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

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 3 Issue 4, Jul 2014, 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. 3 Issue. 4

Optimizing a Cooperative Relay Network Using Advanced Power Allocation and Receiver Diversity Technique

Muhammad H.D. Khan*, Muhammad D. Khan**, Mohammed S. Elmusrati*

* *Communication and System Engineering Group, University of Vaasa, Finland.*

** *National University of Science and Technology, Islamabad, Pakistan*

hazandanish@yahoo.com, danial356khan@gmail.com, moel@uwasa.fi

***Abstract*— Cooperative relaying is a relatively new technique in wireless communication systems that make use of all the nodes present in a wireless sensor network by dynamically sharing their radio resources in a distributed manner. All the nodes present in the periphery of the two communicating nodes will act as relays and forward the information until it reaches the recipient node. By doing this, it achieves a significant diversity gain, which in turn increases the robustness of the communication system. The diversity gain offered by cooperative relay transmission can only be exploited fully if a receiver diversity technique is being employed at the recipient node. Moreover, theses cooperative relay networks inherit the power limitation of a traditional wireless sensor network. Therefore, in this paper an effort has been made to optimize a cooperative relay system by addressing these two issues. First, node powers expressions will be derived for a 3-node configuration using fixed gain amplify and forward protocol over a Rayleigh Fading Channel. Second, performance of a 3-node configuration has been further analyzed by using different receiver diversity techniques at the destination node. Simulation results are presented to validate the performance gains when advanced power allocation and receiver diversity is employed in a cooperative relay network.**

***Keyword*— Cooperative relay network, Maximal ratio combining, Moment generating function, Diversity techniques, Rayleigh fading channel, Fixed gain amplify and forward.**

I. INTRODUCTION

Over the last few decades, many new techniques have been developed to facilitate the process of wireless communication. These techniques have enhanced the performance of a wireless system in terms of throughput, coverage, capacity, reliability, etc. One such technique is of spatial diversity, which mitigates the effect of multi-path fading and provides diversity gains.

The technique of relaying in wireless communication emulates a multiple input multiple output (MIMO) system, as it is not feasible to equip a small node with multiple antennas. Cooperative relay transmission achieves spatial diversity, higher rates and increases robustness by using the antennas of the neighboring cooperating nodes [1] [2] and [3]. The source and the cooperating nodes send the same information to the destination node over independently fading paths, thus making a virtual antenna array [4]. At the destination node a diversity gain is achieved as it receives multiples copies of the same information [5]. Among the trusted and proven cooperative relaying techniques, amplify and forward protocol also known as non-regenerative relaying protocol stands out because of its simple execution and low computational cost. The simplicity comes from the fact, as the nodes running this protocol simply amplify the received signal and then forwards it to the destination node without any complex processing [6]. On the contrary, if each wireless node is running complex decoding and encoding for each transmission hop the performance of a wireless system is noticeably hampered. Therefore analysis of the cooperative relay system has been performed employing amplify and forward relaying protocol.

The process of optimizing the cooperative relay system has been divided into two tasks. The first task is to develop an advanced power allocation algorithm as the cooperative communication system inherits the power limitation of a traditional WSN. The power allocation algorithm is required to effectuate the transmission powers of the corresponding nodes. The prime objective is to allocate optimum transmission power to the source and the cooperating relay nodes while maximizing the quality of service at the receiver. The second task is to replace the traditional receiver diversity technique like maximum ratio combining with a more performance oriented technique.

In [7], the power allocation algorithm has been investigated for a cooperative relay network but regenerative relaying protocol has been used with a rician-fading channel.

Manuscript received May 15, 2014. This work was supported in part by the Communication and System Engineering Group at University of Vaasa, 65200 Vaasa, Finland.

Muhammad H. D. Khan is with the University of Vaasa, 65200 Vaasa, Finland. (phone: +92-346-5280626; e-mail: hazandanish@yahoo.com).

Muhammad D. Khan is with the National University of Science and Technology, 44000 Islamabad, Pakistan. (phone: +92-333-5486816; e-mail: danial356khan@gmail.com).

Mohammed S. Elmusrati is with the University of Vaasa, 65200 Vaasa, Finland. (phone: +358-504-003763; e-mail: moel@uwasa.fi).

In [8], an optimal power allocation OPA technique has been proposed for a cooperative relay network with different network configurations but maximum ratio combining has been employed at the receiver node. In this paper, the powers allocated to the involved nodes have been derived using the moment generation function (MGF) approach and optimization is achieved using the Lagrangian method [9]. Moreover, the sub-optimal receiver diversity technique (MRC) has been replaced with, first equal ratio combining (ERC) and then with enhanced signal-to-noise ratio combining (SNRC).

The remainder of this paper is organized as follows. Section II presents the system model and simulation parameters. In Sections III, the power allocation expressions for the involved nodes have been derived for the 3-node relay network configuration over a Rayleigh channel. In Sections IV, the diversity combining expressions for the receiver nodes have been derived for the corresponding network configuration. The efficiency achieved by the application of the above two proposed techniques is presented in form of performance graphs, in Section V. Section VI, concludes the paper.

II. System Model

A. Cooperative Relay Network

The network configuration is shown below in Figure 1. The network comprises of three nodes, namely a source node (*S)*, destination node (*D)* and a relay node (*R)*. Let $G_{SD,}$ $G_{SR,}$ *and* G_{RD} represent the channel gains for source to destination, source to relay and relay to destination links respectively. The communication channel between the nodes is assumed to be a Rayleigh fading channel and is normalized so that the fading coefficient matrix is complex Gaussian. At all times, each and every communicating node in the network will obey the rules of half duplex transmission. Fixed gain AF protocol has been used as a relaying technique. In the fixed gain AF relaying, the amplifier gain is based on the perfect CSI of the communication link rather than instantaneous knowledge of CSI. In the simulations the system performance has been measured for the end-to-end transmission. Therefore power constraints are applied for the complete transmission cycle instead of intermediate hops.

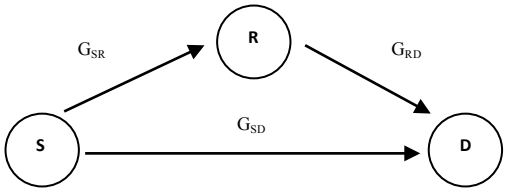


Figure 1. A 3-Node Network Configuration

III. Power Allocation & Diversity Combining

A. Transmission Phase

In the transmission phase, the source node *S* broadcasts data *X* with transmission power P_S to both relay and destination nodes, as shown above in figure 1. The channel gains for the source to relay and from source to destination links are G_{SR} and G_{SD} respectively. The additive white Gaussian noise (AWGN), present at the relay node n_{SR} and destination nodes n_{SD} - respectively. The signal received at the relay and destination will be expressed as Y_R and Y_D respectively. The expressions are given below for the two received signals

$$Y_D[n] = \sqrt{P_S}\ G_{SD}.\ X[n] + n_{SD}[n] \quad (1)$$

$$Y_R[n] = \sqrt{P_S}\ G_{SR}.\ X[n] + n_{SR}[n] \quad (2)$$

After that, the relay node amplifies the signal received Y_R and then transmits it to the destination node with the amplifier gain β_R. Now, the transmission power of the relay node, P_R. G_{RD} is the channel gain for relay to destination link and the noise at the destination node, n_{RD}. The modified signal received by the destination Y'_R, sent from the relay node is given below:

$$Y'_R[n] = \beta_R\ .\ Y_R[n]\ .\ G_{RD} + n_{RD}[n] \quad (3)$$

Here, the fixed amplifier gain β_R is used to accurately tweak the transmission power at the relay to compensate the variations in the relay to destination communication link. The gain is dependent on the channel between the source and relay node [10]. The amplifier gain of the relaying node can provide a maximum improvement, which is defined by the expression below:

$$\beta_R = \sqrt{\frac{P_R}{P_S|G_{SR}|^2 + N_0}} \quad (4)$$

As, the relaying node running AF protocol may also amplify the induced noise so in the next phase receiver diversity combining technique will be used at the receiver node to mitigate this effect.

B. Reception Phase

In the reception phase, the overall performance of the communication system is increased by effectively combing the multiple copies of the transmitted message at the receiver node. Receiver diversity combining particularly targets small scale fading. Therefore, the simulation has been performed using flat Rayleigh fading channel as it is the easiest one to implement and is manageable. Three different signal combining techniques have been employed in the network. With each technique, the objective is to calculate the weights, which compensate for the negative effects of fading. These combining techniques are different in the way they calculate their weight vectors.

1) Maximum Ratio Combining

In maximal ratio combining, the receiver node will perform maximum ratio combining technique on the two received signals. So, the output of the MRC system at the receiver node will be:

$$Y_{MRC}[n] = \alpha_0(\sqrt{P_S}\ .G_{SD}.\ X[n] + n_{SD}[n]) + \alpha_1(\beta_R\ .\ Y_R[n]\ .\ G_{RD} + n_{RD}[n]) \quad (5)$$

Substituting, equation (2) into (5):

$$Y_{MRC}[n] = \alpha_0(\sqrt{P_S}\ .G_{SD}.\ X[n] + n_{SD}[n]) + \alpha_1(\beta_R.\ (\beta_R\ .\ Y_R[n]\ .\ G_{RD} + n_{RD}[n])\ .\ G_{RD} + n_{RD}[n]) \quad (6)$$

In the above expressions, α_0 and α_1 are the weights of the MRC for the communications links between source-relay and between relay-destination. These weights compensate for the effects of channel impairments and are therefore calculated using the expressions given below:

$$\alpha_0 = \frac{\sqrt{P_S}\, G_{SD}^{\ *}}{N_0} \tag{7}$$

$$\alpha_1 = \frac{\sqrt{P_S}\,.\,\beta_R\,.\,G_{SR}^{\ *}\,.\,G_{RD}^{\ *}}{N_0} \tag{8}$$

2) Advanced SNR Combining

In a traditional signal to noise ratio (SNR) combining technique, the weights are assigned depending on the instantaneous SNR of the communication link, which was used to transmit the signal. The signals coming from the communication link having high SNR will be assigned higher weights and vice versa. In advanced SNR combining instead of taking the instantaneous SNR an estimated factor of SNR is calculated making it a less complex. In this technique, only that signal will be chosen whose SNR is greater than SNR of any other signal by the estimated factor.

$$Y_{ASNRC} = \begin{cases} Y_D[\mathrm{n}] & \frac{\gamma_{SD}}{\gamma_{RD}} > 10 \\ Y_D[\mathrm{n}] + Y_R[\mathrm{n}] & 0.1 < \frac{\gamma_{SD}}{\gamma_{RD}} > 10 \\ Y_R[\mathrm{n}] & \frac{\gamma_{SD}}{\gamma_{RD}} < 0.1 \end{cases} \tag{9}$$

C. Optimization Phase

In this phase, the network configuration will be translated into a convex optimization problem, and the next step will be to find the solution of this optimization problem for calculating the optimal transmission powers for the source and all involved cooperating relay nodes.

The SNR for the source-destination link and for the source-relay-destination links are denoted by Γ_0 and Γ_1 respectively.

Where, $$\Gamma_0 = \frac{\sigma_{SD}^2 . P_S}{N_o} \tag{10}$$

As, the transmission with relay is a multi-hop scenario, the SNR can be calculated by considering it as cascaded single hop transmissions. Therefore, the SNR Γ_1 will be the summation of all individual links.

$$\Gamma_1 = \frac{\sigma_{SD}^2 . P_S}{N_o} + \frac{\sigma_{RD}^2 . P_R}{N_o} \tag{11}$$

The total SNR of the system Γ_T will be:

$$\Gamma_T = \Gamma_0 + \Gamma_1 \tag{12}$$

Substituting equation (10) & (11) into (12):

$$\Gamma_T = \frac{\sigma_{SD}^2 . P_S}{N_o} + \left(\frac{\sigma_{SD}^2 . P_S}{N_o} + \frac{\sigma_{RD}^2 . P_R}{N_o}\right) \tag{13}$$

Here, the bit error probability has been calculated using Moment Generating Function (MGF) approach for QPSK modulation scheme [11]. As, it is known to be an effective tool for performance analysis of any modulation scheme in a fading scenario.

$$P_e = \frac{1}{\pi} \int_0^{(\frac{N-1}{N})\pi} \prod_{n=0}^{1} N_{\gamma_n}\left(\frac{g_{QPSK}}{sin^2\theta}\right) d\theta \tag{14}$$

The moment generating function approach computes the bit error probabilities by defining the error probability as an exponential function of γ.

$$N_{\gamma_n} = \int_0^{\infty} P_{\gamma_n}(\gamma) e^{s\gamma} d\gamma \tag{15}$$

$$N_{\gamma_n}\left(\frac{1}{sin\theta^2}\right) = \left(1 + \frac{g_{QPSK}}{sin^2\theta}\gamma_n\right)^{-1} \tag{16}$$

$$N_{\gamma_n}\left(\frac{1}{sin\theta^2}\right) = \left(1 + \frac{\gamma_n}{sin^2\theta}\right)^{-1} \tag{17}$$

Since $(\gamma_n >> 1)$ equation (17) becomes:

$$N_{\gamma_n}\left(\frac{\gamma_n}{sin\theta^2}\right) \cong N_{\gamma_n}\left(\frac{1}{sin\theta^2}\right)$$

$$P_e = (\gamma_0 . \gamma_1)^{-1} \tag{18}$$

Substituting the values of γ_0 and γ_1 in equation (18):

$$P_e = \left[\frac{P_S . \sigma^2_{SD} . \sigma^2_{SR}}{N_o^2} + \frac{P_S . P_R . \sigma^2_{SD} . \sigma^2_{RD}}{N_o^2}\right]^{-1} \tag{19}$$

$$P_e = N_o^2 \left[\frac{1}{P_S . \sigma^2_{SD} . \sigma^2_{SR}} + \frac{1}{P_S . P_R . \sigma^2_{SD} . \sigma^2_{RD}}\right] \tag{20}$$

Now, as the bit error probability has been formulated for this configuration, the prime objective is to minimize this bit error probability while maintaining the total power constraint [12]. The optimization problem can be expressed as:

$$\text{Minimize } P_e = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \prod_{n=0}^{1} N_{\gamma_n}\left(\frac{1}{sin^2\theta}\right) d\theta \tag{21}$$

$$\text{Subject to } P_s + P_R \leq P_T$$

Since, the most common method for solving a constrained optimization problem is Lagrange method. Therefore, the above constrained optimization problem will be translated into a Lagrange cost function. The Lagrange cost function comprises of an objective function, constrained function and a Lagrange multiplier as expressed below:

$$J = P_e + \lambda (P_s + P_R - P_T) \tag{22}$$

Substituting equation (21) into (22):

$$J = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \prod_{n=0}^{1} N_{\gamma_n}\left(\frac{1}{sin^2\theta}\right) d\theta + \lambda (P_s + P_R - P_T) \tag{23}$$

$$J = N_0^2 \left(\frac{1}{P_S{}^2 \sigma^2_{SD} \sigma^2_{SR}} + \frac{1}{P_S P_R \sigma^2_{SD} \sigma^2_{RD}}\right) + \lambda(P_S + P_R - P_T) \tag{24}$$

The next step is to take the partial derivatives of the Lagrange cost function J (P, λ), with respect to P_s, P_R and λ. After that these equations will be equated to zero:

$$\frac{\partial J}{\partial P_S} = N_0^2 \left[\frac{-2P_S . \sigma^2_{SD} . \sigma^2_{SR}}{(P_S{}^2 . \sigma^2_{SD} . \sigma^2_{SR})^2} - \frac{P_R . \sigma^2_{SD} . \sigma^2_{RD}}{(P_S . P_R . \sigma^2_{SD} . \sigma^2_{RD})^2} \right] + \lambda = 0 \quad (25)$$

$$\frac{\partial J}{\partial P_R} = N_0^2 \left[- \frac{P_S . \sigma^2_{SD} . \sigma^2_{RD}}{(P_S . P_R . \sigma^2_{SD} . \sigma^2_{RD})^2} \right] + \lambda = 0 \quad (26)$$

$$\frac{\partial J}{\partial \lambda} = P_S + P_R - P_T = 0 \quad (27)$$

The above expression will be used to calculate the transmission power values of source and all involved relay nodes.

$$P_S = \frac{\sigma^2_{SR} + \sqrt{A}}{B} P_T \quad (28)$$

$$P_R = \frac{2\sigma_{SR}}{B} P_T \quad (29)$$

Where, in the above equation (28) and equation (29):

$$A = (\sigma^2_{SR} + 8\sigma^2_{RD})$$

$$B = (3\sigma^2_{SR} + \sqrt{A})$$

IV. SIMULATION RESULTS

Figure 2 compares the performance of OPA with that of EPA in terms of ABER for a cooperative network having a single relay node. The results indicate that for any given value of E_b/N_o the performance of the cooperative system employing OPA is better than the system having EPA as its power allocation technique, also proposed by [13].

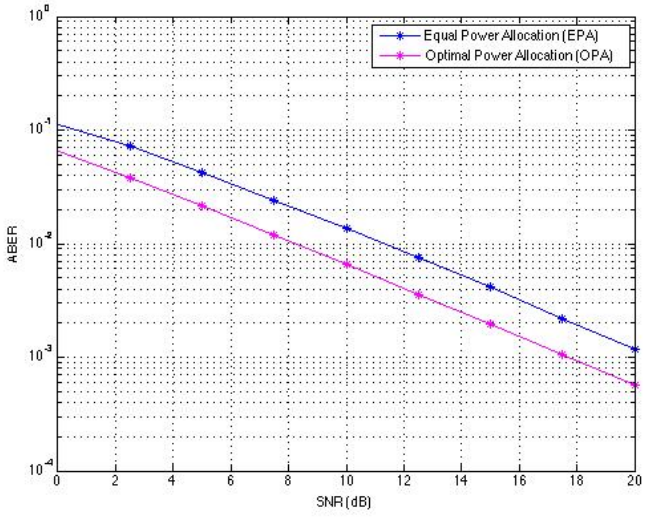


Figure 2. Optimal Power Allocation versus Equal Power Allocation

Table I presents the transmission powers values of the nodes in a 3-node network. These values are calculated using the expressions derived earlier while satisfying the total power constraint of "1". The power values have been calculated for three different scenarios. First, when the relay node is place in between source and destination node. Second, when the relay node is closer to the destination node. Finally, for the scenario when the relay node is closer to source node. It can be seen clearly that the algorithm allocates different power values based on the link quality between the two communicating nodes at a given time.

TABLE I. OPTIMAL POWER VALUES (3-NODE CONFIGURATION)

Link Quality	OPA		EPA	
$\sigma^2_{SD}; \sigma^2_{SR}; \sigma^2_{RD}$	*Source Node*	*Relay Node*	*Source Node*	*Relay Node*
(1, 1, 1)	0.6667	0.3333	0.5	0.5
(1, 1, 10)	0.8187	0.1813	0.5	0.5
(1, 10, 1)	0.5472	0.4528	0.5	0.5

In figure 3, performance comparison of the above mentioned receiver diversity combining techniques is presented. The performance curves show that the traditional diversity technique, i.e, MRC is lacking in performance for each values of SNR. The performance gap between the two receiver diversity schemes increases with the increase in value of SNR, as shown by the lower curve. Along with the visible performance increase, ASNRC also does not require the knowledge of channel state information at the receiver node. This in turn reduces the overall complexity of the communicating node.

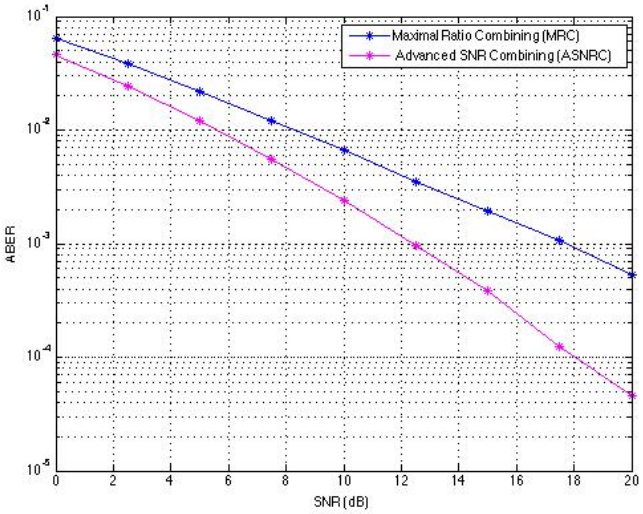


Figure 3. Performance Comparison of MRC and ASNRC

Figure 4, compares the performance of the 3-node cooperative relay system having two different power allocation algorithms and receiver diversity techniques. The first configuration is employing EPA, as its power allocation technique while MRC technique is being used at the receiver node. In the second configuration both of the proposed optimal power allocation and receiver diversity technique are being used. The performance curve of the second configuration outperforms that of the first one for every value of SNR. The performance gaps increases with the increase in the values of SNR.

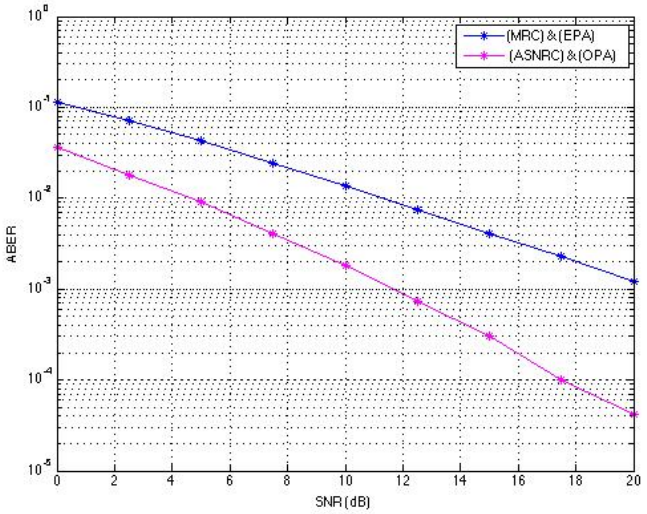


Figure 4. Performance Comparison of Traditional Vs. Proposed Techniques

V. Conclusion

In this paper, we have investigated a cooperative relay network employing advanced power allocation and receiver diversity techniques. First, the expressions for different phases in a cooperative communications were derived. After that the expression for the optimal power allocation and the proposed receiver diversity techniques were derived. The results above show clearly that the system performance is enhanced significantly with the use of these techniques. OPA is an ideal candidate for a cooperative network having un-balanced communication links with nodes placed asymmetrically. Where as, EPA performs only well if the nodes are placed symmetrically. It was also shown that if only a rough estimate about the channel quality is available then more advanced techniques like ASNRC could be employed to increase the performance of the system.

Acknowledgment

The authors would like to thank Vaasa University Foundation for the financial support provided by them and National University of Science and Technology.

References

[1] K. J. Ray Liu and A. K. Sadek, "Cooperative Communications and Networking," Cambridge University Press, 2009.

[2] I. E. Telatar, "Capacity of multiple-antenna Gaussian channels,"*Europ.Trans. Telecommun.,* vol. 10, p. 585, Nov. 1999.

[3] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversityPart I: System description," *IEEE Trans. Commun.*, vol. 51, no. 11, pp.1927–1938, Nov. 2003

[4] J. N. Laneman, G. W. Wornell. "Distributed space-time coded protocols for exploiting cooperative diversity in wireless networks [J],". *IEEE Trans. on Information Theory*, 2003, 49(10).

[5] Youngpil Song; Hyundong Shin; Hong, Een-Kee, "MIMO cooperative diversity with scalar-gain amplify-and-forward relaying," *Communications, IEEE Transactions on* , vol.57, no.7, pp.1932,1938, July 2009

[6] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory,* vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[7] Mulugeta K. Fikadu, Mohammed Elmusrati, and Reino Virrankoski, "Power Allocation in Multi-node Cooperative Network in Rician Fading Channels," *IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* 2012: 496-501.

[8] Khan, M.H.D.; Elmusrati, M.S.; Virrankoski, R., "Optimal power allocation in multi-hop cooperative network using non-regenerative relaying protocol," *Advanced Communication Technology (ICACT), 2014 16th International Conference on* , vol., no., pp.1188,1193, 16-19 Feb. 2014

[9] S. Boyd and L. Vandenberghe, Convex Optimization. Cambridge University Press, 2009.

[10] Diomidis S. M, Zoran H., George K. K. and Robert S, "PAPR of Variable-Gain and Fixed-Gain Amplify and Forward Relaying,". 9th *International Conference on Systems, Communications and Coding* 2013: 1-5.

[11] Ramesh, A.; Chockalingam, A.; Milstein, L.B., "Performance analysis of TCM with generalized selection combining on Rayleigh fading channels," *Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE* , vol.2, no., pp.1403,1407 vol.2, 17-21 Nov. 2002

[12] Rasouli, H.; Anpalagan, A., "SNR-based vs. BER-based power allocation for an amplify-and-forward single-relay wireless system with MRC at destination," *Communications (QBSC), 2010 25th Biennial Symposium on* , vol., no., pp.429,432, 12-14 May 2010

[13] Bin Shen; Rumin Yang; Kyungsup Kwak, "Optimal power allocation schemes for amplify-and-forward relay networks with different levels of channel knowledge," *Communications and Information Technologies (ISCIT)*, 2010 International Symposium on , vol., no., pp.510,513, 26-29 Oct. 2010

VI. Author (s)

Muhammad H. D. Khan (S'13) was born in Rawalpindi, Pakistan, in 1986. He received the B.E. degree in electrical engineering from the COMSATS Institute of Information Technology, Islamabad, Pakistan, in 2010, and the M.Sc. degree in technology from University of Vaasa, Vaasa, Finland, in 2013.In 2010, he joined the Department of Avionics Engineering, Air University, Pakistan, as a Research Assistant, and in 2011 became a Research Associate. His current research interests include wireless communication systems, sensor networks and resource allocation management.

Muhammad D. Khan (S'14) was born in Islamabad, Pakistan, in 1992. He received the B.E. degree from the National University of Science and Technology (NUST), Islamabad, Pakistan, in 2013. In 2013, he joined the Department of Electrical Engineering, NUST, Pakistan, as a Researcher. His current research interests include Communication systems and Signal Processing.

Mohammed Elmusrati (S'00-M'04-SM'12) received the B.Sc. (with honors) and M.Sc. (with high honors) degrees in telecommunication engineering from the Electrical and Electronic Engineering Department, Benghazi University, Libya, in 1991 and 1995, respectively, and the Licentiate of Science in technology (with distinction) and the Doctor of Science in Technology degrees in control engineering from Aalto University - Finland, in 2002 and 2004, respectively. Currently, Elmusrati is full professor and head of communications and systems engineering group at University of Vaasa - Finland. His main research interests include Radio resource management in wireless communication, wireless networked control, game theory, and smart grids.

Enhancing the Implementation of Cloud-Based Open Learning with E-Learning Personalization

Nungki Selviandro[1,2], Mira Suryani[2], Zainal A. Hasibuan[2]

[1]Faculty of Informatics Telkom University, Indonesia

[2]Faculty of Computer Science University of Indonesia, Indonesia

nselviandro@telkomuniversity.ac.id, mira.suryani@ui.ac.id, zhasibua@cs.ui.ac.id

***Abstract* — Indonesia is a developing country that began to utilize information technology in education. A form of its implementation is the use of e-learning. However, in practice there are still some obstacles, such as learning resources are not evenly distributed, limited access to services provided, qualified educators resources are concentrated in specific areas. This led to the emergence of disparities educational process, and technology gap due to differences in ICT infrastructure owned by any educational institution.**

Therefore this study proposes architecture of cloud-based open learning to solve these problems. The term open learning is used in order to encouraging the development of the concept of Indonesia Open Educational Resources (IOER) and as well as the adoption of concept of cloud computing. There are several phase that we conducted in this research such as analysis, design, implementation, testing, and evaluation phase. The design of the proposed architecture consists of six layers: (1) Infrastructure, (2) Platform, (3) Application, (4) Service, (5) Access, (6) User. As a result of the implementation from this architecture is a prototype of Indonesia - Virtual Open Learning System (iVOLS).

In experiment, personalization e-learning runs as a service that need large storage and other shared facilities to conduct the program so the system can delivered different learning materials to different learners. The e-learning personalization in cloud environment classified successful if the learners got the best performance on learning and it shown by their evaluation score. Based on the test results and evaluation showed that the availability on Cloud-Based Open Learning further meet user needs. This is indicated by the presence of a simple infrastructure services, application services with just one stage and the availability of a wider range of data and the resource sharing. In accessibility, Cloud-Based Open Learning provides easy access to the user. By economically, the result of evaluation showed that Cloud-Based Open Learning has an investment of 35.61% efficiency, increase Return On Investment (ROI) of 60.95% and Net Present Value (NPV) of 81.97% from the user's perspective. While from the provider's perspective, Cloud-Based Open Learning has an investment of 200% efficiency, increase Return On Investment (RoI) of 220.4% and Net Present Value (NPV) of 109.55%.

***Keyword* — Cloud Computing, E-Learning, Indonesia Open Educational Resources, Personalization.**

I. INTRODUCTION

E-LEARNING provides many benefits such as flexibility, diversity, measurement, and others [1], even though its implementation still exist many difficulties. The main problem experienced when to start applying e-learning is the high initial cost or in other words is the economic factor [2]. It is becoming a major focus for the institutions that will implement e-learning. The initial cost consists of three main problems: (1) Infrastructure; (2) Human Resources; (3) Maintenance. Another problem might occured when implementing e-learning is access to the learning material. This problem experienced in Indonesia as a country with thousands of islands.

Along with the development of the IT world, cloud computing is gradually become the new paradigm of innovation in the IT world, cloud computing is a computing services that can be used through the Internet in accordance with the needs of users with little interaction between service providers and users. Cloud computing technology as well described as a computing resource that provides a highly scalable as external services through the Internet. Therefore, cloud computing can be considered as an alternative to minimize the cost of infrastructure and human resources for development and maintenance process of e-learning systems [3].

In this paper the author will discussed previous cloud learning architecture and the basic concept of open educational resources. The proposed open learning architecture also will be described in Chapter 4. Further more in this paper also will discuss the approach of the implementation, experiment in personalization learning, and the evaluation. For final chapter author will described the conclusions and discussed the future works of this study.

II. CLOUD COMPUTING

Cloud Computing is a new paradigm to organize and manage ICT resources. There are various definitions of cloud computing, one of which is the definition according to The National Institute of Standards and Technology (NIST) which defines cloud computing as "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly

Manuscript received May 19th, 2014. This work was supported by Faculty of Computer Science University of Indonesia.

N. Selviandro is with the Faculty of Computer Science University of Indonesia. (corresponding author to provide phone: +62856 9720 4002; e-mail: selviandro@yahoo.co.uk).

M. Suryani is with the Faculty of Computer Science University of Indonesia. (e-mail: mira.suryani@ui.ac.id).

Z. A. Hasibuan is with the Faculty of Computer Science University of Indonesia. (e-mail: zhasibua@cs.ui.ac.id).

provisioned and released with minimal management effort or service provider interaction" [22]. Generally speaking, the cloud computing service model consists of three layers [5], among others: (1) Software as a Service (SaaS); (2) Platform as a service (PaaS); (3) Infrastructure as a service (IaaS) [6].

In practice, cloud computing has four implementation models where each model has certain characteristics [7], among others: (1) Private, the model is aimed at an organization where cloud operations are managed by a third party or the organization itself; (2) Public, service on this model is intended for the general public or the industry in which the various services provided by the cloud computing service provider organization (3) Community, this model is managed by several organizations that form a community of practice in which the operations are managed by the community with the division of tasks particular; (4) Hybrid, this model is a combination of various models existing cloud distribution. Typically, this is done with a combination of specific purposes where there is an attachment for example: technological standards and data ownership.

III. Conventional E-Learning Towards Cloud-Based E-Learning

Based on Carroll et al [9] the main advantage of the adoption of cloud computing is the efficiency to manage the cost that user will spend for the services. This is an interesting point of view that with this advantage we could adopt cloud concept in terms of implementation in e-learning. Conventional e-learning commonly used by the university developed by the university itself tend to cause lots of problems such as time to designing e-learning systems will be developed, costs for infrastructure, selecting commercial or open source e-learning platform, the cost to hire professional staff to maintain and upgrade the system of e-learning, and so on. This process is more likely need more time [7].

The implementation of e-learning based on cloud possibly could help educational institutions to use a single e-learning service that running on cloud environment. This model can reduce the initial costs incurred by the institution for the implementation of e-learning by using cloud computing services, because institutions do not need to pay for the purchase of infrastructure, both in terms of procurement of servers and storage. By the adoption of cloud computing, the educational institution can rent the infrastructure of the cloud computing providers [10]. Likewise with the human resources for the development stage, the cloud environment of e-learning has been provided by the cloud service provider, as well as maintenance of the e-learning [11].

Figure 1 illustrated the conventional e-learning implementation and Figure 2 illustrated the cloud-based e-learning implementation. From both of these pictures explain the paradigm shift in the implementation of e-learning, shifting from conventional e-learning implementation to cloud-based e-learning implementation. By using this approach might help educational institution in implementing e-learning with less cost. Generally, the implementation of conventional e-learning consists of some basic element such as e-learning system development,

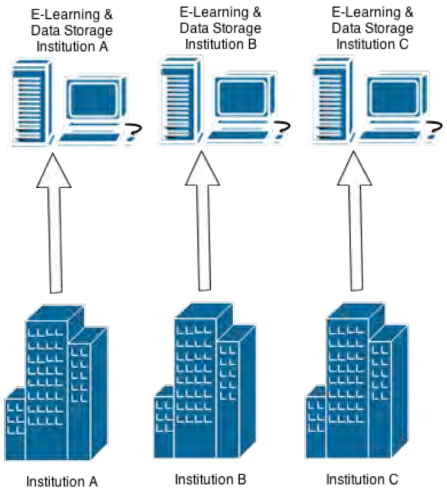


Fig. 1. Conventional E-Learning

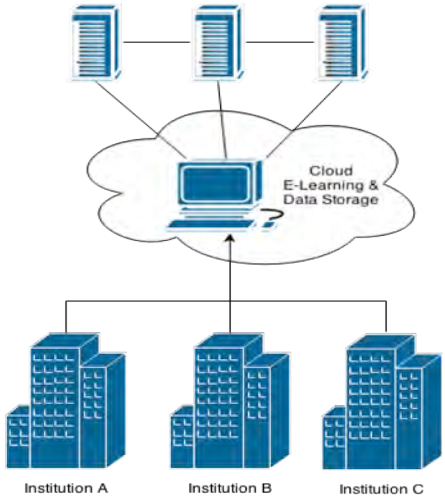


Fig. 2. Cloud-Based E-Learning

system upgrade, and system maintenance [12]. It had a lot of problems, both in terms of flexibility, scalability, and accessibility [13]. According to [14] one of the main important features that can be presented in the use of e-learning in the cloud is scalability, which allows virtualization provide infrastructure layer provided by the cloud service provider. Virtualization helps solve the problem of the physical barriers that are generally inherent in the lack of resources and infrastructure to automate the management of these resources as if they were a single entity through hypervisor technologies such as virtual machine (VM).

IV. Open Educational Resources

Open Educational Resources (OER) initiative is an initiative that enables to share all educational resources to public domain with open access, open license, open format, and open system. This OER implementation can be seen in many countries in the world like MIT Open Courseware, China Open Resource for Education, or Paris OCW Project.

Many educational resource sharing system implementations have been developed all over the world with many different techniques. Web service architecture

more often used in the recent past year. This implementation uses web service as an integration, retrieval and data exchange application [6]. The newer trend that is often used today is the semantic web technology where the resources were formed in the semantic description [7]. Other researchers also are using P2P technology combined with semantic web technologies and formed a super-peer P2P semantic grid where the semantic metadata retrieved from many educational sources [8].

V. Cloud-Based Open Learning Architecture

There are several architectural cloud-based e-learning have been proposed by previous researcher. In this paper will discuss three architectural cloud-based e-learning, such as architecture proposed by [4], [1], and [5].

In [4] they proposed e-learning architecture based on cloud computing that consists of three layers that are infrastructure, platform, and application layer. They explained that infrastructure layer is a hardware layer that supplies the computing and storage capacity for the higher level and this layer, which is used as e-learning and software virtualization technologies, ensures the stability and reliability of the infrastructure. The second layer is Platform layer, which is a middle layer consisting middleware that is Web service they use here. It purpose is for providing the learning resources as a service. This layer consists of two modules, the first module is Item Classification Module (ICM) and the second module is Course Selection Module (CSM). Main jobs both of these modules are focusing on accessing the items from the item bank and selecting suitable learning content from the content database. The last is the third layer they called it as a Application layer which is responsible for interface provision for the students.

The next architecture proposed by [1]. Their proposed architecture consists of five layers. The First layer is infrastructure layer. It is composed of information infrastructure and teaching resources. Information infrastructure contains internet/intranet, system software, information management system and some common hardware. Teaching re-sources stored up mainly in traditional teaching model and distributed in different departments and domain. The second layer is software resource layer. This layer is composed by operating system and middleware. A variety of software resources are integrated through middleware technology to provide a unified interface for software developers to develop applications and embed them in the cloud. The third layer is resource management layer. In order to effectuate on demand free flow and distribution of software over various hardware resources, this layer utilizes integration of virtualization and cloud computing scheduling strategy. The fourth layer is service layer. This layer has three levels of services namely, SaaS, PaaS, and IaaS. In SaaS, cloud computing service is provided to customers, contrasting to traditional software, cloud customers use software via the internet without any need to purchase, maintain, and upgrade, so they only pay a monthly fee for rent the cloud services that used by the customer. The last layer is application layer. This layer is a specific layer consisting of applications of integrated teaching re-sources, including interactive courses and the teaching resources sharing. The teaching resources include teaching material, teaching information, as well as the full sharing human resources.

The last architectures that we referred in this study is from [5]. They proposed architecture of e-learning-based on cloud computing consists of three layers, namely: (1) infrastructure layer, (2) middleware layer, and, (3) application layer. The first layer is infrastructure layer. It is employed as the e-learning resource pool that consists of hardware and software virtualization technologies to ensure the stability and reliability of the infrastructure. This layer also supplies the computing and storage capacity for the higher level. The second layer is middleware layer. It focuses in providing a sharable platform. The final layer is application layer. At this layer, cloud computing provides convenient access to the e-learning resources.

In this study we propose the architecture that we have designed by modifying previous architectures that we used as references. Our proposed architecture depicted in Figure 3 consists of six layers, namely: (1) infrastructure layer; (2) platform layer; (3) application layer; (4) service layer (5) access layer; and (6) user layer.

We have modified the user layer. Our user layer consists of all stakeholders that might involve to the system. We also add two more layers which is Access layer which is consist of multi-channel access from multi devices for addressing the access issue for Indonesian local context and service layer that describes the services that provided by the system, which is: e-learning as a service, data as a service, and infrastructure as a service.

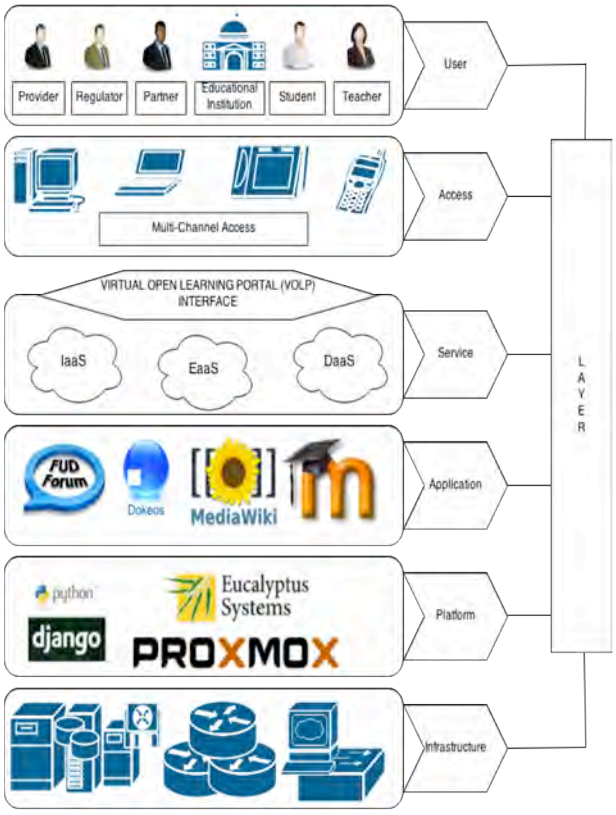


Fig. 3. Cloud-Based Open Learning Architecture

VI. Implementation

Cloud environment developed using Proxmox platform. Table 1 Describes the Hardware and software specification for the environment.

TABLE I
HARDWARE SPECIFICATIONS

Hardware	Proxmox Minimum	Current Hardware	Remark
CPU	64 bit	64 bit	Fulfilled
Memory	1 GB RAM	2 GB RAM	Fulfilled
Hard Drive	Hard Drive	Hard Drive	Fulfilled
Network	1 NIC	1 NIC	Fulfilled

Main activity in this process is developing a working prototype portal. Authors used Java Script and PHP programming language to develop the portal. This portal will be the gate for the users to use their e-learning system and the portal illustrated in Figure 4.

This portal main service called as a E-Learning as a Service. The objective is to provide a e-learning system for the users. This service will provide three possible cases, which is: (1) Enable users to request a e-learning system for users who do not have an e-learning system and create a new one for educational purpose only; (2) Enable users to enroll to existing e-learning system for users who do not have an e-learning system or institution; (3) Enable users to migrate their e-learning system to join the e-learning based on cloud environment for users who already have an e-learning system and willing to entrust the maintenance duty to cloud provider.

Two another services that provided by this portal are data and infrastructure services. By joining open learning portal users automatically rewards by free data storage and cloud based infrastructure. Data services consist of multimedia data that uploaded by another users and every user could store and share their data with another users.

Infrastructure service will be provided to the users by using virtual machine. Virtualization helps solve the problem of the physical barriers that are generally inherent in the lack of resources and infrastructure to automate the management of these resources as if they were a single entity through hypervisor technologies such as virtual machine (VM).

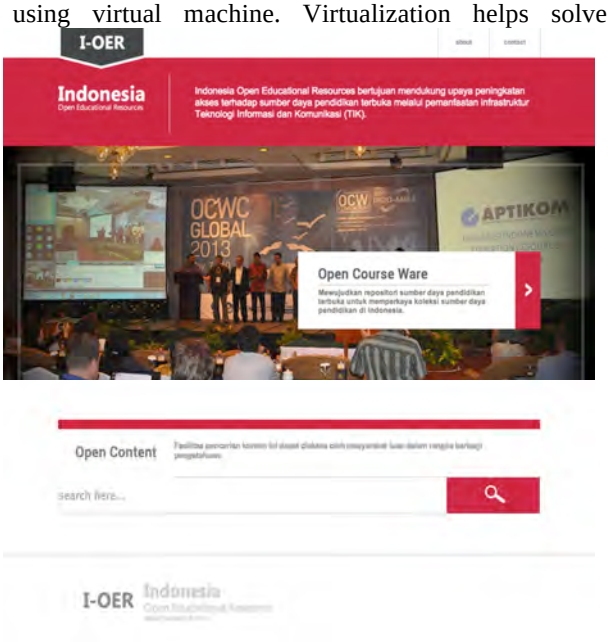


Fig. 4. Prototype of Open Learning Portal

One of the services that run in Open Learning Portal is *"Student-Centered E-learning Environment - Personalization Dynamic E-learning"* or usually called as SCELE-PDE. This service is an e-learning that built from modified Moodle LMS so the system can provide personalization based on triple-factor model concept. The learners that registered use the e-learning to improve their performance in learning. They learn the materials that be given by teachers in the way they like. The e-learning recorded learner's activity such as access to learning material and involved in forums. The learner's activity determined learning behavior patterns of the learner. Learning behavior patterns filled the triple-factor parameter that consists of learning style category, level of motivation, and knowledge ability.

Learning style of the learner determined level of learning material that suitable with the learner preferences. Based on [8], learning style of learner calculated based on mean in frequent table of the group as a threshold. Learning style divide into 3 categories, they are seldom access category for number of access learning materials below the threshold, discipline category for number of access equal with the range of threshold, and diligent access category for number of access greater or equal than the threshold.

Level of motivation determined which forum activity that should be improved by the learner. Level of motivation calculated from mean of activities in frequent table of group as threshold and divide into 3 categories, they are low, medium, and high motivation. Low motivation category gives to learner with number of access to forum discussions is below than the threshold. Medium motivation category gives to learner with number of access to forum discussion equal with the range of threshold. High motivation category gives to learner with number of access to forum discussion is greater than the threshold.

Knowledge ability determined the performance of the learner after they use the e-learning. Knowledge ability calculated based on evaluation score of users. Knowledge ability divide into 4 categories, they are fail for interval score 0-60, fair category for interval score 61-80, good category for interval score 81-90, and very good category for interval score 91-100. The outcomes of the personalization are suitable learning contents for every learner that registered in the system. The architecture of the personalization e-learning illustrated in Figure 5.

In order to improve their performance, level of learning material has been proposed. Level of learning materials that delivered to learner consists of three level, they are LV1 is short material (M), LV2 are short and explanation material (M+P) and, LV3 is short, explanation, and additional material (M+P+T). Short materials delivered in slide form. Explanation materials delivered in audio, video, and multimedia form such as slide-audio mixing and video-slide mixing. Additional materials delivered in link, example, and other references form. Many form of learning materials need large repository and cloud environment used as a solution to

store and delivered it. In the experiment, there are 118 learners that registered in Science Writing subject during a semester. In the subject there are 40 learning materials with different format and size that have been delivered. The composition of learning materials describe in Table 2.

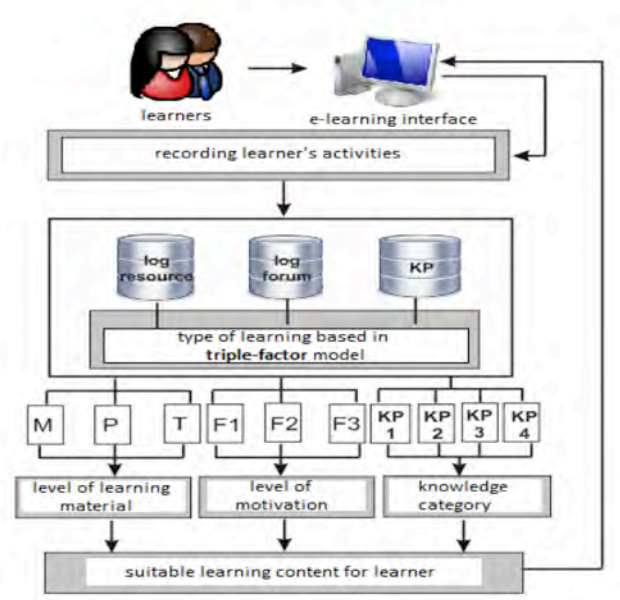


Fig. 5. Architecture of Personalization Learning Content in E-learning

When learner login into personalization e-learning, the system will record the activities. In experiment, learning process with e-learning divided into 2 step. Step 1 is identification step and Step 2 is personalization step. The step 1 held from week 1 unttill 7. The learner used e-learning without personalization and learning content delivered in many form but in limited amount. Based on step 1, learning activities that have been recorded describe in Table 3 and the scenario of personalization learning illustrated in Figure 6.

TABLE II
LEARNING CONTENT THAT DELIVER IN EACH WEEK IN INDENTIFICATION STEP

Week	Topic	slide	audio	forum	animation	video	trigger	reference	outline	assignment	feedback
1	What is scientific writing	x	x	x	-	-	-	x	-	-	-
2	Fundamental concept of reserach	x	-	x	x	-	-	-	x	-	x
3	Scientifi Inquiry and Logical Thinking	x	x	x	-	x	x	-	-	x	-
4	Writing and developing paragraph	x	x	x	-	x	x	x	-	x	-
5	Problem Identification & Hypothesis	x	x	x	-	x	-	x	-	-	-
6	How to Review Literature	x	x	x	x	x	-	x	-	-	-
7	Quantitative Analysis	x	x	x	-	x	-	x	-	-	x
8	Quanlitative Analysis	x	-	-	-	-	-	x	-	-	-
9	Writing Research Proposal	x	x	x	-	-	-	-	-	x	-
10	Plagiarsm & Bibliography	x	-	-	-	-	-	x	-	-	-

There are so many activities in a week. Both of activities need a large storage. Based on experiment, number of activities will increase equally with number of users and learning materials. Cloud environment as a service gives the facilities to enjoy the learner when they use personalization e-learning.

In order to improve performance of learners when use personalization e-learning in cloud environment, relation between level of learning materials and knowledge ability of learners has been observed. The relation in step 1 will be compared with the relation in step 2. Tabel IV shows the distribution of learners about relation between level of learning materials and knowledge ability in identification step.

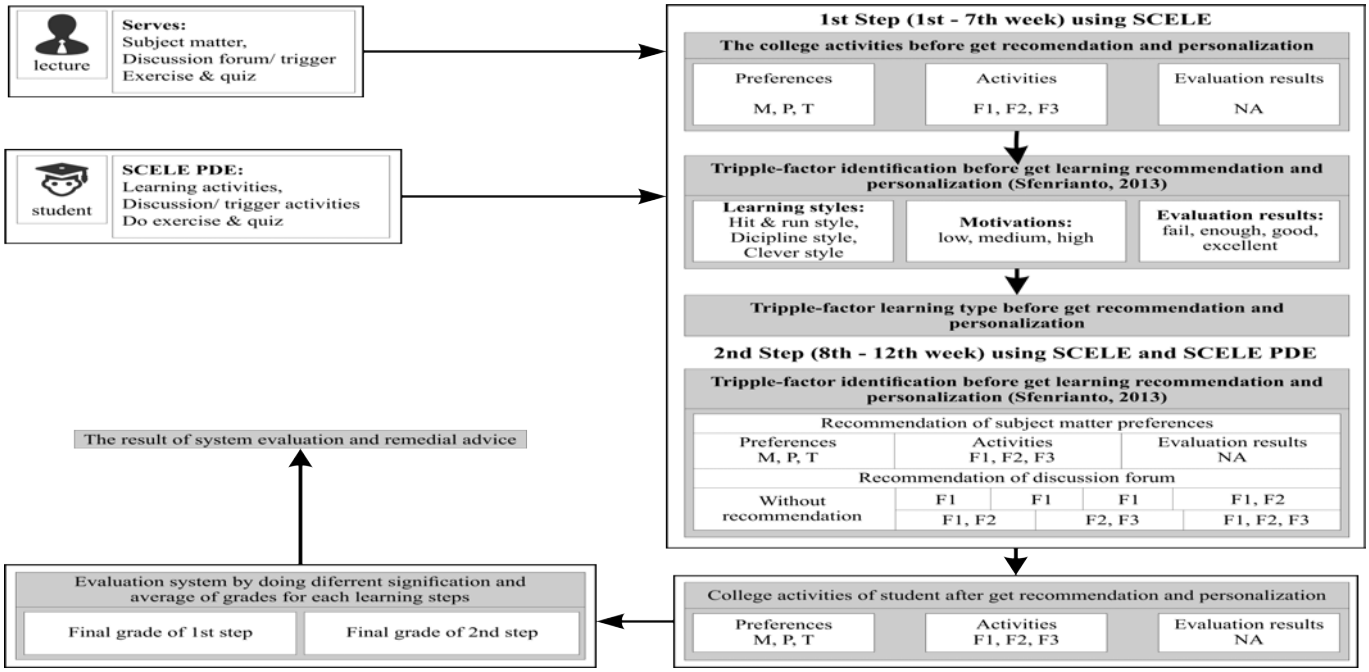


TABLE III
LEARNING ACTIVITES IN IDENTIFICATION STEP

Week	Amount of access to learning materials	Amount of access to forum discussions	Evaluation Score			
			Fail	Fair	Good	Very Good
1	451	1162				
2	236	118				
3	372	197				
4	219	477	6	55	53	4
5	247	-				
6	268	409				
7	-	441				
Sum	**1793**	**2804**	**118**			

TABLE IV
DISTRIBUTION OF LEVEL OF LEARNING MATERIALS AND KNOWLEDGE ABILITY IN IDENTIFICATION STEP

	LV1 (M)	LV2 (M+P)	LV3 (M+P+T)	Sum
Fail (0-60)	4	1	1	6
Fair (61-80)	43	4	9	56
Good (81-90)	46	0	6	52
Very Good (91-100)	2	1	1	4
Sum	**95**	**6**	**17**	**118**

Based on the table IV, the distribution of learners focus on LV 1. There are 6 learners which belong to fail category, 4 of them are in LV1 who only access short learning material but fail to gain more information because lack of knowledge ability. In fair category there are 43 learners that only access short material and gain enough information. The others in this category distributed to different level of learning materials but in small number. In good category, 46 learners have preference to access short learning materials too. They have higher knowledge ability than the category before, so their evaluation score belong to interval 81-90. In very good category there are only 4 learners, 2 learners belong to LV1 and the others belong to LV2 dan LV3.

The experiment continues to step 2 or personalization step. Based on preferences and calculation of means from frequent table of access learning materials, the personalization of learning materials delivered to learners. The step 2 held from week 8th until week 12th. The learner used personalization e-learning and got more different form and size of learning materials. 40 learning materials delivered in the system got the feedback such as number of access and other learning activities. Number of learning activities in learning step 2 describe in tabel V.

TABLE V
LEARNING ACTIVITES IN PERSONALIZATION STEP

Week	Amount of access to learning materials	Amount of access to forum discussions	Evaluation Score			
			Fail	Fair	Good	Very Good
8	221	564				
9	554	344				
10	252	609	4	45	61	8
11	728	1113				
12	380	1301				
Sum	**2135**	**3931**	**118**			

Table V shown that learning activities in personalization step increased more than learning activities in identification step. Number of access to learning materials increased from 1793 to 2135 activities and number of access to forum discussions increased from 2804 to 3931 activities. It shown that personalization e-learning is able to improve learner's participation when they learnt because system deliver type of learning materials that suitable with the learner's need. So the learners will be focused on their exploration to get the information when they learn.

In personalization step, distribution of learners in relation between level of learning materials and knowledge ability was observed and describe in table VI below.

TABLE VI
DISTRIBUTION OF LEVEL OF LEARNING MATERIALS AND KNOWLEDGE ABILITY IN PERSONALIZATION STEP

	LV1 (M)	LV2 (M+P)	LV3 (M+P+T)	Sum
Fail (0-60)	1	0	3	**4**
Fair (61-80)	26	5	14	**45**
Good (81-90)	27	5	29	**61**
Very Good (91-100)	5	1	2	**8**
Sum	**59**	**11**	**48**	**118**

Tabel VI shown that learners in fail category decreased into 4 learners. 45 learners in fair category distributed to LV1, LV2, and LV3 in 26, 5, and 14 respectively. In good category, there are 61 learners. This number increase from 52 in identification step. The last category is very good that increased from 4 to 8.

In addition, this study also observed the activities of learners in discussion forums The main purpose of the activity observed in the discussion forums are to be used as a benchmark for determining the level of motivation of the learner. The discussion forum is divided into three categories of discussion include: lounge F1), self add post (F2), and trigger forum (F3). The observation is divided into two Steps: Step 1 is identification and Step 2 is personalization (see Figure 5). In Step 1, the lounge (F1) is a forum with the highest activity, there is about 2,567 (91.55%) of the 2,804 discussion activities for 7 weeks. Activity on trigger forum there are only 153 (5.45%) of the overall activity in the existing forums. Then for the self add post activity is the lowest activity with only 84 events (2.99%) of the total 2.804 activities. The Observation result of discussion forum activity in step 1 can be seen in Figure 7 below.

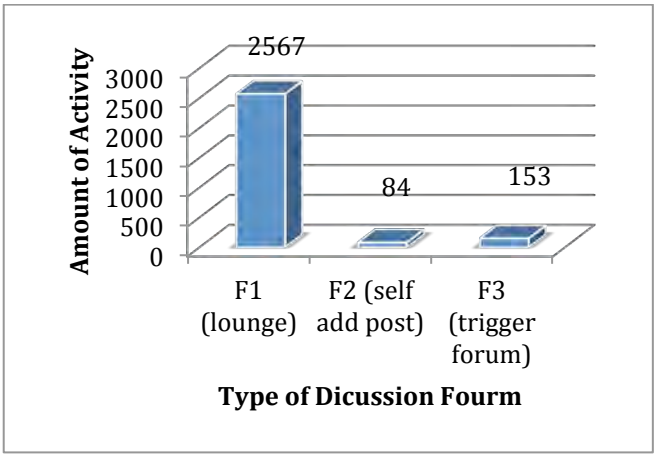


Fig 7. Learner's Discussion Activities in Step 1 : Identification

Then, the special treatment given to all learners who still have low activity discussion forums through the suggestions given in the e-learning during step 2 of personalization. At the end of step 2, the observation of the activity in discussion forums carried back. The comparisons between the activity of step 1 and step 2 in learning activity conducted to determine the increased activity of learner discussion. The observation is illustrated in the Figure 8 as follows.

In step 2, there are 3,237 activities in a public forum (F1). This represents an increase of step 1 which only 2,567 learning activities. In self add post (F2), a very high amount of increased activity at the step 2 where there are 1,401 compared with step 1 with only 84. In the triggers forum, the activity also increased from the previous 153 to 193 activities. This increased activity is assumed to be caused by given recommendations.

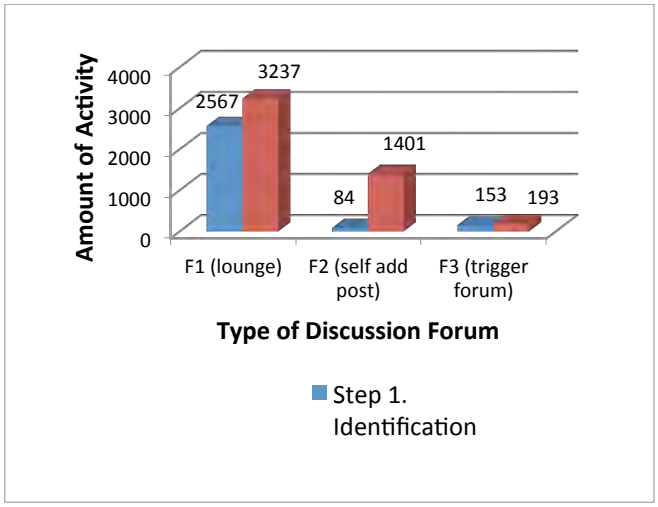


Fig 8. The Comparison about Discussion Forum Activity in Step 1 and Step 2 of Learning Activities

In general, personalization e-learning success to improve performance of the learners. Many learners moved from low category to higher category in knowledge ability, dicussion activity, and get the higher score. It can be happened because in environment level, personalization e-learning runs in cloud computing environment which can provide wide access to broad storage of learning materials, facilities, and others services that support personalization.

VII. Evaluation

The evaluation process for technical system will be used functional testing method. The system will be tested by input scenario and the output will be recorded and matched by the expected output. This scenario aimed to tested that the system will be running properly.

After making sure that the system has running properly by evaluated the functional system, the next evaluation process is concerning to economical aspect. Authors approach for this evaluation is by comparing two cases: non-cloud e-learning and cloud e-learning. This two cases will be evaluated by two approach: (1) Cost (Capex & Opex) analysis; (2) Net Present Value (NPV).

Cost anaylsis is measured by calculating sum of Capex and Opex between non-cloud and cloud open learning then the result will conclude the cost efficiency. The formula for calculating cost analysis (for NC stands for Non Cloud-Based system and C stands for Cloud-Based system could be describes as follows :

$$Cost\ Analysis\ (\%) = \frac{\sum NC_{expense} - \sum C_{expense}}{\sum NC_{expense}} \quad (1)$$

The simulation process with this approach conclude that by using cloud-based system could decrease the investation cost up to 35.61%.

Net Present Value (NPV) is measured by calculating the the difference between the present value of cash inflows and the present value of cash outflows. In this case NPV non cloud based formula could be describes as follows [6]:

$$NPVnc = -CaPex + \sum_{t=0}^{N} \left(\frac{C_t - OpEx}{(1+r)^t}\right) \quad (2)$$

and NPV for cloud based formula described as follows:

$$NPVc = \sum_{t=0}^{N} \left(\frac{C_t - OpEx}{(1+r)^t}\right) \quad (3)$$

The simulation process needs several assumptions such as salary of programmer, analyst, and server procurement cost. Furthermore, the result by calculating the NPV approach shows that the value of NPV is positive (greater than 0) by using NPV percentage formula :

$$NPV\ Percentage = \frac{NPVc - NPVnc}{NPVnc} x\ 100\% \quad (4)$$

with the results shows positive value (43,9%) of NPV that means by using cloud based system could give more benefits than using non cloud based system.

VIII. Conclusions and Future Works

This paper discussed the problems while developing and implementing the e-learning system stressing the initial cost issue. Authors proposed a solution for these problems by adopting cloud technology and the concept of open educational resources to implement the e-learning and expected become a cloud based open learning system.

Authors steps for solved the initial cost problem are designing a architecture of cloud based open learning and implementing this architechture to a working prototype system. Final step is evaluating the prototype system by stressing the initial cost using the Net Present Value method.

The results of the evaluation shows that by implementing the cloud based open learning portal could decrease the infestations cost up to 59% in compares to non cloud e-learning systems and with NPV approach shows that the results is 43,9% of NPV percentage that means by using

cloud based system could give more benefits than using non cloud based system.

In our future work, we will design and develop a semantic based search engine for enhanced the system and integration it with personalization e-learning.

ACKNOWLEDGMENT

Authors wish to thank to Dr. Ismail Khalil from Johannes Keppler University, Austria, for his positive comments and suggestions that improve this article.

REFERENCES

[1] Masud, Md.A.H., & Xiaodi Huang. “An E-learning System Architecture based on Cloud Computing”. IEEE. 2012.
[2] Chuang, S., Chang, K., & Sung, T. “The Cost Effective Structure For Designing Hybrid Cloud Based Enterprise E-Learning Platform”. IEEE CCIS. 2011.
[3] Chandran, D., & Kempegowda, S. “Hybrid E-Learning Platform Based On Cloud Architecture Model: A Proposal”. IEEE. 2010.
[4] Phankokkruad, Manop. “Implement of Cloud Computing For E-Learning System”. IEEE ICCIS. 2012.
[5] Wang, Chun-Chia, Wen-Chang Pai and Neil Y. Yen. "A Sharable e-learning Platform Based on Cloud Computing." 3rd International Conference on Computer Research and Development (ICCRD). Shanghai, 2011. 1 - 5 .
[6] Yang, Z. “Study on an Interoperable Cloud framework for e-Education”. International Conference on E -Business and E -Government (ICEE) (pp. 1 - 4). China: IEEE. 2011.
[7] Selviandro, Nungki, Zainal A. Hasibuan, "Cloud-Based E-Learning: A Proposed Model and Benefits by Using E-Learning Based on Cloud Computing for Educational Institution", ICT-EurAsia, Springer, pp192-201 2013.
[8] Sfenrianto, N. Selviandro, Z. A. Hasibuan, H. Suhartanto, “An Approach for Learning Type Triple Factor In E-learning Process.”, Journal of Next Generation Information Technology. 2013.
[9] Carroll, M., Merwe, A., & Kotzé, P. Secure Cloud Computing Benefits, Risks and Controls. IEEE. 2011.
[10] Ghazizadeh, Aida. Cloud Computing Benefits And Architecture In E-Learning. IEEE. 2012.
[11] Pocatilu, Paul. *Cloud Computing Benefits for E-learning Solutions*. Academy of Economic Studies, Bucharest, Romania. 2010.
[12] Méndez, J. A., & González, E. J. Implementing Motivational Features in Reactive Blended Learning: Application to an Introductory Control Engineering Course. IEEE. 2011.
[13] Masud, Md.A.H., & Xiaodi Huang. An E-learning System Architecture based on Cloud Computing. IEEE. 2012.
[14] Jones, M. Tim. *Cloud computing and storage with OpenStack: Discover the benefits of using the open source OpenStack IaaS cloud platform*. Developer Works. 2012.

Nungki Selviandro was born in Curup, Indonesia in 1988. He received bachelor’s degree in Computer Science from University of Indonesia, Indonesia, 2011, and master's degree also in computer science from University of Indonesia, Indonesia, 2013. Currently, he is a lecturer at Faculty of Informatics Telkom University. His research interests include cloud computing, e-Learning, information system, and software engineering.

Mira Suryani was born in Bandung, Indonesia in 1989. She received bachelor degree in Computer Science Education from Education University of Indonesia, Indonesia, 2011, and master's degree in Computer Science from University of Indonesia, Indonesia, 2014. Currently, she is a research assistant in research laboratory at Faculty of Computer Science, University of Indonesia. Her research interests include digital library, e-learning, information system, information retrieval, and software engineering.

Prof. Zainal A. Hasibuan, Ph.D. was born in Pekan Baru, Indonesia in 1959. He received BSc. degree in Statistic from Bogor Institute of Agriculture, Indonesia, 1986, MSc. and PhD in Information Science, Indiana University, in 1989 and 1995 respectively. Currently, he is a lecturer and PhD supervisor at Faculty of Computer Science, University of Indonesia. He is also the Head of Digital Library and Distance Learning. His research interests include e-Learning, Digital Library, Information Retrieval, Information System, and Software Engineering.

An Efficient and Scalable Key Management Mechanism for Wireless Sensor Networks

Walid Abdallah*, Noureddine Boudriga*, Daehee Kim**, and Sunshin An**
(*)Communication Networks and Security research Lab, University of Carthage, Tunisia;
(**) Computer Network research Lab, Department of Electronics Engineering, Korea University, Seoul, Korea
ab.walid@gmail.com, noure.boudriga2@gmail.com, dhkim@dsys.korea.ac.kr, sunshin@dsys.korea.ac.kr

***Abstract*—A major issue in many applications of Wireless Sensor Networks (WSNs) is ensuring security. Particularly, in military applications, sensors are usually deployed in hostile areas where they can be easily captured and operated by an adversary. Most of security attacks in WSNs are due to the lack of security guaranties in terms of authentication, integrity, and confidentiality. These services are often provided using cryptographic primitives where sensor nodes need to agree on a set of secret keys. Current key distribution schemes are not fully adapted to the tiny, low-cost, and fragile nature of sensors that are equipped with limited computation capability, reduced memory size, and battery-based power supply. This paper investigates the design of an efficient key distribution and management scheme for wireless sensor networks. The proposed scheme can ensure the generation and distribution of different encryption keys intended to secure individual and group communications. This is performed based on elliptic curve public key encryption using Diffie-Hellman like key exchange that is applied at different levels of the network topology. In addition, a re-keying procedure is performed using secret sharing techniques. This scheme is more efficient and less complex than existing approaches, due to the reduced number of messages and the less processing overhead required to accomplish key exchange. Furthermore, few number of encryption keys with reduced sizes are managed in sensor nodes, which optimizes memory usage and enhances scalability to large size networks.**

***Index Terms*—Wireless sensor networks, Security, Key distribution and management, Elliptic curve cryptography, threshold secret sharing**

I. Introduction

Since their advent, Wireless Sensor Networks (WSNs), have been the subject of an increasing interest from the academic and industrial communities, due to their wide and varied number of applications in military and civilian domains. These networks demonstrated high effectiveness in the development of many innovative applications such as battlefield surveillance, border control, structural health monitoring of aircraft, environment parameters measurement, and patient health care[1], [2], [3].

Conceptually, a WSN is composed of a number of sensor nodes, deployed in a specific zone to detect particular events and transmit messages to a base station (sink node) in a multi-hop communication fashion using the wireless medium. Sensor nodes are characterized by their reduced size, limited processing capability, and battery-based power supply. These characteristics must be taken into consideration in developing appropriate communication protocols. Particularly, ensuring communication security is one of the major issues in WSNs, especially when they are distributed in hostile regions where sensors can be captured and easily manipulated by an adversary. Furthermore, with advances achieved in wireless technology, WSNs are being used in critical domains, such as controlling aircraft and avionic systems, surveying health states, and monitoring toxic gas emission where security attacks can have very dangerous consequences on human safety. Therefore, providing security services for data communication in WSNs becomes a main requirement to avoid malicious activities and even terrorist attacks.

Typically, to ensure communication security, at least four services must be provided, namely, confidentiality, authentication, integrity, and availability. Most of these services are based on the implementation of cryptographic techniques which require the establishment of a set of shared encryption keys. A wide range of cryptographic algorithms and schemes had been developed to enable dynamic key distribution and management in classical networking infrastructure, such as asymmetric encryption techniques, digital signature schemes, and Public Key Infrastructure (PKI). However, these techniques cannot be directly used in WSNs. Indeed, sensor nodes cannot sustain the high processing overhead and complexity of these techniques due to their limited computational capacity and reduced memory size. In addition, most of the existing key management protocols must perform extensive message exchanges to establish keys, which increases power consumption, depletes the sensor node limited energy, and shortens the network operational lifetime. Besides, in a WSN, nodes can leave the network because they run out of energy or are captured and eliminated by an adversarial party. Therefore, new sensor nodes must be added after the initial deployment phase to replace the removed nodes

Manuscript received July 1, 2014. This work was supported in part by by the National Research Foundation of Korea (NRF) grant funded by the Korean government and the Tunisian government (No. NRF2012K1A3A1-A09026959).

Walid Abdallah is an Assistant Professor and member of the Communication Networks and Security research Lab, Tunisia (corresponding author; Phone: +21698229840; e-mail: ab.walid@gmail.com). Pr. Noureddine Boudirga is a Professor of Telecommunications in the School of Communication Engineering, SupCom, Carthage University and the Director of the Communication Networks and Security Research Laboratory (CNAS), Tunisia (email:noure.boudriga2@gmail.com). Deahe Kim is a Phd student in the Computer Network research Lab, Department of Electronics Engineering, Korea University, Seoul, Korea (email: dhkim@dsys.korea.ac.kr). Pr. Sunshin An is a Professor of Electronic and Computer Engineering in Korea University, Seoul, Korea (email: sunshin@dsys.korea.ac.kr)

or to enhance the connectivity of the network. Consequently, the key management scheme should deal with this issue to avoid the failure of the network and optimize the re-keying procedure when nodes are deleted or added.

Several research works[4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14] had been devoted to design appropriate key distribution schemes for WSN. The proposed schemes were based on pre-distribution of symmetric or asymmetric keys before the network deployment or on secret sharing using threshold cryptographic techniques. Although some of these schemes can offer extensive security to data transfer on wireless sensor network, they are complex to apply in real environment and do not scale to large networks. In addition, key establishment protocols require a high number of message exchanges which exhausts the limited available energy of sensor nodes and shorten the network operational live time. Moreover, all existing key distribution and management schemes assume static topology and do not consider the case where mobile sensor nodes can be employed.

This paper proposes the design of a key management scheme for wireless sensor networks adapted to hierarchical topologies. It is an enhancement of the work presented in [15]. Our key distribution scheme can perform efficient and scalable generation and sharing of cryptographic keys to provide authentication, integrity, and confidentiality services to all types of data traffic exchanged at the different layers of the network topology. Our proposal uses elliptic curve based Diffie-Hellman like exchange procedure to establish individual secret keys between different elements of the WSN, such as sensor node and base station, the sensor and its cluster head, and each cluster head and the base station. These exchanges are exploited to generate secure group keys to ensure intra-cluster and inter-cluster communications privacy. Authentication of the exchanged values is implemented to overcome vulnerability to the man-in-the-middle attack. Our secret key establishment approach is less complex and requires reduced message exchanges than existing schemes whilst it improves offered security level. Moreover, the use of elliptic curve techniques allows shorter key sizes and decreases the processing overhead of the cryptographic operations while ensuring the same security level as current public key schemes. The main contributions of this work with regard to existing literature are as follows:

- The development of an Elliptic Curve Public Key Cryptography (ECPKC) based key management mechanism for WSNs, allowing dynamic establishment of many kinds of secret keys intended for different usages in various levels of the network topology and taking into consideration node mobility.
- The design of an efficient group key establishment procedure to enable in-network processing and secure intra-cluster and inter-cluster broadcast traffics. This procedure achieves group key sharing in only two rounds, which reduces the processing and communication overheads and saves sensor's energy.
- The proposal of a re-keying procedure based on secret sharing techniques to ensure backward and forward secrecy and improve resilience to node capture attack.

The remaining parts of the paper are as follows: Section II exposes related works to the key distribution problem in wireless sensor networks. Section III describes the proposed key management scheme. Section IV, analyzes the security level provided by the proposed scheme. Section V performs a performance analysis of the proposed scheme, Section VI, presents simulation work conducted to evaluate the effectiveness of the key management approach and demonstrate its scalability. Section VII, concludes the achieved work in this paper and gives some perspectives.

II. Related Work

Key distribution problem in wireless sensor networks, had been the subject of many research works during the last decade[16]. Key distribution and management procedure play a crucial role in guaranteeing the security of any data exchange using cryptographic primitives. Key management encompasses the processes of generating, distributing, storing, and updating encryption keys. The main target is to prevent attacker from exploiting weaknesses in the key management procedure to derive encryption keys and break the security of the wireless sensor network. Due to the limited resources of sensor nodes, the large number of deployed nodes, and missing of infrastructure, key distribution and management is a major issue in wireless sensor networks.

Secret key cryptographic techniques are the most suitable to secure communication in wireless sensor networks. These techniques can be executed in reduced computational capability processors with an acceptable delays. In addition, they manipulate short key sizes requiring few memory occupancy. This has the advantage to reduce the energy consumption, increase efficiency, and ensure reliability of the network. TinySec [17] is an effective implementation adapted to wireless sensor nodes to ensure link layer security in terms of confidentiality, integrity and authentication. Authors studied, specific operational modes for a set of secret key encryption algorithms and message authentication codes, that can satisfy resource constraints of sensor nodes. For instance, in TinySec, RC5 and Skipjack are considered as the most suitable encryption algorithms to offer data confidentiality. One of the main problems in secret key cryptosystems is key distribution consisting in the procedure to securely share secret keys between sensor nodes. Many research works[5], [6], [8], [18], [7], [9], [10], [19], [20], [4], [21], [14] have been devoted for studying key distribution and management issue in wireless sensor networks proposing multiple schemes with various approaches.

Most of the proposed key distribution schemes are based on the pre-distribution of a set of secret keys in the sensor nodes before network deployment [5], [6], [8], [7], [12]. The work presented by Eschenauer et al [5] is the first in this context. The authors proposed a key distribution scheme based on pre-loading a set of secret keys in each sensor node that are randomly selected from a common pool of keys. At the initial phase of network deployment, each sensor node exchanges information about the pre-configured keys with its neighbors to find those that share with it the same keys. When two

neighbors find that they have a common key, they establish a secure communication link between themselves. Furthermore, the established secure links can be used to negotiate the sharing of pairwise keys between nodes that their key sets did not overlap. It was proved, using random graph theory that, if the probability that two selected sets of keys share at least one key is greater than a given value, then secure connectivity of the network can be achieved with high probability. Although, this scheme may be very efficient in establishing shared keys in wireless sensor networks, its main drawback is that when the number of jeopardized nodes increases, the security level significantly degrades. When sensor nodes are captured, all shared keys can be discovered and encrypted data will be disclosed to an adversary. Moreover, given that the same key can be used to secure many links, the attacker may even be able to decrypt data being currently transmitted between non compromised nodes. Besides, to offer full communication security, each sensor node needs to store and manage an important number of keys, which requires a high memory capacity and limits the scalability of this solution to large size networks.

Chan et al [6] introduced the concept of q-composite. In this approach, a secure link between two neighbor nodes is established if they have at least q common keys, where $q \geq 2$. Authors show that increasing the number of shared keys, q, boosts the resilience to node capture, in the sens that the attacker will need to compromise a higher number of nodes than in the original scheme described in [5] to decrypt the same amount of data. Despite resilience enhancement against node capture, this scheme has not resolved the main limits, which are, the complex procedure and the communication overhead needed to establish a full one-hop secure connectivity between neighbor nodes, and the required memory to store and manage shared keys. To enhance random key pre-distribution approach, Du et al [7] presented a technique to establish pairwise keys between sensor nodes based on the random selection of rows and columns in a key matrix. In this scheme, multiple key generation spaces are used to enhance resilience to node capture. Nevertheless, this approach cannot guarantee that two nodes can share a direct secure link, and the key path establishment procedure of the original scheme [5] is still needed. All these schemes are developed for wireless sensor networks configured in a flat topology where all nodes have the same capabilities and thus a key pairwise must be setup between each pair of sensors. This can reduce scalability to larger size networks due to higher power consumption, extensive processing requirement, and communication overhead.

Using a hierarchical topology can simplify and improve the scalability and efficiency of the key distribution procedure. In this case, the sensor node doesn't need to establish a pairwise keys with all nodes in the network, but only with those that are in its communication range. Particularly, a sensor will share keys with its cluster head (CH) and cluster members; this contributes in reducing the communication overhead and saving energy. Several works have studied the design of key distribution mechanism for hierarchical sensor networks [18], [22], [12], [14], [10].

Localized Encryption and authentication protocol (LEAP) [18], [22] is an energy efficient key distribution mechanism developed for large scale hierarchical sensor networks, that is able to generate specific keys for securing various types of uni-cast and broadcast traffics. Four kinds of encryption keys are defined: individual key shared between the base station and each sensor node, pairwise key that is a unique key established between the node and its cluster head, cluster key is a common key used to secure data intended for all members of the cluster, and group key used to secure data broadcast to all nodes of the network. All these keys are derived from a unique master key that is pre-loaded in each node before deployment. This master key is erased from the memory at the end of the initial key distribution process, to avoid that an adversary party capturing a single node, can compromise all data transmitted in the network.

A similar approach was described in [12], where a security architecture was proposed for wireless sensor networks based on a master secret key that is embedded in the source code of the operational system in every sensor node. The authors claim that this can prevent the disclose of the encryption keys derived from the master key and stored in non-volatile memory even if the node is captured. Although, we can agree that configuring the master key in the source code of the application program can harden the task of an attacker to retrieve it, but this is not impossible. Also, it will be very hard to upgrade the security parameters of the encryption scheme such as the key size, encryption algorithms, and the master key itself, because this will require the upload of another operation system in all deployed nodes.

Secret sharing techniques have been investigated in [14] to design a key management mechanism in hierarchical wireless sensor networks. This scheme allows the distribution of keys in different levels of the topology. Indeed, individual secrets are distributed to all nodes of the network. Group keys can be constructed by resembling a minimum number of individual secrets and applying a polynomial interpolation. This has the advantage of ensuring the survivability of the network if a minimum number of nodes are still active and a maximum number of nodes had not been compromised. Nevertheless, to ensure security of the transmitted data, the shared secrets must be modified for every session to prevent key compromising due to the capture of a single node participating in the reconstruction process. This generates an extensive communication and processing overheads and increases power consumption. In addition, sensor nodes are required to store an important number of session secrets overloading the limited memory capacity of sensor nodes.

The previously described key distribution schemes for WSNs are static in the sense that they are based on the preloading of secret keys that remain valid during all the network life-time. More specifically, these schemes do not define rekeying procedures to update encryption keys. This fact, can constitute a serious security limit in these mechanisms, as using an encryption key for a long period of time can increase the probability of being compromised. Some dynamic key management schemes that enable key updating had been proposed for wireless sensor networks [21], [23], [24]. These schemes are mainly based on secret key encryption techniques

which makes them vulnerable to node capture attacks. In these dynamic key management schemes, capturing a specific number of sensor nodes can lead to revealing keys used by non compromised nodes. Public key encryption techniques can be investigated to resolve these problems.

Although, public key cryptosystems have not been considered at the beginning in WSNs to secure key distribution owing to their key sizes and high computation capacity requirement, they are being investigated in some research works[25], [19], [4]. This is motivated by the advances achieved in physical node architecture technology and the enhancement of their computation capacity. In addition, a promising solution is the use of elliptic curve cryptography which significantly reduces key size, achieves key generation in a limited delay, and consumes a few amount of power [13].

In this paper, we investigate the design of a key distribution and management scheme for wireless sensor networks with hierarchical topology. Our approach consists in combining different techniques, each one will be used in a specific context in order to ensure the highest security level while guaranteeing efficiency and scalability of the key distribution process. Our proposal is based on using elliptic curve public key cryptography, in particular on the Diffie-Hellman like key exchange procedure, to establish secret keys in the different levels of the hierarchy. A unique private key is generated by each sensor node at the initial phase of the network deployment. The generation process is based on the identity of the node and a key that is pre-loaded in the sensor node and deleted after the generation of the private key. The validation of the corresponding calculated public key is achieved by the base station. The public and private keys are then used to establish individual and group secret keys to secure different kinds of uni-cast and broadcast traffics. In addition, our scheme enables secure re-keying procedure by using secret sharing techniques to regenerate the initial key and reconfigure the overall security parameters.

III. Key distribution and management scheme description

In this section, we describe the proposed scalable key distribution and management scheme to secure wireless sensor networks. Firstly, we introduce the considered network architecture; then we detail the initial key generation and distribution procedure; finally we investigate issues related to node addition, deletion, and mobility.

A. Network topology and assumptions

Wireless sensor networks can be configured into two main topologies: flat homogenous and heterogeneous hierarchical. In flat topology, all sensors have the same capabilities in terms of sensing, computing and communication. Whereas, in hierarchical topology, the network is composed of many kinds of nodes with divers capabilities and perform different functions. Flat wireless sensor networks are more simple to deploy, however hierarchical architectures are more efficient and scalable.

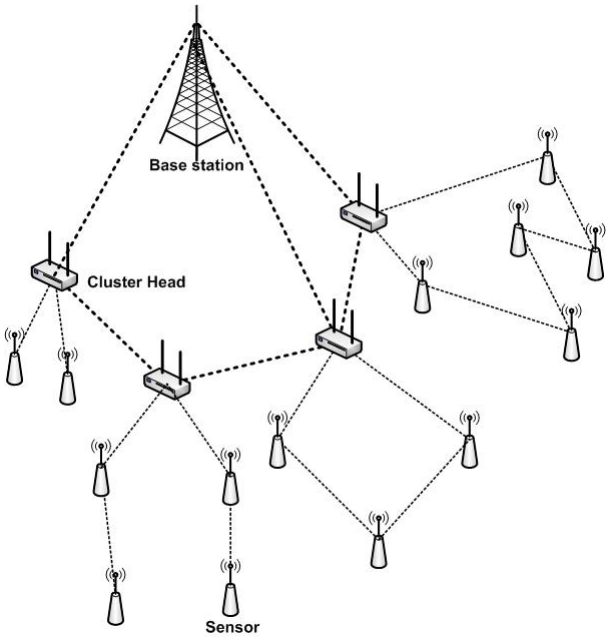


Fig. 1. Network architecture

In this work, we consider a hierarchical wireless sensor network composed of a large number of sensor nodes that are organized into a number of clusters. Each cluster is controlled and managed by a cluster head which is a device with higher processing and communication capabilities than sensor nodes. After deployment, the cluster heads need to execute an appropriate clustering algorithm [26] to divide the network into an optimized number of clusters.

The considered network topology is depicted by Figure 1. As we can see, the network architecture encompasses three types of network devices, sensor nodes, cluster heads, and the base station (or Sink node). In the sequel, we describe the functionality of each one of these devices.

1) Sensor nodes : Sensor nodes are in the lowest level of the hierarchy. They are low-cost devices with a very limited computing, storage, and communication capabilities. Also, they are power supplied using a finite life battery. The main mission of a sensor node is to detect particular events and to exchange messages with its cluster head and the base station. Also, a sensor node can relay messages transmitted by sensor nodes which their communication ranges do not reach the cluster head. In some situations, the base station can exchange messages with the sensor nodes. This can happen for example when the configuration of sensor nodes needs to be updated or when a particular event happens. In addition, we suppose that at any time a sensor can be attached to only one cluster. However, sensor nodes can be mobile and move from one cluster to another with a very low speed.

2) Cluster heads : The cluster head is responsible of collecting data from the members of its cluster and aggregating them in order to optimize transmission channel usage. Also, it manages and controls all procedures of member join and departure. A cluster head needs to be equipped with an extensively higher amount of resources than the sensor node.

In our architecture we suppose that cluster heads encompasses a higher processing devices with large storage capacity and more powered and long live batteries. Moreover, we consider that they are able to achieve more complex operations and have a wider communication range than sensors. Cluster heads can communicate with each other directly and relay data to the base station. Due to their limited number, it can be cost-effective to assume that cluster heads are endowed with a tamper-proof hardware that ensures resistance to node capture attack. Moreover, some advanced security functionality such as auto-destruction and memory eraser in case of unauthorized access attempts can be implemented in these devices.

3) Base station : The base station is the network element that implements the most higher capabilities. We assume that it has unlimited resources such as, computing power, storage capacity and energy. Moreover, the base station has a very large communication range that can reach all nodes in the network. Depending on the application, the base station can be localized either in the center or the corner of the network. In any case, it is supposed that the base station is installed in a well known and secure location. Also, it is considered as the most secure element of the topology and is trusted by all entities of the wireless sensor network.

B. Key generation and distribution procedure

The main objective of our work is to design a key management procedure that ensures robust authentication, integrity and confidentiality services in the sensor network and takes into consideration the limited resources and reduced processing capability of the sensor nodes. The key management mechanism should allow secure generation and distribution of keys in every level of the hierarchy. In addition, it must enable the establishment of different group communication keys that can be used to perform in-network processing. The in-network processing capability consists in a the ability of sensor nodes to decrypt packets transmitted by neighbor nodes in order to avoid event detection redundancy and allow data aggregation. These operations are very useful in many applications and permit energy saving and channel usage optimization. Consequently, we can distinguish the following kinds of keys:

- Individual keys: used to secure communication between a sensor node and the base station.
- Intra-cluster pairwise keys: shared between a sensor node and its cluster head and neighbor sensor nodes belonging to the same cluster
- Cluster key established between all sensor nodes of the same cluster to secure group communications.
- Inter-clusters key: used to secure communication between all clusters heads and the base station
- Network key: shared between all nodes of the network and used to secure message broadcast.

In this work, we investigate the use of elliptic curve public key cryptography to enable efficient and secure key exchange in wireless sensor networks. In the upcoming subsections, we present our Elliptic Curve Public Key Cryptography (ECPKC) based key management mechanism proposed to carry out dynamic establishment of the aforementioned kinds of keys. First, an overview of elliptic curve cryptography is given in this paper. Then, the generation and distribution processes are described.

1) Elliptic curve fields selection: Elliptic curve techniques [27] offer a valuable opportunity to efficiently apply public key cryptography approach to secure wireless sensor networks. These techniques are able to provide equivalent security level as classical public key cryptosystems, namely the Diffie-Hellman key exchange procedure, with significantly reduced key size. For example, in Diffie-Hellman a minimum key size of 1024 bits is required to ensure the security of the key exchange procedure. Indeed, the discrete logarithm problem, on which is based the security of this key establishment protocol, becomes intractable for a key size higher than this value. However, with elliptic curve equivalent approach a key size of 160 bits is sufficient to ensure security. In the following we explain how this was achieved.

Given a Galois field F_p, where p is an integer number, an elliptic curve, $E(F_p)$ is defined by the set of points that satisfy the Weierstrass form defined by the following equality:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

where, $a_i \in F_p$.

In cryptography, two forms of the Galois finite fields are of interest. The first form considers a field F_p, with p a prime number, and an elliptic curve satisfies the equation:

$$E(F_p) = \{(x, y) \in F_p^2,\ y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\} \qquad (2)$$

where a, b are satisfying $4a^3 + 27b^2 \neq 0$ and $\mathcal{O}$is the neutral element of the curve. This form is very useful for a software implementation of the elliptic curve encryption paradigm.

The second form considers a field F_p, with $p = 2^k$, and k is prime number. The elliptic curve in this case is characterized by the equality:

$$E(F_p) = \{(x, y) \in F_p^2,\ y^2 + xy = x^3 + ax + b\} \cup \{\mathcal{O}\} \quad (3)$$

This form is more adapted for hardware implementation of elliptic curve based encryption algorithms.

These two forms are not vulnerable to the sub-exponential attack and can guarantee the security of the key exchange procedure. For both forms a specific addition operation is defined. The more interesting is the equivalent form of the discrete logarithm problem in the elliptic curve field. Recall that, the discrete logarithm problem consists in, given a prime number p, and a generator g and a value h belonging to $\mathbb{Z}_p^*$, it is difficult to find, x where $h = g^x mod(p)$. In elliptic curve cryptography, it is believed that, given a field $F_p$satisfying one of the aforementioned forms, and two points, P and Q belonging to $E(F_p)$, the problem of finding, an integer n, such that $Q = nP = P + P + ... + P$ is more difficult than the discrete logarithm problem. Therefore, mapping between the classical Diffie-Hellman key exchange scheme and its equivalent using elliptic curve paradigm can be simply performed by replacing the exponentiation operation by an integer multiplication (or more precisely n-time addition) in $E(F_p)$.

2) Individual keys establishment : Individual keys are established between each sensor node and the base station during the initial phase of network deployment. We assume that the hierarchical network topology has been created and that sensor nodes can communicate with the base station to establish secret keys. This is performed in our scheme using elliptic curve based Diffie-Hellman key exchange procedure according to the following steps:

Pre-deployment : Before deployment, the base station randomly selects an integer number p, the elliptic curve $E(F_p)$ according to the second form as discussed above, and a generator point $G \in F_p$. Then, it generates its private key, $x_B \in \mathbb{Z}_p$, where $2 \leq x_B \leq p-1$ and calculates the corresponding elliptic curve public key, $Y_B = x_B G$. The parameters p, $E(F_p)$, G , Y_B, and an initial key K_0 will be pre-loaded in each deployed sensor node. The initial key, K_0 will be used to verify the genuineness of the deployed sensor nodes. It is valid only during the short period of the initial deployment phase and will be deleted immediately after the accomplishment of the key establishment procedure. In the following , we denote by N the total number of deployed nodes, where each node is uniquely identified by an id value.

Private/public key pair generation and individual key calculation: Immediately after network deployment and the establishment of clustered communication architecture, every node i, $1 \leq i \leq N$, will generate its private key, $x_i \in \mathbb{Z}_p$. This is performed by applying a hash function as follows:

$$x_i = Hash(id_i||K_0||N_i) mod(p) \tag{4}$$

where N_i is a randomly generated nonce. This generation procedure ensures that all private keys are different from each other, which can enable data origin authentication.

Then, the sensor node calculates its elliptic curve public key, $Y_i = x_i G$. At this point the sensor node is able to calculate its individual pairwise secret key, $K_i = x_i Y_B = x_i x_B G$. The sensor node sends its public key Y_i to the base station to be validated and stored in the public keys repository. The message is authenticated by a Hash Message Authentication Code (HMAC) using K_0, to ensures that it is sent by a genuine deployed sensor node.

Public key validation and individual key establishment in the base station: After verifying the identity of the sensor node and the MAC of the received request, the base station validates the public key of the sensor node, saves it in its public keys repository, and establish the shared individual pairwise key, $K_i = x_B Y_i = x_i x_B G$. Finally, the base station sends to the sensor node an acknowledgment that is authenticated by a MAC calculated using the individual key, K_i. Then, the sensor deletes immediately the initial key, K_0 from its memory.

3) Intra-cluster pairwise keys and cluster key establishment : Intra-cluster pairwise keys must be established to secure communication between each sensor node and its cluster head. In addition, the sensor node can establish a pairwise key with each one of its node neighbors in order to communicate with the cluster head. In addition, a cluster key shared between all nodes of the cluster is established to enable in-network processing and optimize resources usage.

Pairwise keys are established in a similar way as individual keys described above. The only difference is that public values must be retrieved from the base station and each party verifies its validity before key establishment. To this end, the base station calculates a MAC of the public key using the individual key shared with the sensor node that had generated the key request message. After that, neighbor nodes i and j can establish a pairwise key, $K_{ij} = x_j Y_i = x_i Y_j = x_i x_j G$. Similarly, the pairwise key $K_i^c = x_i Y_c = x_c Y_i = x_i x_c G$ can be established between the node i and its CH c.

To set the cluster key a group communication secret key sharing procedure was proposed. This scheme is more efficient than the existing techniques [28] because it allows key establishment in only two rounds. To this purpose, for each node j of the cluster, the CH calculates and sends a public value

$$Y_{cj} = x_c \sum_{n=1,\, n \neq j}^{m_c} Y_n \tag{5}$$

where m_c denotes the number of sensor nodes in the cluster c.

The cluster key, K^c can be determined in each node by simply adding this value to the already established intra-cluster pairwise key as

$$K^c = K_j^c + Y_{cj} = x_c \sum_{n=1}^{m_c} Y_n \tag{6}$$

4) Inter-cluster key and network key establishment: Using the same procedure as for the cluster key, CHs and the base station can share an inter-cluster key $K^B = x_B \sum_{c=1}^{M} Y_c$ to secure message broadcast in the second level of the hierarchy. M is referred to as the number of clusters.

In addition, a network key K_N can be securely distributed to all sensor nodes using two encryption stages. In the first stage, the base station randomly generates K_N, encrypts it with the inter-cluster key, K_B and transmits it to all CHs. In the second stage, each CH, c decrypts the network key and encrypts it with the cluster key, K^c before broadcasting it to all cluster members.

5) Session keys derivation: All the keys that they had been described in last subsections are note used directly to ensure data confidentiality and authentication. To this end, some session keys are derived from these keys. This is performed by the following procedure.

The elliptic curve approach, allows the sharing of a point with two coordinates. Therefore, each key K is a point in $E(F_p)$ that is composed by abscissa, K_x and an ordinate K_y. In order to be conform to the rule of separation between the keys for encryption and authentication, two session keys denoted as, Ke_i, and, Ka_i are derived from the abscissa and the ordinate of the key K. These two keys are used respectively for encrypting and generating the MAC of each message exchanged between the sensor node and any other entity of the network. Here, the key K denotes any kind of the described keys such as individual key, pairwise key, cluster key, inter-cluster key, and a network key. New session key is

derived for each session. If i is the current session number, the session keys used securely exchange messages during this session is given by the following formula

$$Ke_i = Hash(K_x, Ke_{i-1}, MAC_{i-1}) \tag{7}$$

$$Ka_i = Hash(K_y, Ka_{i-1}, MAC_{i-1}) \tag{8}$$

MAC_{i-1} is referred to the message authentication code of the packets that had been correctly received during the last session by the entity with witch the key K was shared. Similarly, $Ke_{i-1}$and $Ka_{i-1}$are the session keys used in the last session for ensuring encryption and authentication during the last session. As it will be explained later in this paper, the selected derivation procedure can ensure backward and forward secrecy of the transmitted data and resilience to node capture and replication attacks.

C. Keys management procedures

In this subsection, we describe procedure of modifying the different types of keys due to new nodes deployment or elimination. Also, we detail the re-keying process that will be executed to initiate the establishment of new keys when the validity of the current keys expires.

1) New nodes deployment: When a new node is deployed in the WSN, it must first create its individual key shared with the base station using the same procedure as described in the previous section. The main difference is that the initial key will be different from the one used in the initial deployment phase. Indeed, suppose that a new node will be added at the instant t after the initial deployment. The base station will generate and configure the node with an initial key K_t. This procedure will prevent an adversary, that have access to previous initial keys, to add its own replicated nodes. Once the individual key is generated and the public value is validated, the sensor follows the previously described steps to establish the other keys.

2) Nodes elimination and revocation: When a compromised node is detected by the CH, it informs the base station to invalidate its public key and adds it to the revocation list. The CH will isolate the compromised node and establish a new cluster key by eliminating the public value of the compromised node. Also, the base station will generate and distribute a new network key using the new cluster key.

3) Mobility Management: The use of public key cryptography approach in the proposed key distribution mechanism enables an efficient key update even in case of mobile sensor nodes. We assume that some sensor nodes can move from one cluster to another with a moderate frequency. The sensor node should establish a pairwise key with its new CH and participate in the generation of a new common cluster key using the same procedures as described earlier. However, the new CH should verify the validity of the public value of the node that wants to join the cluster. Also, the old cluster should be informed that the node has left the cluster to initiate cluster key update.

4) Re-keying procedure: A global re-keying procedure is triggered when the number of compromised nodes reaches a given threshold or the validity period of the generated private keys expires. New private and public keys should be created to renew different shared keys. To this end, each sensor node should reconstruct the key, K_r that will play the same role as the initial key used in the deployment phase. We have investigated the use of threshold secret sharing techniques to manage the distribution and the reconstruction of this key. The basic idea is that every sensor node will possess a partial secret that can be used to reconstitute the key K_r. However, this cannot be achieved unless a minimum number of nodes, denoted by t, collaborate together and assemble their secrets. This approach has the advantage of maintaining the security of the key if the number of compromised nodes is less than $t-1$. Also, the re-keying procedure can be initiated if at least t trusted nodes are still operational in the network. Our proposal uses the Shamir's method[29] based on the Lagrange interpolation. This approach consists in randomly selecting a polynomial function, $f(x) = K_r + a_1x + a_2x^2 + ... + a_{t-1}x^{t-1} mod(Q)$ by the base station, where Q is a prime number. We can notice that, $K_r = f(0)$ and all coefficients of $f(x)$ must belong to $\mathbb{Z}_Q$. For $i = 1, 2, ..., N$, the secret S_i of each sensor node i is calculated as $S_i = f(id_i)$, where id_i is a unique identifier of the node i. Each partial secret must be securely transmitted to the corresponding sensor node. To this end, the base station will encrypt every secret S_i by the individual shared key K_i. According to the Lagrange interpolation, $f(x)$, can be reconstructed by giving t points $(S_1, S_2, ..., S_t)$ using the following formula

$$f(x) = \sum_{i=1}^{t} S_i \left(\prod_{i \neq j} \frac{x - id_j}{id_i - id_j} \right) mod(p) \tag{9}$$

Particularly, the key K_r can be reconstructed by applying the equality

$$K_r = f(0) = \sum_{i=1}^{t} S_i \left(\prod_{i \neq j} \frac{id_j}{id_j - id_i} \right) mod(Q) \tag{10}$$

IV. Security Analysis

The evaluation of the security schemes intended for WSNs is significantly different from those used in conventional networks. Indeed, the evaluation criteria should consider the characteristics of the WSNs deployment and their resource constraints. In this section we analyze the security level offered by our key distribution mechanism with regard to four proprieties that reflect the specificity of WSNs: (1) the possibility of providing backward and forward security for encrypted data, (2) the resilience to node capture, (3) resistance against node replication, (4) the vulnerability to energy depletion attack.

A. Backward and forward security

The forward security propriety is to prevent the possibility to an attacker to predict a future key if he captures a currently used key. On the other hand, backward security is to preclude

an attacker from obtaining information about previously used keys when he can capture the currently used key. These two proprieties are very important in key distribution schemes to ensure data confidentiality. To ensure the forward and backward secrecy, our proposed key distribution scheme is based on public key encryption paradigm where at each re-keying period the private and public keys of any sensor node are generated independently of any previously used keys. Therefore, all symmetric keys established between network entities are not derived from any used key and are recalculated based on the newly generated public and private key pairs. In addition, no future keys must be encrypted by currently used key to be shared. Moreover, all group communication keys are modified each time a change in the network topology occurs in the sensor level or in the cluster level.

B. Node capture

In many applications, sensor nodes are usually randomly deployed by aerial dropping in large areas. Consequently, sensor nodes can be easily captured by an adversary, who can access to their memory content. Security schemes should maximize the network resilience by minimizing the amount of information revealed to attacker on non captured nodes. A sensor node can be accessed either using soft capture or physical capture. In the soft capture, the attacker tries to establish a connection to access to the management console of the sensor node. Many techniques can be used to implement authentication in administrative mode, such as passwords, RFID technology, and challenge-response approaches.

On the other hand, a sensor node can be physically captured. In our case, an attacker can capture either a sensor node or a cluster head. When an attacker captures a sensor node, he can access to the individual keys it shares with the base station and the cluster head, and the cluster key it shares with all members of its cluster. The later key can affect security within the cluster and should be modified by eliminating the public value of the captured node in the key calculation operation. In addition, the sensor node stores a single part of the shared secret used to reconstruct the network re-initialization key. To prevent the discover of this key the number of captured nodes should not exceed the degree of the polynomial function, t.

Besides, getting access to a cluster head is more critical than in the case of a sensor node. In this case, the attacker can access to the individual pairwise key shared between the cluster head and the base station, all individual keys shared between the cluster head and each sensor node, the cluster key, and the inter-cluster key shared with all other cluster heads and the base station. Therefore, all group communication keys must be changed by recalculating the keys without the public value of the compromised cluster head. Also, the cluster member should establish another individual keys with other cluster heads.

In addition, several techniques can be used to prevent that an adversary can access to the content of a sensor or a cluster head such as triggering of a physical auto-destruction, or a soft erasing of the content of all memories when an attempt to access to the sensor is detected. These techniques are mainly appropriate for cluster heads which encompasses a large quantity of information.

C. Node replication

The node replication attack consists in the possibility that an adversary party can introduce malicious nodes after gathering information from captured nodes. In this case, the replicated nodes will try to establish connection with other nodes, cluster head, or even the base station. These nodes should be detected and isolated from the network. In the sequel, we describe how the proposed scheme can resist to cloning attacks according to different situations.

1) Node duplication at the initial deployment phase: In this situation, the attacker tries to add new nodes to the network with copied identities at the initial deployment phase of the network. The inserted nodes will attempt to generate private and public keys and establish symmetric keys with the cluster heads and the base station. The proposed scheme can guarantee resistance against this attack. Indeed, before establishing connections in the network any new node should generate a private key based on its identity and the secret initial key. All initial keys are eliminated from the memory after the deployment of sensor nodes, the generation of their private keys, and the validation of the corresponding public keys. Consequently, these keys cannot be recovered by capturing already deployed sensor nodes. Furthermore, the base station tracks all identities of the deployed nodes and validates and distributes public keys to all entities requesting the establishment of secret keys. Therefore, unused or compromised public keys can be revoked by the base station. Consequently, before establishing any secure connection within a cluster, the identity of the node is checked and unauthorized nodes can be detected and eliminated from the network.

2) The replication of an active node or a sleeping node: In this case the attacker will replicate a number of already deployed nodes that are either in an active state or in a sleeping state. We suppose that the attacker will get access to the private/public key pair of the cloned node. The attacker will try to affect the copies of the replicated nodes to different cluster in order to avoid their detection. In fact, if a clone tries to connect to the same cluster as the original node, it can be easily detected by the cluster head. This can be performed by identifying traffic patterns. For example, the cluster head can notice that two packets are transmitted in a very short period from the same node identity using two different routes. In this case, it can either trigger the revocation of the two nodes or, based on its history, it can detect the false node. Also the inserted node will not be able to reconstruct the session keys which are generated in every session based on the packet transmission history.

Consequently, the clones will try to establish shared keys with new clusters. In our scheme, we can detect copies of nodes even in this situation. As it had been previously detailed, when the new cluster head receives the key establishment request from the false node. It first consults the base station to gather information about its original cluster. After that, it informs the old cluster which verifies the connectivity status

of the node by sending a beacon message to see if the node had effectively left the cluster. If it detects that the original node is still connected to its cluster it will communicate this information to the new cluster head which isolates the false node.

3) The replication of disconnected sensor nodes: In this scenario, the intruder will try to insert duplicated copies of a node that is disconnected from the network due to some reason. The replicated nodes are configured with the private and public keys of the original node. They try to establish keys with different cluster heads. The main problem in this situation is that the original cluster head is not able to detect if the node is still connected to its original cluster or not. To resolve this problem we use authentication using the last known session key of the node. In other words, when the false node wants to establish new secret keys, we will first verify that the original node is not connected to its original cluster by applying the procedure described in the last subsection. Then, the new cluster head will challenge the node by requesting that is encrypts a given packet using its last session key. The encrypted message is then sent to the original cluster head to verify the genuineness of the node. This procedure allows an efficient detection and isolation of the false nodes even if they are deployed in many clusters.

D. Energy depletion attack

Sensor nodes are battery based devices with a very limited life time. Hence, energy management is a very important issue in wireless sensor networks. An attacker can try a denial of service by sending many false key establishment requests with different identities in order to deplete the available energy of a sensor node. We can classify situations where this attack can be performed in three classes:

1) Attacks performed during the identification process: In this situation, a certain number of malicious nodes try to send an important number of false keying requests to the base station in order to make intermediate nodes that are relaying the message, out of energy. One solution to combat this attack is that when the base station receives a number of false keying requests from a specific source higher than a specific value, it will send a message to the neighbors of the source to not relay any packet from it in the future. The attacking node is therefore detected and isolated. However, this solution generates false positives and does reduce completely such an attack.

2) Attacks performed during key establishment between sensor nodes: In this case, a malicious node will send false key establishment requests to a neighbor that will execute costly processing operations that deplete its available energy. Our scheme can prevent this kind of attacks because sensor nodes will not perform any costly key establishment operation before validating the identity and receiving the appropriate public key from the base station. Also, we can set that if a sensor node receives a number of key establishment requests with invalid public keys it will isolate the source of these requests.

3) Attacks performed during data transmission: In this case, the attacker will try to send an important number of false encrypted messages where the destination will apply the costly power consuming and unnecessary decryption procedure. This can dangerously reduce the available energy of the sensor node. One solution for this problem is that the base station stores a profile for each sensor node transmission. The profiling operation can be based, for example, on transmission frequency and sampling. If a transmission deviates from a given profile by a certain threshold, the base station will order the neighbor nodes of the source to not relay any new packet from it.

V. Performances Analysis

In this section, we assess the performance of the proposed key distribution scheme in terms of scalability, key storage requirement, communication overhead and computation power cost.

A. Scalability

The scalability is the ability of the scheme to maintain an acceptable security level regardless of the network size. This is very important is wireless sensor networks that usually encompass a very large number of sensor nodes. To be scalable the number of encryption keys managed by each sensor must not extensively increases when the number of nodes increases in the network. This is due to the limited storage capacity of sensor nodes.

The designed key distribution system is fully scalable because it is based on public key encryption that provides an effective security independently of the number of nodes deployed in the network. In addition, the hierarchical topology ensures the scalability of the communication process and optimizes the resource consumption in the network.

B. Key storage requirement

To provide security for data transmission, in any key distribution scheme, each sensor node should store and manage a specific number of keys in its memory. Due to the large size of WSNs and the limited memory capacity of sensors, the amount of the consumed memory, needed for storing keys is a very important parameter. In our scheme, every sensor node should store very limited number of keys. These are the private key, individual key shared with the base station, an intra-cluster pairwise key established with the cluster head, a cluster key, and the network key. Also, in case where a sensor does not have a direct connectivity with the cluster head, it should share individual keys with the neighbors that are closer to the cluster head to relay transmitted packet. Although, the number of these keys will depend on the connectivity level of the cluster, it will be very limited. Typically, a sensor node will need to set shared keys with two of its neighbors in order to ensure communication reliability. Consequently, by using an appropriate clustering model, the storage capacity required to manage the encryption keys in each sensor node will decrease.

On the other hand, the cluster head will need higher storage capacity than sensor nodes. Indeed, in addition to the encryption keys managed by normal nodes, this device should store an individual pairwise key with each sensor belonging

to the cluster. Furthermore, it should set an individual key with neighbor cluster heads and manage the intra-cluster key. For this reason, cluster heads should be equipped with higher storage resources. The amount of needed memory capacity will depend on average number of sensor that can compose the cluster.

Besides the few number of keys generated by the proposed scheme in each sensor, the use of elliptic curve encryption reduces the keys size. The public keys managed in every node have a size that is almost similar to that of secret encryption keys. This contributes also in decreasing the memory occupancy needed for storing keys in each sensor bonging to the wireless sensor network.

C. Communication Overhead

The communication overhead is referred to the number of exchanged messages needed to achieve keys establishment between different entities of the network. This parameter is very important in WSN due to the fact that communication procedures are the most energy consuming tasks. Therefore, an efficient key distribution scheme should minimize the communications required to share different kinds of keys while ensuring an acceptable security level and effective data management procedure by enabling the in-network processing capability.

In the proposed key distribution scheme, each sensor node needs to exchange two messages with the base station to validate its public key and generate the individual pairwise key. Three other messages and an acknowledgment are required to establish intra-cluster pairwise key with the cluster head and the cluster key. A last message and an acknowledgment are exchanged between the sensor node and the cluster head to share the network key that is sent encrypted with the cluster key. These communication messages should be exchanged independently of the network size and connectivity.

Moreover, each sensor that has not direct connectivity with the cluster head should share keys with neighbors that can relay its packets. This will generate the need for exchanging at least two packets per neighbor to retrieve the public keys of the nodes. However the number of these messages will be very limited and can be significantly reduced if the number of clusters and their deployment is chosen adequately.

Withal, the mobility of nodes or the deployment of new nodes can require extensive exchange of messages to perform group keys update between the cluster heads. However, this is less critical because this devices are supposed to have sufficient energy to sustain these operations.

D. Computation power requirement

Another performance parameter for any key distribution scheme is the computation power required to perform key distribution. Indeed, sensor nodes are tiny devices that are endowed with a cheap processor having a very limited processing capability. In public encryption scheme, the most complicated operations are the computation of the public keys and the establishment of shared keys using the Diffie-Hellman elliptic curve key exchange procedure. Arithmetic operations in the elliptic curve Galois Field are shown to have little complexity compared to conventional public key encryption. Furthermore, sensor nodes execute a very limited number of these operations which are triggered during initial deployment, topology changes, and re-keying procedure. This is due to the clustering topology adopted in our scheme where the sensor node will share keys with only the base station, its cluster head and a very limited number of its neighbor nodes belonging to the same cluster.

However, the re-keying procedure can have also an extensive computation cost. In this case, the sensor should recover the re-initialization key after collecting $t-1$ partial secrets. This operation depends on the threshold t that must be appropriately selected to make a trade-off between security and computation complexity.

Table I
SIMULATION PARAMETERS

Parameter	Value
Number of sensors	100-1000
Packet size	36 Byte
Acknowledgment size	12 Byte
Private, Public keys length	160 bits
Symmetric key length	128 bits
Transmitting energy	$59.2\mu J/Byte$
Receiving energy	28.6 $\mu J/Byte$
ECC private, public key setup energy	22 mJ
MAC computation energy (SHA1)	$5.9\mu J/Byte$
Encryption/Decryption energy (AES)	1.62/2.49 $\mu J/Byte$

VI. PERFORMANCE EVALUATION

In this section we assess the performance of the proposed scheme with regard to the required key storage capacity, communication overhead, and energy consumption. In a first set of simulations, we compare the performance of the proposed security to LEAP [18], [22]. In the second the part of the performance evaluation work we assess the scalability of our scheme by evaluating its performance with regard to the number of clusters for different network sizes. Finally, the last set of simulations is devoted for evaluating the performance of the re-keying procedure.

To this end, we developed a simulation model using the Matlab tool. We consider a clustered topology and we compute performance parameters by varying the number sensor nodes. The number of cluster in each topology is taken as : $M = \lceil 0.05 * N \rceil$ where N is the number of sensor nodes. In the implementation of the simulation model we used the values given by table I.

For each number of sensors we generate 5 topologies, and we compute the memory occupancy, the communication overhead, and the energy consumption needed to establish keys for every network. The final results are obtained by taking the average on all values measured for all generated topologies. The maximum number of topologies (5) is selected based on the observation that this value guarantees a confidence interval of more than 90%.

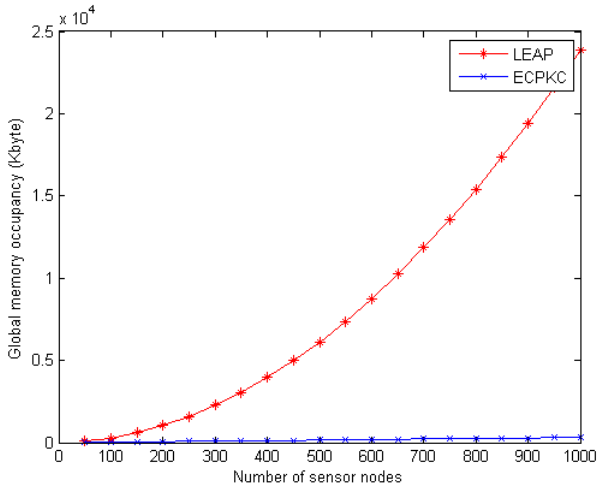


Fig. 2. Memory occupancy

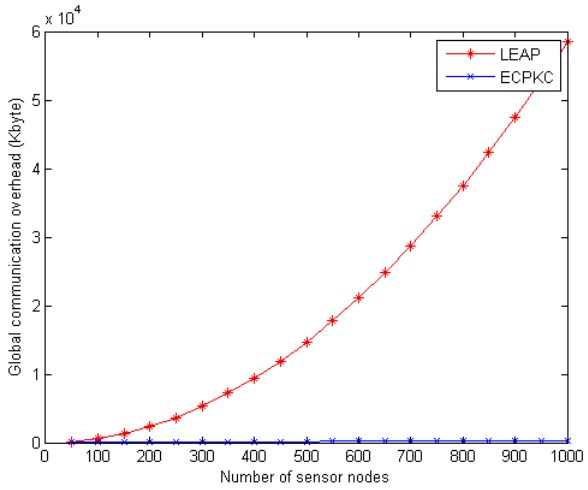


Fig. 3. Communication overhead

A. Comparison with the LEAP protocol

We compare the performances of our scheme to those of the LEAP scheme[18], [22] which implements the in-network processing concept but using symmetric pairwise key pre-distribution paradigm. In each simulation, we execute the proposed elliptic curve public key cryptography based approach, denoted as ECPKC, and the LEAP scheme, on a set of randomly generated topologies composed of a number of sensors with one sink node.

Figure 2 depicts the required storage capacity for managing key distribution in the proposed ECPKC. We can notice that our scheme has remarkably reduced memory occupancy when compared to the occupancy of the LEAP protocol. Moreover, the needed storage capacity of our scheme varies almost linearly with the number of sensor nodes. However, for LEAP, it increases rapidly with the number of sensor nodes. This is due to the fact that in our scheme, each sensor node manage a limited number of public/private keys and symmetric keys that are shared with the base station and the cluster head. Also, each node shares several symmetric keys with its neighbors that can not directly reach the cluster head. On the other hand, in LEAP the number of keys that must be stored in each node depends on the number of its neighbors, since a one pairwise key and a cluster key should be shared with each neighbor node. Consequently, the number of needed keys will increase with the density of the network.

The same observation can be formulated for the communication overhead presented by Figure 3. In our the ECPKC approach the sensor nodes will initiate key exchange procedure with the base station, the cluster head, and a limited number of its neighbor nodes. This, decreases the number of messages needed to establish shared keys. Also, the proposed group key establishment procedure requires only the exchange of one packet and an acknowledgment between the sensor node and its cluster head.

An important parameter for any key distribution scheme is energy consumption. Figure 4 shows the total energy consumption of the proposed scheme compared to the energy consumption of the LEAP scheme. It can be observed that elliptic curve based scheme needs less energy and that it varies linearly with the number of sensor nodes. This can ensure the scalability of our scheme to large scale networks.

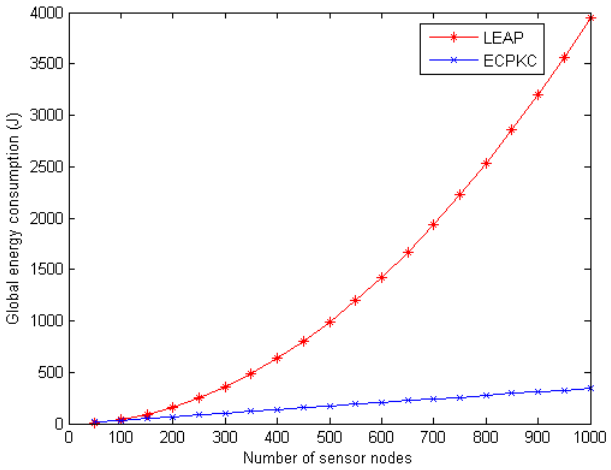


Fig. 4. Energy consumption

B. Evaluation of scalability

In this subsection, we evaluate the scalability of the proposed key distribution scheme. To this end we measure variation of the memory occupancy, the generated communication overhead, and the consumed energy in function of the number of clusters for different network sizes. The simulation results are depicted by Figures 5,6, and 7. We can observe that the needed storage capacity, the communication overhead, and the overall energy consumption of our scheme decreases very fast with the increasing in the number of clusters that compose the network. Also, we can notice the existence of an optimal value for the number of cluster from which the performances become almost constant. This value is around 5% of the number of nodes composing the network. This can be explained by the

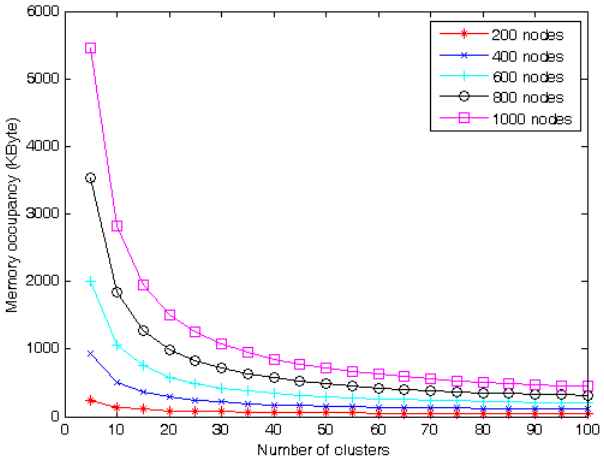


Fig. 5. Variation of memory occupancy in function of the number of clusters for different network sizes

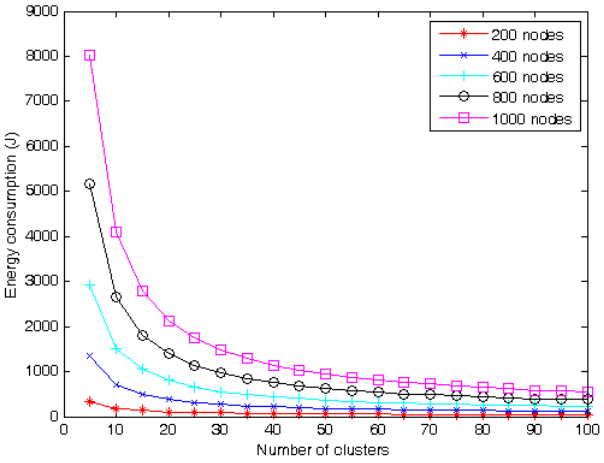


Fig. 7. Variation of energy consumption during key establishment process in function of the number of clusters for different network sizes

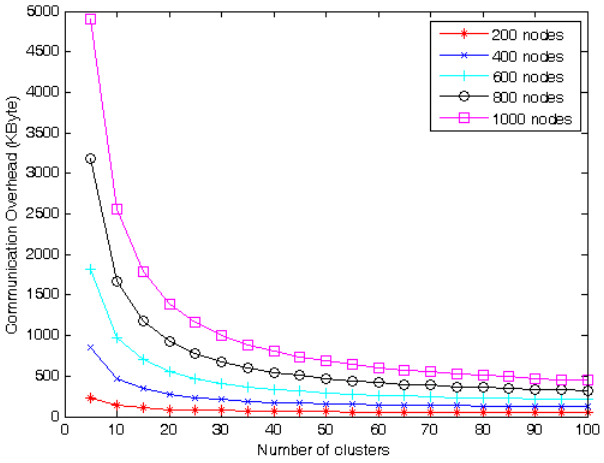


Fig. 6. Variation of the communication overhead needed to establish keys in function of the number of clusters for different network sizes

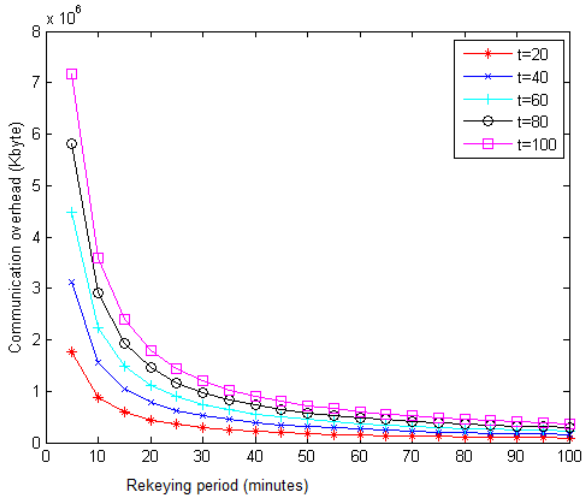


Fig. 8. Variation of the communication overhead in function of the re-keying period for different threshold values

fact that when we divide the network in a higher number of clusters the number of sensor nodes that can connect directly to its cluster head increases. However, the limit is reached when all nodes of the network can be directly connected to its cluster head without any relay. This corresponds to the aforementioned optimal value of the of clusters.

C. Evaluation of the re-keying mechanism

In this subsection, we present results of simulation work conducted to the evaluate the re-keying procedure of the presented scheme that is based on threshold secret key sharing technique. In these simulations the number of sensor nodes composing the network is fixed to 1000 nodes which are divided into 50 clusters. We assess the communication overhead and the energy consumption variation in function of the re-keying period for different values of the threshold t. We execute each simulation during 3600 minutes. At the end of every re-keying interval every sensor node will share its individual secret with $t-1$ nodes to recover the re-initialization key, K_r and after that it executes the key establishment procedure of our scheme. Figures 8 and 9 present the simulation results. We can notice that increasing the re-keying interval contributes to decreasing the communication overhead and the energy consumption. However, for a re-keying period higher that 30 minutes the variation of the performance parameters becomes almost linear. This values can be considered as an optimal values for the re-keying period. We can see also that when the threshold value increases the communication overhead increases. Nevertheless, the variation is less important for the energy consumption parameter.

VII. Conclusion

Key distribution and management in WSNs is much more difficult to achieve than in classical networks owing to the resource constraints, important number of nodes, and the lack of infrastructure support. Consequently, tailored key distribution schemes need to be developed taking into consideration the

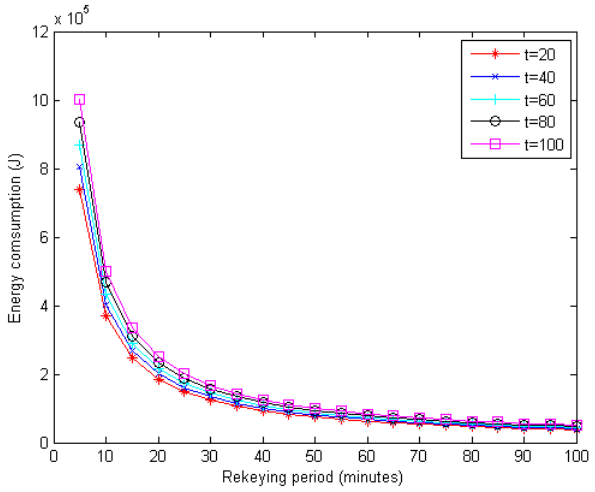


Fig. 9. Variation of energy consumption in function of the re-keying period for different threshold values

limited computation capability, the little storage capacity and the finite energy of sensor nodes. In this paper, we addressed key management problem in WSNs. We proposed an elliptic curve public key cryptography based key management scheme. Our scheme is able to ensure secure sharing of many types of keys in each level of the network topology. Particularly, it uses elliptic curve Diffie-Hellman like key exchange procedure to establish pairwise keys between the sensor node, the base station, and its cluster head. Also, a group key establishment protocol was proposed to create a cluster key used to secure communication within each cluster and an inter-cluster key used to secure message exchange between the cluster heads and the base station. These keys, enable in-network processing, which improves message transmission efficiency and resources usage in the WSN. Furthermore, the proposed approach enables re-keying procedure based on the concept of threshold secret sharing mechanism. Security analysis and performance evaluation using simulation works showed that the ECPKC mechanism ensures an enhanced security level while reducing the required storage capacity, communication overhead, and energy consumption which enables an efficient and scalable implementation of our scheme in large scale WSNs. Finally, developing a strong authentication method for broadcast traffic based of the proposed key distribution scheme and ensuring adaptive security in WSNs can be envisioned in a future work.

ACKNOWLEDGMENTS

This work was partially supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government and the Tunisian government (No. NRF2012K1A3A1-A09026959).

REFERENCES

[1] R. Belleazreg, N. Boudriga, and S. An, "Border surveillance using sensor based thick-lines," in *the proceedings of the 27th International Conference on Information Networking (ICOIN 2013)*, Bangkok, Thailand, January 2013, pp. 221–225.

[2] D. krichen, W. Abdallah, and N. Boudriga, "WSN-based flutter control application for aircraft wings structural health monitoring," in *the proceedings of the 29th Symposium on Applied Computing (SAC 2014)*, Gyeongju, South Korea, March 2014.

[3] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *Communications Magazine, IEEE*, vol. 40, no. 8, pp. 102–114, August 2002.

[4] M. I. Salam, P. Kumar, and H. Lee, "An efficient key pre-distribution scheme for wireless sensor network using public key cryptography," in *proceedings of the sixth International Conference on Networked Computing and Advanced Information Management (NCM 2010)*, Seoul, South Korea, August 2010, pp. 402–407.

[5] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *proceedings of the 9th ACM conference on Computer and communications security, CCS'02*, Washington, DC, USA, November 2002, pp. 41–47.

[6] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *proceedings of the IEEE Symposium on Security and Privacy, SP03*, Berkeley, California, May 2003, pp. 197–213.

[7] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Transactions on Information and System Security TISSEC*, vol. 8, no. 2, pp. 228–258, May 2005.

[8] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *proceedings of the Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, INFOCOM 2004* , March 2004, pp. 586–597.

[9] S. A. Çamtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," *IEEE/ACM Transactions on networking*, vol. 15, no. 2, pp. 346–358, April 2007.

[10] Y. Cheng and D. P. Agrawal, "An improved key distribution mechanism for large-scale hierarchical wireless sensor networks," *journal of ad hoc Networks*, vol. 5, no. 1, pp. 35–48, January 2007.

[11] X. Du, Y. Xiao, S. Ci, M. Guizani, and H.-H. Chen, "A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks," *IEEE Transaction on wireless communications*, vol. 8, no. 3, pp. 1223–1229, March 2009.

[12] V. Thiruppathy Kesavan and S. Radhakrishnan, "Secret key cryptography based security approach for wireless sensor networks," in *proceedings of the International Conference on Recent Advances in Computing and Software Systems RACSS 2012*, Chennai, April 2012, pp. 185–191.

[13] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography," in *First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, October 2004, pp. 71–80.

[14] Y. Zhang, C. Wu, J. Cao, and X. Li, "A secret sharing-based key management in hierarchical wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 2013, pp. 1–7, 2013.

[15] W. Abdallah, N. Boudriga, D. Kim, and S. An, "An efficient and scalable key management mechanism for wireless sensor networks," in *the proceeding of the 16th international Conference on Advanced communication technology (ICACT 2014)*, Phonix Parc, South Korea, February 2014, pp. 686–692.

[16] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Journal of Computer Communications*, vol. 30, no. 11-12, pp. 2314–2341, September 2007.

[17] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," in *Proceedings of the 2nd international conference on Embedded networked sensor systems, SenSys '04*, 2004, pp. 162–175.

[18] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, Washington D.C, October 2003 2003.

[19] Q. Jing, J. Hu, and Z. Chen, "C4w: An energy efficient public key cryptosystem for large-scale wireless sensor networks," in *proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems MASS 2006*, Vancouver, BC, October 2006, pp. 827–832.

[20] W. Zhang, S. Zhu, and G. Cao, "Predistribution and local collaboration-based group rekeying for wireless sensor networks," *Journal of Ad Hoc Networks*, vol. 7, no. 6, pp. 1229–1242, August 2009.

[21] X. He, M. Niedermeier, and H. de Meer, "Dynamic keymanagement in wireless sensor networks:asurvey," *Journal of Networkand Computer Applications*, vol. 36, no. 2, pp. 611–622, March 2013.

[22] S. Zhu, S. Setia, and S. Jajodiadd, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, no. 4, pp. 500–528, November 2006.
[23] R. Divya and T. Thirumurugan, "A novel dynamic key management scheme based on hamming distance for wireless sensor networks," *International Journal of Scientific and Engineering Research*, vol. 2, no. 5, pp. 1–7, May 2011.
[24] X. Zhang, J. He, and Q. Wei, "Eddk: Energy-efficient distributed deterministic key management for wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, 2011.
[25] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *proc. of the third IEEE International Conference on Pervasive Computing and Communications PerCom 2005*, March 2005, pp. 324–328.
[26] S. K. Gupta, N. Jain, and P. Sinha, "Clustering protocols in wireless sensor networks: A survey," *International Journal of Applied Information Systems*, vol. 5, no. 2, pp. 41–50, January 2013, published by Foundation of Computer Science, New York, USA.
[27] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, pp. 203–209, 1987.
[28] G. Ateniese, M. Steiner, and G. Tsudik, "New multiparty authentication services and key agreement protocols," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 4, pp. 628–639, April 2000.
[29] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, November 1979.

Walid Abdallah is an Assistant Professor at the aviation school of Borj Elamri, Tunisia. He received his PhD in Information and communication technologies and the Diploma of engineer in telecommunications from the School of Communications Engineering (Sup'Com), Tunisia. He received his Master Diploma from the National School of Engineer of Tunis (Tunisia). From 2001 to 2005 he worked for the National Digital Certification Agency (NDCA, Tunisia) and from 1997 to 2001 he worked for the national telecommunication operator (Tunisia Telecom). Currently, he is a member of the Communication Networks and Security Lab, where he is conducting research in optical networks and wireless sensor networks.

Noureddine Boudriga is an internationally known scientist/academic. He received his PhD in algebraic topology from University Paris XI (France) and his PhD in computer science from the University of Tunis (Tunisia). He is currently a full Professor of Telecommunications at the University of Carthage, Tunisia and the Director of the Communication Networks and Security Research Laboratory (CNAS). He has served as the General Director and founder of the Tunisian National Digital Certification Agency. He is the recipient of the Tunisian Presidential award in Science and Research (2004). He was involved in very active research and authored and co-authored many journal papers, book chapter, and books on networks and security.

Daehee Kim received the B.S. degree in Electronics Engineering from Yonsei University, Korea, in 2003 and M.S. degree in Electronic and Computer Engineering from Korea University, Korea, in 2006. Currently, he is working for Ph.D. degree on Electronic and Computer Engineering in Korea University, Korea. His research interests include the wireless sensor network, LTE, and security in wireless networks.

SunshinAn received the B.S. degree from Seoul National University, Korea in 1973, and the M.S. degree in Electrical Engineering from KAIST (Korea Advanced Institute of Science and Technology), Korea in 1975 and the Ph.D. degree in Electric and Information from ENSEEIHT, France in 1979. He joined the faculty of Korea University in 1982, where he is currently a Professor of Electronic and Computer Engineering. Prior to joining Korea University, Prof. An was Assistant Professor of Electronic Engineering in Ajou University, Suwon, Korea. He was with NIST (National Institute of Standards and Technology) in U.S.A., as a visiting scientist in 1991. His research interests include the distributed system, communication networks and protocols, information network, intelligent network, multimedia communication system, wireless sensor network and mobile RFID network.

An Efficient LSDM Lighting Control Logic Design for a Lighting Control System

Sung-IL Hong, Chi-Ho Lin

Schools of Computer, Semyung University, 65- Semyung-ro, Jecheon, Chungbuk, Korea

megadriver@hanmail.net, ich410@semyung.ac.kr

***Abstract*—in this paper, we propose an efficient LSDM lighting control logic design for a lighting control system. The proposed LSDM lighting control logic is designed according to the operating conditions by dividing them into the signal control part for the I/O data bus and the timer/counter part for the clock signal control. Also, the control logic is transmitted to the MCU through a data bus based on the environmental information provided by each sensor node. The power dissipation rate of the proposed LSDM lighting control logic was measured in order to demonstrate the efficiency of the applying the control system. In addition, it was demonstrated that the proposed design is effective for the reduction of overall power consumption.**

***Keyword*—Control logic, LSDM, Lighting control, Signal control, Power dissipation, MCU**

I. INTRODUCTION

THE field of lighting design in the 21st century is being developed based on intelligence and automation technology, because the LED lighting device performance was improved quickly in recent years. The LED lighting device needs control logic for LED emitting. The LED lighting is commonly used in lighting devices by configuring to one module the multiple LED. The power consumption of LED affects the life of the LED lighting device by changing the internal temperature of the LED through the operation of the control logic. Also, the LED lighting control system should be provides exceptional identification skills and high color rendering by considering the energy savings [1-6].

The existing lighting device is not made as a complicated control circuit design, in order to implement the simple on-off function according to operation of the sensor. But, the existing lighting control logic for the LSDM (LED streetlight dot-matrix module) control has problems when operating by using each different device drivers and control programs. The lighting control logic for LSDM is sensitive device that directly affects the light output of LED, reliability, efficiency, and life. Also, the LED lighting device is required to be designed by using MCU, because many features can be controlled and operated [7-8].

The current flowing through the LED determines the brightness, and the internal power consumption will change the internal temperature of the LED. Therefore, the lighting control logic is a sensitive device that is related to LED's brightness, reliability, efficiency, long-lasting life, etc., because the operating temperature affects the life of the LED. There have been various studies performed on LED lighting control logic to develop optimal performance of the system configuration or the circuit. However, these researches are incomplete when considering the technology needed to reflect optimal design with modeling of the LSDM lighting control logic.

The existing street lighting control system has been operated by design providing the ability to distinguish objects only to pedestrians or motorists than the light functionality. As a result, the lighting device control system needs to be designed to ensure the safety of pedestrians via a signal placed above the road, using a variety of add-ons. For troubleshooting in this study, we propose the design of an efficient LSDM lighting control logic for a lighting control system using the MCU by considering the compatibility of the devices and the scalability.

II. LSDM LIGHTING CONTROL LOGIC

A. LSDM Control Logic

The ATmega128 is downloaded to your system by compiling the lighting control program created for the control of LSDM with the kernel, the device drivers, and the file systems. The LSDM lighting control logic is used to control the LSDM by configuring the decoders, the drivers, the latches, and the shift registers.

Figure 1 shows the configuration of the LSDM lighting control systems. In this paper, efficient control logic for the LSDM operation is designed by configuring the LSDM as signal controller, timer, and counter parts. The LSDM control signal can be sent to the LSDM lighting control by operating the control logic with the program execution. The LSDM lighting control logic was designed by dividing the controls into the signal control part for the I/O data bus and the timer/counter part for the clock signal control according to operating conditions.

Manuscript received May 30, 2014.

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the Human Resource Development Project for SoC support program (NIPA-2014-H0601-14-1001) supervised by the NIPA (National IT Industry Promotion Agency).

Sung-IL Hong is with the School of Computer, Semyung University, 65 Semyung-ro, Jecheon, Chungbuk, 390-711, Korea. e-mail: (megadriver@hanmail.net).

Chi-Ho Lin is with the School of Computer, Semyung University, 65 Semyung-ro, Jecheon, Chungbuk, 390-711, Korea. e-mail: (ich410@semyung.ac.kr).

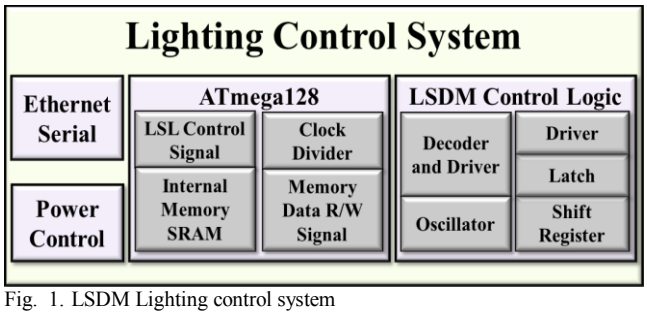


Fig. 1. LSDM Lighting control system

Figure 2 shows the configuration of the LSDM lighting control logic. The control logic is used as a decoder for selected lighting line by considering expansion of the LSDM. The I/O of the lighting control data uses the latch for control. Also, the control logic outputs the lighting data as LSDM uses the driver vertically and horizontally. The oscillator is designed to provide clock synchronization on all circuits using the internal oscillator circuit of ATmega128. To enable this the signal is received from ATmega128 for data output by repeating the latch process after a certain period of time. The R-Data and G-Data are used with the data for lighting of the LSDM. The A0 to A2 of 3-bit address lines are designed to be the line selection of LSDM by serial connection of up to maximum of eight. It outputs the lighting line selection signal of LSDM, because the LSDM I/O data signal controller can be controlled by selecting the LSDM connected as serial by adding a 3-bit decoder. In this case, the LSDM will light up by shifting the lighting data values using a shift register. The anode and the cathode driver are output as LSDM by receiving the lighting data signal of the rows and columns.

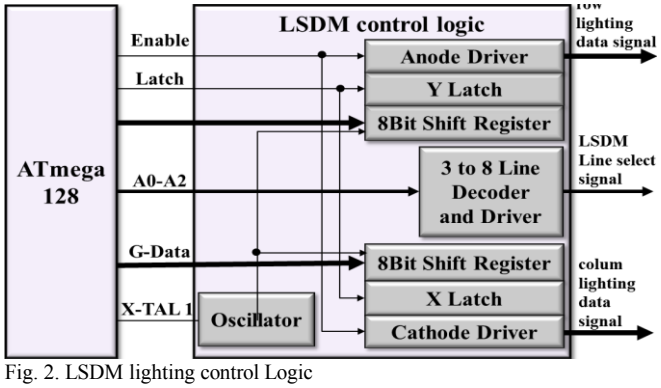


Fig. 2. LSDM lighting control Logic

B. I/O Data Signal Control

The I/O data signal flow of the control logic for LSDM control is entered through LSDM control logic, and the data output pin is determined depending on the address of the ATmega128. It uses address from 0x2500 to 0x2800 for the LSDM control, and stores in the internal memory by applying simultaneously to the data, address, and clock. If the data are read in the control logic of LSDM, the signal and data from ATmega128 is entered into the LSDM, according to the clock and latch signal. When the data is output into the control logic of LSDM, it is entered into the LSDM data when RW output signal is 1. The LSDM input data signal control part is selected and the control is used as the serial connecting LSDM by adding the 3-bit decoder that can be extended, because I/O pins are not simply I/O functionality. It outputs the line selection signal for lighting of LSDM. In this case, the LSDM input data signal control part will light up the LSDM by shifting the lighting data value using the shift register. The anode and the cathode driver will output to LSDM, the lighting data signal of the rows and columns through the shift register and the latch. Figure 3 shows the control flow of LSDM I/O data signal.

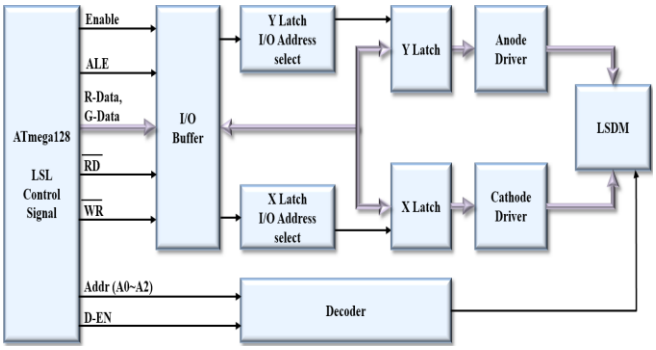


Fig. 3. LSDM control signal flow

Figure 4 shows the configuration default value of the optimization register. The control logic is used the output port C from port A on ATmega128 for data processing. It uses port G for controlling using address latch signal and R/W strobe signal for memory. The signal of the R/W signal roughly accesses the memory to the I/O buffer, and the address latch etc. in order to light up the LSDM. A port that is used at the I/O of the lighting data signals for LSDM lighting control can be the individual bits control when used as general-purpose I/O ports. Therefore, it is to be read/written as lighting data of LSDM using the PORTx data register (Data Register) that corresponds to the output and the DDRx (Data Direction Register) that sets the direction of I/O.

	bit	7	6	5	4	3	2	1	0
DDRx		DDx7	DDx6	DDx5	DDx4	DDx3	DDx2	DDx1	DDx0
	read / write	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
	initial value	0	0	0	0	0	0	0	0

	bit	7	6	5	4	3	2	1	0
PORTx		Px7	Px6	Px5	Px4	Px3	Px2	Px1	Px0
	read / write	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
	initial value	0	0	0	0	0	0	0	0

Fig. 4. LSDM lighting signal control registers

The data for controlling the flow of input and output signals of the LSDM is set to the direction and output of the input and output data, depending on the settings of the DDRx and the PORTx. In the DDRx register sets the input or output when each bit value is 0 or 1 using the 8-bit from 0 to 7. The PORTx register stores the value of the logical output port and verifies DDRxn bit setting contents of the PORTx register. Also, it is designed to load the status value of the corresponding port pin using the PINxn (Port Input Pins Register) bit register. In this case, the PINxn register bits are synchronized in order to optimize the input and output values in order to avoid the intermediate situation lasting phenomenon, whether the bit value is 0 or 1. Table 1 shows the values that the PORTx data register are used for processing of data signals for the lighting control on LSDM.

TABLE 1. $PORT_X$ DATA REGISTER VALUE

DDRx	PORTx			
	~row[1]	~row[2]	~row[3]	~row[4]
0xff	0xff	0xdd	0x01	0xee
	0x01	0x55	0xff	0xaa
	0xff	0x55	0x80	0xaa
	0x80	0x55	0xff	0xaa
	0xff	0x55	0x01	0xaa
	0x01	0x55	0xff	0xaa
	0xff	0x55	0x80	0xaa
	0x80	0x77	0xff	0xbb

The DDRx register value is set to 0xff to be used as the row-by-row lighting control data, with the PORTx register output used as bit-by-bit. It was designed to allow controlling according to the periodic pulse outputs by specifying an output data value of PORTx register.

C. The Timer/Counter for Controlling of LSDM Clock Signal

The LSDM lighting control system requires a periodic pulse output in order to control the LSDM and ATmega128 due to the synchronization. The LSDM control logic behavior cuts off the clock supply using sleep mode individually, providing a separate clock to each part to reduce the power consumption in the timer/counter part. The LSDM control logic behavior avoid fast-paced change of frequency for stable operation of the control logic when you use a separate clock. The timer/counter initial state is designed to be used by changing to other content appropriate for the user environment using the ISP or parallel programmer. The LSDM control logic uses the XTAL divide control register (XDIV) by setting the initial value to 0x90 for the continued use of the same frequency and to reduce the power consumption. Figure 5 shows the default setting values of the XDIV for the control of demultiplying.

Bit	7	6	5	4	3	2	1	0	
	XDIVEN	XDIV6	XDIV5	XDIV4	XDIV3	XDIV2	XDIV1	XDIV0	XDIV
Read/write	r/w	r/w	r/w	r/w	r/w	r/w	r/w	r/w	
Initial value	1	0	0	0	0	1	0	0	

Fig. 5. The XDIV default setting value

The clock source used in the LSDM lighting control logic is 16MHz. Therefore, a clock source has a set value to activate clock frequency, which is set to match the control program during behavior of the control logic. A frequency is set dividing 128 for the use of the control logic.

D. LSDM Control Algorithm

In this paper, the LSDM control algorithm to be used in the LSDM lighting control logic is designed to control the appropriate use of the LSDM to ensure low cost. The LSDM control algorithm is converted to the digital signal of the analog signal using the illuminance sensor, and it can be a pattern control according to the changes in the brightness of the light. . If the convert value of the ambient light is less than the default value, LSDM is continuously illuminated. If the converted value is large than the default value, LSDM will turn off by shutting down all processes automatically to avoid unnecessary energy consumption. This method will improve the energy efficiency of LED lighting device.

Figure 6 shows the control algorithm for the behavior state of the LSDM, controlled by a pre-set time schedule. The control algorithm flow for the LSDM control is defined by the type of I/O data, and transmitted to the MCU using the data bus by starting illuminance measurement and motion detection through installed sensor on lighting device. The control system from MCU can calculate the illuminated level depending on the set control method by correction of the I/O data, and decide whether to the level is maintained by comparing the results. The LSDM control algorithm determines whether to adjust level by comparing with the existing measurement values with the data according to the illumination measurement and motion detection. Therefore, the lighting control system was applied to the control algorithm for an efficient LSDM control.

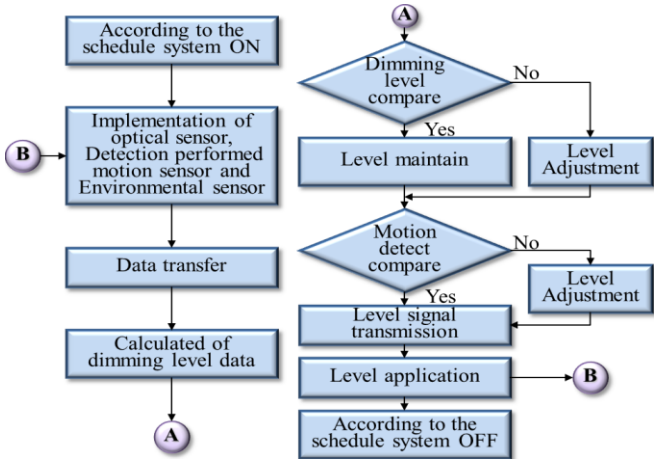


Fig. 6. LSDM control algorithm

III. THE EXPERIMENTAL RESULT

In this paper, a proposed LSDM lighting control logic measured the power of dissipation rate of the control logic on the lighting status by checking the control status, using LSDM lighting control data value of input and output from lighting control system. The Lighting control data confirmed data input for LSDM control that applies to the changes at any time by user needs.

The existing LSDM lighting control logic replaces the street lighting device from the lighting method using sodium lamps and metal halide lamps to LSDM. In addition, the used LED module does not require an MCU, because to light up by placing as the line forms or an array form. The lighting control method is simply implemented with an on/off function by measuring the illuminance. For this reason, the street lighting will be used in the case where lighting shows excessive brightness in comparison to the illuminance of the surrounding, avoiding unnecessary power consumption. The proposed LSDM lighting control logic is lighting control based on factors such as the temperature, humidity, illuminance, vehicle, and pedestrian traffic around streetlights, because the MCU is used so that we can adjust the brightness using PWM (Pulse Width Modulation) or change the lighting pattern by placing the LED module in the form of a matrix.

In this paper, we designed control logic for controlling the LSDM of efficient lighting control system, and the control program was written to operate in device driver and LSDM. The drivers and written programs were preferences using minicom and RS232C communication through the serial port in order to download to the lighting control system. In addition, an environment was set up of the host PC and trivial file transfer protocol (tftp), and transmits. We used this for the cross compiler, because the compiler should behave differently in the host PC and the generated executable file behavior system. The boot loader was compiled for configuring the lighting control system, and the download. Also, we were compiling with the kernel, the file system, and the device drivers and we created a lighting control program. The host PC checked the status of lighting control by downloading the program into the lighting control system through ethernet or serial.

Figure 7 shows the experimental environment of the host PC and the lighting control system had serial connection. It was configured so that it can control behavior of LSDM through the network on client PC in other places. The LSDM controlled lighting by applying the dynamic driving method constructed as 8x8 dot type.

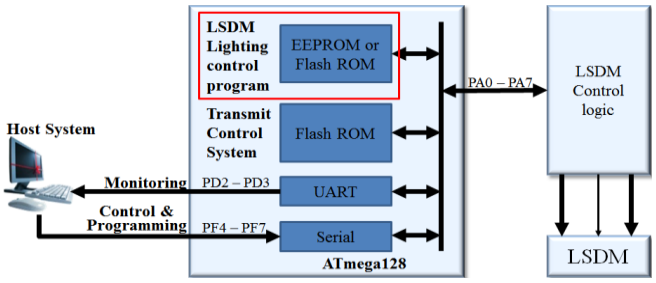


Fig. 7. Experiment environment

The experimental environment of figure 7 confirmed the lighting control status by efficiently controlling the LSDM control logic through I/O LSDM lighting signal data values by operation of LSDM lighting control program.

The lighting control data was confirmed by the data input for controlling the LSDM, because it was applied so that it can be efficiently changed at any time according to the user needs. Figure 8 shows the timing diagram of the lighting control data of the LSDM lighting control logic entered through PORTx of the ATmega128 with application of the LSDM lighting control algorithm. The lighting control data represents the value of the ~row[1] in the register-values for the control signals of Table 1, and the data were entered sequentially from ~row[1] to ~row[4].

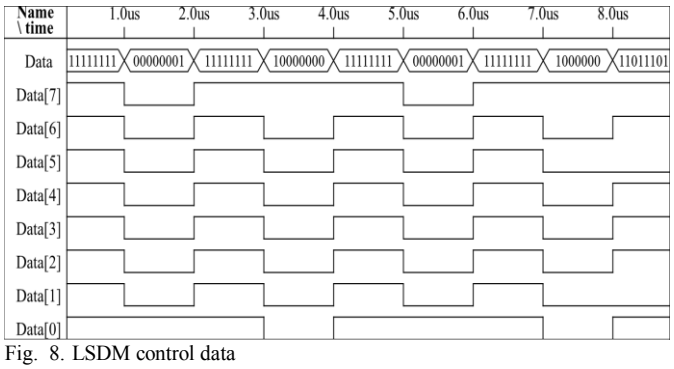


Fig. 8. LSDM control data

Figure 9 shows the time chart of the experimental results on the LSDM lighting control logic operation state of lighting control system that based on the control data entered from the ATmega128 by the LSDM control algorithm.

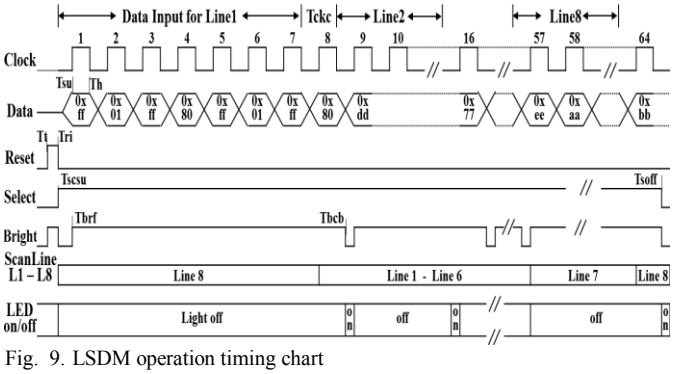
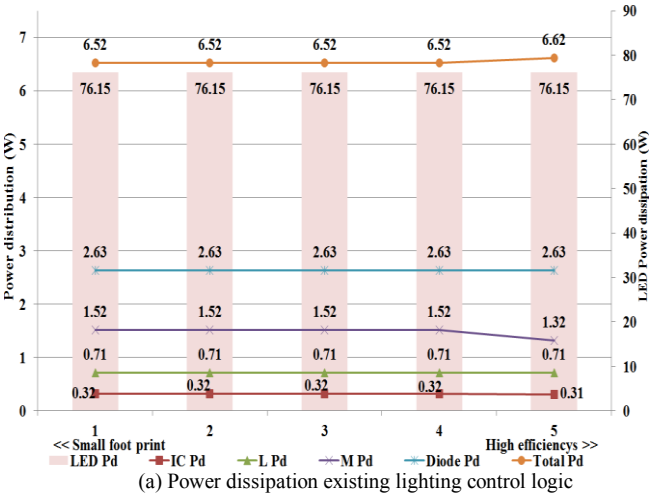


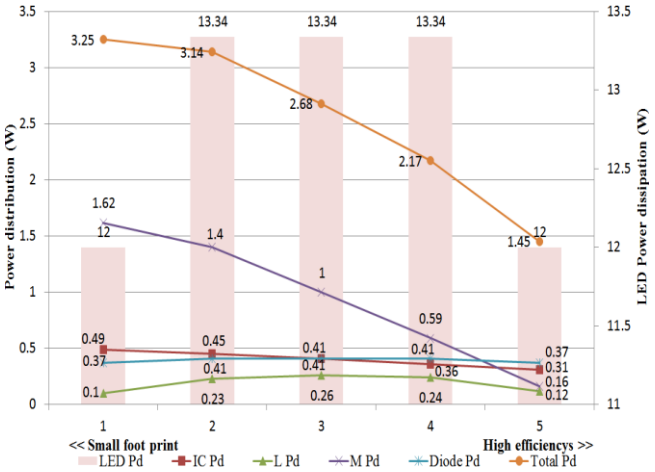
Fig. 9. LSDM operation timing chart

The ATmega128 enters the clock signal to the LSDM for data input and display, and enters the data through the PORTx for LSDM lighting. In addition, the reset signal is entered as "H" in order to counter the value initialized. In this case, the LSDM is not deleting the stored data even though the reset signal is input as "L". If the selected input signal is "H", the data input control is displayed with the data input. If the data input is "L", it is displayed by the set that disables the stored data. The brightness of the LSDM are controlled by determining the pulse width of the “tckc” when the selected signal for lighting control is entered as "H", because it can control the brightness by adjusting the pulse width on the PWM. The LSDM control logic receives a signal to check the on/off status using a dynamically-driven, and it could obtain off results of LSDM while the signal is being input.

Figure 10 is a graph showing measured results of the power dissipation rate by comparing the footprint and the efficiency. For the measured result of the average value of power dissipation rate, IC power dissipation (IC Pd) were increased 0.086W, but LED power dissipation (LED Pd) were decreased 12.80W as 63.34W from 76.15W. The total power dissipation (Total Pd) were decreased 4.01W as 2.53W from an average of 6.54W. The result of comparison to the power dissipation rate of control logic obtained effective results of power dissipation reduction and the power dissipation rate of the proposed control logic was reduced by 61.19% when compared with the conventional control logic.



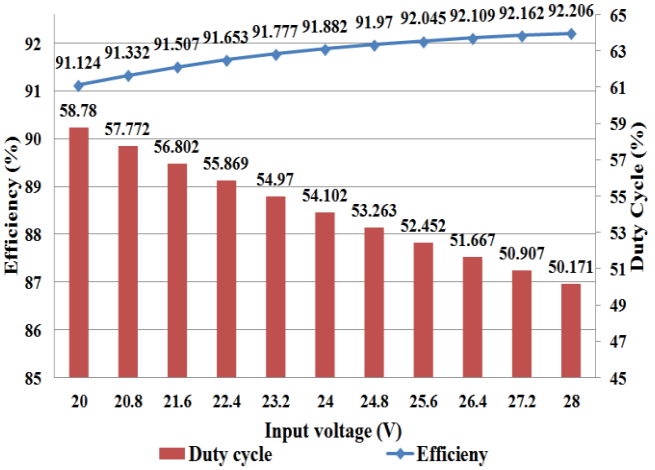
(a) Power dissipation existing lighting control logic



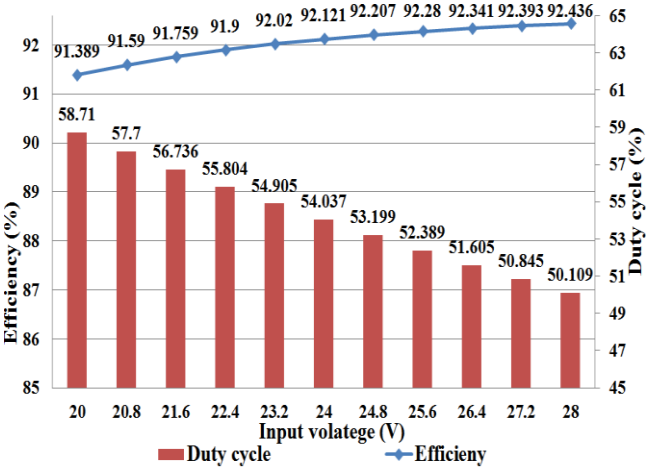
(b) Power dissipation proposed lighting control logic

Fig. 10. Power dissipation

Figure 11 shows the measured results of efficiency and the duty ratio for LSDM operation state by comparing the input voltage when applying the LSDM lighting control algorithm.



(a) Existing lighting control logic



(b) Proposed lighting control logic

Fig. 11. Efficiency and duty cycle

In Figure 11(a), the efficiency of the existing control logic could be obtained at an average efficiency of 91.79% by measured to increasing 1.08% that it measured the 91.124%, when the minimum input power is 20V; and it is measured at 92.206% when the maximum input power is 28V. The duty cycle could obtain an average duty cycle of 54.25% by measured to decreasing 14.64% that it measured the 58.78% when the minimum input power is 20V, and measured at 50.171% when the maximum input power is 28V. In figure 11(b), the efficiency of the proposed control logic was obtained at an average efficiency of 92.03% by measured to increasing 1.14%, it measured at 91.389% when the minimum input power is 20V, and at 92.436% when the maximum input power is 28V. The duty cycle was obtained at an average duty cycle of 54.18% by measured to decreasing 14.65%, it was measured at 58.71% when the minimum input power is 20V, and at 50.109% when the maximum input power is 28V.

Figure 12 shows the comparative results of development costs for efficiency by comparing the area occupied of the existing control logic and the proposed control logic. The BOM (Bill of Materials) cost of the control logic was estimated by the primarily considering efficiency than the area occupied.

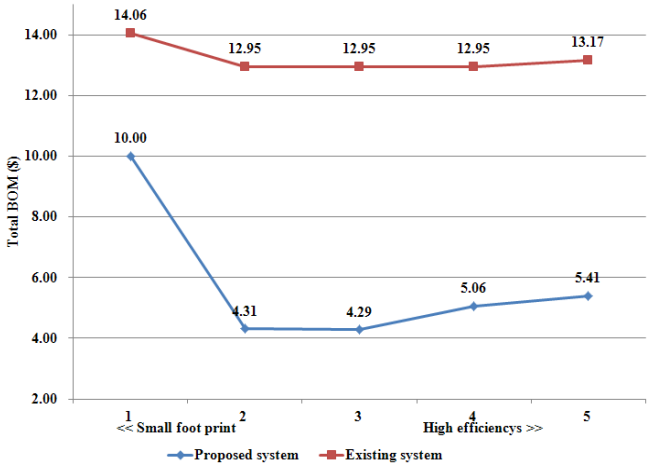


Fig. 12. Total BOM cost of system

IV. Conclusion

In this paper, we proposed an efficient LSDM lighting control logic design for a lighting control system using the LSDM control algorithm. In this paper, a proposed LSDM lighting control logic was measured to power dissipation rate of the control logic on LSDM lighting status, by downloading the LSDM control algorithm into the control logic through serial port. LSDM control algorithm is able to efficiently control the lighting control system by the lighting control signal data value of input and output into LSDM lighting control logic.

As a result of checking the lighting control status, we analyzed the results by measuring the efficiency and the duty ratio for the input power. The efficiency of the proposed LSDM lighting control logic was obtained at an average efficiency of 92.03% by measured to increasing 1.14%. The duty cycle was obtained at an average duty cycle of 54.18% by measured to decreasing 14.65%. As a result, the proposed LSDM lighting control logic was proved to be more effective than the existing control logic for improving the overall efficiency of the lighting control system. The LSDM lighting control logic based on MCU makes it possible to utilize lighting control with real-time monitoring when configuring the sensor network using zigbee communication method.

In the future, LED street lighting control system must be applied to the LSDM lighting control logic to increase the utilization of the proposed LSDM lighting control logic, and more research must be carried out for the establishment of an efficient street lighting management system.

ACKNOWLEDGMENT

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the Human Resource Development Project for SoC support program (NIPA-2014-H0601-14-1001) supervised by the NIPA (National IT Industry Promotion Agency).

REFERENCES

[1] Seoul Semiconductor, Z-POWER LE D Series Technical Data sheet for W4218X, www.zled.com, 2007.

[2] Sang-Bin Song, In-Seon Yeo, "The Thermal and Circuits Design of an LED Bulb Considering Temperature Property", *Institute of Electrical Engineers*, Vol 56, No 7, pp.1261-1267, 2007.

[3] Mi-Young Lee, Woo-Hee Lee, Jun-Ha Lee, Hoong-Joo Lee, "Design of LED Driving Circuits to Detect Degradation Characteristics", *The Korea Institute of Power Electronics, Power Electronics Conference*, pp.81-83, July. 2005.

[4] Jung Kwang-Sung, Kim Chang-Beom, Moon Cheol-Hong, "LED Control Board Design using Xilinx Spartan3 FPGA Module", *KIEE, CICS '09*, pp. 331-332, 2009.

[5] H. Broeck, G. Sauerlander, and M. Vendt, "Power Driver Topologies and Control Schemes for LEDs", *Proc. IEEE. APEC*, pp. 1319–1325, 2007.

[6] Y. Hu and M. Jovanovic, "LED Driver With Self-Adaptive Drive Voltage", *IEEE, Trans. on Power Elec*, vol 23, no. 6, pp. 3116-3125, 2008.

[7] Soo-Bin Han, Suck-In Park, Eugine Song, Hak-Guen Jeoung, Bong-Man Jung, Gue-Duk Kim, "Overview of Classification and Characteristics of Recent LED drive IC", *KIEE AutumnAnnualConference*, pp. 105-107, 2008.

[8] Borbély, A., A. Sámson, and J. Schanda. "The Concept of Correlated Color Temperature Revisited", *Color Research & Application*, vol 26, no. 6, pp.450–457, 2001.

Sung-IL Hong received B.S and M.S. degrees in sciences and education from Semyung University in 2007 and 2009, respectively. Since August 2009, he enters to the Ph.D course. His current research interests include SoC CAD, ASIC Design, CAD Algorithms, SoC Design, RTOS and Embedded Systems. Now, he studies the lighting control systems and remote control & management system.

Chi-Ho Lin received B.S and M.S. degrees in Engineering from Hanyang University in 1985 and 1987, respectively. He also received Ph.D degree in Engineering from Hanyang University in 1996. Since March 1992, he has been with the school of computer in the semyung university as the professor. His current research interests include SoC CAD, ASIC Design, CAD Algorithms, SoC Design, RTOS and Embedded Systems. Now, he studies the lighting control systems and remote control & management system.

A Study on the Performance Evaluation of Container Tracking Device based on M2M

Eun Kyu Lee*, Hyung Rim Choi*, Jae Joong Kim*, Chae Soo Kim*

*Intelligent Container R&D Center of Dong-A university, 37 Nakdong-Daero 550 beon-gil Saha-gu, Busan, Korea 604-714

jabanora@dau.ac.kr, hrchoi@dau.ac.kr, jjkgb@dau.ac.kr, cskim@dau.ac.kr,

***Abstract*—A M2M-based container tracking device is a device installed inside container to detect the open/shut status of container door. In terms of the main features of the device developed in this study, it can not only detect the open/shut status of container door but also perform inquiries on the status of inside container environment and shocks received by container during its transportation upon installing temperature, humidity and shock sensors. This paper focused on the performance evaluation via trial operational test of container safe transportation surveillance & tracking, that monitors in real-time the security status of freight from departure to arrival.**

***Keywords*— Container, Tracking, M2M, Performance evaluation**

I. INTRODUCTION

According to the Container Tracking and Security Market 2012-2022 analysis, companies and organizations in many areas have a need to track and ensure security of their freight assets being transported around the world. In addition to increasing terrorists' threats, freight thefts and biological weapon terror threats, many containers become lost during transportation with increasing cost of goods that go bad. Accordingly, protection of containers through tracking and ensuring security is effectively being utilized in the commercial field, and an analysis forecasts that the container tracking and security market will see a strong growth in the next decade [1]. In particular, as the container tracking market is being rapidly growing since 2000, there is a possibility that it could see a significant scale of revenue. The world is engulfed in the wave of economic recession and there still are regions that are facing a crisis. However, the world's trade volumes are increasing exponentially. The container transportation industry might be experiencing difficulties but the number of containers (TEU) has been increasing in the last several years, which will continue on as it become a catalyst of the growth container tracking and security market. In 2012, the US announced an act that mandates all container freights coming into the US to be installed with security devices certified by the US Customs to verify that containers have not been opened during transportation. In addition to the US, the EU reinforced its logistics security by enacting 'marine & port facilities security regulations' that even mandated the recommendations in the ISPS Code provisions of the International Maritime Organization (IMO). It also legalized logistic security regulations that focus on fulfilling the corporate logistics security system (SAFE Framework) of the World Customs Organization (WCO) with continuous efforts to reinforce logistics security by developing and operating an import freight scanning system. Advanced nations including the US and the EU are developing electronic seal and container security devices and standardizing technologies to prevent any bottleneck in logistics flow while reinforcing security measures. They are moving quickly to preoccupy the market in addition of increasing R&D investment. Representative electronic security devices of freight container include electronic seal (eSeal) using active RFID (Radio Frequency Identification) technology and container security device (CSD) of IEEE 802. 15.4b. Active RFID with longer recognition distance compared to passive RFID tag that can be easily applied to metal object is being used for port & inland logistics transportation management system and container protection for metal containers. The eSeal that uses the technology in this paper is installed on the outside door handle of freight container. Upon detecting any abnormal opening of container door by an outsider or any attempt to open door abnormally, it notifies nearby reader while maintaining a log.

The CSD is installed inside freight container to detect any loss or theft of container, as well as any attempt to infiltrate container. While there isn't any international standard for container security device currently, the US Department of Homeland Security (DHS) has announced a technical specification required by the US Customs and Border Protection (CBP) [2]. Accordingly, various companies centering on GE (US) established Commerce Guard and Savi (US) and CIMC (China) are actively carrying out related R&D activities. However, in the midst of a situation where companies across the world are competing fiercely, there isn't any competitive product in Korea that could compete with foreign products as of now.

Manuscript received April 25, 2014. This work was supported by the Ministry of Land, Infrastructure and Transport, Korea.(KAIA-2013).

Eun Kyu Lee Author is with the Intelligent Container R&D Center, Dong-A university, Busan Korea 604-714 (e-mail: jabanora@dau.ac.kr).

Hyung Rim Choi Author is with the Intelligent Container R&D Center, Dong-A university, Busan Korea 604-714 (e-mail: hrchoi@ dau.ac.kr).

Jae Joong Kim Author is with the Intelligent Container R&D Center, Dong-A university, Busan Korea 604-714 (e-mail: jjkgb@ dau.ac.kr).

Chae Soo Kim Author is with the Intelligent Container R&D Center, (phone: +82-51-200-7690; fax: +82-51-200-7697; e-mail: cskim@ dau.ac.kr)

Accordingly, this paper explains the Advanced Container Security Device (ACSD). ACSD satisfies the user requirement of real-time identification of container position by applying M2M (Machine-to-Machine) technology that uses mobile communication technology. And to evaluate the performance of ACSD and system, we introduces the trial test result which has been applied to container freight being transported between Korea and Poland, while also verifying the reliability of the paper [5].

The composition of this paper is as follows. Chapter Ⅱ examines the future direction of development and advancement of electronic security devices through related researches and comparatively analyzes the features of container security products. Chapter III explains the CSD system using the ACSD developed in this paper. Chapter IV evaluates the system performance through a trial services domestically as well as between Korea and Poland. Chapter V will conclude this paper.

II. RELATED RESEARCH

This chapter examines the future direction of advancement of container security devices and comparatively analyzes the features of a competitive companies' products and ACSD.

Since the early years of logistics using container, plastic or metal "seal" of conventional bolt barrier was used through one or more door hasp mechanisms for container security. Since 2000 in which the importance of container security was emphasize along with IT advancement, eSeal was developed applying active RFID technology, which detects any abnormal opening/shutting of container door upon installing. However, eSeal has the weaknesses of easily breaking down as it is attached outside container door and not being able to be reused. Improving the weakness of eSeal, the development of CSD became active according to the CSD requirement document presented in 2007 by the US DHS for detecting any illegal opening/shutting of container door. As it is installed inside container, CSD can be reused. Since then, ACSD (Advanced Container Security Device) is currently being developed with improved performance, which not only detects any illegal opening/shutting of container door but also monitors inside the container and detects illegal immigrants. In terms of future direction, it is expected that intelligent container will be developed with devices that perform ACSD function are preinstalled inside container rather than separately attaching eSeal device to container. Table 1 compares and analyzes the features of M2M-based container tracking and security devices in commercialization.

TABLE 1
FEATURE COMPARISON

	Starcom	Kirsen
	TRITON	CMD500-S
Shape		
De/attachment	•Left wall	•Center
Weight	•150g	•1500g
Size	•195×96×40(㎜)	•200×150×100(㎜)
Communication	•Zigbee •CDMA, GSM option	•GSM •GPS, RFID option
Battery	•5000mAh Li-lon	•3 years (2 per day)
Position	•GPS	•GPS + Cellular
Status	•Door, illumination	•Illegal infiltration, temperature, humidity, shock, vibration, slope
Temperature	•-40℃-60℃	•-30℃-85℃

The two devices can be used in container security related areas such as the UD DHS CSI, SAFE Port Act, C-TPAT, 10+2 system, etc. Using a clamp type (C-Clamp) auxiliary device, Kirsen's CMD500-S is attached outside container door at the center and detects opening/shutting status of door using breach [3]. It also provides a log of changes in container status during transportation by installing temperature/humidity and shock detection sensors. Using magnet between container wall and door, Starcom Systems' TRITON is attached to detect opening/shutting status of container door by using proximity sensor [4]. It also provides a log of container status during transportation by attaching temperature/humidity sensor. However, CSD that does not include shock sensor cannot detect any shock received by container.

III. INTRODUCTION TO ACSD

The shape and framework of ACSD prototype and the definition of payload for data communication are as follow.

A. About the Prototype

Fig. 2 shows the parts of container security device. This device has been developed according to the requirements of the US DHS, marine shipping companies and shipper. The device is attached on crack between outside wall of container door and the door at an appropriate height at which freight will not be damaged. Using magnetic sensor, it detects container door opening/shutting status and provides a log of the status of container during transportation through temperature/humidity and shock sensors installed. As it is installed inside container, there is a low risk of damage for ACSD that can also be reused. It has been developed to allow communication at any parts of the world with communication stations as the device is M2M-based.

Fig. 1. The shape of ACSD

B. Framework

As shown in Fig. 2, the M2M-based container tracking system framework consists of container tracking device, interface and container tracking control information system. The container tracking device should collect information (position, temperature, humidity, shock, door status) required by global supply chain constituents and be usable even in poor logistics environment. The real-time communication interface needs to consist of interface with mobile carrier's communication station and protocol required for data collected from container tracking device to be sent to container tracking control information system. The container tracking control information system is software for displaying in real-time visual information to constituents of global supply chain once the data collected from container tracking device has been sent via real-time communication interface. The middleware of container tracking control information system consists of middleware that sends only required data to monitoring system by collecting and filtering data from container tracking device, and web-based monitoring system that displays in real-time via electronic map to users the data refined by middleware, and mobile-based system that can send information even via smart phone.

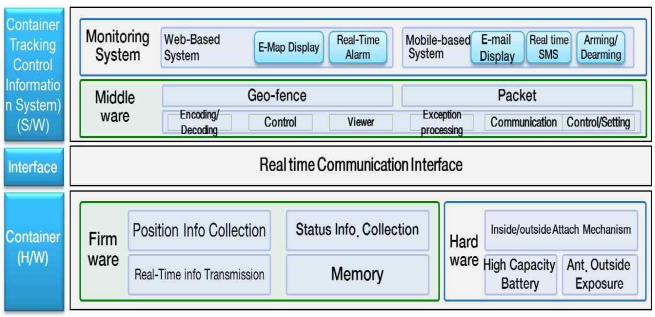


Fig.2. CSD Framework

C. Definition for Payload Data

As shown in Table 1, data being transmitted to/from container tracking device included device ID, status info such as position, temperature, humidity and shock, as well as battery and transmission cycle information. Such information was defined according to the features that can be provided by hardware and protocol rules.

Table 2. DATA DEFINITION

Classification	Content	Length
Index	Index of log stored in the device	2byte
Protocol ID	ID of corresponding protocol	1byte
Device ID	Unique number for distinguishing devices	8byte
Date & Time	Display of event occurrence and info transmission time	6byte
Position Data	Display of current position	11byte
Temp	Value of temperature measured in sensor module	2byte
Humid	Value of humidity measured in sensor module	2byte
Shock	Vector sum of the X, Y, Z axis of acceleration sensor	2byte
Door Status	Opened or closed	1byte
Remaining Battery Power	Display in % remaining battery power	1byte
Device On/Off	Display Device On, In-Process, Off status	1byte
Transmission Cycle	Cycle of transmitting information to server	1byte
RSSI	Display of signal reception sensitivity	1byte
Error Status	Storage of Error Code of error and malfunction of transmitted information	1byte

IV. DEMONSTRATION TEST

This chapter introduces a result of overseas trial test for demonstration and reliability check between Korea and Poland which was conducted to verify the performance of ACSD system developed in this research.

A. Demonstration Test

The ACSD system was applied to a container filled with freight being transported from Paju to Busan Port to Poland, as shown in Fig. 3, with the assistance from Company L to conduct an international trial service between Korea and Poland. The objective of the trial service was to verify the features during container marine transportation and it checked the status of complete transmission of data collected from the device to server to operating server DCP when the container installed with the device passes through the following base points.

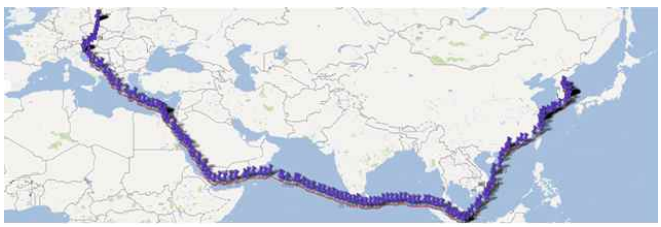


Fig.3. Test Section

TABLE 3. DATA TRANSMISSION AND RECEPTION ANALYSIS

Order	Section	Trans. Cycle (min)	Set Interval (min)	Trans. Frequency (Server Reception)			Trans. Omission Frequency
				Cycle Trans.	Interrupt	Total Reception	
1	Domestic	10	20	2	-	2	0
2	Domestic Inland → Incheon Port	60	360	6	10	16	0
3	Incheon Port → Belarus	180	34,560	191	22	213	1
4	Belarus → Destination (Poland)	60	1,320	22	-	22	0
Subtotal			36,260	221	34	255	-

B. Performance Evaluation

The main firmware features of the container tracking device, which are information collection, real-time information transmission/reception and memory storage features, are features that can be performed on the premise that the main hardware features explained earlier operate normally. This indicates that when the information collection, real-time information transmission/reception and memory storage features used during the trial operation operated normally, the main hardware features of the container tracking device also operated normally. In regards to the main firmware features of the container tracking device, which are information collection, real-time information transmission/reception and memory storage features, number of data transmitted according to information transmission cycle and number of data received will be analyzed for verification. Since the real-time information transmission/reception feature can operate with the prerequisite of information collection and memory storage features, normal operation of information collection and memory storage features can be also verified by analyzing the number of transmitted data and the number of received data.

It is expected that the total number of data transmitted according to the information transmission cycle set as shown in Table 3 would be 222 but the actual number of information received by server was 255 based on trial operation results. This is a sum of 221 times of transmission according to set cycle and 34 times of interrupted transmission that occurred by detecting through shock sensor and door opening/shutting. Except for the number of interruption from the exceptions that occur during transportation, the final number of reception was 221 that is short by one session from the initially expected number of transmission of 222. This is a result one session of information transmission that was omitted in the section transporting from Incheon Port to Belarus and it is estimated that one session of information transmission was omitted due to reasons of real-time information communication network infrastructure (communication station).

It was confirmed through such analysis of data transmission and reception frequencies according to information transmission cycle that the main firmware features of container tracking device used for the trial operation operated normally.

V. CONCLUSION

The M2M-based container tracking system framework presented and the system developed in this paper were evaluated for its performance through trial operation. The CSD system that has been verified through performance evaluation enables shipper and forwarders that need real-time tracking of container the most among the constituents of global supply chain to effectively establish their global supply chain plan. It is difficult to collect in real-time information required by users through conventional container tracking system. However, in the case of container tracking system presented in this paper, effective supply chain management can be expected such as inventory control and production management by collecting and utilizing in real-time container information (position, temperature, humidity, shock, door opening/shutting) required by users upon utilizing M2M real-time communication technology.

In addition, logistics companies such as forwarder, transportation and shipping companies directly verified freight arrival/delivery by utilizing their or partner's manpower at each logistics base point. Among the container tracking control information systems presented in this paper, the main middleware feature of Geo-fencing enables real-time verification of freight arrival/delivery in office. This feature allows logistics companies to save time and cost involved in verifying freight arrival/delivery status with the expected effectiveness of improving their credibility by notifying shippers that their freight is being transported safely.

Upon the logistics paradigm shift mentioned earlier and background of study, logistics security is being reinforced across the world through regulations and policies. The container tracking system according to the M2M-based container tracking system framework presented in this paper can satisfy safety/security regulations required in the US, Europe and Asia. Accordingly, it has the expected effectiveness of simplification of customs procedure and provision of swift clearance benefits at the level of global supply chain management.

REFERENCES

[1] Visiongain Ltd, The Container Tracking and security Market 2012-2022.
[2] U.S Department of Homeland Security Customs and Border Protection, Conveyance Security Device(CSD) Requirements, Version 1.2, December, 10, 2007
[3] Kirsen Ltd, Available: https://kirsenglobalsecurity.com/
[4] STARCOM Ltd, http://www.starcomsystems.com/
[5] Su Jin Kim, Guofeng Deng, Sandeep K. S. Gupta and Mary Murphy-Hoye, "Intelligent Networked Containers for Enhancing Global Supply Chain Security and Enabling New Commercial Value," in the 3rd Int'l Conf. on Communication System Software and Middleware (COM-SWARE'08), 2008.

Eun Kyu Lee is a Senior Researcher of Dong-A University. He received the B.S degree in Information Communication from Young Dong University, Korea in 1999 and M.S degree in Electronic Information Communication from Kunkok University, Seoul, Korea in 2001. He is currently a Ph.D. candidate in Electronic Information Communication from Kunkok University. His main research topics are active RFID and container security Device.

Hyung Rim Choi is a professor of Dong-A University. He received his Ph.D. degree in Management Science from KAIST in 1993. His main research topics are a RFID/USN application and Port and Logistics Systems.

Jae Joong Kim is a professor of Dong-A University. He received his Ph.D. degree in Civil Engineering from Seoul National University in 1989. His main research topics are a RFID/USN application and Port and Logistics Systems.

Chae Soo Kim is a professor of Dong-A University. He received his Ph.D. degree in Industrial Engineering from KAIST in 1999. His main research topics are a RFID/USN application and design & development of Port Logistics Systems.

Volume 3 Issue 4, Jul 2014, 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