International Journal of Security and Its Applications
Vol.7, No.5 (2013), pp.387-396
http://dx.doi.org/10.14257/ijsia.2013.7.5.35

An Improved Overlap-Key-Sharing Key Management Scheme for Wireless Sensor Networks

Li Lan Ying[1], Yi Chun Huan[2], Sun Jian Da[3] and Si Tie Qiang[4]

[1, 2, 3, 4]*Harbin University of Science and Technology*
[1]*lulu08521@sina.com*, [2]*ychmthgh@163.com*

Abstract

Key management is the base of wireless sensor network security, key pre-distribution way is a high feasibility method in key management. The network connectivity rate, resilience against node capture and the storage consumption are important performance indicators in key pre-distribution way. However, most of the existing key pre-distribution schemes of wireless sensor network have the problems of low connectivity rate , large storage consumption or poor resilience against node capture .On the basis of Overlap-Key-Sharing (OKS) management scheme and the group-based model of Wenliang Du and Donggang Liu et, an improved Overlap-Key-Sharing key management scheme is proposed. The management scheme has little storage consumption and good resilience against node capture. In this paper, we mainly do some analyses and evaluations on a basic random key pre-distribution scheme (E-G scheme) which is proposed by Eschenauer and Gligor et and the improved Overlap-Key-Sharing key management scheme. Result analyses show that under the same network connectivity rate, compared to E-G management scheme, the improved scheme has better resilience against node capture and the smaller storage consumption.

Keywords: *Key Management; network connectivity rate; resilience against node capture; storage consumption*

1. Introduction

Wireless sensor networks can be widely used in education, military, medical, transportation and many other fields, having a huge potential and commercial value, causing widespread concern at home and abroad [1]. In order to extend the lifetime of the network, the full utilization and optimization of network resources is particularly important [2]. If the sensor nodes are deployed in the untouched even enemy controlling environment, the nodes will be faced with a wide variety of attacks. For example, the others are easily to monitor communications, to pose as network nodes or provide false information to the other nodes [3]. Therefore, network security has become a critical application of WSN. WSN security includes general network security problem, such as confidentiality, integrity, message authentication, intrusion detection, access control, security management and so on. Security management includes the establishment of a security system and security system alteration, they are also the basis of WSN security system [4]. The core problem of security management is the security key building process. The resources of the sensor nodes are limited and generally distributed in the place of the enemy or field, it's easy to be captured and there is no certification center. The features of the traditional key management scheme don't apply to sensor networks directly [5]. In distributed wireless sensor network key management, the key pre-distribution scheme is proved to be the most suitable for the characteristics of sensor nodes. So, in recent years, at home and abroad, the researchers in the field carry out many

ISSN: 1738-9976 IJSIA

constructive researches. There exist a number of key pre-distribution schemes. A naive way is to let all nodes stored a master key which is secret. Any node can use the master key to communicate with other nodes in a wireless sensor network and obtain a new pairwise key. This scheme has a fatal flaw, that is if one node is captured, the security of the entire wireless sensor network will be compromised.

In 2003, Eschenauer and Gligor proposed a basic random key pre-distribution scheme (E-G scheme) [6], it is used to establish the initial trust between the sensor nodes. The scheme consists of three phases: key pre-distribution phase, shared-key discovery phase and path-key establishment phase.

In the scheme each sensor node receives a random subset of keys from a large key pool, before deployment, if two nodes want to communicate securely, they must broadcast the indexes of their keys and try to find at least one common key in their subsets. Although the scheme can reduce the number of keys stored in a sensor node and achieve connectivity with high probability, but its security is low, because the multi-pair of sensor nodes have the same keys, so the possibility of key repeat is high, and the leakage probability between the nodes is very big. Based on the E-G scheme, Chan Perrig and Song proposed a q-composite random key pre-distribution scheme [7], in the scheme there are q common keys, not only one. By increasing the value of q, the resilience against sensor node capture can be improved because the attacker must compromise more nodes to achieve a high probability of compromised communication. The idea of the Blom's scheme [8] is that any pair of nodes can find common key and as long as no more nodes are captured, the network is secure. Although the security of the Blom's scheme is high, but its calculation is very large.

The OKS scheme [9] generates a long bit-string as the key-string pool of the wireless sensor network, and randomly distributes a subset key-string pool which is stored in each sensor node. This scheme uses the overlap intervals of the key-strings as the shared secret key with their neighbor nodes. It differs from E-G scheme in that the E-G scheme has key-pools of distinct keys. The OKS scheme uses a long bit-string as the key-string pool (not the pool of distinct keys), the shared secret key between them is the bits of the key-string which overlap between two nodes. If node A and node B are neighbors, they use the overlap intervals of KA and KB as the shared secret key KAB between them, as shown in Figure 1. This scheme in comparison to E-G scheme has the following points: taking up less memory, improving network security with no significant memory requirements, and for secure requirements of different applications, the scheme can have flexible adjustment. The problem is that the shared key-string length may vary, namely the key-string length is not equal between the nodes, this will lead to hardware implementation difficult and safety of the entire network is uneven [10].

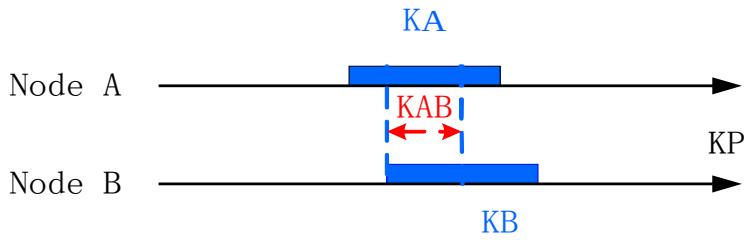

Figure 1. Overlap-Key-Sharing Scheme

In 2004, Wenliang Du and Donggang Liu proposed a key management scheme based on the group-based deployment model [11]. In this scheme, we assume that the sensor nodes are divided into groups, each group of the sensor nodes is deployed at a single deployment point and the probability density functions of the final resident points of all nodes in every group are the same. Assume that the global key pool size of S is $|S|$, and the deployment points are arranged in a grid depicted in Figure 2. Each node stores m keys. The idea of this scheme is that all sensor nodes are divided into groups, and each group of sensor nodes is deployed at a single deployment point.

In Figure 2, we can see that the overlapping factor of the two horizontally or vertically neighboring deployment group is a and $0 \le a \le 0.25$, the overlapping factor of the two diagonally neighboring deployment group is b and $0 \le b \le 0.25$. Two non-neighboring have not overlapping factor.

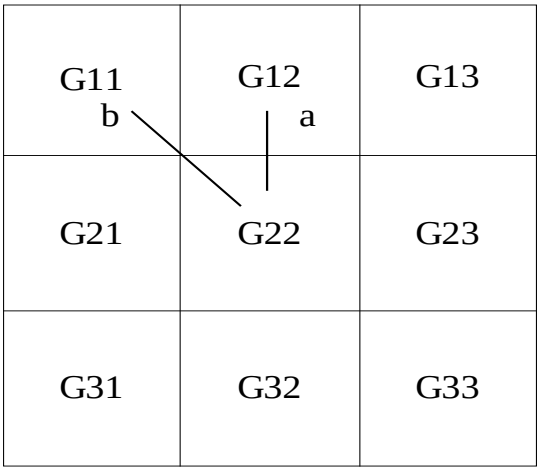

Figure 2. Deployment Groups

Assume that once the sensor nodes are deployed, they are static, and define the deployment point is the point location of sensor node. The deployment area of the sensor nodes is a two-dimensional rectangular region with size $X \times Y$, and firstly, we divide the enter deployment region into the rectangular grids which are the same size. Next, we divide the sensor nodes in the networks into equal size groups, the deployment points are arranged in a grid. Each node group is deployed to a rectangular grid, so the rectangular grid and node deployment group are one-to-one correspondence, the deployment distribution for every node in groups follows a two-dimensional Gaussian distribution:

$$f_k^{ij}\left(x, y \middle| k \in G_{i,j}\right) = f\left(x - x_i, y - y_j\right) \quad (1)$$

where $f(x, y) = \frac{1}{2\pi\sigma^2} e^{-\left(x^2+y^2\right)/2\sigma^2}$

There are three evaluation metrics of key pre-distribution schemes for wireless sensor networks: the network connectivity rate, resilience against node capture and storage consumption.

The network connectivity rate: the communication connectivity is mainly refers to data interoperability between each node and the total network under the wireless communication environment. Secure connectivity is mainly refers to the connectivity of network based on

safe passage .Based on the communication connectivity, each node according to the shared knowledge to establish secure channel .The connectivity within each group is called local connectivity. What we used in this paper is the local connectivity.

Resilience against node capture: we assume that network sensor nodes will be attacked by the enemies after they are deployed, and the adversaries will read secret information from the captured nodes, so we need to reduce the influence of captured nodes for the network security as far as possible. In particular, we need to know how a successful attack on x network sensor nodes by an adversary affects the rest of the total network.

Storage consumption: an ideal key management scheme should have high security level and the low storage consumption. To obtain a higher level of security usually need a lot of storage consumption, however the resources of the sensor node is very limited, large storage is not realistic. So the key is how to don't increase the storage consumption and raise the level of security.

2. The Improved OKS Management Scheme

2.1. The Formation of Key Pool

Assume that node I has been assigned key-string K_I and node J has been assigned key-string K_J. If node I and node J are neighbors, they use the overlap interval of K_I and K_J as the shared secret key K_{IJ} between them. If two sensor nodes want to establish a direct shared key, then they must have overlap interval, in order to ensure that the network key shared figure is connected, the sub key-string pools of the adjacent groups need overlapping intervals. The overlapping factor of key-string pools of adjacent groups is defined as follows:

1. If the overlapping factor of the two horizontally or vertically neighboring deployment group is α, then the two horizontally or vertically neighboring key-string pools share exactly $\alpha|SG|$ bits, where $0 \le \alpha \le 0.25$.

2. If the overlapping factor of the two diagonally neighboring deployment group is β, then the two diagonally neighboring key-string pools share exactly $\beta|SG|$ bits, where $0 \le \beta \le 0.25$ and $\alpha+\beta=0.25$.

3. Two non-neighboring key-string pools share no key-string, as shown in Fig.2, we can know that the overlapping factor of the G_{22} (deployment group)and the deployment groups of G_{12}, G_{21}, G_{23}, G_{32} is α, with the deployment groups of G_{11}, G_{31}, G_{13}, G_{33} is β. In practical applications, the overlapping factor of the extended scheme can be set according to the actual needs.

Assume that the numbers of grid are $m \times n$, the generation step of sub key-string pool of the deployment group can be described as follows:

1. For the deployment group of G_{11}, firstly, select $|SC|$ bits key-strings from the master key-string pool KP, then remove the $|SC|$ bits key-strings from KP.

2. For the deployment group of $G_{1,j}$ (j=2,3,…n), select $\alpha|SG|$ bits key-strings from the deployment group of $G_{1,j-1}$, then select $\omega=(1-\alpha)|SG|$ bits key-strings from the global key-strings pool KP, and remove the selected ω bits key-strings from KP.

3. For the deployment group of $S_{i,j}$, for i=2,3,…,m and j=1,2,…,n, select $\alpha|SG|$ bits key-strings from each of the sub key-string pools of the deployment group $S_{i-1,j-1}$ and $S_{i-1,j+1}$ if they exist; select $\beta|SG|$ bits key-strings from each of the sub key-strings pools of the deployment group $S_{i-1,j-1}$ and $S_{i-1,j+1}$ if they exist; then select ω bits key-strings from KP. And remove these ω bits key-strings from KP. According to the different positions of nodes in the network, the possible values of ω are as follows:

$$\omega = \begin{cases} (1-(\alpha+\beta))\cdot|SG| & (j=1) \\ (1-2(\alpha+\beta))\cdot|SG| & (2 \le j \le n-1) \\ (1-(2\alpha+\beta))\cdot|SG| & (j=n) \end{cases} \quad (2)$$

When key-strings are distributed to the two adjacent groups, we must keep sure that no key-strings are shared by more than two neighboring groups.

According to the key-string pool setup procedure of the scheme, and since key-strings selected from the other groups are all distinct, therefore for $|SG|$ and $|S|$ we have the following equation:

$$|SG| = \frac{|S|}{mn-(2mn-m-n)\alpha-2(mn-m-n+1)\beta} \quad (3)$$

2.2. Second- key Pre-distribution Phase

This key pre-distribution phase is implemented before the sensor nodes are deployed. The key-string pool in this paper is different from the key pool of the Group-based scheme. We assume that the network system randomly generates a long bit-string as the key-string pool (KP) of the sensor network, it contains $|S|$ bits. KP generates a sub key-string pool $KP_{i,j}$ for each square grid area (sensor node deployment group), the size of $KP_{i,j}$ is $|SC|$. After the key-string pools are set up, each sensor node in the deployment group randomly selects $|m|$ bits from its corresponding key-string pool, does not select them from the master key-string pool KP. Sensor nodes in the scheme use the overlap intervals (number of bits overlapping between neighbors) of the key-strings as the shared secret key with their neighbor nodes.

2.3. Shared-key Discovery Phase

After deployment, each node needs to discover whether it shares any key-strings with its neighbors in order to calculate the shared key-strings between two nodes. In the key pre-distribution phase, each node randomly selects a sub key-string pool from a rectangular grid as the key ring of the sensor node, and each key-string has a unique identifier. In the key establishment phase, each node in the network broadcasts its identifier to the neighboring node and each of its neighboring nodes will receive the broadcast message, and compare it with its own identifier, in order to determine whether the overlapping bit string exists for the node of sending broadcasting. Assume that the actual overlap sub-string part is $\{s_1, s_2, \ldots, s_r\}$, the new communication key (K) is generated by the hash function of all the shared parts:

$$K = hash(s_1 \| s_2 \| \ldots \| s_r) \quad (4)$$

where shared parts execute according to the prescribed order, such as the size of identifier of the key-string pool and the size of location index.

2.4. Path-key establishment phase

If there are no common key-strings between two neighboring nodes, the shared key K will not be computed. In this case, a secure path which looking several intermediate nodes needs to be found.

This process is called indirect key establishment phase (or Path-key establishment phase). Assume that the graph G is secure and the connection has been formed. Any two neighboring node a and node b in this graph can always find a secure path: $a, V_1, V_2, ..., V_t, b$.

In order to find a public key between a and b, we first generate a random key K, then the node a using the secure link between a and V_1 sends the key to V_1, V_1 using the secure link between V_1 and V_2 sends the key to V_2, and so on until b receives the key from V_t. Then node a and node b take the key K as their common key. As the key is delivered only on the secure path between node a and node b, so the key will not leak outside the secure path.

2.5. Second-node Addition and Deletion

The new added node needs to find subset key-string pool in the deployment group. Then the new node chooses some bits from the subset key-string pool. As the probability of secure connectivity between adjacent nodes within the same group follows to the same probability distribution, so the connectivity rate between the new node and the adjacent nodes have nothing to do with the order of extract key-strings. For the deleted nodes, network system only needs to broadcast the identifier of the failure key-strings. We can use the idea of flooding to ensure that all nodes are able to remove the failure key-strings.

3. Performance Analysis and Evaluation

In order to be better to study the scheme in this paper, we compare the scheme with E-G scheme in resilience against node capture and memory overhead. In the test environment we assumed bellow, the analysis and calculation results verify the effectiveness of the management scheme in this paper.

3.1. Resilience Against Node Capture

After the distributed-wireless sensor network has been deployed, the security problem is a key factor of maintenance network system. Resilience against node capture refers to that even through a single node or some nodes are captured by the enemy, the entire network will still be able to maintain the ability of secure communication. We can define resistance against as the probability of two nodes can still keep secure communication when S nodes are captured by the enemy. Assume that the sensor nodes which are captured by the enemy over the entire region follow a two-dimensional Gaussian distribution and the key-strings of each node are selected randomly from the sub key-string pool.

Assume that test environment is as follows:

1. The number of nodes in a network is 10000.
2. The key number stored in each sensor node is 200.

3. The deployment area is grouped into 3×3 grids, the side length of the grid is 100m, overlap factor of the key-strings pool is α=0.14, β=0.11.
4. Assume the connectivity rate P = 0.33 and P = 0.5.
5. The communication radius of every node is 50m, and node in the groups follows to the two-dimensional uniform distribution.

When x nodes in the network are captured, the fraction of compromised links between non-compromised nodes is $1-\left(1-m/|SC|\right)^{x}|SC|$, where $|SC|$ is the size of KP, m is the number of the key-string bits stored in each sensor node (the number of key ring). The result is depicted in Figure 3 and Figure 4.

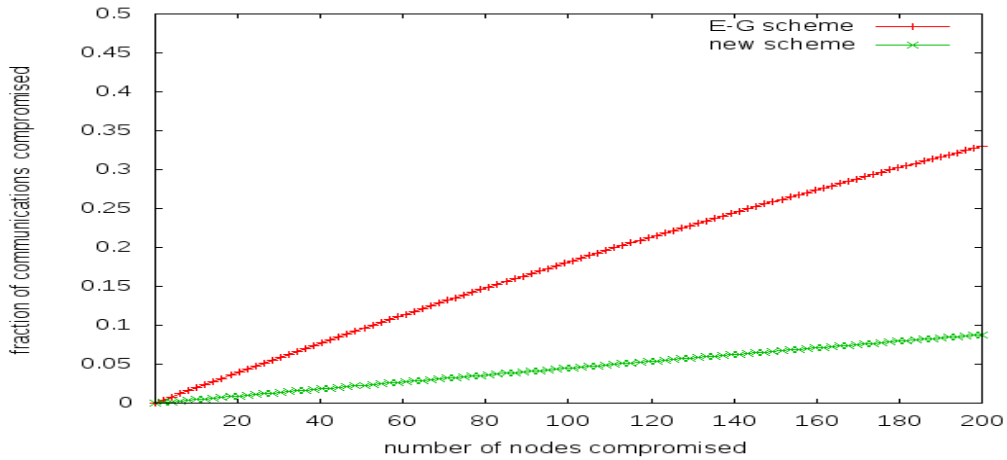

Figure 3. When P=0.33, the Fraction of Compromised

Figure 3 shows the fraction of compromised links of the new scheme compared with the E-G scheme at the same network security connectivity rate P=0.33. In this figure, axis x is the numbers of captured nodes, axis y is the fraction of communications compromised.

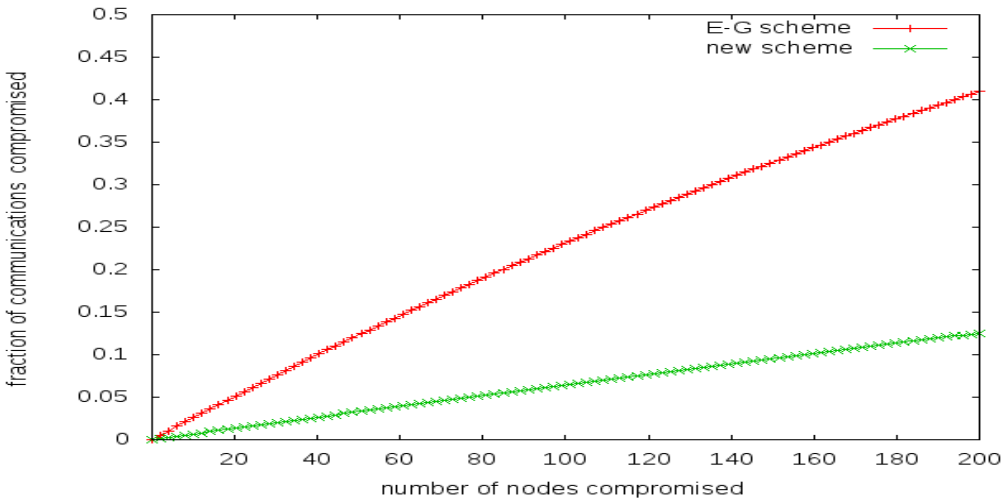

Figure 4. When P=0.5, the Fraction of Compromised

Figure 4 shows the fraction of compromised links of the new scheme compared with the E-G scheme at the same network security connectivity rate P=0.5. From Fig.4 we can see that the scheme in this paper has better resilience against node capture than the E-G scheme, and with the increasing numbers of the captured node, the worse the resilience against node capture becomes.

3.2. Second- storage Overhead

In order to calculate convenience, we assume that the size of key pool is 100, and there are two key-strings in each sensor node in the scheme. For the E-G scheme, we have

$$1-\frac{\left((S-K)!\right)^2}{S!(S-2K)!} \tag{5}$$

where S=100, and for the new scheme, we have

$$1-\frac{KP(KP-2m)}{\left(KP(KP-m)\right)^2} \tag{6}$$

where KP=100. With the different connectivity of the network, the memory required for key storage is different. If each key is 16 bits and each key identity (the address of the key rather than the keys themselves) is 8 bits, at the same connectivity, the total memory required for key storage of the E-G scheme and the new scheme is shown as Table 1.

Table 1. Total Memory Required

Scheme	Size of Memory (bits)					
	0.9999	***0.8561***	***0.7422***	***0.5880***	***0.3170***	***0.1528***
E-G	744	312	264	216	144	96
G-OKS	66	46	40	34	24	24

Table 1 shows that the key storage of the E-G scheme and the improved scheme, when the connectivity is0.9999, the E-G needs 744bits, and the improved scheme only needs 66 bits. When the connectivity is 0.3170, the E-G needs144 bits and the improved scheme only needs 24 bits. So we can see that the improved scheme has lower memory consumption.

4. Conclusion

Based on the analysis of the advantages and disadvantages of overlapping key sharing protocol, introducing the group-based model, we propose an improved OKS key management scheme .The way of key pre-distribution of the improved OKS management scheme is different from the OKS management scheme, it takes the way of key pre-distribution of group-based model. Thus, the improved OKS management scheme can gain a good resilience against node capture. Through the analysis of the above simulation results, we can see that under the same network connectivity rate, for example P=0.33 and P=0.5, compared to E-G management scheme, the improved scheme has better resilience against node capture and the smaller storage consumption.

Acknowledgements

Supported by Scientific Research Fund of Heilongjiang Provincial Education Department (NO:12531107).

Supported by National Collegiate Innovation and Entrepreneurship Training Program (NO:201310214013).

References

[1] W. Haiying, Z. Huashen and L. Ji, "Multicast QoS routing technology based on fixed-length frame", Journal of Southwest Jiaotong University, vol. 45, no. 1, **(2010)**, pp. 76-81.
[2] Z. Yi, F. Li and C. Wei, "Multiconstrained routing algorithm based on mobile agent for mobile Ad Hoc networks", Journal of Southwest Jiaotong University, vol. 45, no. 1, **(2010)**, pp. 94-98.
[3] Z. Shuangfeng, F. Jinlong and L. Nan, "Windows NTFS research and implementation of data recovery", Computer Engineering, vol. 29, no. 1, **(2008)**, pp. 306-308.
[4] X. Song, G. Zhongwen and Q. Haipeng, "Key management scheme for wireless sensor network based on multiple key spaces", Journal of Computer Applications, vol. 29, no. 4, **(2009)**, pp. 932-937.
[5] Z. Juwei and S. Yugeng, "Key management scheme for wireless sensor networks based on deployment knowledge", Computer Engineering, vol. 35, no. 6, **(2009)**, pp. 145-147.
[6] L. Eschenauer and V. Gligor, "A key management scheme for distributed sensor networks", Procedings of the ACM Conference on Computer and Communications Security. New York: ACM Press, **(2002)**, pp. 41-47.
[7] H. Chan, A. Perrig and D. Song, "Random key pre-distribution schemes for sensor networks", Proc. of 2003 IEEE Symposium on Research in Security and Privacy, Orland, Florida, USA, **(2003)** January.
[8] R. Blom, "An optimal class os symmetric key generation system", Lecture Notes in Computer Science 209, Germay: ACM Press, **(1985)**, pp. 335-338.
[9] D. Lai, H. S. Kim and I. Verbauehrde, "Reducing Radio Energy Consumption of Key Management Protocols for Wireless Sensor Networks", Proceedings of ACM/IEEE International Symposium on Low Power Electronics and Design(ISLPEI)04), **(2004)**, pp. 351-356.
[10] H. Xinyang and Y. Ming, "Wireless sensor network key management research", Journal of Computer Applications, vol. 24, no. 3, **(2007)**, pp. 10-15.
[11] D. Wenliang and D. Jiang, "A key management scheme for wireless sensor networks using deployment knowledge", Proc of IEEE INFOCOM'04, **(2004)**, pp. 586-597.