Efficient Key Management Scheme in Wireless Sensor Networks

SHEN ZHAO[1, a], JUN ZHENG[1, b]

[1]Beijing Institute of Technology, Beijing, 100081 China

[a]zhaooshenn@163.com, [b]zhengjun@bit.edu.cn

Keywords: Wireless Sensor Networks, Key Management, Key Establishment, Graph Theory

Abstract. Because of the constraint of sensor nodes in energy powering, storage capacity, and computing power, in order to use less resource and improve the security of WSNs, we propose a novel key management scheme which relies on the remainder of small integer and the connected graph theory. The key management scheme improves the resiliency of WSNs to sensor nodes compromise, and minimizes the storage usage as well as communication load when establishing common keys. The major parts of the scheme include id_key generation and distribution, id_key discovery and common key establishment, secure path establishment, and incremental addition of sensor nodes. Finally, we will analyze the scheme in different aspects.

Introduction

Wireless Sensor Networks are networks which contain sensor nodes with limited battery powering, computing power and storage capability, and the sensor nodes could only communicate in short distance through wireless link [1-2]. WSNs could be used in wide range applications such as health monitoring, data acquisition in hostile environment and military operations [3]. Key establishment and management are the basics and precondition of implementing authentication and encryption in WSNs. During past several years, researchers proposed many novel and improved key management schemes [4-10], and some other schemes [11-12] which focus on efficient energy.

A basic pairwise key pre-distribution scheme is proposed early. In this scheme, a distinct pairwise key between every pair of sensor nodes is pre-distributed and stored in sensor node before sensor deployment. Probabilistic key pre-distribution scheme was proposed in [4]. Pairwise keys in the scheme are established by three phases: key pre-distribution, shared-key discovery and path key establishment. And more, an improved scheme is q-composite random key pre-distribution scheme in [5], which achieves strengthened security under small scale attack while trading off increased vulnerability in face of large scale physical attack on the network sensor nodes. Similarly, some other schemes were proposed. Such as polynomial-based pairwise key pre-distribution, polynomial pool-based key pre-distribution [6] and matrix based key pre-distribution [7]. However, as soon as one sensor node is compromised, the pairwise keys stored in the sensor node will be exposure and which influences other communication secured by the exposure pairwise keys. And the schemes consume much constraint resource such as storage and communication load during key establishment. To solve the problem mentioned above under the all kinds of constraints of WSNs, we propose a novel, improved key management scheme based on the remainder of integer. Compared to previous schemes, our scheme requires less storage, less communication load and is more resilient to sensor nodes compromise.

The rest of this paper is organized as follows. In Section 2 we describe our scheme for key establishment and management. In Section 3 we analyze the resource utilization of WSNs compared to previous key pre-distribution schemes, In Section 4 we analyze the WSNs connectivity based on random graph. In Section 5 we analyze the resiliency to sensor nodes compromise compared to previous schemes. We finally come to a conclusion of the achievements and future work in Section 6.

Overview of the Proposed Scheme

In this section, we exhibit the basic idea, and describe the scheme in detail.

ID_Key Generation and Distribution. In our scheme, the Base Node is with large storage, powerful computing, enough energy supply and a wide range of communication capability.

Firstly, the Base Node generates adequate integers. We call the generated integers id_keys, therefore, there is a pool of $id\_key_1, id\_key_2, \ldots, id\_key_i$. Also, the Base Node generates a master key for communication between Base Node and Sensor Nodes as well as among Sensor Nodes during id_key discovery and common key establishment. Moreover, the Base Node generates a small integer N as the divisor, for instance $\mathrm{N} = 2$ or $\mathrm{N} = 3$ according to practical application.

Secondly, after the generation of id_key, the Base Node starts to choose id_keys from the pool mentioned above and store the chosen id_keys in the sensor nodes before deployment. Note that one sensor node only holds one id_key. Moreover, each sensor node gets the master key and the divisor N at the same time.

In a word, after this part, there are a master key, a divisor and randomly distributed id_key in each sensor node's memory, and all the sensor nodes will be deployed in real environment.

ID_Key Discovery and Common Key Establishment. To begin with, we define id_key discovery as that one sensor node tries to find other sensor nodes that their id_keys have the same remainder when divided by the stored divisor N.

After deployment, the sensor nodes start to communicate with their neighbors within the communication range. In order to let sensor nodes could understand each other, we define the message sent by sensor node as below:

$$\mathrm{\alpha}, E_k(\alpha), E_k(RN), E_k(R), \mathrm{id}$$

a) $\mathrm{\alpha}$ denotes a number generated by sensor node randomly.
b) $E_k(\alpha)$ denotes the result of $\mathrm{\alpha}$ encrypted by master key k.
c) RN denotes the large random integer generated by sensor node randomly.
d) R denotes the remainder of the divisor N dividing id_key (R = id_key % N).
e) $E_k(RN)$ similar to $E_k(\alpha)$
f) $E_k(R)$ similar to $E_k(\alpha)$
g) id denotes the identity of sensor node

each sensor node broadcasts an $\mathrm{\alpha}$ and $E_k(\alpha)$ for the master key authentication.
When a sensor node receives a message from other sensor node, what it does as follows:

a) Decrypt the $E_k(\alpha)$ with the master key k. If the result of decryption is equal to α, then the message is legal, otherwise, the sensor node discards the message.
b) If the message is legal, the sensor node decrypt the $E_k(R)$ with the master key k. If the result of decryption is equal to the remainder that the sensor node's own, then the sensor node starts to establish common direct key, otherwise, the sensor node discards the message.

We denote the received random number as RN_1, and the sensor node's own random number as RN_2. Then $DK_{d_1,d_2} = RN_1 \oplus RN_2$ will be the common key used to encrypt the communication between sensor node d_1 and d_2.

Secure Path Establishment and Delete Master Key and Random Number. To communicate with other sensor nodes which have no common keys with, the sensor node could find a secure path between itself and the sensor nodes using the routing and switching protocol such that any two adjacent nodes in the path can communicate with securely. Then any of the two nodes which have secure path could send messages to each other through the intermediate sensor nodes along the path. In this paper, we ensure that they all could discover secure paths between themselves according to the graph theory.

As long as the secure paths are establishment, we let the sensor nodes erase the master key and random number after a period of time T. In this paper, we assume that the key establishment could be finished during the time T, and any sensor node won't be compromised by the adversary in the period.

Add New Sensor Nodes and Eliminate Compromised Sensor Nodes. Firstly, the Base Node sends a master key to a selected sensor node using an absolutely secure link. At the same time the Base Node distributes the master key and the divisor N to the new sensor nodes before deployment. After deployment, the selected sensor node sends the master key to its neighbors using common keys, and similarly, those sensor nodes which receive the master key send the master key to their linked neighbors again. Because the network is connective, all the sensor nodes could get the master key rapidly. Finally, when all the sensor nodes get the master key, a new key establishment starts. Also, after a period of time T, the sensor nodes erase the master key and random number.

In real hostile environment, it's unavoidable that some sensor nodes are compromised by adversary. The WSNs monitor the whole network and detect the compromised sensor nodes. When the WSNs detect the compromised sensor nodes, the Base Node will send the ids to all the sensor nodes, and the sensor nodes erase the corresponding common keys and ids which are stored in the memory. After the above steps, the compromised sensor nodes are eliminated completely.

Utilization of Resource

In this section, we analyze the utilization of resource compared to previous schemes, and exhibit the achievement of our scheme.

Storage Utilization. In our scheme, each sensor node only stores an id_key, a divisor N, and a master key, which reduces storage usage greatly compared to the schemes in [4,6]. The details are as the **Table 1**:

Table 1: Storage utilization in different schemes

scheme	storage
The scheme in [4]	N keys and corresponding key ids
The scheme in [6]	N polynomials and corresponding polynomial ids
Our scheme	1 id_key and 1 divisor

Communication Load. The major difference of communication load in different schemes is mainly due to the difference of key discovery. In our scheme, the sensor nodes just send messages described **in Section 2**. However, the schemes in [4,6] send many ids of keys or polynomials. The details are as the **Table 2:**

Table 2: Communication load in different schemes, our scheme requires less communication load due to $\mathrm{N} > 10$ in general.

scheme	Communication load
The scheme in [4]	N key ids and the sensor id
The scheme in [6]	N polynomial ids and the sensor id
Our scheme	$\alpha, E_k(\alpha), E_k(RN), E_k(R),$ id

Energy Utilization. In our scheme, the computation such as $\mathrm{R} = \text{id\_key} \,\%\, \mathrm{N}$(id_key is in under ten thousand level), symmetric encryption and XOR is simple, and will not consume much energy. At the same time, the frequency of key establishment is low. Therefore, we could say that our scheme achieves storage and communication minus without increasing energy consumption. In contrast, in [4], when a sensor node is compromised, the network even needs to restart key establishment, which will consume much more energy. However, in our scheme, the network will do nothing but eliminating them when having detected compromised sensor nodes.

Analyze the Connectivity of WSN. In a completed graph, there must be a link between any two nodes, which means the probability P of the link shared by two nodes is equal to 1. However in a connected graph, there need not to be a link between any two nodes, but one node could connect to any other node through direct link or path link. In our paper, random graph theory helps us to address some hard problems. A random graph $\mathrm{G}(n, p)$ is a graph of n nodes for which the probability that a link exists between any two sensor nodes is p.

The first problem we have to address is that what value should p be so that the graph $\mathrm{G}(n, p)$ is connected (not complete). We get reference in [4], which shows that, for monotone properties, there exists a value of p such that the property moves from "nonexistent" to "certainly true” in a very large random graph. And more, we get the desired probability P_c for graph connectivity, and the threshold function p is defined by:

$$P_c = \lim_{n\to\infty} P_r\,[G(n,p)\ is\ connected] = e^{e^{-c}} \qquad （1）$$

$where$

$$\mathrm{p} = \frac{\ln(n)}{n} + \frac{c}{n} \qquad （2）$$

$where$ c is any real constant

From formula (2), we could get p given n, and $\mathrm{d} = \mathrm{p} * \mathrm{n}$ for which the resulting graph is connected with desired probability P_c. Here, n is the number of nodes in the graph, which are in the whole WSN.

One more problem, how could we determine the divisor N in order to satisfy the connectivity of graph according formula (1) and (2). We know that one sensor node just have n' neighbor sensor nodes where $n' \ll n$ in the real WSNs,. Therefore the $p' = \frac{d}{n'} \gg p$. Here, we let n' denotes the average number of neighbor sensor nodes within communication range when all the sensor nodes are deployed in real environment. Because $n' \ll n$, if we satisfy $p' * \ n' >= p * n$, that is to say $p' \gg p$, the WSNs could be connected.

In our scheme, we set N as the common divisor, and the id_keys are distributed uniformly. Then we could get the probability that two sensor nodes within communication range have common link. The detail formula as follows:

$$p' = 1 - p'' = \frac{1}{N} \qquad (3)$$

$where$

$$p'' = \frac{C_N^1 C_{N-1}^1}{C_N^1 C_N^1} \qquad (4)$$

According to formula (3) and (4), we could choose an appropriate divisor N satisfying specific application.

We can see the different probabilities corresponding to different divisor N, and the change trend in the following Fig 1:

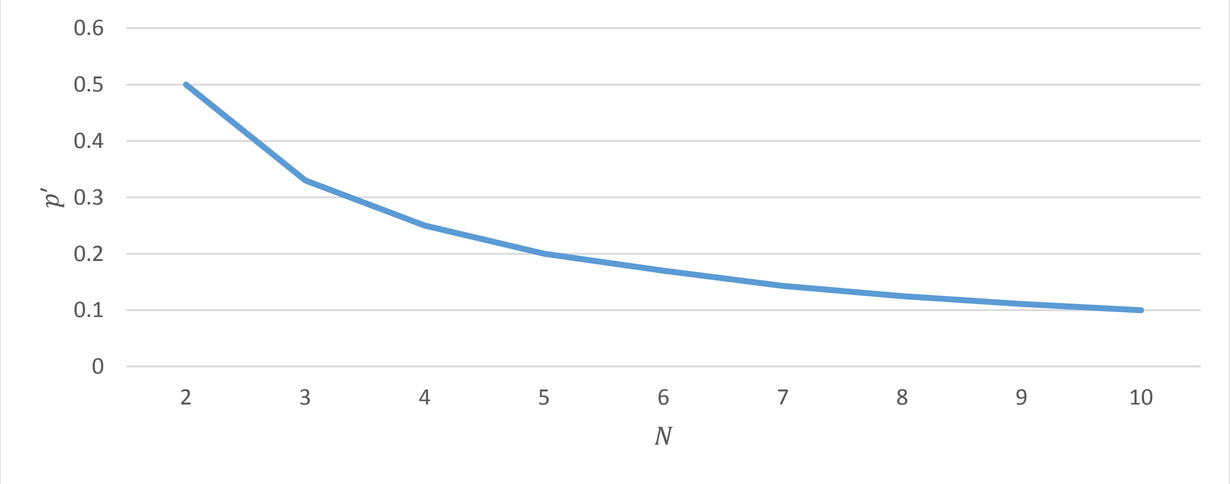

Fig 1: the p' change trend according to different divisor N

Resiliency to Sensor Nodes Compromise

Our key management scheme improves the resiliency greatly not increasing the storage requirement and communication load, because any two sensor nodes have a unique secret common key generated by their unique random large integers, and different pair of sensor nodes has different common keys. When one sensor node is compromised, any other sensor node will be secure except a few of common secure links to the compromised sensor node. Moreover, as long as the compromised sensor nodes are detected, the Base Node will send message to all the sensor nodes to eliminate the compromised sensor nodes, and all the sensor nodes will refuse to communicate with them again.

Summary

In this paper, we proposed a novel key management scheme in WSNs mainly using the remainder of integer. Under the constraint of storage capacity, energy powering and computing power of the sensor nodes in WSNs, our scheme minimizes the storage requirement as well as communication load, and improves the resiliency to sensor nodes compromise. However, there are still several points need to study or improve in our scheme, for example, we could store more integers to each sensor node and regulate that only the sensor nodes which have enough common remainders could establish common key. In the future research, we will focus on more detailed things to improve and optimize the scheme.

Acknowledgement

This paper is supported by the National Natural Science Foundation of China (No. 61272511).

References

[1] Junqi Zhang, Vijay Varadharajan. 2010. Wireless Sensor Network Key Management Survy and Taxonomy. Journal of Network and Computer Applications.

[2] Yun Zhou, Yuguang Fang. 3RD Quarter 2008. Securing Wireless Sensor Networks: A Survey. IEEE COMMUNICATIONS.

[3] Donggang Liu, Peng Ning, Wenliang Du. 2005. Group-Based Key Pre-Distribution in Wireless Sensor Networks. WiSE'05.

[4] Laurent Eschenauer, Virgil D. Gligor. 2002. A Key-Management Scheme for Distributed Sensor Networks. CCS'02.

[5] Haowen Chan, Adrian Perrig, Dawn Song. Random Key Predistribution Schemes for Sensor Networks.

[6] Donggang Liu, Peng Ning. 2005. Improving key pre-distribution with deployment knowledge in static sensor networks. ACM Transactions on Sensor Networks.

[7] Yu Z, Guan Y. 2005. A robust group-based key management scheme for wireless sensor networks. WCNC.

[8] Lan Yun, Chunying Wu, Yiying Zhang. 2013. A Secret-sharing-based Key Management in Wireless Sensor Network. 4th International Conference on Software Engineering and Service Science.

[9] Song Ju. 2012. A Lightweight Key Establishment in Wireless Sensor Network Based on Elliptic Curve Cryptography. ICADE.

[10] Rong cui, Zhaowei Qu, Sixing Yin. 2013. Energy efficient Routing Protocol for Energy Harvesting Wireless Sensor Network. International Conference on Communication Technology.

[11] Sonam Palden Barfunga, Prativa Rai, Hiren Kumar Deva Sarma. 2012. Energy Efficeint Cluster Based Routing Protocal for Wireless Sensor Networks. IEEE.