Journal of Information & Computational Science 11:8 (2014) 2479–2491 May 20, 2014
Available at http://www.joics.com

A Hexagon-based Key Pre-distribution Scheme for Wireless Sensor Networks [⋆]

Xiaokang Wang [a,b,∗], Peiyue Li [a], Yongxin Sui [a], Huaijiang Yang [a]

[a] *State Key Laboratory of Applied Optics, Changchun Institute of Optics, Fine Mechanics and Physics Chinese Academy of Science, Changchun 130033, China*

[b] *Graduate University of Chinese Academy of Sciences, Beijing 100049, China*

Abstract

Key management is the foundation for secure communication in wireless sensor networks. In this paper, a novel key pre-distribution scheme based on deployment knowledge was proposed. In the scheme, the target field is divided into two kinds of hexagon grids: group grids and key grids. Nodes in group grids and key grids are treated differently. By combining deployment knowledge with deterministic schemes, the scheme can drastically reduce the fraction of compromised links when some nodes are captured. The simulation results show that our scheme performs better in terms of resilience against node capture compared with other existing schemes.

Keywords: Wireless Sensor Network; Key Management; Deployment Knowledge; Hexagon Grid

1 Introduction

In recent years, Wireless Sensor Networks (WSN) is playing a more and more significant role in military, industry, science research, etc. WSN usually consist of large quantity of sensor nodes with limited power, computation capacity, storage, and communication capabilities. Besides, in many cases, sensor networks are deployed in a hostile environment especially for those used for military, thus secure scheme against malicious attack is important and necessary for WSN.

To guarantee the reliability of the network, security services such as encryption and authentication are used. Traditional techniques of pair-wise keys, such as asymmetric key cryptography and Key Distribution Center (KDC) might not suit the WSN. In asymmetric system, a private key is used for encryption and a public key is for decryption, however, the computation in the process is too expensive for a node in WSN. As for KDC approach, some nodes have to be chosen as the "center nodes" to take charge of the key distribution. If the center nodes are compromised by an adversary, the entire network will crash.

[⋆] Project supported by Key Project of Chinese National Programs for Fundamental Research and Development (973 Program) (No. 2007CB311201) and the Open Found in SKALO (No. Y1Q03FQK02).

[∗] Corresponding author.
Email address: stkang123@gmail.com (Xiaokang Wang).

1548–7741 / Copyright © 2014 Binary Information Press
DOI: 10.12733/jics20103578

Symmetric cryptography is preferred in WSN because of its low computation and communication cost. In symmetric schemes, two nodes need to share an arranged key before communication. The problem is how to distribute keys to each node efficiently and securely before they communicate with others. This problem is called key pre-distribution and has been widely studied in general network environments.

Since Eschenauer and Gligor proposed the E-G scheme [1], many similar schemes [2-5] for key pre-distribution in WSN have been derived. The basic idea of the above schemes is preloading a set of symmetric keys into a sensor node before they are deployed. If two nodes share a common key or key space, they can communicate securely with the symmetric keys. Two main metrics are used to evaluate the performance of a key pre-distribution scheme: connectivity and security. However, most of the schemes mentioned above have weak resistance against node capture. For example, in Du's multiple-space scheme [2], when 400 nodes are compromised, the fraction of compromised communication links reaches almost 100 percent ($m = 200$, $w = 7$, $t = 2$), and in Chan's q-composite scheme [3], the fraction reaches 25 percent when the number of compromised node is only 150 ($q = 1$), thus the maximum network size is limited. To improve the performance, many researchers [6-11] tried to use deployment knowledge to arrange sensors into groups. Theoretical analysis and simulation result show that deployed schemes have superiority over traditional probability-based schemes.

In this paper, we propose a novel pre-distribution scheme based on deployment knowledge. In our scheme, the target field is divided into two kinds of hexagon grids: group grids and key grids. Sensor nodes in the same group establish keys through multiple-space scheme and nodes in the same key grids use combinatorial design theory to implement the key management. The size of the grids is chosen according to the sensor node's transmission range to make sure that only nodes located in adjacent groups can communicate with each other. The simulation result illustrates that our scheme outperforms Du's multiple-space scheme and many other proposed schemes based on deployment knowledge.

2 Related Work

2.1 Multiple-space Key Pre-distribution Scheme

Based on E-G scheme and Blom's scheme [12], Du and Deng proposed a pair-wise key pre-distribution scheme for WSN. Blom's scheme enables any two nodes in the network to compute a common key for their communication. In Blom's scheme, during the pre-deployment phase, the base station constructs a $(\lambda + 1) * N$ matrix G over a finite field GF (q), where N is the size of the networks. Matrix G is public to every node and any λ columns of matrix G are linear independent. Then the base station creates a random symmetric $(\lambda + 1) * (\lambda + 1)$ matrix D over GF (q) and computes a $N * (\lambda + 1)$ matrix $A = (D * G)^T$. Matrix D needs to be kept secret and should not be disclosed to any adversaries. Since D is a symmetric matrix, it's easy to elicit the Eq. (1).

$$A * G = (D * G)^T * G = G^T * D^T * G = G^T * D * G = (A * G)^T \tag{1}$$

So $K = A * G$ is a symmetric matrix and $K_{ij} = K_{ji}$, we can choose $K_{ij} = K_{ji}$ as the communication key between node i and node j. This can be easily achieved through the following steps. For each node with identity k:

(1) Store the kth row of matrix A

(2) Store the kth column of matrix G

When nodes i and j attempt to establish a pair-wise key, they exchange their identity and columns of matrix A at first then they compute K_{ij} and K_{ji} respectively. Blom proved that an adversary can't recover the matrix D and the network is safe if no more than λ nodes are compromised, however, if more than λ nodes are compromised, the matrix D will be computed and the security disappears. To improve the attack resistance, Du and Deng combined Blom's scheme with E-G scheme and proposed the multiple-space key pre-distribution scheme, they chosen t matrixes from a symmetric matrix pool with size of ω for each node, two nodes can establish their communication key if they share a common symmetric matrix. Compared to Blom's scheme and E-G scheme, Du's scheme has a better performance to resist node compromise.

2.2 Combinatorial Design Theory

Combinatorial design theory [5] aims at arranging elements of a finite set into patterns such as subsets or arrays according to specified rules. A set system or design is a pair (X, A), where A is a finite set of subsets of X, called blocks. The degree of a point $x \in X$ is the number of blocks containing in the point x. The rank of (X, A) is the size of largest block. If all blocks have the same size k, then (X, A) is called uniform (of rank k).

Balanced Incomplete Block Design (BIBD) is a specific arrangement of a finite set S of v distinct objects into a collection B of b blocks so that every block has k distinct objects. Each object occurs in r different blocks, and any two blocks have the same number λ of common objects. The design can be expressed as (v, b, r, k, λ) in which $\lambda(v-1) = r(k-1)$ and $bk = vr$. In [13, 14], a specific BIBD $(q^2+q+1, q+1, 1)$ was proposed to implement the shared keys among nodes using finite projective plane of order q. In the scheme, q is a selected prime number with $q^2+q+1 \geq N$. The key pool is in size of q^2+q+1 and each node stores $q+1$keys, any two nodes in the network can share a common key with the probability of 1.

3 Our Scheme

In this section, we give a brief introduction for our scheme at first and then analyze the local connectivity for two nodes in the network. Furthermore, the scheme's security which is evaluated by the fraction of compromised links when x nodes are captured is discussed and we provide detailed theoretical analysis for it.

3.1 Overview for the Scheme

Different from Du's deployment scheme [9], our scheme doesn't rely on overlapping factors to ensure the connection among nodes in different groups. Instead, we create two kinds of grids: group grids and key grids. Both of the the group grids and key grids are hexagon because each hexagon grids have only 6 neighbor grids, however there are 8 and 12 neighbors for square and triangle respectively. Each group grid contains a complete key grid and six half-grids.

Nodes in the same group grids can establish their communication keys through multiple-space scheme because the threshold model could enhance the resistance against node capture. Each key grid contains q+1 keys, and we use BIBD $(q^2+q+1, q+1, 1)$ to establish the connection between nodes in the same key grids but in different group grids because combinatorial scheme has high connectivity .The group grids and key grids are depicted in Fig. 1. To ensure that nodes in a group can only communicate with nodes in neighbor groups, the size of a group grid is deliberately chosen according to the node's communication range, Fig. 2 provides a simple illustration for it. To simplify the theoretical analysis, we just consider the uniform distribution in our analysis.

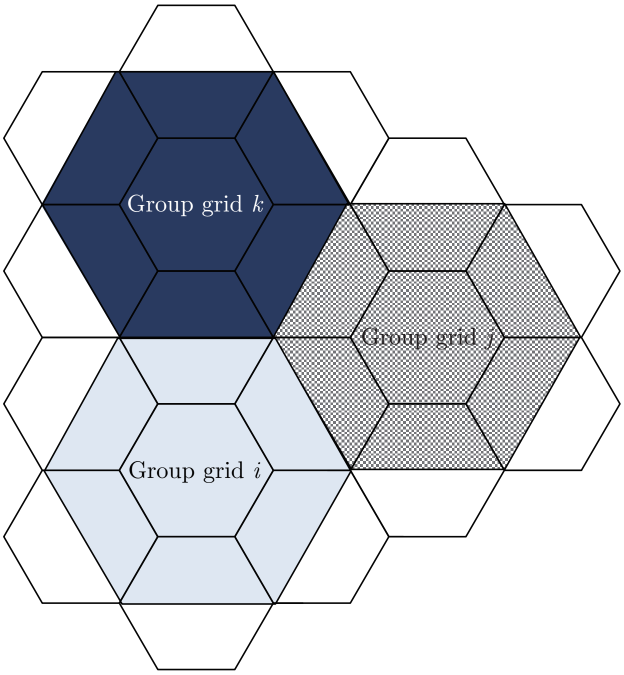

Fig. 1: Group grids and key grids

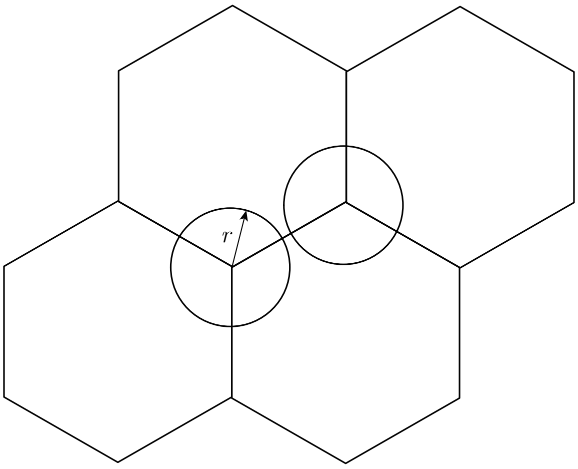

Fig. 2: Choice for grids' size

In Fig. 1, the small hexagons represent the key grids and the shadowed larger hexagons are group grids. Every two group grids share a common key grid and establish shared key through the key grid. In Fig. 2, the hexagons stand for group grids and circles are the covering area of a node in WSN (assuming r is transmission range). To make sure that only nodes in the neighbor grids can communicate with each other, we should choose $l \geq 2r$ in which l is the length of the edge for a group hexagon.

Our scheme consists of two procedures: key pre-distribution phase and key discovery phase. The detailed analysis will be listed in the rest of the paper.

3.1.1 Key Pre-distribution Phase

Assuming that the target area is divided into m group grids and 4m key grids, there are N_c nodes in each key grid and N_m nodes in each group grid and all the nodes conform to uniform distribution. Each node in a key grid is distributed with $q+1$ keys using BIBD $(q^2+q+1, q+1, 1)$ design, and q is the smallest prim which satisfies $q^2+q+1 \geq N_c$. Nodes in different key grids have diverse sets of BIBD designs, so they won't share a common key.

As shown in Fig. 1, each group grid consists of a complete key grid and six half-grids. For each group grid, the base station perform the following behaviors:

(1) Generating a global $N * (\lambda+1)$ matrix G and w secret $(\lambda+1) * (\lambda+1)$ symmetric matrixes $D_1, D_2, \cdots, D_w$;

(2) Computing A_i $(A_i = (D_i * G)^T, i = 1, 2, \cdots, w)$;

(3) Randomly choosing t symmetric matrixes $D_{i1}, D_{i2}, \cdots, D_{it}$ from $D_1, D_2, \cdots, D_w$ for a node k $(1 \leq \text{k} \leq N_m)$ as key space and distributes the kth rows of $A_{i1}, A_{i2}, \cdots, A_{it}$ to the node.

Different groups have different sets of symmetric matrixes, nodes in diverse groups will never share a common symmetric matrix. For a node located in key grid i and group grid j, in key grid j, it will store $q+1$ symmetric keys, and in group grids, it have to store t rows of related matrixes A_i. Assuming that the maximum storage of a node is m, we have $t * (\lambda+1) + (q+1) \leq m$.

We would like to set $t = 2$, because a smaller t will have stronger resistance against node capture when a node's storage is limited. Fig. 3 shows the relationship between number of captured nodes and the fraction of compromised links in multiple-space scheme. In the figure, t represents the chosen key spaces for each node and the maximum storage of a node is $m = 200$. For each t, we choose the largest w which satisfies $p_{connect} \geq 0.33$. From the simulation, the $t = 2$ will have a better performance compared with others.

3.1.2 Key Discovery Phase

A three-dimensional ID (i, j, k) $(1 \leq i \leq m,\ 1 \leq j \leq 4m,\ 1 \leq k \leq N_m)$ is used to represent a node, i represents the group grid index for the node, j stands for key grids index and k is the identity for the node in group grid i. After deployment period, each node broadcasts its ID and receives the same information from its neighbors.

Assuming that two nodes $A(i_A, j_A, k_A)$ and $B(i_B, j_B, k_B)$ are neighbors, the pair-wise key establishment between them are depicted as follows:

(1) If $i_A = i_B$, node A and node B have the same group grid index, they could try to find whether there are shared key spaces between them. If there exist at least one shared symmetric matrix, they can compute the communication key between them; otherwise, they would have to use multi-path key reinforcement to try to establish a key through neighbor nodes' help.

(2) If $i_A \neq i_B, j_A = j_B$, node A and node B have the same key grid index, but different group

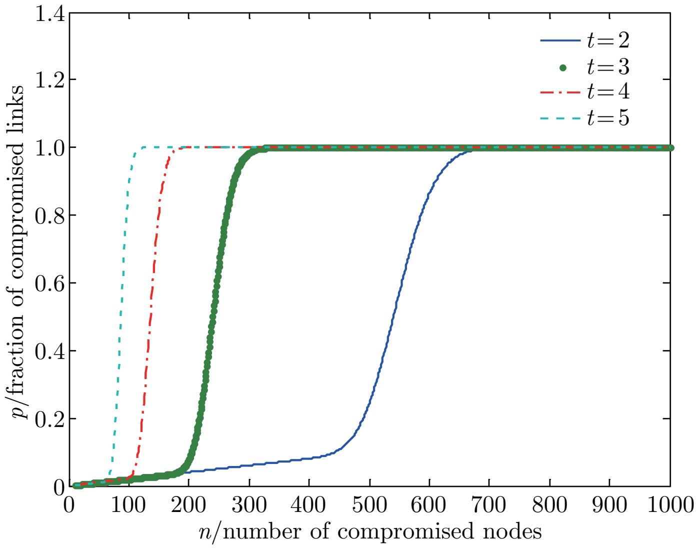

Fig. 3: Security for different t in multiple-space scheme

grid index, they share a common symmetric key with probability of 1 and use the key to encrypt their communication.

(3) If $i_A \neq i_B, j_A \neq j_B$, node A and node B have different group grid indexes and key grid indexes, they can't establish a communication key directly. Similar to the fundamental grid-based key pre-distribution scheme in [4], those nodes can attempt to establish the common key through some intermediary nodes. In fact, through moderating the grid size according to the communication range of a node, the link between two nodes with different group grid index and key grid index is minute (when $l = 2r$, the fraction of this link is no more than 5 percent), to simplify the computation, we ignore the case in theoretical analysis.

3.2 Analysis for Local Connectivity

We use local connectivity to refer to the probability of any two nodes sharing at least one key. Assuming that n_i and n_j are two nodes in the network, let $B(n_i, n_j)$ be the event that node n_i and n_j share at least one common key and $A(n_i, n_j)$ be the event that node n_i and n_j are neighbors. Hence, the local connectivity is shown in Eq. (2).

$$p_{local} = \Pr(B(n_i, n_j)|A(n_i, n_j)) \tag{2}$$

3.2.1 Inner-group Links and In-group Links

To compute the local connectivity for any two nodes n_i and n_j in the network, we have to discuss the fraction of in-group links (links between nodes in different group grids) and inner-group links (links between nodes in the same group grid).

Considering a random node in a group grid, its communication range is r and the edge of the hexagon is $l = 2r$. In Fig. 4, O1 and O2 are two neighbor group grids, node A randomly locates in group grid O1 and the percentage of the area of the arch over the whole circle could be regarded as the fraction of in-group links for a node since all the nodes conform to uniform distribution.

As show in Fig. 4, node A is randomly distributed in group O1, and group O2 is O1's neighbor group grid. For each of the six parts in grid O1, we now consider an infinitesimal rectangular area with width of dx and the distance to the edge of the hexagon is x. The area of the infinitesimal rectangular is $ds = \left(l - \frac{2\sqrt{3}}{3}x\right) * dx$, the probability for a node locating in this area is ds/s (s is the area of the whole hexagon). The area of the arch located in grid O2 is $r^2 \cos^{-1} \frac{x}{r} - x\sqrt{r^2 - x^2}$ (r is the communication range for a node), thus the average area of the arch could be represented as Eq. (3).

$$s' = 6 \int_0^r \left(l - \frac{2\sqrt{3}}{3}x\right) \left(r^2 \cos^{-1} \frac{x}{r} - x\sqrt{r^2 - x^2}\right) /sdx \tag{3}$$

The average fraction of in-group links for a random node in a group grid is

$$p = s'/(\pi r^2) \tag{4}$$

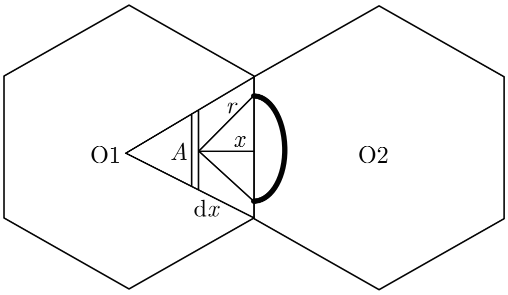

Fig. 4: Fraction of in-group links for a node

3.2.2 Local Connectivity

There are two kinds of links in the network, in-group links and inner group links. For inner-group links, the local connectivity is $p_1 = 1 - \binom{w-t}{t}/\binom{w}{t}$. As for in-group links, to simplify the computation, we assume that those links occur only among nodes in the same key grid, since most of the effective communication nodes in different group grids locate in the same key grids when we set $l = 2r$ and the connectivity is 1.

So the local connectivity for a node in the network could be presented as Eq. (5).

$$p_{local} = (1 - p) * p_1 + p * 1 \tag{5}$$

3.3 Security Analysis

3.3.1 Evaluation Metrics

In most of the proposed key pre-distribution schemes, the security is evaluated by the fraction of compromised links when x nodes are captured. However for schemes based on deployment knowledge, the situation appears to be somewhat complex, because we don't know how many nodes in each group grids are captured. Similar to [10], we discuss local security and global security respectively. Local security is defined as the fraction of links compromised when x nodes in a group grids are captured, and global security deals with the more complicated situation that x nodes in the whole network are captured.

If x nodes in the network are captured, there are three types of influenced links: the direct links with the compromised nodes; the additional links among nodes in the same group grids whose keys might be obtained from the compromised nodes; the additional links among nodes in different group grids but in the same key grid.

For a network with N nodes, and there are d neighbors for each node, if x nodes are captured by an adversary, the fraction of compromised links can be calculated as Eq. (6).

$$p_{compr} = \frac{x * d + (Nd - x * d)p_{\inf}}{Nd} \tag{6}$$

$p_{\inf}$ is the probability that the adversary could compute the key for an additional link after capturing x nodes in the network.

3.3.2 Analysis for Local Security

For a group grid with N_m nodes, if x nodes are captured, the number of three types of influenced links can be computed as bellow.

Direct connected links:

$$n_1 = xd/2 \tag{7}$$

Additional links among nodes in the same group: since the key establishment for nodes in the same group is based on multiple-space key pre-distribution scheme, the probability for an adversary to break a space is $\sum\limits_{j=\lambda+1}^{x} \binom{x}{j}(t/w)^j(1-t/w)^{x-j}$. Thus the influenced links is:

$$n_2 = (1-p)(Nd/2 - x * d/2) \sum_{j=\lambda+1}^{x} \binom{x}{j}(t/w)^j(1-t/w)^{x-j} \tag{8}$$

Additional links among nodes in different group grid but same key grid:

$$n_3 = p(N_m d/2 - xd/2)\frac{q+1}{q^2+q+1} \tag{9}$$

Thus the local security can be depicted as the following Eq. (10):

$$\begin{aligned} p_{locs} &= \frac{n_1+n_2+n_3}{Nd/2} \\ &= \frac{xd + (Nd - xd)\Big[(1-p)\sum\limits_{j=\lambda+1}^{x}\binom{x}{j}(t/w)^j(1-t/w)^{x-j} + p\frac{q+1}{q^2+q+1}\Big]}{Nd} \end{aligned} \tag{10}$$

3.3.3 Analysis for Global Security

Assuming that the whole network consists of N nodes and m groups, x nodes are captured randomly. There are x_i $(0 \leq x_i \leq \min(x, N_m), \sum\limits_{i=1}^{m} x_i = x)$ compromised nodes in group grid i. Let $p_i(x_j)$ denotes the probability that there are x_j compromised nodes in group grid i. Since the x nodes are randomly chosen from the whole network, $p_1(x_j) = p_2(x_j) = \cdots = p_m(x_j)$, and we can use $p(x_j)$ to represent the probability of x_j compromised nodes in a group grid.

$$p(x_j) = \frac{\binom{x+m-x_j-2}{m-2}}{\binom{x+m-1}{m-1}} \tag{11}$$

Similar to the analysis for local security, the global security $p_{g\sec}$ can depicted be as Eq. (12) (p is defined in Eq. (4)):

$$p_{g\sec} = \frac{xd + \sum\limits_{i=1}^{m}(N_m d - x_i d)\left[(1-p)\sum\limits_{j=\lambda+1}^{x_i}\binom{x_i}{j}(t/w)^j(1-t/w)^{x-j} + p\frac{q+1}{q^2+q+1}\right]}{Nd} \tag{12}$$

Considering that compromised nodes in different group grids are independent, the formula above can be simplified as Eq. (13).

$$g\sec = \frac{xd + m\sum\limits_{x_i=0}^{x}\frac{\binom{x+m-x_i-2}{m-2}}{\binom{x+m-1}{m-1}}(N_m d - x_i d)\left[(1-p)\sum\limits_{j=\lambda+1}^{k=\min(x_i,N_m)}\binom{k}{j}(t/w)^j(1-t/w)^{x_i-j} + p\frac{q+1}{q^2+q+1}\right]}{Nd} \tag{13}$$

4 Simulation Results

4.1 Simulation Setup

In this section, we perform simulation studies on network connectivity and security and compare our scheme with other schemes. To better model wireless sensor networks, we use random-graph theory to analysis the connectivity among nodes.

Let V represent all the nodes in the WSN, a key-sharing graph $G_{ks}(V, E)$ is constructed in the following manner: for any two nodes i and j in V, there exists an edge between them if and only if (1) nodes i and j are within each other's wireless transmission range; (2) nodes i and j can establish the shard key between them.

Assuming P_c is the probability that the key-sharing graph is connected, we call it global connectivity. Furthermore, we use local connectivity to refer to the probability of two neighboring nodes sharing at least one key or key space. In the theory of random graphs, the local connectivity must larger than a threshold value decided by P_c and the size of the graph, the threshold value is $p_{required}$. In Erdös and Rényi's theory [15], the relationship between the average node degree d and the global connectivity probability P_c for a network of size N is depicted as Eq. (14).

$$d = \frac{N-1}{N}[\ln(N) - \ln(-\ln(P_c))] \tag{14}$$

For a given density of sensor network deployment, let n be the expected neighbors within wireless communication range of a node, the threshold value can be calculated as Eq. (15).

$$p_{required} = \frac{d}{n} \tag{15}$$

In our design, N nodes (N=10000) are distributed in a 1000 m*1000 m area. The transmission range of a node is $r = 40$ m, so each node have an average number of 50 neighbor nodes. We choose the global connectivity P_c as 0.9999. From these information, we can calculate that $d = 18$ and $p_{required} = 0.36$. Given the above parameters, the length of each group hexagon's edge is $l = 2r = 80$ m, and the length for a *key* grid is $l' = r = 40$ m, there are about $m = 64$ group grids in the whole area, each group grid contains $N_m = 156$ nodes and each key grid contains $N_c = 39$ nodes, so the prime is chosen as $q = 7$. Furthermore, to compare the performance between different schemes in a uniform standard, we assume that the maximum storage for a node is 200.

4.2 Simulation for Local Connectivity

The local connectivity for a node in the network is $p_{local} = (1 - p) * p_1 + p * 1$ in one hop, p and p_1 are defined in chapter 3.4.1, when l=2r, p=0.2034. If the storage of a node is M=200, $t * (\lambda + 1) + (q + 1) = 200$. Fig. 5 illustrates the local connectivity for different t (in the figure, "Du scheme" stands for multiple-space scheme).

Fig. 5 illustrates the local connectivity for different t. To achieve $p_{local} \geq p_{required}$, we have $w \leq 17$ when $t = 2$ and $w \leq 42$ when $t = 3$. In our scheme the local connectivity could reach 0.77 when $w = 10$, $t = 3$. In fact, a high connectivity between two nodes is not necessary, for the multiple hops path-discovery can enhance the probability of establishing communication keys between two nodes. Du and Deng proposed the detailed analysis to calculate the local connectivity with one, two and three hops in [2], but it is so complicated to analyze and simulate in deployment schemes, so we ignore the detailed discussion.

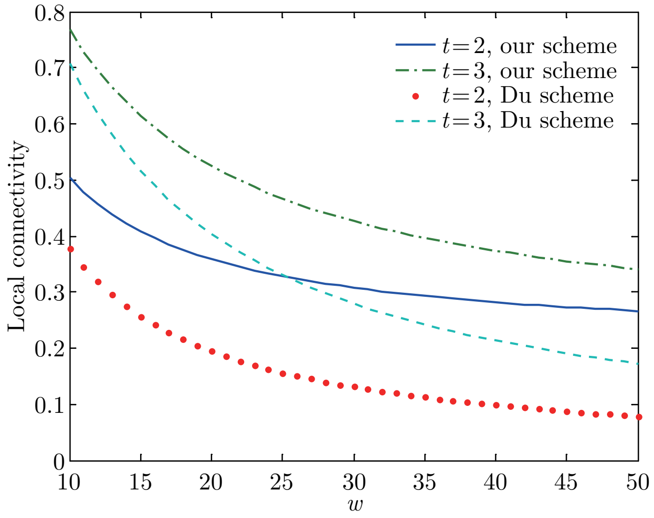

Fig. 5: Local connectivity for different t

4.3 Simulation for Security

4.3.1 Simulation for Local Security

We compare our scheme with Yu and Guan's scheme in [10] on the fraction of compromised links in the whole network when x ($0 \leq x \leq N_m$) nodes in a group are captured. Relevant parameters for the simulation are listed in Table 1 in which N stands for nodes number, sf represents the area to deploy WSN, P_c is the global connectivity. In [10], Yu and Guan used a different graphic theory, so the node's transmission range r are different in the two schemes even with same N, sf and P_c. Besides, in Table 1, l is length of the hexagon's edge, m represents the maximum storage for a node, and λ is the theshold value.

Table 1: Parameters in the simulation

	Our scheme	Yu and Guan's scheme b=3, w=3
N	10000	10000
sf	1000 m*1000 m	1000 m*1000 m
P_c	0.9999	0.9999
r	40 m	24.22 m
l	160 m	66 m
m	200	200
λ	90	66

Fig. 6 depicts the fraction of compromised links as a function of number of nodes compromised in our scheme and "YU and Guan's scheme". The maximum storage for a node in the two schemes is $m = 200$. From the curves in Fig. 6, we find that in "Yu and Guan's scheme", the fraction grows almost linearly with captured nodes when the number of captured nodes is less than the threshold value ($\lambda = 66$). However, as the number exceeds the threshold value λ, the whole key spaces in the group are revealed and the fraction reaches the highest value of 0.020. In our scheme, the number of nodes in each group is not large enough to break one of the key

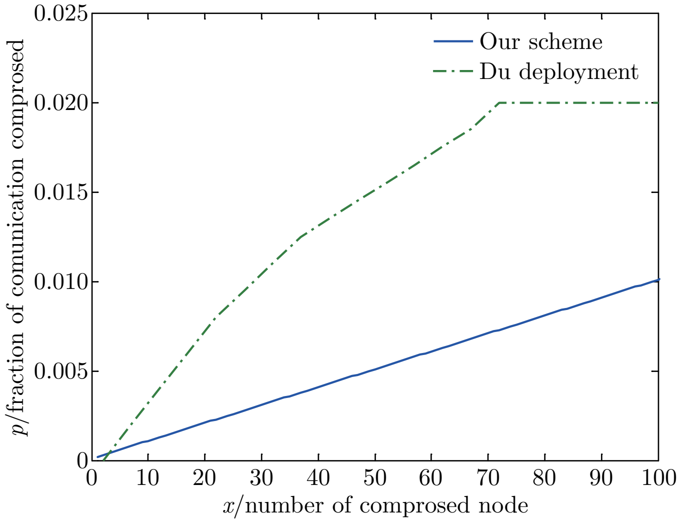

Fig. 6: Simulation for local security

spaces (for $w = 10$, $t = 2$, it needs about 400 nodes, however, in our scheme each group contains only 146 nodes), so there is no abrupt change for the faction curve.

4.3.2 Simulation on Global Security

Fig. 7 shows the comparison among various schemes in terms of global security. In the figure, "Du deployment" represents Du's deployment knowledge scheme [9] and "Basic scheme" stands for multiple-space key pre-distribution scheme [2]. We choose m=200 and $t = 2$ in our scheme and multiple space scheme. As for Du's deployment knowledge scheme, similar to [9], we set $|S| = 100000$, $m = 46$, because a smaller m can enhance the resistance against node compromise.

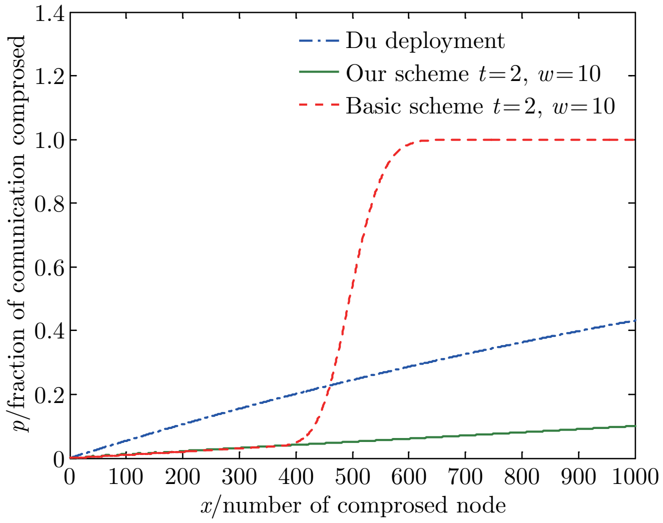

Fig. 7: Simulation for global security

Fig. 7 illustrates that our scheme performs better than other schemes. For example, when less than 400 nodes are compromised, our scheme has a similar performance with multiple-space scheme and both of the two outperform Du's deployment scheme. However, when more than 2.5 percent nodes are captured, our scheme shows its superiority, when 1000 nodes are compromised, the influenced links reaches only about 12 percent, even taking the error for computing p in theoretical analysis into account, the fraction will not larger than 20 percent.

Furthermore, Fig. 7 plots the curve for "multiple-space scheme". Since the fraction of influenced links is independent with network size, the scheme suits small size of network better. However, even 1000 nodes are captured in our scheme, the whole network is still safe, and our scheme could be used in large-scaled WSN. We didn't compare with q-composite scheme and Yu and Guan's deployment scheme [10], as Du etc. had compared their scheme with q-composite in [3] and we failed to get the method to simulate global security in Yu and Guan's scheme.

5 Conclusion

We propose a key management by combining deployment knowledge, Blom's scheme and combinatorial design theory. In our scheme, two types of grids are divided in the network and grid size is carefully chosen to decrease the links among nodes in different groups. We study the network connectivity based on geometric random graph and analysis the resistance against node compromise. We give detailed theoretical analysis on connectivity and security of the scheme. Simulation results show that our scheme outperforms others in terms of resilience against node capture especially for large-scaled WSN. Our further work will aim at establishing a model to simulate different kinds of key pre-distribution schemes accurately and dynamically.

References

[1] L. Eschenauer, V. D. Gligor, A key-management scheme for distributed sensor networks, in Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002, 41-47

[2] W. Du, J. Deng, Y. S. Han, P. K. Varshney, A pairwise key pre-distribution scheme for wireless sensor networks, in Proceedings of the 10th ACM Conference on Computer and Communications Security, 2003, 42-51

[3] H. Chan, A. Perrig, D. Song, Random key predistribution schemes for sensor networks, in Proceedings of 2003 IEEE Symposium on Proceedings of Security and Privacy, 2003, 197-213

[4] D. Liu, P. Ning, Establishing pairwise keys in distributed sensor networks, in Proceedings of the 10th ACM Conference on Computer and Communications Security, 2003, 52-61

[5] S. A. Camtepe, B. Yener, Combinatorial design of key distribution mechanisms for wireless sensor networks, in Proceedings of Computer Security–ESORICS, 2004, 293-308

[6] W. Du, J. Deng, Y. S. Han, S. Chen, P. K. Varshney, A key management scheme for wireless sensor networks using deployment knowledge, in Proceedings of INFOCOM 2004, Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, Vol. 1, 2004

[7] D. Liu, P. Ning, W. Du, Group-based key predistribution for wireless sensor networks, ACM Transactions on Sensor Networks (TOSN), 4(2), 2008, 11

[8] L. Zhou, J. Ni, C. V. Ravishankar, Efficient key establishment for group-based wireless sensor deployments, in Proceedings of the 4th ACM Workshop on Wireless Security, 2008, 1-10

[9] W. Du, J. Deng, Y. S. Han et al., A key predistribution scheme for sensor networks using deployment knowledge, IEEE Transactions on Dependable and Secure Computing, 3(1), 2006, 62-77

[10] Z. Yu, Y. Guan, A key management scheme using deployment knowledge for wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems, 2008, 1411-1425

[11] A. Fanian, M. Berenjkoub, An efficient end to end key establishment protocol for wireless sensor networks, in Proceedings of 2012 9th International ISC Conference Information Security and Cryptology, 2012, 73-79

[12] R. Blom, An optimal class of symmetric key generation systems, in Proceedings of the EUROCRYPT Workshop on Advances in Cryptology, 1985, 335-338

[13] D. R. Stinson, Combinatorial Designs: Construction and Analysis, Springer, New York, 2004

[14] I. Anderson, Combinatorial Designs: Construction Methods, Ellis Horwood, Chichester, 1990

[15] J. Spencer, The Strange Logic of Random Graphs, Springer, Vol. 22, 2001