http://www.icact.org/journal.asp

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 1 Issue 2, Sep 2012, ISSN: 2288-0003

Editor-in-Chief
Prof. Thomas Byeongnam YOON, PhD.

Global IT
Research Institute

Journal Editorial Board

■ Editor-in-Chief

■ Editors

Dr. Youssef SAID, Tunisie Telecom, Tunisia
Dr. Noor Zaman, King Faisal University, Al Ahsa Hofuf, Saudi Arabia
Dr. Srinivas Mantha, SASTRA University, Thanjavur, India
Dr. Shahriar Mohammadi, KNTU University, Iran
Prof. Beonsku An, Hongik University, korea
Dr. Guanbo Zheng, University of Houston, USA
Prof. Sangho Choe, The Catholic University of Korea, korea
Dr. Gyanendra Prasad Joshi, Yeungnam University, korea
Dr. Tae-Gyu Lee, Korea Institue of Industrial Technology(KITECH), korea
Prof. Ilkyeun Ra, University of Colorado Denver, USA
Dr. Yong Sun, Beijing University of Posts and Telecommunications, China
Dr. Yulei Wu, Chinese Academy of Sciences, China
Mr. Anup Thapa, Chosun University, korea
Dr. Vo Nguyen Quoc Bao, Posts and Telecommunications Institute of Technology, Vietnam
Dr. Harish Kumar, Bhagwant institute of technology, India
Dr. Jin REN, North china university of technology, China
Dr. Joseph Kandath, Electronics & Commn Engg, India
Dr. Mohamed M. A. Moustafa, Arab Information Union (AIU), Egypt
Dr. Mostafa Zaman Chowdhury, Kookmin University, Korea
Prof. Francis C.M. Lau, Hong Kong Polytechnic University, Hong Kong
Prof. Ju Bin Song, Kyung Hee University, korea
Prof. KyungHi Chang, Inha University, Korea
Prof. Sherif Welsen Shaker, Kuang-Chi Institute of Advanced Technology, China
Prof. Seung-Hoon Hwang, Dongguk University, Korea
Prof. Dal-Hwan Yoon, Semyung University, korea
Prof. Chongyang ZHANG, Shanghai Jiao Tong University, China
Dr. H K Lau, The Open University of Hong Kong, Honh Kong
Prof. Ying-Ren Chien, Department of Electrical Engineering, National Ilan University, Taiwan
Prof. Mai Yi-Ting, Hsiuping University of Science and Technology, Taiwan
Dr. Sang-Hwan Ryu, Korea Railroad Research Institute, Korea
Dr. Yung-Chien Shih, MediaTek Inc., Taiwan
Dr. Kuan Hoong Poo, Multimedia University, Malaysia
Dr. Michael Leung, CEng MIET SMIEEE, Hong Kong
Dr. Abu sahman Bin mohd Supa'at, Universiti Teknologi Malaysia, Malaysia
Prof. Amit Kumar Garg, Deenbandhu Chhotu Ram University of Science & Technology, India
Dr. Jens Myrup Pedersen, Aalborg University, Denmark
Dr. Augustine Ikechi Ukaegbu, KAIST, Korea
Dr. Jamshid Sangirov, KAIST, Korea
Prof. Ahmed Dooguy KORA, Ecole Sup. Multinationale des Telecommunications, Senegal
Dr. Se-Jin Oh, Korea Astronomy & Space Science Institute, Korea
Dr. Rajendra Prasad Mahajan, RGPV Bhopal, India
Dr. Woo-Jin Byun, ETRI, Korea
Dr. Mohammed M. Kadhum, School of Computing, Goodwin Hall, Queen's University , Canada
Prof. Seong Gon Choi, Chungbuk National University, Korea
Prof. Yao-Chung Chang, National Taitung University, Taiwan
Dr. Abdallah Handoura, Engineering school of Gabes - Tunisia, Tunisia
Dr. Gopal Chandra Manna, BSNL, India

Dr. Il Kwon Cho, National Information Society Agency, Korea
Prof. Jiann-Liang Chen, National Taiwan University of Science and Technology, Taiwan
Prof. Ruay-Shiung Chang, National Dong Hwa University, Taiwan
Dr. Vasaka Visoottiviseth, Mahidol University, Thailand
Prof. Dae-Ki Kang, Dongseo University, Korea
Dr. Yong-Sik Choi, Research Institute, IDLE co., ltd, Korea
Dr. Xuena Peng, Northeastern University, China
Dr. Ming-Shen Jian, National Formosa University, Taiwan
Dr. Soobin Lee, KAIST Institute for IT Convergence, Korea
Prof. Yongpan Liu, Tsinghua University, China
Prof. Chih-Lin HU, National Central University, Taiwan
Prof. Chen-Shie Ho, Oriental Institute of Technology, Taiwan
Dr. Hyoung-Jun Kim, ETRI, Korea
Prof. Bernard Cousin, IRISA/Universite de Rennes 1, France
Prof. Eun-young Lee, Dongduk Woman s University, Korea
Dr. Porkumaran K, NGP institute of technology India, India
Dr. Feng CHENG, Hasso Plattner Institute at University of Potsdam, Germany
Prof. El-Sayed M. El-Alfy, King Fahd University of Petroleum and Minerals, Saudi Arabia
Prof. Lin You, Hangzhou Dianzi Univ, China
Mr. Nicolai Kuntze, Fraunhofer Institute for Secure Information Technology, Germany
Dr. Min-Hong Yun, ETRI, Korea
Dr. Seong Joon Lee, Korea Electrotechnology Research Institute, korea
Dr. Kwihoon Kim, ETRI, Korea
Dr. Jin Woo HONG, Electronics and Telecommunications Research Inst., Korea
Dr. Heeseok Choi, KISTI(Korea Institute of Science and Technology Information), korea
Dr. Somkiat Kitjongthawonkul, Australian Catholic University, St Patrick's Campus, Australia
Dr. Dae Won Kim, ETRI, Korea
Dr. Ho-Jin CHOI, KAIST(Univ), Korea
Dr. Su-Cheng HAW, Multimedia University, Faculty of Information Technology, Malaysia
Dr. Myoung-Jin Kim, Soongsil University, Korea
Dr. Gyu Myoung Lee, Institut Mines-Telecom, Telecom SudParis, France
Dr. Dongkyun Kim, KISTI(Korea Institute of Science and Technology Information), Korea
Prof. Yoonhee Kim, Sookmyung Women s University, Korea
Prof. Li-Der Chou, National Central University, Taiwan
Prof. Young Woong Ko, Hallym University, Korea
Prof. Dimiter G. Velev, UNWE(University of National and World Economy), Bulgaria
Dr. Tadasuke Minagawa, Meiji University, Japan
Prof. Jun-Kyun Choi, KAIST (Univ.), Korea
Dr. Brownson ObaridoaObele, Hyundai Mobis Multimedia R&D Lab , Korea
Prof. Anisha Lal, VIT university, India
Dr. kyeong kang, University of technology sydney, faculty of engineering and IT , Australia
Prof. Chwen-Yea Lin, Tatung Institute of Commerce and Technology, Taiwan
Dr. Ting Peng, Chang'an University, China
Prof. ChaeSoo Kim, Donga University in Korea, Korea
Prof. kirankumar M. joshi, m.s.uni.of baroda, India
Dr. Chin-Feng Lin, National Taiwan Ocean University, Taiwan
Dr. Chang-shin Chung, TTA(Telecommunications Technology Association), Korea

Editor Guide

■ Introduction for Editor or Reviewer

All the editor group members are to be assigned as a evaluator(editor or reviewer) to submitted journal papers at the discretion of the Editor-in-Chief. It will be informed by eMail with a Member Login ID and Password.

Once logined the Website via the Member Login menu in left as a evaluator, you can find out the paper assigned to you. You can evaluate it there. All the results of the evaluation are supposed to be shown in the Author Homepage in the real time manner. You can also enter the Author Homepage assigned to you by the Paper ID and the author's eMail address shown in your Evaluation Webpage. In the Author Homepage, you can communicate each other efficiently under the peer review policy. Please don't miss it!

All the editor group members are supposed to be candidates of a part of the editorial board, depending on their contribution which comes from history of ICACT TACT as an active evaluator. Because the main contribution comes from sincere paper reviewing role.

■ Role of the Editor

The editor's primary responsibilities are to conduct the peer review process, and check the final camera-ready manuscripts for any technical, grammatical or typographical errors.

As a member of the editorial board of the publication, the editor is responsible for ensuring that the publication maintains the highest quality while adhering to the publication policies and procedures of the ICACT TACT(Transactions on the Advanced Communications Technology).

For each paper that the editor-in-chief gets assigned, the Secretariat of ICACT Journal will send the editor an eMail requesting the review process of the paper.

The editor is responsible to make a decision on an "accept", "reject", or "revision" to the Editor-in-Chief via the Evaluation Webpage that can be shown in the Author Homepage also.

■ Deadlines for Regular Review

Editor-in-Chief will assign a evalaution group(a Editor and 2 reviewers) in a week upon receiving a completed Journal paper submission. Evaluators are given 2 weeks to review the paper. Editors are given a week to submit a recommendation to the Editor-in-Chief via the evaluation Webpage, once all or enough of the reviews have come in. In revision case, authors have a maximum of a month to submit their revised manuscripts. The deadlines for the regular review process are as follows:

Evalution Procedure	Deadline
Selection of Evaluation Group	1 week
Review processing	2 weeks
Editor's recommendation	1 week
Final Decision Noticing	1 week

■ Making Decisions on Manuscript

Editor will make a decision on the disposition of the manuscript, based on remarks of the reviewers. The editor's recommendation must be well justified and explained in detail. In cases where the revision is requested, these should be clearly indicated and explained. The editor must then promptly convey this decision to the author. The author may contact the editor if instructions regarding amendments to the manuscript are unclear. All these actions could be done via the evaluation system in this Website. The guidelines of decisions for publication are as follows:

Decision	Description
Accept	An accept decision means that an editor is accepting the paper with no further modifications. The paper will not be seen again by the editor or by the reviewers.
Reject	The manuscript is not suitable for the ICACT TACT publication.
Revision	The paper is conditionally accepted with some requirements. A revision means that the paper should go back to the original reviewers for a second round of reviews. We strongly discourage editors from making a decision based on their own review of the manuscript if a revision had been previously required.

■ Role of the Reviewer

Reviewer Webpage:

Once logined the Member Login menu in left, you can find out papers assigned to you. You can also login the Author Homepage assigned to you with the paper ID and author's eMail address. In there you can communicate each other via a Communication Channel Box.

Quick Review Required:

You are given 2 weeks for the first round of review and 1 week for the second round of review. You must agree that time is so important for the rapidly changing IT technologies and applications trend. Please respect the deadline. Authors undoubtedly appreciate your quick review.

Anonymity:

Do not identify yourself or your organization within the review text.

Review:

Reviewer will perform the paper review based on the main criteria provided below. Please provide detailed public comments for each criterion, also available to the author.

- How this manuscript advances this field of research and/or contributes something new to the literature?
- Relevance of this manuscript to the readers of TACT?
- Is the manuscript technically sound?
- Is the paper clearly written and well organized?
- Are all figures and tables appropriately provided and are their resolution good quality?
- Does the introduction state the objectives of the manuscript encouraging the reader to read on?
- Are the references relevant and complete?

Supply missing references:

Please supply any information that you think will be useful to the author in revision for enhancing quality of the paperor for convincing him/her of the mistakes.

Review Comments:

If you find any already known results related to the manuscript, please give references to earlier papers which contain these or similar results. If the reasoning is incorrect or ambiguous, please indicate specifically where and why. If you would like to suggest that the paper be rewritten, give specific suggestions regarding which parts of the paper should be deleted, added or modified, and please indicate how.

Journal Procedure

Dear Author,

- **You can see all your paper information & progress.**

- **Step 1. Journal Full Paper Submission**

Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Journal Paper/CRF Template

- **Step 2. Full Paper Review**

Using the evaluation system in the ICACT Website, the editor, reviewer and author can communicate each other for the good quality publication. It may take about 1 month.

- **Step 3. Acceptance Notification**

It officially informs acceptance, revision, or reject of submitted full paper after the full paper review process.

Status	Action
Acceptance	Go to next Step.
Revision	Re-submit Full Paper within 1 month after Revision Notification.
Reject	Drop everything.

- **Step 4. Payment Registration**

So far it's free of charge in case of the journal promotion paper from the registered ICACT conference paper! But you have to regist it, because you need your Journal Paper Registration ID for submission of the final CRF manuscripts in the next step's process. Once you get your Registration ID, send it to Secretariat@icact.org for further process.

- **Step 5. Camera Ready Form (CRF) Manuscripts Submission**

After you have received the confirmation notice from secretariat of ICACT, and then you are allowed to submit the final CRF manuscripts in PDF file form, the full paper and the Copyright Transfer Agreement. Journal Paper Template, Copyright Form Template, BioAbstract Template,

Journal Submission Guide

All the Out-Standing ICACT conference papers have been invited to this "ICACT Transactions on the Advanced Communications Technology" Journal, and also welcome all the authors whose conference paper has been accepted by the ICACT Technical Program Committee, if you could extend new contents at least 30% more than pure content of your conference paper. Journal paper must be followed to ensure full compliance with the IEEE Journal Template Form attached on this page.

➢ How to submit your Journal paper and check the progress?

Step 1. Submit	Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Using the Update button, you can change any information of journal paper related or upload new full journal paper.
Step 2. Confirm	Secretariat is supposed to confirm all the necessary conditions of your journal paper to make it ready to review. In case of promotion from the conference paper to Journal paper, send us all the .DOC(or Latex) files of your ICACT conference paper and journal paper to evaluate the difference of the pure contents in between at least 30% more to avoid the self replication violation under scrutiny. The pure content does not include any reference list, acknowledgement, Appendix and author biography information.
Step 3. Review	Upon completing the confirmation, it gets started the review process thru the Editor & Reviewer Guideline. Whenever you visit the Author Homepage, you can check the progress status of your paper there from start to end like this, " Confirm OK! -> Gets started the review process -> ...", in the Review Status column. Please don't miss it!

Volume 1, Issue 2

Beamforming Design of Decode-and-Forward Cooperation for Improving Wireless Physical Layer Security

Hui MA, Piming MA

School of Information Science and Engineering, Shandong University, China

maphoenix@126.com, mapiming@sdu.edu.cn

***Abstract*—Physical-layer-based security aims at ensuring the reliability of communication and preventing eavesdropping by taking advantage of the physical layer's characteristics rather than the data encryption in upper layer. Cooperation is a way to achieve this goal with many benefits for wireless communication. In particular, the cooperation scheme called decode-and-forward (DF) is discussed in this paper and our objective is to design the beamforming weight of each cooperating node which is one antenna equipped for maximum achievable secrecy rate. Considering that individual power constraint is more reasonable than total power constraint and to set noise power levels at the destination and the eavesdropper different is more practical than the same, we get the whole optimization problem which is unconvex. With the help of perfect global channel state information (CSI), the problem is solved through a way where convex optimization and one-dimensional search are combined together. And strict proofs are presented for this method. Then zero-forcing (ZF) based simplification and extension to cope with multi-antenna case are discussed. Numerical results show that the proposed design can significantly improve the security performance of wireless systems.**

***Index Terms*—physical layer security, maximum achievable secrecy rate, cooperating relays, beamforming, convex analysis.**

I. INTRODUCTION

SECURE data transmission plays an important role in wireless communication system. However, the open nature of wireless communication makes it vulnerable to wiretapping. At physical layer, this problem was first studied by Wyner [1] from an information-theoretic perspective. Wyner demonstrated that secure communication is possible without relying on private (secret) keys if the source-eavesdropper channel is a degraded version of the main (source-destination) channel, even though the eavesdropper has unlimited computation ability and know the coding/decoding scheme. He used a concept 'secrecy rate' to describe a rate at which information can be transmitted reliably in the main channel and can not be wiretapped by the eavesdropper, and defined 'secrecy capacity' as the maximal achievable secrecy rate. Then, Wyner's result was generalized to the Gaussian channel [2].In [3] secure communications over broadcast channels were studied by I. Csiszár and J. Körner. In recent years, considerable efforts have been made to extending this line of work to the fading channel like [4] ,[5].

To overcome the problem that the traditional single antenna system based PHY layer security approaches are infeasible when Wyner's condition is not met [1], [2], some recent works have been proposed to make up for this weakness by using multiple antenna technique e.g., multiple-input multiple-output (MIMO) [6-10], single-input multiple-output (SIMO) [11] and multiple-input single-output (MISO) [12-13].

Additionally, another more flexible and practical approach is relaying cooperation where the source to destination transmission is helped by relays. Totally, there are three cooperative schemes which can be used to provide security, i.e. decode-and-forward (DF), amplify-and-forward (AF) and cooperative jamming (CJ). And in particular, the security performance of DF based cooperation system has attracted much attention in recent years [14-17].

In [14] and [15], a DF based cooperative protocol was considered and beamforming vector of relays was designed for the achievable secrecy rate maximization or transmit power minimization. However these works just took the circumstance with a total power constraint into account.

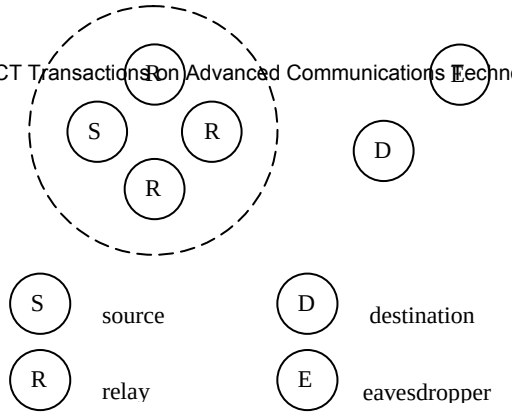
Because relays are distributed and independent in many applications, individual relay power constraints are more reasonable than the total power constraint in these case. As a complement, Junwei Zhang considered the maximization of the secrecy rate of DF model with individual relay power constraints through semidefinite programming (SDP) in [16]. But the optimal value we got through the SDP problem may not be the maximum secrecy rate of the system, because there is no proof that can show the existence of rank-one optimal solutions of the SDP problem in [16].

Figure 1. System model

In this paper, a more practical system model with different noise power at different nodes than that in [16] is studied.

Manuscript received May 15, 2012.

H. Ma and P.M. Ma are with the School of Information Science and Engineering, Shandong University, Jinan, China(corresponding author, P.M. Ma to provide phone:+86-531-88364613; fax:+86-531-88364613; e-mail: mapiming@ sdu.edu.cn).



Based on this model where each cooperating node is one antenna equipped, a new algorithm is proposed by combining the convex optimization and the one-dimensional search together to obtain the maximum achievable secrecy rate with sufficient proofs. Then a simplified problem with zero-forcing (ZF) constraint is discussed. Further more, in the end, the proposed algorithm is generalized to cope with the more complicate multi-antenna case.

This paper is organized as follows. In Section II, we will introduce the system model and the DF-based cooperative protocol. In Section III, we will propose and prove our algorithm for the maximum secrecy rate and the corresponding beamforming vector. Then we discuss the simplified problem in Section IV and the extension in Section V. Simulation results are presented in Section VI, and conclusions are given in Section VII.

II. System Model and Cooperative Protocol

In this paper, we first consider a scenario in which there is only one source node S, one eavesdropper node E, one destination node D and N relay nodes labelled as $\{R_0,.....,R_{N-1}\}$. As Figure 1 illustrates, the source and relays are in the same cluster, while the destination and eavesdropper are located far away from this cluster. Each network node is equipped with only an omni-directional antenna. All channels are flat fading, quasistatic and memoryless. The global CSI is available for system design. And thermal noise at all nodes is zero-mean white complex Gaussian. Besides, it is assumed that the number of relays is known before optimization.

The system works under a DF-based cooperative protocol. The protocol is divided into two stages and can be described as follows. In Stage I, the source transmits a message to other nodes within the cluster, and then the relays receive and decode it. When transmitting the symbol x_S, the received signal at the relay R_i can be expressed as

$$y_{R,i} = x_S l_i + n_{R,i} \tag{1}$$

where $l_i \in \mathbb{C}$ denotes the channel between R_i and S and $n_{R,i}$ is the noise at R_i with variance $s_{R,i}^2$. As the distance between the source and the relays are not too long, the relays can decode the received signal properly. And the power of the signal broadcasted by the source would be small so that the faraway destination and eavesdropper can receive none of it.

In Stage II, relay nodes re-encode the decoded message and then cooperatively transmit weighted versions of the re-encoded symbols to the destination and the eavesdropper. When the re-encoded symbol x_S is transmitted by relays, the signal y_D which is received at D equals

$$y_D = \sum_{i=0}^{N-1} w_i h_i x_S + n_D \tag{2}$$

where $w_i \quad (i = 0,1,.....N-1)$ means the beamforming factor at R_i, $h_i \in \mathbb{C}$ is the channel between R_i and D, and n_D is the noise at D with variance s_D^2. Then the signal y_E which is the signal at E can be expressed as,

$$y_E = \sum_{i=0}^{N-1} w_i g_i x_S + n_E \tag{3}$$

where $g_i \in \mathbb{C}$ denotes the channel between R_i and E, and n_E is the noise at E with variance s_E^2. Without the loss of generality, all the symbols in the re-encoded message are normalized, i.e. $E[|x_S|^2] = 1$ where $E[\cdot]$ denotes expectation.

Let's define $\mathbf{w} = [w_0,....., w_{N-1}]^T$, $\mathbf{h} = [h_0,....., h_{N-1}]^H$, $\mathbf{g} = [g_0,....., g_{N-1}]^H$ and $R_{\mathbf{h}} = \mathbf{h}\mathbf{h}^H$, $R_{\mathbf{g}} = \mathbf{g}\mathbf{g}^H$ where superscripts $(\cdot)^T$ and $(\cdot)^H$ represent transpose and conjugate transpose respectively. Then the SNR at D and E can be expressed as $\gamma_D = |\mathbf{h}^H\mathbf{w}|^2 / s_D^2$ and $\gamma_E = |\mathbf{g}^H\mathbf{w}|^2 / s_E^2$ respectively. As discussed in [2], for a given $\mathbf{w}$ the secrecy capacity $C_S(\mathbf{w})$ is

$$\begin{aligned} C_S(\mathbf{w}) &= \max\{\frac{1}{2}(\log(1+\gamma_D) - \log(1+\gamma_E)), 0\} \\ &= \max\{\frac{1}{2}\log(\frac{1+\gamma_D}{1+\gamma_E}), 0\} \end{aligned} \tag{4}$$

III. Design for Achievable Secrecy Rate Maximization

Aiming at finding out the maximum achievable secrecy rate of this system which works under the protocol we described, it is obvious that we should try to maximize $C_S(\mathbf{w})$ via the design of the beamforming vector. Considering individual power constraints is more practical in the relay system, the problem what we are interested in is formulated as follows,

$$\begin{aligned} &\underset{\mathbf{w}}{\text{maximize:}} \quad C_S(\mathbf{w}) \\ &\text{subject to:} \quad |w_i|^2 \le p_i, \quad i = 0,...,N-1 \end{aligned} \tag{5}$$

where p_i is the power constraint for R_i, $\forall i = 0,...,N-1$.

Because of the property of function $\max\{\cdot,\cdot\}$ and $\log(\cdot)$, in order to solve (5), we could solve the following problem first,

$$\underset{\mathbf{w}}{\text{maximize:}} \quad \frac{1+\frac{\mathbf{w}^H R_{\mathbf{h}} \mathbf{w}}{s_D^2}}{1+\frac{\mathbf{w}^H R_{\mathbf{g}} \mathbf{w}}{s_E^2}} \qquad \text{subject to:} \quad |w_i|^2 \le p_i, \quad i = 0,\ldots,N-1 \tag{6}$$

which can be re-expressed as

$$\underset{\mathbf{w}}{\text{maximize:}} \quad \frac{s_E^2(s_D^2 + \mathbf{w}^H R_{\mathbf{h}} \mathbf{w})}{s_D^2(s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w})} \qquad \text{subject to:} \quad |w_i|^2 \le p_i, \quad i = 0,\ldots,N-1 \tag{7}$$

Because s_E^2 / s_D^2 is a constant, (7) can be simplified into

$$\underset{\mathbf{w}}{\text{maximize:}} \quad \frac{s_D^2 + \mathbf{w}^H R_{\mathbf{h}} \mathbf{w}}{s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w}} \qquad \text{subject to:} \quad |w_i|^2 \le p_i, \quad i = 0,\ldots,N-1 \tag{8}$$

However, solving (8) is challenging owing to its non-convex character. Motivated by [18] and [19], our method is to first study a subproblem with the denominator of (8)'s objective function fixed, and then use one dimension search to find the solution. Moreover, the strict proof of this method is presented.

A. Subproblem With Fixed $s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w}$

Fixing $s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w}$ in (8) to a scalar t, then our problem transforms into

$$\underset{\mathbf{w}}{\text{maximize:}} \quad \mathbf{w}^H R_{\mathbf{h}} \mathbf{w} \qquad \text{subject to:} \quad s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w} = t, \quad |w_i|^2 \le p_i, \quad i = 0,\ldots,N-1 \tag{9}$$

It is shown that the optimal objective value and optimal solution of (9) are influenced by t, which are defined as $f(t)$ and $\mathbf{w}^*(t)$ respectively. To indicate the relationship between the optimal value of (8) and (9), we define a new function $R(t) = (f(t) + s_D^2)/t$. Definitely, if t^* maximizes $R(t)$, then $R(t^*)$ is the optimal value of (8) and $\mathbf{w}^*(t^*)$ is also the optimal point of it.

However, (9) is also difficult to tackle because of the existence of equality constraint. In order to overcome this, we changes (9) into the following optimization problem,

$$\underset{\mathbf{w}}{\text{maximize:}} \quad \mathbf{w}^H R_{\mathbf{h}} \mathbf{w} \qquad \text{subject to:} \quad s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w} \le t, \quad |w_i|^2 \le p_i, \quad i = 0,\ldots,N-1 \tag{10}$$

Let's define the optimal value of (10) as $f_1(t)$ and the corresponding optimal point as $w_1^*(t)$. Let $R_1(t) = j(t)/t$ where $j(t) = f_1(t) + s_D^2$ and denote $R_1(t)$'s maximum point as t_1. Then we will have the conclusion stated in theorem 1 as follows.

Theorem 1: $w_1^*(t_1)$ is the optimal point of (8), and $R_1(t_1)$ is its optimal value.

Proof:

When $t = t^*$, $\mathbf{w}^*(t^*)$ is the optimal point of (9) and also is the feasible point of (10). So $f_1(t^*) \ge f(t^*)$. Then we have the relation below,

$$\max_t R_1(t) = R_1(t_1) \ge R_1(t^*) \quad R(t^*) = \max_t R(t) \tag{11}$$

In addition, when $t = t_1$, assume that $\mathbf{w}_1^*(t_1)^H R_{\mathbf{g}} \mathbf{w}_1^*(t_1) + s_E^2 = t_2 < t_1$. Then we have $f_1(t_1) = f_1(t_2)$. Because $t_2 < t_1$, $R_1(t_2) > R_1(t_1)$, which contradicts with the fact that t_1 is the maximum point of $R_1(t)$. So we have

$$\mathbf{w}_1^*(t_1)^H R_{\mathbf{g}} \mathbf{w}_1^*(t_1) + s_E^2 = t_1. \tag{12}$$

Then in order to obtain $f_1(t_1)$ and $\mathbf{w}_1^*(t_1)$ we could focus on the following problem,

$$\underset{\mathbf{w}}{\text{maximize:}} \quad \mathbf{w}^H R_{\mathbf{h}} \mathbf{w} \qquad \text{subject to:} \quad s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w} = t_1, \quad |w_i|^2 \le p_i, \quad i = 0,\ldots,N-1 \tag{13}$$

Comparing (13) with (9), it is obvious that $f_1(t_1) = f(t_1)$ so we can got

$$\max_t R_1(t) = R_1(t_1) = R(t_1) \le \max_t R(t) \quad R(t^*) \tag{14}$$

Combine (11) and (14) together, we have

$$\max_t R_1(t) = \max_t R(t). \tag{15}$$

According to (13) and (15), t_1 is also $R(t)$'s maximum point, and $\mathbf{w}_1^*(t_1)$ is also (8)'s optimal point. ■

In the light of Theorem 1, we can find out the maximum point of $R_1(t)$ through solving (10) instead of trying to calculate the complicate problem (8) directly. However (10) is also non-convex. In order to solve (10), we define a convex optimization problem as follows

$$\underset{\mathbf{w}}{\text{maximize:}} \quad \mathrm{Re}(\mathbf{w}^H \mathbf{h}) \qquad \text{subject to:} \quad s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w} \le t, \quad |w_i|^2 \le p_i, \quad i = 0,\ldots,N-1 \tag{16}$$

where $\mathrm{Re}(\mathbf{w}^H \mathbf{h})$ is the real part of $\mathbf{w}^H \mathbf{h}$. Then we have the following theorem.

Theorem 2: The optimal solution of problem (16) is also the optimal solution of (10).

Proof:

Assuming that $\mathbf{w}_R^*(t)$ is an optimal solution of (16), then we have

$$\mathrm{Re}^2((\mathbf{w}_R^*(t))^H \mathbf{h}) = (\mathbf{w}_R^*(t))^H R_{\mathbf{h}} (\mathbf{w}_R^*(t)) \tag{17}$$

Supposing that the former equation is invalid, then we have

$(\mathbf{w}_R^*(t))^H R_{\mathbf{h}}(\mathbf{w}_R^*(t)) > \mathrm{Re}^2((\mathbf{w}_R^*(t))^H\mathbf{h})$? . So we can find out v ? $[,2p)$ make $\mathrm{Re}^2((\mathbf{w}_R^*(t)e^{jv})^H\mathbf{h}) = (\mathbf{w}_R^*(t)e^{jv})^H R_{\mathbf{h}}(\mathbf{w}_R^*(t)e^{jv})$ and $\mathrm{Re}((\mathbf{w}_R^*(t)e^{jv})^H\mathbf{h}) > 0$. So $\mathrm{Re}((\mathbf{w}_R^*(t)e^{jv})^H\mathbf{h}) > \mathrm{Re}((\mathbf{w}_R^*(t))^H\mathbf{h})$ which contradicts that $\mathbf{w}_R^*(t)$ is an optimal solution of (16). Then we have (17).

Definitely $\mathbf{w}_R^*(t)$ is also a feasible point of (10) so

$$(\mathbf{w}_R^*(t))^H R_{\mathbf{h}}(\mathbf{w}_R^*(t)) \pounds f_1(t). \tag{18}$$

Now considering the fact that $\$t$? $[,2p)$ which can make $\mathrm{Re}^2((\mathbf{w}_1^*(t)e^{jt})^H\mathbf{h}) = (\mathbf{w}_1^*(t)e^{jt})^H R_{\mathbf{h}}(\mathbf{w}_1^*(t)e^{jt})$ and $\mathrm{Re}((\mathbf{w}_1^*(t)e^{jt})^H\mathbf{h})$? . Here we can find that $\mathbf{w}_1^*(t)e^{jt}$ is still the optimal point of (10) and the feasible point of (16). So

$$\begin{aligned}\mathrm{Re}^2((\mathbf{w}_R^*(t))^H\mathbf{h}) &\,\³\, \mathrm{Re}^2((\mathbf{w}_1^*(t)e^{jt})^H\mathbf{h}) \\ &= (\mathbf{w}_1^*(t)e^{jt})^H R_{\mathbf{h}}(\mathbf{w}_1^*(t)e^{jt}) = f_1(t)\end{aligned} \tag{19}$$

(17), (18), (19) together lead $(\mathbf{w}_R^*(t))^H R_{\mathbf{h}}(\mathbf{w}_R^*(t)) = f_1(t)$ which means $\mathbf{w}_R^*(t)$ is an optimal point of (10). ■

B. Search for the Optimal Solution

In order to obtain $R_1(t)$'s maximum point through which we could find out $w_1^*(t_1)$, let's state some properties of $f_1(t)$ and $R_1(t)$.

Theorem 3: $j(t)$ is a concave function of t.

Proof:

The proof is similar to the steps performed in [19, section IV], and therefore is sketched.

We convert (16) into an equivalent real case as shown below,

$$\begin{aligned}&\underset{\mathbf{W}}{\text{maximize:}} && \mathbf{W}^T\mathbf{H} \\ &\text{subject to:} && s_E^2 + \mathbf{W}^T\mathrm{P}_{\mathbf{g}}\mathbf{W} \text{ ? } t \\ &&& W_i^2 + W_{i+N}^2 \text{ ? } p_i,\quad i = 0,\ldots,N-1\end{aligned} \tag{20}$$

where $\mathbf{W} = [\mathrm{Re}^T(\mathbf{w}), \mathrm{Im}^T(\mathbf{w})]^T$, $\mathrm{P}_{\mathbf{g}} = [\mathrm{Re}(R_g), -\mathrm{Im}(R_g); \mathrm{Im}(R_g), \mathrm{Re}(R_g)]$. And $\mathrm{Im}(R_g)$ is the imaginary part of matrix R_g, W_i is the ith element of vector $\mathbf{W}$.

Then considering the following convex optimization problem,

$$\begin{aligned}&\underset{\mathbf{W}}{\text{minimize:}} && -\mathbf{W}^T\mathbf{H} \\ &\text{subject to:} && s_E^2 + \mathbf{W}^T\mathrm{P}_{\mathbf{g}}\mathbf{W} \text{ ? } t \\ &&& W_i^2 + W_{i+N}^2 \text{ ? } p_i,\quad i = 0,\ldots,N-1\end{aligned} \tag{21}$$

it is obvious that (21)'s optimal value is the opposite to (20)'s and they have the same optimal solutions. The Lagrangian of (21) is

$$\begin{aligned}L(\mathbf{W}, m, \boldsymbol{l}) &= -\mathbf{W}^T\mathbf{H} + m(s_E^2 + \mathbf{W}^T\mathrm{P}_{\mathbf{g}}\mathbf{W} - t) \\ &\quad + \sum_{i=0}^{N-1} l_i(W_i^2 + W_{i+N}^2 - p_i) \\ &= \mathbf{W}^T\left(-\frac{\mathrm{HH}^T}{\mathbf{W}^T\mathrm{H}} + m\mathrm{P}_{\mathbf{g}} + \begin{bmatrix}\mathrm{diag}(\boldsymbol{l}) & 0_{N\times N}\\ 0_{N\times N} & \mathrm{diag}(\boldsymbol{l})\end{bmatrix}\right)\mathbf{W} \\ &\quad + ms_E^2 - mt - \sum_{i=0}^{N-1} l_i p_i\end{aligned} \tag{22}$$

Then the dual objective function is $G(m,\boldsymbol{l}) = \underset{\mathbf{W}}{\text{minimize}} L(\mathbf{W}, m, \boldsymbol{l})$ which reaches the minimum at $\mathbf{W}^*$ which is an optimal solution of (21). So

$$\begin{aligned}&G(m,\boldsymbol{l}) = \\ &(\mathbf{W}^*)^T\left(-\frac{\mathrm{HH}^T}{(\mathbf{W}^*)^T\mathrm{H}} + m\mathrm{P}_{\mathbf{g}} + \begin{bmatrix}\mathrm{diag}(\boldsymbol{l}) & 0_{N\times N}\\ 0_{N\times N} & \mathrm{diag}(\boldsymbol{l})\end{bmatrix}\right)\mathbf{W}^* \\ &+ ms_E^2 - mt - \sum_{i=0}^{N-1} l_i p_i.\end{aligned} \tag{23}$$

Through a similar way in [19], (21)'s dual problem can be written as

$$\begin{aligned}&\underset{m,\boldsymbol{l}}{\text{maximize}} && ms_E^2 - mt - \sum_{i=0}^{N-1} l_i p_i \\ &\text{subject to } m\text{?} \\ &&& \boldsymbol{l} \text{ f\_ } 0 \\ &&& -\frac{\mathrm{HH}^T}{(\mathbf{W}^*)^T\mathrm{H}} + m\mathrm{P}_{\mathbf{g}} + \begin{bmatrix}\mathrm{diag}(\boldsymbol{l}) & 0_{N\times N}\\ 0_{N\times N} & \mathrm{diag}(\boldsymbol{l})\end{bmatrix} \text{ f\_ } 0\end{aligned} \tag{24}$$

Then (20)'s duality can be got through writing out the opposite of (24):

$$\begin{aligned}&\underset{m,\boldsymbol{l}}{\text{minimize}} && mt + \sum_{i=0}^{N-1} l_i p_i - ms_E^2 \\ &\text{subject to } m\text{?} \\ &&& \boldsymbol{l} \text{ f\_ } 0 \\ &&& -\frac{\mathrm{HH}^T}{(\mathbf{W}^*)^T\mathrm{H}} + m\mathrm{P}_{\mathbf{g}} + \begin{bmatrix}\mathrm{diag}(\boldsymbol{l}) & 0_{N\times N}\\ 0_{N\times N} & \mathrm{diag}(\boldsymbol{l})\end{bmatrix} \text{ f\_ } 0\end{aligned} \tag{25}$$

Due to the convexity of (20), strong duality holds and the optimal value of (25) is $(\mathbf{W}^*)^T\mathrm{H}$. Definitely multiplied by $(\mathbf{W}^*)^T\mathrm{H}$, the optimal value of (25) becomes $((\mathbf{W}^*)^T\mathrm{H})^2$. From Theorem 2 we know that the square of optimal value of (20) is equal to (10)'s optimal value. From all this, the optimal value of the following problem is exactly $f_1(t)$:

$$\begin{aligned}&\underset{m,\boldsymbol{l}}{\text{minimize}} && (\mathbf{W}^*)^T\mathrm{H}mt + \sum_{i=0}^{N-1}(\mathbf{W}^*)^T\mathrm{H}l_i p_i - (\mathbf{W}^*)^T\mathrm{H}ms_E^2 \\ &\text{subject to } m\text{?} \\ &&& \boldsymbol{l} \text{ f\_ } 0 \\ &&& -\frac{\mathrm{HH}^T}{(\mathbf{W}^*)^T\mathrm{H}} + m\mathrm{P}_{\mathbf{g}} + \begin{bmatrix}\mathrm{diag}(\boldsymbol{l}) & 0_{N\times N}\\ 0_{N\times N} & \mathrm{diag}(\boldsymbol{l})\end{bmatrix} \text{ f\_ } 0\end{aligned} \tag{26}$$

As there must be $(\mathbf{W}^*)^T\mathrm{H}$? , by defining $m' = (\mathbf{W}^*)^T\mathrm{H}m$, $l_i' = (\mathbf{W}^*)^T\mathrm{H}l_i$ and $\boldsymbol{l}' = (l_0,\ldots,l_{N-1})^T$, (26) can be

expressed as,

$$\begin{aligned} &\underset{m,l}{\text{minimize}}\ \dot{m}t + \sum_{i=0}^{N-1} \dot{l}_i p_i - \dot{m}s_E^2 \\ &\text{subject to } \dot{m} \in \mathbb{R} \\ &\qquad \dot{l} \succeq 0 \\ &\qquad -\mathbf{H}\mathbf{H}^T + \dot{m}\mathbf{P}_{\mathbf{g}} + \begin{bmatrix} diag(\dot{l}) & 0_{N\times N} \\ 0_{N\times N} & diag(\dot{l}) \end{bmatrix} \succeq 0 \end{aligned} \tag{27}$$

Then $j(t)$ can be expressed as

$$\begin{aligned} &\underset{m,l}{\text{minimize}}\ \dot{m}t + \sum_{i=0}^{N-1} \dot{l}_i p_i - \dot{m}s_E^2 + s_D^2 \\ &\text{subject to } \dot{m} \in \mathbb{R} \\ &\qquad \dot{l} \succeq 0 \\ &\qquad -\mathbf{H}\mathbf{H}^T + \dot{m}\mathbf{P}_{\mathbf{g}} + \begin{bmatrix} diag(\dot{l}) & 0_{N\times N} \\ 0_{N\times N} & diag(\dot{l}) \end{bmatrix} \succeq 0 \end{aligned} \tag{28}$$

(28) is a point-wise minimum of a family of affine functions, so $j(t)$ is concave[20, p.80]. ■

Theorem 4: $R_1(t)$ is a quasiconcave function of t.

Proof:

Suppose $p(x)$ is a concave function and $q(x)$ is a convex function, with $p(x) > 0$ and $q(x) > 0$ on a convex set C. We can easily get $f(x) = p(x)/q(x)$ is quasiconcave on C according to the theorem in [20, p.103]. Then at the base of Theorem 3, it can be concluded that $R_1(t)$ is quasiconcave for $j(t) > 0$ is concave, $t > 0$ is affine (so convex). ■

Theorem 5: There's at most a single interval in $Dom(R_1(t))$ where $R_1(t)$ is invariant and any t belongs to this interval will be the maximum point of $R_1(t)$. Here $Dom(R_1(t))$ represents the domain of $R_1(t)$.

Proof:

First, let's consider the fact that $R_1(t) = C$ in an interval if and only if $j(t) = Ct$. Then we just need to prove that there's only a single interval in $Dom(R_1(t))$ where $j(t)$ is proportional to t.

Part I:

Assume $j(t) = Ct$ on two separate interval $[a,b]$ and $[c,d]$ where $a < b < c < d$. Then we can get $j(t)$ is no bigger than Ct on $[b,c]$ from (28). As $j(t)$ is concave, $j(qb + (1-q)c) \geq qj(b) + (1-q)j(c)$ $q \in [0,1]$ [20, p. 67] which means $j(t)$ is no smaller than Ct on $[b,c]$. Consequently, we have $j(t) = Ct$ on $[b,c]$. Therefore, there is only a single interval where $j(t) = Ct$.

Part II:

Assume $j(t) = Ct$ on $[a,b]$ and $j(t) = C_1 t$ on $[c,d]$ with $a < b < c < d$ and $C \neq C_1$. Because of (28) we have $j(t) = Ct < C_1 t$ on $[a,b]$. As $t > 0$, $C < C_1$. Similarly, $j(t) = C_1 t < Ct$ on $[c,d]$. As $t > 0$, $C > C_1$. Then contradiction appears. As a result, there is at most a single straight line through the original which partly overlaps with $j(t)$.

Combining the two parts above, we could easily get that there's at most a single interval in $Dom(R_1(t))$ where $R_1(t)$ is constant.

Suppose $j(t) = Ct$ if and only if $t \in [a,b]$, $a \neq b$. Then from (28) we know $j(t_2) < Ct_2$ for $t_2 > b$. So

$$R_1(t_2) = \frac{j(t_2)}{t_2} < \frac{Ct_2}{t_2}. \tag{29}$$

Through the similar way, for $t_1 < a$, there is

$$R_1(t_1) < \frac{Ct_2}{t_2}. \tag{30}$$

Through (29) and (30), we can conclude $R_1(t)$ achieves its maximum for $\forall t \in [a,b]$ as $R_1(t) = C$ on $[a,b]$. ■

Considering Theorem 3-5, we will find that the optimal point and maximum value of $R_1(t)$ can be efficiently got using Golden Section method which is one of the classic one dimensional search algorithms. Before using this algorithm, we should find an interval including the optimal point of $R_1(t)$. Denote $[t_{\min}, t_{\max}]$ as this interval. Definitely, $t_{\min}$ would be s_E^2, and $t_{\max}$ would be the optimal value of the following problem,

$$\begin{aligned} &\underset{\mathbf{w}}{\text{maximize:}}\ \ s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w} \\ &\text{subject to:}\ \ |w_i|^2 \leq p_i,\ \ i = 0,\ldots,N-1 \end{aligned}. \tag{31}$$

The complete algorithm is summarized as follows.

Proposed Algorithm

1: **Input:** s_D^2, s_E^2, p_i, $\mathbf{g}$, $\mathbf{h}$.
2: **begin**
3: initialize $t_{\min}$, $t_{\max}$, $len = t_{\max} - t_{\min}$.
4: **while** $len > e$, where e is the threshold.
5: $t_{left} = t_{\max} - 0.618(t_{\max} - t_{\min})$.
6: $t_{right} = t_{\min} + 0.618(t_{\max} - t_{\min})$.
7: calculate $R_1(t_{left}), R_1(t_{right})$.
8: **if** $R_1(t_{left}) < R_1(t_{right})$.
9: $t_{\min} = t_{left}$.
10: **else if** $R_1(t_{left}) > R_1(t_{right})$

11: $t_{\max} = t_{right}$

12: **else**

13: $t_{\min} = t_{left}$.

14: $t_{\max} = t_{right}$.

15: **end**

16: $len = t_{\max} - t_{\min}$

17: **end**

18: $t_1 = (t_{\max} + t_{\min})/2$

19: take $t = t_1$ into (16) to find out $\mathbf{w}^*$.

20: calculate $C_S(\mathbf{w}^*) = \max\{\log(s_E^2 R_1(t_1)/s_D^2)/2, 0\}$.

21:**end**.

22:**output:** $\mathbf{w}^*, C_S(\mathbf{w}^*)$.

IV. ZF Constraint Based Simplification

As discussed above, maximizing $C_S(\mathbf{w})$ under individual power constraint is a complicate problem. In this section, we simplify the problem using a zero-forcing (ZF) constraint on the receiving signal at the eavesdropper, which is equivalent to asking $\mathbf{w}^H R_{\mathbf{g}} \mathbf{w} = 0$. It is clear from (5) that the optimal $\mathbf{w}$ under ZF constraint is given by

$$\begin{aligned} \underset{\mathbf{w}}{\text{maximize:}}\ & \mathbf{w}^H R_{\mathbf{h}} \mathbf{w} \\ \text{subject to:}\ & \mathbf{w}^H R_{\mathbf{g}} \mathbf{w} = 0 \\ & |w_i|^2 \le p_i,\quad i = 0,\ldots,N-1 \end{aligned} \tag{32}$$

From the analysis similar to that in Theorem 2, we have (32)'s optimal solution can be got through solving the convex problem

$$\begin{aligned} \underset{\mathbf{w}}{\text{maximize:}}\ & \mathrm{Re}(\mathbf{w}^H \mathbf{h}) \\ \text{subject to:}\ & \mathbf{w}^H \mathbf{g} = 0 \\ & |w_i|^2 \le p_i,\quad i = 0,\ldots,N-1 \end{aligned} \tag{33}$$

Then the maximum secrecy rate under ZF constraint can be written as

$$\max\{\frac{1}{2}\log(1 + \frac{(\mathbf{w}_z^*)^H R_{\mathbf{h}} (\mathbf{w}_z^*)}{s_D^2}), 0\} \tag{34}$$

where $\mathbf{w}_z^*$ is an optimal solution of (33). Note that this value is just sub-optimal, because of the existence of the ZF constraint.

V. Extension to Multi-antenna case

In this section, we will study a more complex scenario as an extension. In this scenario, relay nodes are equipped with multiple omni-directional antennas and other conditions are still the same as those in the former scenario. So in stage I, when the symbol x_S is transmitted, the received signal $y_{R,i}$ at R_i is

$$y_{R,i} = \sum_{j=0}^{N_i-1} x_S l_{i,j} + n_{R,i} \tag{35}$$

where $l_{i,j}$ means the channel between the source and R_i's jth antenna, N_i means the number of R_i's antenna, $n_{R,i}$ is the noise at R_i with variance $s_{R,i}^2$.

In stage II, when symbol x_S is transmitted, the received signal y_D at D equals

$$y_D = \sum_{i=0}^{N-1} \sum_{j=0}^{N_i-1} w_{i,j} h_{i,j} x_S + n_D \tag{36}$$

where $w_{i,j}$ $(i = 0,1,\ldots..N-1; j = 0,1,\ldots..N_i - 1)$ means the beamforming factor at R_i's jth antenna, $h_{i,j} \in \mathbb{C}$ is the channel between R_i's jth antenna and D, and n_D is the noise at D with variance s_D^2. The received signal y_E at E can be shown as,

$$y_E = \sum_{i=0}^{N-1} \sum_{j=0}^{N_i-1} w_{i,j} g_{i,j} x_S + n_E \tag{37}$$

where $g_{i,j} \in \mathbb{C}$ is the channel between R_i's jth antenna and E. Define $\mathbf{w}_i = [w_{i,0},\ldots., w_{i,N_i-1}]^T$, $\mathbf{w} = [\mathbf{w}_0^T,\ldots..,\mathbf{w}_{N-1}^T]^T$, $\mathbf{h}_i = [h_{i,0},\ldots.,h_{i,N_i-1}]^T$, $\mathbf{h} = [\mathbf{h}_0^T,\ldots..,\mathbf{h}_{N-1}^T]^H$, $\mathbf{g}_i = [g_{i,0},\ldots.,g_{i,N_i-1}]^T$, $\mathbf{g} = [\mathbf{g}_0^T,\ldots..,\mathbf{g}_{N-1}^T]^H$ and $R_{\mathbf{h}} = \mathbf{h}\mathbf{h}^H$, $R_{\mathbf{g}} = \mathbf{g}\mathbf{g}^H$. Then we can still express the SNR at D and E as $\Gamma_D = |\mathbf{h}^H \mathbf{w}|^2 / \sigma_D^2$ and $\Gamma_E = |\mathbf{g}^H \mathbf{w}|^2 / \sigma_E^2$ respectively. So the secrecy capacity for a given $\mathbf{w}$ can still be shown as (4).

In order to get the maximum achievable secrecy rate, in this section, the core optimization problem becomes

$$\begin{aligned} \underset{\mathbf{w}}{\text{maximize:}}\ & \frac{s_D^2 + \mathbf{w}^H R_{\mathbf{h}} \mathbf{w}}{s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w}} \\ \text{subject to:}\ & |\mathbf{w}_i|^2 \le p_i,\quad i = 0,\ldots,N-1 \end{aligned} \tag{38}$$

Here we still obtain a subproblem by fixing the denominator of (38)'s objective function as t and change the equality constraint of it by substituting "$\le$" for "$=$" to get another optimization problem. And then, we still denote $f(t)$ and $f_1(t)$ as the optimal value of the two optimization problem above respectively and define $\mathbf{w}^*(t)$, $R(t)$, t^*, $w_1^*(t)$, $R_1(t)$, $j(t)$, t_1 through the same way in section III. It can be seen that in this section we could have theorems similar with those stated in section III. For these theorems, what need to be noted is that (8), (10), (16) should be substituted by their counterpart, i.e. (38), (39), (40) respectively.

$$\underset{\mathbf{w}}{\text{maximize:}} \quad \mathbf{w}^H R_{\mathbf{h}} \mathbf{w}$$
$$\text{subject to:} \quad s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w} \le t \qquad (39)$$
$$|\mathbf{w}_i|^2 \le p_i, \quad i = 0, \ldots, N-1$$

$$\underset{\mathbf{w}}{\text{maximize:}} \quad \mathrm{Re}(\mathbf{w}^H \mathbf{h})$$
$$\text{subject to:} \quad s_E^2 + \mathbf{w}^H R_{\mathbf{g}} \mathbf{w} \le t \qquad (40)$$
$$|\mathbf{w}_i|^2 \le p_i, \quad i = 0, \ldots, N-1$$

So the proposed algorithm can be easily generalized to tackle the multi-antenna case.

VI. Simulation Result

In this section, simulations are carried out to investigate the performance of the proposed algorithm. For simplicity, we use a one-dimensional system model, as illustrated in Fig. 2, where the source, relays, destination and eavesdropper are along a horizontal line. What's more, because the source-relay distance and the distances between relays are very small compared to the source-destination distance and relay-destination distance, the source-destination distance and the distances between different relays and the destination can be considered as the same. So are the source-eavesdropper distance and the distances between the different relays and eavesdropper. To emphasize the effect of distance, a simple line-of-sight channel model which contains the pass loss and a random phase is used. Generally, we can express the channels as $h = d^{-c/2} e^{jq}$ where d is the distance, c is the path loss exponent chosen as 3.5 and random phase q is uniformly distributed over $[0, 2p)$. The number of relays is set to 6, i.e. $N = 6$ and the eavesdropper are fixed at 60 m. For individual power constraints, we assume each relay has the same power budget: $p_i = p_T / N$ where p_T represents the total power constraint of the DF based system. And the noise power $s_D^2 = -55\text{dBm}$ and $s_E^2 = -65\text{dBm}$.

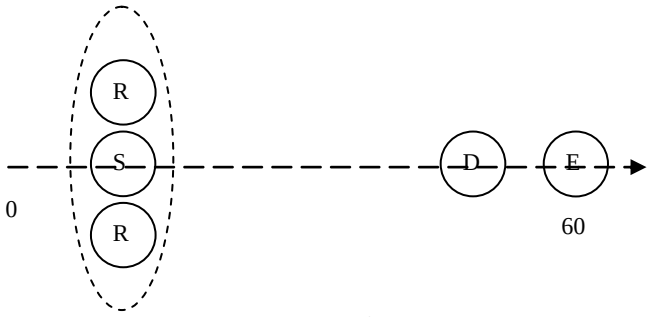


Figure 2. Model used for simulation

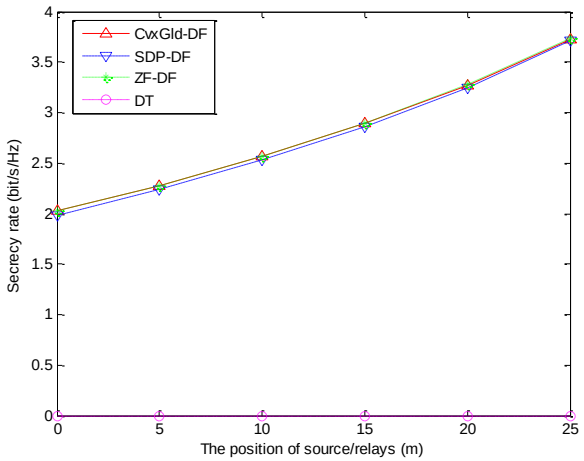


Figure 3. Secrecy rate versus the position of source/relays.

We will examine the maximum achievable secrecy rate of the DF based system calculated by the algorithm proposed in section III (labelled as CvxGld-DF) and the maximum secrecy rate under ZF constraint obtained by the simplified method discussed in section IV (labelled as ZF-DF). For comparison, we also examine the performance of direct transmission (DT) scheme and the SDP algorithm proposed in [16] (labelled as SDP-DF).

Firstly, we fix the position of destination at 50m and move the source/relays from 0 m to 25m. The transmit power is set as 10mdB for DT scheme. And for DF scheme p_T is also set as 10dBm. We can observe from Figure 3 that the maximum achievable secrecy rate always stays at 0 for DT. This is because the source-destination channel is always worse than the source-eavesdropper channel. And for all DF based algorithms, the curves coincided. Maximum secrecy rates got by three DF-based algorithms increase when relays move to the destination. This can be explained by the fact that even through the relay-destination channel and relay-eavesdropper channel both become better when the relays move from 0 to 25, the improving trend of the former is more remarkable.

Then we fix the source/relay location at 25m and move the destination from 40m to 100m with all other parameters unchanged. Figure 4 illustrate that there is a gap between the secrecy rate performances of the CvxGld-DF algorithm in this paper and the SDP-DF algorithm in [16] when the destination located at 90m and 100m. This means that we cannot get the

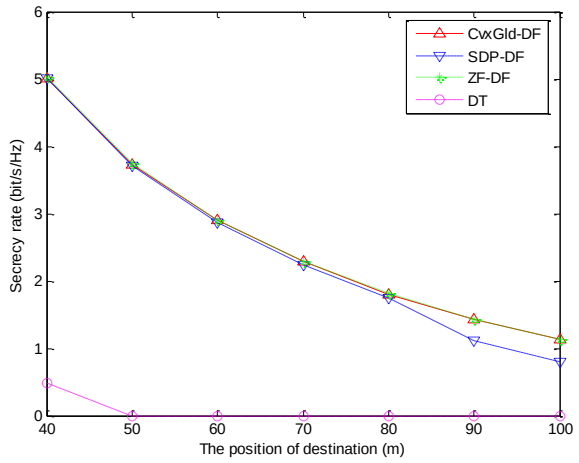


Figure 4. Secrecy rate versus the position of destiantion.

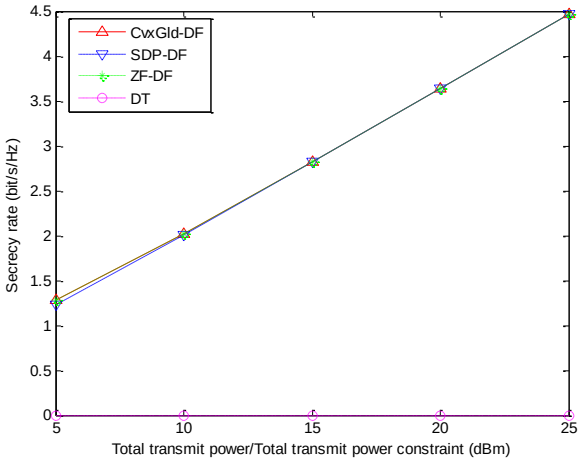


Figure 5. Secrecy rate versus total trasmit power/total transmit power constraint.

optimal beamforming vector through the SDP-DF algorithm in [16] sometimes. This problem comes from the reason that the rank of the optimal solution of the SDP optimization problem in [16] may be larger than one under some situation.

In Figure 5, we fix the destination and source/relays at 50m and 0m respectively and let p_T varies from 5dBm to 25dBm. Correspondingly, the transmit power of DT scheme also changes from 5dBm to 25dBm. Figure 5 shows that similar secrecy rate performances appear for all DF based algorithms with the increase of p_T. It is easy to understand that the secrecy rate performances become better when more power is allowed for transmitting. While for DT scheme, the maximum secrecy rate always stays at 0 even we use more power to transmit signals. This reveals that just enhancing transmit power is meaningless when Wyner's condition is not met for DT scheme.

In Figure 3, Figure 4 and Figure 5, there exists an interesting result that ZF-DF can always achieve nearly optimal performance. Thus we conjecture that, while we want to reach the maximum secrecy rate of an DF-based system under individual power constraint, the ZF constraint may be a good choice to simplify the optimization problem without leading much degradation. However, quantifying the impact of the ZF constraint remains an open problem.

VII. Conclusions

In this paper, we have considered a DF-based cooperative protocol to improve the physical layer security with one eavesdropper. Our attention is focused on the design of beamforming weight of each cooperating node which is one antenna equipped to find out the maximum secrecy rate. However our problem formulation is different from others because we assume a more practical scenario where the beamforming vector is subject to individual power constraints and noise power at different node is different. Under the assistance of perfect CSI, we have solved the optimal problem by combining convex optimization and one-dimensional search together and rigorous proof is presented for the correctness of our method. Further more, a simplified problem with zero-forcing (ZF) constraint and generalization to cope with the more complicate multi-antenna case are considered.

References

[1] A. D.Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, Jul. 1978.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels", *IEEE Trans. Inf. Theory*, vol. 54, no. 6, Jun. 2008.

[5] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, Oct. 2008.

[6] A. O. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[7] R. Negi and S. Goelm, "Secret communication using artificial noise," in *Proc. IEEE Vehicular Tech. Conf.*, Dallas, TX, Sep. 2005, vol. 3, pp. 1906–1910.

[8] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 2547–2553, Jun. 2009.

[9] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, Aug. 2007. [Online]. Available: http://arxiv.org/abs/0708.4219, submitted for publication.

[10] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, Oct. 2007 [Online]. Available: http://aps.arxiv.org/abs/0710.1920, submitted for publication.

[11] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, Australia, Sep. 2005, pp. 2152–2155

[12] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Conf. Information Sciences Systems*, Baltimore, MD, Mar. 2007, pp. 905–910

[13] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 2466–2470

[14] J. Li, A. P. Petropulu, and S. Weber, "Optimal cooperative relaying schemes for improving wireless physical layer security," Jan. 2010 [Online]. Available: http://arxiv.org/abs/1001.1389, submitted for publication

[15] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[16] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," Dec. 2009 [Online]. Available: http://arxiv.org/abs/0910.4132,submitted for publication
[17] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," Proc. *46th Annu. Allerton Conf. Commun., Control, Computing.*, Monticello, IL, Sep.-Oct. 2008.
[18] A.Wiesel, Y. C. Eldar, and A. Beck, "Maximum likelihood estimation in linear models with a Gaussian model matrix," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 292–295, May 2006.
[19] G. Zheng, L. Choo, and K. Wong, "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317—1322, Mar. 2011.
[20] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

Hui Ma received the B.S. degree in electrical engineering from Qufu Normal University, Rizhao, China, in 2010. Currently, he is working toward the M.S. degree in communication and information system in the School of Information Science and Engineering, Shandong University.

His research interests include physical layer security in multiple-input-multiple-output communication system and collaborative communication system.

Piming Ma received the B.S. degree in electrical engineering, the M.S. degree in signal processing and the Ph.D. degree in communications and information system from Shandong University, Jinan, China, in 1992, 1997 and 2005, respectively.

She is currently an Associate Professor in the School of Information Science and Engineering, Shandong University, Jinan, China. From 2008 to 2009, she was a Postdoctoral Fellow at the Ultra Wide Band Wireless Communications Research Center, Inha University, Nam-gu, Incheon, South Korea. She has published more than 20 technical (journal and conference) papers. Her search interests include LDPC codes, signal processing for wireless communications, software radio, physical layer security.

ZigBee RF Signal Strength for Indoor Location Sensing – Experiments and Results

K Subaashini, G Dhivya, R Pitchiah

Centre for Development of Advanced Computing (C-DAC), Chennai, India

***subaashinik@cdac.in*, *dhivyag@cdac.in*, rpitchiah@cdac.in**

***Abstract* -This paper discusses about the variation of signal strength due to the presence of obstacles in an indoor environment. An experimental analysis of impact of various obstacles on ZigBee RF signals strength has been done. The results obtained by the analysis have been used to locate a user inside a smart home. The parameters like Received Signal Strength (RSSI), Link Quality Indication (LQI) and Packet Error Rate (PER) has been measured and analyzed. The location of the user is an important context, based on which various controls and services can be rendered. The objective of finding out the location is to provide various services and controls like location based luminance, personalized HVAC systems. In this paper k mean clustering algorithm has been implemented to predict the location of the user. The results show that 3 to 5 m of location accuracy has been achieved.**

***Index Terms* — ZigBee, RSSI, Packet Error Rate, Localization, Fingerprinting**

I. INTRODUCTION

This paper discusses in detail about how RF signal strength is affected due to various obstacles that are generally found in indoor environments. The usual obstacles are materials like glass, wood, walls in addition to human activity. The analysis has been done in order to find out if signal strength alone can be used to find out the location of the user in order to provide various controls and services in indoor environment like smart home and buildings. The experiments have been done using two different radios RF230 and CC2430. The presence of human activity also affects the signal strength to a greater extent. All these effects on the RF signal strength have to be taken.

Manuscript received June 7, 2012. This work is developed under the project Development of ICT for Smart Buildings with Low Carbon Emission, funded by Department of Electronics and Information Technology (DeitY), Government of India.

Subaashini K. is with the Centre for Development of Advanced Computing, Chennai, India (Email: subaashinik@cdac.in)

Dhivya G is with the Centre for Development of Advanced Computing, Chennai, India (Email: dhivyag@cdac.in)

Pitchiah R is with the Centre for Development of Advanced Computing, Chennai, India (Email: rpitchiah@cdac.in)

Received signal strength indicator (RSSI) is a measure of the signal strength at the receiver expressed in dBm. It is usually five, eight or ten bit value depending on the hardware used. This RF signal strength parameter has been widely used for localization and tracking in indoors as it eliminates the requirement of additional hardware which in turn reduces the cost. Other measurements like Time of Arrival (ToA), Angle of Arrival (AoA) are also used. But time based methods have a disadvantage that line of sight is required for them to give a good level of accuracy which is not possible in indoor environments because of which RSSI is being preferred. More over according to our measurements round trip time of flight method did not give accurate results when the distance was small. Using RSSI means we don't need any extra hardware. But the biggest challenge is mapping of the signal strength to distance in presence of obstacles such as walls, human activity etc. The relation between the two has to be modeled as accurately as possible for developing a precise localization system. In a densely populated and dynamic environment where the modeling is not possible fingerprinting algorithms are used. Fingerprinting has a disadvantage that it requires a large measurement database that needs to be frequently calibrated. Now days to overcome the difficulty of large database compressive sensing techniques are being used. The next section discusses the related work which is followed by other sections that explains the experiments and results obtained.

II. RELATED WORK

Many location tracking systems have been developed based on various measurements of the RF signal. Of these Received signal strength is widely used for location sensing. There are two different types of localization based on RSSI measurement. They are range based and fingerprinting localization. In range based location sensing a relation between the signal strength and distance is derived. The relation ship is used for locating the unknown node by methods like Trilateration and Min-Max. Fingerprinting based methods have two phases. One is offline or training and the second is online phase. In this method the nodes are located by using algorithms like k nearest neighbor, Support vector machines etc… The signal strength has to be analyzed

using probability distribution and models like kalman filters for improving the accuracy of location.

RSSI and Link quality indicator (LQI) are the two parameters well known for link quality estimation. In [2] it has been mentioned that reflection, scattering and other physical properties have an extreme impact on the RSSI measurement. There are three models for describing the distance – path loss. They are free space model, two ray ground model which adds reflection to free space model and log-normal model. The lognormal model has to be derived experimentally. The authors of [2] have done experiments on three different radios and compared the results. They have concluded that RSSI is a bad estimator of link quality.

A survey of wireless indoor positioning techniques has been presented in detail in [3].various measuring principles and algorithms has been presented in this paper. It has been mentioned that the time based location methods are not suitable in Non Line Of Sight (NLOS) conditions and RSSI is preferred in NLOS conditions. If fingerprinting based location sensing has to be done algorithms like k Nearest Neighbors, neural networks, probabilistic methods, Support vector machines have to be used for location estimation. A comparison of localization systems such as UWB, GPS, Bluetooth, WLAN, and GSM has been presented.

Reference [4] proposes a virtual calibration procedure instead of doing a training phase for fingerprinting based location sensing methods. This method is not manual and makes use of measurements between the anchors. In our paper though the experiments are manual the measurements have been done using only the anchors and unknown node.

Paper [5] illustrates a technique to extract an estimate of velocity from signal strength. The characteristic footprints left by the motion of nodes in the network or motion of bodies external to the network have been exploited for movement detection. Experimental results have been presented using Micaz motes. The results are focused how signal strength is affected by motion of the motes. RSSI has been measured at different times and at different velocities. Our paper discusses how RSSI is varying due to obstacles inside a room. Results of [5] focus more on motion detection but our experiments focus on how to improve the location accuracy.

The authors of [6] discuss about the three techniques for automatic location sensing namely triangulation, scene analysis and proximity.

The authors of [7] have discussed about the various measurements, models and algorithms that are commonly used for device free localization. It has been suggested that device free localization is being developed which can be used to improve the existing Real Time Location Systems (RTLs). These methods use the fading characteristics of the RF signal strength for finding out the presence and location of the user. These are termed as sensor less localization as the user need not carry any radio for being localized.

It has been mentioned in [8] that fingerprinting algorithm cannot be used to track more than one user simultaneously. The impact of human presence on RF signal strength due to reflection, diffraction and scattering has been presented. Different models for establishing the relation between distance and signal strength has been described.

In the paper [9] experimental results how signal strength is affected by human presence and sensor node height has been presented. The variations in signal strength with and with out movement has been discussed in detail. Using the results an approach has been proposed for intrusion detection. A threshold has been defined to detect the motion. It has been concluded that the proposed system can be used along with other surveillance system for better accuracy

It has been proved in [10] that the location can be estimated in indoor environments up to accuracy of 1m using RSSI and ToA measurements which means the signal strength can modeled to get that level of accuracy.

In paper [12] the effect of ZigBee RSSI on crowd in an indoor environment has been discussed. Density, velocity and disorder are considered as measures to separate crowd behavior. A 25 pattern of crowd behavior in indoor space with the above measures has been defined. Data is analyzed using both time and frequency series analysis. Average RSSI, variance and median are considered for time series analysis and discrete Fourier analysis for frequency series analysis. A graph plotted between density per experimental area against velocity and disorder shows that with no crowd the RSSI value hardly changes and with crowd the RSSI fluctuates to a greater extent. This is due to the difference of electromagnetic wave absorption rate on the human body, rate of screening electromagnetic wave path and change in environment.

In [13] the RSSI values from WSN nodes are used for the real-time localization of transceiver-free objects. A customized classification approach based on support vector machine has been followed to determine location. The feasibility and effectiveness of the proposed approach has been assessed by experimental test cases.

The performance evaluation of IEEE802.15.4 wireless networks has been presented in [14]. The effect of direct and indirect data transmissions, CSMA-CA mechanisms, data payload size and non beacon enabled mode has been observed through several practical experiments. The data throughput, delivery ratio, and received signal strength indication (RSSI) are investigated as the performance metrics. It has been concluded that IEEE 802.15.4 has better performance in non-beacon mode. Through experiments the authors had achieved an average of 153.02 kbps for direct data transfer and 65.69 kbps for indirect data transfer. It had been concluded that the decrease in data rate for indirect transfer is due to the network device's polling rate. The results for the effects of CSMA-CA mechanism conclude that both the effective data rate and delivery ratio was decreased due to the presence of collisions and random back off. It has been observed that with the increase of payload size, the data rate also increased since the effect of overhead was reduced

leading to a raise of data coding efficiency. From the experiment, the authors of this paper found that the non beacon-enabled network would have larger data rate than the beacon-enabled one.

Statistical Mean Value Model, Distance Between the Fixed-nodes based Model and Gauss Model are the three experimental data processing models that have been discussed in [15]. In "Statistical Mean Value Model", unknown node receives a group of RSSI values and then computers their mean value. In "Distance Between the Fixed-nodes Model", the distance from unknown node to fixed node is computed by taking the distance and signal strength information between fixed nodes as the reference. Principle of "Gauss model" is that when an unknown node receives n RSSI values, there must be some values which are small probability events. ZigBee-based hardware platform and MATLAB are used to test the measurement error of the three methods. This paper concludes that the measurement error of Gauss model is 2 meters within 20 meters.

III. EXPERIMENTAL ANALYSIS

This section describes the measurement setup that has been used for taking the RSSI measurements. A set of measurements has been taken separately for each obstacle. The obstacles such as wood, glass, wall and human presence have been considered for these measurements.

A. Experimental setup

A set of two Crossbow's ZigBee motes (Micaz & IRIS) has been used. Micaz has an eight bit Received signal strength indicator (RSSI) and IRIS has a five bit RSSI. The motes have been programmed using TinyOS 2.x and NesC language. One node acts as a transmitter and the base station connected to PC acts a as a receiver which forwards the received packets to the serial port of the PC. Further packet processing is done at the PC using JAVA programming language. The transmitter and receiver were both kept at a height of 1m above the ground level. These measurements were taken inside a 15 m x 3 m x 2.6m C-DAC's Ubiquitous Computing Lab.

B. Measurements

One mote was programmed as transmitter that sends a packet every 1 second. The other was programmed in such a way that it receives the packet sent by the transmitter, appends the RSSI value and its Node Id, then forwards it to the serial port. The distance between the transmitter and receiver is known. The received packet is parsed and the RSSI and distance value is stored in the database. The above procedure was repeated for different distances between the transmitter and receiver. The measurements were taken initially in Line of Sight condition and later repeated by placing glass, wood and wall obstacle between the transmitter and receiver. The parameters that have been measured are Received Signal Strength Indication (RSSI), LQI and Packet Delivery Rate (PDR). The RSSI values are recorded as signed 2s complement form of the actual value. Later these hex values recorded were converted to actual dBm values according to the datasheets of the CC2420 and RF230 radios. Every packet transmitted is assigned a packet number to check for packet losses at the receiving end. After the measurements a simple localization system has been tested by fingerprinting method with a single reference node and also with multiple reference nodes.

IV. MEASUREMENT RESULTS

In this section the results obtained for various obstacles have been discussed. The measurements have been taken for both Line of Sight and Non Line of Sight conditions. The relationship between distance and RSSI has been obtained for each obstacle. The packet error rate has also been monitored along with RSSI in order to ensure that PER does not fall below 2%.

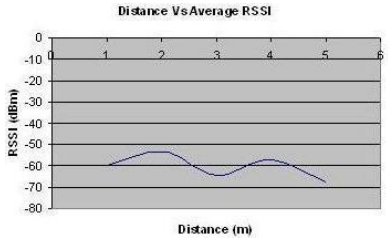


Figure 1.a. Distance vs Average RSSI (CC2420)

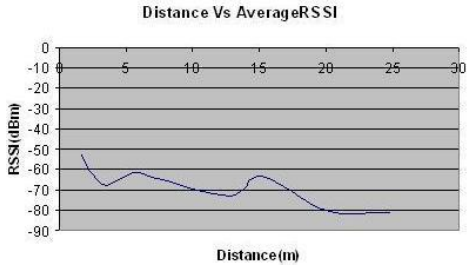


Figure 1.b. Distance vs Average RSSI (RF230)

A. Line of Sight

These measurements were taken without any obstacle or human activity between the transmitter and receiver. Fig.1a and 1b represents a plot of the distance and average RSSI for CC2420 and RF230 radios. At each distance 50 samples of RSSI have been recorded and an average has been taken.

The relationship between the distance and RSSI was obtained by interpolating and fitting a logarithmic curve using the data obtained. Equation (1) gives the relationship between distance and RSSI for RF230 radio.

$$r = -2.503 * \mathrm{Ln}(d) - 56.978 \quad (1)$$

Where r is the RSSI value in dBm and d is distance in meters. The packet error rate at different distances between the transmitter and receiver has also been estimated. The maximum allowed packet error rate is 2%.

$$\beta = 1 - \alpha \quad (2)$$

Where α is the packet delivery rate and β is the packet error rate. Fig. 2 shows the packet count versus average RSSI at different distances.

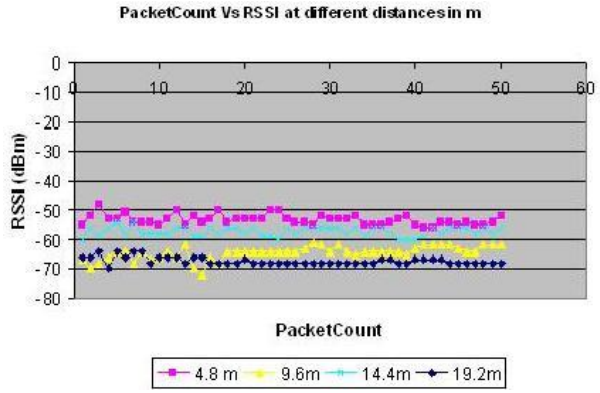


Figure 2. PacketCount vs Average RSSI at different distance between the Tx and Rx.

As long as the packet error rate is less than 2% the communication between the nodes is acceptable. If it is more than 2% the communication is no longer reliable. The RSSI value of the packets also should not fall below the receiver sensitivity for reliable communication. The PER was 0 % even when the distance between the transmitter and receiver was 25m.

The results in Fig. 2 were observed when there was no obstacle or movement between the transmitter and receiver. It can be observed that all the packets were received without any loss when there is no obstacle. The PER was 0% upto a range of 40m.The next section discusses results obtained for various obstacles.

B. Non line of sight

These measurements were taken by placing a glass, glass-wood and partial wall partitions in between the transmitter and receiver. The properties of the obstacles are shown in table I.

TABLE I PROPERTIES OF OBSTACLES

S.No	Obstacle type	Thickness (mm)
1.	Glass (Glazed Door)	10
2.	Glass + Wood (Compressed Wood)	Wood: 120 Glass: 6.35
3.	Partial Wall (Brick + Gypsum board)	35

Location estimation has to be done in lab environment with these obstacles. So to model the lab environment the above obstacles have been chosen. Fig 3.a, 3.b, 3.c shows the measurement results obtained when the obstacles where placed in between transmitter and receiver.

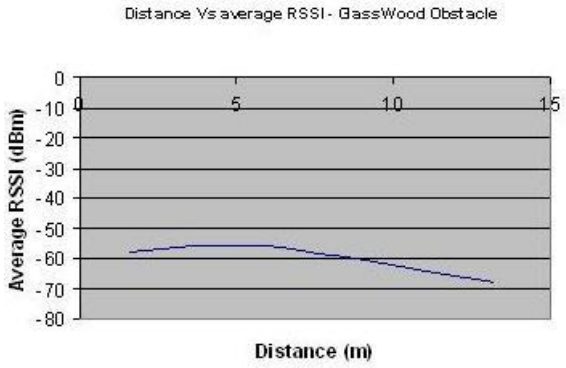


Figure 3.a. Distance vs Average RSSI (glass-wood partition)

When there is an obstacle the packet error rate is also an important parameter to be noted. The obstacles attenuate the signal, so chances for packet loss are more. It is very important to note that the packet error rate should not be above 2%.

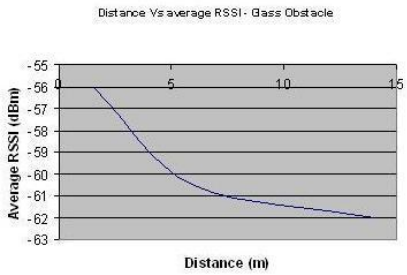


Figure 3.b. Distance vs Average RSSI (glass partition)

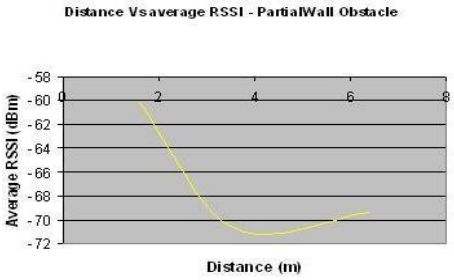


Figure 3.c. Distance vs Average RSSI (partial wall)

Fig 4.a, 4.b and 4.c show the PER results observed for different obstacles. When the measurement was taken through walls the range was reduced to 6.4m. If the distance between the transmitter and receiver was increased beyond 6.4 m, the PER was more than 2 %. So measurements results up to 6.4m are shown in the figure.

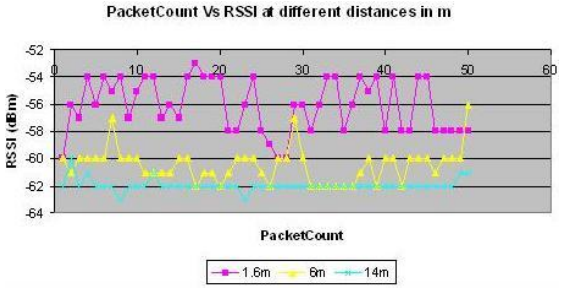


Figure 4.a. Glass wood partition

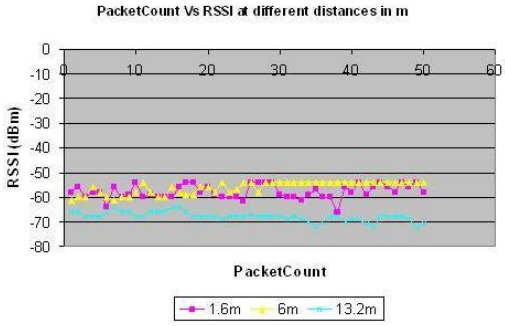


Figure 4.b. Partial wall

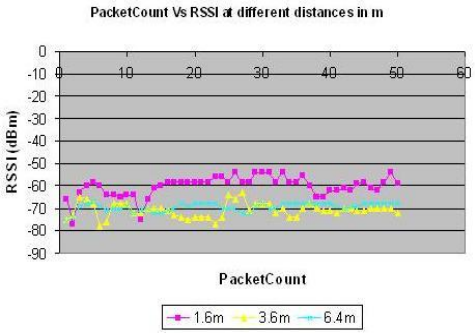


Figure 4.c. Glass door

But for the glass and glass wood obstacles the PER was less than 2% up to a range of 20m.

C. Human Presence

This section discusses about the impact of human presence on the received signal strength values. The measurements have been done for different crowd density by transmitting 1000 packets at the rate of 2 packets per second. The Fig 5.a and 5.b show how the RSSI and LQI values are affected by human presence.

The measurements had been taken by increasing the human count between the transmitter and receiver. It can be noted from Fig 5.a that the RSSI was having the maximum value (-75dBm) when no human was present between the transmitter and receiver.

With increase in human count the RSSI value decreased due to absorption and fading. When the person count was more than 2 the graph (Fig5.a) shows an increase in RSSI value due to reflection and scattering of RF signal. It was observed that the Link Quality remained at 255 through out the experiment up to a distance of 40m.

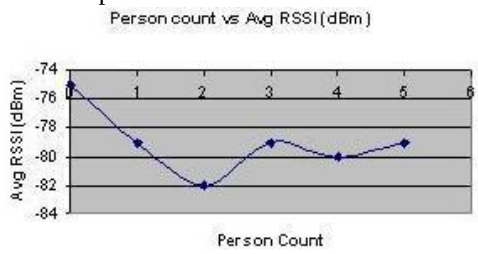


Figure 5.a. Person count vs. Average RSSI

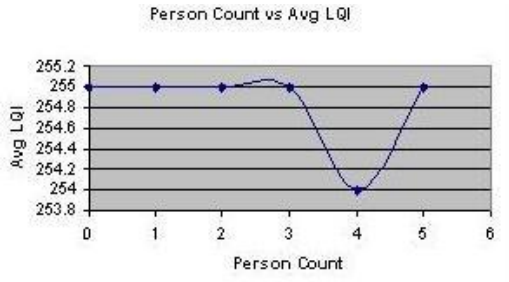


Figure 5.b. Person count vs. Average LQI

V. LOCALIZATION SENSING

After the measurement and analysis a localization algorithm has been implemented and tested inside the UBICOMP Lab of C-DAC Chennai. The location was estimated by fingerprinting method. Since the accuracy was less when simple fingerprinting was used clustering algorithm has been implemented to improve the location accuracy.

A. Location setup

The location sensing algorithm was implemented inside the UBICOMP Lab as shown in Fig 7. One reference or anchor mote has been placed at a known location inside the lab. AT86RF230 radio of Iris motes has been used. The transmission power was set at +0.5 dBm.

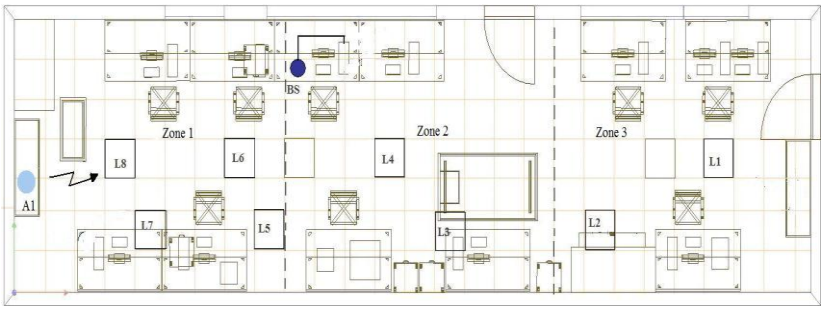


Figure 7. UBICOMP LAB L1, L2….L8 – Training points, A1 - anchor node

The reference or anchor mote (A1) has been placed at a height of 1.4 m above the ground level, so that it can receive the beacon message packet broadcasted by the unknown from any location inside the lab. The placement of reference mote has to be determined empirically. The user to be located will be carrying the unknown mote. The objective is to determine to which LED fixture the user is closer by. The location sensing involves two phases. One is offline and the second is online phase.

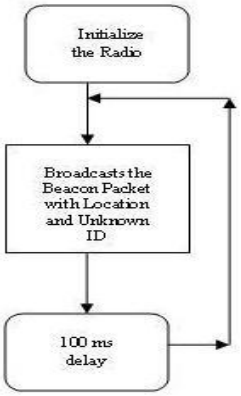


Figure 8a. Offline Phase - Unlnown Mote

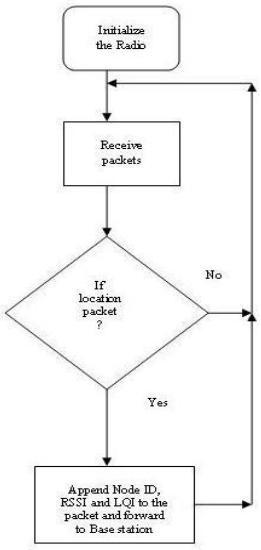


Figure 8b. Offline Phase – Anchor Mote (A1)

B. *Offline/Fingerprinting Phase*

Location estimation by fingerprinting has two phases. The first phase is training phase. The different states of the motes and process involved during the offline phase are shown in Fig 8a, b, c.

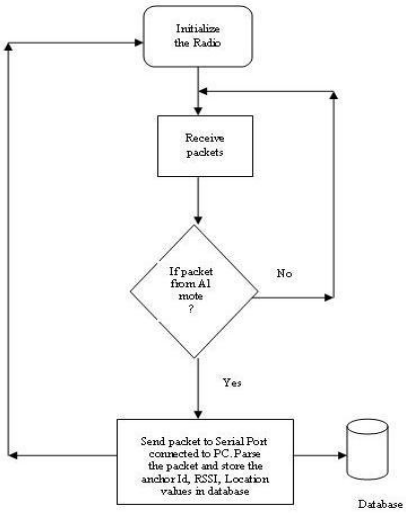


Figure 8c. Offline Phase – Base Station (BS)

The unknown node is placed at every location of interests (L1 to L8).It broadcasts a beacon packet every 100 ms which contains its Node ID and Location at which it is placed. The packet is received by the anchor mote A1. The mote A1 appends the RSSI value, LQI value and its Node ID to the packet and forwards to the Base station (BS) mote which is connected to PC. The BS forwards the packet to the serial port of the PC and the data is received and parsed. After parsing the packet, the Location, RSSI value and Anchor-Id are store in the database. The readings are taken for 1000 packets at every symbolic location in order to find out of the RSSI value that has the maximum probability at that particular location.

C. *Online Phase*

During the online phase, the unknown mote broadcasts a beacon every 100 ms. The anchor mote (A1) receives the broadcast packet and appends the RSSI value and forwards it to base station. At the base station the RSSI value obtained is compared with the fingerprinted values in the database and the maximum likely hood location is chosen. But the location accuracy varied from 1m to 8m. The location obtained has not been consistent for implementing in a smart home environment for Location based Lighting application.

D. *Online Phase with Clustering Algorithm*

In order to improve the accuracy of location, k-Mean Clustering algorithm [16] has been implemented. If a RSSI value that has not been fingerprinted (in the training phase)

occurs during online phase, the location could not be identified. To overcome this issue, Nearest Neighbor identification feature has been incorporated along with the clustering.

E. k Mean Clustering

During the offline phase the unknown mote is kept at every location of interest and the corresponding RSSI values are stored in the database (in PC) that is connected to the base station node. The RSSI data stored in the database is divided into a number of clusters using k mean clustering algorithm. The number of clusters has to be decided by the user. An initial set of centroids have to be chosen. The number of centroids is equal to the number of clusters into which the RSSI data set has to be divided. Each centroid belongs to different clusters.

According to the k mean clustering the Euclidean distance between a RSSI value and the each of the centroid is calculated. After calculating the Euclidean distance between the centroids and the RSSI value, the minimum distance is found out. The RSSI value is now added to the cluster which contains the closest centroid. This step is repeated for all the RSSI data set for one time. After the first iteration, a new set of centroid values is calculated by taking the average of each cluster elements and the same process of finding the minimum distance and clustering is done. The process is repeated until two consecutive iterations result in clusters with the same elements. Fig 9 describes the steps involved in k mean clustering algorithm.

Step 1: *Get the RSSI data set (R) stored in the database during the offline phase*
Step 2: *Let the number of clusters into which R has to be divided be N*
Step 3: *Let the number of centroids be C*
C = N
Set the values of C_0 ..... $C_n = R_0$ ..... R_n
Step 4: *Set the value of i as zero*
i = 0
Step 5: *Check if (i<R.length ())*
Step 5.1: Get R_i
Step 5.2: Calculate the Euclidean distance of R_i *from all the centroids* C_0 *to* C_n
Step 5.3: Find the centroid to which the element R_i *is closest and put the element in the cluster that contains the closest centroid.*
Step 5.4: i = i+1
Step 5.5: Go to Step 5
Step 6: *Calculate the new centroids*
The new centroid of each cluster is the average of the elements present in that cluster
Step 7: *Repeat steps 4 to 6*
Step 8: *The steps 4 to 6 iteration has to be repeated as long as two successive iterations results in the same set of N clusters.*
Step 9: *After completion of the iterations the clusters are stored in a new table in the database.*
Step 10: *The RSSI value, location and the number of times the RSSI value has occurred for a particular location are store in the table.*

Figure 9. Clustering Algorithm

During the online phase the average RSSI of 50 packets is taken as and identified to which cluster it belongs to. After cluster identification, the corresponding locations at which the RSSI value occurred have been retrieved. The final location is predicted based on the maximum number of times the RSSI value occurred for a location. Fig 10 explains the steps involved in predicting the location.

Step 1: *The cluster to which the current RSSI value belongs is determined by comparing the value with the cluster database table. (Result of the clustering algorithm). Let the value belong to ClusterN*
Step 2: *If the current RSSI value is not present in any of the clusters:*
Go to Step 5
Else
Go to Step 3
Step 3: *Search for the locations at which the current RSSI value only in the ClusterN*
Step 4: *If (it has occurred at only one location)*
Return that as the final location
Else if (it has more than one location)
Step 4.1: Get the number of times the RSSI value has occurred at the Locations.
Step 4.2: Find the location for which the RSSI value has occurred the Maximum number of times.
Step 4.3: Return that value as the final location
Step 5: *Implement the Nearest Neighbor algorithm*
Step 5.1: Calculate the Euclidean distance of the current RSSI value from all the elements of the RSSI data set obtained during the fingerprinting phase.
Step 5.2: Find the element which is the closest to the current RSSI values
Step 5.3: Repeat Step 3 and 4.
Step 6: *Wait for the next packet and go back to step 1*

Fig 10 Online phase with clustering and Nearest Neighbour Algorithm

If an RSSI value that has not been fingerprinted occurs then the algorithm first finds its nearest neighbor by directly finding the RSSI value that is closest to the fingerprinted data set. After getting the nearest neighbor value the previous steps of clustering and location prediction is followed.

F. Results

The location accuracy and precision has improved after using the clustering algorithm with the existing fingerprinting location sensing method. Table 2 gives the details of the accuracy obtained after using clustering and nearest neighbor algorithm.

TABLE II LOCATION ACCURACY

S.No	Actual Location (Symbolic)	Obtained Location (Symbolic)	Average Error (m)
1.	L1	L2, L4	5
2.	L2	L2, L1	2
3.	L3	L3	0.8
4.	L4	L4, L7	4
5.	L5	L5, L7	2
6.	L6	L6, L7	2
7.	L7	L6, L7	2
8.	L8	L8, L6, L7	3

VI. CONCLUSION AND FUTURE WORK

The results obtained after including a data classification method, shows that the RSSI based location sensing can be used for indoor environments if the accuracy levels of 3-5 m are acceptable. The algorithm has been tested to locate multiple users simultaneously. The location of the user obtained has been integrated with lighting to control the illuminance of LED Fixtures based on the location of the user. In this method frequent fingerprinting has to be done to retain the location accuracy. In future it is proposed to explore filtering techniques to improve the location accuracy.

ACKNOWLEDGMENT

The work is developed under the project Development of ICT Technologies for Smart Buildings with Low Carbon Emission, funded by Department of Electronics and Information Technology (DeitY), Government of India. We would like to thank Department of Information Technology for providing us this opportunity. We would also like to thank Mrs S. Sridevi, Senior Engineer, C-DAC, Chennai for her programming support for the clustering algorithm.

REFERENCES

[1] Hyo Sung Ahm and Wonpil Yu "Environmental Adaptive RSSI based indoor localization," in IEEE transactions on automation science and engineering, Vol6, No.4, October 2009

[2] K.Benkic, M.Malajner, P.Planinsic and Z.Cucei "Using RSSI value for distance estimation Wireless Sensor Networks based on Zigbee," in Systems, signals and image processing, 2008, IWSSIP 2008

[3] Hui Liu, Pat Banerjee and Jing Liu "Survey of wireless indoor positioning techniques and systems," IEEE Transactions on systems,man and cybernetics – PartC:Applications and reviews, Vol.37,No.6,Novemeber 2007

[4] Paolo Barsocchi, Stefano Chessa, Gaetano Giunta, G.Moruzzi "Virtual Calibrationfor RSSI-based indoor localization with IEEE 802.15.4," in the framework of the FP^ projects PERSONA and INTERMEDIA

[5] Kristen Woyach, Daneiele Puccinelli and Martin Haenggi, "Sensorless Sensing in Wireless Networks: Implementation and Measurements," in Proc. Int. Workshop Wireless Netw. Meas., Boston, MA, April 2006

[6] Jeffrey Hightower and Gaetano Borriello, "Location sensing techniques," pp. 57-66 of the August 2001 issue of IEEE Computer magazine

[7] Shinsuke Hara, Dapeng Zhao, Kentaro Yanagihara, Jumpei Taketsugu, Kiyoshi Fukui, Shigeru Fukunaga and Ken-ichi Kitayama "Propagation characterstics of IEEE 802.15.4 radio signal and their application for location estimation," in IEEE conference, 2005

[8] Neal Patwari and Joey Wilson, "RF Sensor Networks for – Device – Free Localization: Meaurements, Models and Algorithms," Vol.98, No.11, November 2010| Proceedings of the IEEE

[9] P.W. Lee, W.K Seah, H. Tan and Z. Yao, "Wireless sensing without sensors – an experimenal approach," in Proc. Int. Symp. Personal Indoor Mobile Radio Commun., pp. 62-66, Sep 2009

[10] Neal Patwari, Alfred O. Hero, Matt Perkins, Neiyer S. Correal and Robert J.O'Dea, "Relative Location Estimation in Wireless Sensor Networks," IEEE Transactions on Signal Processing, Vol.51, No.8, August 2003

[11] Kannan Srinivasan and Philips Levis, "RSSI is under appreciated," Proceedings of third workshop on embedded sensor nodes, 2006

[12] Masaya Arai, Hidenori Kawamura, Keiji Suzuki, "Estimation of ZigBee's RSSI fluctuated by Crowd Behavior in Indoor Space", SICE Annual Conference 2010, The Grand Hotel, Taipei, Taiwan ,August 18-21, 2010.

[13] F. Viani, L. Lizzi, P. Rocca, M. Benedetti, M. Donelli and A. Massa, "Object tracking through RSSI measurements in wireless sensor networks", ELECTRONICS LETTERS 8th May 2008 Vol. 44 No. 10

[14] Jin-Shyan Lee, "Performance Evaluation of IEEE 802.15.4 for Low-Rate Wireless Personal Area Networks", IEEE Transactions on Consumer Electronics, Vol. 52, No. 3, AUGUST 2006

[15] Zhang Jianwu and Zhang Lu, "Research on Distance Measurement Based on RSSI of ZigBee", ISECS International Colloquium on Computing, Communication, Control, and Management, IEE 2009

[16] http://people.revoledu.com/kardi/tutorial/kMean/index.html, accessed on Feb27th 2012.

K.Subaashini - This author has been working in Centre for Development of Advanced Computing, Chennai since November 2008. She has completed her Masters in Engineering in Embedded Systems from College of Engineering, Guindy, Anna University, Chennai in the year 2008. Her area of interests includes wireless sensor networks using Zigbee and ubiquitous computing for smart homes and buildings.

G.Dhivya – This author has been working in Centre for Development of Advanced Computing, Chennai since Nov 2006. She has completed her Bachelors in Engineering in Electrical & Electronics from Erode Sengunthar Engineering College, Affiliated to Anna University, Erode. Her area of interests includes wireless sensor networks using Zigbee and ubiquitous computing for smart homes and buildings.

R.Pitchiah - This author has functioned as Group Coordinator, Real-time Systems Development Group at C-DAC, Bangalore from 1995 to 2002, and was responsible for architecting R&D projects in the area of Dependable Computing. He had functioned as Programme Coordinator, in National Ubiquitous Computing Research Centre at C-DAC Chennai and has been the Principal Coordinator for many R&D projects. He is currently working as a scientist in Department of Electronics and Information technology, India. He has co-authored more than 10 research publications in National/ International conferences/workshops.

Quantum Communication Scheme for Blind Signature with Arbitrary Two-Particle Entangled System

Jinjing Shi[1], Ronghua Shi[1], Xiaoqi Peng[2] and Moon Ho Lee[3], *Senior Member, IEEE*
[1]School of Information Science & Engineering, Central South University, Changsha 410083, China.
[2]Department of Information Science & Engineering, Hunan First Normal University, Changsha 410205, China.
[3]Institute of Information and Communication, Chonbuk National University, Chonju 561-756, Korea.

***Abstract*—A quantum communication scheme for blind signature is proposed based on two-particle entangled quantum system to create a novel systemetrical quantum cryptosystem. All the messages are encrypted by the private key of the sender Alice during the communication and the authenticity verification of signatures and an arbitrator's batch efficient proxy signature is applied. It demonstrates that a large number of blind signatures can be derived with the characteristics: impossibility of forgery, impossibility of disavowal by the signatory and impossibility of denial by the receiver. The security of our scheme depends on the two-particle entangled system which cannot be deterministically intercepted.**

***Index Terms*—Quantum communication, Blind signature, Proxy signature, Quantum signature, Quantum cryptography.**

I. INTRODUCTION

A classical digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document. It ensures that the original content of the message or document is unchanged [1]. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. A blind signature introduced by David Chaum [2] is typically employed in privacy-related protocols and realized by using a number of common public key signing schemes [3]. Fan and Lei [4] proposed a scheme based on the quadratic residues problem in 1996. Zeng [5]–[7] has introduced a quantum signature scheme based on the correlation of quantum entanglement states in 2001. Gottesman and Chuang [8] have also proposed a quantum digital signature scheme based on quantum one-way function. In 2008, Wen [9] proposed a weak blind signature scheme based on quantum cryptography, Shi *et al.* introduced a multiparty quantum proxy group signature scheme for the entangled-state message [10]–[12] and Lee also presented two quantum signature schemes with message recovery [13]. In 2008, Yang and Wen suggested a multi-proxy quantum group signature scheme with threshold shared verification [14], in which only the cooperation of all the signers in the proxy group can generate the proxy signature on behalf of the original signer.

In this paper, a quantum communication scheme for blind signature is proposed to create a new systemetrical quantum key cryptosystem with two-particle entangled quantum system. A third fully trusted participant Charlie (the arbitrator and proxy) is involved. The responsibility of Charlie is to help Alice and Bob trust each other before communication, verify the legalization and authenticity of the trying blind signature and provide batch efficient proxy blind signatures to Alice. During all the communications, two-particle entangled quantum system are applied to create the quantum message strings and to make distribution of keys. The rest of this paper is organized as follows. Sect. II proposes the quantum communication scheme for blind signature. The security analysis and discussions are made in Sect. III. Finally, the conclusions are drawn in Sect. IV.

II. QUANTUM COMMUNICATION SCHEME FOR BLIND SIGNATURE

The classical blind signature is described like this: Bob is a notary, Alice expects that Bob can sign the message from her and she does not let Bob understand the content of the message. Bob does not care the content of the message and only testifies he has notated it at some time [3]. The quantum communication scheme for blind signature utilizes the arbitrary two-particle entangled quantum system [15] which can be expressed as follows,

$$|\varphi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle, \quad (1)$$

where $|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$.

Suppose that Alice and Bob share a maximally entangled state:

$$|\varphi_{AB}\rangle = \frac{1}{2}(|00\rangle_{AB} + |01\rangle_{AB} + |10\rangle_{AB} + |11\rangle_{AB}), \quad (2)$$

Alice and Charlie share a maximally entangled state:

$$|\varphi_{AC}\rangle = \frac{1}{2}(|00\rangle_{AC} + |01\rangle_{AC} + |10\rangle_{AC} + |11\rangle_{AC}), \quad (3)$$

and Bob and Charlie share a maximally entangled state:

$$|\varphi_{BC}\rangle = \frac{1}{2}(|00\rangle_{BC} + |01\rangle_{BC} + |10\rangle_{BC} + |11\rangle_{BC}) \quad (4)$$

according to Eq. (1).

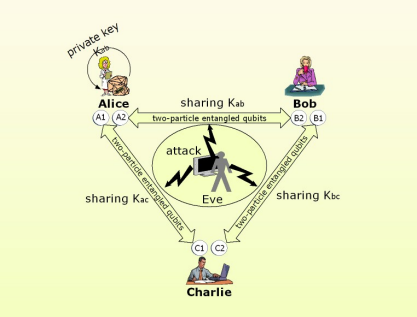


Fig. 1. The relationship among Alice, Bob and Charlie for the distribution of quantum keys in the quantum communication scheme of blind signature.

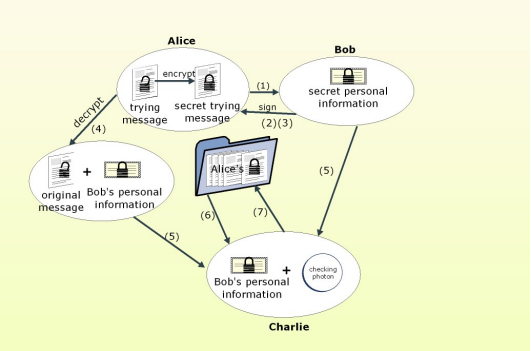


Fig. 2. The process of quantum communication scheme for blind signature. (1) $\sim$ (7) denote that seven steps of quantum communication scheme for blind signature.

The quantum communication scheme for blind signature can be presented as following aspects: preparation of quantum keys and messages, trying quantum blind signature, verification and batch quantum blind signature.

A. *Preparation of Quantum Keys and Messages*

Step 1. Alice owns a private key K_a which is used to encrypt her messages that are excepted to be signed by Bob. Secret keys K_{ab}, K_{ac} and K_{bc} are distributed to Alice, Bob and Charlie, where K_{ab} is employed in the communication between Alice and Bob and it only can be used twice for Bob's encrypting and Alice's decrypting in the first communication, then it will be discarded. K_{ac} and K_{bc} are employed in the communications between Alice and the arbitrator Charlie and between Bob and Charlie respectively. The relationship among Alice, Bob and Charlie for the distribution of quantum keys is given in Fig. 1.

Step 2. Alice prepares quantities of messages which are expected to be signed by Bob which can be described as a matrix

$$M = \begin{array}{c} M_1 \\ M_2 \\ \vdots \\ M_i \\ \vdots \\ M_m \end{array} \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1j} & \cdots & m_{1n} \\ m_{21} & m_{22} & \cdots & m_{2j} & \cdots & m_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ m_{i1} & m_{i2} & \cdots & m_{ij} & \cdots & m_{in} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ m_{m1} & m_{m2} & \cdots & m_{mj} & \cdots & m_{mn} \end{bmatrix}, \quad (5)$$

there are m messages $\{M_1, M_2, \ldots M_m\}$ and each message has n bits, for example:

$$M_i = \begin{bmatrix} m_{i1} & m_{i2} & \cdots & m_{ij} & \cdots & m_{in} \end{bmatrix}, \quad (6)$$

and M_1 is chosen to be considered as the trying message for the first trying quantum blind signature.

The quantum communication scheme for blind signature can be briefly defined as following seven steps corresponding to Fig. 2. (1) Alice firstly sends a trying message M_1 encrypted by her private key K_a to Bob. (2) Bob adds his personal information to this secret message and encrypts it by the shared key K_{ab} with Alice. (3) Bob sends the secret message with his personal information to Alice which is called the trying blind signature. (4) Alice receives this trying blind signature and decrypts it by the shared key K_{ab} with Bob and judge whether the secret trying message has been falsified, and if falsified the signature process stops. (5) Alice and Bob separately inform Charlie the result of the signature and Charlie verifies legalization and authenticity of the trying signature. (6) If the verification is successful, Alice sends quantities of messages to Charlie. (7) Charlie signs quantities of messages from Alice with the the combination of Bob's personal information and Charlie's random checking photons.

B. *Trying Quantum Blind Signature*

Step 1. Alice creates a qubit string $|\psi_{M_1}\rangle$ for the trying message. She transforms the trying message M_1 into a qubit string $|\psi_{M_1}\rangle$, and there are n qubits in this string such as $|\psi_{M_1}\rangle$, i.e.,

$$|\psi_{M_1}\rangle = \{|\psi_{11}\rangle, |\psi_{12}\rangle, \ldots, |\psi_{1j}\rangle, \ldots, |\psi_{1n}\rangle\}, \quad (7)$$

where $|\psi_{1j}\rangle$ is a single qubit in the string $|\psi_{M_1}\rangle$. Any qubit $|\psi_{1j}\rangle (j = 1, 2, \ldots, n)$ in $|\psi_{M_1}\rangle$ can be expressed as a superposition of the two eigenstates $\{|0\rangle, |1\rangle\}$, ,i.e.,

$$|\psi_{1j}\rangle = \alpha_{1j}|0\rangle + \beta_{1j}|1\rangle, \quad (8)$$

where α_{1j} and β_{1j} are complex number satisfying $|\alpha_{1j}|^2 + |\beta_{1j}|^2 = 1$. The general quantum message states $|\psi_{M_i}\rangle$ can be expressed as the tensor product of the qubits in that message string, i.e.,

$$\begin{aligned} |\psi_{M_i}\rangle &= |\psi_{i1}\rangle \otimes |\psi_{i2}\rangle \cdots \otimes |\psi_{ij}\rangle \cdots \otimes |\psi_{in}\rangle \\ &= sum_{\gamma=1}^{2^n} \lambda_{i\gamma} |\mu_{i\gamma}^1 \mu_{i\gamma}^2 \cdots \mu_{i\gamma}^j \cdots \mu_{i\gamma}^n\rangle, \end{aligned} \quad (9)$$

where $\sum_{\gamma=1}^{2^n} |\lambda_{i\gamma}|^2 = 1$ and $\mu_{i\gamma}^j \in \{0, 1\}$.

Step 2. Alice transforms her private key $K_a = \{|K_a^1\rangle, |K_a^2\rangle, \ldots, |K_a^j\rangle, \ldots, |K_a^n\rangle\}$ to a sequence of measurement operators M_{k_a},i.e.,

$$M_{k_a} = \{M_{k_a^1}^1, M_{k_a^2}^2, \ldots, M_{k_a^j}^j, \ldots, M_{k_a^n}^n\}, \quad (10)$$

where the operator $M_{k_a^j}^j$ is defined to arise from the key $|K_a^j\rangle$ for $j \in \{1, 2, \ldots, n\}$. A more detailed method is described in Ref. [5]. After the transformation, Alice measures the information string of qubits $|\psi_{M_1}\rangle$ with M_{k_a} to derive a secret string

$$|T\rangle = M_{k_a}|\psi_{M1}\rangle = \{|t_1\rangle, |t_2\rangle, \ldots, |t_j\rangle, \ldots, |t_n\rangle\}, \quad (11)$$

where $|t_j\rangle = M_{k_a^j}^j |\psi_{1j}\rangle$ and it denotes the j-th qubit in the

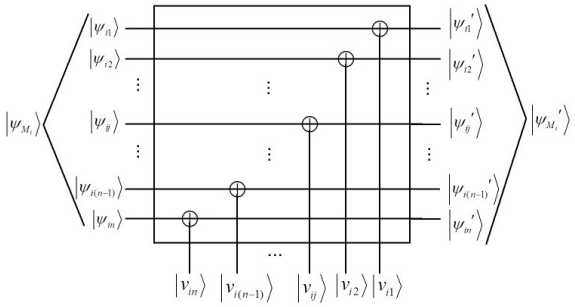


Fig. 3. The comparison quantum circuit for verifying whether $|\psi'_{M_i}\rangle$ matches to $|\psi_{M_i}\rangle$.

string of $|T\rangle$. Thus $|T\rangle$ is the secret state of the trying message and she directly sends it to Bob and expects Bob to sign it.

Step 3. Bob adds his personal information to the secret message $|T\rangle$ though he doesn't understand the content of it.

(1) Bob creates a qubit string $|\psi_p\rangle$ of his own personal information which contains n qubits, i.e.,

$$|\psi_p\rangle = \{|\psi_{p_1}\rangle, |\psi_{p_2}\rangle, \ldots, |\psi_{p_j}\rangle, \ldots, |\psi_{p_n}\rangle\}, \quad (12)$$

where $|\psi_{p_j}\rangle$ is a single qubit in $|\psi_p\rangle$. Any qubit $|\psi_{p_j}\rangle (j = 1, 2, \ldots, n)$ in $|\psi_p\rangle$ can be expressed as a superposition of the two eigenstates $\{|0\rangle, |1\rangle\}$ like $|\psi_{1j}\rangle$ in the Step 1.

(2) Bob doesn't expect Alice know the content of his personal information either and he encrypts $|\psi_p\rangle$ with K_{bc}. He relates the key $K_{bc} = \{|K^1_{bc}\rangle, |K^2_{bc}\rangle, \ldots, |K^j_{bc}\rangle, \ldots, |K^n_{bc}\rangle\}$ to a sequence of measurement operators $M_{k_{bc}}$ and the modus is like Eq.(10). Then Bob measures the personal information string $|\psi_p\rangle$ with $M_{k_{bc}}$ and obtains

$$|P\rangle = M_{k_{bc}}|\psi_p\rangle = \{|P_1\rangle, |P_2\rangle, \ldots, |P_j\rangle, \ldots, |P_n\rangle\}, \quad (13)$$

where $|p_j\rangle$ denotes the j-th qubit in the string of $|p\rangle$ and $|p_j\rangle = M^j_{k_{bc}} |\psi_{p_j}\rangle$.

(3)Bob utilizes k_{ab}, $|T\rangle$, $|P\rangle$ to provide a quantum blind signature to the secret trying message, which can be implemented as this way: he encrypts $|T\rangle$, $|P\rangle$ with k_{ab} to drive

$$S_b = k_{ab}(|T\rangle, |P\rangle), \quad (14)$$

where S_b is a blind signature on Alice's secret trying message.

Step 4. Bob sends S_b back to Alice and waits for the verification of the signature.

C. *Verification*

Step 1. Alice receives S_b and uses k_{ab} to decrypt S_b to derive $|T'\rangle$ and $|P'\rangle$. Then she uses her private key k_a to decrypt $|T'\rangle$ to obtain a quantum string $|\psi'_{M_1}\rangle$.

Step 2. Alice verifies whether the signature is blindness. She compares $|\psi'_{M_1}\rangle$ to her $|\psi_{M_1}\rangle$ which she has reserved in the Step 1 of trying quantum blind signature phase. The comparison quantum circuit is presented in Fig. 3. It implies that $|v_{ij}\rangle = |\psi'_{ij}\rangle \oplus |\psi_{ij}\rangle$ and we can justify whether $|\psi'_{M_i}\rangle$ matches to $|\psi_{M_i}\rangle$ according to the output qubit string $|V_i\rangle = \{|v_{i1}\rangle, |v_{i2}\rangle, \ldots, |v_{ij}\rangle, \ldots, |v_{i(n-1)}\rangle, |v_{in}\rangle\}$. Because $|0\rangle \oplus |0\rangle = |0\rangle$, $|1\rangle \oplus |1\rangle = |0\rangle$, $|0\rangle \oplus |1\rangle = |1\rangle$, $|\psi'_{M_i}\rangle$ may match to $|\psi_{M_i}\rangle$ when $|V_i\rangle = \{|0\rangle, |0\rangle, \ldots, |0\rangle, \ldots, |0\rangle\}$ is derived. If $|\psi'_{M_1}\rangle \neq |\psi_{M_1}\rangle$, it means the secret message has been misrepresented. Maybe there is somebody has measured the trying message or intercepted the whole or parts of the content, because any measurement may change the state of quantum photons. Then the protocol should be terminated. If $|\psi'_{M_1}\rangle = |\psi_{M_1}\rangle$, we can suggest that there is nobody knows the content of the trying message except Alice, thus the blind signature can be established.

Step 3. Bob transmits $|P\rangle$ to the arbitrator Charlie. $|P\rangle$ is the encrypted result of $|\psi_p\rangle$ with $M_{k_{bc}}$, and it is secret to anyone except Bob and the arbitrator Charlie. So Bob can send it directly to Charlie through the quantum channel.

Step 4. Alice sends $|P'\rangle$ to Charlie.

Step 5. The arbitrator Charlie receives $|P'\rangle$ and $|P\rangle$, and he certifies whether the signature is authentic. He firstly compares if $|P'\rangle = |P\rangle$, and then he uses k_{bc} to decrypt $|P'\rangle$ and $|P\rangle$ separately. Charlie obtains $|\psi'_p\rangle$ and $|\psi_p\rangle$, and then he compares whether $|\psi'_p\rangle = |\psi_p\rangle$. If $|P'\rangle = |P\rangle$ and $|\psi'_p\rangle = |\psi_p\rangle$, we can consider this trying blind signature is successful, then Charlie will inform Alice and Bob this trying blind signature is authentic and blindness. Charlie can also apply the comparison quantum circuit in Fig. 3 to implement the verification procedure. Next step, Charlie can sign a large number of messages from Alice as a proxy of Bob. However, when any previous condition is not satisfied, the communication should be terminated.

D. *Batch Proxy Quantum Blind Signature*

Charlie may become a proxy of Bob and sign quantities of messages $\{M_2, M_3, \ldots M_m\}$ of Alice with the combination of Bob's personal information $|P\rangle$ and his random checking photons $|P^k_{check}\rangle$.

Step 1. Alice transforms her remaining messages $\{M_2, M_3, \ldots M_m\}$ into $m-1$ strings of qubits $\{|\psi_{M_2}\rangle, |\psi_{M_3}\rangle \ldots, |\psi_{M_m}\rangle\}$ like the Step $1 \sim 3$ of the trying quantum blind signature phase. Then she encrypts them by her private key k_a, thus the remaining secret messages can be expressed as follows,

$$|M_k\rangle = M_{k_a}|\psi_{M_k}\rangle = \{|m_{k1}\rangle, |m_{k2}\rangle, \ldots, |m_{kj}\rangle, \ldots, |m_{kn}\rangle\}, \quad (15)$$

where $k = 2, 3, ..., m$.

Step 2. Alice sends $\{|M_2\rangle, |M_3\rangle, ...|M_m\rangle\}$ to Charlie successively and waits for the signature from Bob's proxy Charlie.

Step 3. Charlie adds one qubit random checking photon $|P^k_{check}\rangle$ into $|P\rangle$ which Charlie has obtained in the step 3 of verification phase, where

$$|P^k_{check}\rangle = M^r_{k^r_{bc}}|\psi^k_{check}\rangle \quad (16)$$

and $|\psi^k_{check}\rangle (k = 2, 3, \ldots, m)$ is formed as Eq.(9). r is a random number in $\{1, 2, \ldots j \ldots, n\}$. It means Charlie may randomly choose a $M^j_{k^j_{bc}}$ from $M_{k_{bc}}$ to measure $|P^k_{check}\rangle$. Thus the general expression of the combining qubit strings is

$$\begin{aligned} |P^k_{BT}\rangle &= \{|P\rangle, |P^k_{check}\rangle\} \\ &= \{|P_1\rangle, |P_2\rangle, \ldots, |P_j\rangle, \ldots, |P_n\rangle, |P^k_{check}\rangle\} \end{aligned} \quad (17)$$

where $k = 2, 3, \ldots m$. Each message state $|M_k\rangle$ is corresponding to a $|P_{BT}^k\rangle$, and Charlie can randomly use a different $|P_{BT}^k\rangle$ to sign a message from Alice.

Step 4. Charlie separately signs $m-1$ secret messages with the string $|P_{BT}^k\rangle(k = 2, 3, \ldots, m)$ which is the combination of Bob's personal information and Charlie's checking photons, and he encrypts them by k_{ac}. Thus the proxy blind signatures are obtained:

$$S_{T_k} = k_{ac}(|M_k\rangle, |P_{BT}^k\rangle), \tag{18}$$

where $k = 2, 3, \ldots, m$.

Step 5. Charlie sends the secret messages with blind signatures $\{S_{T_2}, S_{T_3}, \ldots, S_{T_m}\}$ back to Alice successively.

Step 6. Alice receives the blind signatures $S_{T_k}(k = 2, 3, \ldots, m)$ and decrypts them by k_{ac} to get $|M_k\rangle(k = 2, 3, \ldots, m)$ and $|P_{BT}^{k'}\rangle(k = 2, 3, \ldots, m)$. Then she decrypts $|M_k\rangle(k = 2, 3, \ldots, m)$ with k_a to obtain $|\psi_k\rangle(k = 2, 3, \ldots, m)$. Because Charlie is the fully trusted arbitrator and the proxy signatures contain his checking photons and Bob's correct personal information, it is not necessary to suspect the accuracy of the signature. However, Alice can randomly measure the accuracy of the signatures by justifying whether they satisfy $|\psi_k\rangle = |\psi_{M_k}\rangle(k = 2, 3, \ldots, m)$ and $|P_{BT}^{k'}\rangle = |P'\rangle(k = 2, 3, \ldots, m)$.

III. Security Analysis And Discussions

The security of this scheme can be analyzed as following four aspects: impossibility of forgery, impossibility of disavowal by the signatory, impossibility of denial by the receiver and the security of the entangled quantum system.

A. *Impossibility of Forgery*

If an dishonest participant Eve wants to forge the signature of Bob, she may sign the illegal messages herself by imitating Bob's signature or pretend the legal user Alice to require for Bob's signature. Even if Eve succeeds to sign her messages by forging Bob's personal information. Denote the spurious Bob's personal information is $|P_s\rangle$, she may be detected in the verification phase, and the arbitrator Charlie can judge $|P_s\rangle$ does not match to the Bob's correct personal information $|P\rangle$. The communication of the signing phase should be terminated immediately.

If the attacker Eve expects to forge the signature of Bob, she may be recognized in the step 3 of initial phase. Even though she is so lucky to escape identity verification and she can send her trying secret message to Bob, Bob doesn't care what the content of the message is but only signs it. Because the signing message is encrypted by k_{ab} before she sends it back to Eve, Eve can not decrypt it for lack of k_{ab}.

B. *Impossibility of Disavowal by the Signatory*

Suppose Bob has added his personal information to sign the trying message, and the signature is obtained by Alice. Because the arbitrator Charlie can judge whether the signature is authentic or not, once it is proved to be authentic, the Bob's personal information has already denoted for a register from him, then the following signing for the last $m-1$ messages is the responsibility of the arbitrator and proxy Charlie, and he will utilize the combination of his checking photons and Bob's personal information to do this. If Bob disavow it, he will be discovered by Charlie immediately. In this scheme, as long as Bob has signed the trying message and the signature has been proved to be authentic by Charlie, the mechanism of proxy signature make Bob have no chance to disavow the remaining $m-1$ signature. Thus the signatory Bob is impossible to disavow the signature.

C. *Impossibility of Denial by the Receiver*

In the verification phase, Alice derives S_b and use k_{ab} to decrypt S_b to obtain $|T'\rangle$ and $|P'\rangle$. After the arbitrator Charlie's authentication, if $|P'\rangle = |P\rangle$ and $|\psi_p'\rangle = |\psi_p\rangle$, Charlie informs Alice and Bob this trying blind signature is authentic, otherwise, the trying signature will be considered incredible and the process of signature is discontinued at once. It means the two participants Alice and Bob can not deny the signature any way and Charlie is considered to be a judge. If one of them deny or disavow the signature, Charlie can unconditionally suspect the identification of them, and they may be no longer join in this communication.

D. *Security of Entangled Quantum System*

Suppose an attacker Eve can entangle her ancila system with the two-particle entangled quantum system $|\varphi\rangle$ in Eq. (1) by applying the strongest collective attack with probabilities. The combined Eve's and quantum system state can be expressed as

$$\begin{aligned} |E\varphi\rangle &= \lambda_{00}a_{00}|00\rangle|e_{00}\rangle + \lambda_{01}a_{01}|01\rangle|e_{01}\rangle \\ &\quad +\lambda_{10}a_{10}|10\rangle|e_{10}\rangle + \lambda_{11}a_{11}|11\rangle|e_{11}\rangle, \end{aligned} \tag{19}$$

where $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$ and $|e_{11}\rangle$ are un-normalized states of Eve and $|\lambda_{00}\rangle$, $|\lambda_{01}\rangle$, $|\lambda_{10}\rangle$ and $|\lambda_{11}\rangle$ are parameters relative to her attack probabilities. If Eve is clever enough to implement single qubit QND measurement on one particle of $|\varphi\rangle$ with the measurement operator $\rho = \frac{1}{2}|0\rangle\langle 0| \pm \frac{1}{2}|1\rangle\langle 1|$, she can derive the ideal entangled states

$$\begin{aligned} |E\rangle &= \frac{1}{2}\{(\lambda_{00}a_{00}|0e_{00}\rangle + \lambda_{01}a_{01}|1e_{01}\rangle) \\ &\quad \pm(\lambda_{10}a_{10}|0e_{10}\rangle + \lambda_{11}a_{11}|1e_{11}\rangle)\} \end{aligned} \tag{20}$$

according to Eq. (19). Thus the entanglement entropy of $|E\rangle$ can be analyzed based on the degree of entanglement [16] to indicate the maximal amount of information which can be intercepted by Eve. The entanglement entropy is

$$\begin{aligned} \mathcal{S}_E &= -\frac{1+\sqrt{1-\varepsilon}}{2}\log_2\frac{1+\sqrt{1-\varepsilon}}{2} \\ &\quad -\frac{1-\sqrt{1-\varepsilon}}{2}\log_2\frac{1-\sqrt{1-\varepsilon}}{2}, \end{aligned} \tag{21}$$

where $\varepsilon = 4|\lambda_{00}\lambda_{11}a_{00}a_{11} - \lambda_{01}\lambda_{10}a_{01}a_{10}|^2$. Even though Eve can adjust the parameters $|\lambda_{00}\rangle$, $|\lambda_{01}\rangle$, $|\lambda_{10}\rangle$ and $|\lambda_{11}\rangle$ to make $\mathcal{S}_E$ approach the maximal value 1 (when $\varepsilon = 1$) while the maximal entropy of the two-particle entangled quantum system $|\varphi\rangle$ is 2. Therefore the entangled quantum system state cannot be deterministically intercepted.

IV. CONCLUSIONS

A quantum communication scheme for blind signature with two-particle entangled quantum system is proposed, which is a new quantum key cryptosystem that combines proxy signature and blind signature. The two-particle entangled quantum states are applied to create the strings of qubits for messages and make distribution of keys. No matter the trying message or the remaining $m-1$ messages, they are encrypted by the private key k_a of Alice. Moreover, an authenticity verification of signatures and an arbitrator's efficient proxy signature are both applied. The analysis shows that a large number of blind signatures for quantities of messages can be achieved with the characteristics: impossibility of forgery, impossibility of disavowal by the signatory and impossibility of denial by the receiver. The security of our scheme depends on the two-particle entangled system which cannot be deterministically intercepted.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61272495), WCU R32-2010-000-20014-0 (Fundamental Research2010-0020942NRF, Korea), the Hunan Provincial Innovation Foundation For Postgraduate (Grant Nos. CX2011B087) and the Excellent Doctoral Dissertation Fund of Central South University (Grant Nos. 2011ybjz030).

REFERENCES

[1] S. William, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, New Jersey, 2^{nd} ed., 2003, p.67.
[2] D. Chaum, *Advance in Cryptography*, Proceedings of Crypto'82 Springer-Verlag, Berlin, 1982, p.267.
[3] B. Schneier, *Applied Cryptography:Protocols, Algorithms, and Source Code in C*, John Wiley and Sons, New York, 2^{nd} ed., 1996, p.79.
[4] C. Fan and C. Lei, Efficient blind signature scheme based on quadratic residues, Electronic Letters., vol. 32, no. 811, 1996.
[5] G. H. Zeng and C. H. Keitel, Arbitrated quantum-signature scheme, Phys. Rev. A., vol. 65, no. 042312, 2002.
[6] M. Curty and N. Lutkenhaus, Comment on "Arbitrated quantum-signature scheme", Phys. Rev. A., vol. 77, no. 046301, 2008.
[7] G. H. Zeng, Reply to "Comment on 'Arbitrated quantum-signature scheme'", Phys. Rev. A., vol. 78, no. 016301, 2008.
[8] D. Gottesman and I. Chuang, Quantum digital signatures, arXiv:quant-ph/0105032.
[9] X. J. Wen, X. M. Niu, L. P. Ji, and Y. Tian, A weak blind signature scheme based on quantum cryptography, Optics Communications., vol. 282, no. 666, 2009.
[10] J. J. Shi, R. H. Shi, Y. Tang and M. H. Lee, A multiparty quantum proxy group signature scheme for the entangled-state message with quantum Fourier transform. Quantum Information Processing, Vol. 10, No. 5, 653-670, 2011.
[11] J. J. Shi, R. H. Shi, Y. Guo, X. Q. Peng and Y. Tang, Batch proxy quantum blind signature scheme, SCIENCE CHINA Information Sciences, doi: 10.1007/s11432-011-4422-5, 2011.
[12] J. J. Shi, R. H. Shi , Y. Guo, X. Q. Peng, M. H. Lee and D. S. Park, A (t,n)-Threshold Scheme of Multi-party Quantum Group Signature with Irregular Quantum Fourier Transform, International Journal of Theoretical Physics, DOI 10.1007/s10773-011-0978-5, 2011.
[13] H. Lee, C. H. Hong, and H. Kim, Arbitrated quantum signature scheme with message recovery, Phys. Lett. A. **32**, 295-300 (2004).
[14] Y. G. Yang, Multi-proxy quantum group signature scheme with threshold shared verification, Chin. Phys. B. Vol. **17**, No. 2, 415-418 (2008).
[15] M. Nielsen and I. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000, p.171.
[16] R. V. Buniy and S. D. H. Hsu, Entanglement entropy, black holes and holography, Phys. Lett. B., 64 (2007), pp. 72-76.

Jinjing Shi is now a joint Ph.D. student of Central South University, China and Chonbuk National University, Korea, and participating in the World Class University (WCU) project sponsored by the National Research Foundation (NRF), Korea. She received her B. E. degree in the School of Information Science and Engineering, Central South University, Changsha, China, in 2008. Her research interests are quantum communications, quantum cryptography and network security.

Ronghua Shi received the B.S., M.S., and Ph.D. degrees in electrical engineering from Central South University (CSU), Changsha, China, in 1986, 1989, and 2007, respectively. He is presently a Professor and the Vice Dean of the School of Information Science and Engineering at Central South University. His research interests include information security, quantum cryptography and network security.

Xiaoqi Peng received the B.S., M.S., and Ph.D. degrees in automation and control from Chongqing University, Harbin Institute of Technology and Central South University respectively. He is presently a Professor of the School of Information Science and Engineering at Central South University, and the dean of Hunan First Normal University. His research interests include intelligent detection of complex industrial processes, optimization of the decision-making and intelligent control.

Moon Ho Lee is a professor in Chonbuk National University, Korea. He received the Ph.D. degree from Chonnam National University, Korea in 1984, and from the University of Tokyo, Japan in 1990, both Electrical Engineering, He was in University of Minnesota, U.S.A, from 1985 to 1986 as a post-doctor. He was conferred an honorary doctorate from the Bulgaria Academy of Sciences in 2010. Dr. Lee has made significant original contributions in the areas of mobile communication code design, channel coding, and multidimensional source and channel coding. He has authored 34 books, 135 SCI papers in international journals, and 240 papers in domestic journals, and delivered 350 papers at international conferences. Dr. Lee is a member of the National Academy of Engineering in Korea and the National Academy of Mathematical Sciences in India, and a Foreign Fellow of the Bulgaria Academy of Sciences. He is the inventor of Jacket Matrix and it in Wikipedia was cited over 49,559 times.

A Epidemic Style Super-node Election Method Based on Self-information Theory

Zhiwei Gao*, yingxin Hu*

**Department of Computer Science, Shijiazhuang TieDiao University, Shijiazhuang, 050043, China*

gao_zhiwei@163.com, huyinxin@163.com

***Abstract*—Many distributed applications such as cloud computings, grids use peer-to-peer (P2P) paradigm as the lower service. In P2P technology, the super-node paradigm can lead to improved efficiency, without compromising the decentralized nature of P2P networks. So the above applications adopt super-node paradigm to provide services. However, due to inherent dynamism, decentralisation, scale and complexity of P2P environments, self-managing super-node selection is a challenging problem. This paper present a super-node election protocol based on self-information theory and gossiping technology(SPSI). In SPSI, every node has a information vector (VI), and SPSI uses a weighted mean mechanism based on VI to promote the "best" nodes to super-node status. As we know we are the first to use self-information theory to select super-node. The paper also includes extensive simulation experiments to prove the efficiency, scalability and robustness of SPSI.**

***Keywords*—self-information quantity, super-node, scalability, SPSI**

I. INTRODUCTION

Many distributed applications such as cloud computing, grids use super-node paradigm as the lower service. Super-nodes allow these applications to run more efficiently by exploiting heterogeneity and distributing load to machines that can handle the burden. On the other hand, because this architecture allows multiple, separate points of failure, increasing the health of the distributed network, it does not inherit the flaws of the client/server model. The use of P2P protocols is expected to improve the efficiency and scalability of information services in these systems [1],[4],[5].

However, due to inherent decentralisations, scale, dynamism, and complexity of P2P environments, self-managing super-node selection is a challenging problem.

A number of P2P systems address the heterogeneity of P2P environments by electing super-nodes and assigning them extra responsibilities [6],[7],[10],[11]. Solutions based on flooding, random walking or other traditional election algorithm, potentially require communication with all peers in the network and thus do not scale to large networks. Other solutions such as manual or static configuration of super-nodes are inappropriate due to a lack of global knowledge of application characteristics.

Manuscript received May 21, 2012. This work was supported by the National Natural Science Fund of China (No: 50975185).

Z.W is a Associate Professor of Information Science and Technology, Shijiazhuang TieDao University. Gao's research interests center around peer-to-peer computing, PKI and certificate chain, PKI based on P2P technology. (phone: 086-0311-87939496; fax: 086-0311-8795288; e-mail: gao_zhiwei@163.com).

Y.X is a Associate Professor of Information Science and Technology, Shijiazhuang TieDao University. (Email: huyinxin@163.com)

II. RELATED WORK

In this section, we briefly review some related work. We start with P2P based on super-node technology, and then present the related work on super-node selection problem.

The super-node approach to organize a P2P overlay is a trade-off solution that merges the client-server model relative simplicity and the P2P autonomy and resilience to crashes. The need for a super-node network is mainly motivated by the fact to overcome the heterogeneity of peers deployed on the Internet.

Meirong Liu[1] et al. present a super-peer-based coordinated service provision framework (SCSP) to coordinate the service groups to work collaboratively and share their service peers. The SCSP is made up of an S-labor-market model, a recruiting protocol based on a weighting mechanism, and an optimal dispatch algorithm.

KaZaA [8] and Gnutella [9], [10] have explored using heterogeneity of peers to improve search performance. These systems have efficient peers hold more neighbors and process more queries. An efficient peer (super-peer) acts as a server in a local area, builds an index of the shared files provided by those peers connected to it and offers a searching index service for those who have connected to it by flooding queries to other super-peers. These systems mainly explored improving performance by decreasing the number of transmitted messages and latency hops.

Yang and Garcia Molina [12] proposed some design guidelines. A mechanism to split node clusters is proposed and evaluated analytically, but no experimental results are presented.

Garces-Erice[13] et al. studied hierarchical DHTs, in which peers are organized into groups, and each group has its autonomous intra-group overlay network and lookup service. The groups themselves are organized in a top-level overlay network. To find a peer that is responsible for a key, the top level overlay first determines the group responsible for the key; the responsible group then uses its intra-group overlay to determine the specific peer that is responsible for the key. They concluded that hierarchical organization could improve a

system's scalability. A hierarchical system demonstrates better stability due to selection of peers who are more reliable as the members of the upper overlay, generates fewer messages in a wide area and can significantly improve the lookup performance by transmitting queries through the upper overlay.

Nejdl et al. proposed a design organizing super-peers with a hypercube structure in [14]. In their approach, every super-peer serves a subset of peers and all super-peers are arranged in a hypercube topology. Because the topology is vertex-symmetric, it features inherent load balancing among super-peers. When a super-peer wants to transmit a query, according to the spanning tree algorithm, it forwards the query to its neighbors instead of flooding the system with queries. Each super-peer wants to maintain at most d neighbors' information and it takes at most d logic hops for a query from any super-peer to the farthest super-peer, where d is the dimension of the hypercube.

Mizrak [15] et al. proposed a design based on the Chord ring. In their approach, there are two rings, named the inner-ring and outer-ring respectively. Each peer is placed on a circular identifier space in the "outer-ring", using a DHT algorithm such as Chord. Of all the peers, m peers who joined the system first are selected as super-peers to create a smaller core "innerring". The outer-ring is divided into m equal arcs and each arc is assigned to one super-peer. Each super-peer is responsible for maintaining two pieces of information: the addresses of the peers contained within its arc and the mapping between arcs and their responsible super-peers. Each peer registers in only one super-peer, and requests searching services from its super-node. Each super-peer offers searching services for its registered peers and the other super-peers. The lookup is performed using super-peers in constant time. When a super-peer's load approaches its capability, it may share part of its load with its neighbors if they have sufficient excess capacity or with a new super-peer selected from the volunteer peers. In either case the super-peer splits its arc appropriately and reassigns pieces of this range to the neighbors accepting the load.

In [16], the authors propose a socio-economic inspiration based on Shelling's model to create a variation of the super-node topology. Such variation allows ordinary peers to be connected with each other and to be clients of more than one super-node at the same time. This topology focuses on efficient search. As in our case, the super-nodes are connected to each other to form a network of hubs and both solutions are suited for unstructured networks. However, they do not address the problem of the super-node election.

In [18], a mechanism for the construction and the maintenance of overlay topologies based on super-nodes SG-1 was proposed. This mechanism is based on the well-known gossip paradigm, with nodes exchanging information with randomly selected peers and re-arranging the topology according to the requirements of the particular P2P application. In [19], the author presents SG-2, a protocol for building and maintaining proximity-aware super-node topologies. Like SG-1, SG-2 also uses a gossip-based protocol to spread messages to nearby nodes and a biology-inspired task allocation mechanism to promote the "best" nodes to super-node status.

Unlike all these studies, our implementation is based on information theory, and as we know we are the first to introduce information theory to super-node selection. Our contribution is as follows: (1) Propose a super-node election protocol SPSI based on self-information. (2) Give the relation between node's capacity and online time through experiments. (3) Propose a weighted mean algorithm to describe node's properties. Our model's efficiency is equal to SG-1 or SG-2, but the super-nodes we elected are more stable, so the costs of network maintenance are lower than them.

III.BACKGROUND THEORY AND TERMINOLOGY

The framework of SPSI can be considered as a natural evolution of Rigorous binary tree model. We propose a framework based on our own efficient and scalable Rigorous binary tree model and its theorem[6,17]. If the size of network is small, file lookups are resolved with only one hop. As the system's scale become larger, it can expand automatically based on the super-node's capability and suit for large scale system. In the worst case, file lookups are resolved with only three hops. But this model did not discuss super-node selection problem, and this is the main concern of this thesis.

Here, we first provide the definition of a rigorous binary tree and the other relevant theory to give readers a better understanding of our model.

A. Rigorous binary tree and its mapping theorem

Definition 1: Rigorous binary tree

For a random node of a binary tree, if it has at least one child node, its left child node and right child node must exist at the same time. If this condition is satisfied, the binary tree is defined as a rigorous binary tree.

Definition 2: Rigorous binary tree extension

After a random leaf of a rigorous binary tree produces two child nodes, the original rigorous binary tree becomes a new rigorous binary tree. This is called rigorous binary tree extension.

Definition 3: Rigorous binary tree code algorithm: The letter *T* represents a rigorous binary tree, "*A*" represents a random node in *T*, ha represents the depth of node *A*, and N_a represents its code. The code of T's root node was set as 0. The code of *A*'s left child is equal to N_a. The code of *A*'s right child is equal to ($N_a + 2^{h_a}$), The depth A's child is h_a+1.

Theorem 1: Rigorous binary tree mapping theorem: For any one integer I (I >=0), there is one and only one leaf node X whose code (N_x) and depth (h_x) can accord with $N_x = I \% 2^{h_x}$, among all leaf nodes in a fixed rigorous binary tree. (Here % denotes modular arithmetic.) the proof process is included in our prior work[6], [17].

Figure.1 illustrates a rigorous binary tree. When we extend its leaf node G in Figure.1(1) by adding two children nodes to G, the rigorous binary tree becomes that described in Figure.1(2). According to the rigorous binary tree code algorithm, node A is the root node, so its code and depth are (0, 0). Node B is A's left child, so B's code is equal to A's code (0)

and B's depth is A's depth plus one (0+1=1). Node C is A's right child, so C's code is equal to ($0+2^0$=1) and C's depth is equal to B's depth (1). In the same way, we can compute the remaining nodes' code and depth as described in Figure. 1(3).

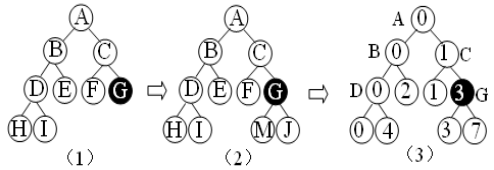


Figure 1. The extending and coding of a rigorous binary tree

Based on Rigorous binary tree extension and mapping theorem, we design RBTree model. In the model, when the number of peers registered in a super-peer reaches the quantity limit, in order to balance the load and avoid a bottleneck, the super-peer will use SPSI protocol to select a high-powered peer from its registered-peer table as a new super-peer, code it with the rigorous binary tree code algorithm and share one part of its load with the new super-peer.

B. Self-information

Definition 4: Let *E* be an event belonging to a given event space and having probability $\Pr(E) = p_E$, Let *I(E)* – called the self-information of *E* – represent the amount of information one gains when learning that *E* has occurred (or equivalently, the amount of uncertainty one had about *E* prior to learning that it has happened).

Theorem 2: The only function defined over $p \in [0, 1]$ and satisfying

- I(p) is monotonically decreasing in p;
- I(p) is a continuous function of p for $0 \leqslant p \leqslant 1$;
- I(p1 × p2) = I(p1) + I(p2);

where $\mathbf{I}(p) = -c \bullet \log_b(p)$, *c* is a positive constant and the base b of the logarithm is any number larger than one.

In SPSI, every node has a information vector (VI), and SPSI uses a weighted mean mechanism based on VI to promote the "best" nodes to super-node status.

C. Weighted Arithmetic Mean

In calculation of arithmetic mean, the importance of all the items was considered to be equal. However, there may be situations in which all the items under considerations are not equal importance. For example, we want to find average number of marks per subject who appeared in different subjects like Mathematics, Statistics, Physics and Biology. These subjects do not have equal importance. If we find arithmetic mean by giving Mean. For example, A student obtained 70, 80, 80, 70, and 65 marks in the subjects of Math, Statistics, Physics, Chemistry and Biology respectively. And we assume weights 5, 4, 2, 3, and 1 respectively for the above mentioned subjects. The solution was listed in table 1.

TABLE 1.

SOLUTION OF WEIGHTED ARITHMETIC MEAN

Subjects	**Marks Obtained**	**Weight(*w*)**	***wx***
Math	70	5	350
Statistics	80	4	320
Physics	80	2	160
Chemistry	70	3	210
Biology	65	1	65
Total		$\sum w = 15$	$\sum wx = 1105$

Defination 5: arithmetic mean computed by considering relative importance of each items is called weighted arithmetic mean. To give due importance to each item under consideration, we assign number called weight to each item in proportion to its relative importance. Weighted Arithmetic Mean is computed by using following formula:

$$\overline{X}_w = \frac{\sum wx}{\sum w}$$

Where:

$\overline{X}_w$: Stands for weighted arithmetic mean.

x : Stands for values of the items and

w : Stands for weight of the item.

IV. SYSTEM MODEL AND ALGORITHM

Generally speaking, our goal is to create a topology where the most powerful nodes (in terms of capacity) and the enough stable nodes are promoted to the role of super-nodes.

The main topology features of the SPSI protocol algorithm are that each client just connected to a super node, and super node of each other connected together by random. This protocol can find a smaller number of nodes and super nodes set which has a longer online time, and these super nodes can serve as client nodes to cover the rest nodes. Such a topology structure can be easily used to implement file sharing, also can reduce the traffic caused by the application program.

To build a topology with such characteristics, we propose a mechanism based on NEWCAST [19]. Topology information such as identifier, capacity, online time, current role and neighborhood of participating nodes are disseminated through periodic gossip messages between randomly selected nodes. Based on the received information, nodes update their

neighborhoods in order to obtain a better approximation of the target topology.

In NEWSCAST, the state of a node is called partial view and it is constituted of a fixed-size set of peer descriptors. A peer descriptor contains the address of the node, along with a logical timestamp identifying the time when the descriptor was created. The size of a partial view is denoted by s. Generally, we chose the maximal view size to c = 30 and can get enough robust target topology[19].

A. Node Capacity

Apparently, Nodes are heterogenous: they may differ in their computational and storage capabilities, and also (and more importantly) on the bandwidth of its network connection. In order to distinguish nodes that are capable to act as super-nodes from nodes that can join just as clients, we associate each node n with a parameter Cn representing its capacity, i.e. the number of clients that can be handled by n. In other words, we use the concept of capacity to abstract in a single quantity all the characteristics listed above. In order to simplify our simulations, we assume that each node knows its capacity parameter; in a real implementation, this value could be computed on the fly, by performing on-line measurements; the result is strongly dependent on the particular application to be implemented. The techniques used to perform this computation are outside the scope of this paper.

In [20], through measurements done over existing P2P networks, the author concluded that most of the nodes have low capacity, while very few of them are able to support a large number of clients and the node's capacity obeys power-law distribution. So we have node *n* has a capacity of *x* with the probability $P(C_n = x) = x^{-\alpha}$, In which $x \in [1, C_{\max}]$, α is the distribution parameters (usually the parameter α = 2). The node capacity does not necessarily follow a strict power distribution, but it provides a reasonable distribution close to that.

B. Online time of nodes

In any super nodes based peer-to-peer network, super nodes take charge of both data block index and overlay organization. When a super node logouts from the system or a super node decides to alleviate its load, it has to transfer the corresponding block index and child nodes to another super node. This process will bring about considerable communication cost, so it is necessary to select a highly stable peer to act as a super node.

Many research papers such as [2], [3] study the online time of nodes through measurement method. They observed that session times (in minutes) with a mean=266, standard deviation=671. Network nodes joining or leaving is considered a Poisson distribution, and online time of nodes is subject to the negative exponential distribution of λ. So its probability density function is:

$$f(x) = \lambda e^{-\lambda x} \qquad x > 0 \qquad (1)$$

We use maximum likelihood estimation method to estimate the parameter λ, assuming that x1, x2, x3 ... is a set of random sample values, representing the node's Online time, Then Likelihood function

$$L(\lambda) = \lambda^n \prod_{i=1}^{n} \exp(-\lambda x_i) = \lambda^n \exp(-\lambda \sum_{i=1}^{n} x_i) \qquad (2)$$

then $$\frac{d \ln L(\lambda)}{d\lambda} = \frac{n}{\lambda} - \sum_{i=1}^{n} x_i = 0$$

We obtain $$\hat{\lambda} = \frac{n}{\sum_{i=1}^{n} x_i} = \frac{1}{\bar{x}} \qquad (3)$$

As long as we estimate the average online time roughly, we can figure out the estimated value to the equation of (3). From [20] we set $\bar{x} = 266$, then the parameter is $\hat{\lambda} \approx 0.004$. When the distribution parameter is determined, it will generate the random exponential distribution number as the node's online time, specific methods are:

$$F(x_i) = 1 - \exp(-\lambda x_i) \qquad (4)$$

Online Time $$x_i = \frac{\ln(1 - F(x_i))}{-\lambda} \qquad (5)$$

Depending on the fundamental theorem of random variable sampling, there is R = F (x), where R is a uniformly distributed random variable among [0,1]. As the 1-R and R have the same distribution, so (5) can be written

$$x = -\frac{\ln R}{\lambda} \qquad (6)$$

C. Weighted Arithmetic Mean in SPSI

Our goal in SPSI is to select "best" nodes as super-nodes. And we formalize the problem as follows: We are given a set S of n nodes(vi,wi), where vi denotes the one of a node's attribute value such as computational, storage capabilities, bandwidth of its network connection, online time etc. and wi denotes the weight of the value.

In peer-to-peer systems, different application emphasizes different capacity of super-nodes. Here our emphasis is the relation of node's online time and the other capacity. In order to simplify discussion, we use the concept of capacity to abstract in a single quantity all the characteristics such as computational, storage capabilities, bandwidth of its network connection etc. we associate each node n with a parameter Cn representing its capacity, i.e. the number of clients that can be handled by n, and the node's online time is Tn. The easiest way is a linear combination of the two parameters, then to arrive at a parameter:

$$\delta(C_n, T_n) = \xi C_n + \eta T_n \qquad (7)$$

where coefficient ξ is a value between 0 and 1, $\xi + \eta = 1$,denoting the importance of node's online time in relation with node's capacity.

Apparently, There are some questions we must resolve. One is C_n and T_n has different dimensions, and the other is C_n and T_n has different quantity scale. If Cn or Tn is very large, and T_n or C_n is very small, so $\delta(C_n,T_n)$ is large. This selected node is not our expected super-node. In order to resolve these questions, we introduce the information quantity theory to resolve it.

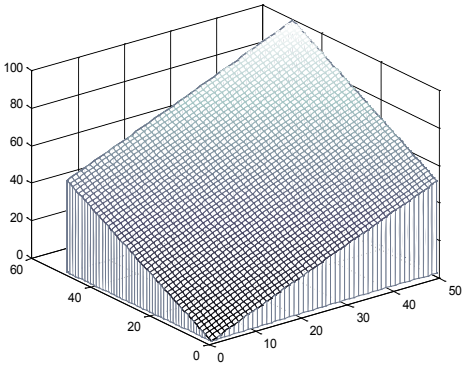


Figure 2. $\delta C_n, Tn)=Cn+Tn$

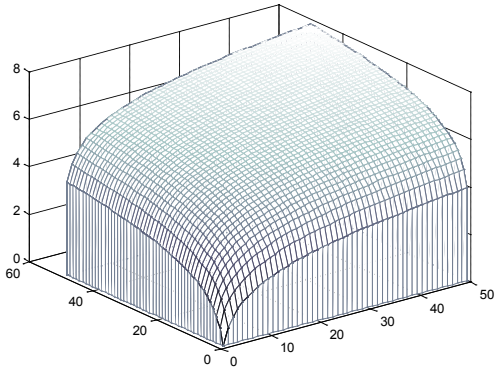


Figure 3. $\delta C_n, Tn)=logCn+logTn$

Defination 6: In joint probability space [XY,P(xy)], on the condition of event y ∈ Y, Event x ∈ X 's conditional information quantity is:

$$I(x \mid y) = -\log p(x \mid y) \qquad (8)$$

For the same reason,

$$I(y \mid x) = -\log p(y \mid x) \qquad (9)$$

Defination 7: In joint probability space [XY,P(xy)], any joint event xy, the joint information quantity of (x∈X，y∈Y) is:

$$I(xy) = -\log p(xy) \qquad (10)$$

Based on the definition of joint information quantity, conditional information quantity, then

$$\begin{aligned} I(xy) &= -\log p(xy) \\ &= -\log(p(x)p(y \mid x)) \\ &= -\log p(x) - \log p(y \mid x) \\ &= I(x) + I(y \mid x) \end{aligned} \qquad (11)$$

For the same reason,

$$I(xy) = I(y) + I(x \mid y) \qquad (12)$$

When the event X and Y independently of each other, then

$$I(xy) = I(x) + I(y) \qquad (13)$$

Assuming that the total number of node in the network is m, and node n has a capacity of Cn and online time Tn. The total capacity of all nodes in the network is

$$C_s = \sum_{n=1}^{m} C_n$$

and Online time of all nodes is

$$T_s = \sum_{n=1}^{m} T_n$$

Apparently, the probability of node n with capacity Cn become super-node is

$$p_{Cn} = C_n / C_s \qquad (14)$$

The greater Cn is the more probability to be a super-node. Similarly, the node's probability to become super-node is

$$p_{Tn} = T_n / T_s \qquad (15)$$

When a node has a capacity of Cn, and online time Tn, we assume that Cn, Tn is independent, then from (13) the combined amount of information is

$$I(C_nT_n) = I(C_n) + I(T_n) = -\log P_c - \log P_t \qquad (16)$$

In order to avoid the appearance of Cn , Ts in the formula, the above equation becomes

$$I(C_nT_n) = -\log\frac{C_n}{C_s} - \log\frac{T_n}{T_s}$$

Let

$$\delta(C_n,T_n) = \log C_n + \log T_n$$

Then

$$I(C_nT_n) = -\delta(C_n,T_n) + \log(C_n * T_s) \qquad (17)$$

Since $\log(C_n * T_s)$ is a constant，I (C_n,T_n) changes only with δ(C_n,T_n), So we can use δ(C_n,T_n) as conditions for selecting a super node 。The difference is that if the amount of information based on self-selected super-node, then I(C_n,T_n) the smaller the better, If bases on δ(C_n,T_n), then δ(C_n,T_n) the bigger the better. Since δ(C_n,T_n) only connected with Cn, Tn, not with Cs , Ts, equation of (17) is more feasible than (16). So the selection of super-nodes problem becomes the selection of δ(C_n,T_n).

D. Super-node Selection Algorithm

Our goal is to produce a super-node topology characterized by a about minimum number of super-nodes and the stability

of every super-nodes is taken into account. In order to do that, we adopt a classification criteria based on the measure introduced above: nodes with higher $\delta(C_n, T_n)$ are considered better candidates as superpeers. At each time, the target topology is the one composed by the about minimum set of nodes whose total capacity is sufficient to cover all other nodes as clients, moreover the super-nodes are stable as far as possible. Clearly, only in a static network the target topology may be obtained; in the presence of dynamism, the real topology will just approximate it.

The epidemic style algorithm for establishing the super-node and client relationships of the target topology is illustrated in Figure 4. The algorithm is executed only by super-nodes: being more powerful, they can more easily pay the cost of their selection protocol.

The rationale behind function RANDOMGET is the following: all super-nodes try to push clients towards more powerful nodes that are willing to accept more load. To do that, RANDOMGET performs a random selection among those superpeers that are underloaded and whose capacity is larger or equal than the capacity of the local node. Since UNDERLOADED may contain obsolete information, multiple selections are made until a node is found whose capacity is effectively larger than the current number of clients. Ties (nodes with the same capacity) are broken by selecting the node with the larger number of clients. The process continues until such a node is found or no other nodes can be probed.

```
RANDOMGET ()
  Define ξ 0.6
  ξ =1- η
  S←{r|(log(cr)* ξ + log(tr)* η )≥
     (log(C_p)* ξ + log(T_p)* η )∧r∈UNDERLOADED}
  q←null
  whil(S≠Φ∧q=null)
     r←<pick a random node from S>
     S=S-{r}
     lr←<request load from r>
       if (lr<cr∧((log(C_p)* ξ +log(tp)* η )
       <(log(C_r)* ξ +log(T_r)* η )∨lr>lp))
       q←r
  return q

UPDATE(C,p)
  CLIENTS←CLIENTS∪C
  if (lp == 0∧lp<cp)
     CLIENTS←CLIENTS∪{q}
     <q becomes a client>
  else if ( r∈CLIENTS：(log(cr)* ξ + log(tr)* η )
              > (log(cp)* ξ + log(tp)* η ))
     <transfer clients of q to r>
     CLIENTS←CLIENTS∪{q}-{r}
     <q become a client，r becomes a server>
```

Figure 4. Super nodes selection algorithm in SPSI

V. EXPERIMENTAL EVALUATION

To validate our framework, we have performed numerous experiments based on simulation. Three main questions were interested in by us: first, what is the behavior of the protocol with respect to its parameters; second, what are the communication costs and time consumed associated with its execution; and third, how robust the protocol is.

TABLE 2.

INITIAL PARAMETERS IN EXPERIMENTS

Parameters	Values
SIZE	40000
MAXCAPACITY	180
MAXTIME	4000
DEGREE	30
REDUCED_DEG	30
ATTEMPTS	30
RATIO	1
LIMIT	0.95
WHEN	30
CRASH	0.90
LAMD	0.02
ALPHA	1.8

All experiments are performed using Peersim and its round-driven Style. In all figures, 20 independent experiments have been performed. Unless stated otherwise, most of the parameters are fixed in all experiments: the maximum capacity of a peer is 500; and the size s of partial views used in NEWSCAST[19] is 30. All these values can be reasonably adopted or measured in realistic settings; yet, the behavior of the algorithm observed under variations of these parameters are analyzed in the following. The initial parameter settings are showed in Table 1.

Value of weighted arithmetic mean coefficient From (7), There are some questions we must resolve. One is C_n and T_n has different dimensions, and the other is C_n and T_n has different quantity scale. If C_n or T_n is very large, and T_n or C_n is very small, so $\delta(C_n, T_n)$ is large. Here the selected node is not our expected super-node. In order to resolve these questions, we introduce the information quantity theory to resolve it. The value of ξ is important. We get the value of ξ from experiments. From [20] we set $\bar{x} = 266$, then the parameter is $\hat{\lambda} \approx 0.004$. When the distribution parameter is determined, it will generate the random exponential distribution number as the node's online time, and the value of C_n is generated from [18].

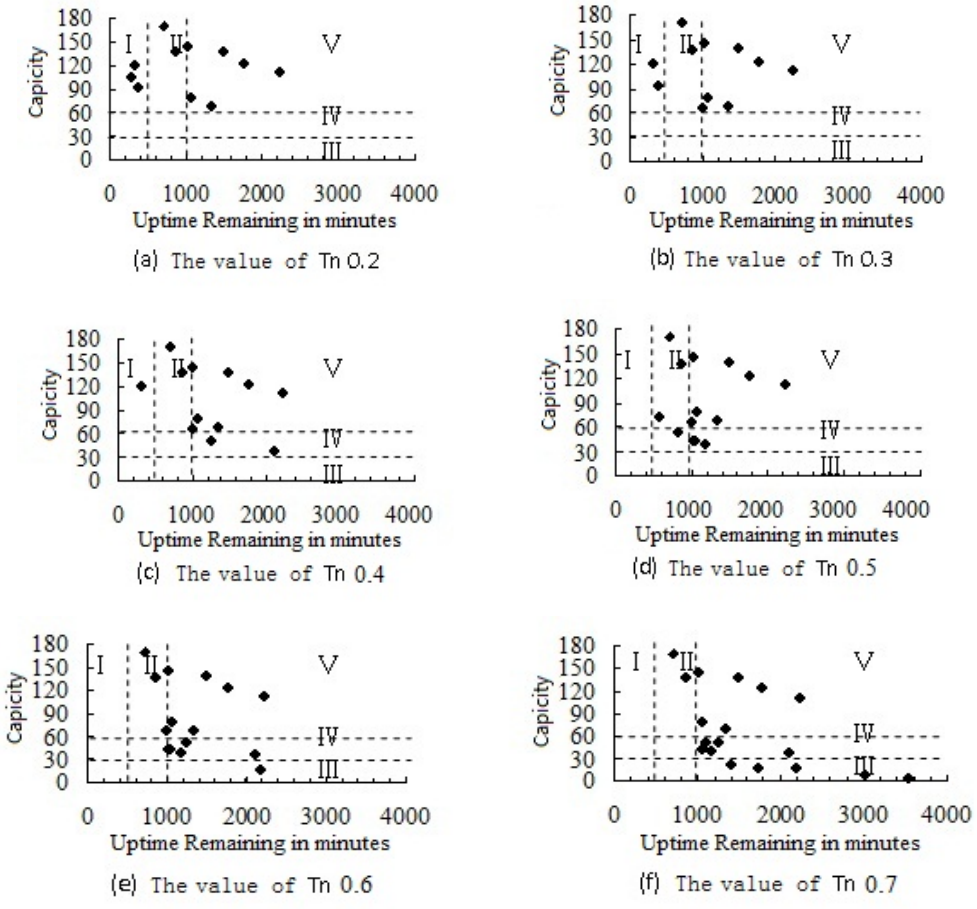


Figure 5. Values of coefficient Test

For a given online time weight T_n, 0.2,0.3,……,0.8, and the corresponding node content weight C_n as 0.8,0.7,……,0.2. The experiments are carried out, and the results are shown in Figure 5.

To illustrate easily, we divide the figure into four region. $T_n \in [0,500]$ are defined region I, $T_n \in [500,1000]$ is region II, and the nodes of the region are more active than the nodes of region I. $C_n \in [0,30]$ are defined region III, the nodes belong to this region, their capacity are lower, and $C_n \in [0,30]$ are defined region IV. If $T_n > 1000$ and $C_n > 500$, that is to say that the nodes belong to this region have longer online time and higher capacity, these nodes are those we try to select as super-nodes.

From Figure 5 we can see that when the weight of T_n is 0.2, there are too many nodes in region I, that is to say the super-nodes we selected are too active, and the network have to reselect when the super-node is left. When the weight of T_n is 0.6 or 0.7, and too much nodes are located in region III, region IV, that is to say the super-nodes we selected have lower capacity. So it is better to set the weight of T_n 0.4 or 0.5 and it is better to set the weight of C_n is 0.6.

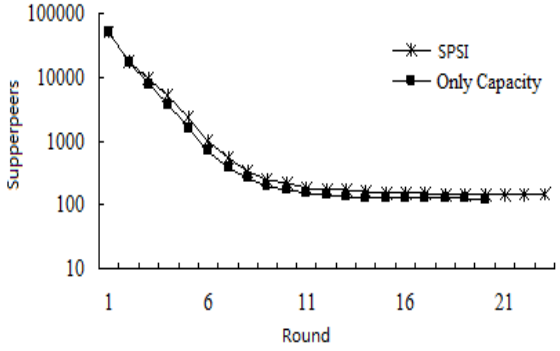


Figure 6. Network convergence Test

A. The Convergence Speed of Network Construction

The goal of convergence experiment is to measure the speed of convergence, it's important in overlay network construction. In the experiments we also make our protocol with SG-1, a famous super-node construction protocol based on NEWSCAST[19] to compare the convergence speed. The results are showed in Figure 6. In the picture, dashed line indicates the number of super nodes with SPSI protocol, while Solid line represents the number of super nodes with SG-1. It can be seen that the convergence speed of SPSI and SG-1 are basically consistent. The time needed to reach such utilization

thresholds is independent from network size and around 10 and 13 rounds, respectively. As initial configuration, we selected a topology that is the farthest from the target: a random topology where all nodes behave as super-nodes, although none of them is responsible for any client. The curves represent the number of super-nodes contained in the network after the specified number of rounds, averaged over 20 experiments. Individual experiments are shown; their x-coordinates have been shuffled with a small random increment to separate similar results. The algorithm proves to be extremely fast, independently from the distribution considered: after less than 15 rounds, the resulting topologies approximate extremely well the target.

B. The Selected Super-nodes

Figure 7 and Figure 8 shows the online time parameter's impact on the number of selected super nodes. The horizontal axis is the uptime remaining (in minutes) of nodes, the vertical axis is the capacity of node. There are 1000 nodes in the network being tested. Each "fork" represents client nodes (shown using "+") and a box indicates the super node (shown using □).

From Figure 7, we can see that some nodes with low remaining uptimes are selected as super-nodes, and as these nodes leave the system, the system has to select another node in the network to take over its work. Figure 8 shows that most super nodes are located at the center of the graph, explaining that the selected super-node has a certain capacity and a longer time line. It can be seen that the SPSI protocol can effectively avoid selecting active nodes as super nodes, thus increasing the stability of the target topology.

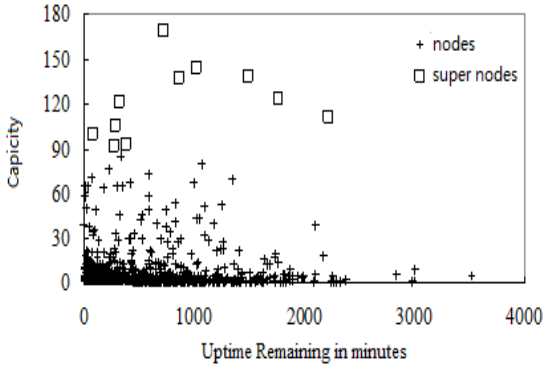


Figure 7. Super nodes selection without online time parameter

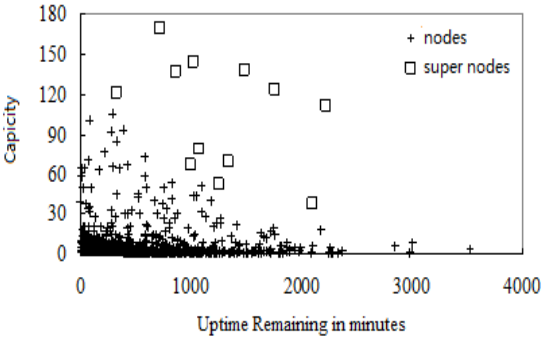


Figure 8. Super nodes selection with online time parameter

C. Communication Costs

In order to verify the effect of the protocol to lower communication costs, we conduct experiments 9. Two communication costs are to be considered: the total number of probes sent in protocol to discover the load of other super-nodes, and the total number of client transfers performed.

Super nodes take more responsibility in a super nodes based peer-to-peer network. When a super node logouts from the system or a super node decides to alleviate its load, it will bring about considerable communication cost. The main purpose of the SPSI protocol is to select a relatively stable node as super-node and save part of the network overhead. In Figure 9, the solid line represents the results of SPSI protocol, while the dotted line shows only the case of the node capacity. The SPSI protocol can select out relatively stable nodes when selects super-nodes, thus it has fewer reconfiguration. Only using the node capacity as selection method, the super nodes will have higher activity, and the network is not stable enough, thus it has more reconfiguration than the self-information algorithm.

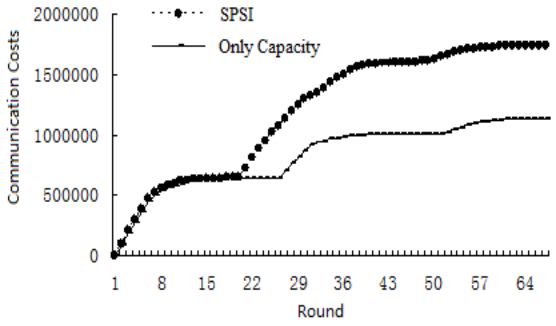


Figure 9. Communication Costs

Figure 9 shows the difference between the capacity and the self-information amount algorithm in the overhead costs. The overhead costs include exchange of messages between nodes and conversion cost between client nodes. It can be seen from the figure, the cost has not been decreased with the self-information amount algorithm in the early time of the network construction, but after a long period, when there are nodes exiting the network, the cost of the self-information amount algorithm is significantly less than that of capacity algorithm. It can be seen that the algorithm can effectively limit the number of active nodes as super nodes, thereby reducing the overhead for building the network.

D. Roubst Test

In order to demonstrate the robustness of our protocol, we hypothesis a catastrophic scenario and the test result is shown in Fig.10.: at round 30, 50% of the super-peers are removed. After the initial period when all clients whose super-peer has crashed become super-peer by themselves, the protocol behaves as usual and repair the overlay topology by selecting new super-peers among the remaining nodes.

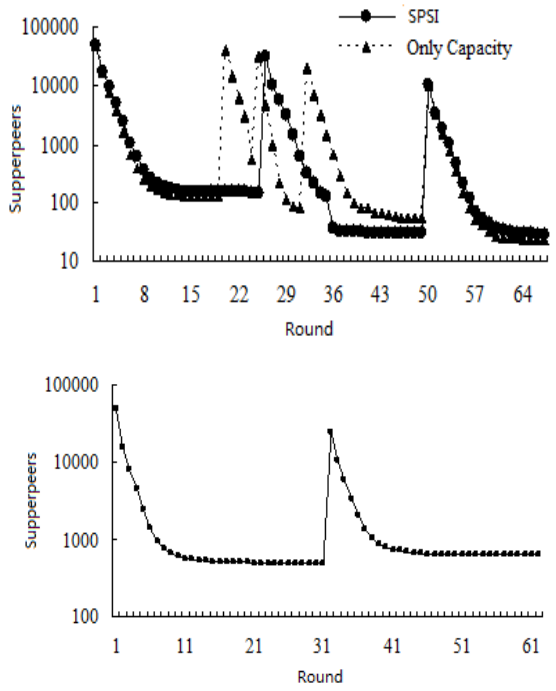


Figure 10. Roubst Test

VI. CONCLUSIONS

This paper presented SPSI, a fully decentralized, self-organizing general protocol for the construction of super-node-based overlay topologies. To our best knowledge, we are the first to introduce information theory to super-node selection. The number of generated super-nodes is a little more than SG-1 but small with respect to the network size (only 3-5%), and it's important that the more stable peers are promoted as super-nodes, so the communication costs are degraded and the target topology is more stable. The protocol shows also an acceptable robustness to churn.

REFERENCES

[1] L. Meirong, K. Timo, O. Zhonghong, Z. Jiehan, R. Jukka, Y. Mika, "Superpeer-based coordinated service provision", Journal of Network and Computer Applications,Vol 34, pp. 1210–1224, July 2011.
[2] S. Moritz, E.N. Taoufik, W.B. Ernst, "Long term study of peer behavior in the KAD DHT". IEEE/ACM Trans. Netw. Vol. 17, pp. 1371-1384, October 2009.
[3] Z. Liu, C. Wu, B. Li, S. Zhao, "Distilling Superior Peers in Large-Scale P2P Streaming Systems". In Proc. of INFOCOM'2009. pp.82~90.
[4] D.T. Talia, P.Trunfio, "Towards a Synergy between P2P and Grids", IEEE Internet Computing, vol4, pp. 94-96, July.2003.
[5] A.I. Iamnitchi, I. Foster, J.Weglarz, J. Nabrzyski, "A Peer-to-Peer Approach to Resource Location in Grid Environments", In: Proceedings of the 11th Symposium on High Performance Distributed Computing, Edinburgh, UK, August 2002.
[6] Z. W. Gao, Z. M. Gu, P. Luo, "RBTree: a new and scalable p2p model based on gossiping". In:Proceedings of the IEEE International Symposium on Ubiquitous Multimedia Computing (UMC 2008). October, 2008.
[7] J. P. Gian, M. Alberto, and B. Ozalp, "Proximity-aware Superpeer Overlay Topologies". IEEE Transactions on Network and Service Management (TNSM), Vol. 4, pp:74-83, September 2007.
[8] KaZaA, [Online]. Available: http://www.kazaa.com/.
[9] K. Truelove, Gnutella and the transient web, Whitepaper, 2002.
[10] S. Q. Lv, Ratnasamy, S. Shenker, "Can heterogeneity make gnutella scalable?". in: Proc. IPTPS, March 2002.
[11] B. Yang, H. Garcia-Molina, "Designing a superpeer network". In: Proceedings of the 19th International Conference on Data Engineering. (2003) 49–60.
[12] A.T. Mizrak, Y. Cheng, V. Kumar, S. Savage, "Structured superpeers: Leveraging heterogeneity to provide constant-time lookup". In: Proceedings of the 3rd IEEE Workshop on Internet Applications. (2003) 104–111.
[13] L. Garces-Erice, E. Biersack, P. Felber, K. Ross, G. UrvoyKeller, "Hierarchical peer-to-peer systems", in: Proceedings of EuroPar, Klagenfurt, Austria, 2003.
[14] W. Nejdl, M. Wolpers, W. Siberski, C. Schmitz, M. Schlosser, I. Brunkhorst, A. L¨oser, "Super-peer-based routing and clustering strategies for RDF-based peer-to-peer networks", in: Proceedings of the 12th International World Wide Web Conference, Budapest, Hungary, 2003.
[15] A. Mizrak, Y. Cheng, V. Kumar, S. Savage, "Structured super-peers: Leveraging heterogeneity to provide constant-time lookup", in: IEEE Workshop on Internet Applications, 2003.
[16] A. Singh and M. Haahr, "Creating an adaptive network of hubs using Schelling's model," Commun. ACM, vol. 49, no. 3, pp. 69–73, 2006.
[17] H.J. Liu, P. Luo et.al, "A structured hierarchical P2P model based on a rigorous binary tree code algorithm". Future Generation Computer Systems-The International Journal of Grid Computing Theory Methods and Applications 23 (2): 201-208 Feb 2007.
[18] A. Montresor, "A robust protocol for building superpeer overlay topologies," In Proc. of the 4th Int. Conf. on Peer-to-Peer Computing. Zurich, Switzerland: IEEE, August 2004.
[19] J. Márk, V. Spyros, G. Rachid, K. Anne-Marie, and S. Maarten, "Gossip-based peer sampling". ACM Transactions on Computer Systems, 25(3):8, August 2007.
[20] S. Saroiu, P. K. Gummadi, and S. D. Gribble, "A measurement study of peer-to-peer file sharing systems". In Proc of Multimedia Computing and Networking 2002 (MMCN '02), San Jose, CA, USA, January 2002.

Zhiwei Gao is an associate professor at the Department of Computer Science, ShiJiaZhuang TieDao University. He is a Ph.D. student in the Department of Computer Science at Beijing Institute of Technology, Beijing, China. He received her Master degree from school of information and computer technology,Beijing Jiao Tong University.His current research interests are in network security, distributed computing and peer-to-peer systems.

Yingxin Hu is a lecture at the Department of Computer Science, ShiJiaZhuang Railway Institute. His current research interests are in e-commerce, distributed computing and peer-topeer systems. He received his master's degree in computer science from ShiJiaZhuang Railway Institute, China.

SFML: Screening Form Markup Language for Healthcare Service

Kyuchang Kang*, Seonguk Heo*, Changseok Bae*

**BigData Software Research Lab. Electronics and Telecommunication Research Institute*

218 Gajeongno Yuseong-gu Daejeon Korea

{k2kang, h7530, csbae}@etri.re.kr

***Abstract*— This paper proposes a markup language to describe and deliver the contents of health screening form and a case study for data transfer. In this paper, we define elements and schema needed to generate a health screening form based on personal lifelogs including data from daily, health and medical domain. In our proposal, we allow for three categories of data. First, the daily domain includes lifestyle data represented as activity, a sleeping pattern and eating habits. Second, the health domain includes height, weight, blood pressure, glucose and so on. Third, the medical domain includes the result of medical treatment information from a medical institute. This information is structured as SFML and can be exchanged with participant of health service entities.**

***Index Terms*—Healthcare, lifelog, markup language, screening form**

I. INTRODUCTION

MAJOR challenges to modern healthcare is to find solutions to cope with aging population, rising of inpatient and ambulatory costs, lack access to facilities and personal of rural residents. Due to the aging population, chronic disease began to emerge as the central healthcare issue. Chronic disease is the major cause of disability, the principle reason why patients visit hospitals [1]. Especially, South Korea is expected to become the most aged country in the world in 2050, raising worries it could erode the economy's growth potential.

To prevent or monitor chronic diseases, we need continuous monitoring of lifestyle and connection with healthcare professionals. A health screening in everyday life can be one of solution for these objects.

Screening, in medicine, is a strategy used in population to detect a disease in individual without signs or symptoms of that disease. Unlike what generally happens in medicine, screening tests are performed on persons without any clinical sign or disease [2].

Todays, almost all the people have chance of a regular health screening supported by a company or the government every year. As preparing the checkup, people may generally fill up the health screening questionnaire to describe their health-related condition. From the point of personal information, an individual's lifelog of everyday life is a good record of behavior. Therefore, using the personal lifelogs is good approach to provide personalized healthcare service after the analysis of individual's behavior.

In addition to individual's behavior, we can consider health-oriented information to configure screening questionnaire. As one solution to describe individual's condition and current status of body, we describe a health screening form leveraging personal lifestyles, biometric information, and medical treatments. By the health screening form, individual's health-related data can be commonly utilized in private and public medical institutes. To this end, users can generate and leverage their screening form. As the result, users can provide their screening form with medical staff on demand when they visit a medical center.

On the other hand, the health screening form is melting pot of various personal data and maybe used various entities of healthcare service. Therefore, we also consider the cooperation and compatibility of them. To meet this need, we propose SFML (screening form markup language) to embrace various data and to exchange them with associated entities.

In this work, we define and specify XML elements for control and data transmission and describe case study for personal lifelog-based screening form, as a part of screening system architecture.

The remainder of this paper is organized as follows. In section II, we present related background of this work. Section III shows the concept of the health screening form, a prototype implementation and related data specifications. In section IV, we present SFML scheme and a case study including data transfer. Section V discusses related studies and the needs for standardization. Finally, we conclude this paper in Section V.

Manuscript received June 30, 2012. This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST)(No. 2012-0001002).

Kyuchang Kang is with Electronics and Telecommunication Research institute, 218 Gajeongno Yuseong-gu Deajeon 305-700 Korea (phone: +82-42-860-1695; fax: +82-42-860-5545; e-mail: k2kang@ etri.re.kr).

Seonguk Heo is with Electronics and Telecommunication Research institute, 218 Gajeongno Yuseong-gu Deajeon 305-700 Korea (e-mail: h75304@ etri.re.kr).

Changseok Bae is Electronics and Telecommunication Research institute, 218 Gajeongno Yuseong-gu Deajeon 305-700 Korea (e-mail: csbae@ etri.re.kr).

II. BACKGROUND

This section presents the background environment of this work.

In the medical field, it is necessary to gather as much personal information as possible about patients in order to achieve high-quality diagnosis and treatment. Until now, the personal information used in diagnosis and treatment has basically been gathered and used only within medical facilities. It consists of clinical records, test results, medical images, and other such information. However, the medical information that can be gathered within a medical facility is very limited. It would seem that there is a large amount of data that would be useful for medical purposes within the voluminous and varied data gathered in daily life, most of which is spent outside medical facilities, but such lifelog data has gone unused in most cases [3].

In Korea, SBI (systems biomedical informatics) research center aims to create personalized 'health avatar', representing individuals genomic through phenomic reality (or 'digital self') using multi-scale modeling and data driven semantics for the purpose of personalizing healthcare [4].

'The health avatar platform' will be created as an agent space and health data integration pipeline. 'Health avatar platform' will create a space for interacting plug-in intelligent health agents and data analysis toolkits and provide a data and access grid for heterogeneous clinical and genomic data. The health avatar platform will function as an infra-structure for the development and evaluation of intelligent health applications for personalized medicine.

Fig. 1 shows the conceptual diagram of health avatar and this work is conjunction with the 'Connected Self' of health avatar project supporting lifelogs and stream-type data mining for health protection.

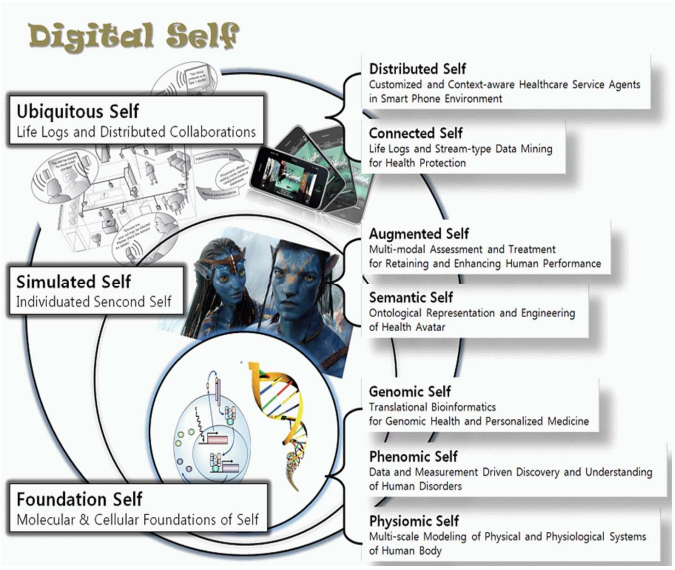


Fig. 1. Conceptual diagram of health avatar

III. HEALTH SCREENING FORM

Basically, the health screening form should reflect individual's lifestyles, health-related information and medical treatments. And it is also compatible with a conventional paper-based screening questionnaire.

In order to satisfy these requirements, we can summarize components of the health screening form as three categories of data as followings:

- Lifestyle logs: representing user's lifestyles such as activity, sleeping patterns, and eating habits
- Health logs: representing biometric information of individuals such as height, weight, blood pressure, heart rate, blood glucose, total cholesterol, high-density lipoprotein (HDL), low-density lipoprotein (LDL), triglycerides and so on
- Medical logs: representing medical treatments such as genetic disease history, previous drug reaction and so on

Additionally, we can also consider interactive question & answer tool on behalf of paper-based screening questionnaire.

Fig. 2 shows the conceptual model of a health screening form and operational flow.

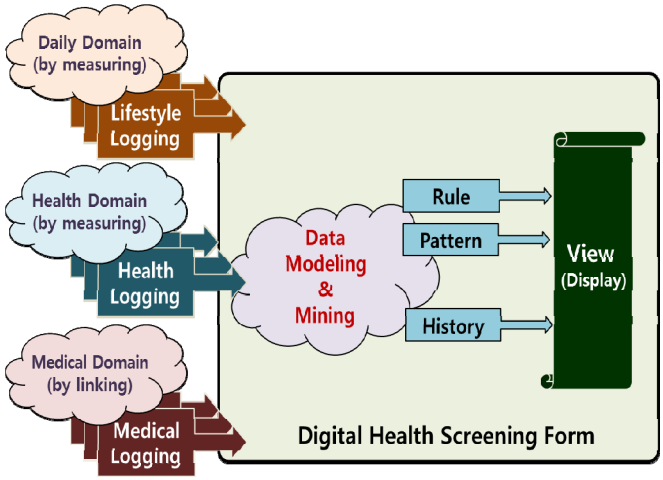


Fig. 2. Basic concept of a health screening form and its operational flow

Basically, the health screening form consists of user's data from daily, health and medical domain. Then, these data are mixed and mined with knowledge from various expertises. From these processing, we can summarize the user's lifelogs as 'rule', 'pattern', and 'history'. These elaborated data can be seen to user through a smart device and transferred to a care giver for an advanced care.

Fig. 3 shows the screenshot of prototype implementation for health screening form in current project [5-6]. Current version of the health screening form focuses on gathering and displaying data.

Fig. 3. The screenshot of prototype health screening form

As data items considered in daily domain for generating screening form, we can leverage data such as activity, sleeping pattern, and eating habits associated with lifestyle. The data associated with lifestyle in daily domain can be collected by wearable or portable life logging device or a smartphone embedding various sensors.

These data are formalized as 'lifestylelog descriptor' in XML document. Fig. 4 shows the example of the lifestylelog descriptor.

```
<?xml version="1.0"?>
<lifestylelog name="Lifestylelog Descriptor"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation=
  "http://www.etri.re.kr/ncrc/connectedself/lifestylelog.xsd">
    <log_info>
        <owner name="Gildong Hong"/>
        <id>gd_hong</id>
        <device>
            <description>smart phone lifestylelog collector</description>
            <identifier>kr.re.etri.ncrc.lifestylelogger.type1</identifier>
            <vendor>ETRI</vendor>
            <model_number>2000-1000</model_number>
            <model_info>http://www.etri.re.kr/ncrc/lifestylelogger/2000-1000
            </model_info>
        </device>
    </log_info>
    <items>
        <item data="sleeping">
            <start_time>2011.11.22:23:00:00</start_time>
            <end_time>2011.11.23:07:00:00</end_time>
        </item>
        <item data="meal" type="lunch">
            <menu>Chines Noodle</menu>
            <start_time>2011.11.22:12:00:00</start_time>
            <end_time>2011.11.22:12:45:00</end_time>
            <base_calorie>1200</base_calorie>
            <photo>13098896899.jpg</photo>
        </item>
    </items>
</lifestylelog>
```

Fig. 4. Example of the lifestylelog descriptor

As data items considered in health domain for generating screening form, we can leverage data used in home healthcare or mobile healthcare which are usually gathering data with dedicated devices from a user. In general, the device collects data associated with user's biometric information such as height, weight, blood pressure, glucose, heart rate and so on.

These data are formalized as 'healthlog descriptor' in XML document. Fig. 5 shows the example of the healthlog descriptor.

```
<?xml version="1.0"?>
<healthlog name="Healthlog Descriptor"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:noNamespaceSchemaLocation=
  "http://www.etri.re.kr/ncrc/connectedself/healthlog.xsd">
    <log_info>
        <owner name="Gildong Hong"/>
        <id>gd_hong</id>
        <device>
            <description>wearable bio-signal collector</description>
            <identifier>kr.re.etri.ncrc.healthlogger.type1</identifier>
            <vendor>ETRI</vendor>
            <model_number>1000-2000</model_number>
            <model_info>http://www.etri.re.kr/ncrc/healthlogger/1000-2000
            </model_info>
        </device>
    </log_info>
    <items>
        <item data="blood_pressure">
            <value time="2011.11.22.13:00:00" option="min">80</value>
            <value time="2011.11.22.13:00:00" option="max">120</value>
        </item>
        <item data="heart_rate">
            <value date="2011.11.22:13:00:00">80</value>
        </item>
    </items>
</healthlog>
```

Fig. 5. Example of the healthlog descriptor

As data items considered in medical domain for generating screening form, we can leverage data generated by medical institute such as disease history, genetic disease history, total cholesterol, high-density lipoprotein (HDL), low-density lipoprotein (LDL) and so on. These data associated with medical field should be linked with the database of medical institute. Therefore, we define the element for the healthlog descriptor but do not specify the consisting sub-elements. We use just link of the medical data sources instead of defining sub-elements because the medical data allow only very constrained access.

IV. SFML: Screening Form Markup Language

This section describes SFML (screening form markup language) defining 'action' and 'data' elements and case study for data transfer.

The components that comprise a health screening form have a hierarchical structure. The top layer consists of 'action' element and 'data' element. The 'action' element defines control action messages including 'request' element and 'response' element. The 'data' element defines three categories of items such as 'lifestylelog', 'healthlog' and 'medicallog'. Each category item has its own sub-items. Each item is

represented by XML elements and includes formatted data respectively.

A. Action and Data Elements

Fig. 6 describes XML structure, named as SFML, including 'action' and 'data' elements.

The root element is 'sfml' representing 'screening form markup language'. The root element has 'action' element for control action message and 'data' element for data presentation. As a sub-element, 'data' element has 'items' element containing three 'category' properties such as 'lifestylelog', 'healthlog", and 'medicallog'.

```
<?xml version="1.0"?><!DOCTYPE sfml []>
<sfml name="Health Screening Form"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation=
  "http://www.etri.re.kr/ncrc/connectedself/sfml.xsd">
    <action>
        <request>...
        <response>...
    </action>
    <data>
        <items category="lifestylelog">...
        <items category="healthlog">...
        <items category="medicallog">...
    </data>
</sfml>
```

Fig. 6. XML structure of SFML

Fig. 7 shows the 'action' element of SFML in detail. The 'action' element consists of 'request' and 'response' elements. The 'request' element is a request form for any action and can have multiple messages encapsulated by 'message' element. The number of each 'message' element is mapped with the number of 'session' element in 'response' element.

Each 'message' element is composed of three sub-elements such as 'target', 'command' and 'parameter' elements. The 'target' element indicates the action executor such as a module name of a message recipient. The 'command' element indicates the method name of the action executor. The 'parameter' element contains parameter values needed to run the method of the action executor. The sub-elements of 'parameter' element such as 'id' and 'interval' depend on the value of command.

The 'response' element is a response form for any action execution. The 'response' element can have multiple 'session' elements for each control action respectively. The number of each 'session' element is mapped with the number of 'message' element in 'request' element.

Each 'session' element is composed of two sub-elements such as 'result' and 'results'. The 'result' element only indicates success or failure for the request action. If the action is performed successfully, the 'results' element is filled with the results of the action execution. The sub-elements of the 'results' element depend on the executed command.

The description of the 'message' element of request action shown in Fig. 7 is as following.

- The value of the 'target' element indicates that the logmanager module of SFML recipient may process this request
- The value of the 'command' element indicates that the 'getWeight' method of the logmanager may be executed
- The values of the 'parameter' element indicates; the related data owner is 'gd_hong', the response data should start from November 22, 2011, and the data is needed two days

The description of 'session' element of the response action shown in Fig. 7 is as following.

- The 'true' value of the 'result' element indicates that the request action is successful
- The 'results' element indicates that the 'gd_hong' has 70kg in November 22, 2011 and 71kg in November 23, 2011

The XML document of Fig. 7 is just an example so that we describe the 'request' and 'response' elements together. In practical case, the request action includes only 'request' element and the response action contains only 'response' element respectively.

```
<action>
    <request>
        <message num="1">
            <target>kr.re.etri.ncrc.connectedself.
                healthlog.logmanager</target>
            <command>getWeight</command>
            <parameter>
                <id>gd_hong</id>
                <start_time>
                    <unit>day</unit>
                    <time>2011.11.22</time>
                </start_time>
                <duration>2</duration>
                <interval>1</interval>
            </parameter>
        </message>
        <message num="2">
        </message>
    </request>
    <response>
        <session num="1">
            <result>true</result>
            <results>
                <id>gd_hong</id>
                <time>2011.11.22</time>
                <data>70</data>
                <time>2011.11.23</time>
                <data>71</data>
            </results>
        </session>
        <session num="2">
        </session>
    </response>
</action>
```

Fig. 7. Example for the 'action' element of SFML

Fig. 8 shows the 'data' element of SFML in detail. The 'data' element can have three items which have category properties such as 'lifestylelog', 'healthlog' and 'medicallog'. Each 'items' element has 'id' and 'item' elements. The 'id' element indicates the owner of the item data and the 'item' element contains real data values. The 'data' property of the 'item' element indicates what kind of data.

```
<data>
    <items category="lifestylelog">
        <id>gd_hong</id>
        <item data="sleeping">
            <start_time>2011.11.22:23:00:00</start_time>
            <end_time>2011.11.23:07:00:00</end_time>
        </item>
        <item data="meal" type="lunch">
            <menu>Chinese Noodle</menu>
            <start_time>2011.11.22:12:00:00</start_time>
            <end_time>2011.11.22:12:45:00</end_time>
            <base_calorie>1200</base_calorie>
            <photo>13098896899.jpg</photo>
        </item>
    </items>
    <items category="healthlog">
        <id>gd_hong</id>
        <item data="blood_pressure">
            <value time="2011.11.22.13:00:00"
              option="min">80</value>
            <value time="2011.11.22.13:00:00"
              option="max">120</value>
        </item>
        <item data="heart_rate">
            <value date="2011.11.22:13:00:00">80</value>
        </item>
    </items>
    <items category="medicallog">
        <id>gd_hong</id>
        <link>http://healthportal.org/sfml/gd_hong</link>
    </items>
</data>
```

Fig. 8. Example for the 'data' element of SFML

Generally, the 'data' element of SFML can contains lifestylelog descriptor, healthlog descriptor and medicallog descriptor in a manner of full text. In a case of just simple querying data, the 'response' element of SFML can support the action. However, in case of the request action requires full data of the user, the 'data' element is used by embracing mentioned three descriptors.

The XML document example of Fig. 8 contains three descriptors of 'gd_hong'. The 'items' element with 'lifestylelog' category property contains the 'item' elements following the lifestylelog descriptor. And the 'items' element with 'healthlog' category property includes the 'item' elements following the healthlog descriptor. On the other hand, the 'items' element with 'medicallog' category property, the link to the medical information is used.

B. Case Study for Data Transfer

This section describes cases of data transfer from data sources to Screening Form Generator, functional module of health screening form.

As the device of data sources, we can use smartphones, tablets or 3rd party's devices. In this case, for gathering lifelogs, we can use built-in sensors of the smart devices such as accelerometer and GPS or connected 3rd party's devices such as blood pressure meter, weighting scale and blood glucose meter.

Fig. 9 shows the data transfer example of daily and health domain. In this configuration, each Collector Driver is gathering data from built-in sensors of the smart device and 3rd party's devices as a proprietary format. Then, Convertor transforms and formalizes the data sent from Collector Driver by referencing Schema such as lifelog descriptor or healthlog descriptor according to the data sources respectively.

In this case study, we only consider lifestylelog and healthlog descriptors for gathered data in Lifelogging application. However, this module can be extended or modified according to the standardization activities described next section.

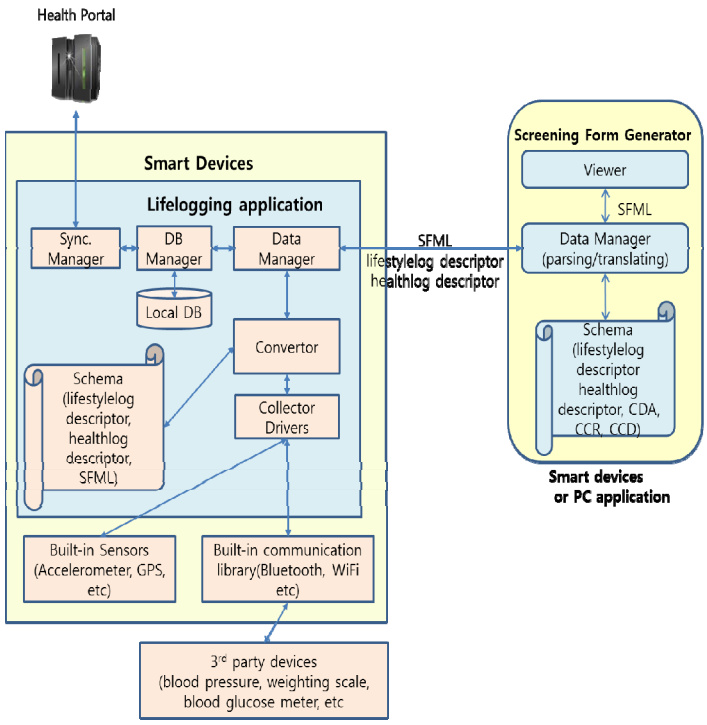


Fig. 9. Data transfer for daily and health domain

Data Manager can store the transformed data in Local DB, which can be used as data cache. The transformed data can be also sent to Screen Form Generator. Then, Data manager module of Screening Form Generator refers Schema description and can extract data values. Consequently, the data values can be displayed in Viewer user interface.

Generally, Screening Form Generator can be running in smart devices or conventional personal computers.

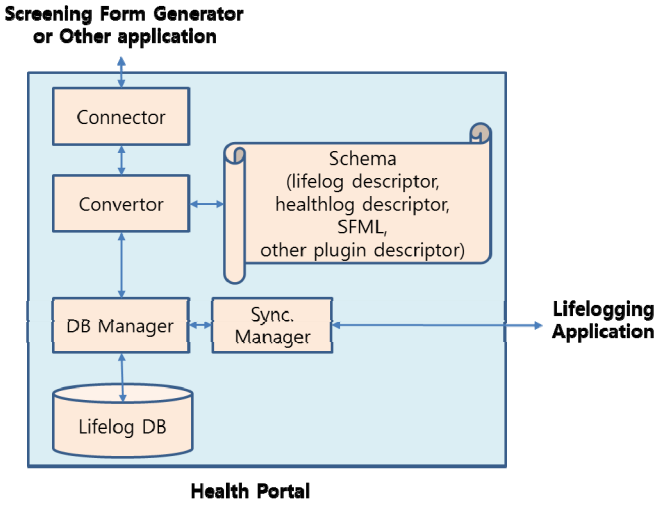


Fig. 10. Data synchronization and its utilization for daily and health domain

On the other hand, the transformed data by Convertor can be

synchronized with the DB of Health Portal through Sync. Manager. In this case, the synchronized data can be used in another screening form generator or independent other application shown in Fig. 10.

In the result, data structured by SFML can be exchanged and transferred to SFML viewer of a care giver for an advanced care.

In order to define the data sets for transferring medical treatment documents, we can use CDA (Clinical Document Architecture) [7] of HL7 (Health Level Seven), CCR (Continuity of Care Record) [8] of ASTM (American Society of Testing and Materials), or CCD (Continuity of Care Document) [9], combined model of CDA and CCR.

As the data transfer specification in health screening form, we can use those international standards. Therefore, we only parse and translate the data, encapsulated with standardized XML format, instead of defining new 'medical descriptor'. This operational flow is shown in Fig. 11.

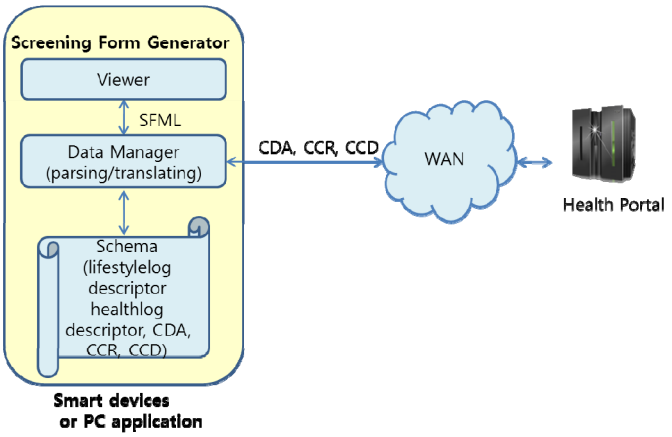


Fig. 11. Data transfer for medical domain

V. Discussion

From the perspective of a health screening questionnaire, Chris et al [10] proposed an adaptable health screening questionnaire that is computer-based lifestyle questionnaire allowing individual doctors to modify the questionnaire to their requirement. K. D. Akan et al [11] developed electronic screening tool providing a graphical user interface with audio outputs for users who may be functionally or computer illiterate. However, these previous trials are only subsidiary function of the health screening form described in this paper and does not suggest how to transfer data and control messages.

From the lifelog utilization point of view, NTT have studied several subjects [12-13] enabling lifelogs to be used in the practical service implementation. In case of these NTT's previous work, we can coordinate these results as a lifestyle category of the health screening form.

From a device point of view, there are several commercial life logging devices [14-17]. These devices can provide a health screening form with the lifestyle data.

As increasing of multiple vendors' devices, we need to standardize the transmission of data and control messages. For this needs, we are participating in standardization activities of TTA (Telecommunication Technology Association) in Korea.

Currently, two standard documents are released with respect to digital health screening form. TTAK.KO-10.0516 [18] is a standard document for a reference model for personal lifelog based system. TTAK.KO-10.0517 [19] is a standard document for link data specifications based on personal lifelog. However, these standardization activities are now on the initial phase of work. Therefore, we also need to do additional work to update and specify standard documents in detail.

Furthermore, from the perspective of user interfaces, the Viewer of Screening Form Generator may need to be changed into HTML5-support. To support the concept of "Write Once, Run Anywhere" by providing compatibility of heterogeneous devices such as Android-based devices and iOS-based devices, we need to do more work by keeping pace with standardization activities in [18-19].

VI. Conclusion

This paper proposes a markup language, SFML, to describe and deliver the contents of health screening form and case study for data transfer.

In this paper, we define elements and schema needed to generate health screening form based on personal lifelogs including data from daily, health and medical domain.

SFML defines 'action' element and 'data' element. The 'action' element is used to control any action through 'request' and 'response' elements. The 'data' element is used to present data including lifestylelog, healthlog and medicallog.

Currently, because this work is an initial phase to make a health screening form, we lack of an elaborate algorithm or a breakthrough idea. However, we think this work will contribute to make a personalized and mobilized health screening form reflecting personal lifestyles, health information and medical histories.

In the future, we plan to continue our research efforts in this field with the aim of making an intelligent screening form. So we need to allow for an interpretation of relationship between data by means of data mining algorithm.

References

[1] H. Holman and K. Lorig, "Patient Self-Management: A Key to Effectiveness and Efficiency in Care of Chronic Disease," Public Health Report, Vol. 119, pp.239-243, 2004

[2] Wikipedia, "Screening (medicine)," http://en.wikipedia.org/wiki/Screening_(medicine).

[3] T. Ito, T. Ishihara, Y. Nakamura, S. Muto, M. Abe, and Y. Takagi, "Prospects for Using Lifelogs in the Medical Field," NTT Technical Review, Vol.9, No. 1, Jan., 2011.

[4] National Core Research Center, "Health Avatar", http://healthavatar.snu.ac.kr.

[5] Kyuchang Kang, Seonguk Heo, Changseok Bae, Dongwon Han, "Mobile Health Screening Form Based on Personal Lifelogs and Health Records," Lecture Notes in Electrical Engineering 107, IT Convergence and Services, Spinger 2011, pp.557-565

[6] Seonguk Heo, Kyuchang Kang, Changseok Bae, "Lifelog Collection Using a Smartphone for Medical History Form," Lecture Notes in Electrical Engineering 107, IT Convergence and Services, Spinger 2011, pp.575-582

[7] Health Level Seven (HL7), CDA, http://hl7book.net/index.php?title=CDA.
[8] ASTM E2369 – 05e1, Standard Specification for Continuity of Care Record (CCR), http://www.astm.org/Standards/E2369.htm.
[9] Wikipedia, CCD, http://en.wikipedia.org/wiki/-Continuity_of_Care_Document.
[10] Chris Carey-Smith, David Powley and Keith Carey-Smith, "An Adaptable Health Screening Questionnaire," Proceedings of Artificial Neural Networks and Expert Systems, pp.259-260, 1993
[11] K. Doruk Akan, Sarah P. Farrell, Lisa M. Zerull, Irma H. Mahone, and Stepanie Guerlain, "eScreening: Developing an Electronic Screening Tool for Rural Primary Care," Proceedings of System and Information Engineering Design Symposium, pp.212-215, 2006
[12] H. Tezuka, K. Ito, T. Murayama, S. Seko, M. Nishino, S. Muto, and M. Abe, "Restaurant Recommendation Service Using Lifelogs," NTT Technical Review, Vol.9, No. 1, Jan., 2011
[13] T. Watanabe, Y. Takashima, M. Kobayashi, and M. Abe, "Lifelog Remote Control for Collecting Operation Logs Needed for Lifelog-based Services," NTT Technical Review, Vol.9, No. 1, Jan., 2011
[14] Microsoft, Introduction to SenseCam, http://research.microsoft.com/en-us/um/cambridge/ projects/sensecam/
[15] ZEO, Sleeping Monitoring Device, http://www.myzeo.com/
[16] Livescribe, Pen-shaped Gadget, http://www.livescribe.com/ko/
[17] Evernote, Remember Everything, http://www.evernote.com/
[18] Telecommunication Technology Association, "Reference Model for Personal Lifelog based System – Digital Health Screening Form Part 1," http://www.tta.or.kr/data/ttas_view.jsp?rn=1&pk_num=TTAK.KO-10.0516
[19] Telecommunication Technology Association, "Link Data Specification based on Personal Lifelog – Digital Health Screening Form Part 1," http://www.tta.or.kr/data/ttas_view.jsp?rn=1&pk_num=TTAK.KO-10.0517

Kyuchang Kang (M'06) received his B.S. and M.S. degrees in electronic engineering from Kyungpook National University, Korea, in 1994 and 1997 respectively. From 1997 to 2000, he worked on Test and Evaluation Center at Agency for Defense Development as a member of engineering staff, where he developed Doppler signal analyzer and measurement system. Since 2001, he is working on BigData software laboratory and post-computer research division at Electronics and Telecommunications Research Institute, where he is developing open service platform for the healthcare service. He is also interested in mobile applications, distributed computing and network management.

Seonguk Heo received his B.S. degrees in computer engineering from Korea University of Technology and Education, Korea, in 2011. He is currently working toward the M.D. in computer engineering from the University of Science and Technology, Korea. He is interested in mobile applications, embedded computing, and lifelog data mining.

Changseok Bae (M'03) received his B.S. and M.S. degrees in electronic engineering from Kyungpook National University, Korea, in 1987 and 1989 respectively. He also received his Ph.D. degree in electrical and electronic engineering from Yonsei University, Korea, in 2003. From 1989 to 1996, he was a senior researcher at Systems Engineering Research Institute, where he worked on image processing and pattern recognition. From 1997 to 1999, he worked with Korea Ministry of Information and Communication, where he participated in establishing national software research and development policy. Since 2000, he has been a principal research staff of Post-PC Platform Research Team and the team leader of Personal Computing Research Team at Electronics and Telecommunications Research Institute (ETRI). From 2004-2005, he was a Research Fellow at School of Information Technologies, University of Sydney, Australia. His research interests include image processing, multimedia codec, information hiding, personal life-log and stream type data mining.

Volume 1 Issue 2, Sep 2012, ISSN: 2288-0003

ICACT-TACT JOURNAL

Global IT Research Institute

1713 Obelisk, 216 Seohyunno, Bundang-gu, Sungnam Kyunggi-do, Republic of Korea 463-824

Business Licence Number : 220-82-07506, Contact: secretariat@icact.org Tel: +82-70-4146-4991