International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

A Security Approach for Wireless Sensor Network in Agriculture Industry

Piya Techateerawat
Department of Electrical and Computer Engineering
Faculty of Engineering, Thammasat University
Khlong-Luang, Pathumthani, Thailand
tpiya@engr.tu.ac.th

***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). Farmers are mainly focused on agriculture products and process, so providing an extra effort on technology should keep to the minimum. The agriculture products are the final result which is the most important for agriculture process. Therefore, the best product is the goal of agriculture industry.**

Wireless sensor network is a technology that can distributed deploy and construct network sharing among their group. The main advantage of sensor network are collecting sensor data and transferring back to base center without the maintenance of power supply, network structure and data control. Therefore, wireless sensor network is one of the candidate solutions for future in assisting agriculture industry.

In general, security solution needs an experienced and skilled specialist to set up, maintain and troubleshoot. This is a challenge for sensor network to implement in agriculture industry. The main three factors (large area, farmers and agriculture products) are also need to be considered.

Our security approach is presented related factors and customized configuration for the process of deployment, maintenance, information feedback. The detailed process is concealed from farmer. Only selected information is showing to the farmer. The security solution should be customized the configuration for the specific agriculture and area. The scenarios, matching with familiar technology and simplified devices is the supportive of success solution. Therefore, the security approach is provided a solution for setting-up the security in agriculture industry. As a result, security implementation for wireless sensor network in agriculture industry can be more effortless by the given security approach.

***Keywords* - Sensor Network, Security, Agriculture, Farm, Management.**

I. 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, farmer 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 a suggested factors and customization solution for agriculture industry by demonstration in ordered as 1.) A security approach for wireless sensor network, 2.) A mechanism for security in wireless sensor network.

II. 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. Wireless sensor network is only need to setup and rely for 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 type 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

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

with agriculture user. In the last, special needs or personas needs special equipments 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].

III. A Mechanism for Security in Wireless Sensor Network

The following part presents the core technology that can be use as security mechanism in wireless sensor network. The main benefit is self-constructed, use limited energy and maintain the sufficient security for agriculture application.

Notation

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

M1 | M2 is the concatenation of message M1 and M2
H[D] is the hash function which digests data D
F1[D] is the first one-way function which covert data D
F2[D] is the second one-way function which covert data D
KC is the common key to use when secret key is not set up
KM is the master key to generate keys for the 1st time.
K0 is the storing key to save previous key session
K[M] is encryption of message M with key K
S1 is the signature of key from F1
S2 is the signature of key from F2
L, N are the random numbers in the key generating

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 $K_C(S_1|S_2)$

Fig.1. Generating hint procedure in HKD

IV. Security Out-of-the-Box

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

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 KC which is used as a secret key when the key is not distributed. Master key, KM is also installed as a part of key computation.

Two one-way functions F1 and F2 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).

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^t x N to attack (where t is number of key distribution).

decrypt message with key K_C
extract S_1 *and* S_2 *from broadcasted message*
load key $K = K_M$
while $H[K]$ *not equal to* S_1
compute key $K = F_1[K]$
end while
store key $K_M = K$
while $H[K]$ *not equal to* S_2
compute key $K = F_2[K]$
end while
until store K *as secret key*

Fig.2. Receiver procedure in HKD

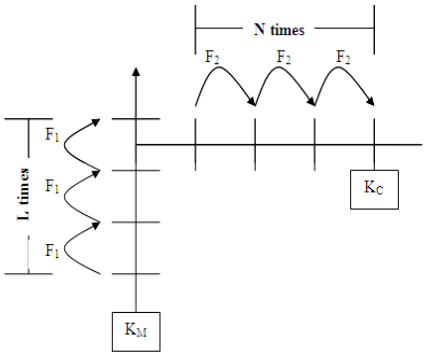

Fig.3. Procedure to find current key K_C from master key K_M by using one-way function F_1 and F_2 where L and N arerandom numbers.

Sender Process

Secret key is generated from repeatedly computing one-way function F1 and F2. Then, sender broadcasts encrypted message which contains signature key from both F1 and F2 as in figure 1.

Receiver Process

When broadcasted message is received, receiver decrypts message and extracts signature S1 and S2. Then it repeatedly computes KM until its hash value matches with S1 and then repeats for S2 as in figure 2.

Key Renewing Process

Sender and receiver start computing the secret key from previous key, K0 instead of KM. So there is no key duplication and it helps minimizing the computation.

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 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 number 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

The 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.
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.

User Interaction

The objective is to develop security solution which involves less interaction with user or farmer and simple for non-technical skilled people to 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 tasks but only turn on the devices. At the same time, devices initiate themselves and set up key by HKD protocols.
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.

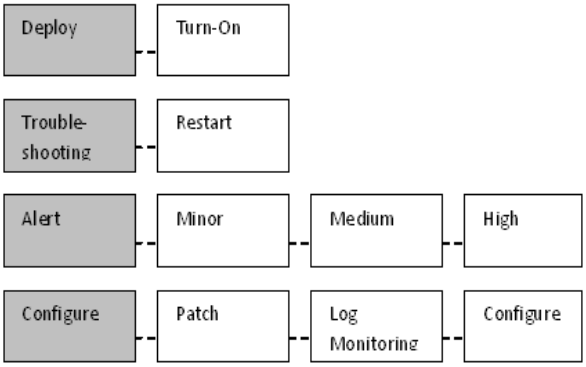

Fig.4. User Interaction for Security Module

V. 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.

This paper suggests the challenge main factors: location, device handling, activities and personas. Since the agriculture can be difference in location, 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.

Acknowledgment

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.

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 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

Author’s Profile

Piya Techateerawat
is currently teaching and researching at Thammasat University. He received his Ph.D. in Computer Engineering from Royal Melbourne Institute of Technology and his Bachelor of Computer Engineering from University of New South Wales.