Pair-Wise Key Predistribution Using the Deployment Knowledge in WSN

Lingxiao Zhao
College of Communication and Engineering
Nanjing University of Posts and Telecommunications
Nanjing China
zhlx900812@gmail.com

Ling Ye
College of Communication and Engineering
Nanjing University of Posts and Telecommunications
Nanjing China
yeling@njupt.edu.cn

***Abstract*—Key management is one of the most challenging security issues in wireless sensor networks where sensor nodes are randomly deployed in a hostile field. Considering the limitations of power, computation and communication capabilities in wireless sensor networks, key predistribution is found to be a better choice. In this paper ,we propose a new key predistribution scheme by using the deployment knowledge and the key matrix. The deployment knowledge is used in this paper to divide the nodes and keys into several groups. Then we distribute different key chain in the key matrix into the nodes according to the group of the node and establish pairwise key. In this way, the resilience and connectivity will be enhanced.**

Keywords-wireless sensor network; key predistribution; the deployment knowledge; hexagon division; key matrix

I. INTRODUCTION

Wireless sensor networks(WSNs) are booming research interests in recent years. Because it gets a wide range of application areas such as scientific exploration in dangerous environment, military target tracking and environment monitoring. Wireless sensor networks usually consist of a large number of tiny sensor nodes which can be deployed anywhere and work unattended. Because they are deployed in a hostile environment, where nodes can be readily captured and tampered by adversaries, the security becomes extremely important. To provide security, key management plays a great role in WSNs. The primary problem in key management is to establish the secure keys between the sensor nodes. Unfortunately, when considering the energy resources of sensor nodes and the limited computation, the usual public key management is not available in WSNs [1].

Recently, pairwise key management is preferred in WSNs because of its low computation and communication cost. In pairwise key management, two communication parties need to share a pairwise key before they communicate with each other. Due to unpredictable network situation such as sensor network, distributing pairwise keys to the sensor nodes securely and efficiently is a big challenge. So many key predistribution schemes are proposed. The basic idea of the above schemes is pre-loading a set of keys into sensor nodes before they are deployed. If the deployed nodes share a pairwise key, they can communicate securely with each other [2].

Another important information can be used to improve the performance of the key predistribution schemes is the

Deployment knowledge. If the deployment follows a specific order, the information is achievable. It provides

WSNs with many advantages such as reducing network overhead, achieving better storage and minimizing the number of keys[3].

In this paper ,we propose a new key predistribution scheme by using the deployment knowledge and the key matrix. The deployment knowledge is used in this paper to divide the nodes and keys into several groups. Then we distribute different key chain in the key matrix into the nodes according to the group of the node and establish pairwise key. In this way, the resilience and connectivity will be enhanced.

The remainder of this paper is organized as follows. Section II presents some related works on key predistribution schemes. Section III offers the definitions and the notions in our scheme, Section IV describes our scheme in detail. Section V gives the performance and evaluation of the proposed scheme. Section VI concludes this paper.

II. RELATED WORKS

With the WSNs improved in recent years, key management problem has already been extensively studied and several pairwise key predistribution schemes have been proposed. A basic random key predistribution scheme has been proposed by Eschenauer and Gligor [4]. In the scheme, they selected a key ring of k keys from a large pool S of keys randomly and pre-loaded each node with it. In order to identify the common keys, the list of key ID was exchanged between each node and its neighbors after the deployment step. If there are some keys shared by two neighbors, the two neighbors will establish a secure link and one of the common keys will be considered as their communication key. On the contrary, if there are no common keys, secure paths composed of successive secure links should be determined by the two neighbors.

Based on the E-G scheme, the Q-composite scheme which enhances the resilience is proposed by Chan et al. [5]. In this solution, a secure link can not be established by two neighboring nodes unless the two nodes share at least Q keys. The pairwise communication key is treated as the hash of all shared keys which concatenated to each other. More overlap keys are needed if the attacker wants to break a secure link,

so this approach makes the resilience against node capture attacks more powerful. However, as neighboring nodes must have at least Q common keys to establish a secure link, the scheme make the communication key sharing less possible.

Du et al. proposed a pairwise key predistribution scheme combing the basic scheme and Blom's key predistribution mechanism together [6]. In this scheme each node i stores a column i and a row i of two matrices G and $(D.G)^T$ respectively where : $D(\lambda+1)\times(\lambda+1)$ is a symmetric matrix. $G(\lambda+1)\times n$ is a public matrix and $(D.G)^T$ is a secret matrix. The matrix of pairwise keys is then $K = (D.G)^T.G$. It exhibits a good threshold valve: if the threshold is more than the number of compromised sensor nodes, the probability that other sensor nodes are compromised is nearly zero. On the contrary, if more nodes are compromised, almost all connections will be compromised.

Liu and Ning proposed a new key management scheme. Bivariate polynomials instead of keys are pre-loaded in the nodes[7]. A global pool of symmetric bivariate polynomials (f(x, y) = f(y, x)) is generated off-line and each node i is pre-loaded with a subset of polynomials f(i, y). When two neighbor nodes have a common polynomial, the communication key is derived by computing the polynomial value at the neighbor identifier. his approach makes the resilience against node capture more powerful. Nonetheless, storing the polynomials requires more memory and more computational overhead will be induced.

Due to the large numbers of the nodes in WSNs, the node should store a large number of keys, which increase the memory consumption. To solve this problem, Du et al proposed a scheme involving the deployment knowledge of the nodes [3]. Because the Gaussian distribution is best fit to the real world deployment scenarios, the scheme assumes that nodes are distributed according to it. Nodes are organized in regional groups to which are assigned different key pools, each node selects its keys from the corresponding key pool. In this way, the nodes in the same group have a high probability to share keys, but the distant nodes do not. Thus the scheme can improve the resilience against node capture attacks as well as the probability of sharing common keys.

In this scheme, we combine the deployment knowledge and the basic nature of the matrix. Then we can have the higher connectivity and resilience. Furthermore, the distant nodes can also share a pairwise key compared to the Du's scheme.

III. DEFINITIONS AND NOTATIONS

A. Definitions

Group key pool: contain the keys used for group pairwise key

Cross-group key pool: contain keys used for cross-group pairwise key

Group pairwise key: the same key between two neighboring nodes in the same group

Cross-group key: the same key between two neighboring nodes in the different group

B. Notations

N: The number of sensor nodes in WSN
n: The number of sensor nodes in a group
m: The number of groups
$|S_g|$:The size of group key pool S_g
$|S_c|$:The size of cross-group key pool S_c
$N_{i,j}$: The j^{th} common node in i^{th} group
H_i: The pre-distribution matrix of the i^{th} group
H: The pre-distribution matrix of the cross-group
$K^i_{j,k}$: The key of j row and k column in H_i
$K_{j,k}$: The key of j row and k column in H

IV. THE PROPOSED SCHEME

A. Assumptions

This paper assumes that the total field is divided into m hexagons equally (Fig. 1). Accordingly, N nodes are also averagely divided into m groups and each group has n=N/m nodes. Every group corresponds to a hexagon region [8]. Then the node grouping information is known and they can be deployed in some way to the target region. Each node has the same energy, memory and communication radius. The center of a hexagon is the deployment point which is the desired location of nodes. So the real location of the sensor node Ni,j (x,y) follows the function of the Gaussian distribution:

$$f_{i,j}(x,y) = \frac{1}{2\pi\sigma^2} e^{\frac{-[(x-\mu_{xi})^2+(y-\mu_{yi})^2]}{2\sigma^2}}$$

(μ_{xi},μ_{yi}) is the center coordinate of the ith hexagon. According to the Gaussian distribution, the probability of nodes within 3 σ area is 0.9987.

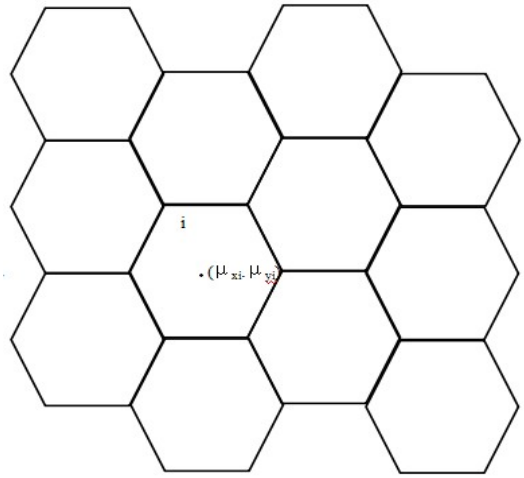

Figure 1. The field division

B. Key distribution scheme

1) The key matrix generation: A Key Distribution Server (KDS) can generate two large size key pool S_c and S_g. And the actual situation of the network decides the key pool size. The number of keys in the key pool is $|S_g|$ and $|S_c|$.

First we divided the pool S_g into m groups (m is the number of the hexagons), so the number of keys in each group is $|S_g|/m$. Then we make the keys in i^{th} group form a matrix H_i:

$$H_i = \begin{bmatrix} K^i_{1,1} & K^i_{1,2} & .... & K^i_{1,L} \\ K^i_{2,1} & .... & .... & K^i_{2,L} \\ .... & .... & .... & .... \\ K^i_{L,1} & .... & .... & K^i_{L,L} \end{bmatrix}$$

$L \le \sqrt{\frac{S_g}{m}}$, normally we take the max integer as the L.

In this way ,we can form m matrices H1,H2....Hm for m hexagons. Each key in different H is not the same.

For the key pool Sc, we form the matrix H as usual. But $L \le \sqrt{S_c}$ and it is usually decided by the number of the hexagons m.

2) Key predistribution: After the matrix formed, we randomly selected a row and a column from the matrix form a key chain and distribute it to the nodes. The node group information decides which matrix it selects. For the matrix H_c, every node in the same group is distributed the same key chain. But the different groups have the different selection. So every node has 2 key chains: group key chain and cross-group key chain.

For example:

$$N_{1,1} = \left(K^1_{1,1}, K^1_{1,2}..K^1_{1,L}, K^1_{2,1}..K^1_{L,1}\right) \cup \left(K_{1,1}, K_{1,2},..K_{1,L'}, K_{2,1}..K_{L',1}\right)$$

$$N_{1,2} = \left(K^1_{3,1}..K^1_{3,L}, K^1_{1,2}..K^1_{L,2}\right) \cup \left(K_{1,1}..K_{1,L'}, K_{2,1}..K_{L',1}\right)$$

$$N_{2,1} = \left(K^2_{1,1}..K^2_{1,L}, K^2_{2,2}..K^2_{L,2}\right) \cup \left(K_{2,1}..K_{2,L'}, K_{1,2}..K_{L',2}\right)$$

3) Pairwise key establishment phase: After the predistribution, nodes are deployed to the sensor field according to the group. Then each node sends a message including the ID to the neighbor nodes. And the neighboring node check the ID to determine whether they are in the same group.

If both nodes are in the same group, they send the group chain to each other, then they can find the same key through the group key chain.If the nodes are in different groups, they send the cross-group chain to each other, then they can also find the same key. No matter in which situation, only one chain is used to compare.

For example, if $N_{1,1}$ and $N_{1,2}$ are neighboring nodes. First, they check the other's ID (1,1) and (1,2), 1=1,so they are in the same group. Then they exchange their group chain with each other, we can easily find they have the common keys $K^1_{3,1}$ and $K^1_{1,2}$. And any one can be the group pairwise key between $N_{1,1}$ and $N_{1,2}$.

If $N_{1,2}$ and $N_{2,1}$ are neighboring nodes. First, they check the other's ID (1,2) and (2,1), 1≠2,so they are in different groups. Then they change their cross-group chain with each other, we can also find they have the common keys $K_{2,1}$ and $K_{1,2}$. And this is the cross-group pairwise key.

Above all, the phases are most operated in the key distributions server. So it isn't limited by the WSN node resource. And it is available in the reality WSNs.

V. PERFORMANCE ANALYSIS

To evaluate the performance of our proposed scheme, we compared several key predistribution schemes. We present our aanalysis on the three metrics: network connectivity, energy consumption and storage overhead, resilience against node capture.

A. Network connectivity

Network connectivity is a very important metric to evaluate a key predistribution. It is the probability of two nodes that share at least one key. Because of the key matrix used in our scheme, it is obviously that two neighboring nodes share at least two keys. Figure 2 gives the comparison between our scheme and the scheme in [4,5] under the size of key pool is 10000.

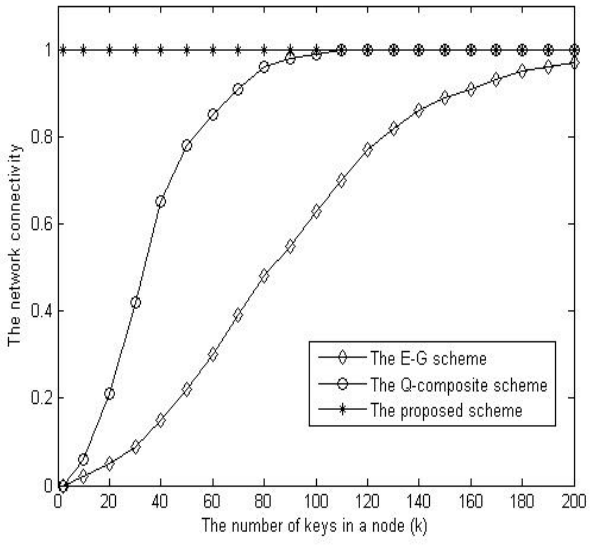

Figure 2. The connectivity comparison

Furthermore, the scheme in [6,7] also has the high connectivity, but more memory is needed because of the complicated computation. The scheme in [3] used the deployment information as ours, but it can't guarantee the connectivity between two nodes indifferent groups.

B. *Energy consumptions and Storage overhead*

The energy consumption is mainly consisted of two aspects: computation consumption and communication consumption. Because of the high connectivity, we don't need establish a path key between two nodes. So the computation in nodes is just equation judgment and the consumption is small. In our scheme, only ID of the node and one key chain is transmitted. So the communication consumption is small too. Above all, less energy will be consumed.

We use the number of the keys in one node to describe the storage overhead. In our scheme, each node stores 2 key chains and the number of keys is (2L-1)+(2L'-1). As mentioned before, we define $L=\sqrt{\frac{S_g}{m}}$. L' is determined by the number of the groups. For each group has its unique row and column, we define $L'=\sqrt{m}$. So Figure 3 gives the relationship between the storage overhead and the number of groups under S_g=10000.

In the Figure 3, we can see that a good choice of m can reduce the storage overhead. If we define m=100, then the storage overhead is 38. It is much smaller than the basic E-G scheme and Q-composite scheme in [3,4].

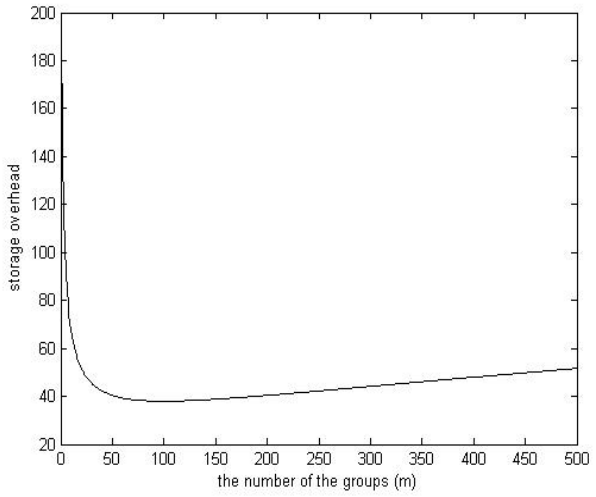

Figure 3. The relationship between the storage overhead and the number of groups

C. *Resilience against node capture*

In a hostile environment, adversary can attack a sensor node after it is deployed and stored keys. Then the adversary can capture the key chains in the node. So the resilience against node capture is a significant aspect in security of WSNs.

Now we calculate the keys being exposed when x nodes are captured to evaluate the resilience against capture. In the worst situation, we assume that each captured node in one group has no common row or column in the key matrix, then the number of exposed keys y is:

$$y = \frac{(4L - 2x)x}{2}$$

If L=20, Figure 4 shows the relationship between the exposed keys and the captured nodes. Obviously in the worst situation, when x=L, the whole key matrix will be exposed. So L is the threshold of this scheme. We can increase L to enhance the resilience and the node storage overhead will be increased.

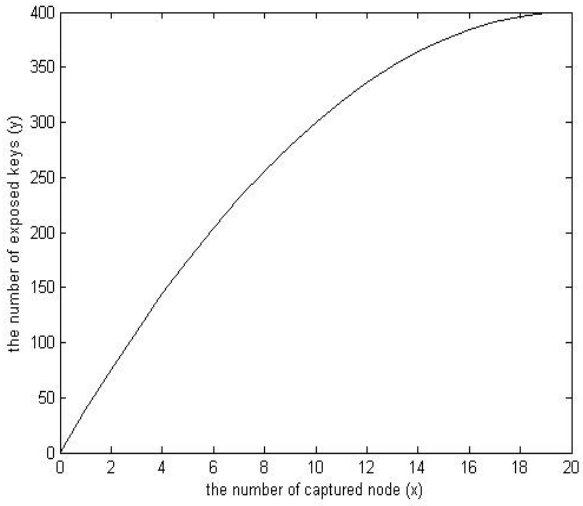

Figure 4. The relationship between exposed keys and captured nodes

However, even L nodes are captured in the worst situation, only one group key matrix is exposed. The cross-group key matrix and other groups' key matrix are still confidential. So the adversary can only destroy the network of one hexagon field. And the whole network is not influenced severely by the adversary. So our scheme has a good resilience to node capture in the whole network.

VI. CONCLUSION

In this paper, we propose a scheme to improve the pairwise key predistribution in WSNs. The scheme consists of deployment knowledge and key matrix. The deployment knowledge is used to deploy the nodes into regarding hexagon groups. And we use the key matrix to establish key chain that stored in the node. Compared to the existing key predistribution schemes, we found that our scheme has a better connectivity and resilience. Furthermore, the low energy consumption is more suitable in WSNs.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramanian. "A survey on wireless sensor networks." IEEE Communication Magazine, 2002, 38(8),pp.102~114

[2] Agrawal, D.P. Zeng. "Introduction to Wireless and Mobile System." Brooks/Cole Publishing (August 2003)

[3] Du W, Deng J and Han Y S, " A Key management Scheme for Wireless Sensor Network Using Deployment knowledge." IEEE INFOCOM'04,2004,pp.586-597

[4] L. Eschenaure and V.D. Gligor. “A key-management scheme for distributed sensor networks.” Proc. of the 9the ACM Conference on Computer and Communications, Washington DC, USA, Nov. 2002,pp.41-47.

[5] H. Chan, A. Perrig and D. Song. “Random key predistribution schemes for sensor networks.” IEEE Symposium on Security and Privacy, May 2003,pp.197-313,.

[6] Du w, Deng J, han Y S and Varshney P K. “A Pairwise Key Preistribution Scheme for Wireless Sensor Networks.” ACM Conference on Computer and Communications Security (CCS), 2003.

[7] D. Liu and P. Ning. “Establishing pairwise keys in distributed sensor networks”. ACM Conference on Computer and Communications Security (CCS), 2003,pp.52–61.

[8] Du W, Deng J and Varshney P K. “A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge”. IEEE transactions on Dependable and Secure Computing, Vol.3,2006,pp.62-77.

[9] L. Cherlyflar, R. Kishore and S. Radha. “securing Wireless Sensor Network Using Deployment Knowledge Based Key Predistribution”. 2012 International Conference on Solid State Devices and Materials Science

[10] Jianmin Zhang, Qingmin Cui. “An Efficient Key Management Scheme for Wireless Sensor Networks in Hostile Environments”. 2009 International Conference on Multimedia Information Networking and Security

[11] Yanan Wang, Yongjin Liu, Huishang Jin. “The Study on Key Pre-distribution Methods for Wireless Sensor Networks”. 2012 International Conference on Solid State Devices and Materials Science

[12] Xiaofei Ma, Zhuoya Dong and Jie Li. “A Novel Key Management Scheme for Wireless Sensor Networks”. 2012 Sixth International Conference on Internet Computing for Science and Engineering