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

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 7 Issue 4, July. 2018, ISSN: 2288-0003

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

GIRI
Global IT Research Institute

Journal Editorial Board

■ Editor-in-Chief

Prof. Thomas Byeongnam YOON, PhD.
Founding Editor-in-Chief
ICACT Transactions on the Advanced Communications Technology (TACT)

■ Editors

Prof. Jun-Chul Chun, Kyonggi University, Korea
Dr. JongWon Kim, GIST (Gwangju Institute of Science & Technology), Korea
Dr. Xi Chen, State Grid Corparation of China, China
Prof. Arash Dana, Islamic Azad university , Central Tehran Branch, Iran
Dr. Pasquale Pace, University of Calabria - DEIS - Italy, Italy
Dr. Mitch Haspel, Stochastikos Solutions R&D, Israel
Prof. Shintaro Uno, Aichi University of Technology, Japan
Dr. Tony Tsang, Hong Kong Polytechnic UNiversity, Hong Kong
Prof. Kwang-Hoon Kim, Kyonggi University, Korea
Prof. Rosilah Hassan, Universiti Kebangsaan Malaysia(UKM), Malaysia
Dr. Sung Moon Shin, ETRI, Korea
Dr. Takahiro Matsumoto, Yamaguchi University, Japan
Dr. Christian Esteve Rothenberg, CPqD - R&D Center for. Telecommunications, Brazil
Prof. Lakshmi Prasad Saikia, Assam down town University, India
Prof. Moo Wan Kim, Tokyo University of Information Sciences, Japan
Prof. Yong-Hee Jeon, Catholic Univ. of Daegu, Korea
Dr. E.A.Mary Anita, Prathyusha Institute of Technology and Management, India
Dr. Chun-Hsin Wang, Chung Hua University, Taiwan
Prof. Wilaiporn Lee, King Mongkut's University of Technology North, Thailand
Dr. Zhi-Qiang Yao, XiangTan University, China
Prof. Bin Shen, Chongqing Univ. of Posts and Telecommunications (CQUPT), China
Prof. Vishal Bharti, Dronacharya College of Engineering, India
Dr. Marsono, Muhammad Nadzir , Universiti Teknologi Malaysia, Malaysia
Mr. Muhammad Yasir Malik, Samsung Electronics, Korea
Prof. Yeonseung Ryu, Myongji University, Korea
Dr. Kyuchang Kang, ETRI, Korea
Prof. Plamena Zlateva, BAS(Bulgarian Academy of Sciences), Bulgaria
Dr. Pasi Ojala, University of Oulu, Finland
Prof. CheonShik Kim, Sejong University, Korea
Dr. Anna bruno, University of Salento, Italy
Prof. Jesuk Ko, Gwangju University, Korea
Dr. Saba Mahmood, Air University Islamabad Pakistan, Pakistan
Prof. Zhiming Cai, Macao University of Science and Technology, Macau
Prof. Man Soo Han, Mokpo National Univ., Korea
Mr. Jose Gutierrez, Aalborg University, Denmark

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

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

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

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

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

Dr. Che-Sheng Chiu, Chunghwa Telecom Laboratories, Taiwan
Dr. Chirawat Kotchasarn, RMUTT, Thailand
Dr. Fateme Khalili, K.N.Toosi. University of Technology, Iran
Dr. Izzeldin Ibrahim Mohamed Abdelaziz, Universiti Teknologi Malaysia , Malaysia
Dr. Kamrul Hasan Talukder, Khulna University, Bangladesh
Prof. HwaSung Kim, Kwangwoon University, Korea
Prof. Jongsub Moon, CIST, Korea University, Korea
Prof. Juinn-Horng Deng, Yuan Ze University, Taiwan
Dr. Yen-Wen Lin, National Taichung University, Taiwan
Prof. Junhui Zhao, Beijing Jiaotong University, China
Dr. JaeGwan Kim, SamsungThales co, Korea
Prof. Davar PISHVA, Ph.D., Asia Pacific University, Japan
Ms. Hela Mliki, National School of Engineers of Sfax, Tunisia
Prof. Amirmansour Nabavinejad, Ph.D., Sepahan Institute of Higher Education, Iran

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

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:

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

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.

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

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.

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

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,

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

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!

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

Volume. 7 Issue. 4

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

A solar power generation facility state monitoring system using drone aerial photographing

Younlae Lee*, Young-Geol Lee**, Hyunah Kim***, Minjae Park**

*R&D Center, KGI, LTD., South Korea

**Department of Computer Software, Daelim University, South Korea

***Division of General Studies, Kyonggi University, South Korea

candy143@daum.net, yglee@daelim.ac.kr, hyuna486@kgu.ac.kr, mjpark@daelim.ac.kr

***Abstract*—Recently, there has been a lot of interest and issues related to solar power generation, and accordingly, various studies related to the solar power facility are being carried out. We would like to describe a solar power generation facility state monitoring system during research related to solar facility research. Proposed system will be based on drone aerial photographing technology, analyzing photographing data, and managing facilities based on the collected data. This paper describes the process of data collection, processing, and management, and proves its contents through the proposed system.**

***Keyword*— solar power generation facility state monitoring system, drone aerial photographing**

I. INTRODUCTION

In recent years, the development of photovoltaic business is becoming more and more likely due to the implementation of the Renewable Energy Supply (RPS) system in Korea. The definition of RPS (New Renewable Energy Supply) means a system requiring operators with power generation capacity of 500 MW or more to supply a certain amount of power with renewable energy.It has implemented RPS and is doing well. Until December 2016, four years after RPS was implemented, its supply volume of FIT facilities (1 GW as of late 2011) was about 7.6 times that as much as that of current FIT facilities (solar energy 3.3 GW, non-flowing energy). The replacement rate of renewable energy in the year 2017 range is around 4 %. The government aims for 10 % in 2023 and it is forecast to rise to 28 % in 2030.

Therefore, a monitoring system for IT-related facilities will be needed. So, we would like to propose a solar power generation facility state system.

TABLE I
RPS facility confirmation by year, as of the end of 2016, Source: Korea Energy Corporation

		Y2012	Y2013	Y2014	Y2015	Y2016	Total
Solar	Number of power plants	1,670	1,898	5,501	6,944	4,056	20,069
	Facility Capacity (MW)	245	385	869	986	804	3,289
Non-Solar	Number of power plants	74	43	67	51	34	269
	Facility Capacity (MW)	1,731	509	873	441	711	4,266
Total	Number of power plants	1,744	1,941	5,568	6,995	4,090	20,338
	Facility Capacity (MW)	1,975	895	1,742	1,472	1,515	7,555

Manuscript received March 27, 2018. This work was supported by Software Convergence Cluster, Incheon SW Convergence R&D Support program of Incheon Business Information Techno park[Grant ID: R17-128-02].

Yoonlae Lee is with R&D Center, KGI CO. LTD., 129, Gaetbeol-ro, Yeonsu-gu, Incheon, 21999, South Korea(first- author, e-mail:candy143@daum.net)

Youn-Geol Lee is with department of computer software, Daelim University, 29, Imgok-Ro, Dongan-Gu, Anyang-Si, Gyeonggi-Do, 13916, South Korea (co-author, phone: +82-31-442-4423, fax: +82-31-442-4428, e-mail: yglee@daelim.ac.kr)

Hyunah Kim is with department of computer science, Kyonggi University, 154-42, Gwanggyosan-Ro, Teongtong-Gu, Suwon-Si, Gyeonggi-Do, 16227, South Korea (co-author, phone: +82-31-249-1467, fax: +82-31-249-9173, e-mail: hyuna486@kgu.ac.kr)

Minjae Park is with department of computer software, Daelim University, 29, Imgok-Ro, Dongan-Gu, Anyang-Si, Gyeonggi-Do, 13916, South Korea (Corresponding author, phone: +82-31-442-4434, fax: +82-31-442-4428, e-mail: mjpark@daelim.ac.kr)

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

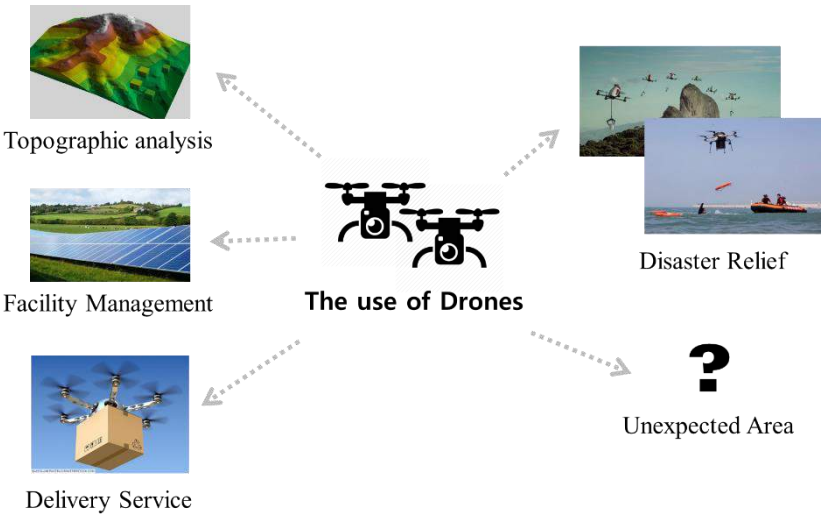

Fig. 1 Various Applications of Drones

II. Related Works

We want to use drone technology to collect basic data for facility management. Facilities mean solar power generation facilities and collects thermographic information about the solar power generation facilities. Therefore, not only solar facilities technology, but also drone technology is also relevant.

Currently, drone technology[1] is used in a wide variety of fields[6,7,8,9] like topographic analysis, facility management, delivery service, disaster relief, and it is being used in fields that were not predicted early on. As the navigation, communication, and sensor technologies related to drones have developed dramatically, the convergence market for drones such as facility inspection, disaster safety, disaster prevention, and logistics transportation is growing rapidly. The global drone market is expected to grow from $ 6.6 billion in 2013 to $ 11.4 billion in 2022, and is growing very rapidly[2]. The Korean Geographical Survey Institute is conducting ‘a study on UAV introduction[3]’ in the field of public surveying in order to establish a standard for using the drone in the field of public survey, and the research will be completed in December 2017.

In the United States, a study was made on the use of drones in the measurement of bridges, slopes and road pavement aging for the purpose of eliminating traffic congestion, improving safety, and reducing budgets.

In Europe, the efficiency of the survey was maximized by using drones in the investigation of road pavement aging mainly in Germany and Italy.

In China, research is being carried out on the use of drones for life structure, current status, and transportation of emergency goods in the event of slope failure using drone.

In the field of solar power, the drone technology can be very useful. In order to measure the overheating of the solar module, the drones can be equipped with an infrared camera to collect millions of pieces of photo information. This would save labor costs significantly compared to using individual measuring devices to inspect solar cell module information.

First Solar, the leading solar power company in the United States, is using the SkyCatch Drones service[4] at the world's largest 290MW solar power plant.

Drones are also useful for protecting wildlife around large solar power plants[5]. In the US, large-scale solar power plants are obliged to maintain and manage wildlife habitats. When drilling in the construction planning stage, wild animals and plants in the construction area can be identified and appropriate action taken. Based on this drone technology, we are going to overlook thermal camera technology, communication technology, and monitoring technology.

This study is also related to remote management[9,10,11,12,13] of facilities. Compared with various remote facility management methods, this study is distinguished in terms of using solar facility management, drone and thermal camera technique.

III. A Solar Power Generation Facility State Monitoring System Using Drone Aerial Photographing

We propose a solar power generation facility state monitoring system using drone aerial photographing. Figure 2 shows the overall of the proposed system.

The facilities can be monitored by the drones taking aerial photographs, real-time or batch data transmission and processing. Of course, data collection and processing are based on the IT infrastructure which consists of maps and database servers, and application servers.

The system we propose consists of two main functions. One is the thermal imaging camera image analysis function and the other is the solar power facility state monitoring function.

A. Thermal imaging camera image analysis function

We use a variety of information to recognize specific phenomena. In particular, we perceive phenomena based on visual information. And we want to know about the state of facilities based on visual information. Drones generally provide visual information for facility management. At this time, the thermal imaging camera is mounted on the drone, and thermal imaged photograph information is analyzed.

1) Location analysis of images

Drones thermal cameras are based on aviation cameras. EXIF (EXchangeable Image File Format) information is input into the image data taken for the air. In particular, the

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

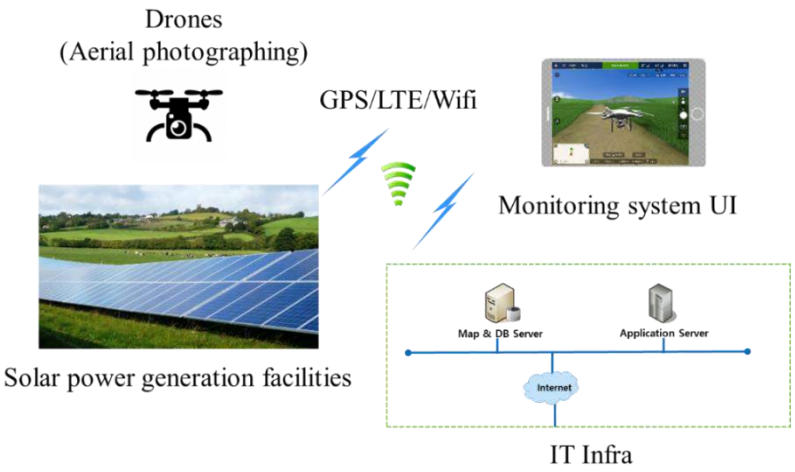

Fig. 2 Overall of the proposed system which is solar power generation facility state monitoring system using drone aerial photographing

equipment equipped with GPS will store latitude, longitude and altitude data when shooting. In order to find out the characteristics of a specific area, a color image analysis is carried out after taking an image with an infrared camera, and a specific temperature point can be found based on the color analysis. After finding a specific temperature point, map the relevant image data and corresponding point of the solar facility site and display it on the screen. Map the position data (latitude, longitude) to the scene image as a preliminary task.

Image formats that contain location (latitude, longitude) data include GeoTiff information. For images without general location (latitude, longitude) data, you can enter the latitude and longitude data using the map mapping system.

2) Metadata for data exchange: EXIF

EXIF (Exchangeable Image File Format), which is metadata recorded in an image file or the like, is recorded in an image file of JPEG or TIFF format as an exchange image file format.

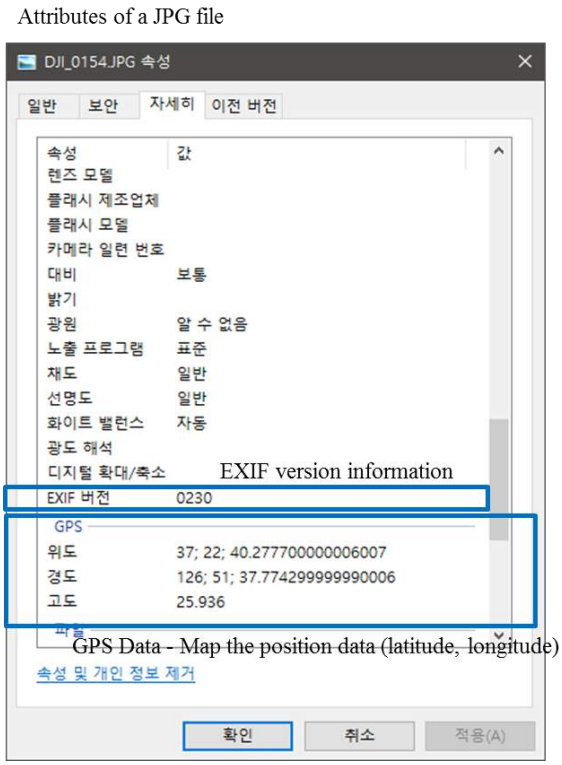

Fig. 3 EXIF information in JPG file

The EXIF data includes the following information.

- Camera information
- Camera settings
- Copyright Information
- Location information

TABLE Ⅱ

GPS information

Tag ID	Variable name	Description
0	GPSVersionID	GPS version
1	**GPSLatitudeRef**	**N (north), S (south)**
2	**GPSLatitude**	**Latitude**
3	**GPSLongitudeRef**	**E (east), W (west)**
4	**GPSLongitude**	**Hardness**
5	**GPSAltitudeRef**	**Relationship between altitude and sea level**
6	**GPSAltitude**	**Altitude**
7	GPSTimeStamp	The time (hours, minutes, seconds)
8	GPSSatellites	Satellite used for measurement
9	GPSStatus	The status of the GPS receiver used in the shooting
10	GPSMeasureMode	GPS measurement mode
11	GPSDOP	Accuracy of GPS data
12	GPSSpeedRef	Code for GPS receiver speed
13	GPSSpeed	Speed of GPS receiver
14	GPSTrackRef	Code for GPS receiver direction
15	GPSTrack	Direction of GPS receiver
16	GPSImgDirectionRef	Symbol for the direction of the subject
17	GPSImgDirection	The direction of the subject
18	GPSMapDatum	Information on geopolitical location
19	GPSDestLatitudeRef	N (north), S (south)
20	GPSDestLatitude	Latitude of target point

We want to use GPS information. There are various types of GPS information as shown in the table 2. Of the EXIF GSP

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

information provided in Table 2, we use the latitude, longitude, and altitude information 'GPSLatitudeRef', 'GPSLatitude', 'GPSLongitudeRef', 'GPSLongitude', 'GPSAltitudeRef', and 'GPSAltitude'. We extract latitude, longitude, and altitude information from images as shown above.

3) Thermal imaging camera image analysis

And analyzes the captured images based on the positional information and the thermal image information described above in a complex manner.

The data captured by the thermal imaging camera has its own color depending on the temperature of each pixel of the entire image, so that the entire image has color. There are various modes as follows.

Figure 3 below shows the change information according to the mode of the thermal imaging camera.

Among the various modes, White Hot is suitable for specific temperature detection and Rainbow is suitable for temperature distribution detection.

In case of 'White Hot' mode, it is suitable for specific temperature detection. For 'Rainbow' mode, it is suitable for temperature distribution. In other words, 'Rainbow' mode is suitable for 'measuring temperature distribution' and 'White Hot' mode is suitable for 'measuring specific temperature precision'.

The characteristics of the 'measuring temperature distribution' are as follows:

- The overall temperature distribution of the shooting area can be distinguished by color
- Quickly identify temperature changes around each shot
- Maximum temperature, minimum temperature and average temperature can be checked
- It is possible to check temperature distribution of temperature change by radiant heat over time
- It is possible to check temperature distribution according to seasonal temperature change.

And, the characteristics of the 'measuring specific temperature precision' are as follows:

- prediction of specific temperature spots in large areas
- Possible location determination at specific temperature
- Data base can be analyzed by data base

4) Image analysis for specific temperature detection

The steps of image photographing and analysis are as follows:

① Copying the original data shot by the thermal camera to the system

② Copy the temperature distribution data and specific temperature data separately

③ Display temperature distribution image on screen

④ Displays a specific temperature image on the screen, detects a specific temperature, and displays the corresponding point

Figure 4 shows the steps of image photographing and analysis.

5) Thermal imaging camera image analysis

The steps of thermal imaging camera image are as follows:

① The selected images stored on the SD card are copied to a specific folder for analysis as shown Figure 5. If we already have the same date data when we copy images, we can create a new date folder and copy it several times a day.

② The original image can be called a temperature data image and the spontaneous data image, respectively, and the copied image is stored as an image by date as shown Figure 6.

③ Select a temperature distribution image and check the temperature distribution of the entire low-firing range on the main screen. Map the latitude and longitude coordinates stored in the respective images to the latitude and longitude coordinates stored in the main map image and outputs them to the corresponding screen positions.

④ Select a specific temperature image as shown in Figure 7 to start temperature analysis for each image, and the image with a specific temperature color is displayed in the same position as the temperature distribution image.

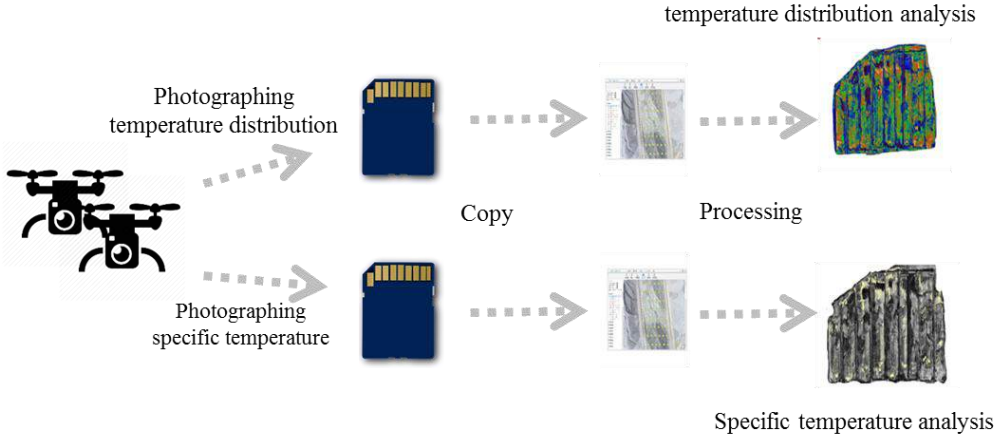

Fig. 4 Steps of image photographing and analysis

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

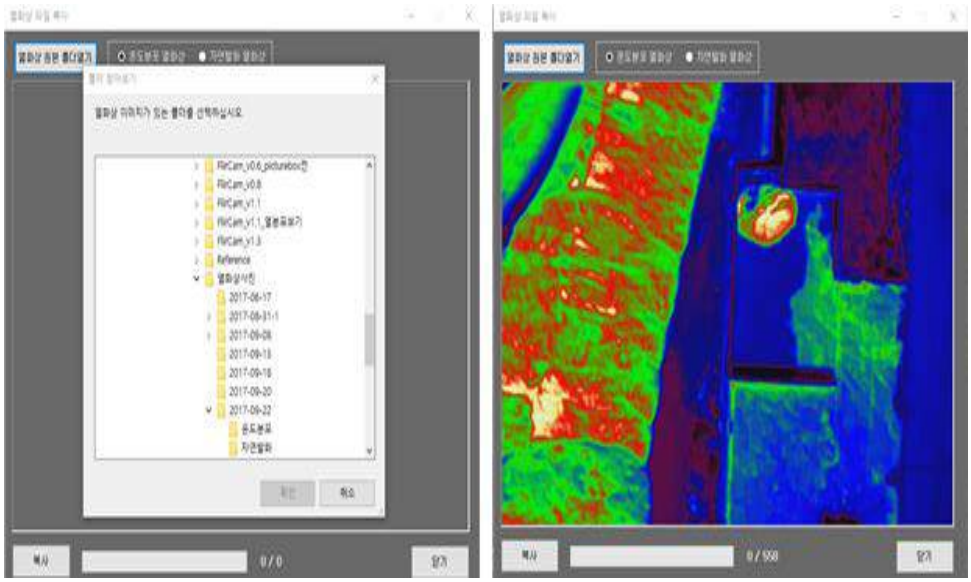

Fig. 5 Photographing images copy

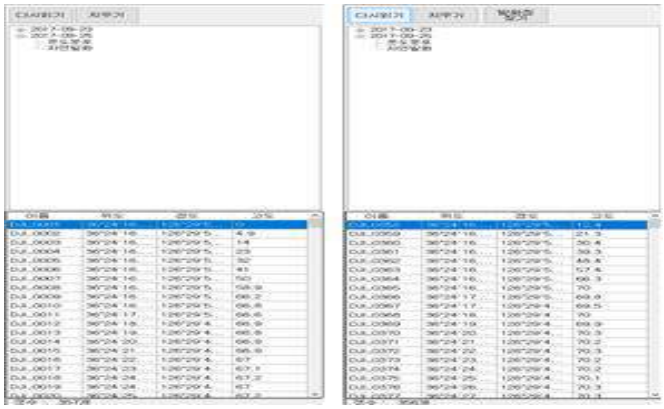

Fig. 6 Save by image

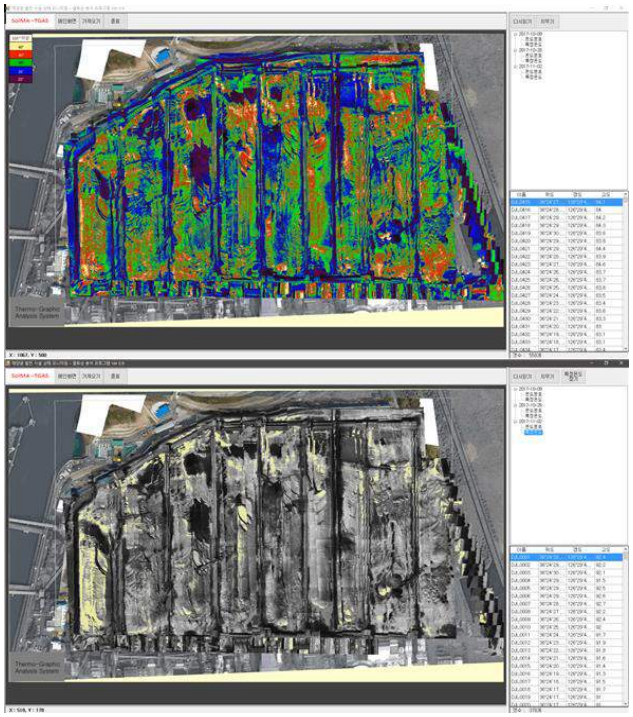

Fig. 7 Temperature distribution and specific temperature detection

B. Solar power facility state monitoring function

We can define and operate a monitoring process based on thermal imaging camera image analysis function.

Figure 8 is the operating process of the solar power facility state monitoring system. It is a process that is configured to analyze the thermal image information collected through the drone, and to check and review the status of facilities.

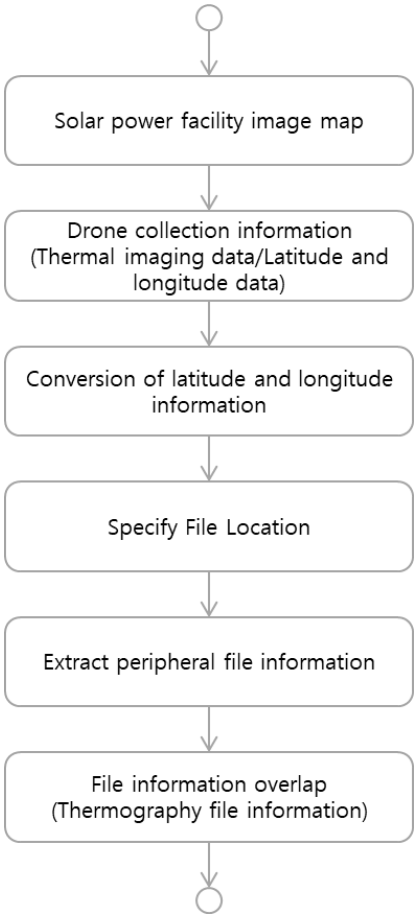

Fig. 8 Operating process definition of the solar power facility state monitoring

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

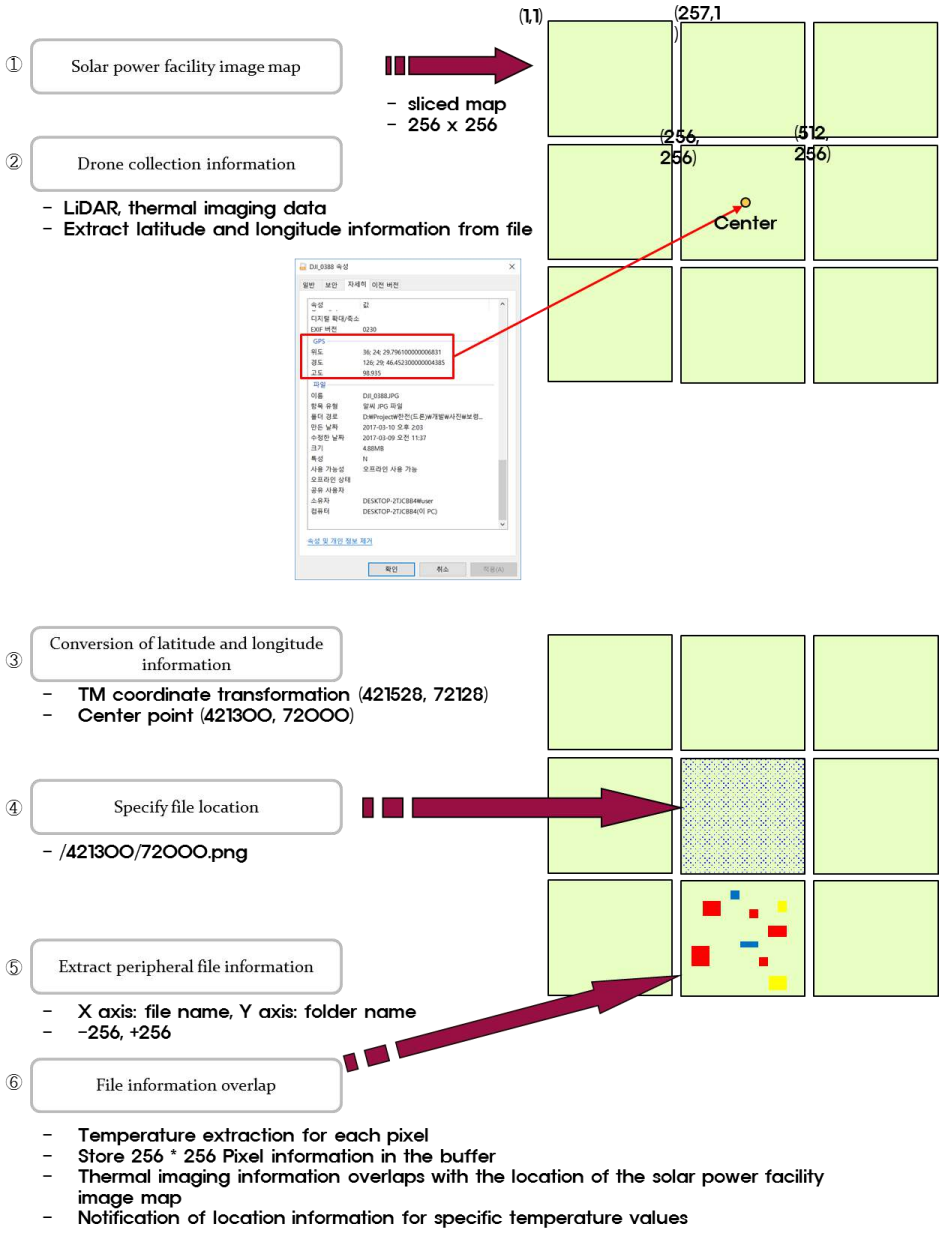

Fig. 8 Operating process of the solar power facility state monitoring system specific temperature detection)

Figure 8 shows operation which is the solar power facility state monitoring system specific temperature detection of the process defined in Figure 7. According to this operating method, we can monitor the state of the solar power facility.

First step is to import the solar power facility image map. The image map is composed of a slice map of (256*256) sizes. Second step is to gather information from the drones. At this time, the thermal image data and the latitude and longitude information in the file are extracted together. Third step is to convert latitude and longitude information as appropriate. Fourth step, the location file name is extracted at the center. In fifth step, the file name and the folder name are extracted. The sixth step is the last step, extracting the temperature of each pixel, repeatedly storing the pixel information in a buffer and overlapping the thermal image information.

It also provides information on the location of a specific temperature with anomalous signs. In this way, the monitoring system can be operated and the management of solar power facility state can be systematically automated.

IV. CONCLUSIONS

In this paper, we propose a solar power generation facility state monitoring system using drone aerial photographing.

We describe the thermal camera technology and the related analysis technology that we are dealing with in the proposed system, and describe the operation method to monitor the facility management using the technology. The technology includes techniques for processing photographic data as well as technologies for the thermal imaging camera itself, including methods for managing images and for analyzing and monitoring managed images.

We believe that this proposed system is a study on facility management and that it will play an important role in the future of new technology energy management.

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

ACKNOWLEDGMENT

This work was supported by Software Convergence Cluster, Incheon SW Convergence R&D Support program of Incheon Business Information Techno park[Grant ID: R17-128-02].

REFERENCES

[1] DANIEL, Kai, et al. *AirShield: A system-of-systems MUAV remote sensing architecture for disaster response. In: Systems conference*, 2009 3rd Annual IEEE. IEEE, 2009. p. 196-200.
[2] US Teal Group, *US Teal Group Report*
[3] Korean Geographical Survey Institute, *a study on UAV introduction*
[4] Skycatch, Inc., *Skycatch: Drone Image Processing Platform*, https://www.skycatch.com/
[5] Quater, Paolo Bellezza, et al. *"Light Unmanned Aerial Vehicles (UAVs) for cooperative inspection of PV plants."* IEEE Journal of Photovoltaics 4.4 (2014): 1107-1113.
[6] RESTAS, Agoston. *Drone applications for supporting disaster management.* World Journal of Engineering and Technology, 2015, 3.03: 316.
[7] KIMA, C.; MOON, H.; LEEA, W. *Data Management Framework of Drone-Based 3d Model Reconstruction of Disaster Site.* ISPRS-International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, 2016, 31-33.
[8] Ok Hyun and Kim Seong-Jin, *"Application Method of Remote Site Monitoring in Public Road Construction Projects,"* Journal of the Korea Academia-Industrial cooperation Society, Vol. 14, No. 12 pp. 6550-6557, 2013
[9] Kyoon-Tai Kim, *"Development of a Mountainous Area Monitoring System based on IoT Technology,"* Journal of the Korea Academia-Industrial cooperation Society, Vol. 18, No. 3 pp. 437-446, 2017
[10] Barker, William E., et al. *"Method for computer internet remote management of a telecommunication network element."* U.S. Patent No. 6,363,421. 26 Mar. 2002.
[11] Hunter, Robert R., David A. Vogt, and Leslie Cheong. *"Multi-capability facilities monitoring and control intranet for facilities management system."* U.S. Patent No. 6,363,422. 26 Mar. 2002.
[12] Wang, Shengwei, and Junlong Xie. *"Integrating Building Management System and facilities management on the Internet."* Automation in construction 11.6 (2002): 707-715.
[13] Yun, Chang Ho, et al. *"Intelligent management of remote facilities through a ubiquitous cloud middleware."* 2009 IEEE International Conference on Cloud Computing. IEEE, 2009.
[14] Suiter, F. J., and T. M. Cortes. *"Considerations for a reliable telecommunication power system at remote facilities utilizing valve regulated lead-acid battery management system technologies."* Telecommunications Energy Conference, 1994. INTELEC'94., 16th International. IEEE, 1994.

Younlae Lee is the director of KGI Corp., the South Korea Software Development Co. He received B.S. degrees in physics from Inha University and M.S. degrees in civil engineering from Kangwon University. He developed BlastAZ, the blasting simulation program. And his Research interests include 3D modeling and Imaging processing, Simulation systems, IoT(Internet of Things) and location-based infrastructure maintenance systems.

Young-Geol Lee is a full professor of computer software at Daelim University, South Korea. He received B.S., M.S., and Ph.D. degrees in computer science from Inha University in 1993, 1995, and 1999, respectively. His research interests include Database, Spatial Database, Geographic Information System, Spatial Warehousing, Data-centric Constraint Language and Process-aware facility management systems.

Hyunah Kim is an adjunctive professor and a faculty member of the collaboration technology research laboratory in the department of computer science at Kyonggi University, South Korea. She received her B.S. degree in computer science from Korea Nazarene University in 2001. Also, she received her M.S. and Ph.D. degrees in computer science from Kyonggi University in 2003 and 2009, respectively. Her research interests include workflow systems, SCORM-based e-Learning process models, BPM, BPI, ACM, workflow-supported social networks discovery and analysis, and process-aware Internet of Things.

Minjae Park is an assistant professor of computer software at Daelim University, South Korea. He received B.S., M.S., and Ph.D. degrees in computer science from Kyonggi University in 2004, 2006, and 2009, respectively. His research interests include groupware, workflow systems, BPM, CSCW, collaboration theory, process warehousing and mining, workflow-supported social networks discovery and analysis, process-aware information systems, data intensive workflows, and process-driven Internet of Things and process-aware factory automation systems.

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

Security Enhancement for Access Control Mechanism in Real-time Wireless Sensor Network

Mangal Sain*, Amlan Jyoti Chaudhray**, Satyabrata Aich***, and Hoon Jae Lee*

**Division of Computer Information Engineering, Dongseo University, Busan, South Korea*

***Department of ECE, Kaziranga University, Jorhat, 785-001, India*

****Department of Computer Engineering, Inje University, South Korea*

mangalsain1@gmail.com, choudhuryamlanjyoti@gmail.com, satyabrataaich@gmail.com, hjlee@dongseo.ac.kr

Corresponding author email id: mangalsain1@gmail.com

***Abstract*— A wireless sensor network (WSN) based real-time application, both physical nodes (i.e., unguarded nodes) as well as open communication channels are accessible to the adversaries. Such channel openness and unguardedness of the WSN nodes may lead to various attacks to the application. Therefore an access control mechanism is essential for such WSNs that are deployed in the hostile environments. In this regards, recently, two practical access control protocols (PACPs) are being proposed for WSNs. The authors claimed that their proposed protocols are suitable for practical implementation and are secure against most of the known attacks. Unfortunately, PACPs have inherent security weaknesses and difficulty in real-time implementation. In this paper, we identify few security pitfalls. In addition, a new node addition phase is impractical in the real world deployment. In order to overcome the PACPs issues, we also proposed an enhanced practical access control protocol that provides more security features at low computation and communication costs.**

***Keywords*— Access control protocol, authentication, key establishment, wireless sensor networks**

I. INTRODUCTION

Wireless sensor networks (WSNs) are known as novel and intelligent systems, and are continuously deploying in wide range of real-world applications (military, healthcare, smart building, security systems, etc) [1].

Manuscript received January 2, 2018. This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology. (Grant number: NRF-2011-0023076). This paper is a follow-up the invited journal to the outstanding paper of the 20th International Conference on Advanced Communication Technology (ICACT 2018).

Mangal Sain is with the Department of Computer Engineering, Dongseo University, South Korea. He is the corresponding author of this paper.

Amlan Jyoti Chaudhray is with Department of ECE, Kaziranga University, Jorhat, India (e-mail: choudhuryamlanjyoti@gmail.com)

Satyabrata Aich is with the Department of Computer Engineering, Inje University, South Korea (e-mail: satyabrataaich@gmail.com)

Hoon Jae Lee is with the Department of Computer Engineering, Dongseo University, Busan, South Korea, South Korea (e-mail: hjlee@dongseo.ac.kr)

Mangal Sain is with the Department of Computer Engineering, Dongseo University, South Korea. He is the corresponding author of this paper. (Corresponding author phone: +8251-320-2009; e-mail: mangalsain1@gmail.com).

WSN have emerged as a field of research. WSN have long term economic potential and capability to transform daily lives. In addition, Wireless Sensor Networks increase many of the latest problems such as abstractions and optimization problems, tracking, localization etc.

The incorporation of several types of sensors, such as acoustic, seismic and optical, in a network platform and the study of the general scope of the system presents several interesting challenges. Due to recent development in WSN technology Wireless sensors, they are a great tool for military applications related to admission, monitoring of outline and information gathering and elegant logistic support in an area that is implemented. Some additional applications: site detection, personal health monitoring based on sensors with sensor and motion sensor networks [2]

Low-cost deployment is one of the acclaimed benefits of sensor networks. Limited power and memory are two biggest constraints in WSN. But with the development of in fabrication technique these two problems can be resolved in future. Also, due to the unattended nature of sensor nodes and dangerous sensing environments, replacing battery is not a viable solution. Alternatively, the monitoring characteristics of many sensor network applications require a long service life. Therefore, providing a form of energy efficiency monitoring service for geographical areas is a very important research topic.

These sensor nodes are deployed in a wide area for performing their intended task efficiently. Due to the novelties of WSNs such as, large scale deployment, resource scarcity and wireless communication nature makes them vulnerable to various attacks. It is possible that an adversary can introduce the malicious nodes into the network and may disturb the network functionality. However, to protect WSNs from adversaries and maintain the network working continuously (life-time), security mechanisms (e.g., access control [3] [4]) are highly desirable for the applications.

Zhou et al. proposed an access control protocol based on ECC [5], which is more efficient than RSA-based public-key cryptography schemes. The authors state that the new node (with the timestamp) could join the network at any time and support key exchange. However, to authenticate a sensor node, the Zhou et al. scheme incurred extremely high computing and

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

communication costs. In real WSN, high consumption rates can be the real problem. Thereby, based on ECC and hash chain, Huang proposed a novel access control protocol (NACP) [6] which is quite good for low power sensor nodes. He also showed that NACP can be easily implemented as a dynamic access control system because all the secrets and information transmission information in existing nodes should not be updated once a new node has been added to the network.

In 2009, Kim and Lee proposed an enhanced novel access control protocol (ENACP) which exploits the hash-chain approach and performs the node authentication and key establishment [7]. Unfortunately, Zeng et al., [8] and Shen et al., [9] demonstrated that ENACP has natural design flaws and vulnerable to many attacks. In 2012, Lee et al pointed out that ENACP is susceptible to message forgery and new node masquerade attacks, and proposed practical access control protocols (also known as PACPs) for WSNs [10]. PACPs consist of two sub-schemes, namely, secure PACP (secPACP) and memory-efficient PACP (ePACP). Moreover, authors claimed that PACPs are secure against many attacks and very practical for the real WSNs.

However, in this paper we demonstrate that PACPs are not secure against message replay attack, Sybil attack and impersonation attack. More importantly, we will show that the new node addition is very limited (i.e., only for certain nodes) and hence, PACPs are not highly scalable. Next section will briefly review the PACPs. In order to mitigate the issue of pacps we, also we also proposed an enhanced access control protocol for real time WSN. The proposed scheme is strong against message replay attack and Sybil attack. We also discuss the enhanced security features of our proposed protocol and prove that the scheme is secure against message replay attack, strong against Sybil attack and possess important security features such as user anonymity. Similar to PACP our proposed algorithm exploits hybrid cryptosystem i.e. elliptic curve and symmetric cryptography.

The Remainder of this article is organizes as follows. Section II consist a review of PACPS. Section III presents the analysis of security pitfalls in PACPs. Section IV presents an Enhanced Access Control Protocol. Section V presents security analysis. Finally, Section VI concludes our results and future research.

II. REVIEW OF PACPS[7]

PACPs have two variant, namely, *secPACP* and *ePACP*.

A. *secPACP (secure PACP):* It is composed of three phases: initialization, authentication and key establishment, and new node addition.

1) Initialization phase: This phase is performed off-line by the base station (BS); it generates a large key space *(LKS)*, key identifiers, and identities (IDs) for all sensor nodes (i.e., *N* sensor nodes). BS randomly chooses *Q* nodes for the initial deployment (or network). Thereafter, BS randomly picks one secret key and *m* keys from *LKS* for each node and computes an authentication set *(AS)* (i.e., set of hash values, and their identifiers). Finally, BS installs a secret key and *AS* into the nodes, which are selected of the network deployment. *More general example*, BS randomly chooses K_X and $\{K_{Ri}\}_{i\in\{1,2,\ldots,x\}}$ from *LKS* for the node *X*. Then, BS computes $AS_X = \{(HID_i, h(ID_X||K_{Ri}))\}_{i\in\{1,2,\ldots,z\}}$ for node *X*. Here, HID_i means the owner of secret key K_{Ri}. Thereafter, BS installs K_X and AS_X into the node *X*. Now sensors are ready for the deployment.

2) Authentication and key establishment phase: Assume that two nodes *(e.g., node A* and *node B)* are neighbors and each node recognizes the identities of its neighboring nodes using some beaconing technique which includes the node identity in the beacons. If node *A* shares $h(ID_A||K_B)$ with node *B*, then two nodes *(A and B)* start key establishment as follows.

i. Node *A* generates a random integer t_A, and computes the point $N_A = t_AP = (Nx_A, Ny_A)$ over the elliptic curve *E* and $S_A = h(ID_A||Nx_A||h(ID_A||K_B))$. Now, it *(Node A)* broadcasts ID_A, N_A, and S_A.
ii. After receiving the broadcasted message from the node *A*, node *B* checks whether $h(ID_B||K_A)$ is in $AS_B = \{(HID_i, h(ID_B||K_{Ri}))\}_{i\in\{1,2,\ldots,z\}}$ or not. If it is not true then aborts the system. Otherwise, node *B* verifies $h(ID_A||Nx_A||h(ID_A||K_B)) = S_A$ with its own key K_B. If S_A is verified then node *B* assured that N_A is generated by a legal node who knows the $h(ID_A||K_B)$. After that, node *B* generates a random integer t_B and computes $N_B = t_BP = (Nx_B, Ny_B)$ and $S_B = h(ID_B||Nx_B || h(ID_B||K_A))$. And it broadcasts ID_B, N_B, and S_B.
iii. Upon receiving the broadcasted message from the node *B*, node *A* checks $h(ID_B||Nx_B||h(ID_B||K_A)) = S_B$ with its own key K_A. If S_B is verified then node *A* assured that N_B is generated by a legal node who knows the $h(ID_B||K_A)$. Thereafter, node *A* computes $SK_{AB} = t_AN_B = (SKx_{AB}, SKy_{AB})$ and $Z_A = h(ID_A||SKx_{AB}||h(ID_A|| K_B))$, and broadcasts Z_A.
iv. Node *B* computes $SK_{AB} = t_BN_A = (SKx_{AB}, SKy_{AB})$ and checks $h(ID_A||SKx_{AB}||h(ID_B|| K_A)) = Z_A$. If it is true, then node *B* approves SK_{AB}. Now node *B* computes $Z_B = h(ID_B|| SKx_{AB} || h(ID_A|| K_B))$ and broadcasts it to the node *A*.
v. Finally, node *A* checks $h(ID_B||SKx_{AB}||h(ID_A|| K_B)) = Z_B$. If it holds, then node *A* also approves SK_{AB}.

The authentication and key establishment phase of *secPACP* is shown in Fig. 1.

3) Node addition phase: This phase is invoked when a new node is entering into the existing network. First, BS assigned an identity to the new node (ID_{Q+1}) and also preloads secret key K_{Q+1} and $AS_{Q+1} = \{(HID_i, h(ID_{Q+1}||K_{Ri}))\}_{i\in\{1,2,\ldots,z\}}$. Thereafter, new node will perform the authentication and key establishment phase as shown in Fig. 1, and becomes the legal member of the network.

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

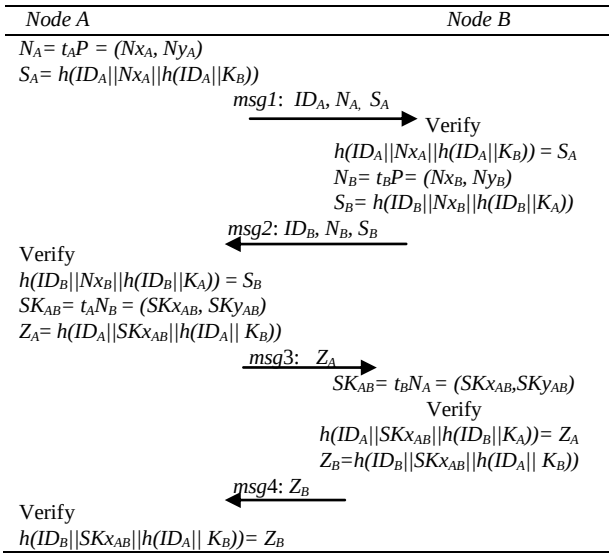

Fig. 1. secPACP: Authentication and key establishment phase

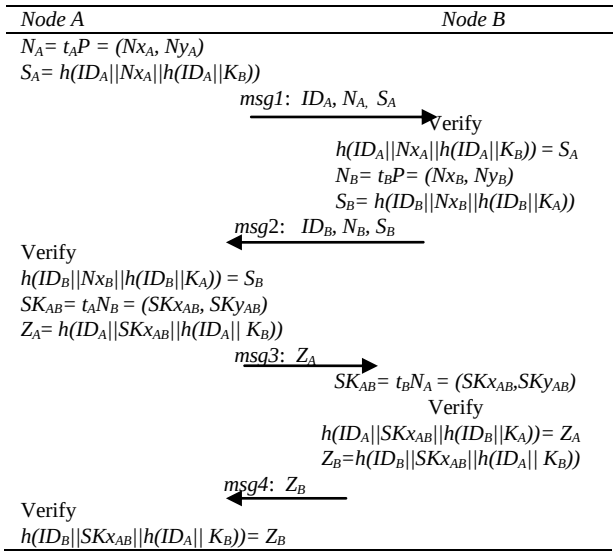

Fig. 2. ePACP: Authentication and key establishment phase

B. ePACP (memory-efficient PACP): It is composed of two phases, namely, initialization, and authentication and key establishment. This subsection reviews *ePACP*, which is a variant of *secPACP* except the initialization phase.

1) Initialization phase: This phase performed offline by the base station (BS); it generates a large key space *(LKS)*, key identifiers, and identities for all *N* sensor nodes. BS randomly chooses *Q* nodes for the initial network deployment. Now it is assumed that the identities of all nodes are in a circular order (i.e., the last identity is equal to the first identity). Therefore, each sensor node has its inner nodes and outer nodes in circular order. The number of all candidate node is Q' $(Q \leq Q' \leq LKS)$, we describe the *inner* nodes of node *X* as $\{ID_{Yi}\}_{(X<Yi\leq X+\lceil Q'/2 \rceil)}$ and the other nodes are represented as the *outer* nodes of node *X*.

Thereafter, BS randomly chooses one secret key from the large key space *(LKS)* and installs it into the each node. Then, it (BS) chooses *m* keys from *LKS* for each sensor's inner nodes; derives an authentication set *(AS);* and finally, installs *AS* into its corresponding sensor node. *For example*, BS randomly chooses K_X and $\{K_{Ri}\}_{i\in\{1,2,\ldots,x\}}$ from *LKS* for node *X*. Here *X* is a node, and K_{Ri} are randomly selected secret keys for node *X's* inner nodes. For node *X*, BS computes $AS_X = \{(HID_i, h(ID_X||K_{Ri}))\}_{i\in\{1,2,\ldots,z\}}$, here HID_i means the owner of secret key K_{Ri}. Thereafter, BS installs K_X and AS_X into node *X*.

2) Authentication and key establishment phase: Assume that two nodes *(e.g., node A and B)* are neighbors and each node recognizes the identities of its neighboring nodes using some beaconing technique which includes the node identity in beacons. If sensor node *B* is an inner node of node *A*, then *A* starts the pairwise key establishment with node *B*, otherwise, node *B* starts. The authentication and key establishment phase is same as in *secPACP* (refer to the *secPACP* authentication and key establishment phase). However, the flow of *ePACP* is depicted in Fig. 2.

Next section will demonstrate the security pitfalls in PACPs.

III. Analysis of Security Pitfalls in PACPs

Indeed, PACPs are strong against eavesdropping, message forgery attack, and new node masquerade attack. However, a single loophole can become a big danger to the network, if all possible security threats are not considered (with their destructive impact) while designing the protocol. In this section we present the inherent PACPs security pitfalls, such as, message replay attack, Sybil attack and impersonation attack, and other practical issues. For the comprehensive analysis of PACPs, we have assumed that an attacker has full control over wireless channels (e.g., it can insert, drop, modify or replay the wireless messages). Based on above assumptions, we generalize the message replay attack in PACPs, as follows.

1) Message replay attack: In this attack, an adversary actively captures on-air wireless messages between two communicating entities (e.g., node *A* and node *B*) and replays the captured messages, later, as it is. Although, it is a very common attack on wireless communication protocols but it (replay attack) could cause of one of the network destructive denial-of-services attack if it would not be protected efficiently and resultant, node's (AA) battery power depletion.

Attack description: In PACPs, it is worth noting that, as shown in Fig.1 *(secPACP)* and Fig.2 (*ePACP*), an active adversary easily captures the wireless messages *(msg1)* between the node *A* and the node *B* (refer-Section II, authentication and key establishment phase). In *secPACP*, assumed that after some later time adversary transmits, *msg1* (ID_A, N_A, S_A) to the node *B*. Upon receiving *msg1* from adversary, node *B* starts computations as follows: verifies $h(ID_A||Nx_A||h\ (ID_A\ ||K_B\ )) = S_A$. It will be verified easily because every time node *B* considers *msg1* as a fresh message (because random number/ nonce is not properly verified) and node *B* computes: $N_B = t_B P$

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

$= (Nx_B, Ny_B)$ and $S_B = h(ID_B||Nx_B||h(ID_B||K_A))$ and sends *msg2* (ID_B, N_B, S_B) to attacker. *Note that*, here the node *B* is not aware about that it has sent *msg2* to an attacker or to a legal node. Now upon receiving the *msg2* from the node *B*, an attacker generates a fake *msg3* ($Z_A' = h(ID_A|| SKx_{AB}' || h(ID_A|| K_B))$) and sends it to the node *B*. Here, SKx_{AB}' is attacker's fake key. Now, the node *B* computes the key ($SK_{AB} = t_B N_A = (SKx_{AB}, SKy_{AB})$) and verifies the message (Z_A'). Obviously, attacker's fabricated fake message (i.e, Z_A') will not be verified by the node *B* because $SKx_{AB} \neq SKx_{AB}'$ and hence Z_A' will not be verified. Thus, due to the very late detection of an attacker, *secPACP* is vulnerable to the message replay attack. By imposing the message replay attack again and again, an attacker can make sensor node battery depletion which is not acceptable in the mission-critical WSN applications.
Likewise, *ePACP* is also vulnerable to the *replay attack*.

Authors of [11] argued that preloading the number of keys (i.e., either pairwise or not) onto exposed devices (i.e., not tamper-proofed) strengthens the incentive for attackers to compromise a node. In PACPs, authors exploit the pairwise key pre-distribution scheme and suggested that each PACPs node contains number of keys (e.g., 5,740 keys in *secPACP* and 1650 keys in *ePACP*). Though, *Kim et al* claimed that *secPACP* and *ePACP* are resilience against node capture attack and node fabrication attacks means if a node is captured then the pairwise keys of non-captured nodes are node reveled. However, the high number of keys in a node motivates to the attackers for corrupting more nodes. Moreover, *Tyler Moore* demonstrated that a small colluding node (less than 5% of the entire network) can control half's of its neighbors' communication channels. Thus in PACPs, an adversary can collect the energy-exhausted sensor nodes from the terrain and can dig outs the all secrets from a node. Based on above assumptions, we generalize the Sybil attack and impersonation attack on *secPACP* and *ePACP*.

***2) Sybil attack*:** In this attack, a malicious sensor node can present itself with multiple fake identities (IDs) and impersonates other legitimate nodes as a legal node [12]. Moreover, it can manifest in a severe form leading to the failure of basic protocols functioning, such as network routing, network resource allocation and network functioning.

Attack description: In mission-critical applications (e.g., military, homeland security, etc) where sensor networks are often deployed in hostile environments. Consider *secPACP* case, where 5,750 keys suggested for an exposed sensor node. Assumed that a motivated adversary collects some energy-exhausted sensor nodes and reprogram them or make replication of the nodes (known as clone). Thereafter adversary deploys these malicious/clone nodes into the terrain, authenticates itself with non-compromised nodes and may control the network, accordingly. Now onwards, we call a malicious node as a *Sybil node*. It is assumed that a *Sybil node* can recognize the identities of its neighboring nodes using some beaconing technique which includes the node identity in beacons. A Sybil node illegitimately takes on multiple identities [12]. Moreover these identities may belongs to its *authentication set* (i.e., $AS_X = \{(HID_i, h(ID_X || K_{Ri}))_{i \in \{1,2,\ldots,z\}}\}$) or belong to the existing nodes identities, here, HID_i means the owner of secret key K_{Ri}. Fig.3 depicts the Sybil attack running example.

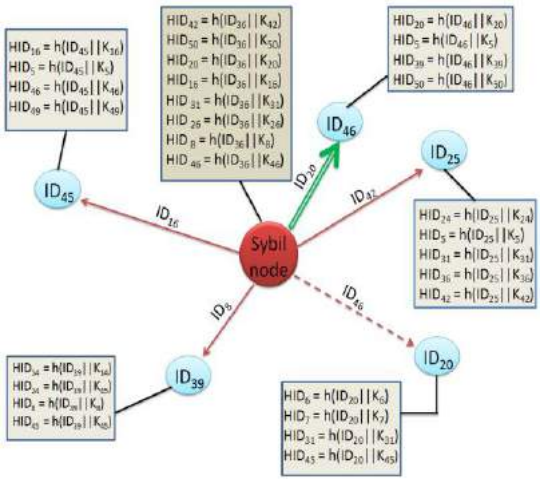

Fig. 3. Sybil attack in *secPACP* scheme

For the simple generalization of the Sybil attack, we assume the size of a large key space *(LKS)* is 50. As shown in Fig. 3, a *Sybil node* presents its multiple identities to its neighboring nodes and tries to authenticate and establish a pairwise key, as a legal node. For instance, it *(Sybil node)* shows own multiple identities as follows: ID_{42} to the node 25, ID_8 to the node 39, ID_{16} to the node 45 and ID_{46} to the node 20. The solid (red) line represents that the node 25 has HID_{42}, the node 39 has HID_8, and the node 45 has HID_{16} are corresponding to the *Sybil node*. Hence, the node 25, node 39 and node 45 authenticate to the *Sybil node* as a legitimate node and establish pairwise keys with the *Sybil node*.

The flow of Sybil attack between the *Sybil node* (i.e., ID_{42}) and the node 25 (says node *B*) is as follows.

A. *Sybil node* generates a random integer St_A and computes the point $SN_A = St_A P = (SNx_A, SNy_A)$ over the elliptic curve *E*, and computes $SS_A = h(SID_A||SNx_A||h(SID_A||K_B))$. Now *Sybil node* sends SID_A, SN_A, *and* SS_A to the node 25 (i.e., *B*).

B. After receiving the message from the *Sybil node*, node *B* checks whether $h(SID_B||K_A)$ is in $AS_B = \{(HID_i, h(SID_B||K_{Ri}))\}_{i \in \{1,2,\ldots,z\}}$. Since, the node *B* holds, and it verifies $h(SID_A||SNx_A||h(SID_A||K_B)) = SS_A$ with its own key K_B . Here, SS_A will be verified and node *B* assured that SN_A is generated by a legal node. *Note that*, here the node B does not know whether this message (SID_A, SN_A, *and* SS_A) is received from legitimate node or an attacker (*Sybil node*). After that, node *B* generates a random integer t_B and computes $N_B = t_B P = (Nx_B, Ny_B)$ and $S_B = h(ID_B||Nx_B||h(ID_B||K_A))$. And it sends ID_B, N_B, and S_B to the *Sybil node*.

C. Upon receiving the messages from the node *B*, *Sybil*

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

node easily checks $h(ID_B||Nx_B||h(ID_B||K_A)) = S_B$ with its own key K_A. Thereafter, *Sybil node* computes $SSK_{AB} = St_AN_B = (SSKx_{AB}, SSKy_{AB})$ and $SZ_A = h(SID_A||SSKx_{AB}||h(SID_A||K_B))$, and sends SZ_A to the node *B*.

D. Node *B* computes $SK_{AB} = t_BSN_A = (SSKx_{AB},SSKy_{AB})$ and checks $h(SID_A||SSKx_{AB}||h(ID_B||K_A)) = SZ_A$. Since it will be verified and node *B* computes $Z_B = h(ID_B||SSKx_{AB}||h(SID_A||K_B))$ and sends it to the *Sybil node*.

E. Now *Sybil node* computes $h(ID_B||SSKx_{AB}||h(SID_A||K_B))$ and establishes a pairwise key with the legitimate node (i.e., node *B*).

Similarly, *Sybil node* can establish a pairwise key with the node 39, 45, and many more. The *Sybil node* authentication and key establishment phase is shown in Fig. 4.

Moreover, in Fig. 3, the (red) dotted line represents that the node 20 do not contain any HID_{46}, and hence, cannot authenticate to the *Sybil node*. The double (green) solid line represents that a *Sybil node* can impersonates its neighboring nodes. For example, it *(Sybil node)* sends own neighbor's identity (i.e., ID_{20}) to the node 46 and *impersonates* as a legal node. Since, the node 46 has HID_{20}; it authenticates and establishes a pairwise key (as shown in Fig. 4) with the node 46.

Likewise, *ePACP* is also susceptible to the *Sybil attack and impersonation attack*, where 1,650 keys are recommended for an exposed sensor node.

Resultant, PACPs are not secure against the *Sybil attack and impersonation attack* where a sole *Sybil node* can control PACPs's neighbouring nodes communication channels without misbehaviour detections.

3) Limited scalability in secPACP (new node addition): Recall a new node addition phase in *secPACP* (refer section-II), where a new node is entering into the existing networks. The base station (BS) assigned a new identity to the new sensor node (ID_{Q+1}) and also preloads secret key K_{Q+1} and $AS_{Q+1} = \{(HID_i, h(ID_{Q+1}||K_{Ri}))\}_{i\in\{1,2,\ldots,z\}}$. However, *secPACP* allows only limited scalability (i.e., new node addition) to the network. In *secPACP* network, where *N* numbers of identities were generated offline for the *N* nodes and *Q* nodes were selected for the initial network deployment (recall initialization phase in *secPACP*, Section-II). Now, only *Q+1 (i.e., new node))* can easily enter into the existing network because it may have shared secrets (*i.e.,* K_{Q+1} and $AS_{Q+1} = \{(HID_i, h(ID_{Q+1}||K_{Ri}))\}_{i\in\{1,2,\ldots,z\}}$) with the existing nodes. *Note that*, here an *N+1* node can never be entered into the network since it does not contain any secret shared (*i.e.,* K_{N+1} and $AS_{N+1} = \{(HID_{N+i}, h(ID_{N+1}||K_{Ri}))\}_{i\in\{1,2,\ldots,z\}}$) with the existing *N* nodes. For more simple generalization consider a *simple running example*. Assumed that a BS generates offline 50 nodes *(N)* identities and the size of key space is 50. Then BS randomly chooses 45 nodes *(Q)* for the initial deployment (or network). Then only, 5 nodes *(N-Q)* can be easily added into the network, because these *(N-Q)* nodes may have secret shared with the existing *(Q)* nodes. Therefore, *N+1* (e.g., node 51) node cannot join the network. Consequently, *secPACP* has limited scalability, which is not practical for the MAMMOTH size distributed WSNs, where scalability is highly required.

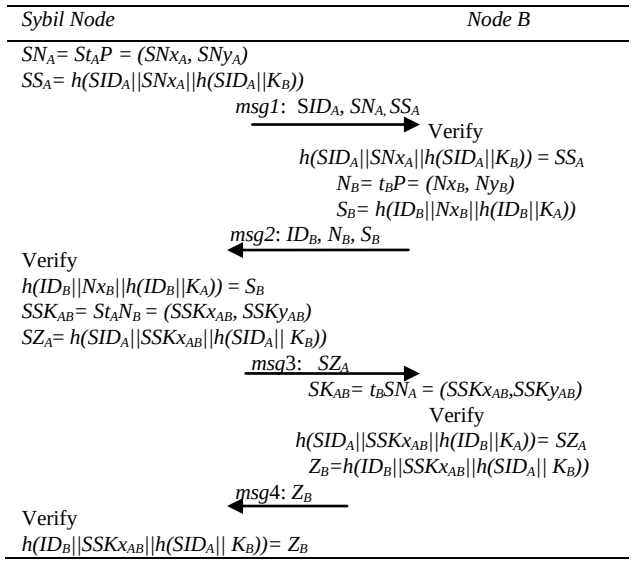

Fig. 4. Authentication and key establishment phase for Sybil attack in secPACP

4) Node anonymity: In *secPACP* and *ePACP* schemes, nodes IDs of all nodes are openly transmitted. This will help adversaries to perform Sybil attack and make life much easier for them. In any access control or user authentication scheme, user anonymity is an security feature and the protocol designer has to make sure that the user IDs of nodes are kept secret [10].

Other practical issues: PACPs also have other practical issues, which are highly desirable for the real WSNs, as follows.

- In PACPs, if node *A* shares $h(ID_A||K_B)$ with the node *B*, only then both the nodes *(A and B)* can start key establishment. Otherwise, it is possible that a big part of network may isolates from the entire network, if shared secrets are not found. Hence, in PACPs shared secret is not guaranteed (i.e., 100%).

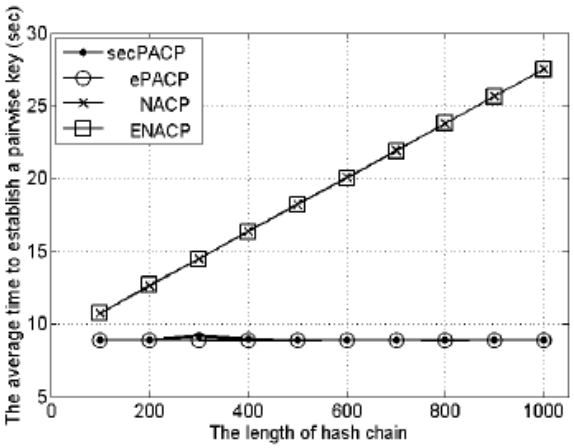

Fig. 5. The average time to establish a pairwise key [7]

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

More importantly, in PACPs, the computation time (or computation cost) is very high (as depicted in Fig.5), where the average time for establishing a pairwise key is about 9 seconds, which is expensive for the real WSNs.

IV. ENHANCED ACCESS CONTROL PROTOCOL

In this section, we propose an enhanced access control protocol which is strong against message replay attack and Sybil attack.

In the *initialization phase* of the proposed scheme, base station randomly choses k_X and $\{k_{Yi}\}_{i\in\{1,2,\ldots,m\}}$ from *LKS* for node *X*, and a common random number, *q* for all nodes. Subsequently, BS then computes $AS_X = \{(HID_i, h(ID_X \| k_{Yi})\}_{i \in\{1,2,\ldots,m\}}$ where HID_i is the identity of hash value $h(ID_X \| k_{Yi})$. Afterward, the base station puts k_X and AS_X, and *q* into node *X*.

In the *Authentication and key establishment phase*, two nodes *(e.g., node A* and *node B)* are neighbors and each node recognizes the identities of its neighboring nodes using some beaconing technique which includes the node identity in the beacons. If node *A* shares $h(ID_A||K_B)$ with node *B*, then two nodes *(A and B)* start key establishment as follows.

i. Node *A* generates a random integer t_A, and computes the point $N_A = t_AP = (Nx_A, Ny_A)$, $d=ID_A \oplus q$ and $S_A = h(ID_A||K_B)$ which is already stored in the node and sends over the elliptic curve *E*.

ii. After receiving the broadcasted message from the node *A*, node *B* computes $ID_A=d\oplus q$ and checks if $h(ID_B||K_A)$ is in $AS_B = \{(HID_i, h(ID_B||K_{Ri}))\}_{i\in\{1,2,\ldots,z\}}$ or not. If it is not true then aborts the system. Otherwise, node *B* verifies $h(ID_A||K_B) = S_A$ with its own key K_B. If S_A is verified then node *B* assured that N_A is generated by a legal node who knows the $h(ID_A||K_B)$. After that, node *B* computes $e= q\oplus ID_B$, generates a random integer t_B and computes $N_B= t_BP= (Nx_B, Ny_B)$ and $S_B= h(ID_B||K_A)$. And it broadcasts *e*, N_B, and S_B.

iii. Upon receiving the broadcasted message from the node *B*, node *A* computes $ID_B=e\oplus q$ and checks if checks if $h(ID_A||K_B)$ is in $AS_B = \{(HID_i, h(ID_A||K_{Ri}))\}_{i\in\{1,2,\ldots,z\}}$ or not. If it is not true then aborts the system. Otherwise, A verifies if $h(ID_B||K_A) = S_B$ with its own key K_A holds true or not. If S_B is verified then node *A* assured that N_B is generated by a legal node who knows the $h(ID_B||K_A)$. Thereafter, node *A* computes $SK_{AB}= t_AN_B = (SKx_{AB}, SKy_{AB})$ and generate current timestamp t_1 and compute $C_1= SK_{AB}$ *mod t*, and $Z_A= h(ID_A||SKx_{AB})$, and broadcasts t_1, C_1, Z_A.

iv. Node *B* computes $SK_{AB}= t_BN_A = (SKx_{AB}, SKy_{AB})$ and checks $h(ID_A||SKx_{AB})= Z_A$. If it is true, then node *B* approves SK_{AB}. Node *B* checks if t_1'-t_1 does not exceed maximum threshold time Δt (to check message freshness). Subsequently, only if message freshness is justified, then node *B* computes $SK_{AB}= t_BN_A = (SKx_{AB}, SKy_{AB})$ and generate current timestamp t_2 and compute $C_2= SK_{AB}$ *mod t*, Now node *B* computes $Z_B= h(ID_B|| SKx_{AB})$ and broadcasts t_2, C_2, and Z_B to the node *A*.

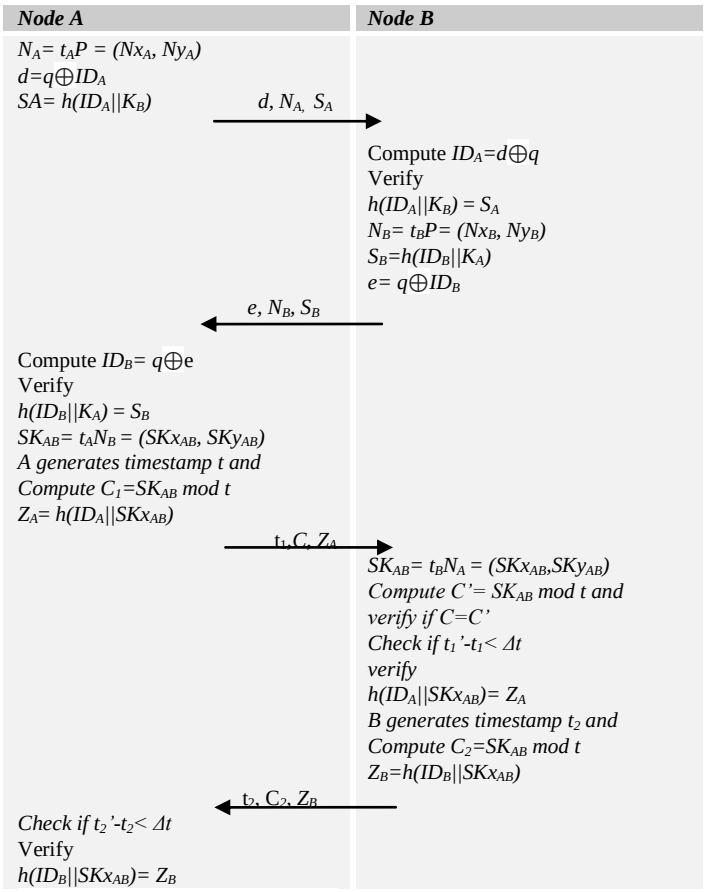

Fig. 6. Authentication and key establishment phase of enhanced access control protocol

v. Node *B* computes $SK_{AB}= t_BN_A = (SKx_{AB}, SKy_{AB})$ and checks $h(ID_A||SKx_{AB})= Z_A$. If it is true, then node *B* approves SK_{AB}. Node *B* checks if t_1'-t_1 does not exceed maximum threshold time Δt (to check message freshness). Subsequently, only if message freshness is justified, then node *B* computes $SK_{AB}= t_BN_A = (SKx_{AB}, SKy_{AB})$ and generate current timestamp t_2 and compute $C_2= SK_{AB}$ *mod t*, Now node *B* computes $Z_B= h(ID_B|| SKx_{AB})$ and broadcasts t_2, C_2, and Z_B to the node *A*.

vi. Finally, node *A* checks $h(ID_B||SKx_{AB}))= Z_B$. If it holds, Node *A* checks if t_2'-t_2 does not exceed maximum threshold time Δt (to check message freshness). Subsequently, only if message freshness is justified, then node *A* also approves SK_{AB}.

V. SECURITY ANALYSIS

In this section we will compare between different proposed schemes with our access control protocol. We will also discuss the enhanced security features of our proposed protocol and prove that the scheme is secure against message replay attack, strong against Sybil attack and possess important security features such as user anonymity.

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

TABLE I
COMPUTATION COST COMPARISON

	ENACP[7]	[16]	Sec PACP[10]	ePACP[10]	EPACP
T_{pm}	$2T_{pm}$	$5T_{pm}$	$2T_{pm}$	$2T_{pm}$	$2T_{pm}$
T_{hc}	$2T_{hc}$	-	-	-	-
T_h	$4T_h$	$2T_h$	$5T_h$	$4T_h$	$4T_h$
T_c	--	--	--	--	$4T_c$

Table I illustrates the computational overhead comparison between ENACP [7], Huangs [16] and PACPs [10]. We can see ENACP need two point multiplications (2Tpm), two hash chain operations (2Thc) and four hash computations (4Th); on other hand Huangs scheme requires five point multiplications (5Tpm) and two hash computations (2Th), and secPACP and ePACP (in PACPs) requires (2Tpm + 5Thc) and (2Tpm + 4Th), respectively. Proposed scheme computes a two point multiplication operation (2Tpm), and four-way hash operations (4Th). However the proposed is more secured then secPACP and ePACP.

Strong against message replay attack: In this attack, an attacker wants to perform a message replay attack using previously broadcasted messages. In the proposed enhanced access control p rotocol individual nodes verify message freshness mutually (refer section IV, authentication and key establishment phase points iii, iv, and v) and make sure that no adversaries can replay the existing messages after certain duration of time, giving them less time to perform different types of attacks.

Strong against Sybil attack: In this attack, a malicious sensor poses multiple fake identities to other non-compromised nodes. Practically it is very difficult to prevent Sybil attacks as it is a type of physical attack trying to temper existing legitimate nodes by some means. However, our scheme do not transmit node IDs openly in the public channel. Hence, the individual user IDs of the nodes are not available to the adversaries. In addition, the adversaries cannot use session messages as these expires once loses freshness as discussed earlier this section. Hence, even if the adversaries capture some energy exhausted nodes, they cannot determine node IDs and making them impossible to impersonate the other nodes.

In addition, intrusion detection techniques based on mutual protection have been proposed by Buse et al. [14] [15] means that if the attacker manages to send a false identity to a legal node, then it is practical to detect the Sybil attack using a mutual protection mechanism. For this mechanism, when two or more nodes are in the direct transmission range in which the transmitted data sent by both nodes can be received by them, they are said to be mutually protected.

User anonymity: Our scheme do not transmit node IDs openly as already mentioned in this section. Hence, node IDs are kept secret, providing anonymity to the nodes.

VI. CONCLUSIONS

In this paper, we have pointed out that PACPs are neither secure nor practical for the real mission-critical WSN applications. PACPs have still inherent security pitfalls; and can give enough incentives to the attackers. We have shown that how a sole energy-exhausted node (i.e., a Sybil node) can easily control the big part of a mission-critical application. We have also designed an enhanced practical access control protocol which overcomes the previous drawbacks and provide practical implementation platform in WSN environment.

REFERENCES

[1] I.F. Akyildiz, W. Su, and Y. Sankarasubramamiam,"A Survey on sensor Network," *IEEE Comm. Mag.* 2002, 40, pp. 102-114.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102-114, August 2002.

[3] Y. Zhou, Y. Zhang, and Y. Fang, "Access Control in Wireless Sensor Networks," *Ad Hoc Networks* 5 (2007), pp. 3-13.

[4] H. Huang, "Novel Access Control Protocol for Secure Sensor Networks," *Computer Standard & Interfaces*, 2009, vol. 31, pp. 272-276.

[5] Y. Zhou, Y. Zhang, and Y. Fang, "access control in wireless sensor networks," ad hoc Netw., vol. 5, no. 1, pp. 3-13, jan 2007

[6] H.-F Huwang, "A novel access control protocol for secure sensor networks," Comput. Standards inter., vol. 31, no. 2, pp. 272-276, feb. 2009

[7] H-S Kim and S-W Lee, "Enhanced Novel Access Control Protocol over Wireless Sensor Networks," *IEEE Trans. on Consumer Electronics*, vol. 55, No.2, May 2009, pp. 492-498.

[8] P. Zeng, K-K. R. Choo, and D-Z. Sun, "On the Security of an Enhanced Novel Access Control Protocol for Wireless Sensor Networks," *IEEE Trans. on Consumer Electronic*s, vol. 56, No. 2, May 2010, pp. 566-569.

[9] J. Shen, S. Moh, L. Chung, "Comment: "Enhanced Novel Access Control Protocol over Wireless Sensor Networks", " *IEEE Trans. on Consumer Electronics*, vol. 56, No. 3, August 2010, pp.2019-2021.

[10] H. Lee, K. Shin, and D-H Lee, "PACPs: Practical Access Control Protocols for Wireless Sensor Networks," *IEEE Trans. on Consumer Electronics*, vol.58, No. 2, May 2012, pp.491-499.

[11] M. Tyler, "A Collusion Attack on Pairwise Key Predistribution Schemes for Distributed Sensor Networks," *In the proceeding 4th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)*, 2006, 13-17 March 2006.

[12] D. Mukhopadhyay, I. Saha, "Location Verification based defense against Sybil attack in Sensor Networks," *In the proceedings of the 8th International Conference on Distributed Computing and Networking*, 2006, pp 509-521.

[13] A. Choudhury, P. Kumar, M. Sain. H. Lim, H. J. Lee, "A strong user authentication framework for cloud computing", 2011 *IEEE Asia-Pacific Services Computing Conference*, pp. 110-115, December 2011.

[14] V. Bushe, A gupta, and A. AL-Fuqaha, "Detection of masquerade attacks on wireless sensor networks," in proc. IEEE international conference on communication. (ICC), Jun. 200, pp. 1142-1147

[15] V. Bhuse, "lightweight intrusion detection: A second line of defense for unguarded wireless sensor networks," PhD dissertation, department of computer. science., Western Michigan university, Kalamazoo, MI, USA, 2007

[16] H.F. Huwang, "A new design of access control in wireless sensor networks," *International Journal of Distributed Sensor Network*., vol. 2011, Art. no. 412145

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

Mangal Sain received the M.Sc. degree in computer application from India in 2003 and the Ph.D. degree in computer science in 2011. Since 2012, he has been an Assistant Professor with the Department of Computer Engineering, Dongseo University, South Korea. His research interest includes wireless sensor network, cloud computing, Internet of Things, embedded systems, and middleware. He has authored over 50 international publications including journals and international conferences. He is a member of TIIS and a TPC member of more than ten international conferences.

Amlan Jyoti Chaudhary received his MS from Dongseo University in 2012 in computer science. Since then he has been an assistant professor at Department of ECE, Kaziranga University, India. His research interest include cryptography, Network Security, Security in Cloud computing and WSN. His publication include paper on network security, Secure Authentication and designing new algorithm for secure network architecture.

Satyabrata Aich is working as a researcher in the field of computer engineering He has over four years of teaching, research and industry experience in India and abroad. He has published many research papers in journals and conferences in the realms of Supply Chain Management and data analytics. His research interests are natural language processing, Machine learning, supply chain management, data mining.

Hoon-Jae Lee received his BS, MS, and PhD. degrees in Electrical Engineering from Kyungpook National University, Daegu, South Korea, in 1985, 1987, and 1998, respectively. He is currently a professor in the Department of Information and Communication Engineering at Dongseo University. From 1987 to 1998, he was a research associate at the Agency for Defense Development (ADD). His current research interests include developing secure communication system, side-channel attack, and ubiquitous sensor network/radio frequency identification security.

Copyright ⓒ 2018 GiRI (Global IT Research Institute)

Volume 7 Issue 4, July. 2018, ISSN: 2288-0003

ICACT-TACT JOURNAL

GIRI

Global IT Research Institute

1713 Obelisk, 216 Seohyunno, Bundang-gu, Sungnam Kyunggi-do, Republic of Korea 13591
Business Licence Number : 220-82-07506, Contact: tact@icact.org Tel: +82-70-4146-4991