Secure Key Management Protocol in the Wireless Sensor Network

Yoon-Su Jeong*, and Sang-Ho Lee*

Abstract: To achieve security in wireless sensor networks (WSN), it is important to be able to encrypt messages sent among sensor nodes. We propose a new cryptographic key management protocol, which is based on the clustering scheme but does not depend on the probabilistic key. The protocol can increase the efficiency to manage keys since, before distributing the keys by bootstrap, the use of public keys shared among nodes can eliminate the processes to send or to receive keys among the sensors. Also, to find any compromised nodes safely on the network, it solves safety problems by applying the functions of a lightweight attack-detection mechanism.

Keywords: Cluster, Key Management Protocol, WSN

1. Introduction

Digital images have many applications in daily life, including for digital cameras and HDTV (High Definition Television), and in areas of research and technology such as GIS (Geo-graphical Information System). The datasets collected by image sensors are generally contaminated by noise, which can be introduced by transmission errors and compression. The problem of image de-noising is that of recovering an image that is cleaner than its noisy observation. Thus, noise reduction is an important technology in terms ofimage analysis, and it is the first step to be taken before images are analyzed [1].

Recent developments in computer and communication technology have made it easier to expand the WSN (Wireless Sensor Network) [1]. As good examples of sensor network application, WSN has been applied to military sensing and tracking, environmental monitoring, patient monitoring, and smart environment. The security issue is very important for sensor nodes installed in dangerous places. In order to offer security to the WSN, communication needs to be encoded and authenticated; there have been some partial solutions to achieve a stable communication between sensor nodes. There are three key management methods including a distribution key method, a dissymmetric encryption method, and a key pre-disposition method. The first one is difficult to apply to a structural base-free environment such as the sensor network. The second is undesirable for application in Diffie-Hellman or RSA where sensor nodes have limited calculation and energy [4]. For the last one, all of the information should be decided in advance, but it is hard to obtain sufficient preliminary knowledge because it is arbitrarily made to install the sensor nodes. In this paper, the suggested technique uses the inter-sensor sharing public key during bootstrap before pre-disposition, so as not to require the sensor key transmission/reception process. Therefore, it is more effective in terms of key management than the existing technique.

The remainder of this paper is organized as follows: Section 2 presents some related works; Section 3 describes the considered wireless sensor network model and proposes a hierarchical key management protocol which consists of sub-protocols for key distribution, sensor node addition, node key revocation, key renewal, and also describes the assumptions made in the protocol and the design choice;. Section 4 presents the simulation setting and environment and shows the simulation results for the proposed protocol; and, finally, Section 5 draws the conclusions.

2. Related Work

One method of key distribution for WSN uses the base-system to great extent, or is based on a pre-distribution method. In particular, a study for minimizing the energy needed to form sensor network structures has actively progressed, and the clustering structure is rated as having the greatest performance in terms of energy efficiency.

BS (Base Station) is a reliable sensor node with similar performance features to a work station, creating stronger security. However, the key management method has various drawbacks in that the confidentiality before and after key distribution is not guaranteed, it cannot nearly exists BS with stronger functions, and a large-scale sensor network environment is impossible to control. Based on the Eschenauer-Gigor technique, [2] applied a q-composite random key pre-distribution method to the technique in order to strengthen the security for the key set-up. However, this technique does not take sensor network features into consideration, but stochastically distributes the key, so that inter-sensor node public key is highly unlikely to exist. Blundo's techniques focus on cost-saving

Manuscript received January 24, 2006; accepted March 3, 2006.
Corresponding Author: Yoon-Su Jeong

* Dept. of Electronics and Computer Engineering, Chungbuk National University, Cheong-Ju, Korea (bukmunro@netsec.cbnu.ac.kr, shlee@chungbuk.ac.kr)

for communication, so that memory consumption is not in a group member. Also, at SPINS suggested by Perrigetis, two sensor nodes cannot directly make the secret key. However, the base station of a reliable third party was needed to set the secret key. Tatebayashi, Matsuzaki and Newman thought that key distribution for resource consumption in the mobile environment is inefficient, since much time and energy are needed to find the public key. In the authentication execution method, the public keys of the cluster heads should be distributed to all of the cluster heads. Since in this method the cluster heads should distribute their own public keys to all the cluster heads, there is a large communication overhead. In Khalili's method, the public keys of corresponding nodes are led by a master public key that is distributed when the nodes participate in the network and open the host ID publicly, and as many partial personal keys as the number of thresholds corresponding to the ID from peripheral nodes are obtained, thereby acquiring a perfect personal key. However, the method cannot clearly authenticate the subject requesting the secret key, and is therefore weak to a man-in-the-middle attack.

3. Cluster-based Key Management Protocol Design

The cluster-based key management protocol proposed in this paper uses a method of symmetry key and expresses protocol as a location algorithm in order to perform key management in the wireless sensor network. In addition, safe communication between SN (Source Node) and BS (Base Station) is enabled by using pre-set keys. The operation of each object in the key management protocol is assumed as below:

① Sensors: no assumption is made that the sensor is reliable or may be abused.

② Gateways: All the gates in the network can directly communicate with each other and perform broadcast communication. It is assumed that safe group communication will occur between gateways [3].

③ Command node: safe and reliable regarding all the nodes of the sensor network.

The key management protocol proposed in this paper is aimed at efficiently clustering the sensor network between gate nodes with high energy. Using a symmetry key mechanism, the proposed protocol performs 4 subordinate protocols including key distribution/addition/abolition/renewal during the life cycle of the sensor network. Each detailed subordinate approach method performs key management-related extensible calculating or the calling of a key-creating sensor.

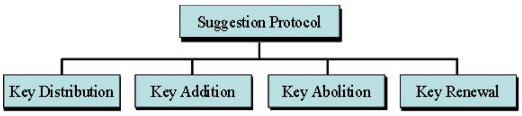

Fig. 1. Experimental Results

Key distribution uses a secret key mechanism and pre-stores 2 keys at the sensor through a pre-distribution method. One of keys stored at the sensor is shared with the gateway and the other is shared with the command node. In general, since sensors are not reliable and their memory is consumed, only a small number of keys are stored at the sensor, which is beneficial to network security.

Table 1: Protocol major terms

Concept	Explanation
C	Command node
G_i	Gateway i
S_i	Sensor node i
G	Entire gateway
S	Entire sensor node
id_i	Node recognition i
nonce	Sensor location and energy level data
S data	Sensor location and energy level data
$E_K()$	Symmetry code function using key K
||	Link operator
G_h	Head gateway used for recovery

A gateway with abundant memory resources is capable of storing many keys, but is not perfectly reliable. All the keys allocated at the gateway are compromised by the entire network and by a single gate. Under the assumption that the command node is safe, it has sufficient memory to store all secret keys in the network. Table 1 describes the major terms used in the protocol technology.

The number of keys stored at the command node is |G|+|S|. |G| represents the number of gates and |S| represents the number of sensors. Each gateway stores keys, and the command node shares the key with the sensors in the cluster.

The sensor node is allocated with an ID number for keys, expressing 2 symmetry keys set at the sensor through a pre-distribution method. In cases where the wireless transmission of ID information is not safe, the ID information is newly allocated to nodes during manufacture syntax, before disposition. Each gateway is arbitrarily allocated with |S|/|G| number of keys during the distribution period. After the keys are exchanged at the gate level, each gateway maintains the key of a sensor in the cluster and removes the rest of keys because the keys of the cluster collected by the gateway may be used by an enemy. The operation process of the protocol in the initial syntax is as follows:

① $S_i \rightarrow S: \ id_{S_i} \| id_{G_i} \| E_m[sdata \| nonce \| h(sdata)]$

② Clustering process

③ $G_i \rightarrow G: \ id_{G_i} \| E_{K_m}[nonce \| id_i\} \| h(id_i)]$

④ $G_i \leftarrow G_j: \ E_{K_M}[\,nonce! \| \{id_{S_K}\}_i\,]\|$ticket

⑤ $S_i \leftarrow G_i: \ id_{G_i} \| E_m[nonce \| id_{G_i} \| msg \| h(id_{G_i} \| msg)] \| ticket$

The new sensors added to the network are artificially disposed. The sensors are not pre-allocated to the cluster, but pre-store two keys just like other sensors, according to the steps below.

① $C \rightarrow G_i: \ E_{K_M}[nonce \| \{id_{S_K}\}_i]$

② $S_i \rightarrow S: \ id_{S_i} \| id_{G_i} \| E_m[sdata \| nonce \| h(sdata)]$

③ Clustering process

④ $G_i \rightarrow G: \ id_{G_i} \| E_{K_m}[nonce \| id_i \| h(id_i)]$

⑤ $G_i \leftarrow G_h: \ E_{K_m}[nonce \| \{id_{S_K}\}_i] \| ticket$

⑥ $S_l \leftarrow G_i: \ id_{G_i} \| E_m[nonce \| id_{G_i} \| msg \| h(msg)] \| ticket$

Key withdrawal (node abolition) is performed after detecting a compromise node and the intrusion detection mechanism informs the command node of the compromised node. If a sensor group is compromised, a sensor list of the command node from the gateway to the cluster is removed. The procedures are as follows:

① $C \rightarrow G_h: \ \begin{array}{l} nonce \| \{id_{S_K} \| id_{G_i} \| E_m[nonce' \| id_{S_K} \| h(id_{S_K}) \\ \| E_{K_m}[nonce'' \| id_{G_i} \| h(id_{G_i})]]\}_j \end{array}$

② Clustering process

③ $G_i \rightarrow S_K: \ E_m[nonce \| id_{G_i} \| h(id_{G_i})] \| ticket$

For key renewal it may be risky to use the same code key during extension. In order to perform sensor key renewal, the command node creates a new key and, in the case of withdrawal, passes the key to the gateway. While renewal is successively performed, the time intervals depend on data traffic volume, the remainder of the cryptology theory length, and the processing load at the gateway.

4. Simulation

In this paragraph, a new model developed by the Monarch Research Group at CMU (Carnegic Mellon University) for NS-2 simulation was used. The suggestion protocol uses an arbitrarily created model through an experiment scenario shown in Table 2 [2].

For safety analysis under the conditions in Table 2 {IP address, key}, batch security depends on secret key code algorithm security and the second pre-image resistance of the hash function. The hash function with the second pre-image resistance with MD5 or SHA-1 reading and 64 bit-output (if we keep one of 64 bits) is tried 2^{62} times on average, for an attacker to find the second secret key in a given IP area. Secondly, the result for the efficiency analysis found that when the number of nodes is smaller than 25, the suggestion technique is 4% higher than the pre-distribution method in terms of overhead, while the pre-distribution method is 1.5% higher on average than the suggestion technique in terms of overhead, when the number of nodes is greater than 25. In terms of the entire traffic overhead, the pre-distribution method is 0.33% higher on average than the suggestion technique.

Table 2. Scenario of the ns-2 experiments

Number of nodes	1000
Wireless range	200m
Number of sources	10
Scene	1000m X 1000m
Buffer	50 packet
Initial energy	0.5 joules
Traffic	4 pkts/s

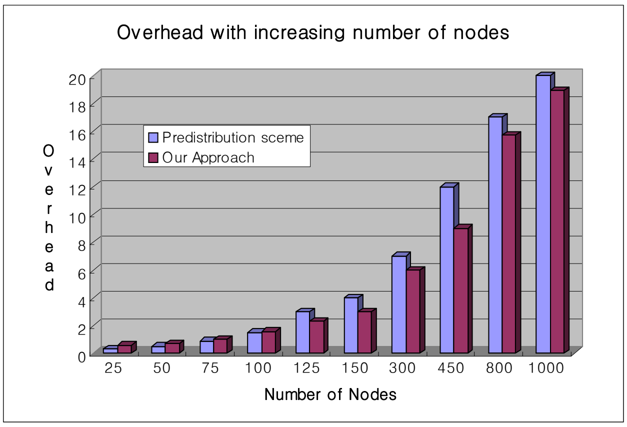

Fig. 2. Overhead of nodes

As seen in [Fig. 2], over 60% of the entire sensor nodes use less than 50J of energy, with 22%, 6.5%, and 3.5% for 50~100J, 100~150J, and 150~200J respectively.

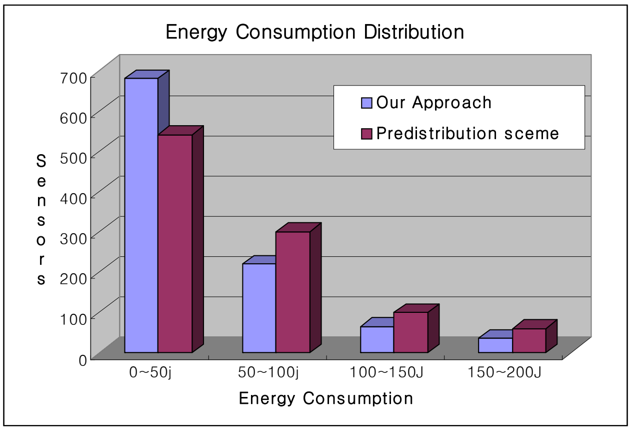

Fig. 3. Energy consumption

The average results for [Fig. 3] energy consumption vary according to the concentration and performance of the gateway.

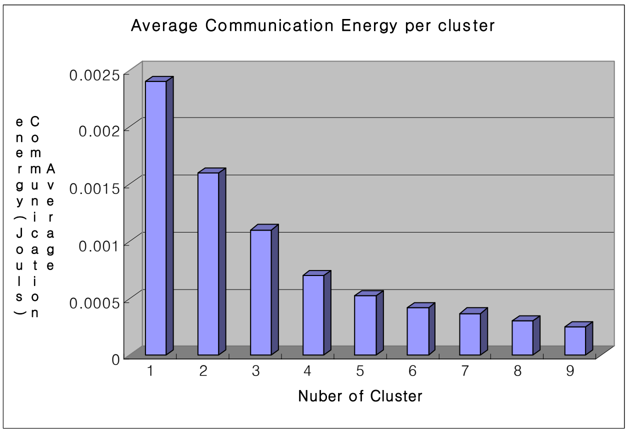

Fig. 4. Average comm. energy

In Fig. 4, the communication energy is directly proportional to the distance between two nodes. However, the ratio of average communication energy with the increasing number of clusters is inversely proportional.

Three results were obtained from the experiment. Firstly, traffic overhead increases according to the number of nodes and many controlling packets are required. Secondly, traffic overhead does not increase in a uniform manner, unlike the nodes, because the number of nodes does not increase fanwise due to the limited size of the network. Thirdly, the traffic overhead is achieved by the different traffic patterns used for simulation, as in the case of the existing technique. The node adds the traffic key by (to? through?) all the traffic packets sending nodes. In addition, the entire overhead is mainly determined by the number of data sources and by the traffic mode of the node.

5. Conclusion

A new key management protocol that does not depend on the stochastic key has been proposed to solve the problem of inter-sensor key pre-distribution in the WSN environment. A suggestion protocol removed the sensor key transmission/ receipt process, using the common key shared between nodes during bootstrap; therefore, it is effective in key management. There is a need to study a method for improving LEACH (Low Energy Adaptive Clustering Hierarchy), the representative algorithm to solve defects in the head node through re-clustering, as well as a method for combining the duplicated costs of the sensor node to the suggestion technique.

Reference

[1] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy Efficient Communication protocol for Wireless Microsensor Networks", Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, pp. 3005-3014, Jan. 2000.

[2] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for Sensor networks", In IEEE Symposium on Research in Security and Privacy, pp. 197-213, May. 2003.

[3] D. Carman, P. Kruus, and B. Matt, "Constraints and approaches for distributed sensor network security", Tech. Rep. 00-010, NAI Labs, September 2000. http://download.nai.com/products/media/nai/zip/nailabs-report-00-010-final.zip.

[4] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

Yoon-Su Jeong
Jeong received an M.S. degree from the Department of Computer Science, Chungbuk National University, in February 2000. He is currently working towards a P.H.D. degree on computer science. His research interests also include cryptography, network security, information security, AAA, and mobile communication security.

Sang-Ho Lee
Lee received a B.S. degree from the Department of Computer Science, Soongsil National University, in February 1976. He received an M.S. degree from the Depsartment of Computer Science, Soongsil National University, in February 1981. He received a P.H.D. degree from the Department of Computer Science, Soongsil National University, in February 1989. He is currently a professor in the Department of Electrical and Electronics Engineering, Chungbuk National University. His research interests include Protocol Engineering, Network Security, Network Management, and Network Architecture