N-Dimensional Grid-Based Key Predistribution in Wireless Sensor Networks[*]

Jong-Myoung Kim, Young-Ju Han, Seon-Ho Park, and Tai-Myoung Chung

Internet Management Technology Laboratory,
Department of Electrical and Computer Engineering,
School of Information and Communication Engineering,
Sungkyunkwan University,
300 Cheoncheon-dong, Jangan-gu,
Suwon-si, Gyeonggi-do, 440-746, Republic of Korea
Tel.: +82-31-290-7222, Fax: +82-31-299-6673
{jmkim,yjhan,shpark}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Abstract. Security service is one of the fundamental elements required to realize the wireless sensor networks. To distribute key in WSNs, the predistribution technique is commonly used, because the traditional cryptography techniques such as public key cryptography and key distribution center (KDC) are impractical to be applied in the WSNs due to resource constraints of sensor node. The most common technique in famous predistribution schemes is random key predistribution scheme which use probability method. The random key predistribution scheme has a demerit that heavy overhead is occurred on establishing a path key. To reduce the overhead, the grid-based key predistribution scheme was proposed. They uses t-degree bivariate polynomial keys and 2-dimensional grid to provide good properties such as good resilience against the node compromise, high probability of establishing a pairwise key and the minimized overhead on establishing a path key. We extend the dimension of the grid-based key predistribution scheme which is more efficient than other existing schemes. Our scheme improves many properties, except the resilience, of the grid-based key predistribution scheme. So, we introduce n-dimensional grid-based key predistribution using group based deployment as one of methods which can enhance the resilience. Through a mathematical model, we show that our scheme is more efficient than other existing schemes including 2-dimensional grid-based scheme.

Keyword: Wireless sensor networks, key management, key predistribution.

1 Introduction

Wireless sensor networks (WSNs) consist of a large number of low-cost, low-power and small sensor nodes. These sensor nodes are deployed in hostile

[*] This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement) (IITA-2006-C1090-0603-0028).

O. Gervasi and M. Gavrilova (Eds.): ICCSA 2007, LNCS 4706, Part II, pp. 1107–1120, 2007.

environments and monitor the area. They usually collect some information and report it to Base Station (BS) collaborating with each other. For example, some specific applications of WSNs are habitat monitoring, object tracking, nuclear reactor controlling, fire detection, traffic monitoring and so on[5]. Many algorithms and protocols are developed to realize these applications[6,7].
Intuitively, security service is the fundamental one to make up WSNs. On the security point, the basic services are integrity, confidentiality and authentication on data communication and key management is the essential part to provide these services. However, it is usually impractical to use traditional cryptographic methods ,such as public key cryptographic and key distribution centers (KDC), in the WSNs because of the resource constraints of sensor nodes themselves. The limited computation in nodes makes them vulnerable to denial-of-service (DoS) attacks[8]. Additionally, the lack of fixed infrastructure and unknown network topology prior to deployment make the key management more complex. Moreover, sensor nodes can easily captured in physically and can be compromised by adversaries because they are deployed in hostile environment and use wireless radio signals to communicate each other[9].

To realize security service in WSNs, many key management techniques have been developed[10,11]. Eschenauer and Gligor[1] proposed the first basic random key distribution scheme. In this scheme, to overcome the limitation on key storage size, the probability model is used. The main idea is that k keys are randomly selected by each node out of a large pool of P keys. However, its main drawback is that an attacker can easily threat the network survivability by capturing some nodes. To solve the problem, Chan[4] suggested the q-composite random key distribution scheme. Although the q-composite random key distribution scheme makes the resilience against node capture more strong, it has a demerit that the probability any pair of nodes share a key is decreased as the resilience is increased.

Liu and Ning proposed more enhanced scheme using t-degree bivariate polynomials[2]. They proposed two key management schemes. One is called random subset assignment scheme which perfectly provides network resilience until $t + 1$ nodes are captured for any specific polynomial keys. The other scheme is the grid-based key predistribution scheme that uses t-degree bivariate polynomial keys and two-dimensional grid. They proved that their schemes have more resilience against node compromise and reduce the computational overheads on establishing path keys compared to the existing key management schemes[1,2]. In this scheme, the probability that any pair of nodes share a key is very low. The low probability makes a path key establishment process be performed more frequently. This process can cause the overhead which may be reduced if the probability is high.

To reduce overhead of the grid-based key predistribution scheme, we extend 2-dimensional grids to N-dimensional grid. We analyzed the N-dimensional grid-based key predistribution scheme and concluded some properties according to the degree N of dimension. One property is that the probability of sharing a key between any two sensor nodes is increased as the degree N increases. The other is that the number of direct intermediate nodes that can help any two nodes establish a pairwise key indirectly in the middle of them without other intermediate nodes is increased exponentially. These two properties make the key establishment more energy efficient but the resilience is decreased. In the last of this paper, we introduce the method using the group-based key deployment[12] as one of techniques[12,13] to solve this problem.

The rest of this paper is organized as follows. In section 2, we briefly review t-degree bivariate polynomial key and grid-based key predistribution scheme. We will refer the grid-based key predistribution scheme as the grid-based basic scheme in this paper. In Section 3, we will extend the dimension of grid and propose N-dimensional grid-based key predistribution scheme. In section 4, we will propose the method using the group-based deployment as one of the methods to enhance our scheme. Finally, in section 5, we will summarize our paper and discuss about future research.

2 Background Technology

2.1 t-Degree Bivariate Polynomial Key

Blundo[2] proposed a polynomial-based key predistribution scheme that was aimed to group key predistribution. In this scheme, the BS generates a t-degree bivariate polynomial $f(x, y)$ that has a property $f(x, y) = f(y, x)$ over a finite filed Fq. The q is a prime number and is enough large to generate cryptographic keys. For each node which having a unique ID i, the BS distribute the polynomial key $f(x, i)$. Based on this polynomial key, any two nodes sharing the key can generate a pair-wise secret key.

Let's have an example. When the node i want to communicate with a node j, it generate a key $f(j, i)$ and the node j can also generate a key $f(i, j)$. Due to the property of $f(x, y) = f(y, x)$, the two keys are same and this key becomes a unique fair-wise key between node i and node j.

The compromise of a specific polynomial key means that adversaries can compute the original t-degree bivariate polynomial key $f(x, y)$ from $f(x, i)$, $f(x, j)$ and so on. If an adversary wants to obtain one polynomial key $f(x, y)$, he must capture at least $t+1$ nodes that have the polynomial key[2]. In other words, until the t nodes that have the same polynomial key are compromised, the adversary can know only the direct key between any two non-compromised nodes. In this scheme, each sensor node needs to store a t-degree polynomial and this requires $(t + 1) \log q$ storage space. The more t increases, the more scheme's security strength increases. So, this scheme has to consider trade-off between storage efficiency and security strength because the value of t is delimited by the resource constraint of sensor node.

2.2 Grid-Based Key Predistribution Scheme

In this section, we introduce the grid-based key predistribution scheme which is basis of our scheme.

This scheme uses t-degree bivariate polynomial keys and 2-dimensional grid. Because of the nature of grid, there are many paths between two different intersection points and each row and column has t-degree polynomial keys to establish a pairwise key between nodes in the same row or column.

These characteristics make this scheme have many good properties. First, it is guaranteed that any two nodes can establish a pairwise key directly if they are in the same row or column and can establish a pairwise key indirectly through intermediate nodes if they are not. Second, this scheme has also resilience against node compromise. Even if some sensor nodes are compromised, any two uncompromised sensor nodes can establish indirectly a pairwise key with a high probability. Third, a sensor node can directly establish a pairwise key with another node using the predetermined paths on the grid. This property means that there is no communication overhead during a pairwise key establishment.

To explain clearly this scheme, we define terminologies as following:

- *Intermediate node*: Intermediate node is defined as node which can help two sensor nodes establish a pairwise key indirectly in the middle of them and is divided into two classes - direct intermediate node and indirect intermediate node.
- *Direct intermediate node*: Direct intermediate node is defined as node which can help two sensor nodes establish a pairwise key directly in the middle of them without other intermediate nodes.
- *Indirect intermediate node*: Indirect intermediate node is defined as node which can help two sensor nodes establish a pairwise key indirectly in the middle of them with other intermediate nodes at least one.
- *Direct key share probability*: Direct key sharing probability is a probability that at least one key is shared by any two sensor nodes.

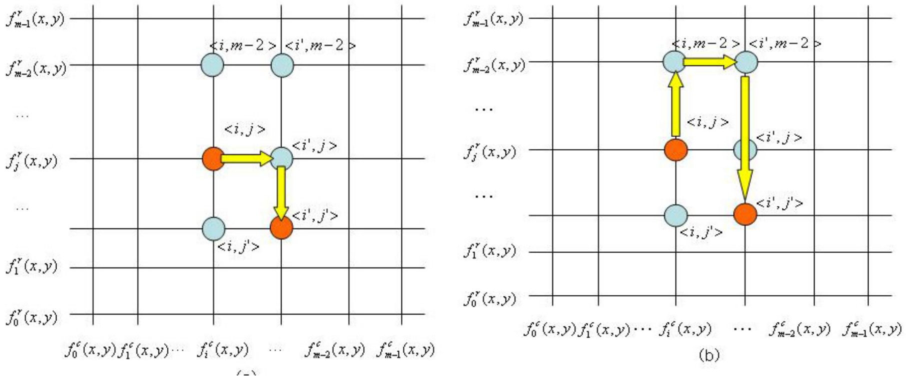
The grid-based key predistribution scheme consists of three phases - subset assignment, polynomial share discovery and path discovery.

Subset assignment

If the N number of sensor nodes are deployed, the key distribution server constructs a $m \times m$ grid with $2m$ number of t-degree bivariate polynomials $\{f_i^c(x,y), f_i^r(x,y)\}_{i=0,\ldots,m-1}$, where $m = \lceil \sqrt{N} \rceil$. Figure 1 shows the configuration of the grid-base basic scheme. Each column and row has a unique polynomial key. The key distribution server selects an unoccupied intersection (i,j) in the grid and assigns $\{ID, f_i^c(j,x), f_j^r(i,x)\}$ at each node. In this case, the ID of the node is $< i,j >$ where i and j represents the indices of $f_i^c(j,x)$ and $f_j^r(i,x)$ respectively.

Polynomial share discovery

If $i = i'$, nodes $< i,j >$ and $< i',j' >$ can establish a pairwise key directly using $f_i^c(j,j')$ and also if $j = j'$, the two nodes can establish a pairwise key using $f_j^r(i,i')$. This polynomial share discovery is easily performed because each node has an ID according to the polynomial keys assigned to the node.



(a) Using a direct intermediate node (b) Using indirect intermediate nodes

Fig. 1. Path discovery in the grid-based key predistribution

Path discovery

If two nodes $< i, j >$ and $< i', j' >$ cannot establish a pairwise key directly, they can perform a path discovery to establish a pairwise key indirectly. If $< i, j >$ tries to establish a pairwise key with $< i', j' >$, one of $< i', j >$ and $< i, j' >$ can help as a direct intermediate node. Although $< i', j >$ and $< i, j' >$ can be compromised, there are still some alternative paths using indirect intermediate nodes. In Figure 1, (a) and (b) describe the path discovery processes using a direct intermediate node and indirect intermediate nodes respectively.

2.3 Drawback of Grid-Based Key Predistribution Scheme

The drawback of the grid-base basic scheme is that the direct key sharing probability is extremely low. Table 1 shows the probabilities according to various conditions. Even though the grid-base basic scheme can establish a pairwise key using intermediate nodes, the low direct key sharing probability makes the nodes frequently perform path discovery and this would be a heavy overhead that may be not produced if they share keys.

Table 1. The direct key sharing probabilities in the grid-based predistribution scheme

Number of nodes	The number of necessary keys	Direct key sharing prob.
20000	$142 \times 2 = 284$	0.0140
10000	$100 \times 2 = 200$	0.0199
1000	$32 \times 2 = 64$	0.0615
200	$15 \times 2 = 30$	0.1289
100	$10 \times 2 = 20$	0.1900

3 *N*-Dimensional Grid-Based Key Predistribution Scheme

To increase the direct key sharing probability in the grid-base basic scheme, we extend the 2-dimensional grid to the N-dimensional grid. This scheme has not only good properties inherited from the grid-base basic scheme but also good property rooted in dimension extension. That is, this scheme guarantees that any pair of nodes can establish a pairwise key and has resilience against node compromise and there is no communication overheads in polynomial share discovery. Additionally, as the number of direct intermediate node is increased by extending the dimension, the cost in establishing indirect keys is reduced.

The basic operation is almost same with the grid-base basic scheme except that the number of polynomial keys which must be assigned at each node is increased by one as the degree of dimension of grid is increased.

3.1 Operation

Subset assignment

If N sensor nodes are deployed, the key distribution server constructs a k-dimensional gird with $k \times m$ number of t-degree bivariate polynomials $\{f_{i_1}^{D1}(x,y), f_{i_2}^{D2}(x,y), f_{i_3}^{D3}(x,y), ..., f_{i_k}^{Dk}(x,y)\}_{i=0,...,m-1}$, where $m = \lceil \sqrt[k]{N} \rceil$. The key distribution server selects an unoccupied intersection $(i_1, i_2, i_3, ..., i_k)$ in the grid and assigns $\{ID, f_{i_1}^{D1}(\alpha,y), f_{i_2}^{D2}(\alpha,y), f_{i_3}^{D3}(\alpha,y), ..., f_{i_k}^{Dk}(\alpha,y)\}$ at each node where node ID is $< i_1, i_2, i_3, ..., i_k >$ and α is $i_1||i_2||i_3||...||i_k$ or hashed value of ID. $i_1, i_2, i_3, ..., i_k$ represents the indices of $f_{i_1}^{D1}, f_{i_2}^{D2}, ..., f_{i_k}^{Dk}$ respectively.

Polynomial share discovery

To establish a pairwise key directly, two sensor nodes simply compare their IDs respectively. If they share polynomial keys at least one, they can establish a pairwise key using one of the shared polynomial keys. For example, if node $< i_1, i_2, i_3, ..., i_k >$ and node $< j_1, j_2, i_3, ..., j_k >$ have a i_3 commonly, they can establish a pairwise key $f_{i_3}^{D3}(\alpha, \alpha')$ using $f_{i_3}^{D3}(\alpha, y)$ and $f_{i_3}^{D3}(\alpha', y)$ where α is $i_1||i_2||i_3||...||i_k$ and α' is $j_1||j_2||i_3||...||j_k$.

Path discovery

Even if there are no shared keys between two nodes, they can establish a pairwise key using the intermediate nodes which would be found directly without communication overheads based on the grid similar to the grid-base basic scheme. For instance, if node $< i_1, i_2, i_3, ..., i_k >$ and $< j_1, j_2, j_3, ..., j_k >$ want to establish a key, the nodes that can help directly are $< j_1, i_2, i_3, ..., i_k >$, $< i_1, j_2, i_3, ..., i_k >$, $< i_1, i_2, j_3, ..., j_k >$ and so on.

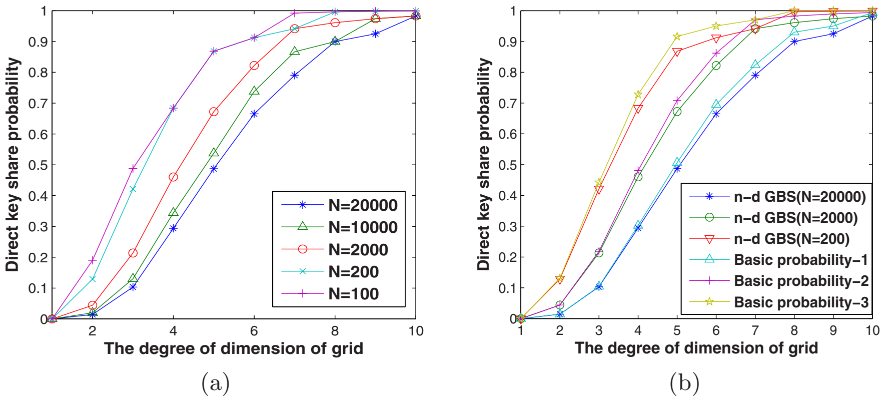


Fig. 2. Direct key sharing probability v.s. Dimension of gird

3.2 Analysis

By extending the degree of dimension of grid, the direct key sharing probability is increased. Equation 1 provides the direct key sharing probability where the k is the degree of dimension of grid and N is the number of nodes.

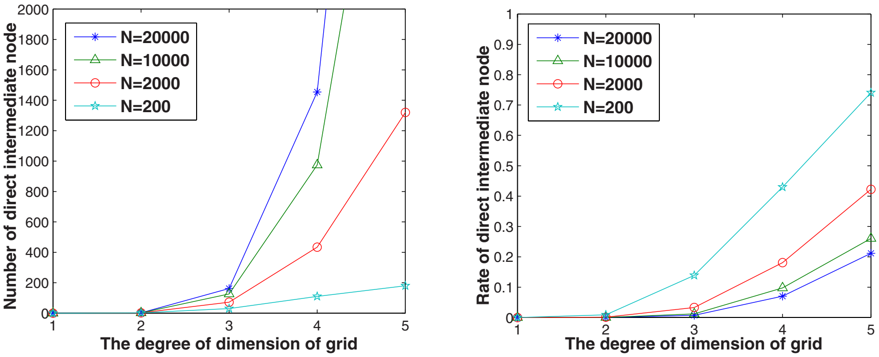
$$P_{DKSP}(k) = 1 - \{(\lceil \sqrt[k]{N} \rceil - 1)/\lceil \sqrt[k]{N} \rceil\}^k \tag{1}$$

Figure 2-(a) describes the relationship between the direct key sharing probability and the dimension degree k of a grid under the various network size N. As the dimension is increased, the direct key sharing probability is increased. In Fig.2-(b), the basic probability 1, 2 and 3 are based on the basic random predistribution scheme[1] and each probability is calculated according to the total number of keys and the number of keys assigned at each node in n-dimensional grid-based key predistribution scheme.

The number of direct intermediate node is increased by extending the dimension of grid and can be calculated by Eq. 2. The m is the number of keys in each dimension of grid. Figure 3-(a) shows that the number of direct intermediate node is increased exponentially as the dimension of grid is increased. Even if the network size is 200, there are 24 direct intermediate nodes when the degree of dimension is 3. Figure 3-(b) shows that the ratio of direct intermediate node is increased as the dimension is increased. In other words, there are more chances that the direct intermediate node can be found near the nodes that want to establish a key.

$$f_{DIN}(k) = m^k - \{2\sum_{i=1}^{k} \frac{k!}{i!(k-i)!}(m-2)^{k-i} + (m-2)^k\} \tag{2}$$

The increased direct key sharing probability and direct intermediate node make the key management more energy efficient than the grid-base basic scheme.



(a) The number of direct intermediate node v.s. dimension of grid

(b) Rate of direct intermediate node v.s dimension of grid

Fig. 3. Relationship between the number of direct intermediate node and dimension of grid

If the following assumptions are satisfied, we can calculate the energy consumption simply.

- The Energy consumption in establishing a pairwise key only depends on sending, receiving, encrypting and decrypting operations and the total message length.
- Any pair of nodes can communicate with one hop.

Equation 3 shows the average energy consumption in establishing one pairwise key directly or indirectly. The E represents the average energy consumption for delivering one hop and the p is the probability that one sensor node is not available. The d is the maximum number of intermediate nodes that is required to establish an indirect key.

$$f_E(k) = E \cdot P_{DKSP}(k) + (1 - P_{DKSP}(k)) \sum_{i=1}^{d} E \cdot (i+1)(1 - p^{f_{DIN}(k)})(p^{f_{DIN}(k)})^{i-1} \tag{3}$$

Figure 4 depicts Eq. 3 based on the energy consumption analysis in sensor nodes[14]. In all case, we assume that the value of d is 2 because the probability of a path key establishment using more than 3 indirect intermediate nodes is extremely low. As the degree of dimension is increased, the energy consumption is converged at one point where the $E = 91.91\mu J$ and this point represents direct key establishment.

All of above results indicates that extended dimension of grid gives many good properties. However, there is a defect on extending dimension.

In grid-base basic scheme, two kinds of attacks are available. The first attack is that an adversary captures or compromises nodes to disclose one bivariate polynomial key. In this case, if the adversary captures or compromises $(t+1)l$

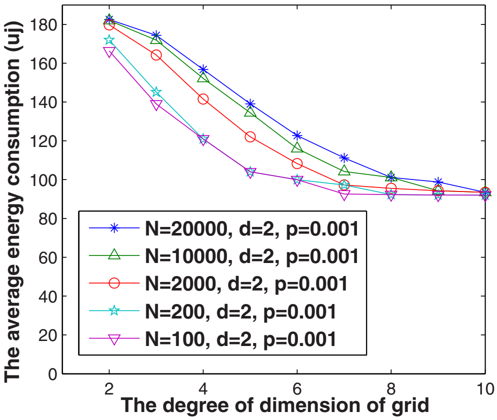


Fig. 4. Average energy consumption on establishing one key as the dimension is increased($E = 91.91\mu J, d = 2, p = 0.001$)

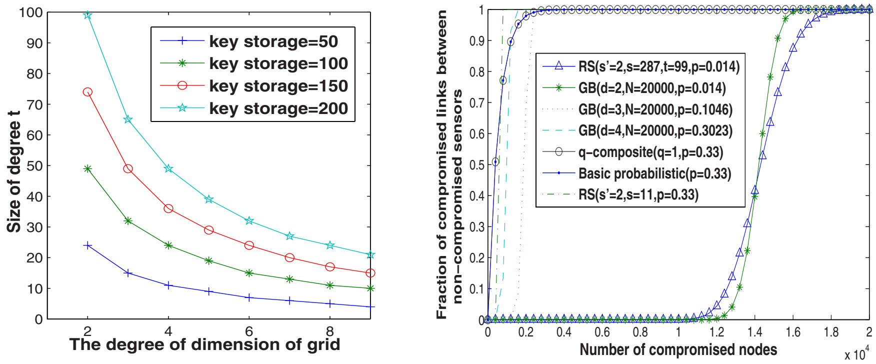
nodes, he can disclose l keys because the scheme uses node ID as a key index. The resilience of each polynomial key depends on the t. As the dimension k is increased, k keys have to be assigned at each node and the t must be decreased due to the storage limitation. The second is that an adversary may randomly compromise nodes to attack the path discovery process. Because the adversary compromise nodes randomly, the probability of a specific bivariate polynomial being compromised can be computed as Eq. 4, where the r_c is the ratio of compromised nodes in the network and the t is the degree of polynomial key.

$$P_c = 1 - \sum_{i=0}^{t} \frac{m^{k-1}!}{i!(m^{k-1}-i)!} r_c^i (1-r_c)^{m^{k-1}-i} \tag{4}$$

Figure 5-(a) shows the limited size t according to the degree of dimension and the key storage size of sensor nodes. The degree of bivariate polynomial t is decreased as the degree of dimension is increased. It means that the adversary can disclose a specific bivariate polynomial key by capturing less number of nodes.

Figure 5-(b) shows that our scheme is more vulnerable than the grid-base basic scheme against the node compromise but is more resilience than the q-composite, random subset and basic random key distribution scheme. Although our scheme is more resilient than the existing schemes, it is very less resilient than the grid-base basic scheme. This is because the t is decreased and the direct key sharing probability is increased.

In next section, we will introduce one of possible methods to make our scheme more resilient.



(a) Size of t according to the dimension and key storage size

(b) The fraction of compromised links between non-compromised nodes according to the number of compromised nodes where the key storage size is 200

Fig. 5. Evaluation of n-dimensional grid-based key predistribution scheme

4 One Solution: Group-Based Deployment

As explained in previous section, the N-dimensional grid-based key predistribution scheme has one demerit that resilience is not good compared to the grid-base basic scheme. It is basically rooted in the decreased degree t of polynomials and the increased direct key sharing probability. These two factors directly influence the problems but there is another factor that maximizes the problems. The last factor is the size of network. The smaller the network size is, the more nodes relative to the number of entire node have to be captured by an adversary.

One of the useful solutions to solve the network size problem is the group-based deployment method [5]. The basic idea of this method is that the nodes belong to the same group are deployed close to each other. So, the nodes are divided into some number of groups and the each group is treated as one network. Thus, we can logically treat a large network as some small networks. This method is also very practical because the WSNs have the characteristic of locality in general. The locality comes from the communication pattern that the local communications take place frequently but the end-to-end communications among nodes are rarely occurred.

4.1 Key Assignment at Each Grid

We can divide the sensor nodes into n groups and each group have to be assigned at one N-dimensional grid. To assign keys at each grid, we use the idea of group construction introduced in [5]. In [5], the element of the group construction is node, while we use the key as element for assigning key at each grid. Figure 6 describes the key assign method at each grid. One row and one column are

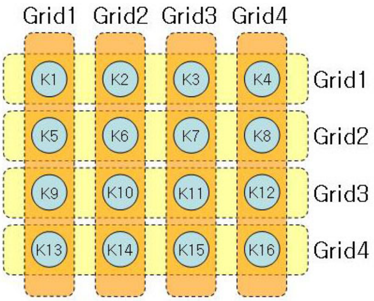


Fig. 6. Key assignment method at each grid

assigned at one grid. For example, $< K1, K2, K3, K4, K5, K9, K13 >$ is assigned at the grid1 and is used by group1. The size of each row and column is $\lceil k \cdot \frac{\lceil \sqrt[k]{N} \rceil}{2} \rceil$ at least because the number of keys that have to be assigned at each grid is $k \cdot \lceil \sqrt[k]{N} \rceil$ where the network size is N.

4.2 Grid Construction

Once the keys are assigned at each grid, we can construct an appropriate grid to distribute keys. In some cases, the number of keys assigned at each grid may be more than the number of necessary keys. In that case, we can simply drop some keys but we need to have a rule that we must not drop both keys intersected with other group at a time. For example, in Fig. 6, if the group1 drops $K2$ and $K5$, then group1 and group2 cannot establish pairwise keys directly. We simply assign the keys at the each dimension and distribute keys at the nodes according to the method that is discussed in Section 3.

4.3 Analysis

In this section, we evaluate the solution to find out how much it improves the resilience against the node capture and node compromising. As we mentioned earlier, there are two kinds of attacks on the n-dimension grid-based key distribution scheme. Thus, we evaluate the solution according to each case.

First case is that the node capture or compromise attack is performed to disclose one bivariate polynomial key. In this case, the number of nodes that an adversary must capture is not changed because the degree t does depend on not the network size but the degree of dimension, k. However, we can compare fraction of captured nodes that have a same key under the same key storage constraint. We can compute the fractions using Eq. 5. The results are shown in Fig. 7 and represents that the adversary has to capture large fraction of nodes that have the same key if the size of one group is small. This also means that even if the adversary discloses the key in the N-dimensional grid-based scheme

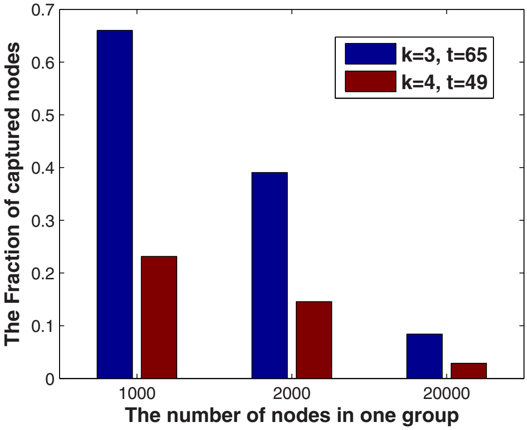


Fig. 7. The fraction of captured nodes that have a same key under the key storage size is 200

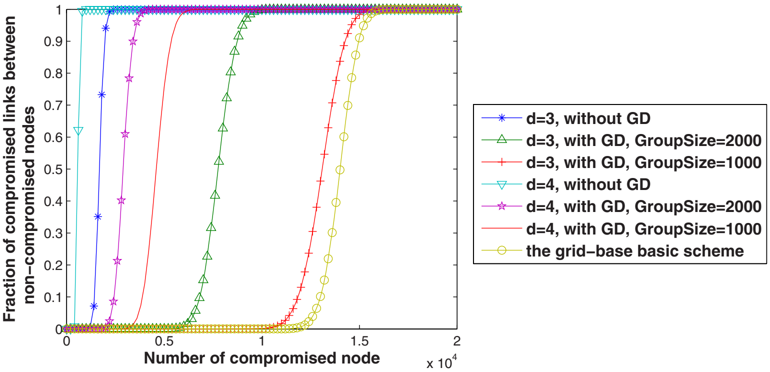


Fig. 8. The fraction of compromised links between non-compromised nodes according to the number of compromised nodes where the key storage size is 200

using group-based deployment, there are small numbers of nodes that have the same key relative to the original N-dimensional grid-based scheme.

$$F = \frac{\lfloor \frac{storagesize}{k} \rfloor}{(\lceil \sqrt[k]{N} \rceil)^{k-1}} \tag{5}$$

Second case is that an adversary may randomly compromise nodes to attack the path discovery process. In this case, the fraction of compromised links between non-compromised nodes according to the number of compromised nodes is simply calculated by using the Eq. 4. We assume that the groups affect each other very weakly so that we will treat the groups independently. Thus, the fraction of compromised link in the N-dimensional grid-based scheme using group-based deployment can be calculated by summing an evaluation result per each group. Figure 8 shows the results and proves that the group-based deployment can be the good solution. When the degree of dimension is 3 and the size of one group is 1000, the resilience against the node compromising becomes almost similar to the grid-base basic scheme.

5 Conclusion and Future Works

The grid-based key predistribution scheme has many good properties compared to the existing key management scheme. But, due to the low direct key sharing probability, the grid-based key predistribution scheme must do path discovery process that might be an overhead. To reduce the overheads, we extended the dimension of grid and analyzed it. As the dimension is increased, the direct key sharing probability is also increased and the direct intermediate node is increased exponentially. These two properties make the n-dimensional grid-based key predistribution scheme is more energy efficient than the grid-base basic scheme. However there is one defect. The resilience against the node capture and compromising is decreased as the dimension of grid is increased. Solving these problems may be the future works and we introduced one of methods to solve the problem.

References

1. Eschenauer, L., Gligor, V.: A Key Management Scheme for Distributed Sensor Networks. In: Proc. 9th ACM Conf. Comp. and Commun. Sec., pp. 41–47 (November 2002)
2. Liu, D., Ning, P.: Establishing pairwise keys in distributed sensor networks. In: CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, pp. 52–61. ACM Press, New York (2003)
3. Blundo, C., Santis, A.D., Herzberg, A., et al.: Perfectly-Secure Key Distribution for Dynamic Conferences. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 471–486. Springer, Heidelberg (1993)
4. Chan, H., Perrig, A., Song, D.: Random Key Predistribution Schemes for Sensor Networks. In: Proc. IEEE Sec. and Privacy Symp., pp. 197–213 (2003)
5. Cerpa, A., Elson, J., Estrin, D., Girod, L., Hamilton, M., Zhao, J.: Habitat Monitoring: Application Driver for Wireless Communications Technology. In: Proceedings of the ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean, San Jose, Costa Rica (2001)
6. Akyildiz, I.F., Su, W., Sankasubramaniam, Y., Cayirci, E.: Wireless Sensor Networks: A Survey. Computer Networks 38, 393–422 (2002)
7. Pottie, G.J., Kaiser, W.J.: Embedding the Internet: Wireless Integrated Network Sensors. Communications of the ACM 43(5), 51–58 (2000)
8. Wood, A.D., Stankovic, J.A.: Denial of Service in Sensor Networks. Computer 35(1), 54–62 (2002)
9. Carman, D.W., Kruus, P.S., Matt, B.J.: Constraints and Approaches for Distributed Sensor Security, NAI Labs Technical Report, ##00-010 (2000)

10. Camtepe, S.A., Yener, B.: Key distribution Mechanisms for Wireless Sensor Networks: A Survey, Technical Report TR-05-07, Rensselaer Polytechnic Institute (March 2005)
11. Liu, D., Ning, P., Du, W.: Group-Based Key Pre-Distribution in Wireless Sensor Networks. In: Proc. 2005 ACM Wksp. Wireless Security (WiSe 2005), pp. 11–20. ACM Press, New York (2005)
12. Liu, D., Ning, P., Du, W.: Group-Based Key Pre-Distribution in Wireless Sensor Networks. In: Proc. 2005 ACM Wksp. Wireless Security (WiSe 2005), pp. 11–20. ACM Press, New York (2005)
13. Du, W., Deng, J., Han, Y.S., Chen, S., Varshney, P.K.: A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge. In: IEEE INFOCOM2004, vol. 1, pp. 7–11 (2004)
14. Wander, A.S., Gura, N., Eberie, H., Gupta, V., Shantz, S.C.: Energy analysis of public-key cryptography for wireless sensor networks. In: Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference, pp. 324–328. IEEE Computer Society Press, Los Alamitos (2005)