International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

A Security Approach for Wireless Sensor Network in Agriculture Industry

Piya Techateerawat [a*]

[a] *Department of Electrical and Computer Engineering, Faculty of Engineering, Thammasat University Khlong-Luang, Pathumthani, THAILAND*

ARTICLEINFO

Article history:
Received 24 April 2013
Received in revised form
20 August 2013
Accepted 26 August 2013
Available online
26 August 2013

Keywords:
Security Framework;
Key Distribution;
Intrusion Detection System

ABSTRACT

An overview of agriculture industry is involved with large area, farmers and agriculture products. A large scale of area requires time consuming for collecting data to make decision on agriculture (e.g. watering, pruning and harvesting.). From these requirements, wireless sensor network can be a supported technology because it can deploy distributed and construct network sharing among their group. In general, security solution needs an experienced and skilled specialist to set up, maintain and troubleshoot. This is a challenge for wireless sensor network to implement in agriculture industry.

Our security approach is presented related factors and customized configuration for the process of deployment, maintenance, information feedback. This paper presents the security mechanism to support the needs of self-setup and minimum operation for wireless sensor network in agriculture industry. The security module has automated initiate key by HKD protocol and has Adaptive IDS to alert when threat is detected via speaker. This system is also simplified the configuration, deployment and maintenance by only powering on and system will then initiate the key among the agents. As a result, this security module is proposed to balance between the moderate security with the limited resource and technician.

*Corresponding author (P.Techateerawat). Tel/Fax: +66-2-5643001 Ext.3249. E-mail address: tpiya@engr.tu.ac.th. ©2013 International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies. Volume 4 No.4 ISSN 2228-9860 eISSN 1906-9642. Online Available at http://TuEngr.com/V04/269-282.pdf

Nomenclature and Symbols

We use the following notation to describe a protocol and operation in this paper:

$\mathbf{M_1 \mid M_2}$	the concatenation of message M_1 and M_2
H[D]	the hash function which digests data D
$\mathbf{F_1[D]}$	the first one-way function which covert data D
$\mathbf{F_2[D]}$	the second one-way function which covert data D
$\mathbf{K_C}$	the common key to use when secret key is not set up
$\mathbf{K_M}$	the master key to generate keys for the 1st time.
$\mathbf{K_0}$	the storing key to save previous key session
K[M]	encryption of message M with key K
$\mathbf{S_1}$	the signature of key from F_1
$\mathbf{S_2}$	the signature of key from F_2
L, N	the random numbers in the key generating

1. Introduction

A wireless sensor network is developed for self-established network infrastructure with data sensor technology. In addition, it can reduce the complexity of device deployment on small and large area. The sensor data can monitor different types of data e.g. monitoring water, humidity, temperature and etc. These could be the keys to support various industries including the agriculture industry [1-3].

A security approach for wireless sensor network is required to consider three main factors: area, farmers and agriculture products. A large area of agriculture field requires a technology that has a low cost of technology devices to cover large area of farm. A farmer is skilled person for specific agriculture but requires the simplified technology for less time learning as well as less human-error for the user. For the last factor, agriculture product is the main objective for agriculture industry, therefore selected technology needs to support the growing process and improve the agriculture product in the final result.

As SensorScope [4] presents the benefit of wireless sensor network could be operated as a simple management system. The end-user can minimize the learning curve by let the self-operated algorithm to manage the technical task such as power management, sensor data,

network infrastructure and ad-hoc management. In addition, it is expected that the network is flexible and adaptable to the additional of new nodes. It also manages routing changes in the event of node failure. These features also need to consider the energy efficiency which is the most critical aspect of sensor network application [5-8].

However, security in sensor network needs to consider variety of factors for a completed approach. This paper shows the suggested factors and customization solution for agriculture industry by demonstration in ordered as 1) A security approach for wireless sensor network, and 2) A mechanism for security in wireless sensor network.

2. A Security Approach for Wireless Sensor Network

A security approach for wireless sensor network is covered: agriculture industry challenge, user approach and technology implementation. These approaches are the support factors for successive in security implementation. Although difference agriculture needs a difference solution, a main structure and framework can be prepared for agriculture field [9].

The agriculture industry challenge is taking part on the location, device handling, activities and personas. The location of agriculture can be differentiated for each place. In the case of rural area, the infrastructure and technology platform cannot be expected to be installed. The set up configuration of wireless sensor network relies on data transfer as well as security establishing. For device handling scheme, a farmer and equipment can be changed and cannot rely on the exact procedure or timeline. The activities are also difference from types of agriculture and time but the main time during seeding and harvesting need to be rush. Therefore, only a compulsory activity for security in wireless sensor network is needed to involve with agriculture user. In the last, special needs or personas needs special equipment and simplified interaction [10].

The user approach is the second challenge for security implementation. As part of operation people is in rural area, communication can be more effective by customized interaction as a local culture. Also, survey and training should have communicate in person can gain more attraction and cooperative with the system. The final solution also should fill the gap between core technology and user familiarity [11].

*Corresponding author (P.Techateerawat). Tel/Fax: +66-2-5643001 Ext.3249. E-mail address: tpiya@engr.tu.ac.th.

Volume 4 No.4 ISSN 2228-9860 eISSN 1906-9642. Online Available at http://TuEngr.com/V04/269-282.pdf

3. Security Out-of-the-Box

The following part presents the core technology that can be used as security mechanism in wireless sensor network. The main benefit is self-constructed, use limited energy and maintain the sufficient security for agriculture application. The system is based on the SensorScope [4] but adds the solution module on top of the system. The security module is consisted with two main functions: HKD and Adaptive IDS**.**

3.1 Hint Key Distribution (HKD)

HKD [12] is inspired by using of hint messages in ELK [13]. It uses symmetric encryption to secure transmissions. The confidentiality and simplicity are provided from encryption and decryption. When every sensor node has the secret key, it can establish secured communication without altering the routing (or tree hierarchy).

To construct a key, we describe two sides of operations. Sender and receiver have common key K_C which is used as a secret key when the key is not distributed. Master key, K_M is also installed asa part of key computation.

Two one-way functions F_1 and F_2 could minimize the computation while maintain a large key domain. There are more key possibilities to protect from intruders in guessing the secret key. In the long term, despite both sender and receiver remain computing in the same range (L, N).

select random number L
load key $K = K_M$
for $j =$ L *downto 0 do*
compute key $K = F_1[K]$
end for
store key $K_M = K$
compute hashed value $S_1 = H[K]$
select random number N
for $j =$ N *downto 0 do*
compute key $K = F_2[K]$
end for
compute hashed value $S_2 = H[K]$
encrypt message $(S_1|S_2)$ *with key* K_C
broadcast message $K_C(S_1|S_2)$

Figure 1: Generating hint procedure in HKD.

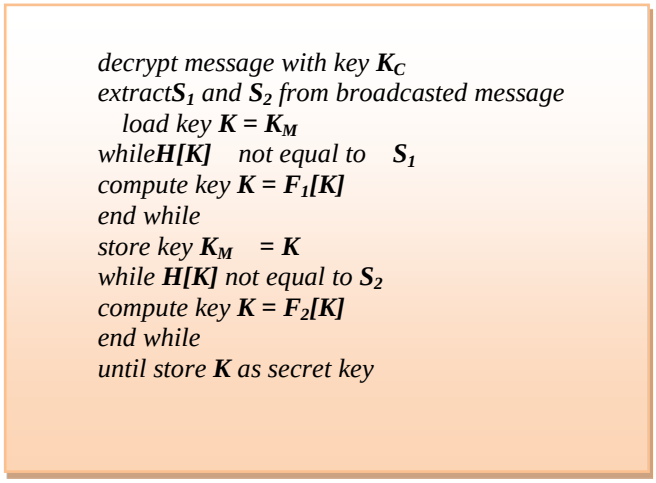

Figure 2: Receiver procedure in HKD

Intruders require a large set of key to attack. Since secret key is generated from previous key, this adds up the number of possible keys to L^tx N to attack (where t is number of key distribution).

Sender Process

Secret key is generated from repeatedly computing one-way function F_1 and F_2. Then, sender broadcasts encrypted message which contains signature key from both F_1 and F_2 as in figure 1.

Receiver Process

When broadcasted message is received, receiver decrypts message and extracts signature S_1 and S_2. Then it repeatedly computes K_M until its hash value matches with S_1 and then repeats for S_2 as in figure 2.

Key Renewing Process

Sender and receiver start computing the secret key from previous key, K_0 instead of K_M. So there is no key duplication and ithelps minimizing the computation.

3.2 Adaptive Intrusion Detection System (Adaptive IDS)

Adaptive Intrusion Detection System (Adaptive IDS) [14] uses either anomaly detection or misuse detection. This paper uses a decision mechanism derived from Siraj and et

*Corresponding author (P.Techateerawat). Tel/Fax: +66-2-5643001 Ext.3249. E-mail address: tpiya@engr.tu.ac.th.

Volume 4 No.4 ISSN 2228-9860 eISSN 1906-9642. Online Available at http://TuEngr.com/V04/269-282.pdf

al. [15]. Within IDS, tasks are combined to minimize energy consumption. So, anomaly detection is proceeding while event data is pre-checked for misuse detection. The signature records are combined to a single database to reduce memory use. In normal situation, both systems operate with the same record.

Event Data is the network activities (for example numbers of success and failure of authentication). This set of data is prepared for further analysis.

Misuse Detection analyses event data from signature record. In case of event data is matched with any rules, alert signal will be raised. Otherwise, event data is forwarded to anomaly detection for further analysis.

Anomaly Detection compares event data with signature record to find harmful attacks from intruder. If probability reaches the risk threshold, alert signal will be raised.

Signature Record is a database which contains signature of unauthorized and high risk activities. In addition, each record contains level of harm for misuse detection and probability chance for anomaly detection.

Voting algorithm for the selection of nodes in distributed defense consists of four steps: vote preparation, voting, vote counting, and IDS activating. There are two parameters in this algorithm. First, number of hop count determines the threshold of selection for the number of hops between a candidate node and itself. A larger hop count means less activated nodes and each IDS node has to take responsibility for more nodes. Second, the voting threshold is the minimum number of votes before activating IDS. The procedure allows each node to elect its gateway. The stages are:

1. *Vote Preparation*: Each node decides their gateway or nearest node. A hop count parameter determines distance between agent node and neighboring nodes.

2. *Voting*: Each node transmits their vote message to their gateway.

3. *Vote Counting*: To count a received vote.

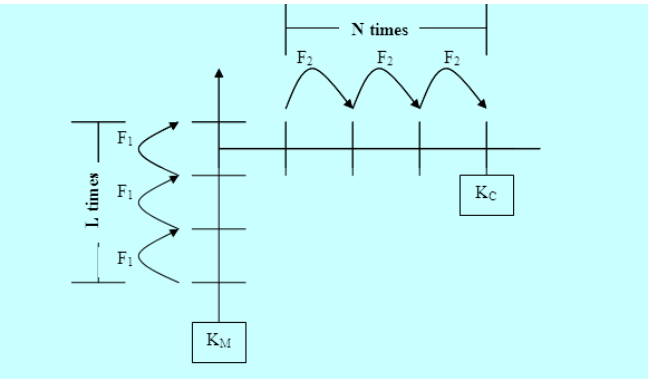

Figure 3: Procedure to find current key $K_c$by using one-way function F_1 and F_2 where L and N are random numbersfrom master key KM.

4. *IDS Activating*: If the number of votes exceeds the threshold, and IDS is then activated. The node will remain active until timeout; at this point the process 1-4 will be commenced again.

To address some of the limitations, we have further investigated the use of adaptive thresholds. The approach is outlined in the protocol flow chart of figure 4. We assume that each node has been synchronized to be accurate within a 5 second window. Initial threshold number is 0 which increases and reduces based on pre-set number. A suggestion is reducing number should be less than increasing number so activated node can be distributed wider. For example, in 80 nodes cluster we use increasing increment number as 5 and reducing increment number as 1.Note that a tree structure is not employed for the adaptive distributed defense. Instead we rely on the adaptive threshold to guide selection.

The approach shows both a positive reinforcement for the threshold, and an active reduction of threshold to promote candidate nodes for intrusion detection. The protocol also avoids the difficulty of maintenance a tree hierarchy. Instead we use the dynamics of the threshold to control which nodes are activated. This is potentially more robust.

3.3 User Interaction

The objective is to develop security solution which involves less interaction with user or farmer and simple for non-technical skilled peopleto understand and implement the system. We divide into four scenarios that system may interact with the user.

1.) Deployment: user requires not involving with complex tasksbut only turn on the devices. At the same time, devices initiate themselves and set up key by HKD protocols.

*Corresponding author (P.Techateerawat). Tel/Fax: +66-2-5643001 Ext.3249. E-mail address: tpiya@engr.tu.ac.th. Volume 4 No.4 ISSN 2228-9860 eISSN 1906-9642. Online Available at http://TuEngr.com/V04/269-282.pdf

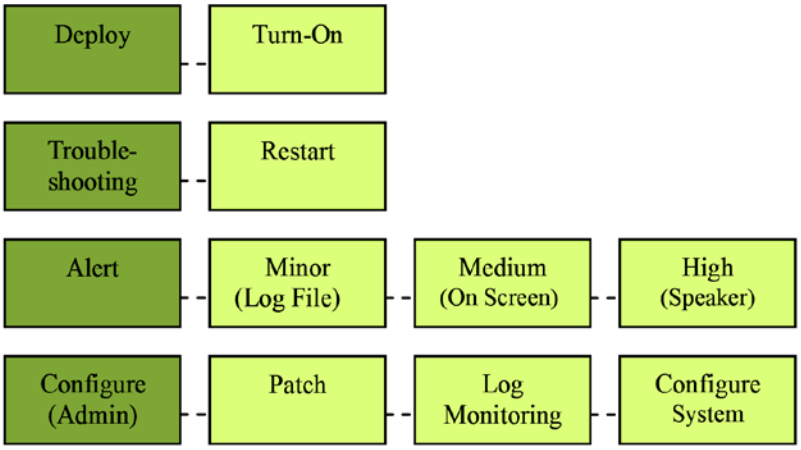

Figure 4: User Interaction for Security Module.

2.) Troubleshooting: in the case that security protocol is corrupted or mal-function user can simply re-start all the devices so HKD will start the initiate the key as well as Adaptive IDS will be restarted itself.

3.) Alert: In case that security system raises the warning to user, the system communicates to user in three levels:-

3.1) Minor Level Alert: warning will be logged on the central database.

3.2) Medium Level Alert: warning will be shown on the monitor which user can observe and monitor the system.

3.3) High Level Alert: warning will be connected high power speaker so user can immediately notice. Optional, in the complex system may connect via telephone or SMS system.

4.) Configuration: this scenario is designed for skilled people or administrator to configure the system, read the log file, upgrade the software or configure the integration system via telephone or SMS system.

4. Evaluation

4.1 Security

Brute Force Attach (BFA) is used to evaluate the resistance of SPINS and HKD. The evaluation is based on a pair of communications which follow the theory and algorithm. However, in practice, adversaries may reduce their computation time when they collect information from a group of nodes.

Among these protocols: SPINS and HKD, they protect master key with hash or one-way function. To obtain current secret key, adversary can directly perform BFA, but it is infeasible to generate next key or master key.

However, breaking current secret key requires $2^{\text{key length - 1}}$ x Computation Time. In 40 bits key length, there are 2^{40} possible keys which average half (2^{39}) must be attempted to find the correct key while 128 bits key needs 2^{127} attempts. Since UltraSparc II computes each key in 2 μs [16], in 40 bits key. It requires 1.10×10^{6} s (12.7 days). To compare with 128 bits key, it requires 3.4×10^{32} s (1.08×10^{25} years). So 128 bits key can enhance security protection as shown in figure 5. However, breaking master key requires more computation than current key. Since, it needs to compute for the entire key chain from master key to current key. To compute key chain, MD5 and SHA-1 use the same 128bits hash. Let maximum key chain length is N and assuming that adversary knows this information. To break master key, it needs to try every key chain. In each key chain, it needs to compute hash function N_0 times. Since number of computing function N_0 depends on key chain length N (for key chain length N, it requires to compute function N! times). So it must run $2^{\text{key length - 1}}$ x N! x Computation Time. Then, let the key chain length is 10 for the worst case which actual protocols use larger number. In UltraSparc II, its execution times for MD5 and SHA-1 are 39 μs and 56 μs [15]. In MD5, BFA will find the master key for 40 bits keychain in 7.78×10^{13} s (2.47×10^{6} years) and 128 bits key chain in 2.41×10^{40} s (7.64×10^{32} years). In SHA-1, it will find the master key for 40 bits key chain in 1.12×10^{14}s (3.54×10^{6}years) and 128 bits key chain in 3.46×10^{40}s (1.10×10^{33}years) as in Figure 6.

*Corresponding author (P.Techateerawat). Tel/Fax: +66-2-5643001 Ext.3249. E-mail address: tpiya@engr.tu.ac.th.

Volume 4 No.4 ISSN 2228-9860 eISSN 1906-9642. Online Available at http://TuEngr.com/V04/269-282.pdf

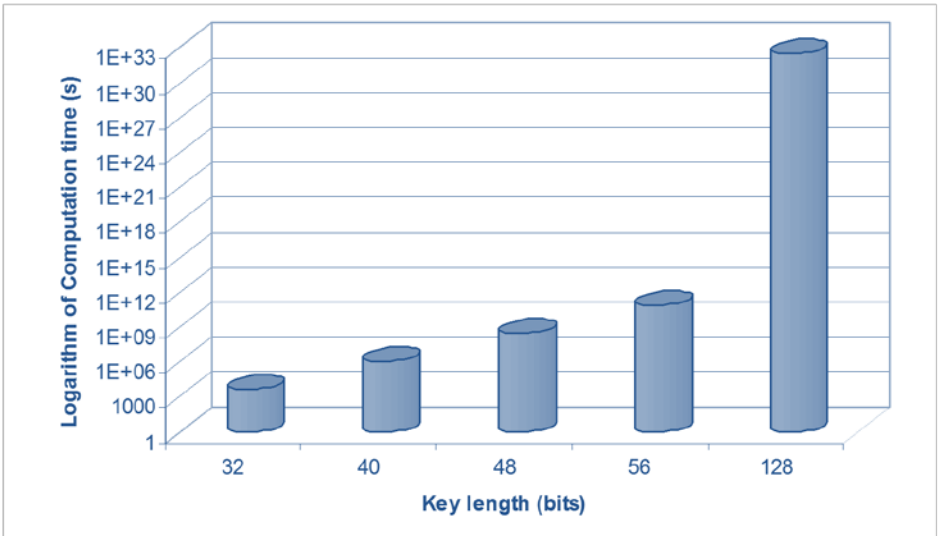

Figure 5: Logarithm of computation times for current key in brute force attack.

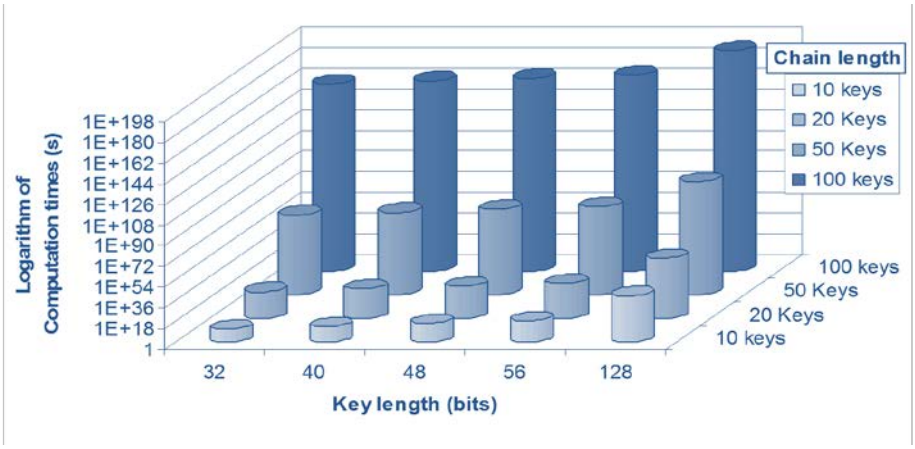

Figure 6: Logarithm of computation times for the key chain in brute force attack.

In short key length (40 bits key), it can secure data in a short period of time (less than 12 days) before renewing key. However, for sensitive information, a longer key (128 bits key) is required. To protect the system with master key, both short and long key show a secure protection from BFA. However, SPINS can renew their master key in a period of time while HKD can still uses its master key for longer. This can improve the security in the long term.

4.2 Energy Consumption

Energy consumption is the significant issue in sensor networks. MD5 consumes 0.59 μJ/Byte when comparing to 3DES computation, 6.04 μJ/Byte. So it can be assured that system has capability to operate encryption, also able to perform HKD [17-19].

Table 1 illustrates the simulation result that shows the energy consumption in HKD, SPINS and ELK. This simulation focuses on message size and energy consumption. This result presents that HKD has almost three times expected lifetime than SPINS. However, ELK in the best case scenarios reveals the best performance in the simulation.

Table 1: Energy consumption in communication.

Protocol	Message size (bytes)	Estimated operation time (days)
ELK (best case)	23-38	**967**
ELK (average)	23-38	**108**
ELK (worst case)	23-38	**53**
SPINS	598	**277**
HKD	**64**	**715**

4.3 User Interaction

User requires the least operation with security module. User needs only turning on to activate HKD and Adaptive IDS to operate. In the case that system is corrupted, user needs to re-start the system. For the output from system, user does not require to monitor regularly. In case that critical threat, system raises the alert via speaker (or telephone/SMS if integrated with this system). As a result, user requires zero-configuration and zero-maintenance for day-to-day operation.

4.4 Cost

Cost of configuration and maintenance has a benefit from zero-configuration and zero-maintenance so user does not require paying extra for security module as well as implementing and maintenance cost. This is a significant factor for agriculture in developing countries with limited budget and skilled technicians.

5. Conclusion and Future Works

According to the nature of agriculture industry, wireless sensor network can support the large area, simple setup and operation. However, the security technology is complicated and can be the challenge to implement security in wireless sensor network.

*Corresponding author (P.Techateerawat). Tel/Fax: +66-2-5643001 Ext.3249. E-mail address: tpiya@engr.tu.ac.th.

Volume 4 No.4 ISSN 2228-9860 eISSN 1906-9642. Online Available at http://TuEngr.com/V04/269-282.pdf

This paper suggests the challenge main factors: location, device handling, activities and personas. Since the agriculture can be difference in locations, equipments, activities and personas, the customized security solution is required for specific type of agriculture. However, the framework and approach can be set as a guideline. Location can affect by rural area have less or none of technology infrastructure. The equipments are varied from type of agriculture similar as the activities. Therefore, security approach needs to be simple and keep the simple interaction with user. In addition, user approach requires having a customization to match with local culture and balance with user interaction can be more effective for overall system.

This paper also presents the security mechanism to support the needs of self-setup and minimum operation for wireless sensor network in agriculture industry. The security module has automated initiate key by HKD protocol and has Adaptive IDS to alert when threat is detected via speaker. This system is also simplified the configuration, deployment and maintenance by only powering on and system will then initiate the key among the agents. Since HKD uses key chain, the key is updated regularly to increase the security of system. The benefit from HKD is used less energy from communication with hint message as well as error handling when message is lost during key change. In addition, HKD also reduces the energy consumption by small size of message and increases the operation time. As a result, this security module is proposed to balance between the moderate security with the limited budget and knowledge of user where focusing on agriculture in developing country.

For the future, research should focus on error-handling of security system. Since the current model needs to restart system to initiate the key, the future model should provide flexible solution for non-technician user to manage the security issues.

6. Acknowledgements

We would like to thank Faculty of Engineering, Thammasat University, Optical and Quantum Communication Research Lab, National Research Council of Thailand and the Thailand Research Fund (TRF) for the support and cooperation.

7. References

[1] A. Dunkels, T. Voigt, N. Bergman and M. Jonsson. “The Design and Implementation

of an IP-based Sensor Network for Intrusion Monitoring", *Swedish National Computer Networking Workshop*, Nov 2004

[2] C. Murthy and B. Manoj. *Ad Hoc Wireless Networks*, Ed 1st, Prentice Hall PTR, United States of America, 2004, pp. 204-219

[3] A. Hac. *Wireless Sensor Network Designs*, Ed 1st, Wiley, Great Britain, 2003, pp. 213-234

[4] G. Barrenetxea, F. Ingelrest, G. Schaefer, M. Vetterli, O. Couach and M. Parlange,"SensorScope: Out-of-the-Box Enbironmental Monitoring", *Information Processing in Sensor Networks*, 2008.

[5] A. Perrig, J. Stankovic and D. Wagner. "Security in Wireless Sensor Networks", *Communications of the ACM*, vol. 47, pp 53-57, Jun 2004

[6] E. Shi and A. Perrig. "Designing Secure Sensor Networks", *IEEE Wireless Communications*, pp. 38-43, Dec 2004

[7] J. Newcome, E. Shi, D. Song and A. Perrig. " The Sybil Attack in Sensor Networks: Analysis & Defenses", *Information Processing in Sensor Networks 2004*, pp. 259-268, Apr 2004

[8] J. Deng, R. Han and S. Mishra. "Security Support for In- Network Processing in Wireless Sensor Networks", *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pp. 83-93, 2003

[9] J. Burrell, T. Brooke and R. Beckwith. "Vineyard Computing: Sensor Networks in Agricultural Production", *IEEE Pervasive Computing*, pp. 38-45, Jan 2004

[10] M. de Sá and L. Carriço. "Lessons from early stages design of mobile applications", *Proceedings of the 10th international conference on Human computer interaction with mobile devices and services (MobileHCI '08)*. ACM, New York, NY, USA, 127-136, 2008.

[11] A. Sukumaran, S. Ramlal and et. el. "Intermediated technology interaction in rural contexts". *Proceedings of the 27th international conference extended abstracts on Human factors in computing systems (CHI EA '09)*. ACM, New York, NY, USA, 3817-3822, 2009.

[12] P. Techateerawat and A. Jennings. "Hint Key Distribution for Sensor Networks", in *International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE 2006)*, 2006.

[13] Penrig, D. Song, and D. Tygar, "ELK, a new protocol for efficient large-group key distribution," presented at *Security and Privacy, 2001*. S&P 2001. Proceedings. 2001 IEEE Symposium on, 2001.

[14] P. Techateerawat and A. Jennings. "Adaptive Intrusion Detection in Wireless Sensor

*Corresponding author (P.Techateerawat). Tel/Fax: +66-2-5643001 Ext.3249. E-mail address: tpiya@engr.tu.ac.th. Volume 4 No.4 ISSN 2228-9860 eISSN 1906-9642. Online Available at http://TuEngr.com/V04/269-282.pdf

Networks", in *The 2007 International Conference on Intelligent Pervasive Computing (IPC-07)*, 2007.

[15] A. Siraj, S. Bridges and R. Vaughn. "Fuzzy Cognitive Maps for Decision Support in an Intelligent Intrusion Detection System", *IFSA World Congress and 20th NAFIPS International Conference 2001*, vol. 4, pp. 2165-2170, Jul 2001

[16] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F.Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes " in *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications San Diego*, CA, USA ACM Press, 2003 pp. 151-159

[17] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications.* San Diego, CA, USA: ACM Press, 2003, pp. 151-159.

[18] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "Analyzing the energy consumption of security protocols," in *Proceedings of the 2003 international symposium on Low power electronics and design*. Seoul, Korea: ACM Press, 2003, pp. 30-35.

[19] J. D. Touch, "Performance analysis of MD5," in *Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication*. Cambridge, Massachusetts, United States: ACM Press, 1995, pp. 77-86.

Dr. P. Techateerawat is Assistant Professor of Computer Engineering Department, Faculty of Engineering, Thammasat University. He received his B.Eng. from University of New South Wales, Australia with Honors in 2004. He continued his PhD study at Royal Melbourne Institute of Technology University, Australia, where he obtained his PhD in Wireless Sensor Network Security. Dr. PiyaTechateerawat current interests involve applications of Sensor Network, Security and Quantum Cryptography.

Peer Review: This article has been internationally peer-reviewed and accepted for publication according to the guidelines given at the journal's website.