Quorum based Peer to Peer Key Sharing Protocol over Wireless Sensor Networks

Soong Yeal Yang[a], Nam-Sik Won[a], Hyun-Sung Kim[1a] and Sung-Woon Lee[b]

[a] School of Computer Engineering, Kyungil University
Buhori, Hayangup, Kyungsan, Kyngbuk, 712-701, Korea
Tel: +82- 53-850-7288, Fax: +82- 53-850-7609, E-mail:didzmd@nate.com
[b] Dept. of Information Security, Tongmyong University
Busan, 608-711, Korea
Tel: +82-51-610-8751, E-mail:staroun@tu.ac.kr

Abstract

The key establishment between nodes is one of the most important issues to secure the communication in wireless sensor networks. Some researcher used the probabilistic key sharing scheme with a pre-shared key pool to reduce the number of keys and the key disclosure possibility. However, there is a potential possibility that some nodes do not have a common share in the key pool. The purpose of this paper is to devise a peer to peer key sharing protocol (PPKP) based on Quorum system and Diffie-Hellman key exchange scheme (DHS). The PPKP establishes a session key by creating a shared key using the DHS and then scrambles it based on Quorum system to secure that. The protocol reduces the number of necessary keys than the previous schemes and could solve the non-common key sharing possibility problem in the probabilistic schemes.

Keywords:

Wireless sensor networks; Security; Key sharing scheme; Diffie-Hellman key exchange; Quorum system;

1. Introduction

A wireless sensor network (WSN) is vulnerable to threats and risks. An adversary can compromise a sensor node, alter the integrity of the data, eavesdrop on messages, inject fake messages, and waste network resource. Unlike wired networks, wireless nodes broadcast their messages to the medium. Hence, the issue of security must be addressed in WSNs. There are constraints in incorporating security into a WSN such as limitations in storage, communication, computation, and processing capabilities. Designing security protocols requires understanding of these limitations and achieving acceptable performance with security measures to meet the needs of an application [1].

In general, there are two way to secure peer-to-peer communication which are key pre-distribution scheme and dynamic key management scheme. The key pre-distribution scheme is that base-station distributes key sets before configuring network. Another is that each node makes dynamic value to establish keys after configuring network, called the dynamic key management scheme [2,3]. This section gives an overview of the key pre-distribution scheme and the dynamic key management scheme. The key pre-distribution scheme cannot be used in circumstances demanding heightened security and offers bad connectivity. However, the main characteristic of the dynamic key management scheme is heterogeneous and it depends on a central base station.

Thereby, the purpose of this paper is to propose a peer to peer key sharing protocol (PPKP) to keep the advantages and remove the disadvantages in both of the key pre-distribution scheme and the dynamic key management scheme. The PPKP is based on Quorum system and Diffie-Hellman key exchange scheme (DHS). The PPKP establishes a session key by creating a shared key using the DHS and then scrambles it based on Quorum system to secure that. The protocol reduces the number of necessary keys than the previous schemes and could solve the non-common key sharing possibility problem in the probabilistic schemes.

2. Related Works

This section describes two basic key establishment schemes in WSN [2-5]. They are the key pre-distribution scheme and the dynamic key management scheme. The PPKP proposed in this paper uses both schemes. One of the schemes is Quorum system which belongs to key pre-distribution scheme. Another one is key transmission scheme using Diffie-Hellman which belongs to dynamic key management scheme.

2.1 Key Pre-distribution Scheme

Random pair-wise key scheme [4] is one of the representative key pre-distribution scheme and is proposed

[1] Corresponding author : Hyun-Sung Kim, kim@kiu.ac.kr. This research was supported by Ministry of Knowledge and Economy, Republic of Korea, under the ITRC(Information Technology Research Center) support program supervised by IITA(Institute for Information Technology Advancement)(IITA-2008-C1090-0801-0004)

to solve disadvantages in all pair-wise key establishment schemes that a node stores keys for all other nodes. In the scheme, a node keeps N*p* random keys to reach *p%*, connection probability between two nodes. It has some advantages including flexibility, efficient, fairly simple to employ, and offering good scalability. Disadvantages of the scheme include that it cannot be used in circumstances demanding heightened security and peer-to-peer authentication and it offers bad connectivity.

Closest pair-wise key pre-distribution scheme is another scheme in the key pre-distribution scheme. Each sensor node in the deployed position, if predictable, between a node and *n* of the nearest neighbor nodes shares a key. This scheme can provide connectivity and less memory usages, only if the location of the node can be predicted. But there is a big overhead for key searching and computing PRF function.

2.2 Quorum System

Quorum system is one of the pre-distribution scheme and is that two or more sets have common elements. The important point of Quorum system is that each distributed key sets have at least a common element in it. There are three Quorum systems : Grid Quorum System, Taurus Quorum System and Cyclic Quorum System [5].

[Grid Quorum System] Grid Quorum System is that a node has two or more common elements with other nodes due to it uses a row and a column from a key pool of 2-D grid square. Figure 1 shows an example of gird Quorum system.

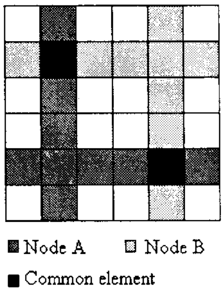

Figure 1 – Grid Quorum System

[Taurus Quorum System] Taurus is based on 2-D grid key pool the same as Grid quorum system, but the size of the breadth of rectangle is 2 times longer than the height. A node is distributed in a column and an element of other columns. 2 or more common elements can be guaranteed. Figure 2 shows an example of taurus Quorum system.

[Cyclic Quorum System] Cyclic quorum system can have common elements using a difference set *D* with subtractions between elements of *D*. For example, if we suppose a network $N = \{n: 0 <= n < 6\}$, difference set is D = {0, 1, 2, 3}. Figure 3 shows the computing. All cyclic quorum system is computed by the way like SQ = {{0,1,2,3}, {1,2,3,4}, {2,3,4,5}, {0,1,2,4}, {1,2,3,5}}. We can see that all set has common elements.

Cyclic Quorum system uses the way to make common set with a small number of elements. Therefore the advantages are providing high level connectivity and less memory usages.

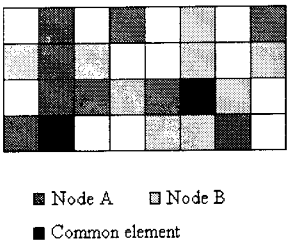

Figure 2 – Taurus Quorum System

$(0-0) \bmod 6 = 0$
$(1-0) \bmod 6 = 1$
$(2-0) \bmod 6 = 2$
$(3-1) \bmod 6 = 3$
$(0-2) \bmod 6 = 4$
$(0-1) \bmod 6 = 5$

Figure 3 – Example of Difference Set

[Advantages and Disadvantages of Quorum System] Quorum system has an advantage that all nodes can connected to any node in one Quorum system due to the set of Quorum system has at least a common element with the other nodes. However, the system depends on the key pool so much to connect with other nodes. Furthermore, if an attacker gets an access to the key pool, the overall network is not safe.

2.3 Dynamic Key Management Scheme

Eltoweissy et al. proposed a dynamic key management system, called exclusion-based system (EBS) [3]. The EBS assigns each node *k* keys from a key pool of size $k + m$. If node capture is detected, rekeying occurs throughout the network. A disadvantage of the EBS scheme is that if even a small number of nodes in the network are compromised, information for the entire network could be uncovered by an adversary. The first application of the EBS scheme was done with anonymous nodes in the network. The nodes did not have IDs. Instead, nodes were identified by their locations. This scheme is heterogeneous and depends on a central base station for key distribution. This EBS scheme is very efficient, but it does not prevent collusion among nodes that are compromised.

There is another Dynamic key management scheme which uses Diffie-Hellman algorithm to exchange a random value. A sink node transports an encrypted group key to cluster heads which use the group key after decryption [6]. The scheme using Diffie-Hellman (DHS) has advantages that it uses less memory because of dynamic key generations, and has short time to complete the exchange of the keys in a group. But if an attacker tries to attack the nodes to take the exchanged values and also encrypted data at the middle of the nodes, the data would be able to be decoded.

3. Peer to Peer Key Sharing Protocol

This section proposes peer-to-peer key sharing protocol (PPKP) to increase security which combines the advantages in the pre-distributed scheme and the dynamic scheme. The PPKP is based on Quorum system and Diffie-Hellman key exchange scheme (DHS). The PPKP establishes a session key by creating a shared key using the DHS and then scrambles it based on Quorum system to secure that. The protocol reduces the number of necessary keys than the previous schemes and could solve the non-common key sharing possibility problem in the probabilistic schemes.

This section describes assumptions and notations for the protocol, details the scramble algorithm which will be used in the PPKP, and proposes the proposed protocol.

3.1 Assumption and Notation

The PPKP assumes that the clustering is established already and a cluster uses only one quorum system set and each cluster uses different quorum set. Table 1 gives definitions for notations used in the proposed protocol.

Table 1 – Notations for PPKP

Item	Explanation
K	A session key
L	The length of a session key
a	A primitive element of the finite GF(*p*) $(1 < a < p)$
P	Modulus (a prime)
x	A random generated by node *A*
y	A random generated by node *B*
h( )	A one-way hash function
SD	Scramble Data
KSF	Key scrambling function
RKSF	Reverse key scrambling function
QE	A common element of Quorum system
QI	Quorum index for QE

3.2 Scramble Algorithm

The PPKP uses the scramble algorithm proposed in [6] to transmit a session key securely. The scramble algorithm follows the steps.

Step 1. A Node generates a ModSet which is used to the scramble algorithm. A ModSet is generated by a^{xy} mod *p* what is computed in communication.

Step 2. The length of a ModSet is extended as *L* by repeating elements of the ModSet. If the element does not fit the length of the last remaining bits, the last remaining bits would be one block.

Step 3. After completing the ModSet configuration, each block is exchanged with *SD* generated by a random function to be transporting data.

In Step 1, the parameters of a ModSet are *a, p, x* and *y*. For an example, if we suppose $a = 2, p = 11, x = 3$, and $y = 2$, where *x* is first nodes value and *y* is the second nodes value, a common value between two nodes is 2^6 mod 11. A ModSet from the parameters has elements from a^1 to a^{xy}. As shown in Figure 4, a ModSet is composed with {2, 4, 8, 5, 10, 9}. Figure 5 explains a configuration of each block by using the elements from the ModSet.

$2^1 \bmod 11 = 2$

$2^2 \bmod 11 = 4$

$2^3 \bmod 11 = 8$

$2^4 \bmod 11 = 5$

$2^5 \bmod 11 = 10$

$2^6 \bmod 11 = 9$

Figure 4 – Example of a ModSet

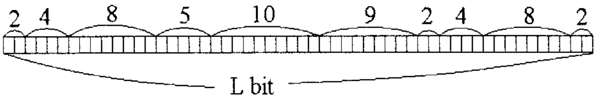

Figure 5 – Example of Blocking

3.3 The PPKP

This sub-section proposes a peer-to-peer key sharing protocol (PPKP) based on Quorum system and the DHS. The PPKP establishes a session key by creating a shared key using the DHS and then scrambles it based on Quorum system to secure that. The protocol reduces the number of necessary keys than the previous schemes and could solve the non-common key sharing possibility problem in the probabilistic schemes.

In the PPKP, node *A* and *B* share Quorum key and a key from the DHS. The key from the DHS is combined with the Quorum key and the combined key is scrambled by the scrambling algorithm and transferred to the counter part. The overall steps are as follows :

Step 1. Node *A* generates a random value *x* and computes $X = a^x$ mod *p*. Thereafter node *A* sends $M_1 = \{ X, QI_A \}$ to node *B*.

Step 2. Node *B* generates a random value *y* and computes $Y = a^y$ mod *p* as the node *A*. And node *B* sends $M_2 = \{ Y, QI_B \}$ to node *A*.

Step 3. Node *A* computes $K{=}a^{xy}$ mod *p* using received a^y mod *p* and combines it with *QE* which is identified from *QI*. After that, node *A* extends it as *L* to be *K* and scrambles *K* with *SD* generated randomly by *KSF* and sends M_3={Scrambled *K*} to node *B*.

Step 4. Node *B* extracts *QE* and a^{xy} mod *p* from the received scrambled *K* by *RKSF*. And checks whether the extracted session key is matched with the computed session key $K= a^{xy}$ mod *p*. And the node checks the extracted *QE* using its own. After that, Node B hashes *K* and *QE* and sends M_4={ *h*(*K*, *QE*) } to node *A*. Node A checks with its own.

Each Node uses *K* to communicate after completing a key transmission and authentication between each other. Figure 6 describes the whole key sharing protocol between node *A* and node *B*.

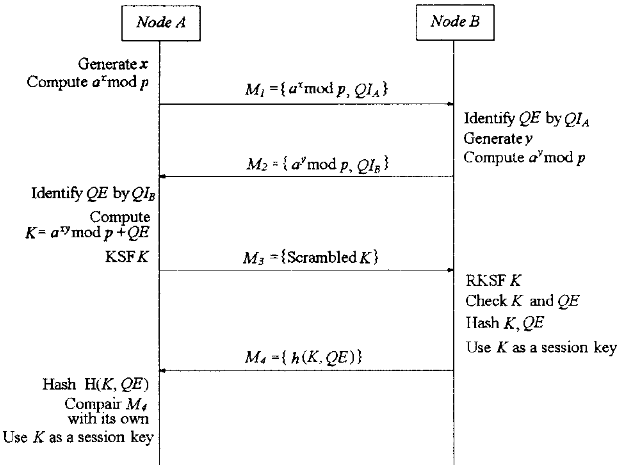

Figure 6 – The PPKP

4. Security Analysis

This section gives the security analysis of the PPKP in the perspective of the node capture attack and the man in the middle (MITM) attack.

4.1 Node Capture Attack

An attacker could read information after a node capture attack. Previous Quorum System is vulnerable to the attack due to it only depends on the pre-shared key pool. However, the PPKP is safe from the node capture attack due to it does not only depend on the Quorum but also depend on the dynamic session key, a session key *K* from the DHS. Therefore, even the attacker gets the Quorum system, the session key *K* is not exposed because the attacker can not know the random values. If an attacker takes *QE* and *K* at the same time, the attacker is only able to damage a cluster and a session because Quorum system is only dependent with a cluster and each session uses new random values. For getting the algorithm of generating key, the attacker should know about *x* and *y*. But it is very difficult to know the random number and the Quorum system at the same time.

4.2 MITM Attack

An attacker tries MITM attack by tapping the messages between nodes. In the previous DHS case, the attacker can compromise because attacker is able to make the session key by MITM attack which snatches random value of each node. However, the PPKP generates a session key with random values with the combination with *QE* which is pre-distributed. For that reason, even if an attacker could get the exchanged message, the attacker can not get any necessary information from them to disguise each node or to retransmit to other sessions. And even if the attacker takes the scrambled data, the attack would be failed because the counter part checks *QE* and the session dependent random value.

5. Conclusion

The key establishment between nodes is one of the most important issues to secure the communication over wireless sensor networks. Some research proposed the probabilistic key sharing scheme with a pre-shared key pool. However, there is a potential possibility that some nodes do not have a common share in the key pool. This paper proposed a peer to peer key sharing protocol (PPKP) based on Quorum system and Diffie-Hellman key exchange scheme (DHS). The PPKP establishes a session key by concatenating a shared key from the DHS and a common key from Quorum in two peers. And the key are scrambled using the scrambling algorithm and are transmitted to the counter part. The protocol reduces the number of necessary keys than the previous schemes and could solve the non-common key sharing possibility problem in the probabilistic scheme.

6. References

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *computer networks*, Vol. 52, No. 12, pp. 2292-2330, 2008.

[2] Y. Xiao, V. K. Rayi, B. Sun, X. Du, and F. Hu, "A survey of key management schemes in wireless sensor networks," *Computer Communications*, Vol. 30, pp. 2314-2341, 2007.

[3] M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic key management in sensor networks," *IEEE Communications Magazine*, Vol. 44, No. 4, pp. 122-130, 2006.

[4] L. Eschenauer, and V. D. Gligor, "A key management scheme for distributed sensor networks," *Proc. of the 9th ACM Conference on Computer and Communication Security*, pp. 41-47, 2002.

[5] J. M. Kang, S. R. Lee, S. H. Cho, C. K. Kim, and J. C. Ahn, "Key Pre-distribution using the Quorum System in Wireless Sensor Networks," *Proc. of KISS Conference*, Vol. 33, No. 03, pp. 193-200, 2006.

[6] J. W. Lee, J. Heo, and C. S. Hong, "A Logical Group Formation and Key Distribution Scheme in WSN," *Proc. of KISS Conference*, Vol. 34, No. 04, pp. 296-304, 2007.