2011 International Conference on Asia Agriculture and Animal
IPCBEE vol.13(2011) © (2011)IACSIT Press, Singapore

Wireless Sensor Network: Security Out-of-the-Box for Agriculture

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

Abstract. Agriculture accounts for a large scale of developing country but managing information on the field is lacked of skilled resources, budget and effective information system. The information system should be easy to access and maintain. As a result, developed out-of-the-box monitoring system includes wireless sensor network agents that operate and maintain for data gathering, hardware and network architecture. However, security solution requires maintaining the data integrity and confidential information.

In general, security protocol requires skilled technician to configure and maintain the system. Also, monitoring, updating and configuring the system are too complex for farmers to understand and utilize. Therefore, we propose the security out-of-the-box system for wireless sensor network in agriculture. The protocol contains HKD and Adaptive IDS so key chain is updated frequently and randomly as well as monitoring system and alert when threat is founded.

Our system is covered during the process of deployment, maintenance, information feedback and alert. Deployment and maintenance are hindered from farmer. Farmer only reads the information feedback and alert. The information feedback is simplified to number of connected agent. Alert feedback is simplified to 3 levels: 1.Low level alert 2.Medium level alert 3.High level alert. Low level alert is kept the event information in the log of central database. Medium level alert acknowledges the user on screen/dash board. High level alert raises the high pitch voice via speaker or sends SMS to farmers' mobile phone (if available). Overall, farmers are required only powering on the devices to operate the security out-of-the-box system.

Keywords: Sensor Network, Security, Out-of-the-Box, Agriculture, Farm, Management

1. Introduction

Sensor networks are developed for deployment at locations without infrastructure support. It may provide a solution to many applications including agriculture for monitoring water, humidity, temperature and etc [1-3].

Out-of-the-Box system is proposed for ready to deploy including hardware, network architecture and management. As SensorScope [4] shows that sensor network could be implemented simple management system. The end-user can ignore the inner mechanism such as power source, sensor, network design, neighborhood management, network routing, synchronizing and power management.

However, security in sensor network needs to be added in the out-of-the-box monitoring system to ensure the integrity and privacy. However, security of sensor networks is limited by the nature of wireless, network structure and resources. 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].

This paper presents the integrated security solution for out-of-the-box wireless sensor network system which focuses on agricultural implementation. Since agriculture is a significant production in most of developing countries, data management helps improving the system effectiveness and increasing

productivity. The limitation of agriculture in those countries is lack of skilled technicians especially IT and engineering. Also, data management requires the security in moderate level where data is important. However, it is a less critical than other industries such as financial, banking and health industry. Therefore, this paper proposes integrated security solution by using Hint Key Distribution (HKD) and Adaptive Intrusion Detection System (Adaptive IDS) to balance between simplicity of usage and security of system. Power consumption in this system also performs better than using similar protocols e.g. Security Protocols for Sensor Networks (SPINS) and Efficient Large-Group Key Distribution (ELK).

2. Notation

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

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
L, N	are the random numbers in the key generating

3. 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

3.1. Hint Key Distribution (HKD)

HKD [9] is inspired by using of hint messages in ELK [10]. 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).

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.

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.

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.

3.2. Adaptive Intrusion Detection System (Adaptive IDS)

Adaptive Intrusion Detection System (Adaptive IDS) [11] uses either anomaly detection or misuse detection. This paper uses a decision mechanism derived from Siraj and et al. [12-14]. 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.

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. 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 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.

4. Evaluation

4.1. Hint Key Distribution (HKD)

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 2key 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 [15], in 40 bits key. It requires $1.10x10^{6}$ s (12.7 days). To compare with 128 bits key, it requires $3.4x10^{32}$ s ($1.08x10^{25}$ years). So 128 bits key can enhance security protection. 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 128 bits hash. Let maximum key chain length is N and assuming that adversary know 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 key chain in $7.78x10^{13}$ s ($2.47x10^{6}$ years) and 128 bits key chain in $2.41x10^{40}$ s ($7.64x10^{32}$ years). In SHA-1, it will find the master key for 40 bits key chain in $1.12x10^{14}$ s ($3.54x10^{6}$ years) and 128 bits key chain in $3.46x10^{40}$ s ($1.10x10^{33}$ years).

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 [16-18].

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

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 the limited with budget and skilled technicians in developing countries, security out-of-the-box is proposed for agriculture industry. The system which is proposed to meet the requirement for user in the agriculture industry needs to balance between usability and security. User should involve the configuration, deployment and maintenance as the least number. In addition, the interaction and responsive from system should be simplified to meet the behavior of agriculture life style.

This paper propose the security module which 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.

6. Acknowledgements

For this paper, we would like to thank Thammasat University and the National Research University Project of Thailand Office of Higher Education Commission 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] 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.

[10] 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.

[11] P. Techateerawat and A. Jennings. “Adaptive Intrusion Detection in Wireless Sensor Networks”, in *The 2007 International Conference on Intelligent Pervasive Computing (IPC-07)*, 2007.

[12] 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

[13] T. Ohta and T. Chikaraishi. “Network Security Model”, *International Conference on Information Engineering 1993* , vol 2, pp. 507-511, 1993

[14] J. Tao, L. Jiren and Q. Yang “The research on Dynamic Self-Adaptive Network Security Model”, *International Conference on Technology of Object-Oriented Language and Systems*, pp. 134-139, 2000

[15] 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

[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] 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.

[18] 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.