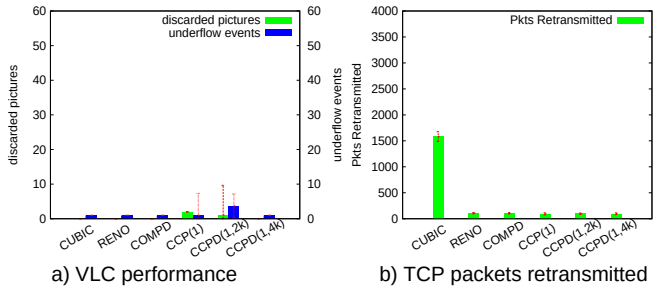


Fig. 7: Perf: AvgVR<NetBW; NoRanLoss; rtt=10msec

present the largest number of picture discards and playout buffer underflow events. Cubic, CCP and CCPD variants present negligible number of picture discards and playout buffer underflows, albeit with larger number of packet retransmits. Overall, random losses drag Reno and Compound TCP variants to a lower throughput, which in this case is below the average video playout rate, increasing playout buffer underflow events. One may conclude that responsive TCP variants deliver better streaming performance in the presence of random packet losses.

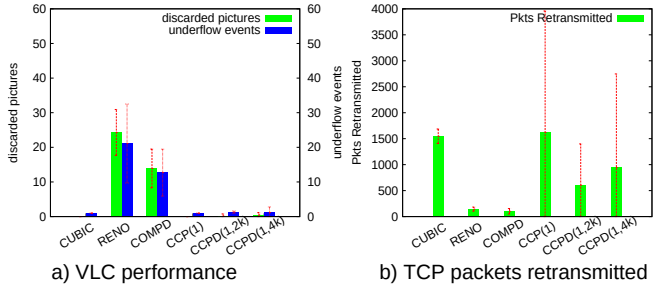


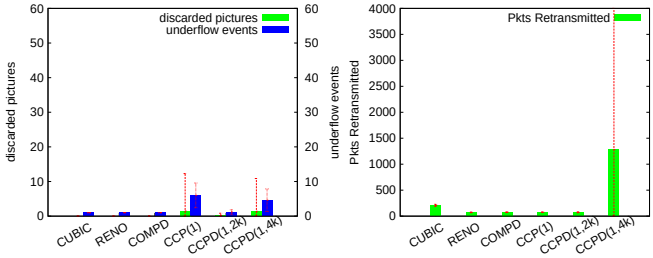
Fig. 8: Perf: AvgVR<NetBW; 0.01 % RLoss; rtt=100msec

C. Network bandwidth much larger than video playout rate

In this experiment, network bandwidth is set to a typical wireless link bandwidth, 20Mbps. Fig. 9 presents results with no random packet losses. We first notice that, when network bandwidth is plenty, there is negligible playout buffer underflow events across all TCP variants. In addition, packet retransmissions are much reduced in all TCP variants except CCPD(1,4000). In contrast, when a random packet loss rate of 0.01% is injected (Fig.10), most TCP variants increase playout buffer underflows, most notably Reno and CCPD(1,2000). All TCP variants continue to present few packet retransmissions.

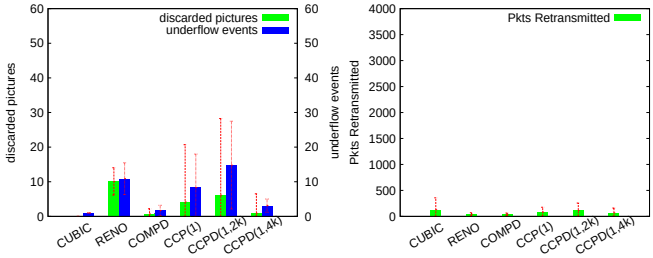
 ISBN: 978-1-61208-285-1

Overall, Cubic, Compound TCP and CCPD(1,4000) variants present the least number of picture discards.



a) VLC performance b) TCP packets retransmitted

Fig. 9: Perf: AvgVR<<NetBW; NoRanLoss;rtt=100msec

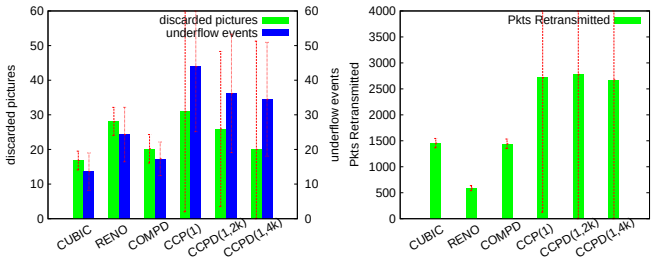


a) VLC performance b) TCP packets retransmitted

Fig. 10: Perf:AvgVR<<NetBW; 0.01%RLoss;rtt=100msec

D. WiFi access link experiment

In this experiment, the VLC client is attached to the network via a WiFi link. Before running the experiments, Iperf was used to measure the available wireless link bandwidth: 31.9Mbps, which is higher than the average video playout rate. Results are as per Fig. 11. We see that in case of plenty WiFi bandwidth, Cubic, Reno, and Compound TCP variants present the least number of discarded pictures and buffer playout underflows, followed closely by CCP and CCPD variants. In addition, CCP and CCPD protocols have the largest number of packet discards, as compared with Cubic, Reno, and Compound TCP variants. This attests to the aggressiveness of CCP and CCPD variants in pushing packets through.



a) VLC performance b) TCP packets retransmitted

Fig. 11: Perf: AvgVR<WiFiBW; rtt=100msec

In our performance evaluation, we have not attempted to tune VLC client to minimize frame discards, even though VLC settings may be used to lower the number of frame discards. In addition, as mentioned earlier, no tuning of TCP parameters was performed to better video client performance for any of the TCP variants studied. For our variants, we have simply used parameter values from our previous study of CCP/CCPD performance of file transfers [8].

VI. Conclusion and Future Work

In this paper, we have characterized TCP variants performance when transporting video streaming applications over wireless network type of paths via open source experiments. For widely used TCP variants, Cubic, Reno, and Compound, as well as our delay based variants, CCP and CCPD, the following can be said: i) A number of picture discards is commonplace in video streaming across all TCP variants, especially when video source and client are far apart; ii) When network bandwidth is scarce or in the presence of (wireless) packet loss, aggressive TCP variants, such as Cubic, ensure low number of picture discards; iii) Delay based TCP variants, such as CCP and CCPD, are effective in combatting random packet losses commonplace in wireless links.

Our next step is the design of a TCP variant tailored specifically for video streams. The goal is to minimize picture discards in all network conditions, as well as to avoid retransmissions of packets that are likely to be part of discarded frames at the client. This current work may also serve as a motivation for new video encoder/renderer and TCP coupling approaches, such as dynamic playout buffer re-sizing according to network bandwidth conditions.

Acknowledgment

Work supported in part by JSPS Grant-in-Aid for Scientific Research (B) (No 23300028).

References

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

[2] M. Allman, V. Paxson, and W. Stevens, “TCP Congestion Control,” IETF RFC 2581, April 1999.

[3] M. Alnuem, J. Mellor, and R. Fretwell, “New Algorithm to Control TCP Behavior over Lossy Links, ” IEEE International Conference on Advanced Computer Control, Jan 2009, pp. 236-240.

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

[5] A. Argyriou, “Using Rate-Distortion Metrics for Real-Time Internet Video Streaming with TCP, ” IEEE ICME06, 2006, pp. 1517-1520.

[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,” IEEE Second International Conference on Evolving Internet, best paper award, September 2010, pp. 42-48.

[7] D. Cavendish, Hiraku Kuwahara, K. Kumazoe, M. Tsuru, and Y. Oie, “TCP Congestion Avoidance using Proportional plus Derivative Control,” IARIA Third International Conference on Evolving Internet, best paper award, June 2011, pp. 20-25.

[8] D. Cavendish, K. Kumazoe, H. Ishizaki, T. Ikenaga, M. Tsuru, and Y. Oie, “On Tuning TCP for Superior Performance on High Speed Path Scenarios,” IARIA Fourth International Conference on Evolving Internet, best paper award, June 2012, pp. 11-16.

[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, Sept. 2009, pp.279-284.

[10] P. Papadimitriou, “An Integrated Smooth Transmission Control and Temporal Scaling Scheme for MPEG-4 Streaming Video,” In Proceedings of IEEE ICME 08, 2008, pp. 33-36.

[11] I. Rhee, L. Xu, and S. Ha, “CUBIC for Fast Long-Distance Networks,” Internet Draft, draft-rhee-tcpm-ctcp-02, August 2008.

[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 2008.

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

 ISBN: 978-1-61208-285-1

A Novel Component Carrier Selection Algorithm for LTE-Advanced Heterogeneous Networks

Zanyu Chen, Tsungnan Lin
Graduate Institute of Communication Engineering,
National Taiwan University,
Taipei, Taiwan,
d98942025@ntu.edu.tw, tsungnan@ntu.edu.tw

***Abstract*—Carrier aggregation has been proposed in LTE-advanced to support a wider bandwidth up to 100 MHz. The basic aggregated unit is called component carrier (CC). CCs are shared among different devices. Therefore it may cause performance degradation due to severe interference. A good CC assignment mechanism is desired to alleviate the interference problem. In this article, we propose a CC selection algorithm called Interference Management based Component Carrier (IMCC) scheduling to tackle the problem in heterogeneous networking environments of Femto Access Points (FAPs) and Macro-cell base stations. IMCC assigns CCs according to the entire system information, such as, location of FAPs, location of UEs (User Equipments), and the channel quality based on an evolutionary approach. In this way, IMCC mitigates the interference, and improves the system throughput. We construct a simulation environment with some stripes of apartments, which is often used to evaluate the performance of FAPs in prior works. The simulation results indicate the proposed approach outperforms other algorithms and show the effectiveness of IMCC.**

***Keywords*—component carrier; carrier aggregation; interference management; LTE-advanced.**

I. INTRODUCTION

Nowadays, the total mobile traffic of the whole world is growing exponentially thanks to the number of mobile users. Mobile users want higher throughput and lower latency while using wireless communication. Long Term Evolution-Advanced is developed to meet the increasing demand. It can support the throughput of 100 Mbps for high mobility users (such as user in the train) and 1 Gbps for low mobility users. Carrier aggregation is proposed as a solution to support a wider bandwidth up to 100 MHz for LTE-Advanced to deliver such a high throughput.

In carrier aggregation, the basic aggregated unit is called component carrier (CC). Carrier aggregation supports a wider bandwidth by aggregating two or more CCs. However, LTE-Advanced standard hasn't specified the way of CC assignment. Many issues remain to be answered in CC assignment. CCs can not only be aggregated to support a wider bandwidth, but also shared among many devices. It is inevitable to produce interference in such a CC-sharing scheme. Despite using carrier aggregation, to shrink the cell size is also a key technique to improve the performance in cellular networks.

Shrinking the cell size may reduce coverage range of a macro cell. On the other hand, users need high data rate and a macro cell may not satisfy all users' demand in the cell. Therefore, femtocell would be a viable solution to handle this situation. However, there are some challenges to deploy femtocells, such as, massive deployment, uncoordinated deployment, and high density [1]. These challenges cause the interference between Femto Access Points (FAPs) [2] to be severe and unpredictable. So, the interference is the main factor affecting the system performance, and CC selection of each FAP is an important topic to be explored.

In this paper, we consider the CC selection of each FAP in a heterogeneous networking environment. The goal of the proposed approach called "IMCC" (Interference Management based Component Carrier scheduling algorithm) is designed to mitigate the interference and achieve the maximum throughput. Since the determination of CC selection can not be solved analytically, IMCC is an evolutionary computation approach based on PSO (Particle Swarm Optimization) mechanism [3]. We devise a discrete computing approach, which is used in IMCC to solve the CC selection problem. One advantage of IMCC is the adaptive capability since IMCC takes the whole system information into consideration, such as, the location of FAPs, the location of UEs (User Equipments), and the channel quality. Therefore, the interaction between deployed FAPs is also considered in IMCC. When the CC selection is determined, IMCC then assigns the appropriate power on each used CC of each FAP.

We construct the simulation environment of a heterogeneous networking environment which consists one marcocell and many FAPs. FAP are deployed in an environment with some stripes of apartments which is a commonly used scenario in prior works to evaluate FAP performance. The performance of IMCC is compared with several existing CC-selection algorithms [1], [4], [5]. From our computer simulations, the results indicate the proposed approach outperforms other algorithms.

The rest of this paper is organized as follows: In Section II, we introduce some related work. The system model is explored in Section III and in Section IV, we describe the proposed algorithm. The simulation results are presented in Section V, and Section VI is our conclusion.

II. RELATED WORK

The purpose of carrier aggregation is to aggregate multiple CCs to get a wider bandwidth for transmission. LTE-advanced

 ISBN: 978-1-61208-285-1

[2] is an intensive spectrum sharing environment, while many cells aggregate the same CCs to form a wider bandwidth at the same time, which leads to severe interference. Therefore, the interference is an important factor to affect system performance. Interference management inevitablely becomes an important topic and many works focus on this issue. The simplest strategy of CC selection is called universal reuse or reuse of factor 1. Universal reuse allows each cell to access each CC without any restriction. A. Simonsson [6] shows us that universal reuse performs best for wideband services. From another aspect, Y. Wang [7] tells us that an appropriate reuse factor leads to an improvement in 5%-outage user throughput in uncoordinated local area deployment. Decentralized Intercell-Cell Interference Coordination (D-ICIC) was proposed by Ellenbeck [8], which parametrized by the amount of channels N that each femtocell can allocate. G. Costa et al. [1] propose a dynamic channel selection algorithm to increase system performance in a femtocell scenario. He shows that dynamic channel selection is better than the static amount of channels.

L. Garcia et al. [4] propose an algorithm called "Autonomous Component Carrier Selection" (AACS) which is a fully distributed and slowly-adaptive algorithm. The CC selection criterion is to estimate the carrier-to-interference ratio to decide which CC can be chosen. The values of this ratio are static in ACCS, so there are some drawbacks in using these static values. Because of the nature of distributed properties, the complexity of ACCS is low, but ACCS may not obtain the optimal solution about CC selection in each cell. On the other hand, ACCS only provides a method of CC selection, it doesn't take transmission power of each CC into consideration. The author improves ACCS with power adaption on each CC in his following work [5].

R. Menon et al. [9] use potential game to provide a work about interference avoidance (IA). Similarly, K. Son et al. [10] also use potential game to formulate distributed IA which focuses on transmission over multiple channels in cellular network scenario. G. Costa et al. [1] propose an algorithm called "Timeout Based Reuse Selection" (TBRS). In his algorithm, each FAP determines its own reuse factor to approach IA in the whole system. He shows the performance of TBRS is better than D-ICIC. Therefore, in this work, we compare IMCC with ACCS, G-ACCS, and TBRS.

III. System Model and Problem Formulation

In this section, we present the system model, and formulate the CC selection in a heterogeneous networking environment with the system performance. In addition, we give a simple analysis about the complexity of the problem at the end of this section.

A. System Model

We consider an environment with a LTE-advanced macro cell, several LTE-advanced FAPs, and several user equipments (UEs). Suppose that the number of FAPs is N, and the number of UEs is K. LTE-advanced adopts carrier aggregation, therefore the bandwidth of the communication system is aggregated by L CCs. The macro cell always uses the whole bandwidth to transmit data, and FAPs transmit data by using the selected CCs, which is a subset of L CCs. We apply a full buffer traffic model with infinite data packets in the queue for each FAP. h_{fj} denotes the channel gain between FAP f and user j, and $h_{bs,j}$ is the channel gain between macro cell and user j. $\mathbb{I}$ denotes the CC assignment matrix where an element of $\mathbb{I}$, i_{fl}, equals to 1 if FAP f uses CC l.

Our work is first to focus on component carriers scheduling for each FAPs. Therefore, to simplify the problem, we suppose the transmission power is fixed and denoted by P_f and P_{bs} for each FAP and macro cell respectively. We suppose FAPs and macro cells allocate their power in each used component carrier uniformly. P_{fl} and $P_{bs,l}$ denote the transmission power on component carrier l of FAP f and macro cell respectively. U_f and U_{bs} denote the set of users associated with FAP f and the macro cell. $|U_f|$ and $|U_{bs}|$ are the number of elements of U_f and U_{bs}. An UE can only belong to a FAP or the macro cell, so we can describe the situation using the following equations:

$$\begin{aligned} &\textstyle\sum_{f=1}^{N} \mid U_f \mid + \mid U_{bs} \mid = K \\ \text{and} \quad &U_i \cap U_j = \phi, \forall \ i \neq j \end{aligned} \tag{1}$$

Suppose the transmission power of each FAP is P, and the power is uniformly distributed on each selected CCs, therefore P_{fl} can be computed as the follows:

$$P_{fl} = \frac{P_f}{\sum_{b=1}^{L} i_{fl}} \times i_{fl} \tag{2}$$

The modified Shannon formula developed in [11] is used to calculate the system performance. The formula can be depicted as below:

$$S = BW_{eff} log_2(1 + \frac{SINR}{SINR_{eff}}) \tag{3}$$

where B denotes the system bandwidth. W_{eff} and $SINR_{eff}$ adjust the system bandwidth efficiency and the Signal to Noise plus Interference Ratio (SINR) implementation efficiency respectively.

Next, we denote C_{fl} be the capacity of FAP f on selected CC l. We calculate the capacity of each user in FAP f, and sum up all of the capacity of user in FAP f to get C_{fl}. The equation is as the follows:

$$\begin{aligned} C_{fl} \quad = \quad & \textstyle\sum_{u \in U_f} \frac{B}{L|U_f|} \\ & \times log_2(1 + \frac{P_{fl} h_{fu}}{\frac{BN_0}{L} + \sum_{f'=1, f' \neq f} P_{f'l} h_{f'u} + P_{bs,l} h_{bs,u}}) \times i_{fl} \end{aligned} \tag{4}$$

where N_0 is the noise power per hertz, and L is the number of component carriers. Analogously, $C_{bs,l}$ is the capacity of the macro cell on CC l. We calculate the capacity of each user in the macro cell, and sum up all of the capacity of users in the macro cell to get $C_{bs,l}$. The equation is shown below:

$$C_{bs,l} = \sum_{u \in U_{bs}} \frac{B}{L|U_{bs}|} \times log_2(1 + \frac{P_{bs,l} h_{bs,u}}{\frac{BN_0}{L} + \sum_{f'=1}^{F} P_{f'l} h_{f'u}}) \quad (5)$$

The total capacity C_{total}, the sum of capacity of FAPs and the macro cell, can be depicted as the follows:

$$C_{total} = \sum_{l=1}^{L} (C_{bs,l} + \sum_{f=1}^{F} C_{fl}) \quad (6)$$

B. Problem Formulation

The binary assignment matrix $\mathbb{I}$ records the selected CC used by each FAP. For a specific assignment matrix $\mathbb{I}$, the system performance will be calculated according to (6). The goal of the proposed approach is to find a suitable CC assignment matrix $\mathbb{I}$ such that the maximum system throughput can be achieved. Therefore, the problem is depicted as follows:

$$\underset{\mathbb{I}}{\text{Maximize}} \qquad C_{total} \quad (7)$$

Each FAP can choose a CC for transmission or not. The number of CCs is L, so each FAP has 2^L different ways to choose CCs for transmission. The system has N FAPs, so the complexity of this problem becomes $O(2^{NL})$ if the exhausted search mechanism is used to find the optimal solution. The complexity increases exponentially with respect to the number of CCs and FAPs. When the parameter is large, it becomes impractical to use such a mechanism.

IV. Proposed Algorithm

Our design is based on an evolutionary computation approach called particle swarm optimization to find a suitable CC assignment matrix $\mathbb{I}$. The original PSO algorithm [3] is used in continuous case, but our problem is a discrete case. In this paper, we redefine position and velocity in order to determine the binary assignment matrix.

A. Particle Swarm Optimization

Particle Swarm Optimization is an optimization algorithm developed by James Kennedy and Russell Eberhart in 1995 [3]. In PSO, each candidate solution is seen as a particle. The algorithm is to randomly spread particles in the search space, and assign the position and velocity of each particles. Each particle would move in the search-space according to its position and velocity, and each particle has its own performance. In this way, local and global maximum performance can be defined since we know each particle's performance. The movement of each particle is influenced by these two maxima, namely the particle would move approach to the particle with maximum performance. The behavior of particles at time t is shown as follows:

$$\begin{aligned} V_i(t) &= W \times V_i(t-1) + C_1 \times rand \times (P_{best}(t-1) - X_i(t-1)) \\ &\quad + C_2 \times rand \times (G_{best}(t-1) - X_i(t-1)) \\ X_i(t) &= X_i(t-1) + V_i(t) \end{aligned} \quad (8)$$

where $V_i(t)$ is the velocity of particle i at time t, X_i is the position of particle i at time t, and W is the inertial weight. C_1 and C_2 are the positive constant parameters, rand is the random function which takes value in range [0,1], P_{best} is the best position of the particle, and G_{best} is the position of the particle with best performance among all particles.

B. IMCC

In our problem, a particle represents a specific assignment matrix which represents component carriers selected by femto cells. Suppose that the communication environment has K users, N FAPs, and L CCs. Each user links to the nearest FAPs or macro cell, which means the user would receive the largest signal power. Each particle is an $N \times L$ matrix to represent an assignment method for FAPs. We suppose there are P particles in the proposed algorithm, denoted by $\{Particle_1, Particle_2, ..., Particle_p\}$, and $Partcile_i(j,k)$ is the element in row j and column k of the particle i. $Particle_i(j,k)$ equals to 1 if FAP j use CC k in particle i, otherwise, it equals to 0.

Then, the performance of each particle can be computed according to 6. Rec_i is denoted as the best score of the $Particle_i$ from the beginning to the current iteration and $recParticle_i$ is the assignment matrix of this best score. This best score is referred to the P_{best} in the original PSO algorithm. The initial values of Rec_i and the elements of $recParticle_i$ are all zero for $i \in \{1, 2, ..., p\}$. New C_{total} of 6 is computed in each iteration, and Rec_i is updated accordingly. Let Opt be the global maximum matrix among all Rec_i , and

$$\text{Opt} = \arg\max_i \{Rec_i\}, i \in \{1, 2, ..., p\} \quad (9)$$

Rec_{opt} is referred to G_{best} in the original PSO algorithm and $recParticle_{opt}$ is its assignment matrix.

Before we define the movement operation of the assignment matrix to approach closer to P_{best} or G_{best}, we need to define the distance $D(P_1, P_2)$ between two particles of P_1 and P_2. The definition is shown below:

Definition: The distance between matrices $\mathbb{A}$ and $\mathbb{B}$ ($\mathbb{A}$ and $\mathbb{B}$ are both N by M matrices) is

$$D(\mathbb{A}, \mathbb{B}) = \sum_{i=1}^{N} \sum_{j=1}^{M} a_{ij} \oplus b_{ij} \quad (10)$$

where a_{ij} and b_{ij} are the element of ith row and jth column of matrix $\mathbb{A}$ and $\mathbb{B}$ respectively, and notation $\oplus$ represent XOR operation.

The goal of the movement is to approach either the local maximum or the global maximum, namely to decrease the

distance between particle and P_{best} or G_{best}. The particle usually can get a higher score with this movement. Two moving operations are defined as:

Definition: The move operation $Move_{\mathbb{G}}(\mathbb{P})$ and $Move_{\mathbb{L}}(\mathbb{P})$ are defined as follows:

$$\begin{aligned} Move_{\mathbb{G}}(\mathbb{P}) &: p_i^t = g_i^t, i = randi(1, M) \\ Move_{\mathbb{L}}(\mathbb{P}) &: p_i^t = l_i^t, i = randi(1, M) \end{aligned}$$

where $\mathbb{P}$, $\mathbb{G}$, $\mathbb{L}$ are $M \times N$ matrix, and $\mathbb{P} = [p_1^t p_2^t ... p_M^t]^t$,$\mathbb{G} = [g_1^t g_2^t ... g_M^t]^t$,$\mathbb{L} = [l_1^t l_2^t ... l_M^t]$. $randi(a, b)$ returns a random integer between a and b. $\mathbb{G}$ is referred to the global maximum assignment matrix $recParticle_{opt}$, and $\mathbb{L}$ is referred to the local maximum assignment matrix $recParticle_i$ mentioned before. While doing $Move_{\mathbb{G}}(\mathbb{P})$ operation, we arbitrarily change a row of $particle_i$ to the same row of $recPartcile_i$ to move closer to P_{best}, and $Move_{\mathbb{L}}(\mathbb{P})$ operation is similar.

Proposition: The action $Move_{\mathbb{G}}(\mathbb{P})$ and $Move_{\mathbb{L}}(\mathbb{P})$ can decrease $D(\mathbb{P}, \mathbb{G}_{best})$ and $D(\mathbb{P}, \mathbb{P}_{best})$ respectively.

Proof: Let the $\acute{P}$ be the particle after particle P did operation $Move_{\mathbb{G}}(\mathbb{P})$. Without loss of generality, we suppose the kth row of $\mathbb{P}$ is chosen to be changed to the kth row of $\mathbb{G}_{best}$. From Eq.10, we know the distance between $\mathbb{P}$ and $\mathbb{G}_{best}$ is:

$$\begin{aligned} D(P, G_{best}) &= \sum_{i=1}^{N}\sum_{j=1}^{M} p_{ij} \oplus g_{ij} \qquad (11) \\ &= \sum_{i=1, i\neq k}^{N}\sum_{j=1}^{M} p_{ij} \oplus g_{ij} + \sum_{j=1}^{M} p_{kj} \oplus g_{kj} \end{aligned}$$

The only difference between $\mathbb{P}$ and $\acute{\mathbb{P}}$ is the kth row, so we have

$$\sum_{i=1, i\neq k}^{N}\sum_{j=1}^{M} \acute{p_{ij}} \oplus g_{ij} = \sum_{i=1, i\neq k}^{N}\sum_{j=1}^{M} p_{ij} \oplus g_{ij} \qquad (12)$$

Since the kth row of $\acute{P}$ and G_{best} are the same

$$\sum_{j=1}^{M} \acute{p} \oplus g_{kj} = \sum_{j=1}^{M} g_{kj} \oplus g_{kj} = 0 \leq \sum_{j=1}^{M} p_{ij} \oplus g_{kj} \qquad (13)$$

Therefore, we have

$$\begin{aligned} &\textstyle\sum_{i=1}^{N}\sum_{j=1}^{M} \acute{p_{ij}} \oplus g_{ij} \leq \sum_{i=1}^{N}\sum_{j=1}^{M} p_{ij} \oplus g_{ij} \\ \Rightarrow \quad & D(\acute{\mathbb{P}}, \mathbb{G}_{best}) \leq D(\mathbb{P}, \mathbb{G}_{best}) \qquad (14) \end{aligned}$$

■

In our design, there is a probability that $Particle_i$ does not get close to local maximum nor global maximum. The purpose is letting particles find more, possibly better solutions, in the solution space. So, we define an operation called "Row-Addition" as below.

Random Movement: Row-Addition RA($\mathbb{P}$)

Algorithm 1 The procedure of CC selection in IMCC

Initialization: $P(k), k = 1, ..., N$, denote N particles, and the algorithm runs i iterations.
repeat
  repeat
    $temp$ = score of $P(k)$
    if $temp < rec(n)$ **then**
      $Move_{\mathbb{G}}(P(k))$
      $Move_{\mathbb{L}}(P(k))$
    else if $temp > rec(k)$ **then**
      $rec(k) \leftarrow temp$
      $recParticle(k) \leftarrow P(k)$
    else if $temp > opt$ **then**
      $opt \leftarrow temp$
      $recParticle_{opt} \leftarrow P(k)$
    end if
    if $rand < \delta$ **then**
      $P(k) \leftarrow RA(P(k))$
    end if
    $k \leftarrow k + 1$
  until $k = N$
  $k \leftarrow 1$
  $i \leftarrow i - 1$
until $i = 0$

RA(P) means to do row-addition on particle P. The row-addition is operated in a random row of $\mathbb{P}$. If row j of particle P is chosen, we regards this row as a binary number and add this row by 1 ($mod\ F$), where F is equal to $2^L - 1$. Because the maximum value of each row is $2^L - 1$, the mod operation is to be sure that this binary number wouldn't exceed this value. For example, the row j of $Particle_i$ is [0 1 0 1], which is 5 in binary, and it is changed to [0 1 1 0] by adding 1 to it.

So, the movement of our algorithm is defined. We would repeat these operations, namely evaluation, record, and movement, iteratively. For simplicity, each user chooses the FAP with maximum channel gain for transmission. The final solution to the problem is $recParticle_{Opt}$. The pseudo code of CC selection procedure in IMCC is shown in Algorithm 1.

After determining the binary assignment matrix, IMCC further adjust power using the original PSO algorithm. Therefore, IMCC can also perform power adaption on each FAP. The procedure of IMCC is to determine the CC assignment matrix at first. The next step is to applied the original PSO to allocate power on each selected CC of each FAP.

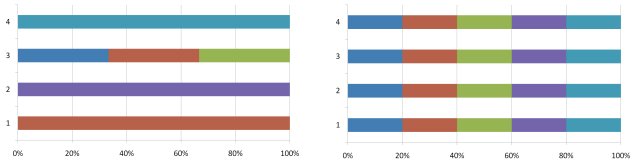
V. Simulation Results

A. Simulation set-up

Several experiments are performed to evaluate the performance of the proposed algorithms and other algorithms. In our simulation environments, we set the maximum power of the base station and FAPs to 43dBm and 13dBm, respectively. The bandwidth of component carrier is 20MHz for each CC. The deployment of carrier aggregation is that each CC is on the same or little frequency separation spectrum. We consider a layout of 1-tier 7 hexagonal cells with 3 identical sectors in each cell. The simulation scenario and indoor path loss modeling are the same as in the literature [12] for the evaluation of femtocells. We suppose the temperature of the

 ISBN: 978-1-61208-285-1

environment is 300K, therefore the noise of the system is -174 dBm/Hz. We compare the performance of IMCC, ACCS [4], G-ACCS [5], and TBRS [1]. The PCC threshold is 10dB and the SCC threshold is 8dB, which are the same as described in [4]. The parameters of TBRS are TBRS(2,10) which lead to the best average performance while the FAPs are crowded [1]. δ in IMCC is set to 0.3. The number of iterations, i, is set to 500, which can obtain a nearly optimal solution in our experiments. Therefore, the computation time of IMCC is a few seconds in a computer with Matlab R2009 and Intel(R) Core(TM) i5 CPU k655.



(a) crowded (b) sparse

Fig. 1. The CC allocation of 4 FAPs. (a) is the crowded topology, and (b) is the sparse topology. 5 different colors are used to denote different CCs.

B. Crowded and sparse environments

The design of the simulation is to evaluate how the selected CCs are determined by the proposed IMCC algorithm. Two simple topologies are considered: crowded and sparse distribution of FAPs. When FAPs are placed in a crowded environment, the selected CCs should show the orthogonal characteristics to avoid severe interference between each other in order to deliver the maximum system performance. On the other hand, if FAPs are placed in a sparse environment, they should use the whole bandwidth because the interference between each other is negligible.

In both topologies, the BS is placed at location (0,0), and there are 20 users. The users are randomly distributed in a 40m$\times$40m square with center 800m far from the base station which is on the cell edge. Four FAPs are distributed circularly with the same center as users, the radius of crowded and sparse topology are 5m and 20m respectively.

Figure 1 shows the selected CCs for the four FAPs in both topologies. In Figure 1, there are five colors in each figure, and each color stands for a CC. Subfigure (a) in Fugure 1 shows the CC allocation of the crowded case. The interference is serve among FAPs, so FAPs trend to using the different CCs for transmission. The neighboring FAPs use different CCs, and a CC is shared by FAP 1 and FAP 3. This is because that the distance between FAP 1 and FAP 3 is far enough such that the interference is light. Sharing the same CC can improve the system performance. Subfigure (b) in Figure 1 shows each FAP has five colors. That means every FAP uses the whole bandwidth for transmission. The interference is too light to be ignored while the distance between FAPs is large. In our intuition, using the whole bandwidth leads to the highest aggregate throughput.

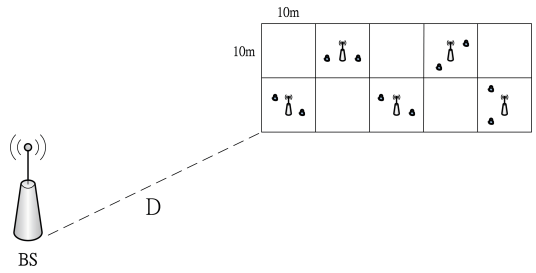


Fig. 2. The topology of 5 FAPs in an apartment with two stripes.

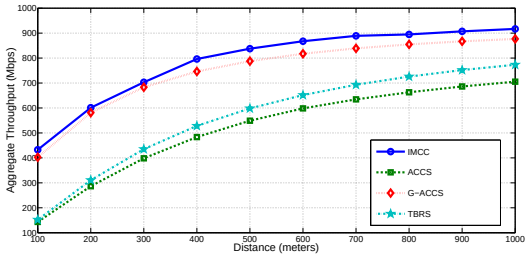


Fig. 3. The throughput v.s. distance of all algorithms.

C. Two stripes of apartments

In this simulation, the scenario we apply is that a floor with two stripes of apartments, each stripe having 5 apartments. The size of each apartment is 10m$\times$10m, and we set FAPs in the center of this square. We suppose each FAP serves two users which are randomly distributed in the apartment. The distribution topology is shown in Figure 2, where D is the distance between FAPs and BS. The purpose of this scenario is to investigate performance in a LTE-advanced cellular network. We change the distance between the stripes and the BS from 100 meters to 1000 meters. The performance results are shown in Figure 3 for different algorithms.

While the distance is short, the interference caused by BS is very severe. In this condition, IMCC and G-ACCS is better than other two algorithms as seen in Figure 3. The reason is that G-ACCS and IMCC change the power allocation for each CC while ACCS, and TBRS just use uniform power allocation and use the maximum power on each used CC. Therefore, the interference is more severe than G-ACCS and IMCC. The severe interference makes the performance lower. However, the gap between these algorithms becomes smaller while the

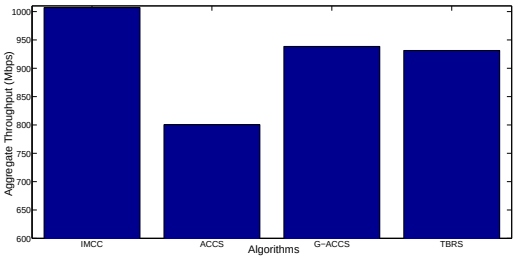


Fig. 4. The throughput of all algorithms when the distance between Marco BS is large.

 ISBN: 978-1-61208-285-1

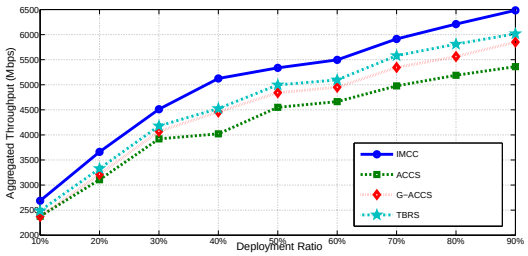


Fig. 5. The aggregate throughput with different deployment ratio in all algorithms.

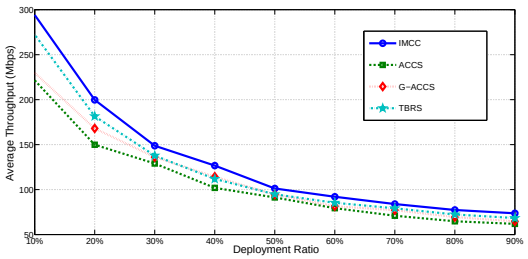


Fig. 6. The average throughput of FAPs with different deployment ratio in all algorithms.

distance gets larger because the interference from BS becomes smaller while D becomes larger.

If the distance is far enough, the interference caused by BS can be ignored, which is the same as the situation where there is no BS. Under such a circumstance, Figure 4 shows IMCC is still the best among all algorithms. Although G-ACCS performs power adaption and TBRS uses only uniform power allocation, the performance of G-ACCS and TBRS are almost the same. These results clearly indicate that an appropriate CC allocation is more important than power adaption. While managing interference among FAPs, the CC assignment is important and should be determined first.

D. Different Deployment Ratio

In this experiment, we construct a scenario with 100 apartments in a square and the size of each apartment is 10m$\times$10m. If there is a FAP in an apartment, it would be put in the center of the apartment, and two users are randomly distributed in the apartment. We vary the FAP deployment ratio of each apartment from 10% to 90%. The distance between these apartments and the BS is very large. Therefore we can ignore the interference caused by BS. We perform the experiment several times, and average these results.

Figure 5 shows the aggregate throughput of FAPs and Figure 6 is the average throughput of each FAP. Both figures show that IMCC has the best performance no matter if the deployment ratio is low or high. The results show that IMCC can work efficiently whether in light or severe interference environments. On the other hand, it can be shown that TBRS, which only determines the CC assignment, has performance better than G-ACCS. The results, again, show the appropriate CC assignment can obtain more performance gain.

VI. Conclusion

In this article, we propose a CC selection algorithm called IMCC (Interference Management based Component Carrier scheduling) to tackle the problem in heterogeneous networking environments of Femto Access Points (FAPs) and Macrocell base stations. IMCC assigns CCs according to the entire system information, such as, location of FAPs, location of UEs (User Equipments), and the channel quality based on an evolutionary approach. The approach is based on a devised discrete-type optimization mechanism. After the selected CCs are determined, the power on each CC can be further adjusted accordingly. Several simulation topologies are performed to compare the performance with existing algorithms. The simulation results indicate the proposed approach outperforms existing algorithms.

Acknowledgement

This work was supported by the Taiwan National Science Council under the Grants NSC99-2221-E-002-143-MY3 and NSC100-2221-E-002-177-MY2.

References

[1] G. Costa, A. Cattoni, I. Kovacs, and P. Mogensen, “A fully distributed method for dynamic spectrum sharing in femtocells,” in *IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pp. 87 –92, April 2012.

[2] T. Zahir, K. Arshad, A. Nakata, and K. Moessner, “Interference management in femtocells,” *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 1, pp. 293–311, 2013.

[3] J. Kennedy and R. Eberhart, “Particle Swarm Optimization,” in *IEEE International Conference on Neural Networks*, vol. 4, pp. 1942 – 1948, 1995.

[4] L. G. U. Garcia, K. I. Pedersen, and P. E. Mogensen, “Autonomous Component Carrier Selection: Interference Management in Local Area Environments for LTE-Advanced,” *IEEE Communications Magazine*, vol. 47, pp. 110 – 116, September 2009.

[5] L. G. U. Garcia, I. Z. Kovacs, K. I. Pedersen, G. W. O. da Costa, and P. E. Mogensen, “Autonomous Component Carrier Selection for 4G Femtocells - A fresh look at an old problem,” *IEEE Journal on Selected Areas in Communications*, vol. 30, pp. 525 – 537, 2012.

[6] A. Simonsson, “Frequency Reuse and Intercell Interference Co-Ordination In E-UTRA,” in *IEEE 65th Vehicular Technology Conference (VTC Spring)*, pp. 3091 –3095, April 2007.

[7] Y. Wang, S. Kumar, L. Garcia, K. Pedersen, I. Kovacs, S. Frattasi, N. Marchetti, and P. Mogensen, “Fixed Frequency Reuse for LTE-Advanced Systems in Local Area Scenarios,” in *IEEE 69th Vehicular Technology Conference*, pp. 1 –5, April 2009.

[8] J. Ellenbeck, C. Hartmann, and L. Berlemann, “Decentralized inter-cell interference coordination by autonomous spectral reuse decisions,” in *14th European Wireless Conference*, pp. 1 –7, June 2008.

[9] R. Menon, A. MacKenzie, R. Buehrer, and J. Reed, “A Game-Theoretic Framework for Interference Avoidance in Ad hoc Networks,” in *IEEE Global Telecommunications Conference (GlobeCom)*, pp. pp.1 –6, December 2006.

[10] K. Son, S. Lee, Y. Yi, and S. Chong, “REFIM: A practical interference management in heterogeneous wireless access networks,” *IEEE Journal on selected areas in communications*, vol. 29, pp. 1260 – 1272, June 2011.

[11] P. Mogensen, W. Na, I. Kovacs, F. Frederiksen, A. Pokhariyal, K. Pedersen, T. Kolding, K. Hugl, and M. Kuusela, “LTE Capacity Compared to the Shannon Bound,” in *IEEE 65th Vehicular Technology Conference (VTC Spring)*, pp. 1234 –1238, April 2007.

[12] 3GPP TR 36.814, “Further Advancements for E-UTRA: Physical Layer Aspects,” *Technical Specification Group Radio Access Network*, June 2009.

 ISBN: 978-1-61208-285-1

An Analysis of Users in a Q&A Site Submitted Many Answers Where First Polar Words are Negative Words

Masashi Minamiguchi, Kenji Umemoto, Yasuhiko Watanabe, Ryo Nishimura, Yoshihiro Okada
Department of Media Informatics, Ryukoku University
Seta, Otsu, Shiga, Japan
Email: t12m107@mail.ryukoku.ac.jp, t11m074@mail.ryukoku.ac.jp,
watanabe@rins.ryukoku.ac.jp, r_nishimura@afc.ryukoku.ac.jp, okada@rins.ryukoku.ac.jp

***Abstract*—In this study, we investigate that the evaluations of answers in a Q&A site are affected by whether the first polar words are negative words. We first investigate answers where the first polar words were negative words. The result shows that the evaluations of answers in a Q&A site were less affected by whether the first polar words were negative words. Furthermore, we investigate users in a Q&A site who submitted many answers where the first polar words were negative word. The result show that answers submitted to a Q&A site were evaluated based on whether their explanations were detailed and informative, rather than whether the first polar words were negative words. In this study, we use the data of Yahoo! chiebukuro, a widely-used Japanese Q&A site, for observation and examination. We also use the opinion extraction tool and model data, which were developed by Knowledge Clustered Group in National Institute of Information and Communications Technology (NICT).**

Keywords*—*negative word; opinion polarity; opinion expression; Q&A site; Yahoo! chiebukuro.

I. INTRODUCTION

Some words have the polarity. These words are called *polar words* and classified into positive words and negative words [1]. In face-to-face communication, some people tend to speak stories where the first polar words are negative words, even if their stories include not only negative words but also positive words. This way of speaking stories may affect the evaluations of their stories. Furthermore, negative non-verbal signals, such as folded arms, frowning, distance increase, and looking away, often make their stories more negative. On the other hand, in question and answer (Q&A) sites, such as Yahoo! answers [2], Yahoo! chiebukuro [3], Oshiete! goo [4], Hatena [5], and OKWave [6], negative non-verbal signals rarely make their stories more negative. It is because it is difficult to send negative non-verbal signals via Q&A sites. However, we do not know whether the way of writing stories where the first polar words are negative words affects the evaluations of their stories, especially, answers submitted to Q&A sites. To solve this problem, we investigate answers where the first polar words are negative words. Furthermore, we investigate users who submitted many answers where the first polar words were negative words. In this study, we used the data of Yahoo! chiebukuro, a widely-used Japanese Q&A site, for observation and examination.

The rest of this paper is organized as follows: In Section II, we surveys the related works. In Section III, we describes the data of Yahoo! chiebukuro, which we used for observation and examination. In Section IV, we describes a method of detecting users submitted many answers where the first polar words were negative words. In Section V, we show the experimental results and discussions. Finally, in Section VI, we present our conclusions.

II. RELATED WORKS

In these years, a large number of studies have been made on sentiment analysis based on the polarities of words. Sharifi and Cohen proposed a method of using conditional random fields for extracting polar words and determining the overall sentiment of text [1]. Takamura et al. developed a lexical network out of glosses in a dictionary, a thesaurus and a corpus, and extracted the semantic polarities of words by regarding semantic polarities of words on the network as spins of electrons [7]. Goto et al. proposed a method for improving the performance of the polarity lexicon extraction based on Takamura et al.'s spin model [8]. Ikeda et al. propose a machine learning based method of sentiment classification of sentences by using the polarities of words [9]. Also, in these years, a large number of studies have been made on how to evaluate answers submitted into Q&A sites. Kuriyama et al. proposed a method of evaluating answers by using answerers' records of postings to a Q&A site [10] [11]. Ishikawa et al. proposed a method of evaluating answers by using machine learning techniques [12]. However, there are few studies whether the evaluation of answers are affected by the order of polar words. On the other hand, Kido reported that rhetorical structure is affected by the order of non-fact sentence (e.g., comments and opinion sentences) while rhetorical structure is less affected by the order of fact sentence (e.g., sentences that report actual survey figures) [13]. However, Kido did not consider the order of polar words in reports.

III. YAHOO! CHIEBUKURO

In this study, we used the data of Yahoo! chiebukuro for observation and examination. In Japanese, chiebukuro means "bag of wisdom". The data of Yahoo! chiebukuro was published by Yahoo! JAPAN via National Institute of Informatics in 2007 (http://research.nii.ac.jp/tdc/chiebukuro.html). This data consists of about 3.11 million questions and 13.47 million answers, which were posted on Yahoo! chiebukuro

 ISBN: 978-1-61208-285-1

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	number of questions	number of questioners	number of answers	number of answerers
PC	171848	43493	474687	27420
social issues	78777	13259	403306	25766
all 286 categories	3116009	165064	13477785	183242

TABLE II. THE EXTRACTION RESULT OF ANSWERS WHERE THE FIRST POLAR WORDS WERE NEGATIVE WORDS (SOCIAL ISSUE CATEGORY IN THE DATA OF YAHOO! CHIEBUKURO).

answers	number of answers	best answer ratio
all the answers in social issue category	403306	19.5
answers where the first polar words were negative words	162878	19.5

from April/2004 to October/2005. In the data, each question has at least one answer because questions with no answers were removed. Each user can submit his/her answer only one time to one question. Each questioner is requested to determine which answer to his/her question is best. The selected answer is called the *best answer*. 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.

In order to detect answers which include negative words, we use an opinion extraction tool [14]. This tool was developed by Knowledge Clustered Group in National Institute of Information and Communications Technology (NICT) and released in September/2011. This tool detects opinion expressions in given sentences and outputs the polarities of them (positive/negative polarity) when they have the polarities. Knowledge Clustered Group in National Institute of Information and Communications Technology (NICT) also developed and released model data for the opinion extraction tool [15]. This model data consists of about 35000 words (10000 positive words and 25000 negative words). These words were extracted from 20000 sentences in Web document corpus. This model data is useful to detect negative words in answers precisely. For example, when we apply this tool to (A1), the opinion extraction tool detect negative words in second sentence "*jimin tou nado ga matomo na kyougi, touron mo naku kyoukou ni kokki kokka wo kimeta.* (The Liberal Democratic Party and other political parties set Kimigayo as Japan's national anthem, without sufficient discussions in the Diet.)" and third sentence "*konna daiji na koto wo jibun tachi no omou toori ni kyoukou shita noda.* (It was so serious, however, they got their way.)".

(Q1) *Hinomaru kimigayo wo kyohi suru hito ni shitsumon desu. puro yakyu nado no kansen no toki mo yahari kyohi desu ka? K-1 nado ha takoku no kokka ni tsuite mo kiritsu wo motome rare masu ga donoyouna kanngae de dou koudou suru no desu ka?* (I have a question to persons who deny Hinomaru and Kimigayo. Do you deny them even when you watch professional baseball games? In case of sport games like K-1, we are asked to stand up during singing of the national anthem, not only ours but other's national song. Tell me what you think and how you act.)

(A1) *touzen kyohi desu. jimin tou nado ga matomo na kyougi, touron mo naku kyoukou ni kokki kokka wo kimeta. konna daiji na koto wo jibun tachi no omou toori ni kyoukou shita noda. motto shintyo ni kimeru hitsuyou ga atta.* (Of course, I refuse. The Liberal Democratic Party and other political parties set Kimigayo as Japan's national anthem, without sufficient discussions in the Diet. It was so serious, however, they got their way. We should discuss this issue more careful.)

Both (Q1) and (A1) were submitted to social issues category in Yahoo! chiebukuro. (A1) was an answer to (Q1). In case of (A1), the opinion extraction tool determines the second sentence is the first sentence which include an opinion expression, and the polarity is negative. As a result, (A1) is determined to be an answer where the first polar word was a negative word. By using this opinion extraction tool, we extract answers where the first polar words were negative words from the data of Yahoo! chiebukuro.

We applied this tool to 403306 answers submitted to social issues category in Yahoo! chiebukuro, and obtained 162878 answers where the first polar words were negative words. Table II shows the result of this extraction. As shown in Table II, in social issue category, the best answer ratio of answers where the first polar words were negative words is similar to that of all the answers. As a result, it may be said that the evaluations of answers in Yahoo! chiebukuro were less affected by whether the first polar words are negative words.

IV. USERS SUBMITTED MANY ANSWERS WHERE THE FIRST POLAR WORDS WERE NEGATIVE WORDS

In this study, we detect users who submitted many answers where the first polar words were negative words to Yahoo! chiebukuro and investigate whether they got good evaluations of their answers. In order to detect and discuss users who submitted many answers where the first polar words were negative words, we test one hypothesis, Hypothesis NWFA:

 ISBN: 978-1-61208-285-1

TABLE III. THE RELATION BETWEEN THE BEST ANSWER RATIO AND THE AVERAGE NUMBER OF SENTENCES

	the average number of sentences		
	1.0 – 3.0	3.0 – 6.0	6.0 –
number of users	8	13	12
best answer ratio of answers where the first polar words were negative words	21.7	25.3	33.3

Hypothesis NWFA If user i submitted not many answers where the first polar words were negative words, we would expect that user i submitted at most $N_{NWFA}(i)$ answers where the first polar words were negative words.

$$N_{NWFA}(i) = P_{NWFA} \times ans(i) \quad (1)$$

where $ans(i)$ is the number of user i's answers and P_{NWFA} is the probability that one randomly selected answer is an answer where the first polar word is a negative word. As a result, P_{NWFA} is

$$P_{NWFA} = \frac{N_{NWFA}}{N_{ans}} \quad (2)$$

where N_{ans} is the number of all the answers and N_{NWFA} is the number of answers where the first polar words are negative words. As shown in Table II, N_{ans} and N_{NWFA} of social issue category in Yahoo! chiebukuro are 162878 and 403306, respectively. As a result, P_{NWFA} of social issue category is 0.404.

When this hypothesis is rejected by a one-sided binomial test, we determine that user i submitted many answers where the first polar words are negative words.

V. EXPERIMENTAL RESULTS AND DISCUSSIONS

We applied the detection method based on Hypothesis NWFA to 25766 users who submitted one or more answers to social issue category in Yahoo! chiebukuro. In this study, the significant level of Hypothesis NWFA was set to 0.000000005. It was extremely low because we intended to detect users who submitted extremely many answers where the first polar words were negative words. Our method detected 33 users and the best answer ratio of their answers is 25.4%. It is higher than the best answer ratio of all the answers submitted to social issue category in Yahoo! chiebukuro (19.5%). In face-to-face communication, persons who tend to speak stories where the first polar words are negative words often get poor evaluations of their stories. On the other hand, in Q&A sites, answerers who tend to write answers where the first polar words are negative words often get good evaluations of their answers. As a result, it may be said that answers submitted to Q&A sites were evaluated based on whether explanations were detailed and informative, rather than whether the first polar words were negative words.

Next, we discuss the relation between the best answer ratio and the average number of sentences in these 33 users' answers. We classified the detected 33 users into three groups depending on the average number of sentences in their answers indicated below:

group A less than 3.0
group B not less than 3.0 and less than 6.0
group C not less than 6.0

Table III shows the number of users in each group and the best answer ratio of their answers where the first polar words were negative words. As shown in Table III, the best answer ratio is often high when the average number of sentences in answers is large. It is because, we think, explanations consisted of many sentences is often more detailed and informative than those consisted of few sentences. As a result, it also may be said that answers submitted to Q&A sites were evaluated based on whether explanations were detailed and informative, rather than whether the first polar words were negative words. For example, user 273731 submitted 203 answers where the first polar words were negative words to social issue category. Because the average number of sentences in his/her answers was 6.7, user 273731 was classified into group C. The explanation of user 273731's answers were generally detailed and informative. Possibly because of it, the best answer ratio of user 273731's answers is 45.3 %. It is higher than the average of the best answer ratio of answers submitted into social issue category (19.5%). On the other hand, user 169784 submitted 131 answers where the first polar words were negative words to social issue category. Because the average number of sentences in his/her answers was 2.8, user 169784 was classified into group A. The explanation of user 169784's answers were generally short and not informative. Possibly because of it, the best answer ratio of user 169784's answers is 15.6 %. It is lower than the average of the best answer ration of answers submitted into social issue category (19.5%).

VI. CONCLUSION AND FUTURE WORK

In this study, we investigated answers where the first polar words were negative words and found that the evaluations of answers in Yahoo! chiebukuro were less affected by whether the first polar words were negative words. Furthermore, we investigated users who submitted many answers where the first polar words were negative words to Yahoo! chiebukuro, and found that these users often get good evaluations of their answers in Yahoo! chiebukuro. We think that answers submitted to Q&A sites were evaluated based on whether explanations were detailed and informative, rather than whether the first polar words were negative words.

In the future, we intend to investigate whether the evaluations of answers in Yahoo! chiebukuro are affected by whether the first polar words are positive words. Furthermore, we want to investigate various kinds of online documents, for example, messages in blog comments, web-based bulletin boards, and micro blogs.

 ISBN: 978-1-61208-285-1

REFERENCES

[1] M. Sharifi and W. Cohen, "Finding domain specific polar words for sentiment classification," in *the LTI Student Research Symposium*, 2008. [Online]. Available: http://www.cs.cmu.edu/~mehrbod/polarity_08.pdf [retrieved: May, 2013]

[2] *Yahoo! Answers*, Yahoo!, 2005. [Online]. Available: http://answers.yahoo.com/ [retrieved: May, 2013]

[3] *Yahoo! chiebukuro*, Yahoo! JAPAN, 2004. [Online]. Available: http://chiebukuro.yahoo.co.jp/ [retrieved: May, 2013]

[4] *Oshiete! goo*, NTT Resonant Incorporated, 2000. [Online]. Available: http://oshiete.goo.ne.jp/ [retrieved: May, 2013]

[5] *Hatena*, Hatena Co., Ltd., 2005. [Online]. Available: http://q.hatena.ne.jp/ [retrieved: May, 2013]

[6] *OKWave*, OKWave, 2000. [Online]. Available: http://okwave.jp/ [retrieved: May, 2013]

[7] H. Takamura, T. Inui, and M. Okumura, "Extracting semantic orientations using spin model," in *Transactions of Information Processing Society of Japan*, vol. 47, no. 2, Feb. 2006, pp. 627–637.

[8] T. Goto, Y. Kabashima, and H. Takamura, "Extracting semantic orientations using lexical networks: Performance improvement from the viewpoint of statistical mechanics," in *Technical Report of The Institute of Electronics, Information and Communication Engineers (IEICE) on Information-Based Induction Sciences and Machine Learning (IBISML)*, vol. 110, no. 265, Oct. 2010, pp. 19–25.

[9] D. Ikeda, H. Takamura, and M. Okumura, "Learning to shift the polarity of words for sentiment classification," in *Transactions of the Japanese Society for Artificial Intelligence*, vol. 25, no. 1, Jan. 2010, pp. 50–57.

[10] K. Kuriyama and N. Kando, "Analysis of questions and answers in q&a site (2) - based on document structures and attributes -," in *Technical Report of Information Processing Society of Japan (IPSJ)*, vol. 2009-FI-96, no. 3, Nov. 2009, pp. 1–8.

[11] K. Kuriyama and N. Kando, "Analysis of questions and answers in q&a site (3) - predicting best-answers based on users' histories -," in *Technical Report of Information Processing Society of Japan (IPSJ)*, vol. 2010-FI-97, no. 7, Jan. 2010, pp. 1–8.

[12] D. Ishikawa, T. Sakai, Y. Seki, K. Kuriyama, and N. Kando, "Automatic prediction of high-quality answers in community qa," in *Joho Chishiki Gakkaishi (Japan Society of Information and Knowledge)*, vol. 21, no. 3, Sep. 2011, pp. 362–382.

[13] M. Kido, "The influence of sentence ordering and sentence function on rhetorical structure : the ordering of fact and non-fact sentence," in *University of Tshukuba International Student Center Journal of Japanese language teaching*, vol. 12, Feb. 1997, pp. 1–10.

[14] *Opinion extraction tool (version 1.2)*, Knowledge Clustered Group of National Institute of Information and Communications Technology (NICT), 2012. [Online]. Available: http://alaginrc.nict.go.jp/opinion/ [retrieved: May, 2013]

[15] *C-3 Model for opinion extraction tool (version 1.2)*, Knowledge Clustered Group of National Institute of Information and Communications Technology (NICT), 2012. [Online]. Available: http://alaginrc.nict.go.jp/opinion/ [retrieved: May, 2013]

 ISBN: 978-1-61208-285-1

An Analysis of Unsounded Code Strings in Online Messages of a Q&A Site and a Micro Blog

Kunihiro Nakajima, Subaru Nakayama, Yasuhiko Watanabe, Kenji Umemoto, Ryo Nishimura, Yoshihiro Okada
Ryukoku University
Seta, Otsu, Shiga, Japan
Email: {t13m071, t090433}@mail.ryukoku.ac.jp, watanabe@rins.ryukoku.ac.jp,
t11m074@mail.ryukoku.ac.jp, r_nishimura@afc.ryukoku.ac.jp, okada@rins.ryukoku.ac.jp

***Abstract*—In this study, we compare answers in a Q&A site with messages in a micro blog and discuss how we use unsounded code strings at the end of online messages. We first show that unsounded code strings at the end of answers in a Q&A site are used not only smooth communication but an other purpose, minimum length limit avoidance. Next, we show that the length of unsounded code strings at the end of answers in a Q&A site, which are used for smooth communication, have a similar distribution pattern to those of messages in a micro blog. On the other hand, the length of unsounded code strings used for minimum length limit avoidance have a different distribution pattern. In this study, we used the data of Yahoo! chiebukuro, a widely-used Japanese Q&A site, and twitter for observation and examination.**

***Keywords*—unsounded code string; micro blog; twitter; Q&A site; Yahoo! chiebukuro.**

I. INTRODUCTION

We often find consecutive unsounded marks and characters are used at the end of online messages, such as mails, chattings, and questions and answers in Q&A sites. As a result, it is important to investigate how these expressions were used.

(exp 1) *sound recorder demo aru teido ha dekiru kedo, yappari Sound Engine ga osusume kana...* (You may be able to do a lot by using sound recorders, however, the one I would like to recommend is Sound Engine...)

(exp 1) is an answer submitted to a Japanese Q&A site, Yahoo! chiebukuro. In this case, periods are used consecutively at the end of it. It is because the answerer of (exp 1) is thought to use the three consecutive periods for expressing his/her opinion gently, in other words, for smooth communication. In this study, we define unsounded marks and characters as *unsounded codes*. Furthermore, we define three or more consecutive unsounded codes as *unsounded code strings*. For example, in Yahoo! chiebukuro, 25 % of answers have unsounded code strings, in other words, three or more consecutive unsounded codes at the end of them. Although unsounded code strings are popular, there are few studies on them. As a result, in this study, we investigate how we use unsounded code strings at the end of online messages. Especially, we compare answers in a Q&A site with messages in a micro blog and discuss how we use unsounded code strings at the end of online messages. We used the data of Yahoo! chiebukuro [1], a widely-used Japanese Q&A site, and twitter for observation and examination. The results of this study will give us a chance to understand the usage of unsounded code strings, and the purposes and behaviors of users in online communities. Especially, the results could be useful to predict and analyze the impacts of communication constraints on users' messages and communications.

The rest of this paper is organized as follows: In Section II, we surveys the related works. In Section III, we describes how unsounded code strings used at the end of answers in a Q&A site. On the other hand, in Section IV, we describes how unsounded code strings used at the end of messages in a micro blog. Finally, in Section V, we present our conclusions.

II. RELATED WORKS

Emoticons, sometimes called face marks, are a kind of unsounded code strings. First emoticon, smiley face ";-)", was proposed by Scott Fahlman in September 1982 [2]. After his proposal, many emoticons have been used widely in online messages, such as email, chat, and newsgroup posts [3]. As a result, a large number of studies have been made on emoticons.

Many researchers in computational linguistics proposed methods of extracting and classifying emoticons in online messages. Inoue et al. analyzed 1000 sentences in email messages and developed a system which extracted emotional expressions, especially emoticons, embedded in email messages [4]. Nakamura et al. proposed a method of learning emoticons for a natural language dialogue system from chat dialogue data in the Internet [5]. Tanaka et al. proposed methods for extracting emoticons in text and classifying them into some emotional categories [6]. Bedrick et al. proposed robust emoticon detection method based on weighted context-free grammars [7]. Hogenboom et al. showed that sentiment classification accuracy was improved by using manually created emoticon sentiment lexicon [8].

On the other hand, many researchers in social science analyzed how we use emoticons in online messages. Witmer and Katzman reported that women use more graphic accents (emoticons) than men do in their computer-mediated communication (CMC) [9]. Walther and D'Addario showed that emoticons' contributions were outweighed by verbal content [10]. Derks et al. reported emoticons are useful in strengthening the intensity of a verbal message [11]. Byron and Baldridge reported readers were likely to rate sender's emails more likeable if they used emoticons [12]. Harada discussed how Japanese speakers use emoticons for promoting communication smoothly from the viewpoint of politeness

 ISBN: 978-1-61208-285-1

TABLE I. THE NUMBERS OF USERS AND THEIR MESSAGES (QUESTIONS AND ANSWERS) SUBMITTED TO YAHOO! CHIEBUKURO (FROM APRIL/2004 TO OCTOBER/2005).

	number of questioners	number of questions	number of answerers	number of answers
the data of Yahoo! chiebukuro	165,064	3,116,009	183,242	13,477,785

TABLE II. THE NUMBER OF ANSWERERS, ANSWERS, AND BEST ANSWERS IN CASE OF (1) ALL THE ANSWERS IN YAHOO! CHIEBUKURO AND (2) ANSWERS WHICH HAVE UNSOUNDED CODE STRINGS AT THE END OF THEM.

	number of answerers	number of answers	number of best answers
all the answers	183,242	13,477,785	3,116,009
answers which have unsounded code strings at the end of them	89,133	3,242,694	477,462

[13]. Kato et al. analyzed positive and negative emoticons and reported that negative emoticons are misinterpreted more frequently than positive ones [14]. Furthermore, Kato et al. reported that emoticons are used more frequently between close friends than ordinary acquaintances [15].

We think emoticons are a kind of unsounded code strings, however, there are few studies on other kinds of unsounded code strings. As a result, we should investigate not only emoticons but other kinds of unsounded code strings. The results of this study will give us a chance to understand the purposes and behaviors of users in online communities.

III. UNSOUNDED CODE STRINGS AT THE END OF ANSWERS IN A Q&A SITE

In this section, we discuss unsounded code strings at the end of answers submitted to a Q&A site.

Before we define a unsounded code string, we explain the data of Yahoo! chiebukuro, which we used for investigating unsounded code strings in a Q&A site. Yahoo! chiebukuro is a Japanese version of Yahoo! answers and one of the most popular Q&A sites in Japan. In Yahoo! chiebukuro, each user can submit his/her answer only one time to one question. (Each questioner is requested to determine which answer to his/her question is best. The selected answer is called *best answer*.) The data of Yahoo! chiebukuro was published by Yahoo! JAPAN via National Institute of Informatics in 2007 [16]. 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 questions and answers in the data of Yahoo! chiebukuro.

Next, we define an unsounded code and unsounded code strings. In this study, we define that an unsounded code string is three or more consecutive unsounded codes. In this study, unsounded codes are limited to the following marks and characters:

- punctuation marks,
- Greek characters,
- Cyrillic characters, and
- ruled lines.

These marks and characters are generally unsounded when they are used at the end of Japanese sentences. We observed unsounded code strings at the end of answers submitted to Yahoo! chiebukuro, and found they were used for

1) smooth communications

(exp 2) *koko ni kaki shirushita bunmen wo sonomama kanojyo ni misete ageru koto wo osusume shimasu. futari no aida ni shinrai kankei ga kizukete iru nara kitto daijyobu!!!* (You had better show what you described here to your girl friend with no change at all. If you have a trust relationship with her, you don't worry!!!)

2) minimum length limit avoidance

(exp 3) *alumi foiru ni tsutsun de hi no naka ni pon!!!!!!!!!!!!!* (Wrap aluminum foil around and pop it into a fire!!!!!!!!!!!!!)

The minimum length limit was introduced into Yahoo! chiebukuro in May/2004. Due to this limit, users in Yahoo! chiebukuro are prohibited from submitting answers less than 25 multibyte characters long. In this rule, one single byte character is counted as 0.5 multibyte character. In order to avoid this limit, the answerer of (exp 3) used 13 "!" at the end of his/her answer. We may note that, in case of Japanese texts, the length of words and sentences are generally counted by multibyte characters. In this study, single byte characters are counted as 0.5 multibyte characters.

Table II shows the number of answerers, answers, and best answers, in case of all the answers submitted to Yahoo! chiebukuro, and answers which have unsounded code strings at the end of them.

Figure 1 shows the cumulative relative frequency distribution of

- the length of all the answers,
- the length of answers which have unsounded code strings at the end of them, and
- the length of unsounded code strings.

As shown in Figure 1, the median of the length of unsounded code strings at the end of answers is 10 multibyte characters.

 ISBN: 978-1-61208-285-1

TABLE III. THE NUMBER OF ANSWERERS, ANSWERS, AND BEST ANSWERS IN CASE OF ANSWERS THE LENGTH OF WHICH, EXCLUDING UNSOUNDED CODE STRINGS AT THE END OF THEM, WERE (1) LESS THAN 25 MULTIBYTE CHARACTERS AND (2) 25 MULTIBYTE CHARACTERS OR LONGER.

length of answers (excluding unsounded code strings at the end of them)	number of answerers	number of answers	number of best answers
less than 25 multibyte characters	52,998	1,745,797	191,791
25 multibyte characters or longer	77,299	1,496,897	285,671

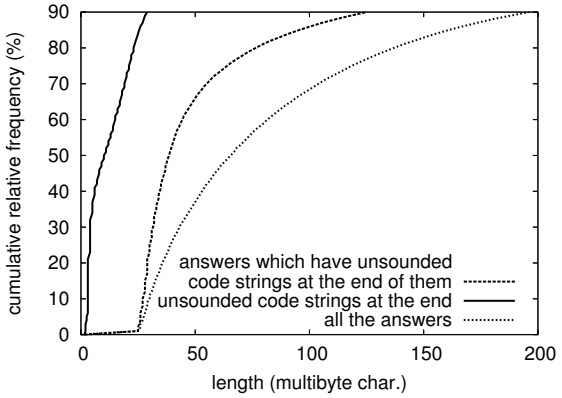


Fig. 1. The cumulative relative frequency distribution of the length of (1) all the answers, (2) answers which have unsounded code strings at the end of them, and (3) unsounded code strings at the end of them.

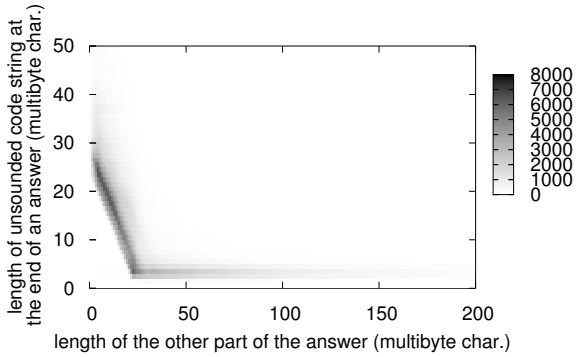


Fig. 2. The heatmap which shows the association between the length of unsounded code string at the end of answers and the other part of the answers.

This value is more than twice the length of unsounded code strings at the end of (exp 1) and (exp 2). We think that it is too long for smooth communication. As a result, we investigate the association between the length of unsounded code string at the end of answers and the other part of them. The result is shown in Figure 2. In Figure 2, the heatmap shows the association between the length of unsounded code string at the end of answers and the other part of the answers. In the heatmap, darker color denotes more frequent data element. The heatmap shows long unsounded code strings at the end of answers are mainly used when the other part of the answers are less than 25 multibyte characters long. Furthermore, unsounded code strings at the end of the answers come in a variety of lengths, however, the sum of the length of unsounded code string at the end and the other part of them, in other words, the length of the answers are frequently 25–30 multibyte characters long. On the other hand, when the other part of answers are more

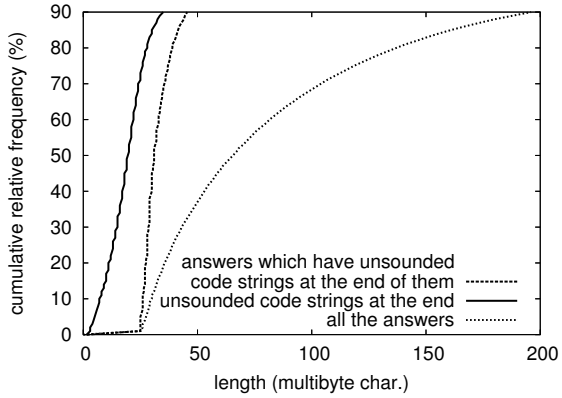


Fig. 3. The cumulative relative frequency distribution of the length of (1) all the answers, (2) answers which are less than 25 multibyte characters long (excluding unsounded code strings at the end of them), and (3) unsounded code strings at the end of them.

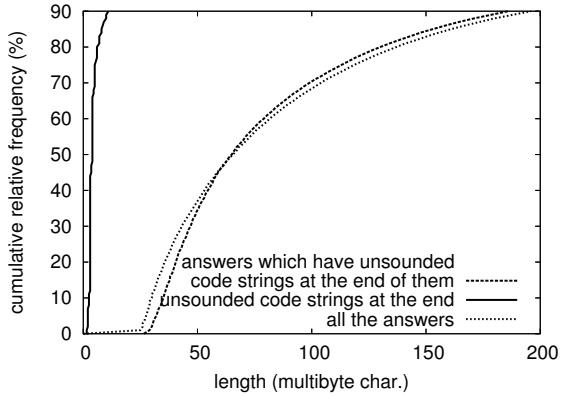


Fig. 4. The cumulative relative frequency distribution of the length of (1) all the answers, (2) answers which are 25 multibyte characters or longer (excluding unsounded code strings at the end of them), and (3) unsounded code strings at the end of them.

than 25 multibyte characters long, unsounded code strings at the end of the answers are mainly 3–4 multibyte characters long, and the answers come in a variety of lengths. It may be said that the usage of unsounded code strings at the end of answers differs greatly depending on whether the other part of the answers are less than 25 multibyte characters long. As a result, we divided answers which have unsounded code strings at the end of them into

- answers the length of which are less than 25 multibyte characters (excluding unsounded code strings at the end of them)
- answers the length of which are 25 multibyte characters or longer (excluding unsounded code strings at

TABLE IV. THE NUMBERS OF NORMAL TWEETS, REPLIES, AND RETWEETS IN TWITTER (FROM NOVEMBER/2012 TO DECEMBER/2012).

type of tweets	number of tweets	
normal	3,823,066	(53.97%)
reply	2,517,781	(35.54%)
retweet	743,336	(10.49%)
total	7,084,183	(100.00%)

TABLE V. THE NUMBERS OF NORMAL TWEETS, REPLIES, AND RETWEETS WHICH HAVE UNSOUNDED CODE STRINGS AT THE END OF THEM (FROM NOVEMBER/2012 TO DECEMBER/2012).

type of tweets	number of tweets	
normal	439,639	(38.15%)
reply	527,257	(45.75%)
retweet	185,547	(16.10%)
total	1,152,443	(100.00%)

the end of them)

and investigated them in the following points:

- the number of answerers, answers, and best answers (Table III),
- the length of answers and unsounded code strings at the end (Figure 3 and Figure 4),

First, we discuss answers the length of which are less than 25 multibyte characters (excluding unsounded code strings at the end of them). In case of these answers, unsounded code strings at the end of them were used for avoiding the minimum length limit. This limit is a special problem in Yahoo! chiebukuro, not introduced into twitter. As a result, we do not compare unsounded code strings for avoiding the minimum length limit with those used in online messages of twitter.

Next, we discuss answers the length of which are 25 multibyte characters or longer (excluding unsounded code strings at the end of them). In case of these answers, unsounded code strings at the end of them were used for smooth communication, not for minimum length limit avoidance. As shown in Figure 4, the length of these answers (excluding unsounded code strings at the end of them) have a distribution similar to those of all the answers submitted to Yahoo! chiebukuro. As a result, it may be said that, when the length of answers are 25 multibyte characters or longer (excluding unsounded code strings at the end of them), the length of these answers are less affected by whether unsounded code strings are used at the end of them. We compare these unsounded code strings with those used in online messages of twitter.

IV. UNSOUNDED CODE STRINGS AT THE END OF MESSAGES IN A MICRO BLOG

In order to compare with unsounded code strings at the end of answers in Yahoo! chiebukuro, we investigate unsounded code strings at the end of messages in twitter. We obtained messages submitted to twitter, in other words, tweets by using the streaming API. However, the streaming API allows us to obtain only 1% of all public streamed tweets because of API restriction. We used the streaming API and obtained 7,084,183 Japanese tweets in three weeks in November and December 2012. These tweets can be classified into three types:

- reply
  A reply to a particular user. It contains "@username" in the body of the tweet.
- retweet
  A retweet is a reply to a tweet that includes the original message.
- normal tweet

A normal tweet is neither reply, nor retweet.

Table IV shows the number of normal tweets, replies, and retweets. From these tweets, we extracted 1,152,443 tweets which have unsounded code strings at the end of them. These 1,152,443 tweets are 16.27% of all the tweets. Table V shows the number of normal tweets, replies, and retweets which have unsounded code strings at the end of them. As shown in Table IV and Table V, 45.75% of tweets which have unsounded code strings at the end of them are replies while 35.54% of all the tweets are replies. As a result, replies have unsounded code strings at the end of them more frequently than other kinds of tweets. It is because each reply is sent to a particular person. When we send a message to a particular person, we generally try to avoid unnecessary frictions with him/her. As a result, we use unsounded code strings at the end of our replies more frequently than other kinds of tweets.

Before we discuss unsounded code strings at the end of tweets, we remove retweets. It is because, messages in retweets are created not by submitters, but by other users. As a result, retweets are inadequate to investigate how we use unsounded code strings at the end of online messages. Figure 5 shows the cumulative relative frequency distribution of

- the length of all the tweets (excluding retweets),
- the length of tweets (excluding retweets) which have unsounded code strings at the end of them, and
- the length of unsounded code strings at the end of tweets (excluding retweets).

In Figure 6, the heatmap shows the association between the length of unsounded code string at the end of tweets and the other part of the tweets. Figure 5 and Figure 6 show unsounded code strings at the end of the tweets are mainly 3–4 multibyte characters long, and the tweets come in a variety of lengths. The length of unsounded code strings at the end of tweets have a similar distribution pattern to those of answers in Yahoo! chiebukuro, which are 25 multibyte characters or longer (excluding unsounded code strings at the end of them). As a result, unsounded code strings at the end of online messages are mainly 3–4 multibyte characters long when they are used for smooth communications with particular persons.

Next, we discuss unsounded code strings at the end of normal tweets and replies, individually. Figure 7 shows the cumulative relative frequency distribution of the length of all the normal tweets, the length of normal tweets which have unsounded code strings at the end of them (excluding unsounded code strings at the end of them), and the length of unsounded code strings at the end of normal tweets. Also, Figure 8 shows the cumulative relative frequency distribution of the length of all the replies, the length of replies which have unsounded code

 ISBN: 978-1-61208-285-1

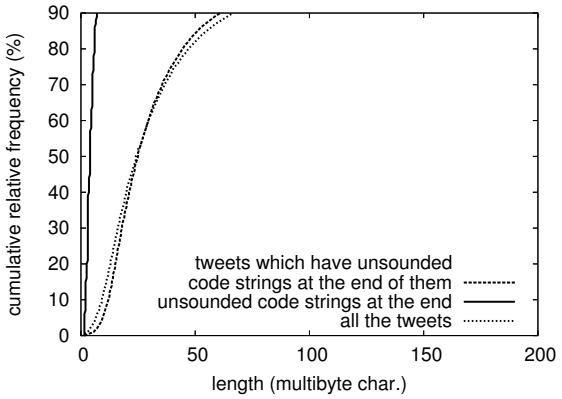


Fig. 5. The cumulative relative frequency distribution of the length of (1) all the tweets, (2) tweets which have unsounded code strings at the end of them, and (3) unsounded code strings at the end of them.

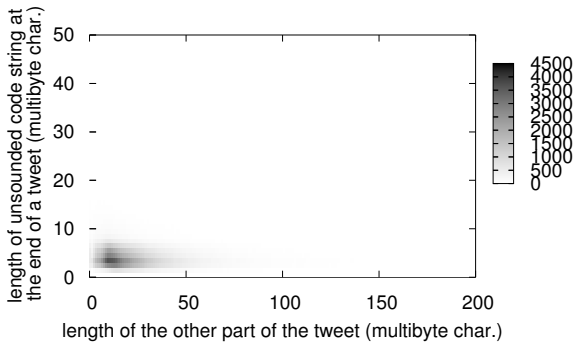


Fig. 6. The heatmap which shows the association between the length of unsounded code string at the end of answers and the other part of the tweets.

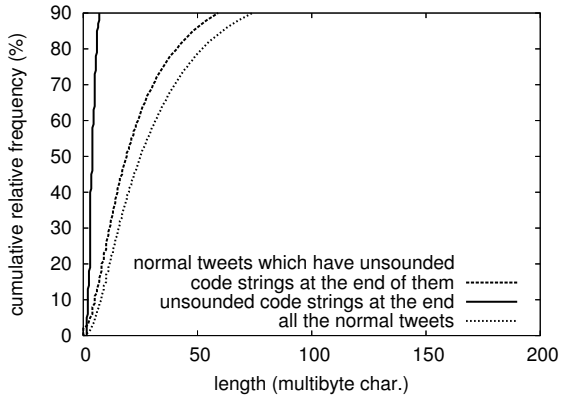


Fig. 7. The cumulative relative frequency distribution of the length of (1) all the normal tweets, (2) normal tweets which have unsounded code strings at the end of them (excluding unsounded code strings at the end of them), and (3) unsounded code strings at the end of them.

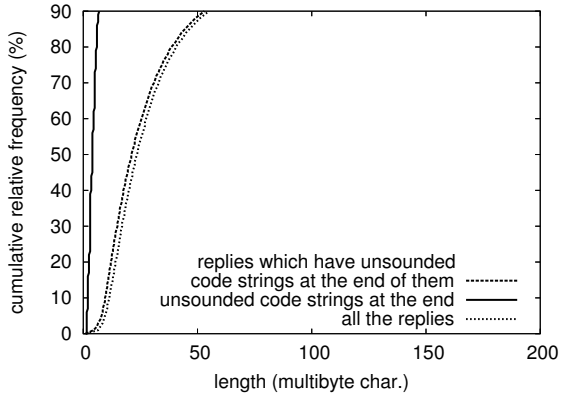


Fig. 8. The cumulative relative frequency distribution of the length of (1) all the replies, (2) replies which have unsounded code strings at the end of them (excluding unsounded code strings at the end of them), and (3) unsounded code strings at the end of them.

strings at the end of them (excluding unsounded code strings at the end of them), and the length of unsounded code strings at the end of replies. As shown in Figure 8, there are few short replies, especially less than 5 multibyte long. It is because each reply includes "@username". Also, as shown in Figure 8, the length of replies which have unsounded code strings at the end of them have a similar distribution pattern to the length of all the replies. It may be said that the length of replies are less affected by whether unsounded code strings are used at the end of them. This result is similar to the result obtained when we investigated answers in Yahoo! chiebukuro. The length of answers in Yahoo! chiebukuro, which are 25 multibyte characters or longer (excluding unsounded code strings at the end of them), are less affected by whether unsounded code strings are used at the end of them. In both cases of Yahoo! chiebukuro and twitter, unsounded code strings are used for smooth communication with particular persons. As a result, it may also be said that the length of online messages to particular persons are less affected by whether unsounded code strings for smooth communication are used at the end of them. On the other hand, as shown in Figure 7, the length of normal tweets which have unsounded code strings at the end of them have a slightly different distribution pattern to the length of all the normal tweets. It is because there are many normal tweets each of which was sent to general public, not to a particular person. We think a message to general public, not to a particular person, tend to be long because we intend to avoid unnecessary misunderstanding. On the other hand, a message to a particular person is sometimes short. As a result, the distribution of the length of all the normal tweets shifts to longer ranges than the length of normal tweets which have unsounded code strings at the end of them.

V. CONCLUSION

In this study, we investigated unsounded code strings at the end of answers in Yahoo! chiebukuro and tweets in twitter. Although unsounded code strings are popular, there were few studies on them.

In twitter, unsounded code strings at the end of tweets are used for smooth communication. On the other hand, in Yahoo! chiebukuro, unsounded code strings at the end of answers are used for not only smooth communication but minimum length limit avoidance. The minimum length limit is a special problem in Yahoo! chiebukuro, not introduced into twitter. We showed that the usage of unsounded code strings at the end of answers in Yahoo! chiebukuro differs greatly depending on

 ISBN: 978-1-61208-285-1

whether answers are longer than the minimum length limit. When answers are longer than the minimum length limit, unsounded code strings at the end of them are used for smooth communication. In this case, the length of the unsounded code strings at the end of answers have a similar distribution pattern to the length of unsounded code strings at the end of tweets. Unsounded code strings at the end of the tweets in twitter and answers in Yahoo! chiebukuro, which are longer than the minimum length limit, are mainly 3–4 multibyte characters long. Furthermore, we showed the length of replies in twitter and answers in Yahoo! chiebukuro, which are larger than the minimum length limit, are less affected by whether unsounded code strings are used at the end of them.

In this study, we analyzed and compared unsounded code strings only in answers in Yahoo! chiebukuro and tweets in twitter. However, it is not enough to obtain general knowledge about unsounded code strings. It is because both of Yahoo! chiebukuro and twitter have character length limits: Yahoo! chiebukuro has a minimum character length limit, on the other hand, twitter has a maximum character length limit. As a result, we intend to analyze unsounded code strings in a computer aided communication media which has no character length limit.

REFERENCES

[1] *Yahoo! chiebukuro*, Yahoo! JAPAN, 2004. [Online]. Available: http://chiebukuro.yahoo.co.jp/ [retrieved: May, 2013]

[2] S. Fahlman. (2012) Smiley:30 years old and never looked happier! [Online]. Available: http://www.cs.cmu.edu/smiley/

[3] H. Nojima, "(smily face) as a mean for emotional communication in networks," in *Proc. IPSJ summer programming symposium*, 1989, pp. 41–48.

[4] M. Inoue, M. Fujimaki, and S. Ishizaki, "System for analyzing emotional expression in e-mail text: collection, classification, and analysis of emotional expressions," in *Technical Report of IEICE on Thought and Language (TL)*, vol. 96, no. 608, 1997, pp. 1–8.

[5] J. Nakamura, T. Ikeda, N. Inui, and Y. Kotani, "Learning face marks for natural language dialogue systems," in *Proc. 2003 International Conference on Natural Language Processing and Knowledge Engineering*, 2003, pp. 180–185.

[6] Y. Tanaka, H. Takamura, and M. Okumura, "Extraction and classification of facemarks," in *Proceedings of the 10th international conference on Intelligent user interfaces*, 2005, pp. 28–34.

[7] S. Bedrick, R. Beckley, B. Roark, and R. Sproat, "Robust kaomoji detection in twitter," in *Proceedings of the Second Workshop on Language in Social Media*, 2012, pp. 56–64.

[8] A. Hogenboom, D. Bal, F. Frasincar, M. Bal, F. de Jong, and U. Kaymak, "Exploiting emoticons in sentiment analysis," in *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, 2013, pp. 703–710.

[9] D. F. Witmer and S. L. Katzman, "On-line smiles: Does gender make a difference in the use of graphic accents?" *Journal of Computer-Mediated Communication*, vol. 2, no. 4, 1997. [Online]. Available: http://jcmc.indiana.edu/vol2/issue4/witmer1.html

[10] J. B. Walther and K. P. D'Addario, "The impacts of emoticons on message interpretation in computer-mediated communication," *Social Science Computer Review*, vol. 19, no. 3, pp. 324–347, 2001.

[11] D. Derks, A. E. R. Bos, and J. von Grumbkow, "Emoticons and online message interpretation," *Social Science Computer Review*, vol. 26, no. 3, pp. 379–388, 2008.

[12] K. Byron and D. C. Baldridge, "Email recipients' impressions of senders likeability," *Journal of Business Communication*, vol. 44, pp. 137–160, 2007.

[13] T. Harada, "The role of "face marks" in promoting smooth communication and expressing consideration and politeness in japanese," *the journal of the Institute for Language and Culture*, vol. 8, pp. 205–224, 2004.

[14] S. Kato, Y. Kato, M. Kobayashi, and M. Yanagisawa, "Analysis of the kinds of emotions interpreted from the emoticons used in e-mail," *the journal of Japan Society of Educational Information*, vol. 22, no. 4, pp. 31–39, 2007.

[15] S. Kato, Y. Kato, Y. Shimamine, and M. Yanagisawa, "Analysis of functions of emoticons in e-mail communication by mobile phone: Investigation of effects of degrees of intimacy with partners," *the journal of Japan Society of Educational Information*, vol. 24, no. 2, pp. 47–55, 2008.

[16] *Distribution of "Yahoo! Chiebukuro" data*, National Institute of Informatics, 2007. [Online]. Available: http://www.nii.ac.jp/cscenter/idr/yahoo/tdc/chiebukuro_e.html [retrieved: May, 2013]

 ISBN: 978-1-61208-285-1

A Collaboration Mechanism Between Wireless Sensor Network and a Cloud Through a Pub/Sub-based Middleware Service

Mohammad Hasmat Ullah[1,3]
Sung-Soon Park[1,3]
[1]Department of Computer Science and Engineering
Anyang University,
Anyang, Korea
e-mails: {raju, sspark}@anyang.ac.kr

Jaechun No[2]
[2]Dept. of Computer Software,
Collage of Electronics and Information Engineering
Sejong University,
Seoul, Korea
e-mail: jano@sejong.ac.kr

Gyeong Hun Kim[3]
[3]Gluesys Co., Ltd.
Anyang, Korea
e-mail: kgh@gluesys.com

***Abstract*— Cloud computing has emerged as a new paradigm of computing platform. It covers almost every area of computing and provides platform to most of the data services. On the other hand, Wireless Sensor Networks (WSN) has gained attention for their potential supports and attractive solutions such as environment monitoring, bio-median acknowledgment, healthcare monitoring, industrial automation, etc. Additionally, our virtual groups and social networks are in main role of information sharing. However, this sensor driven data is not available to community groups or cloud environment for general purpose research or utilization yet. If we reduce the gap between real and virtual world by adding this WSN driven data to cloud environment and virtual communities by providing censor driven contents to general researchers, and it can gain a remarkable attention from all over, by giving us the benefit in various sectors. Collaboration between WSN and the cloud environment can achieve this. We have proposed an integrated Publish/Subscribe (pub/sub)-based middleware service for the cloud platform to collaborate with WSN. This collaboration will provide resource, service, and storage with sensor driven data to the community. Furthermore, we have proposed a content-based event matching algorithm to analyze subscriptions and publish proper contents easily. We have evaluated our algorithm which sows better performance comparing with previously proposed algorithms.**

Keywords-Cloud computing; WSN; middleware service; event matching; pub/sub

I. INTRODUCTION

Interests are increasing about WSN for their essentiality. Multiple small sensing nodes gather information and monitor events to provide data processing, which couples the digital world with physical environment. It has been gaining importance for their contribution by sensing processing and communicating in vast areas like environmental monitoring and forecasting, medical, military, transportation, crisis management, bio-median acknowledgment, industrial automation, etc. They allow the interaction between users and physical environment. Although a WSN has unlimited potentiality for numerous application areas, it contains sensor devices with limited sensing capability, low processing power, and poor communication power.

Besides, cloud computing provides unlimited resource, processing power, storage and reliable services. Cloud computing provides access to applications and data from anywhere and anytime. The applications are hosted as "Software as a Service". Only cloud computing can provide unlimited resource, computing power, bandwidth, storage, dedicated servers to access from anywhere anytime to use application like software. If we can utilize both powerful platforms together, we may get benefitted by all means.

Super computer may provide resource and power to process sensor data, but it is not easily available for general use and needs much overhead. Cloud computing can analyze, process and store the vast amount of data collected by sensors and these sensors can be shared by applications and users easily, which is the main reason to collaborate WSN to the cloud. Not only cloud provides powerful computation but also serves with huge amount of storage to store processed sensor data for further use.

We propose an integrated pub/sub-based middleware for cloud platform to collaborate with sensor network. It will monitor the subscriptions for sensor driven data through cloud and will receive sensor produced data, also will encapsulate those data as event and will provide them to appropriate subscribers. This middleware will deliver information to the subscribers, who has subscribed for the sensor driven data through cloud-based application.

To accomplish this, we need an algorithm for event matching, which will provide sensor driven data to subscribers. Our proposed middleware will simplify the integration of sensor network with cloud-based community centric applications. The middleware provides an efficient event matching algorithm to bring appropriate sensor driven data to appropriate users.

[1]This research is supported by WBS (World Best S/W) Development Project, Grants No. 10040957, funded by Ministry of Knowledge Economy Korea, 2011 and by Global IT Development project, Grants No. 10043026, funded by Ministry of Knowledge Economy Korea, 2012.

[2]This work is also supported by the 2008 Sabbatical year project from Anyang University.

 ISBN: 978-1-61208-285-1

In Section II, we review the previous work in this field. Section III illustrates the content-based middleware and describes our system overview, Section IV presents our proposed algorithm, Section V provides experimental methodology and experimental evaluation of content-based event matching algorithm for sensor cloud middleware, and Section VI states the conclusion of our work.

II. RELATED WORKS

So far, no many efforts were taken to address the issue of integrating sensor networks to cloud computing-based networks. SGIM [4] addresses the opportunity and challenges for sensor-cloud framework only for analyzing the healthcare sensor data for range predicate case only. Sensor-Grid [5] architecture is already proposed, but grid computing is not same as cloud computing [6] and setting up the infrastructure is not easy. Grid focuses on High Performance Computing (HPC) related applications, whether cloud focuses on general purpose applications, which is easily accessible from anywhere anytime for general users.

Our proposed middleware contains a content-based pub/sub model to deliver sensor driven processed data to subscribers, facilitating exchange between sensor networks and cloud-based networks. Pub/Sub system encapsulates sensor data into events and provides the service of event publications and subscriptions for asynchronous data exchange. The most notable pub/sub systems implemented in recent years are:

The MQTT-S [7] is a topic-based pub-sub protocol that hides the topology of the sensor network and allows data to be delivered based on interests rather than individual device addresses. It allows a transparent data exchange between WSNs and traditional networks and even between different WSNs. Mires [8] is a pub/sub architecture for WSNs. Basically sensors only publish readings if the user has subscribed to the specific sensor reading. Subscriptions are issued from the sink node which then receives all publications. Subscriptions are made based on the content of the desired messages in Distance Vector/Dynamic Receiver Partitioning (DV/DRP) [9]. Though subscriptions are flooding over the network, but DV/DRP only publishes data if there are some subscriptions for the specific data.

Several event matching algorithms are proposed to deliver published sensor data or events to subscribers. In Sequential and sub-order [10] algorithm, according to each predicate, searching space is gradually reduced by deleting unsatisfied subscriptions. The second algorithm, sub-order, reduces the expected number of predicate evaluations by analyzing the expected cost differences when subscriptions are evaluated in different orders. If two predicates are same and trying to create a chain in range predicate case, it is difficult to make chain in such scenario. So, it creates heavy overloads while inserting and deleting subscriptions as it has to maintain a complete graph.

III. MIDDLEWARE ARCHITECTURE

A. Pub/Sub Middleware

Our current environmental data monitoring and analyzing system does not provide real-time auto generated data when sensor gets such information about natural calamities just started to take place by passing sensor driven data to cloud environment through some collaborating middleware to share with the community. On the other hand, the researchers who are trying to solve some complex problems need data storage, computational capability, security at the same time to process vast amount of real time data. For example, assume that a team is working on the unusual environmental situation. They plot sensors on some specific regions to monitor the magnitude continuously and use this data for large multi-scale simulations to track the natural calamities along with providing auto generated forecast to the end-users, who has subscribed to know the forecast. This may requires computational resources and a platform for sharing data and results that are not immediately available to the team. Traditional HPC approach like Sensor-Grid model [5] can be used in this case, but setting up the infrastructure as mentioned above is not easy in this environment. Cloud data centers, such as Amazon EC2, can provide resource and platform to keep many copies in a data center and to provide them when needed. Though, they did not address the issue of integrating sensor network with cloud applications, and thus, have no infrastructure to support this scenario. Here, the subscribers need to register their interests to get various environmental states (magnitude, temperature of ionosphere, electromagnetic field, etc.) from sensors for large scale parallel analysis and to share this information with each other for finding useful solutions for their research related problem. So, the sensor data needs to aggregate first, then process and, lastly disseminate based on user's subscriptions.

B. System Overview

In our proposed system, we have a pub/sub-based middleware to make interaction between cloud and a WSN to provide appropriate data to appropriate subscribers. WSN generates real-time data and needs to be processed at the same time. Our proposed middleware connects to such WSNs and receives real-time data, then processes them and prepares those data as events. The sensor data come in many forms, such as raw data and that raw data must be captured, filtered and analyzed in real-time, and also sometimes it should be stored and cached for further use. Pub/Sub-based middleware also has registry, analyzer and disseminator. Subscribers can request for sensor data through cloud API (Application Programming Interface). There may be two kinds of subscription: i) general purpose for end-users or community-based users to get processed data like forecast about earthquake or natural calamities, ii) special purpose for encapsulated data as event for further research.

 ISBN: 978-1-61208-285-1

Simple architecture of our proposed middleware is shown in Fig. 1

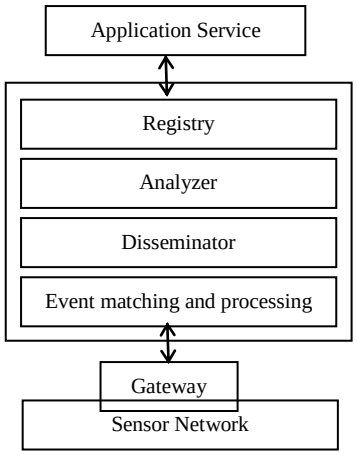


Figure 1. Simple middleware architecture

Interested subscribers can subscribe through cloud application; this subscription will be stored and categorized. The Pub/Sub middleware receives sensor driven data from the gateway between WSN and the middleware, then event matching and monitoring section encapsulates these data as event and passes to the analyzer. The analyzer analyzes subscription types and the disseminator provides corresponding data to subscribed users by matching the registry through the cloud API. The cloud environment may manage these data, process them and may also keep to the repository for further utilization as needed. General user will be able to get user friendly output of these complex data by matching its predicates and by normalizing it.

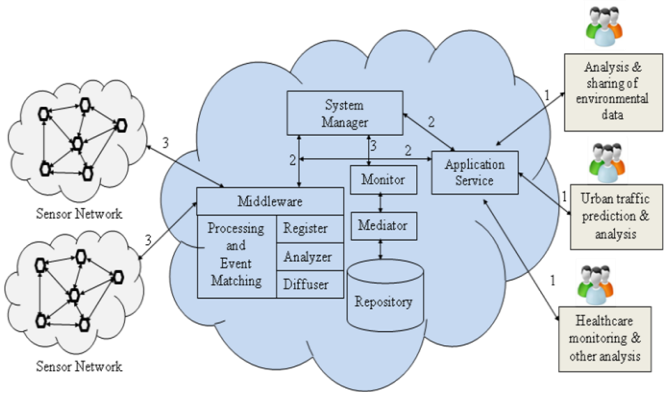


Figure 2. Middleware service integrating WSN and cloud environment.

Figure 2 shows the overview of proposed system. Our proposed middleware service is integrated with cloud platform joining the WSN with cloud. Cloud service provides the application for users to subscribe based on their interests as needed. The proposed event matching algorithm will provide appropriate data efficiently to the subscribers.

IV. EVENT MATCHING ALGORITHM

We need an efficient event matching algorithm for our system to deliver published data to appropriate subscribers. Our target is a cloud-based environmental data monitoring and analyzing system, where researchers can express their interests into attributes, and also general end-users can request for easy to understand outputs. First, we have implemented to support range predicates to cover multi range data only; then, we have extended the algorithm to support overlapping predicates also.

A. *Event Matching*

In our system, a subscription S is expressed by a pair (ID, C_i, P_i), where ID is the subscriber's ID, C is subscription category and P is a set of predicates specifying subscriber's interest.

Here is an example of a subscription and an event in the system. Subscription: S [magnitude, 7(+), ionosphere temperature, 300K(+)] contains two predicates that are joined together to specify a discrete value predicate; here, magnitude 7(+) represents 7 and more alternately ionosphere temperature 300K(+) indicates from 300K to max, i.e., P_1 = magnitude >= 7 and P_2 = ionosphere temperature >= 300K. We also can express it as 6.9 < magnitude < 8 and 299K < temperature < 500K. Let event e be; e: [magnitude = 7.6, ionosphere temperature = 350K].

```
1.  C is set of indexes {C1, ,….Cn-1,Cn} where n is no of indexes
2.  Each Ci points to a set of category index or single category S'
3.  P is set of predicates {p1, p2,….pm-1,pm} where m is number of
    predicates in a subscription
4.  Initialize pj = searching predicate
5.  Event E containing set of predicates P' = {p'1, p'2,….p'm-1,p'm}
6.  Procedure Search (pj, C, E, C_out)     search event E in C where
    C_out is output subscription set    ⊳
7.  S_tmp is a temporary set
8.  for each Ci in C     check each category for desired subscription
9.      if (Ci contain⊳ E) then
10.         if (j ≠ m) then
11.             Procedure Search(pj, Ci, E, C_out)
12.         else then    already found
13.             Initializ⊳S_tmp = S'
14.             C_out = C_out U S_tmp
15.             for each p'j in P'
16.                 for each s'r in S_tmp
17.                     if (s'r. p'j doesn't match E. p'j) then
18.                         Delete the subscription from output set
19.                         Delete the subscription from temporary set
20.                     end if
21.                 end for
22.             end for
23.         end if
24.     end if
25. end for
```

Figure 3. Pseudo code for event matching algorithm

An event satisfies a subscription only if it satisfies all predicates in the subscription. Here, the event [magnitude = 7.6, ionosphere temperature = 350K, 375K] satisfies the subscription S as our proposed method supports discrete predicate values also. So, the matching problem is: Given an event e and a set of predicates in subscription set S. We need to find all subscriptions in set S that are satisfied by e. Our middleware supports various expressions of predicates. First, "(data >= LV || data <= UV)" [here LV = lower value and UV = upper value] is used when consumers want to know normal patterns of sensed data. Second, "(LV > data || UV < data)" is used when consumers need to receive unusual states of the situation such as natural calamities.

B. Proposed Method

Here, we describe the Category Matching Algorithm (CMA). This algorithm operates in three stages. In the first stage, it preprocesses subscriptions by categorizing them through the predicates corresponding to the relevant properties of events. The basic categorizing idea from statistics is employed to decide the number of category. In the second stage, matching subscriptions or predicates are derived sequentially. All predicates stored in the system are associated with a unique ID. Similarly, subscriptions are identified with subscription ID. Finally, it will store the sensor driven data to knowledgebase for future analysis.

Suppose S is a set of subscriptions, $S = \{s_1, s_2, \ldots s_{n-1}, s_n\}$, where n is total number of subscriptions and P is a set of predicates in S, $P = \{p_1, p_2, \ldots p_{m-1}, p_m\}$, where m is the total number of predicates in a subscription. In our system, we have two predicates in a subscription (i.e., data > LV and data < UV) and these two predicates are used to categories the subscriptions. We define a set S' that contains all the subscriptions of S sorted by LV value in ascending order. Then, we define a categorizing sequence (mC_1, $mC_2, \ldots mC_g$). The categorizing space, denoted by SP (S', c), is defined as the set containing all such category sequences over S' and c. Now, each $mC_{i=1\ldots c} \in SP$ (S', c) contains k = n/c subscriptions; that are why category index is created for each $cI_i \in mC_{i=1\ldots c}$. Here, this categorizing sequence is called almost balanced categorizing sequence since every category contains same number of subscriptions except the last one which may or may not contain the same number of subscriptions. It depends on the value of c and n.

When categorizing of subscriptions is done in the above way, first predicate of an event is compared with category index $cI_1 \in mC_1$ and, if any match found then second predicate is compared with category indexes $hI_i \in MC_{i=1\ldots h}$. This way all categories are found that matches with event data. Finally, sequential matching is done in the selected categories to find the subscriptions that are satisfied by all predicates in the event.

V. EVALUATION

Our experimental methodology and simulation results are presented in this section. We have compared our proposed method with sequential sub-order [10], forwarding [14], and naïve [10] algorithms. Naive, a baseline algorithm, evaluates the subscriptions independently. Specifically, it evaluates the subscriptions one by one and for each subscription, evaluates its predicates until either one of them becomes false or all of them are evaluated.

A. Experimental Methodology

Due to the lack of real-world application data, it is not easy to evaluate this kind of pub/sub system. Previous works show that in most applications, events and subscriptions follow either uniform or Zipf [10] distribution. We have used both distributions to evaluate our proposed algorithm. We used subscription evaluation cost, which is the average number of predicates that the system evaluates to match an event for the subscription. This is only a rough estimation of the absolute time that the matching process may take, because different operators may have different complexity and even the same operator may take different time slots for different parameters. However, in a long-term average sense, we believe the number of evaluated predicates can well reflect the efficiency of the evaluation process.

B. Experimantal Results

We have compared Naïve, Sequential and sub-order algorithms with our CMA using a uniform distribution. The experiment results of evaluation are given below:

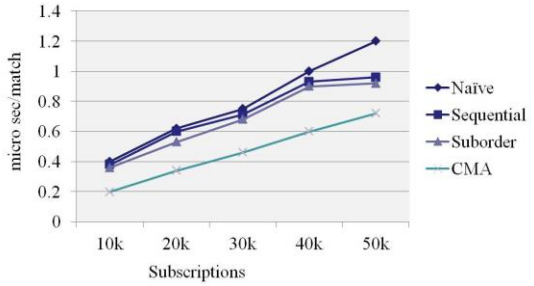


Figure 4. Matching time vs. number of subscriptions.

From first comparison, we can observe that CMA performs better than all other algorithms. For example, with 10K subscriptions and 5000 events, the naïve, sequential, sub-order and CMA evaluate predicates in 0.4, 0.38, 0.36, 0.2 micro sec respectively. Thus, CMA reduces the evaluation cost by 50%, 42%, and 38% as compared to naïve, sequential, and sub-order algorithms, respectively.

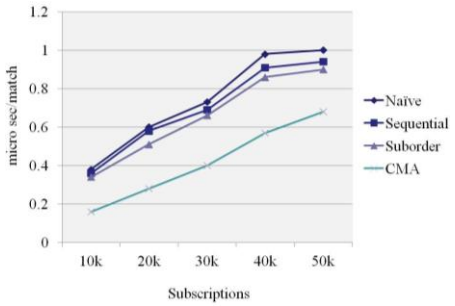


Figure 5. Matching time vs. number of subscriptions (Zipf distribution)

Again, we repeated the experiments with the same parameter settings except the distribution follows Zipf rather than the uniform distribution. The experiment results exhibit similar trends as in first comparison.

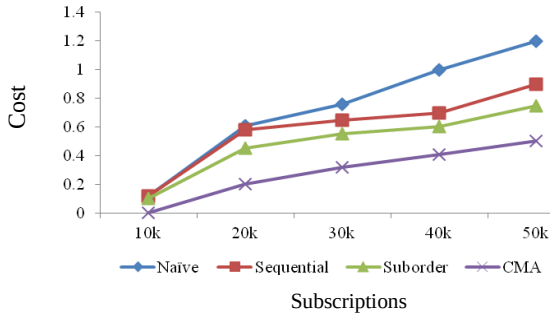


Figure 6. Evaluation cost for multi range predicates

Figure 6 shows that for multiple ranges of predicates, our algorithm performs much better than others. For example, beginning from 10k subscriptions and 5000 events; Naïve, sequential, and sub-order event matching performed 35% ~ 55% poorer than CMA. The cost is evaluated in micro seconds.

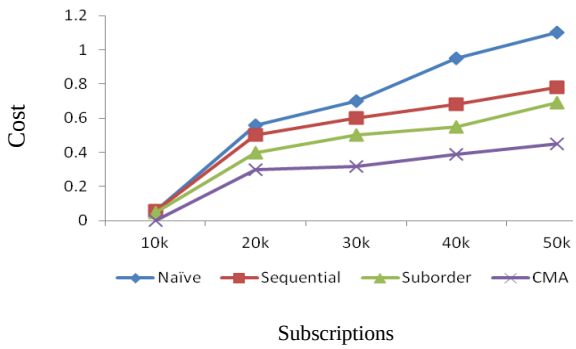


Figure 7. Evaluation cost for overlapping predicates

Figure 7 shows the comparison result for the overlapping predicates. As the subscription increases, CMA shows better and better performance than others. So, it will outperform if the subscriptions are larger.

The above experiments clearly show that our CMA algorithm performs better (in case of uniform and Zipf distribution) than the existing ones in terms of efficiency and scalability.

VI. Conclusions And Future Work

In this paper, we have proposed a pub/sub-based middleware service for the collaboration between sensor networks and the cloud environment for utilizing the ever-expanding sensor data for various next generation community-based sensing applications. For the computational tools needed to launch this exploration, it is more appropriate to build them in the data center of "cloud" computing model than the traditional HPC approaches or Grid approach. We proposed a middleware to enable this by content-based pub/sub model. To deliver published sensor data or events to appropriate users of cloud applications, we also have proposed an efficient and scalable event matching algorithm. We evaluated its performance and also compared it with existing algorithms in a cloud based environment analysis scenario. In the future, we will study further to make the middleware more efficient for distributing sensor driven data to appropriate subscribers and will try to simplify the communication overhead between WSNs and cloud environment.

References

[1] R. Buyya, C. S. Yeo, and S. Venugopal, "Market Oriented Cloud Computing: Vision, Hype and Reality for Delivering IT Services as Computing Utilities," Proc. of 10th IEEE Conference on HPCC, Dalian, China, Sep 2008, pp. 5-13.

[2] K. K. Khedo and R. K. Subramanian, "A Service-Oriented Component-Based Middleware Architecture for Wireless Sensor Networks," International Journal of Computer Science and Network Security, vol. 9, no. 3, Mar 2009, pp. 174-182.

[3] A. Weiss, "Computing in the Clouds," netWorker magazine, ACM Press, vol. 11(4), Dec 2007, pp. 16-25, doi: 10.1145/1327512.1327513.

[4] M. M. Hassan, B. Song, and E. N. Huh, "A framework of sensor-cloud integration opportunities and challenges," Proc. ICUIMC'09, ACM, 2009, pp. 618-626, doi: 10.1145/1516241.1516350.

[5] H. B. Lim, et al., "Sensor Grid: integration of wireless sensor networks and the grid," Proc. of the IEEE Conf. on Local Computer Networks, Nov 2005, Sydney, Australia, pp. 91-98.

[6] D. Harris, "The Grid Cloud Connection (Pt. l): Compare and Contrast," http://www.hpcinthecloud.com/hpccloud/2008-10-08/the_grid-cloud_connection_pt_i_compare_and_contrast.html, retrived: July, 2013.

[7] U. Hunkeler, H. L. Truong, and A. S. Clark, "MQTT-S – A publish/subscribe protocol for Wireless Sensor Networks," IEEE Conf. on COMSWARE, Bangalore, India, Jan 2008, pp. 791-798, doi: 10.1109/COMSWA.2008.4554519.

[8] E. Souto, et al., "Mires: a publish/subscribe middleware for sensor networks," ACM, Personal and Ubiquitous Computing, vol. 10(1), Dec 2005, pp. 37-44, doi: 10.1007/s00779-005-0038-3.

[9] C. P. Hall, A. Carzaniga, J. Rose, and A. L. Wolf, "A content-based networking protocol for sensor networks," Department of Computer Science, University of Colorado, Technical Report, Aug 2004.

[10] Z. Liu, S. Parthasarthy, A. Ranganathan, and H. Yang, "Scalable event matching for overlapping subscriptions in pub/sub systems," Proc. DEBS'07, ACM Press, 2007, pp. 250-261, doi: 10.1145/1266894.1266940.

[11] M. Gaynor, et al., "Integrating wireless sensor networks with the grid," IEEE Internet Computing, vol. 8(4), Jul-Aug 2004, pp. 32–39, doi: 10.1109/MIC.2004.18.

[12] P. Th. Eugster, P. A. Felber, R. Guerraoui, and A. M. Kermarrec, "The many faces of publish/subscribe," ACM Computing Surveys, vol.35(2), June 2003, pp. 114–131, doi: 10.1145/857076.857078.

[13] T. Luckenbach, P. Gober, S. Arbanowski, A. Kotsopoulos, and K. Kim, "TinyREST – A Protocol for Integrating Sensor Networks into the Internet", Proc. of Real-World Wireless Sensor Networks (REALWSN), Stockholm, Sweden, June 2005.

[14] A. Carzaniga and A. L Wolf, "Forwarding in a content-based network," Proc. SIGCOMM, ACM Press, 2003, pp. 163-174, doi: 10.1145/863955.863975.

 ISBN: 978-1-61208-285-1

A Network-based Solution to Kaminsky DNS Cache Poisoning Attacks

Tien-Hao Tsai
Chunghwa Telecom Laboratories,
Yang-Mei, Taiwan, ROC,
skyno717@gmail.com

Yu-Sheng Su
Research Center for Advanced Science and Technology
National Central University
Taoyuan, Taiwan
ncuaddison@gmail.com

Shih-Jen Chen
Institute for Information Industry
Taipei, Taiwan
sjchen@iii.org.tw

Yan-Ling Hwang
School of Applied Foreign Languages
Chung Shan Medical University
Taichung, Taiwan
yanling@csmu.edu.tw

Fu-Hau Hsu
Department of Computer Science and Information Engineering
National Central University
Taoyuan, Taiwan
hsufh@csie.ncu.edu.tw

Min-Hao Wu
Department of Computer Science and Information Engineering
National Central University
Taoyuan, Taiwan
mhwu@csie.ncu.edu.tw

***Abstract*—In this paper, we propose a network-based solution, *Cache Poisoning Solver* (CPS), to defend an organization against the notorious Kaminsky DNS cache poisoning attack. DNS cache poisoning has been used to attack DNS servers since 1993. Through this type of attacks, an attacker can change the IP address of a domain name to any IP address chosen by him. Because an attacker cannot obtain the transaction number and port number of a DNS query sent by a DNS resolver, in order to forge the related DNS response with one of the attacker's IP address, the attacker needs to send many fake DNS responses to the related resolver. All these fake DNS responses map the target domain name to the above attacker's IP. Based on this observation, CPS solves DNS cache poisoning by detecting, recording, and confirming the IP addresses appearing in contents of fake DNS replies. As a result, CPS not only can block DNS cache poisoning attacks but also can identify the malicious hosts, which attackers plan to use to redirect target hosts' traffic. Usually, these malicious hosts are botnet members and used as phishing sites; hence, identifying these bots and disconnecting traffic to them can provide further protection to the hosts in a network. Besides, through the utilization of Bloom Counter and host confirmation, CPS maintains its detection accuracy even when it is bombarded with tremendous fake DNS replies. Experimental results show that with low performance overhead, CPS can accurately block DSN cache poisoning attacks and detect the related bots.**

Keywords-*DNS; resolver; cache poisoning attack*.

I. INTRODUCTION

Domain Name System (DNS) is an important part of the Internet. DNS provides mapping between domain names and IP addresses. With its assistance, network applications, such as web browser, FTP client, and E-mail client and server, can find the location of their communication targets easily. To reduce the processing time, DSN-related payload is usually delivered through UDP packets [10]. However, UDP is a less reliable protocol than TCP. In addition, it is difficult to check the correctness of UDP packet payload. To enhance the reliability of DNS, DNS only accepts answers in a DNS query whose IP address, port number, and Transaction ID (a random 16-bit number) match the related DNS query. DNS cache poisoning is an attack that changes the IP address of a domain name to any IP address chosen by the attacker. In the past, due to the difficulty to obtain the transaction ID and port number of a DNS query, a DNS cache poisoning attack was usually launched through sending a large amount of packets with various port numbers and Transaction IDs to increase its chance to match the port number and transaction ID of an unsolved DNS query.

In 2008, Kaminsky [1] presented a threatening model making the attack easier. Following this model, Hubert and Van Mook [2] shows that, by sending 7000 forged packets per second (around 4.5MB/Sec) to a strict-port DNS resolver, a Kaminsky attack could have a 50% chance to spoof the DNS resolver only in 7 seconds. We call the success probability a cache poisoning attack has the *spoofing probability* of the cache poisoning attack. Fortunately, if 64,000 ports are randomly used, it will cost more than 116 hours to reach the 50% spoofing probability. However, if an attacker increases the rate of issuing forged DNS responses to 4.5 GB/Sec, it could get 50% chance after 7 minutes. Nowadays, the above transmission requirement is easy to be satisfied for most bot masters who can easily control tens of thousands of bots simultaneously. Hence, developing an anti-cache poisoning attack solution that is also robust enough to handle Kaminsky attacks becomes an important issue.

In this paper, we propose a network-based solution, Cache Poisoning Solver (CPS), to defend an organization against the notorious DNS cache poisoning attack. CPS also records IP addresses appearing in fake DNS messages. These IP addresses usually belong to the hosts that are bots of some botnets and perform malicious activities, such as phishing, launching drive-by-download attacks. Thus, CPS further blocks traffic to or from these IP addresses. CPS only records the IP addresses, which appear in many DNS responses, because an authoritative name server only uses one DNS response to notify a resolver the IP address of a domain name. By counting Bloom filter [4], we can effectively observe the incoming frequencies of fake DNS responses in a cache poisoning attack.

The rest of this paper is organized as follows. Section 2 describes the system structure of the CPS. Section 3 analyzes the effectiveness and overhead of the CPS. Section 4 discusses previous work. Section 5 concludes this paper.

 ISBN: 978-1-61208-285-1

II. SYSTEM STRUCTURE

As shown in Fig. 1, there are three major components in CPS: IP collector, analysis crawler, and traffic controller. The IP collector is inside a DNS resolver to collect IP addresses appearing in DNS responses. The traffic controller resides at a router. Based on the malicious IP addresses extracted by the IP collector and analysis crawler, the traffic controller blocks traffic to or from malicious IP addresses. The analysis crawler analyzes the hosts with malicious IP addresses to gather more information about these hosts. This section gives a detailed introduction about these components.

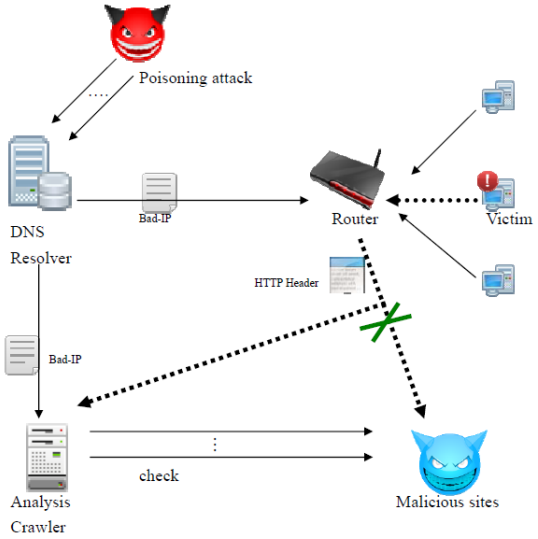


Figure 1. CPS system structure

A. IP Collector

The IP collector on a DNS resolver monitors all DNS queries received by the resolver, and looks over each DNS response to check if it matches a previous DNS query. A DNS response provides the IP address of a domain name, called *response domain name* hereafter. A DNS response matches a DNS query only if they have the same Transaction ID, port number, and IP address. The above matching rule is also adopted by most DNS software to verify a DNS response. We call the triple (Transaction ID, port number, IP address) of a DNS query or DNS response the *DNS packet ID* of the packet hereafter. After a resolver sends a DNS query to an authoritative name server to query the IP address of a domain name, before the server sends the corresponding DNS response to the resolver, the DNS query is called an *unsolved DNS query* and the queried domain name is called an *unsolved domain name*. A DNS response is called a *candidate DNS response*, if there is an unsolved DNS query whose unsolved domain name matches the response domain name of the DNS response. The DNS packet ID of a candidate DNS response may or may not match the DNS packet ID of the related unsolved DNS query. The IP collector only handles candidate DNS responses. Non-candidate DNS responses are ignored by the IP collector. A candidate DNS response, which does not have a matching DNS query is deemed as a *suspected DNS response*. A suspected DNS response could be a *fake DNS response* issued by a DNS cache poisoning attack.

A group of suspected DNS responses that try to set a domain name to the same IP address is called a *fake DNS response set*. Because an authoritative name server does not reply a DNS query with multiple DNS responses, a group of DNS responses that try to answer the same DNS query must try to set the IP address of a domain name to an IP address controlled by an attacker. We call the above IP address a *cheat IP address* of the fake DNS response set. The above domain name is usually contained in the additional section of a DNS response. Even though the domain name may also be contained in the answer section of a DNS response, it appears in old non-efficient cache poisoning attacks and it rarely happens nowadays.

IP collector maintains two lists, *suspicious IP list* and *black IP list*. The former contains the cheat IP addresses of fake DNS response sets whose sizes are greater than a threshold, called *size threshold*. The later contains the IP addresses, which have been confirmed to be used in malicious activities.

IP collector extracts information from suspected DNS responses, such as (1) IP addresses in the answer section and IP addresses (cheat IP addresses) in the addition sections of the DNS responses and (2) target name servers in the authority sessions of the DNS responses. Since fake DNS responses usually contain the IP addresses of bots, intuitively we can collect these IP addresses to unveil a partition of some botnets. After the IP collector extracts the cheat IP address from a suspected DNS response, it adds the cheat IP address to its bloom counter. If the counter of the cheat IP address is greater than the size threshold, it means that someone may be launching a cache poisoning attack to map the cheat IP address to a target domain name. The cheat IP address is added to the suspicious IP list of the IP collector. Whenever 9,000 ~ 10,000 cheat IP addresses are added to the suspicious IP list, the hash tables used by bloom counter are cleared to yield space to store new cheat IP addresses. To prevent the IP address of the target domain name from being poisoned, the IP collector performs a DNS lookup immediately to find the real IP address of the target domain. Hence, later on, even if an attacker sends a DNS response with the correct DNS packet ID, the real IP address of the target domain will not be replaced by a cheat IP address. The cache poisoning attack can be blocked.

The suspicious IP list of CPS only records cheat IP addresses whose corresponding fake DNS response sets contain more than size threshold suspected DNS responses during a period of time. Based on this strategy, CPS can decrease the amount of IP addresses to record in its *suspicious IP list*. We will discuss the size threshold later in this paper.

CPS extracts the following information from a DNS response of a suspected DNS response set, which contains more than size threshold suspected DNS responses.

1. The legal domain, name servers, and the fake IP addresses in the additional and authority session.
2. The counterfeit destination IP corresponding to the domain in the answer session.

 ISBN: 978-1-61208-285-1

B. *Analysis Crawler*

UDP packets are easy to forge and difficult to check the correctness of the sources; hence, an attacker may pollute the suspicious IP list of a resolver with IP addresses, which are not owned by the attacker. Thus, cheat IP addresses will be further analyzed by analysis crawler to avoid misjudging normal IP addresses as malicious IP addresses. Because web sites are frequently involved in various attacks, our analysis focuses on checking whether a suspicious IP is used by a malicious web site. The analysis crawler sends HTTP requests to the IP address to check whether the host with the IP address is a web server. If it is a web server, CPS utilizes [9] to check whether the web site is a benign one or a malicious one. A malicious web site may contain a phishing page or launch drive-by-download attacks. To reduce the number of IP addresses to check, IP addresses in "Alexa Top 500 Global Sites" [3] are skipped and classified as benign IP addresses. Besides, to further improve the performance overhead of the CPS, the CPS only performs the above check when an inner host tries to contact an external host with the IP address in the suspicious IP list. We call this approach *lazy confirmation*. IP addresses that are confirmed to be malicious ones will be added to the *black list* in the IP collector. After the examination, the IP address is removed from the suspicious IP list.

C. *Traffic Controller*

The traffic controller of CPS blocks any IP packet with an IP addresses listed in the black list. When the router receives an IP packet with an IP address listed in the suspicious list, the traffic controller informs the analysis crawler of this event so that the later can perform lazy confirmation to check whether the IP is a benign one.

III. ANALYSIS AND EVALUATION

This section analyzes the probabilities of successfully polluting a DNS cache under various fake DNS response rates and discusses the size threshold that CPS uses to move a cheat IP address into the suspicious IP list. This section also discusses various overhead introduced by CPS.

A. *Analysis*

In this section, we analyze the success probability a cache poisoning attack can have and the time it takes to complete an attack when various approaches are used to launch such an attack. In addition, we also discuss the thresholds of incoming rates and incoming duration of a DNS response set.

The probability that a resolver is polluted in one second of cache poisoning attacks is denoted as P_S.

$$P_S = \frac{W * R}{N * P * I} \qquad (1)$$

`W`: Window of opportunity, a period of time (in seconds), bounded by the response time of the authoritative servers (often 0.1 Sec)

`R` (*incoming rate*): Number of fake DNS responses sent per second. The fake DNS responses belong to the same fake DNS response set.

`N`: Number of authoritative Name Servers for the domain (around 2.5 on average)

`P`: Number of available UDP ports (maximum value is around 64000 as ports under 1024 are not always available)

`I`: Number of Transaction IDs (maximum 65536)

The probability that a resolver is polluted in `T` seconds of cache poisoning attacks is denoted as P_T. `T` is larger than or equal to `TTL`.

$$P_T = 1 - (1 - P_S)^A = 1 - \left(1 - \frac{W * R}{N * P * I}\right)^{(T/TTL)} \qquad (2)$$

According to the Kaminsky method, `TTL` is equal to `W` (Window of opportunity). So, equation (2) becomes:

$$P_T = 1 - \left(1 - \frac{0.1 * R}{2.5 * 64000 * 65536}\right)^{(T/W)} \qquad (3)$$

Fig. 2 shows that the probability of successfully polluting a resolver under different incoming rates. However, some domains are processed by only one authoritative name server. Under this environment, the value of `N` becomes one and the time it takes to pollute a resolver decreases around 40%. Fig. 3 shows the probability that a resolver is polluted under different incoming rates when the number of authoritative name servers is 1 and 2.5.

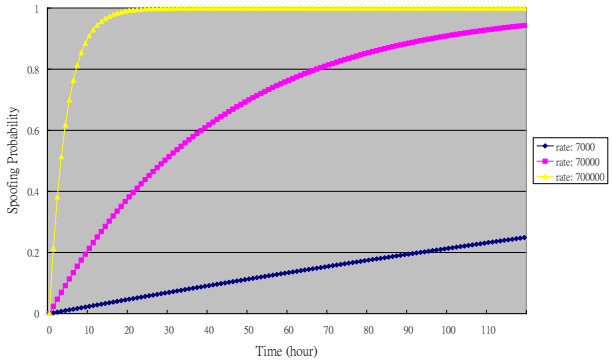


Figure 2. The probability of successfully polluting a resolver under different incoming rates

The suspicious IP list of CPS only records the cheat IP addresses in a fake DNS response set whose size is greater than 5 packets in 50 seconds. In other words, to avoid being recorded by CPS, an attacker cannot send more than 5 fake DNS responses every 50 seconds. We use *5-50 thresholds* to represent the above pair of thresholds.

The result of the 5-50 thresholds can be seen in the following paragraph. If an attacker wants to have a 0.01 success probability when launching a cache poisoning attack without being detected by the CPS, he needs to spend 490 days to continuously send fake DNS responses that map a domain name to the same IP address. However, the above price can only map the IP address of a domain name to the IP address of a bot controlled by the attacker.

 ISBN: 978-1-61208-285-1

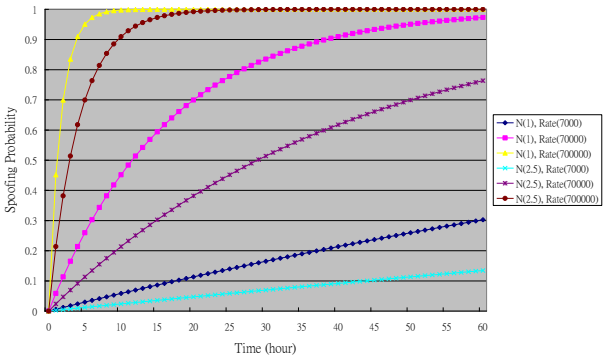


Figure 3. The probability that a resolve is polluted under different incoming rates when the numbers of authoritative name servers are 1 and 2.5

However, if an attacker controls a botnet, the attacker can reduce the attack time by launching a cache poisoning attack through issuing multiple DNS response sets from several bots simultaneously. Each DNS response set maps the same domain name to a different cheat IP address. Each different cheat IP belongs to a different bot of the attacker's botnet. Because the attacker controls all the bots whose addresses appear in the above DNS response sets, no matter, which fake DNS response set successfully changes the IP address of the target domain to the IP address of an attacker's bot, the attacker can redirect victims' traffic to that domain name to his bot.

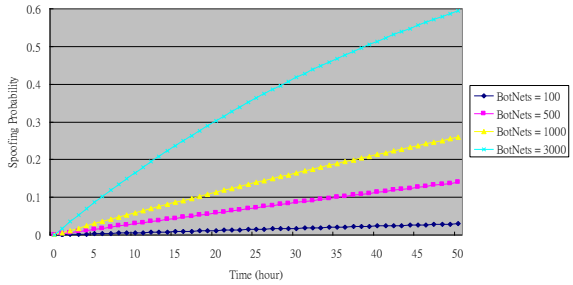


Figure 4. The spoofing probability when 100, 500, 1000, and 3000 DNS response sets are used to attack

Fig. 4 shows the success probability when multiple DNS response sets are used to attack and each DNS response set sends a fake DNS response using its highest incoming rate and incoming duration. In Fig. 4, the numbers of bots involved are 100, 500, 1000, and 3000. As shown in Fig. 4, when 1000 DNS response sets were used, the time it takes to complete a cache poisoning attack with 0.01 success probability is only 700 minutes. Hence, the lower the thresholds are, the more bots the attacker needs to use. In other words, if an attacker only wants to spend 7 minutes to have a 0.01 success probability to fake the IP address of a single domain name, he needs to use 100,000 bots, which is inefficient for the attackers.

B. *Evaluation and Discussion*

We built an IP collector on a DNS resolver with Intel Celeron 2.93GHz CPU and running the Ubuntu 9.10 operating system. To measure the performance overhead, we sent 5000 queries in different time periods of three days. We notice that the extra cost of our IP collector is very little and the usage of CPU is almost not increasing. We simulated attacks by sending fake DNS messages with the rates 0, 2000, 20000, and 120000 packets/sec. The zero rate means no attack. We use the average query time of 5000 DNS queries to represent the query time. Fig. 5 and Table 1 show that our extra overhead is around 3% in normal situation.

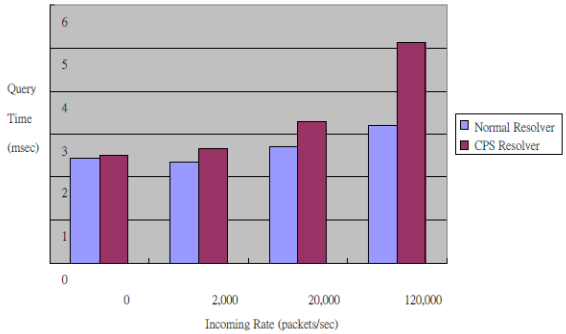


Figure 5. CPS performance overhead

TABLE I. PERCENTAGE OF CPS OVERHEAD

Incoming Rate	CPS Overhead
0	0.03
2,000	0.14
20,000	0.22
12,0000	0.60

C. *Attack Analysis*

UDP packets are easy to forge and difficult to confirm the correctness of the sources. However, sending non-candidate DNS responses (subsection III. *A*) does not have any influence on the bloom filter or of the suspicious IP list of the IP collector, because CPS ignores non-candidate DNS responses. As a result, an attacker may send plenty of candidate DNS responses to cause the analysis crawler busy confirming cheat IP addresses that appear in more than three candidate DNS responses, which in turn causes a DoS attack on CPS. However, with or without CPS, an attacker still can launch a DoS attack upon a local network. Hence, CPS does not make things worse, even though it makes the threshold to complete a DoS attack lower.

IV. RELATED WORK

This section discusses various solutions to the cache poisoning attacks. DNSSEC [6] is one of the most famous solutions of cache poisoning attacks. DNSSEC uses the asymmetric cryptography and verifies the DNS resource record by digital signature (*RRSIG*). This kind of authority needs an upper layer name server approving the public key (*DNSKEY*) by assigning the *DS*. DNSSEC provides extreme security to DNS, but it is not popularly spread.

 ISBN: 978-1-61208-285-1

A response packet often shows the correctness in the authority and additional session. Each session includes the name of the authority server and server's IP addresses. While a domain does not exist, Google name server will respond "No Such answer", but exclude the IP address of the server. Most of these attacks commit mapping a malicious IP to a target name server. Google prevents the spoofing by giving up the unreliable cache data. It's an easy way to defend poisoning but the new protocol is not deployed yet.

Kalafut *et al.* [5] use Autonomous System (AS) number to enhance history and shows that IP address may change but AS number would be stable. However, it has 0.2~3.1% false positive so it's not a robust solution.

DepenDNS [8] is built on client computers and concurrently queries multiple different resolvers to verify a trustworthy answer. It gets more robust answers by sending more queries but decreasing query times is benefit for performance. However, this work may increase much network traffic overhead.

Alexiou et al. [7] used the probabilistic model checker PRISM to model and analyze the Kaminsky DNS cache-poisoning attacks. They used PRISM to introduce a Continuous Time Markov Chain representation of the Kaminsky attack. Moreover they proposed an approach to perform the required probabilistic model checking. Finally, they demonstrated an increasing attack probability with an increasing number of attempted attacks or increasing rate at which the intruder guesses the source-port ID.

The above solutions solve DNS cache poisoning attacks through DNS servers or DNS clients or DNS protocols. There solutions improve the security of current DNS system and make current DNS system more robust against DNS cache poisoning attacks. We believe more solutions that solve the DNS cache poisoning attacks from different viewpoints will be proposed in the future.

V. CONCLUSION

In this paper, a new defending system against Kaminsky DNS cache poisoning is proposed. To solve DNS cache poisoning attacks, CPS detects, records, and confirms the IP addresses appearing in contents of fake DNS responses. The system not only blocks DNS cache poisoning attacks but also identifies the malicious hosts which may be the members of various botnets. As a result, unlike traditional anti-cache poisoning solutions whose main purpose is to protect a DNS server, CPS can also identify bots that try to attack the related network. CPS is effective in detecting cache poisoning attacks and capable of indirectly protecting other resolvers. Experimental results show that the system has low performance overhead. CPS can accurately block DNS cache poisoning attacks and reveal the related bots.

ACKNOWLEDGMENT

Our work is funded by National Science Committee of Taiwan (ROC), and the number of the Project is NSC 101-2221-E-008-028-MY2.

REFERENCES

[1] D. Kaminsky, "Black Ops 2008–It's the end of the cache as we know it," in *Black Hat USA*, 2008.

[2] A. Hubert and R. Van Mook, "Measures for making DNS more resilient against forged answers," RFC 5452, January 2009.

[3] Alexa Top 500 Global Sites, http://www.alexa.com/topsites, [retrieved: June, 2013]

[4] L. Fan, P. Cao, J. Almeida, and A. Z. Broder, "Summary cache: a scalable wide-area web cache sharing protocol," in *IEEE/ACM Transactions on Networking (TON)*, vol. 8, June 2000, pp. 281-293.

[5] A. Kalafut and M. Gupta, "Pollution resilience for DNS resolvers," in *ICC'09. IEEE International Conference on Communications*, June 2009, pp. 1-5.

[6] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS security introduction and requirements," RFC 4033, March, 2005.

[7] N. Alexiou, S. Basagiannis, P. Katsaros, T. Dashpande, and S. A. Smolka, "Formal analysis of the Kaminsky DNS cache-poisoning attack using probabilistic model checking," in *IEEE 12th International Symposium on High Assurance Systems Engineering*, San Jose, CA, November 2010, pp. 94-103.

[8] H. M. Sun, W. H. Chang, S. Y. Chang, and Y. H. Lin, "DepenDNS: Dependable mechanism against DNS cache poisoning," in *Cryptology and Network Security*, vol. 5888, 2009, pp. 174-188.

[9] C. S. Wang, "Shark: Phishing Information Recycling from Spam Mails," M.S. thesis, Dept. Computer Science and Information Engineering, National Central University, Taoyuan, Taiwan, 2010.

[10] Network Ports Used by DNS, http://technet.microsoft.com/en-us/library/dd197515(v=ws.10).aspx, [retrieved: June, 2013]

 ISBN: 978-1-61208-285-1

Advanced OTP Authentication Protocol using PUFs

Jonghoon Lee, Jungsoo Park, Seungwook Jung, and Souhwan Jung
School of Electronic Engineering
Soongsil University
Seoul, Republic of Korea
{ttaz, ddukki86, seungwookj, souhwanj}@ssu.ac.kr

***Abstract*—The One-Time Password (OTP) is an ephemeral password that can be used as a multi-factor authentication method when secure authentication is needed. This OTP is used to counter not only Man-in-the-Browser (MITB) attacks, but also memory hacking attacks. Alternatively, the financial systems use time synchronous OTP using Hash Message Authentication Code (HMAC)-based protocol to support secure authentication. However, it is possible to generate correct OTPs due to potential of stealing sensitive information of the OTP generator through intelligent phishing attacks. Therefore, it needs another scheme to prevent from generating the same OTPs. This paper proposes a new scheme using Physical Unclonable Functions (PUFs) to solve these problems. First, it is impossible to generate the same OTP values because of the physically unclonable features of PUFs. Moreover, sensitive information encrypted by hash and encryption function is exchanged through communication channel. Hence, the proposed protocol provides stronger OTP and robust authentication protocol by adding PUFs in the OTP generator.**

Keywords-OTP; authentication; PUF; HMAC

I. INTRODUCTION

The OTP [1] [2] [3] is an ephemeral password that is used as a strong and secure authentication method. Especially, financial systems utilize the OTP as an additional authentication factor to verify a user's identity. However, as social engineering and phishing attacks become more and more intelligent, various threats still exist. Recent attackers set up specific targets to collect privacy information related to public-key infrastructure (PKI) certificates [4], financial transaction, and the OTP generator, etc. These behaviors have enough availability to cause financial accidents. For instance, some information of SecurID, OTP generator, which is manufactured by RSA Security Inc. [5] was leaked in 2011 because of hacking in their systems. If this information was mixed with user's privacy information, an accident could have occurred. As above instance, there are various attacks. Therefore, it is urgent to make countermeasures to prevent those attacks.

First, we inquire about basic principles of the OTPs and look into their problems before proposing the countermeasure. Consequently, we propose an effective method to prevent its drawbacks. The OTP basically generates random values through an advantage of one-way functions, hash functions, to counter the replay attack. But the eavesdrop, social engineering, or active attacks still exist. There are many kinds of methods for generating OTP. First, an OTP authentication system such as S/KEY One-Time Password System was proposed by Bellcore Inc. [1]. The S/KEY uses hash function (md5 [4], SHA-1 [4], HMAC [4], etc) chains because it is impossible to invert the hash functions [1]. The Time Synchronized OTP [3], such as SecurID, uses the same time information between the server and the client. The Challenge-Response OTP uses the response corresponding with the challenge generated by the server. The Event Synchronized OTP [2] uses the shared counter that increases equally between the server and the client. Nowadays, the Time Synchronized OTP, among many methods, is generally used. However, as attacks become more and more intelligent, many threats still exist. An attacker can generate the same OTP value if he collects enough information of a targeted person and it is available to clone the OTP generator using hardware techniques. Therefore, it is necessary to consider secure measures because of these above reasons. This paper proposes a new secure OTP mechanism using the characteristic of PUF not to generate the same outputs of PUFs.

The remainder of this paper is organized as follows. In Section 2, security threats for OTP are described. Section 3 shows our proposed protocol. Section 4 analyzes the proposed protocol. Finally, Section 5 concludes this paper.

II. SECURITY THREATS

The principle of generating an OTP value is to use the output of a cipher function, such as hash function, using secret key and security token. Figure 1 describes the principle of the OTP.

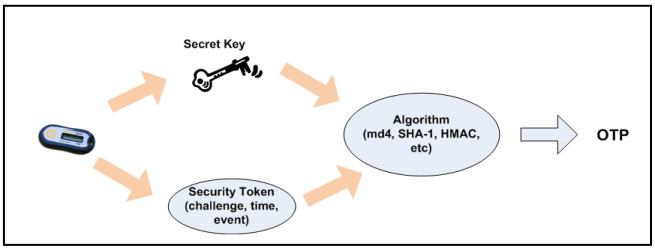


Figure 1. The Principle of Generating OTP

There are three types of the OTP generator approaches: Challenge-Response, Time Synchronous, and Event Synchronous approaches. First, the Challenge-Response OTP generator receives a challenge from the server. The user inserts the challenge, security token, into the OTP generator and then sends the output of the OTP generator, response, to the server. Figure 2 describes the principle of the Challenge-Response OTP. Time/Event Synchronous OTP is the

 ISBN: 978-1-61208-285-1

authentication approach using synchronous time/counter information between the OTP generator and the server as the security token. Figure 3 shows the principle of Time/Event Synchronous OTP. First, a user log in to the server. The server verifies the user's ID and password and request an OTP value to the user. The OTP generator creates the OTP value using time/counter information and secret key. The user sends it to server and the server compares it with the output of the server. Considering the principles of these approaches, we describe the pros and cons of these approaches in Table 1.

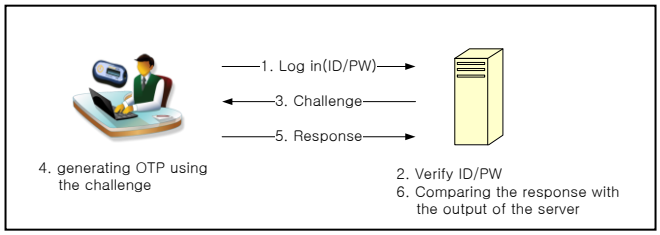


Figure 2. The Principle of Challenge-Response OTP

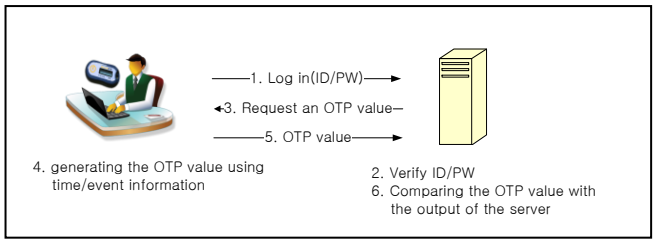


Figure 3. The Principle of Time & Event Synchronous OTP

TABLE I. PROS AND CONS OF APPROACHES GENERATING OTP

	Methods		
	Challenge-Response	***Time Synchronous***	***Event Synchronous***
Security Token	- Challenge from the server	- Time Sync	- Event Sync
Pros	- No need to maintain security token continuously	- Low error rate by users - Low traffic	- Low error rate by users Low traffic
Cons	- to need secure channel - to maintain CRPs	- to correct time sync deviation	- to correct event sync deviation

However, attackers can sufficiently generate the same values if they acquire information related in Security Token and Key using various and elaborate social engineering, phishing, and pharming attacks. It is possible to generate the same values because OTP values are generated by only software methods if they insert the same input information. In addition, it is an enough threat that attackers can clone OTP generators using hardware techniques. Thus, it is not desirable to count these threats through software methods alone. Therefore, by adding hardware components, such as PUFs, it is impossible for attackers to generate the same outputs even though they clone the OTP generator because of characteristics of the PUF. Also, it is impossible to discover its characteristics. In next section, we look into previous OTP protocols and then propose a new protocol using PUF to enhance security.

III. PROPOSED PROTOCOL

We first look into presenting the OTP protocol in financial systems and propose a stronger and more secure OTP protocol. The security model of Time Synchronous OTP generator is presented in Figure 4 [6].

There are three methods to insert Transaction Information in the OTP generator.

ⓐ The user directly inserts the Transaction Information using the keypad of the OTP generator.

ⓑ The user inserts the Transaction Information using sensor, 3D barcode reader, and Quick Response (QR) code reader of the OTP generator.

ⓒ The financial company inserts the Transaction Information through communication channel between the financial company and the OTP generator.

First, the OTP generator verifies the Personal Identification Number (PIN) the user inserts. If it isn't correct, the authentication is denied. If the PIN is correct, it prints the OTP value using the Secret Information (K) stored in the OTP generator, the Synchronous Information and Transaction Information (TI). The user inserts the OTP value in the user's terminal (Web Browser) and sends it to the server of the financial company. The server of the financial company compares this OTP value with the OTP value generated in the server using the function with the same information. If its value is matched, the server allows its transaction. Figure 5 describes the flow of Transaction Verification Protocol using OTP and Table II describes its notations. However, TI is not used in real financial systems. Problems can arise if attackers modify TI using the same OTP value by MITB or eavesdropping attacks. In other words, attacker can remit the user's money to the modified account. Financial systems allow its clients to use the OTP value once a minute to prevent this problem. A potential problem arises if attackers input the OTP value before the user inserts it. However, it is very difficult for the attackers to insert the OTP value through the man-in-the-middle attack (MITM), MITB, and sniffing, etc before the user uses it. To prevent these problems, this paper proposes a robust and secure authentication method using PUFs.

A. *PUFs*

PUFs utilize a hardware characteristic of an integrated circuit (IC) and this characteristic is different for each PUF. In other words, it is impossible to clone the characteristic of IC even if an attacker clones an IC of the PUF. Therefore, it is impossible to generate the same output even though the attacker clones the PUF. Since PUFs generate random outputs corresponding to each input, it is possible to use outputs corresponding to inputs as challenge-response pairs (CRPs). The Arbiter PUF creates two delay paths for each input, and produces an output based on which path is faster [7]. G. E. Suh and S. Devadas [7] also introduced PUF-based

 ISBN: 978-1-61208-285-1

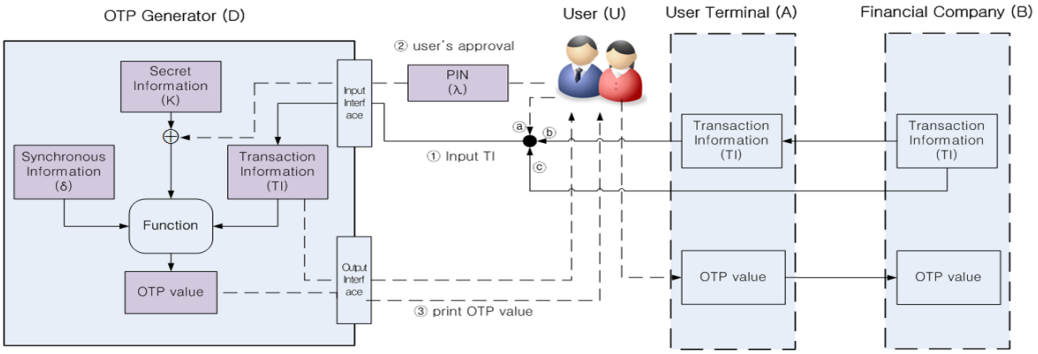


Figure 4. The Security Model of Time Synchronous OTP

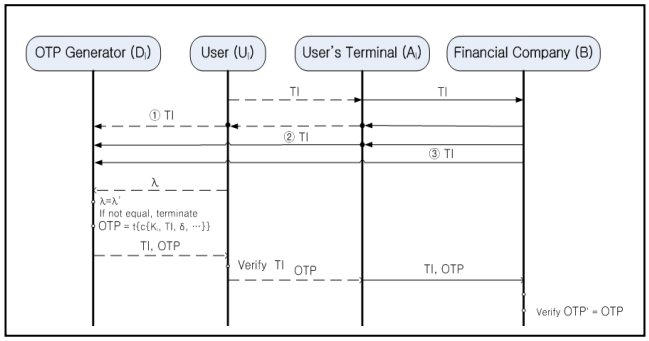


Figure 5. The Previous Protocol Flow

TABLE II. THE NOTATIONS OF THE PREVIOUS PROTOCOL

Notation	*Description*	*Notation*	*Description*
A_i	ith user's terminal	TI	transaction information
B	financial server	OTP	An OTP value
D_i	ith user's OTP generator	c{.}	cipher algorithm
K_i	ith user's secret information	t{.}	truncation algorithm
U_i	ith user	f{.}	OTP generation algorithm
δ	sync information	A→B: M	Send M from A to B through the communication channel
λ	PIN	A ⇢ B: M	Send M from A to B through the channel that user recognizes

authentication and cryptographic key generation with PUFs. The proposed protocol prevents from expecting the outputs of the OTP using the advantage of PUFs. However, the server has to maintain and store many CRPs for PUF-based authentication. L. Kulseng, Z. Yu, Y. Wei, and Y. Guan [8], M. Akgu¨n, M.S. Kiraz, and H. Demirci [9], S. W. Jung and S. H. Jung [10] proposed HMAC-based mutual authentication protocol using PUF in Radio-Frequency Identification (RFID) to solve this problem. By applying that protocol in OTP protocol, the proposed protocol in this paper could solve the above problem and assure strong authentication.

B. *Proposed Protocol*

We assume that the OTP generator is equipped with a communication channel to exchange challenge-response of the PUF. We add a PUF in the OTP generator and use the output of the PUF to generate the OTP values.

Figure 6 depicts the flow of the proposed protocol and Table III shows its notations. The main difference from the previous protocol is to use a PUF to assure secure transactions. The PUF basically utilizes cipher function to secure challenge-response pairs of the PUF and HMAC-based function to check the errors of PUF messages between the OTP generator and the server.

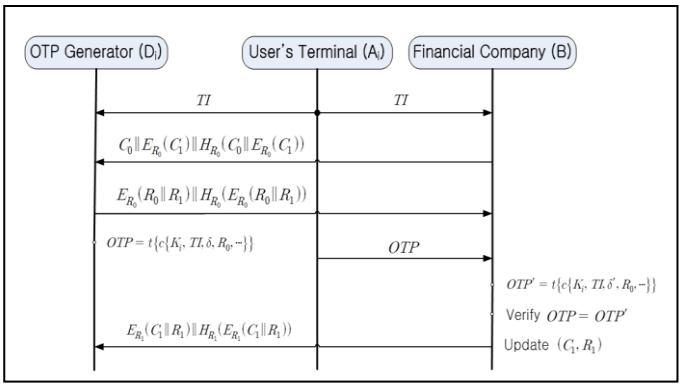


Figure 6. The Proposed Protocol Flow

Step 1: The user sends TI to the server and the OTP generator as a Hello message.

Step 2: The server sends the challenge and next challenge to the OTP generator

$$C_0' \| E_{R_0}(C_1') \| H_{R_0}(C_0' \| E_{R_0}(C_1'))$$

Step 3: The OTP generator sends the response and next response to the server.

$$E_{R_0}(R_0' \| R_1') \| H_{R_0}(E_{R_0}(R_0' \| R_1'))$$

Step 4: The OTP generator generates an OTP value and sends it to the server.

Step 5: The server verifies the OTP value and updates next challenge-response pair. The server sends ACK message after update.

$$E_{R_1}(C_1' \| R_1') \| H_{R_1}(E_{R_1}(C_1' \| R_1'))$$

 ISBN: 978-1-61208-285-1

TABLE III. THE NOTATIONS OF THE PROPOSED PROTOCOL

Notation	*Description*
C_n	nth challenge from the Financial Company
R_n	nth response of PUF from C_n
$E_K(\cdot)$	Encryption Function with K(Secret Key)

The server only stores initial CRP, (C_0, R_0), and updates next CRP, (C_1, R_1) in the authentication process to reduce loads of CRPs. By adding a response of PUF, it is difficult for the attackers to predict and re-create the same value.

IV. ANALYSIS OF THE PROPOSED PROTOCOL

B The attacks we mentioned in Section 2, such as phishing, pharming and social engineering attack, are serious issues. This section analyzes other threats, such as eavesdropping, blocking message, and replay attack.

The proposed protocol prevents eavesdropping attack and secures user information because sensitive values are protected by the cipher and hash function. Furthermore, this protocol also prevents blocking message because the server does not update the CRP unless the server verifies the OTP value from the OTP generator. The replay attack is impossible since this protocol uses fresh CRPs and OTPs every time. Moreover, financial information is sent through secure channel such as SSLv3. The secret information of the OTP generator and the PUF is only shared between the user and the server, thus spoofing attack is impossible unless this information is exposed. As the PUF is Physical Unclonable Function, it is also impossible to clone the OTP generator. Even though an attacker tries to clone an OTP generator using hardware technique, the outputs of the cloned PUF are totally different from an original one because of its characteristic. Therefore, cloning attack is impossible. U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber [11] described the attack modeling on PUFs. This paper presume that an adversary Eve has collected a subset of all CRPs of the PUF, and tries to derive a numerical model from this data using machine learning techniques [11]. Our protocol protects the response of the PUF by encryption. Therefore, it is impossible for an attacker to collect CRPs of the PUF. The hacking memory attack does not have any impact on the OTP generator because the OTP generator does not have to store its output values. This feature of the PUF is the most benefit among its features. However, attacks such as intelligent phishing and pharming still exist as problems. To prevent the above problems, the proposed OTP protocol also uses transaction information that consists of account information, transaction time, and user information, etc.

V. CONCULSION

Existing Time Synchronous OTP protocol uses Secret Information and Sync Information shared between the OTP generator and the server to verify user's transaction in financial systems. It is also used as the multi-factor authentication in other systems. Attacks to acquire user's privacy information through various and intelligent social engineering, phishing attacks have increased in the past years. If attackers effectively use this sensitive information, it causes another financial incident. Many systems use the OTP generator to reduce these threats as a multi-factor authentication method. However, it is possible to clone an OTP generator and generate the same OTP values if an attacker acquires enough information about a user.

This paper introduced a new protocol using PUFs to assure more secure authentication. Moreover, our protocol not only prevent from cloning the OTP generator because of the characteristic of PUFs, but also phishing attack through Transaction Information. However, the proposed protocol requires the OTP generator, which is equipped with a communication channel to exchange information of PUFs. By using the OTP generator equipped with keypad, it is possible to implement a new protocol without communication channel. In conclusion, our protocol enhances security and provides more robust authentication method than existing ones.

ACKNOWLEDGMENT

This research was supported by the MSIP(Ministry of Science, ICT&Future Planning), Korea, under the ITRC(Information Technology Research Center)) support program (NIPA-2013-H0301-13-1003) supervised by the NIPA(National IT Industry Promotion Agency).

REFERENCES

[1] N. Haller, C. Metz, P. Nesser, and M. Straw, A One-Time Password System, RFC 2289 IETF, Feb. 1998, pp. 1-8.

[2] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, HOTP: An HMAC-based One-Time Password Algorithm, RFC 4226 IETF, Dec. 2005, pp. 1-7.

[3] D. M'Raihi, S. Machani, M. Pei, J. Rydell, TOTP: Time-Based One-Time Password Algorithm, RFC 6238 IETF, May. 2011, pp. 1-7.

[4] W. Stallings, Cryptography and Network Security, 4th ed., Pearson Prentice Hall, 2006, pp. 318-372, 419-430.

[5] RSA SecurID, http://www.emc.com/security/rsa-securid.htm.

[6] H. W. Sim, W. J. Kang, and H. Y. Park, An One Time Password based e-Financial Transaction Verification Protocol, TTAK.KO-12.0167 TTA, Dec. 2011, pp. 1-9.

[7] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," Proc. 44th ACM Annual Design Automation Conference 2007, Jun. 2007, pp. 9-14.

[8] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight Mutual Authentication and Ownership Transfer for RFID systems," Proc. IEEE INFOCOM 2010, Mar. 2010, pp. 1-5.

[9] M. Akgün, M.S. Kiraz, and H. Demirci, "Cryptanalysis of Lightweight Mutual Authentication and Ownership Transfer for RFID System," Proc. IEEE Lightweight Security & Privacy: Devices, Protocols and Applications, Mar. 2011, pp. 20-25.

[10] S. W. Jung and S. H. Jung, "HRP: A HMAC-based RFID mutual authentication protocol using PUF," Proc. International Conference on Information Networking 2013, Jan. 2013, pp. 578-582.

[11] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling Attacks on Physical Unclonable Functions," Proceedings of the 17th ACM Conference on Computer and Communications Security, Oct. 2010, pp. 237-249.

 ISBN: 978-1-61208-285-1

HMAC-based RFID Authentication Protocol with Minimal Retrieval at Server

Seung Wook Jung, Souhwan Jung
School of Electronic Engineering
Soongsil University
Seoul, Korea
seungwookj@ssu.ac.kr, souhwanj@ssu.ac.kr

***Abstract*—This paper proposes a HMAC-based RFID mutual authentication protocol to improve performance at the back-end server. In existing hash-based protocols, the tag ID is a secret value for privacy, so the back-end server computes a lot of hash operations or modular operations to retrieve the tag ID. In our protocol, the Tag ID is used as a secret key of HMAC and sends the tag ID XOR-ed by a random number, where XOR-ed tag ID is stored at the back-end server and the tag. The XOR-ed tag ID is changed every session like OTP. The tag sends XORed ID to the back-end server for authentication. Thus, simple matching operation is required to retrieve the tag ID. Therefore, our protocol is much more practical than existing protocols.**

Keyword- RFID; HMAC; mutual authentication

I. INTRODUCTION

Radio Frequency Identification (RFID) is an automatically identifying mobile object called RFID tags through wireless radio. RFID system has three components: low-cost RFID tag, RFID reader, and back-end server. The RFID tag contains a unique identifier, and the RFID reader can obtain the unique identifier from the RFID tag through short-range wireless radio channel. The RFID reader sends the unique identifier to the back-end server in order to recognize information of the object attaching RFID tag [2] [3][7][9].

RFID has various advantages over traditional bar code [1][2]. However, it has various security risks including privacy violation [7], impersonate attack, and message blocking attack [4].

Recently, lightweight mutual authentication protocols [4][14][15] are studied. These protocols are suitable for passive tags. However, such lightweight mutual authentication protocols seem to be vulnerable to various attacks [15], because of not using cryptographic functions of which security are proven.

Another direction of researches for securing RFID is using cryptographically secure hash functions such as SHA-1[16]. S. Wang et al.[8], S-S. Yeo et al. [9], and J. Cho et al. [17] proposed Hash or a keyed-Hash Message Authentication Code (HMAC) based mutual authentication protocols in RFID system. However, these protocols have a disadvantage that the back-end server retrieves IDentifier(ID) with 2*n* hash operations in the worst case, where *n* is the number of tags that are registered to the back-end server. Recently, Cho et al. [17] reduces the cost of retrieving the ID, but still 2*n* modular arithmetic operations in the worst case are required at the back-end server.

This paper proposes a HMAC-based mutual authentication protocol with minimal retrieval cost at the back-end server for RFID system. The proposed protocol uses a tag ID as a secret key of HMAC and sends the tag ID eXclusive OR(XOR)-ed by a random number rather than sending a tag ID in plaintext, where XOR-ed tag ID is stored at the back-end server and the tag. Also, XOR-ed tag ID is changed every session like One-Time Pad (OTP) to provide privacy. The back-end server can retrieve the tag ID with simply comparing the XOR-ed tag ID in DB with received XOR-ed tag ID rather than computing 2*n* hash operations or modular arithmetic operations like [8][9][17] do. Moreover, the proposed protocol is strong against the message blocking attack, called also denial of service or desynchronization problem.

The remainder of this paper is organized as follows: In Section 2, various attacks are described. Section 3 describes the proposed protocol. Section 4 analyzes the security and performance of the proposed protocol. Finally, Section 5 concludes this paper.

II. SECURITY THREAT AND ATTACKS

Because the wireless communication channel between the tag and the reader is an insecure channel, RFID system is vulnerable to various attacks as following

A. Eavesdroppin

The communication channel between the tag and the reader can be eavesdropped, because the radio frequency channel is not secure communication channel [5][6]

B. User privacy

The attacker can monitor the tag using the tag identifier in order to know the user's behavior, when the user identity is linked to a certain tag. Also, the attacker can trace the user location with the tag identifier, when the output of the tag such as the tag identifier is unchangeable [7].

C. Blocking message attack

When an attacker blocks a message between the tag and the reader, the attack causes de-synchronization problem between the tag and the reader/the back-end server [4][8].

 ISBN: 978-1-61208-285-1

D. *Replay attack*

The attacker obtains messages between the tag and the reader by eavesdropping and reuses the message in order to impersonate a legitimate tag or a legitimate reader.

E. *Spoofing attack*

The attacker can impersonate a reader, send a query to a tag and obtain the response of the tag. When the legitimate reader queries the tag, the attacker will send the obtained response to reader in order to impersonate the tag [8].

III. PROPOSED PROTOCOL

This paper proposes a HMAC-based mutual authentication protocol for RFID which is secure against various types of attacks that are described in the previous section. The proposed protocol is based on HMAC [1].

A. *Prior condition and Notation*

In the proposed protocol, a secure communication channel between the reader and the back-end server is established at the enrollment phase, while the communication channel between the tag and the reader is insecure at the authentication phase. The notations are depicted at Table 1.

TABLE I. NOTATION

Notation	Definition
HMAC	***Hash-based Message Authentication Code***
C_A	***A random number of a entity A***
ID_A	***Identity of an entity A***
T_A	***Timestamp from an entity A***

B. *Description of the proposed protocol*

The proposed mutual authentication protocol is based on HMAC having a tag ID (ID_t) as a secret key. The ID is shorter than the cryptographic key length which is required for ensuring required security level. Therefore, actually the tag ID is used as a seed of a random number generator of which an output is a cryptographic key. For convenience, in this paper, 'tag ID' means 'a secret key generated from a random number generator. The processes of proposed protocol are following and Fig. 1 shows authentication procedures.

Step 0: Enrollment phase

- The back-end server and the tag share HMAC function, the identifier of tag (ID_t), a secret key k, and a random number (C_0).
- The back-end server and the tag stores a tuple <ID_t, $ID_t \oplus C_0$> in his/her own database.

Step 1: Reader sends hello message with his/her ID (ID_r)

Step 2: Tag response

- A tag selects a random number (C_1).
- A tag sends $ID_t \oplus C_0$, $k \oplus C_0 \oplus C_1$, $\alpha = HMAC_{ID_t}(T_t, ID_r)$, ID_r and T_t, where T_t is a timestamp of the tag.

Step 3: Tag authentication

- Reader forwards $ID_t \oplus C_0$, $k \oplus C_0 \oplus C_1$, α, ID_r, and T_t to the back-end server
- The back-end server retrieves a tuple <ID_t, k, $ID_t \oplus C_0$> with $ID_t \oplus C_0$ and extracts ID_t.
- The back-end server computes C_1 ($=k \oplus C_0 \oplus C_1 \oplus k \oplus C_0$) and $\alpha' = HMAC_{ID_t}(T_t, ID_r)$.
- The back-end server checks whether $\alpha' = \alpha$.
- The back-end server computes $\beta = HMAC_{ID_t}(T_t + 1, ID_r, C_1)$ and sends β to the reader.

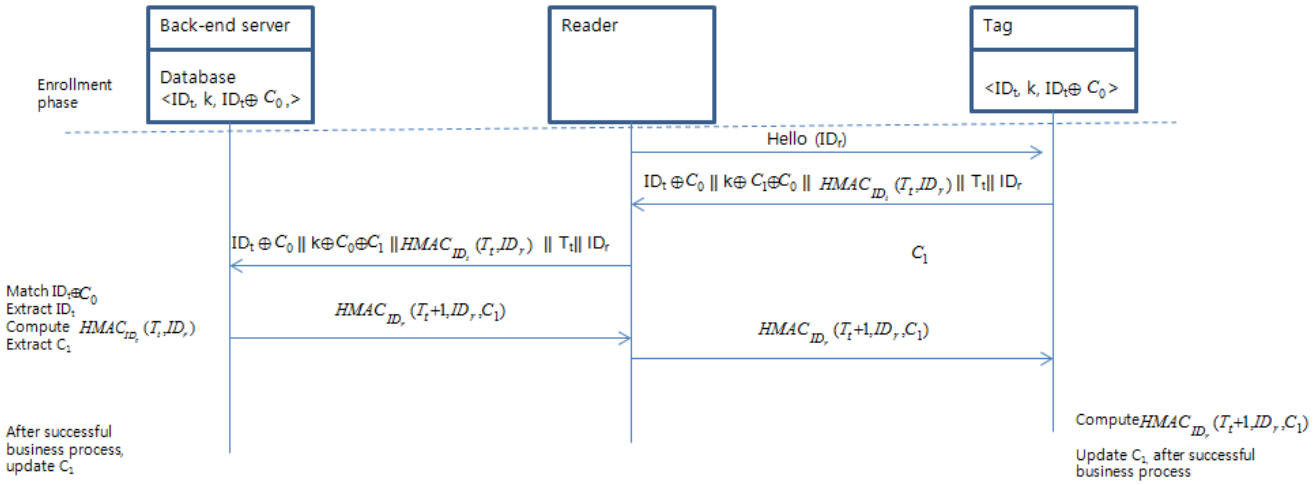


Figure 1. The Proposed Protocol

- The reader forwards β to the tag.

Step 3: back-end server authentication

- The tag computes β' = $HMAC_{ID_t}$ (T_t +1, ID_r, C_1,) using his/her T_t, C_1, and received ID_r.

The tag checks β' = β. If β' = β, the back-end server is authenticated and actual business communication such sending the tag information will be started.

Step 3: update C_1

- After successful business communication such as sending Tag Information, the back-end server and the tag replace <ID_t, k, $ID_t \oplus C_0$> as <ID_t, k, $ID_t \oplus C_1$>, where $ID_t \oplus C_1$ will be used for next session. With successful the business communication, the back-end server and the tag know C_1 is properly transmitted.

IV. Security Analysis and Preformance Analysis

The attacks mentioned in Section 2 such as replay attack, privacy violation, and blocking message attack are common security threat that a RFID faces. This section analyzes the security of the proposed protocol.

A. Eavesdropping

Throughout the proposed protocol, ID_r, T_t, $ID_t \oplus C_0$, $C_0 \oplus C_1$, $HMAC_{ID_t}$ (T_t, ID_r), $HMAC_{ID_t}$ (ID_r, C_1, T_t +1) can be eavesdropping by an attacker. The attacker can try to use this information to obtain ID_t, C_0, and C_1. All these values are XORed and ID is also used as a secret key so the attacker cannot compute any of these values. Therefore, the proposed protocol is secure against eavesdropping.

B. User privacy

The tag identity ID_t is XORed by C_0 which is a random value and is known to only the tag, and the back-end server. Moreover, every session uses different C_i to encrypt ID_t and each C_i has no relationship with other C_{i+n} values, so the attacker cannot link $ID_t \oplus C_i$ of each session. Therefore, the attacker cannot track the tag.

C. Blocking message attack

The proposed protocol updates C_{i+1} at the session i for next session during the mutual authentication. After mutual authentication, the tag and the back-end server communicates business protocol such as sending the tag information. Therefore, the tag and the back-end server know that both are authenticated and updated C_{i+1}. Therefore, the blocking message attack is prevented.

D. Replay attack

Every session uses a fresh C_i and C_{i+1}, and uses a new timestamp. Therefore, the replay attack is impossible.

E. Spoofing attack

When the attacker who impersonates a legitimate reader queries the tag, the attacker can only get the public values ID_r, T_t, $ID_t \oplus C_0$, $C_0 \oplus C_1$, $HMAC_{ID_t}$ (T_t, ID_r). Therefore, the spoofing attack with reusing the values cannot be successful because of a timestamp and a fresh C_i, and C_{i+1}.

TABLE 2
PERFORMANCE EVALUATION (WORST CASE)

Performance		Cho[9]	Wang[8]	Cho[17]	Our Protocol
Computation Cost	Tag	$2H$+2 *MOD*	$2H$	$2H$+4× *MOD*	$2H$
	BS	$(2n+2)\times H$	$(n+1)\times H$	$3H+(6n+2)\times$ *MOD*	$2H$
Communication Cost	T→BS	$1l+1l_H$	$1l+1l_H$	$1l+1l_H$	$3l+1l_H$
	BS→T	$1l+1l_H$	$1l_H$	$2l+2l_H$	$1l_H$

BS: Back-end Server,*n:*number of tags,
*H:*hash or Keyed Hash operation
l: the length of timestamp, challenge or random number,
l_H: the length of hash value
MOD: modular operation

F. Performance Analysis

The proposed protocol can effectively retrieve a tuple <ID_t, $ID_t \oplus C_i$ > with received $ID_t \oplus C_i$. The previous hash-based protocol computes 2*n* hash operations [8][9] or 2*n* modular arithmetic operations [17] in the worst case. Comparing with Wang's protocol [8], Cho's protocol l[9], and Cho's protocol [17], the proposed protocol is very efficient to retrieve the tuple in DB.

The proposed protocol has to compute HMAC function two times at the tag and the back-end server. Which means the proposed protocol is more efficient than previous protocols [8][9][17].

Also, the proposed protocol requires $3l$+2 l_H during mutual authentication. When comparing the most efficient protocol [8] for communication cost, the proposed protocol requires 2*l* more communication cost. However, the proposed protocol solves retrieval problems at the back-end server and message blocking problem of [8].

V. Conclusion and Further Work

Existing lightweight mutual authentication protocols for RFID are vulnerable to various attacks because of not using cryptographic functions of which security are proven.

Existing hash-based mutual authentication protocols for RFID have a problem that should compute 2*n* hash operations in the worst case, where n is the number of tags enrolled at the back-end server. Most recent protocols also have to compute 2*n* modular operations in the worst case. It is not efficient.

 ISBN: 978-1-61208-285-1

This paper introduced a HMAC-based mutual authentication protocol with minimal retrieval cost at the back-end server for RFID system to solve all above problems: (1) the propose protocol is secure because of standard cryptographic function; (2) simple comparison for retrieving ID is required. Also, the proposed protocol is secure against eavesdropping, replay attack, and spoofing attack using HMAC and XOR. Moreover, the proposed protocol solves desynchronization problem with only two communication paths, while the previous protocols are suffered from the message blocking attack. The proposed protocol can be used for the active tags, which are more powerful than the passive tags.

The proposed protocol will be implemented for the active tag in hardware and we will experiment the feasibility for the real-world usages.

ACKNOWLEDGMENT

This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program (NIPA-2012-H301-12-4008) supervised by the NIPA(National IT Industry Promotion Agency)

REFERENCES

[1] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-hashing for Message Authentication," RFC 2104 IETF, Feb. 1997.

[2] EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz Version 1.2.0, EPCglobal.

[3] S. Devadas, G. E. Suh, S. Praal, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based unclonable RFID ICs for anti-counterfeiting and security applications", Proceedings of the IEEE International Conference on RFID, Apr. 2008, pp. 58–64.

[4] R. Bassil, W. El-Beaino, W. Itanti, A. Kayssi, and A. Chehab, "PUMAP : PUF-based Ultra-Lightweight Mutual-Authentication RFID Protocol," Internation Journal of RFID Security an Cryptography, vol. 1, Mar. 2012, pp. 58-66.

[5] X. Leng, K. Mayes, and K. Markantonakis, "HB-MP + protocol: an improvement on the HB-MP protocol," IEEE International Conference on RFID, Apr. 2008, pp. 118–124.

[6] Y.-C. Lee, Y.-C. Hsieh, P.-S. You, and T.-C. Chen, "An improvement on RFID authentication protocol with privacy protection," Third International Conference on Convergence and Hybrid Information Technology – ICCIT 2008, vol. 2, Nov. 2008, pp. 569–573.

[7] A. Juels, "RFID security and privacy: a research survey," IEEE Journal on Selected Areas in Communications, vol. 24, No. 2, Feb. 2006, pp. 381-394.

[8] S. Wang, Q-m, Ma, Y-l. Zhang, and Y-s, Li, "A HMAC-Based RFID Authentication Protocol," 2nd International Symposium on Infromation Engineering and Electronic Commerce (IEEC), July 2010, pp. 1-4.

[9] S-S. Yeo, J-S. Cho, and S. K. Kim. "Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value," Computer Communication, vol. 34, 2011, pp. 391-397.

[10] P. Tuyls and L. Batina, "RFID-tags for Anti-Counterfeiting, Topics in Cryptology CT-RSA," Lecture Notes in Computer Science, Vol.3860 , 2006, pp.115-131.

[11] G.E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," Proc. 44th ACM Annual Design Automation Conference 2007, June 2007, pp. 9-14.

[12] P. Cortese, F. Gemmiti, B. Palazzi, M. Pizzonia, and M. Rimondini,. "Efficient and Practical Authentication of PUF-Based RFID Tags in Supply Chains," IEEE International Conference on RFID-Technology and Applications (RFIDTA), June 2010, pp.182-188.

[13] H. Ghaith, O. Erdinc, and S. Berk, "A Tamper-Proof and Lightweight Authentication Scheme,", Pervasive Mobile Computing, Vol.4(6), 2008, pp. 807-818.

[14] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight Mutual Authentication and Ownership Transfer for RFID systems," Proc. Of IEEE INFOCOM 2010, March 2010, pp. 1-5.

[15] M. Akgün, M.S. Kiraz, and H. Demirci, "Cryptanalysis of Lightweight Mutual Authentication and Ownership Transfer for RFID System," IEEE Lightweight Security & Privacy: Devices, Protocols and Applications (LightSec), March 2011, pp. 20-25.

[16] National Institute of Standards and Technology (NIST), SHA-1 Standard, Secure Hash Standard," FIPS PUB 180-1, www.itl.nist.gov/fipspubs/fip180-1.htm, 1995, [retrieved: Apr. 2013].

[17] J. Cho, S-C. Kim, and S. K. Kim, "Hash-based RFID tag Mutual Authentication Scheme with Retrieval Efficiency" 9th IEEE Internation Symposium on Parallel and Distributed Processing with Applications, May 2011, pp. 324-328.

[18] M. Safkhani, P. Peris-Lopez, J. C. Hernandez-Castro, N. Bagheri, and M. Naderi, "Cryptanalysis of Cho et al.'s protocol, A Hash-Based Mutual Authentication Protocol for RFID Systems," http://eprint.iacr.org/2011/331.pdf, 2011. [retrieved: Apr. 2013].

 ISBN: 978-1-61208-285-1

Network Neutrality – Measures and Measurements: A Survey

Clemens H. Cap, Andreas Dähn, Thomas Mundt
Department of Computer Science
University of Rostock
Rostock, Germany
{clemens.cap, andreas.daehn, thomas.mundt}@uni-rostock.de

***Abstract*—Over the last five years, network neutrality (which means that network infrastructure is treating all data packets equally) has grown to a valuable research area which can be seen as application of anomaly detection. Neutrality violations result from a combination of traffic differentiation (either by statistical protocol identification or deep packet inspection) and infrastructure components which are capable of classification based packet handling. We examine some examples for neutrality violations and then go on to neutrality testing. Neutrality testing approaches can be divided into three categories: Active approaches (which usually utilize specialized testing peers), passive approaches (which monitor the incoming and outgoing network traffic at the user's computer or local network) and hybrid approaches (which combine both). In this article, we take a look at some implementations and at assets and drawbacks of both approaches and implementations. Some major drawbacks originate from ambiguous test results (such as a test reporting a neutrality violation for what really is a network congestion). Depending on the approach and the implementation, different testing programs have very different statements which shall not be compared without consideration of testing principle and implementation details. Aside from algorithmic testing, crowdsourcing approaches which use volunteers' observations have been developed recently.**

Keywords — ***Network neutrality; Network performance anomaly detection; User-oriented performance metrics; Intrusive and non-intrusive performance measurement mechanisms***.

I. Introduction

Network neutrality is the idea of a network treating all handled packets equally (a more detailed definition is provided in the following Subsection). Over the last years, an increasing number of network equipment became capable of traffic differentiation, lowering the barrier to violations of network neutrality. Subsequential, identification of network neutrality violations became a research topic and led to the development of several neutrality violation detection systems. In this survey, we provide an overview on current technical measures, which are used to violate neutrality, as well as measurement techniques. We focus on conceptual rather than on implementation details and cover active, passive, and hybrid neutrality violation detection techniques.

The article starts with a short terminology chapter. In the following Section, we provide a brief digest on the historical development and the debate surrounding network neutrality. Section 3 then contains technical details, covering symptoms of neutrality violations, traffic differentiation techniques, and neutrality violation detection approaches. Section 4 provides a short outline about Internet service providers' ways to tamper with measurements. Section 5 is practical oriented: It contains examples of observed neutrality violations and provides a review of currently available neutrality detection software. Section 6 finally concludes the article.

A. Terminology

When the term "network neutrality" is used in this article, we assume the following definition: *A network is neutral, if all data packets are processed equally, regardless of their origin, destination, protocol or content* [1] (translation A.D.). This definition has been chosen because of its shortness and clearness, although it needs a well defined reference point. The arising problems are discussed in detail in Section II. Other definitions relate neutrality violations to turning away from the "best effort" principle. Best effort commonly means that a infrastructure component works "first in, first out" with no guarantees regarding packet delivery or any quality of delivery. More thoughts on the definition by "best effort" can be found in [2].

We will use the term "network provider" in general as neutrality violations seem not restricted to Internet service providers nor other network carriers.

II. Development of network neutrality

One may ask whether the Internet has ever been neutral, since there has always been a relation between network quality and paid fee. In contrast to this observation, one detail has changed over the last ten years: Network infrastructure equipment became capable of traffic differentiation. According to the above definition of network neutrality, the Internet has been neutral as long as all infrastructure components worked best-effort.

Currently, two factors influence the network-neutrality-debate: One is the rising impact of next generation networks which unite television, telephone and Internet connection. The other concerned with media rumors is network providers changing their terms of service [3], the European Union taking a new approach on network neutrality evaluation [4] and activities of media companies working towards a "free

 ISBN: 978-1-61208-285-1

Internet" [5] as well as (probably other) companies working against piracy using filtering mechanisms [6]. Recent versions of service level agreements used by Internet service providers contain restrictions of throughput whenever a specified amount of data has been transferred using defined services. This change is probably due to the widespread practice of "over-selling", which means that the ISPs sell e.g. more throughput to customers than they can theoretically provide if all customers would acquire the maximum capacity the same time. In this context one may take a look at contracts between Internet service providers and customers and ask whether general network access or even specific characteristics are sold. Do contracts assure minimum values for at least some of the network properties such as latency, throughput or jitter (as specified e.g in [7])?

Next generation networks feature their own problem regarding network neutrality. The question whether the wall socket or just the PC connection of the user's router shall be subject to the definition of network neutrality remains unanswered currently. In this article, we focus on the user's home network Internet uplink, not the wall socket.

III. Detecting network neutrality

Detecting network neutrality contains a basal problem: To prove a network connection to be truly neutral, testing connections to every possible target with every possible protocol would be necessary. As such a practice would obviously be impossible, tests scan for violations of network neutrality.

A. Symptoms of network neutrality violations

Violating network neutrality can result in four observable symptoms (respective to single data streams (i.e. the set of all data packets belonging to one transfer as seen from upper layers)):

1) unavailability of sites or services,
2) enhanced quality of service,
3) reduced quality of service,
4) low-level phenomena such as changed arrival times of data packets compared to each other.

The term "quality of service" is used as defined in [7], covering throughput, latency, jitter, and error rate.

This list reveals one of the problems making detection of network neutrality a difficult task: some of these symptoms can also be caused by other reasons than a violation of network neutrality.

B. How network neutrality is violated

Network providers violate network neutrality for three main reasons: Political, social, or economical reasons. A further discussion of network providers' motivation to violate network neutrality is beyond this article's scope.

To violate network neutrality, network providers distinguish data streams originating from the same IP address. We take a look at practical relevant methods: Deep packet inspection (DPI) and statistical protocol identification (SPID). The basic ideas of DPI and SPID are explained as follows. A detailed introduction with a review of current DPI implementation techniques can be found in [8] or [9]. General information on SPID can be found in [10], in which the use of Bayes' classifier is demonstrated. An example for the use of SPID to differentiate web applications is described in [11]. The results of these measures are subsequently used to apply policies to data streams. Such policies may contain modifications of transferred contents, denial of packet forwarding as well as enhanced or degraded priority.

Both methods originate from network security systems, which scan for malicious data or suspect behavior, and have been developed and improved in this context.

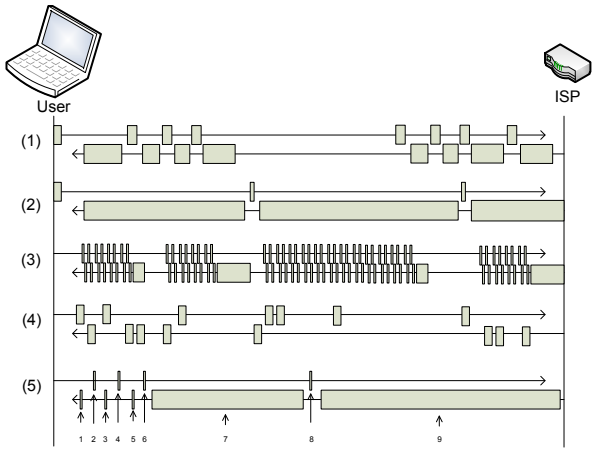
Statistical protocol identification analyzes packet contents and the meta data surrounding a transmission. One of the SPID-methods is analyzing the byte-distribution within a data packet. Other methods analyze transmission frequencies or sizes. These methods lead to satisfying statements about the used upper layer protocol even if the payload is encrypted [12].

Figure 1 illustrates how SPID identifies protocols or applications using meta data of data streams: Different types of network usage generate different data exchange pattern. The first example might be a browsing session: The user load a page. The page refers to several other files (images, style sheets, ...) which are loaded subsequently. Once the user finished reading, he may open the next page. The second example depicts probably a download (without identifying the actual protocol): Only small acknowledgment packets originate from the client. Example (3) could result from an interactive shell session: Small packets represent single keystrokes as well as the appearing characters. Some keystrokes trigger longer responses, e.g. directory listings. Example (4) contains no obvious pattern except all packets having a comparable size; this pattern might probably indicate a chatting user. Example (5) resembles a POP3-session; the actual exchanged data is provided aside the drawing.

Deep packet inspection considers knowledge about upper layer protocols as their headers are necessarily included in the packet. Only encrypted (application-) protocol headers are not available to deep packet inspection. Consequently deep packet inspection needs to make assumptions about assignment between ports and protocols.

In a typical DPI use case, specific data can be found at specific offsets within a data packet (for example in a HTTP-request (in a TCP-packet without extra headers): The sender address starts at bit 96, the destination address at 128; the TCP-source-port at bit 160, the destination point at 176. The HTTP-request itself starts at bit offset 352). As the packet including its payload is analyzed, DPI tends to be a bottleneck in packet forwarding. Especially the deployment of a new rule set was a problem. This problem has triggered the development of new algorithms, e.g. [13]. Identified data streams can subsequently be marked as high- or low-priority or payload may get modified. It is also possible to silently drop the packet.

 ISBN: 978-1-61208-285-1



Client → Server		Server → Client
	1	+OK POP server ready H alicenet001
user alice@alice.net	2	
	3	+OK password required for user "alice@alice.net"
pass alicessecret	4	
	5	+OK mailbox "alice@alice.net" has 3 messages (138711 octets)
retr 1	6	
	7	Body of mail #1
retr 2	8	
	9	Body of mail #2

Fig. 1. Example for statistical protocol identification by packet sizes and frequencies.

C. Detection Approaches

To detect symptoms of neutrality violations, two major approaches have been developed. Some additional approaches have been made, e.g. to gain information on neutrality violations using crowdsourcing.

All approaches have two constraints: The number of false positives and false negatives shall be as small as possible. False positives would be scenarios in which a neutral (but perhaps congested) network is reported as non-neutral; a negative would be a neutrality-violating network reported as neutral. The fine tuning on these indices is usually done by means of statistical evaluation.

1) The Active Approach: The active approach tests connections explicitly for neutrality violations. During a test, data is exchanged between a testing client on the user's computer and one or more testing servers on one or more well-known hosts on the Internet. Both sides observe the data exchange carefully and apply statistical tests to it. This statistical evaluation results in a statement whether the test found neutrality violations – or not (or that the test results are inconclusive).

The typical setup for a measurement based on the active approach can be divided in two active parts: One on the user's computer located in his home network; the other on well-known testing servers. The intermediate routing can neither be influenced nor examined actively.

This approach features a huge drawback: As long as specific testing peers are necessary, tests can only state whether connections to *these* specific peers are neutral. Statements regarding the neutrality of connections to other targets can not be derived. The active approach has been implemented, e.g. in the project *Glasnost* [14].

2) The Passive Approach: The passive approach monitors the user's everyday network usage. A piece of software records a detailed statistic about exchanged network packets. Additional information has to be provided by the user. These information is used to evaluate data exchanges. Statistic methods are applied to distinguish discriminated from promoted traffic. Finally, a statement about the neutrality of the network uplink is made. Some implementations of the passive approach aggregate collected data from all users on central systems to boost the approaches efficiency. This collection of data is necessary to have a sufficiently large sample. Otherwise detection would rely purely on a single user's behavior – who probably would not generate enough data to allow statements related to each connection.

The network setup for a measurement using the passive approach needs only a monitoring client on the users computers and a server for central evaluation which has to be reachable through the Internet.

Blasting the restriction on testing peers is a great advantage of the passive approach. The approach provides an answer to the question "is the network uplink neutral regarding everything I do" (which is nothing else than "is the network uplink neutral" to a single user) and not "is a bunch of connections through my network uplink neutral". This advantage is bought by submitting detailed information about the network usage to a central (and potentially unsafe) server. Implementations of the passive approach react on this problem by allowing the user to disable data aggregation for a specified timeout or specific domains. However, this restriction hits exactly the big advantage: If the user decides to disable data aggregation while visiting some sites, neutrality violations applied to those sites can not be detected. The passive approach has been implemented, e.g. in the project *NANO* [15] which analyzes the network usage at a rather low level; other projects such as *Fanthom* [16] utilize a view from within the user's browser.

3) Hybrid Approaches: Combining the active and the passive to a hybrid approach is promising. It may combine the advantage of easy measurements (inherited from the active approach) while using all used network connections as view port (inherited from the passive approach). Two ideas of hybrid approaches seem feasible. They shall be described briefly.

A first approach would connect multiple instances of the passive approach. Whenever the central evaluation cannot decide whether something is a neutrality violation, additional instances of the measurement client are acquired to act ac-

 ISBN: 978-1-61208-285-1

tively. They would reproduce a connection whose neutrality cannot be decided. This supplement would allow quick tests whenever something seems to come up. However, this idea contains the possibility of abuse by its design: The design resembles a bot net. Furthermore, this part could even falsify a measurement: Imagine a site suffering from congestion. Its reduced performance is noted by a passive instance and submitted to the central evaluation. Additional instances are ordered to perform measurements (by opening additional connections to the target). This feedback loop causes additional traffic which intensifies the congestion.

Possibly due to the problem of feedback loops and abuse, to the authors knowledge this approach has not been implemented yet.

A different idea of an hybrid approach embeds a "black box" in the providers network. A measurement is performed by establishing an encrypted tunnel between the user's computer and the "black box". This setup enables differential measurements, as packets crossing the providers network and packets sent through the same network encrypted (and therefore possibly invisible to deep packet inspection) can be compared. The assumption of encrypted traffic to be indifferentiable to the provider may turn out to be a problem as current SPID algorithms also target encrypted data [18]. Thus, additional measures will be necessary to obfuscate the encrypted channel. Consequently, there will be an off-trade to the measurement's accuracy. This approach has been implemented in the "N00ter"-project [17], Figure 2 shows the network setup for such an hybrid approach. In contrast to the active and the passive approach, a "black box" within the network providers infrastructure is necessary.

4) Crowdsourcing: The previously sketched approaches base on technical (using algorithms and statistics) evaluation – crowdsourcing uses human resources instead. The basic idea is: Ask people browsing the Internet to submit noticed cases of the Internet behaving "abnormal", e.g. sites being unavailable. The costs are very low: basically such a service would only need a public communication channel such as a web site or an e-mail-address.

The drawbacks of this approach are the drawbacks of crowdsourcing: Users have varying ideas of "blocking a site", probably depending on their knowledge.

IV. Counter-Measurement-Measures

Obviously, Network providers may have less to no interest in customers proofing their networks to be non neutral. Thus they may implement strategies to tamper with measurements. This goal could be reached by changing policies applied to network uplinks (from non-neutral to neutral). Such a measure would need a trigger – at this point the differences between active and passive approaches become additionally important.

This approach of avoiding neutrality violation proofs may work with every measurement utilizing data packets to well-known testing targets: Traffic to these targets can be interpreted as indicator for an immanent (or ongoing) test and used as trigger for a policy change.

V. Examples

This Section starts with examples of neutrality violations which have been observed. Subsequently software for detection of neutrality violations shall be presented.

A. Neutrality violations

It is worth to mention that this Subsection shows possibilities of neutrality violations. The observed techniques may not have been used with the intention of violating network neutrality, the observations can also be due to misconfiguration. Please keep in mind that the described phenomena could also be used in more harmful scenarios, e.g. to filter contents for political statements.

1) Connection interception: If users search for the term "falun gong" using the Chinese search engine "baidu.cn", the connection will be intercepted. According listings are provided in [19].

The user's client receives TCP-packets with active reset-flag which cause the connection to terminate. It is not possible to determine the origin of those packets: The server at baidu.cn or some routing station may have injected them. Even if (in case of injection) the server keeps sending packets after a connection reset has been injected, those original packets would probably be dropped by every stateful firewall.

2) Content manipulation: Today's network infrastructure equipment is capable of changing the payload of redirected packets. We will show this capability in two real-world scenarios.

In our first example, network equipment manipulates SMTP-connections. The response to the command "ehlo" gets manipulated. We observed a manipulation which caused the server identification and the announcement of encrypted communication with "STARTTLS" to be obfuscated. This obfuscation results in mail clients assuming the absence of encrypted connections via "STARTTLS" (which is probably prompted to the user who will eventually switch back to the use of plain connections, allowing the network provider to read transmitted contents). The listings (modified and unmodified) can be found at [19].

In the second example, web site contents are modified massively. Our example was a HTML-file just embedding an image. When requested through an UMTS network connection provided by the local Internet Provider "1und1", the file contents change: JavaScripts are included and the location of the embedded image points now to a location at the virtual (mapped) IP address 1.1.1.1. The image file at this different location is a size-compressed version of the original image (showing more artifacts). One can assume this manipulation is due to short network capacities. Detailed listings of this example can be found in [19].

3) Manipulation of HTTP Transfers: A different method of neutrality violation utilizes IP address spoofing to impersonate other entities. The "BlueSocket" wlan-access-control system shall be described here as example for commercial use of IP address spoofing. A manipulation takes place whenever an unauthenticated user tries to request a web site. In this

 ISBN: 978-1-61208-285-1

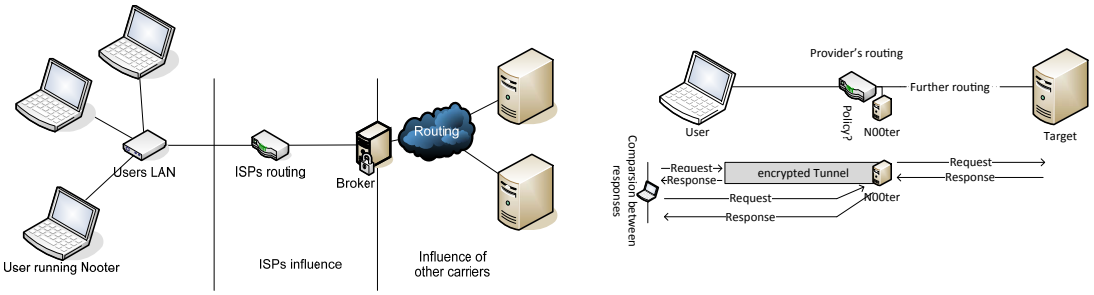


Fig. 2. Typical network setup for a hybrid measurement as proposed for N00ter [17] and illustration of N00ter's working principle: N00ter establishes an encrypted tunnel to a broker within the provider's network to perform differential measurements.

case, the answer does not originate from the queried server but from the BlueSocket-System: It redirects the user to its logon-page. To do so, it spoofs the original server address. Note that without domain knowledge it is not possible to differentiate whether the answer originates from the queried server or has been injected. A detailed dump can be found in [19].

B. Neutrality tests

This Section introduces some projects which aim to detect violations of network neutrality. Glasnost and NANO implement the active respectively passive approach. N00ter is a hybrid approach based on N00ter-boxes embedded in the network provider's infrastructure. ShaperProbe derives statements about traffic shaping from an evaluation of incoming data packets. Herdict represents an approach for detection of network blockages purely based on crowdsourcing.

1) Glasnost: Glasnost ([14], [20]) deploys the active approach. A test consists of several data exchanges, which are monitored by the server and the client application. Subsequently the data transfers are analyzed and a statement about neutrality is presented.

Glasnost was designed for easy usage. The end-user-part of Glasnost has been implemented as a Java applet embedded into a web page. The applet features only one user interface object: A "start"-button. The usability-thinking continues along the measurement: It has been designed to finish within a time which is short enough for the user to wait. Longer measurements would raise the method's precision, but testing showed that most users lost patience (or interest) whenever measurements took longer than 6 minutes [20].

According to [20], the statistical evaluation has been tuned to gain a false-positive rates about 0.7% – even in short tests.

To gain knowledge about traffic differentiation, Glasnost transfers two kinds of traffic. This data differs only in its contents, not in packet size or sequence. Consequently, timings and packet sizes remain the same allowing only deep packet inspection to differentiate between the dummy and the actual packets.

2) NANO: NANO ([15],[21]) represents the passive approach. An agent observes the network usage on a specified network interface. Additional information (e.g. the uplink media and a contact e-mail-address of the user) has to be provided during setup. NANO sends bundled data to an evaluation server using a secured channel. Currently all data is stored at the Georgia Institute of Technology. NANO is currently available for Linux users only; a Windows-Version had been announced.

Privacy concerns are considered in configurations: The user can disable the logging of traffic to specified hostnames. An additional piece of software may be used to suspend the monitoring service for a specified amount of time.

As described in [21], the accuracy of statements concerning traffic differentiation depends highly on the amount of analyzed data. Additional causal interferences make it difficult to provide an overall amount of false positives or false negatives.

3) N00ter: N00ter ([17]) follows a hybrid approach. As illustrated in Figure 2, the active part establishes an encrypted tunnel to a black box ("N00ter") within the Internet service providers network. Subsequently the N00ter acts as a proxy: It receives requests through the tunnel and forwards them to the (arbitrary) target. The N00ter receives the answer and sends it twice to the user's PC: Through the tunnel as well as through the ISPs plain network. The received answers are finally compared as the setup allows for differential measurements.

Additional measurements can be performed by sending the requests plain through the providers network, too.

4) ShaperProbe: ShaperProbe ([22], [23]) utilizes basal effects of traffic shaping: In typical scenarios, the activation of shaping algorithms can be easily noticed by tracking the times of incoming data packets. The effect is caused by some shaping algorithms: To limit the connection "speed" (packets per time or bytes per time) to a specified value, it needs to quantify its current value. To do so, an amount of time has to pass. Subsequently, packets get delayed.

This difference in packet timing between the first seconds and the following time (very fast start, long pause (to speed down), finally continuous amount of bytes/second) can be detected and evaluated.

After the actual network testing, statements about the existence of shapers on the data path are derived. Although the approach should be usable with arbitrary data transfers, ShaperProbe currently uses well-known targets.

5) Herdict: Finally we introduce Herdict ([24]) as representative of the crowdsourcing approach. It is quite straightforward: The user announces pages to be "accessible" or "inaccessible" and the site adds this entry (connected with

the user's Internet service provider which is detected automatically) to its database. Entries can also be submitted to Herdict by Mail or twitter-message, although, as the Herdict-FAQ states, there exist exceptions: No sites exposing pornographic material will be accepted; additional the "Google SafeSearch"-filter is applied.

VI. Conclusion

Over the last five years, network neutrality violations became more frequent. This change led also to new development on the field of neutrality violation analysis. There are currently two ready-to-use testing methods, the active and the passive method. Still, neutrality violations can never provide absolutely trustworthy results: Active tests may be detected by network operators (and thus be manipulated), passive tests either suffer from a lack of raw data to evaluate or need to collect data of multiple users for central evaluation. Differentiation between intended neutrality violations and network congestions remain a difficult task.

A comparison of the different approaches' results is not useful: They test different network properties. Statements derived from active approaches concern well-known testing connections. While some active approaches enable the user to test multiple protocols and multiple test targets (Glasnost), other approaches rely on single targets (ShaperProbe). This difference is caused by different design tenets: ShaperProbe does not assume shaping to differentiate between different kinds of data streams – Glasnost does. Statements derived from crowdsourcing depend highly on users posting neutrality violation suspects. Statements generated by passive approaches depend on user's Internet usage. Therefore, this approach has to deal with noise, perhaps more than other approaches. Combination of these approaches leads to hybrid approaches (as N00ter), which finally allow clear statements as they use the same viewpoint as purely passive approaches extended to a second channel (which is assumed not to be influenced by the provider). This allows a direct comparison between data exchange through a provider's network while it may be influenced on one channel and not influenced on the other channels.

Although the perfect solution for network neutrality analysis is yet to be found, existing approaches provide a wide range of analytic tools. Existing approaches enable users to scan for (dumb) shapers, or to test singular protocols. Passive approach driven projects seem a promising field of future work as they solve the active approaches' problem of restricted viewpoints.

References

[1] G. M. Bullinger, "Netzneutralität: Pro und Contra einer gesetzlichen Festschreibung," *Deutscher Bundestag: Wissenschaftliche Dienste*, June 2010.

[2] J. Crowcroft, "Net Neutrality: The Technical Side of the Debate: A White Paper," *SIGCOMM Comput. Commun. Rev.*, vol. 37, pp. 49–56, January 2007.

[3] U. Mansmann, "Kabel Deutschland drosselt Filesharing für Bestandskunden," 2012. http://heise.de/-1652920, last accessed 2013-04-29.

[4] EC, DG Communications Networks, Content and Technology, "Online public consultation on "specific aspects of transparency, traffic management and switching in an Open Internet"," 2012. http://ec.europa.eu/information_society/digital-agenda/actions/oit-consultation/index_en.htm, last accessed 2013-04-29.

[5] A. Wilkens, "Große Internet-Untrnehmen formen Lobbyverband für ein 'freies Internet'," 2012. http://heise.de/-1653423, last accessed 2013-04-29.

[6] A. Wilkens, "Musikindustrie setzt weiter auf Websperren, Warnhinweise und Filter," 2012. http://heise.de/-1653013, last accessed 2013-04-29.

[7] A. S. Tanenbaum and D. Wetherall, *Computer Networks*. Pearson, 5. ed., 2011.

[8] A. Chaudhary and A. Sardana, "Software Based Implementation Methodologies for Deep Packet Inspection," in *Information Science and Applications (ICISA), 2011 International Conference on*, pp. 1 –10, april 2011.

[9] R. K. Lenka and P. Ranjan, "A Comparative Study on DFA-Based Pattern Matching for Deep Packet Inspection," in *Computer and Communication Technology (ICCCT), 2012 Third International Conference on*, pp. 255 –260, nov. 2012.

[10] A. Ali and R. Tervo, "Traffic identification using Bayes' classifier," in *Electrical and Computer Engineering, 2000 Canadian Conference on*, vol. 2, pp. 687 –691 vol.2, 2000.

[11] R. Archibald, Y. Liu, C. Corbett, and D. Ghosal, "Disambiguating HTTP: Classifying web Applications," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, pp. 1808 –1813, july 2011.

[12] W. Jiang and M. Gokhale, "Real-Time Classification of Multimedia Traffic Using FPGA," in *Field Programmable Logic and Applications (FPL), 2010 International Conference on*, pp. 56–63, 31 2010-sept. 2 2010.

[13] Kefu, X. and Deyu, Q. and Zhengping, Q. and Weiping, Z., "Fast Dynamic Pattern Matching for Deep Packet Inspection," in *Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on*, pp. 802 –807, april 2008.

[14] "Glasnost: Test if your ISP is shaping your traffic." http://broadband.mpi-sws.org/transparency/bttest.php, last accessed 2013-04-29.

[15] Feamster, N. and Ammar, M. and Mukarram bin Tariq, M. and Motiwala, M., "GTNOISE Network Access Neutrality Project," 2011. http://gtnoise.net/nano/, last accessed 2013-04-29.

[16] M. Dhawan, J. Samuel, R. Teixeira, C. Kreibich, M. Allman, N. Weaver, and V. Paxson, "Fathom: A Browser-Based Network Measurement Platform," in *Proceedings of the 2012 ACM conference on Internet measurement conference*, IMC '12, (New York, NY, USA), pp. 73–86, ACM, 2012.

[17] D. Kaminsky, "Black Ops Of TCP/IP 2011," *Defcon*, 2011. http://dankaminsky.com/2011/08/05/bo2k11, last accessed 2013-04-29.

[18] C. Liu, G. Sun, and Y. Xue, "DRPSD: An novel method of identifying SSL/TLS traffic," in *World Automation Congress (WAC), 2012*, pp. 415 –419, june 2012.

[19] http://opsci.informatik.uni-rostock.de/index.php/NN2013, last accessed 2013-04-29.

[20] M. Dischinger, M. Marcon, S. Guha, K. P. Gummadi, R. Mahajan, and S. Saroiu, "Glasnost: Enabling End Users to Detect Traffic Differentiation," March 2010.

[21] M. B. Tariq, M. Motiwala, N. Feamster, and M. Ammar, "Detecting Network Neutrality Violations with Causal Inference," in *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, CoNEXT '09, (New York, NY, USA), pp. 289–300, ACM, 2009.

[22] P. Kanuparthy, "Shaperprobe." http://www.cc.gatech.edu/~ partha/diffprobe/shaperprobe.html, last accessed 2013-04-29.

[23] P. Kanuparthy and C. Dovrolis, "ShaperProbe: End-to-End Detection of ISP Traffic Shaping using Active Methods," in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, IMC '11, (New York, NY, USA), pp. 473–482, ACM, 2011.

[24] "Herdict: Help spot web blockages." http://www.herdict.org/, last accessed 2013-04-29.

 ISBN: 978-1-61208-285-1