International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 135-146
http://dx.doi.org/10.14257/ijsia.2015.9.6.14

An Efficient Key Predistribution Protocol for Wireless Sensor Networks via Combinatorial Design

Jianmin Zhang, Xuerui Wang and Jian Li

College of Computer, Henan Institute of Engineering, Zhengzhou 451191, China
zjm1996@163.com, zzhngc@163.com, lj2006@163.com

Abstract

As Wireless Sensor Networks (WSNs) are usually deployed in remote or even hostile environment, the adoption of security mechanism is fundamental. To achieve secure communication between sensor nodes in WSNs, it is important to establish efficient key predistribution schemes. Unfortunately, key management scheme is a challenging issue for WSNs because of the resource limitations in the sensor nodes. In this paper, we propose an efficient key management scheme for WSNs, which assigns the key spaces to sensor nodes via combinatorial design. In the scheme Finite Projective Plane is mapped to obtain efficient key distribution scheme. Connectivity, resistance against attacks, storage and communication overhead are studied analytically and computationally. Compared to related schemes, the proposed scheme performs better against compromised node attacks.

Keywords: *Wireless sensor networks; Key predistribution; Network security; Matrix*

1. Introduction

Nowadays, wireless sensor networks (WSNs) are increasingly used in many applications like habit monitoring, health care, military or security areas [1, 2]. Since sensor nodes often reside in unattended or hostile environment, particularly with military applications, an adversary could easily access the wireless channel and intercept the transmitted information, or distribute false information in WSN. Under such circumstances, authentication and confidentiality should be undergone to ensure integrity of sensor node and proper functionality of the network. This requires the establishment of secure keys between sensor nodes in the WSNs [3]. Key management can be defined as a set of process and mechanisms that support key establishment and maintenance of ongoing keying relationships between valid parties according to a security policy. The design and implementation of any security service for WSNs must keep in mind that compared with conventional computers for the low-cost sensor nodes have limited energy supply and stringent capabilities. For key management it is not feasible for WSNs to use traditional pairwise key establishment techniques such as public key cryptography and key distribution center (KDC) [4, 5].

Generally speaking, key management protocols are based on either symmetric or asymmetric cryptographic functions. However due the resource limitation in the sensor nodes, use of public cryptographic (asymmetric functions) is not suitable. Generally, there are two types of symmetric key management schemes based on on-demand trust center or key predistribution. However, as there is no an infrastructure in WSNs, the former schemes are not suitable to be used in WSNs. With the key predistribution schemes, key materials are distributed among all sensor nodes before the network deployment. In this regard, various key predistribution schemes have been proposed for key management in WSNs.

ISSN: 1738-9976 IJSIA

In [7] Eschensuer and Gligor proposed the Basic Random Key Predistribution scheme denoted by EG scheme. In this scheme, before deployment, a large key pool which contains many distinct keys with key identifier is randomly generated. And each sensor node is loaded with a predefined number of keys that constitute its key rings. Keys in the key rings are randomly picked form the key pool. After deployment, two sensor nodes can communicate securely provided they share a common key. In the literature, this procedure of discovering of the common key between two sensor nodes is called shared key discovery. If there is no common key between two nodes, they have to establish a key through an intermediate sensor node which has common keys with both sensors, which is called path key establishment. In this scheme, there is a tradeoff between connectivity and security. As the size of the key pool increase, connectivity decreases, but protocol security increased. Chen *et al.*, [8] generalized this scheme to the q-compromised scheme aiming to increase the network resilience at the cost of some processing overhead. The main difference between [7] and [8] is that the later scheme require two neighboring nodes shares at least q (q>1) keys to establish secure communication links. This scheme is more resilient when few nodes are captured, but becomes less secure when many nodes are captured.

Du *et al.*, [9] proposed a combination of the EG scheme [7] and Blom's scheme [10]. This scheme first constructs many key spaces using Blom's scheme, and then have each sensor nodes carried key information from several randomly selected key spaces. If two sensor nodes carry key information from a common space they can compute a shared key. This scheme exhibits a nice threshold property, which means that when the number of compromised nodes is less than the threshold, the probability that communications between any additional nodes are compromised is close to zero. A similar method was also developed by Liu *et al.*, [11], in which polynomials are uses instead of matrixes. Later, these two schemes have been further explored in [12-14].

Camptepe and Yener [15, 16] proposed novel deterministic and hybrid approaches based on Combinatorial Design for deciding how many and which keys to assign to each key-chain before the sensor network deployment. In particular, Balanced Incomplete Block Designs (BIBD) and Generalized Quadrangles (GQ) are mapped to obtain efficient key distribution schemes. Performance and security properties of the proposed schemes are studied both analytically and computationally. Comparison to related work shows that the combinatorial approach produces better connectivity with smaller key-chain sizes. Lee and Stinson [17, 18] proposed a class of key pre-distribution schemes based on combinatorial designs. Their approaches improve the efficiency in direct-key and path-key establishments compared with the random key pre-distribution protocols.

Du *et al.*, [19] proposed the Group-Based Deployment Scheme, which combines the Basic Scheme[7] with deployment knowledge. They assumed that the sensor node is deployed in groups of sensor nodes over a rectangular area. The key pool is divided into sub key pools, one for each group, such that each key pool has some correlated keys with its neighboring sub key pool. By using location information, Liu and Ning [20, 21] were able to improve the scalability and the key connectivity of the network, without impacting on the amount of memory needed for storing keys. Zhou *et al.*, [22] proposed a new approach, which separates the nodes into groups, the nodes in a group communicate with each other using pairwise keys pre-distributed, the communications between any two neighbor groups are accomplished also through pairwise keys, which is computed based on the pre-distributed Hash chain.

In this paper, we exploit the combinatorial design in conjunction with the Blom schemes [10] to establish a secure link between sensor nodes and improve network

resilience to node captures. With the advantages of the combinatorial design, this scheme has higher local connectivity than the Multiple-Space Key Predistribution scheme(MSKPD) [9]. And this scheme will perform better security than MSKPD scheme under the same local connectivity.

The rest of this paper is organized as follows. In Section 2, we give an overview on matrix-based key establishment schemes, followed by some basics on combinatorial designs which will be which will be used in designing the key predistribution scheme. Section 3 describes our propose protocol in details. Section 4 describes the performances of our scheme, and Section 5 concludes the paper.

2. Background

2.1. Matrix-Based Key Establishment Schemes

In [10], Blom proposed a key establishment scheme that allows each pair of sensor nodes to establishment a common key. In this scheme, there are two matrices over $F(q)$: a public $(\lambda+1)\times n$ matrices M and a secret $(\lambda+1)\times(\lambda+1)$ symmetric random matrix D. These matrices are used to compute the symmetric $n\times n$ matrix $K=(DM)^TM$, whose element $K_{ij}=K_{ji}$, corresponds to the key between sensor nodes i and j. During the key predistribution scheme, each senor node i is loaded with col_i, the i-th column of matrix M , which is used as public information; each node also receives row i, the i-th row of matrix $(DM)^T$, which is kept private.

After deployment, all sensor nodes broadcast their column instances of M, allowing any pair of sensor node i and j to compute $K_{ij}=row_i\times col_j=row_j\times col_i$. This scheme is λ secure, which means that an attacker who captures up to λ sensor nodes is unable to recover link keys from any other sensor nodes. However if more than λ sensor nodes are compromised all keys can be recovered.

Blom scheme has some attractive properties. As it allow the creation pairwise keys, the deployment of sensor node authentication and revocation functionalities are made easier. Additionally, the scheme provides perfect key connectivity and its resilience can be adjusted by choosing an adequate λ parameter. However, the larger the size of λ ,the larger become the message broadcast, the storage requirements and the complexity of the vector multiplication involved in this solution. Thus, one has to choose the adequate trade-off between security and efficiency.

Du *et al*., [9] proposed the Multiple-Space Key Predistribution(MSKPD), which is a combination of the random key generation schem [7] and Blom's Scheme[10] in order to improve the resilience of the last solution without increasing λ. The resulting Multiple-Space Key Pre-Distribution Scheme employs a $(\lambda+1)\times N$ matrices D_i, $1\le i\le\omega$, which define a set of w spaces (D_i, M).During Key Pre-distribution, every sensor j is loaded with the jth column of M (*i.e.*, col_j); additionally, for $\tau(1\le\tau\le\omega)$ randomly chosen spaces (D_i, M), node j is loaded with the *i-th* row from the corresponding matrices $(D_iM)T$(*i.e.*, the nodes receives τ IDs of the spaces it carries. If two neighboring nodes share a common space, the can establish a pairwise key using Blom's Scheme; otherwise, a common key can be generated using the Basic Scheme's Path-key Establishment protocol. According to the authors' analysis, the Multiple-Space Key Predistribution schemes present a very good resilience.

2.2. Basics on Combinatorial Design

Definition 1: *A combinatorial design* is a pair (X, A), where A is a set of subsets of X, called blocks. The elements of X are called varieties. A Balanced Incomplete Block Design (BIBD) is an arrangement of v district object into b blocks such that each block contains exactly k distinct objects, each object occurs in exactly r

different blocks, and every pair of distinct objects occurs together in exactly τ blocks. The design can be expressed as (v, k, τ), where: $\tau(v-1)=r(k-1)$ and $bk=vr$.

Definition 2*: A BIBD* is called Symmetric BIBD or Symmetric Design when $b=v$ and therefore $v=k$. A Symmetric Design has four properties: every block contains $k=r$ elements; every element occurs in $r=k$ blocks; every pair of elements occurs in τ blocks, and every pair of blocks intersects in τ elements.

Example 1: Consider (v, b, τ)=(7,3,1), or equivalently (v,b,r,k,τ)=(7,7,3,3,1), Symmetric Design. Let S={ 1,2,3,4,5,6,7} be the set of |S|=v=7 objects. There are b=7 blocks and each bock contains k=3 objects. Every object occurs in $r=3$ blocks. Every pair of district objects occurs in τ=1 blocks and every pair of blocks intersects in τ=1 objects. The blocks of the Symmetric Design are:

{ 1,2,3}{ 4, 5,6}{ 1,6,7} {2,4,6}, {2,5,7}{3,4,7}{3,5,7}

In this paper, we are interested in a subset of Symmetric Designs, called a Finite Projective Plane.

Definition 3: An (n^2+n+1, n^2+n+1,$n+1$,$n+1$, 1)-BIBD is called a *Finite Projective Plane of order n*. Finite projective plane consists of a finite set P of points and a set of subsets of P, called lines. For an integer n where $n \geqslant 2$, and n is a prime or prime-power. Finite Projective Place of order n has four properties:

we consider lines as blocks and points as objects, then a Finite Projective Place of order n is a Symmetric Design with Parameter(n^2+n+1, $n+1$,1). An example of systematic design X=(7, 3, 1) when n=2 is A={{1, 2,3}, {1, 4,5},{1,6,7}, {2,4,6}, {2, 5,7}, {3, 4,7}, {3,5,6}}.

3. The Proposed Scheme

In this subsection, we first describe how finite projective plane are used to assign key spaces to sensor nodes and then give the details of the proposed scheme.

3.1. Mapping from Finite Projective Plane to Key Space Distribution

In this work, we are interested in Finite Projective Plane of order n which is a BIBD with parameters(n^2+n+1, $n+1$,1).

For a WSN, a Symmetric Design with b blocks is constructed by using a set S with $|S|=v=b$ objects. That means $b=v=n^2+n+1$ for a prime power n. Each object in S can be associated with a distinct key space and each block can be used as a group of key spaces. Each sensor node has t key spaces which are randomly selected from a set B of a group of key spaces. If two sensor nodes have a common key space they can generate a pairwise key by using this key space. Based on this, Table 1 gives the mapping form symmetric design to key distribution in our proposed protocol.

Table 1. Mapping from Symmetric Design to Key Distribution

Symmetric Design		Key Distribution
object (point) set(P)	→	key space pool (P)
object (point)set size $\|P\|=v=n^2+n+1$	→	key space pool size(|P|)
blocks(lines)	→	key space groups
# blocks(lines)($b= n^2+n+1$)	→	# key space groups($N= n^2+n+1$)
# objects (points)in a block(line)	→	# key spaces in a key space

(k=n+1)		group(s=n+1)
#blocks(lines) that an object(points) is in(r=n+1)	→	# key space groups that a key space group is in
Two blocks(lines) share(τ=1) object(points)	→	# two key space groups share (τ=1)key space

3.2. Details of the Proposed Scheme.

In this section, we describe the proposed key predistribution scheme works in detail. The proposed scheme can be divided into three phases: key distribution phase, pairwise key establishment phase, and path key establishment phase.

3.2.1. Key Predistribution Phase

This phase is performed offline before the sensor nodes are deployed and includes the following steps.

Step 1: The setup server first selects a prime or prime-power n and constructs a symmetric design with $b= n^2+n+1$ blocks by using a set S with $v= n^2+n+1$ objects.

Step 2: The setup server generates $|P|= n^2+n+1$ key spaces and uses the method in step 1 to divide these n^2+n+1 key spaces into n^2+n+1 key space groups. According to the properties of finite projective place, there are $n+ 1$ key spaces in each key space groups and any two key space groups have a common key space.

Step 3: Each sensor node picks one key space group from the n^2+n+1 key space groups and then randomly selects t key spaces from this group as its preload key spaces. And then the sensor node loads the corresponding columns of these t matrixes to its memory.

3.2. Pairwise Key Establishment Phase and Path Key Establishment Phase

In the network bootstrap phase, each sensor node is required to broadcast the ID of key spaces in it. If they have a common key space, they can use it to generate the communication key as in [9]. If they share no common key space, they can use intermediate sensor nodes to generate the communication key.

4. Performance Analysis

In this section, the proposed scheme is analyzed, including network connectivity, resilience against node capture and performance overhead.

4.1. Local Connectivity

Local connectivity is defined as the probability that two neighboring nodes can establish can establish communication pairwise keys directly. Suppose there are two sensor node u and v in the WSNs. Let $E(u, v)$ be the event that node u and v have at least one key space, then local connectivity $P_{local}=P(E(u,v))$.

Suppose $E_1(u,v)$ be the event that node u and v pick the same group and $E_2(u, v)$ be the event that node u and v pick different groups. As there are n^2+n+1 groups, we have

$$P(E_1(u,v)) = \frac{1}{n^2+n+1} \tag{1}$$

$$P(E_2(u,v)) = \frac{n^2+n}{n^2+n+1} \tag{2}$$

According to the property of the finite projective plane, we have

$$P(E(u,v) \mid E_1(u,v)) = 1 - \frac{\binom{t}{n+1}\binom{t}{n+1-t}}{\binom{t}{n+1}\binom{t}{n+1}} = 1 - \frac{\binom{t}{n+1-t}}{\binom{t}{n+1}} \tag{3}$$

$$P(E(u,v) \mid E_2(u,v)) = \frac{t}{(n+1)} \cdot \frac{t}{(n+1)} = \frac{t^2}{(n+1)^2} \tag{4}$$

As the event $E_1(u,v)$ and $E_2(u,v)$ are two complementary events, We can get the local connectivity of node u and v as follows.

$$\begin{aligned} P_{local} &= P(E(u,v)) = P(E(u,v)(E_1(u,v) + E_2(u,v)) \\ &= P(E(u,v)(E_1(u,v)) + P(E(u,v)E_2(u,v)) \\ &= P(E(u,v) \mid (E_1(u,v)) \cdot P(E_1(u,v)) + P(E(u,v) \mid E_2(u,v))P(E_2(u,v)) \\ &= \frac{1}{n^2+n+1} \cdot \left(1 - \frac{\binom{t}{n+1-t}}{\binom{t}{n+1}}\right) + \frac{n^2+n}{n^2+n+1} \cdot \frac{t^2}{(n+1)^2} \end{aligned} \tag{5}$$

Figure 1 shows the network local connectivity of the proposed scheme for different. It is also noted that the larger n is, the smaller the local connectivity is. And when the number of key spaces in sensor node is greater than or equal to n+1 the local connectivity is 1. That is that according to the property of Symmetric Design that any two blocks (lines) are surely have a common object or point.

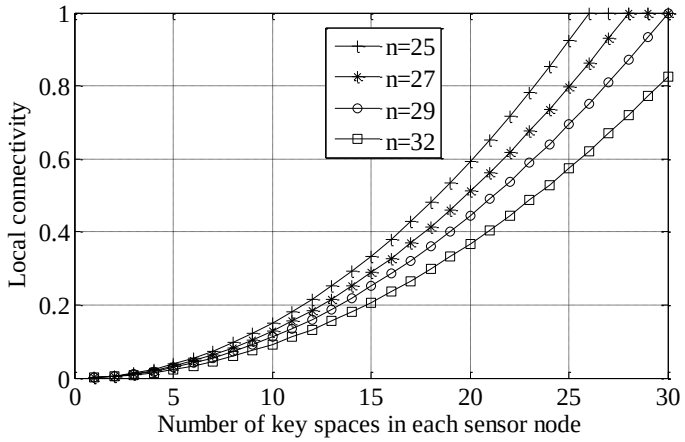


Figure 1. Local Connectivity for Different *n*

Figure 2 gives the local connectivity comparison of the MSKPD scheme and the proposed scheme. In the simulation, we assume that the key spaces in the key space

pool is 625(=25^2+25+1) in (1) and 871(=29^2+29+1) in (2) respectively. Figure 2 clearly shows that under the same situation the local connectivity of the proposed scheme is super to that of the MSKPD scheme. For two key predistribution schemes, the scheme with higher local connectivity will generally have a better security against node capture attack. This will be proved in the following subsection 4.2.2.

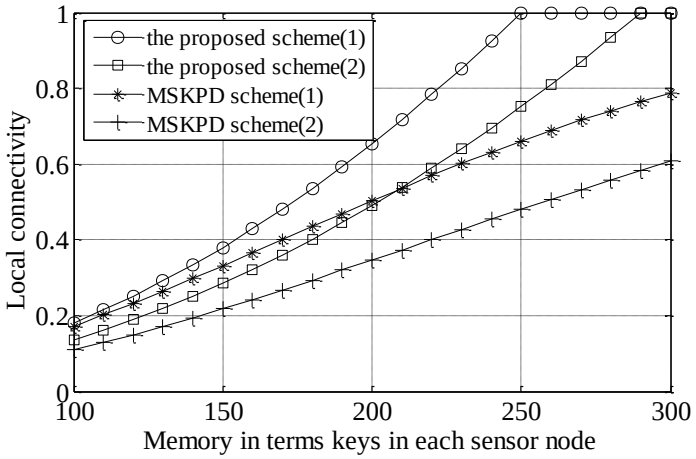


Figure 2. Local Connectivity Comparison of the MSKPD Scheme and the Proposed Scheme

4.2. Resilience against Node Capture

In this section, we evaluate how the proposed scheme improves the network security in terms of resilience against node capture. We compare our scheme with some existing schemes by calculating the fraction of compromised communication among non-compromised nodes.

4.2.1. Fraction of Compromised Network Communication: Now we study the resiliency property of the proposed scheme against node compromise by calculating the fraction of communication keys in the network that are compromised due to key revealing resulted from captured nodes. Here, we calculate the probability the compromising the shared pairwise key between these two non-compromised sensor nodes when there are x sensor nodes have been captured.

Suppose K be the communication key used by two non-compromised sensor node u and v and L is the communication link between node u and v. Let S_i denote the i-th polynomial (for $i \in \{1, 2,\ldots, n^2+n+1\}$, and D_i represent the joint event that K are computed by the polynomial S_i and S_i is compromised. We use the notation $K \in S_i$ to represent that "Key K was derived from the key K_i". When x nodes have been compromised, the probability of the communication key K been compromised is:

$$P(L \text{ is broken} \mid C_x) = P(D_1 \cup D_2 \cup \cdots D_{n^2+n+1} \mid C_x) \tag{6}$$

Since L uses only one key, the events $D_1, D_2, \cdots, D_{n^2+n+1}$ are mutually exclusive. Therefore

$$P(L \text{ is broken} \mid C_x) = \sum_{i=1}^{n^2+n+1} P(D_i \mid C_x) \tag{7}$$

As all events D_i is equal probability likely, we have

$$P(L\ is\ broken|\ C_x) = (n^2+n+1)P(D_1|\ C_x) \tag{8}$$

Note that

$$\begin{aligned} P(D_1|C_x) &= P((K \in S_1 \cap (S_1\ is compromised))|C_x) \\ &= \frac{P((K \in S_1) \cap (S_1\ is compromised) \cap C_x)}{P(C_x)} \end{aligned} \tag{9}$$

Since the event $K \in S_1$ is independent of the event $(S_1\ is compromised) \cap C_x$, then

$$P(D_1|C_x) = \frac{P(K \in D_1)P((S_1\ is compromised) \cap C_x)}{P(C_x)} \tag{10}$$

As K is derived from one key space and there are n^2+n+1 key spaces, then

$$\Pr(K \in S_1) = \frac{1}{n^2+n+1} \tag{11}$$

$$P(L_{broken}|\ C_x) = (n^2+n+1)\cdot\frac{1}{n^2+n+1}P(S_{1compromized}|\ C_x) = P(S_{1compromized}|\ C_x) \tag{12}$$

To facilitate the presentation, here we first give the following definition.

Definition 4: *The* u*nsafe node of the first key space* is the node that selects the key space group which contains the first key space.

Now, we need to calculate $P(S_{1compromized}|\ C_x)$ the probability of the first key space being compromised when x sensor nodes are compromised. According the property of finite symmetric projective plane, the first key space can only in (n+1) key space groups. As there are n^2+n+1 key space groups and each sensor nodes picks one group, the probability that a compromised nodes is a unsafe node of the first keys space is $\frac{n+1}{n^2+n+1}$ .Then when x nodes are compromised, the probability of there are j unsafe nodes of first key space is

$$p(j) = \sum_{i=0}^{j}\binom{x}{j}\left(\frac{n+1}{n^2+n+1}\right)^j\left(1-\frac{n+1}{n^2+n+1}\right)^{x-j} \tag{13}$$

As there are t key spaces in each node and these key spaces are selected from a key space group, then the probability that the fist key spaces is compromised when there are j compromised unsafe node to the first key spaces is $\frac{t}{n+1}$, then we have

$$\begin{aligned} P(S_{1compromized}|\ C_x) &= \sum_{i=\lambda+1}^{x} p(j)\sum_{h=\lambda+1}^{j}\binom{j}{i}\left(\frac{t}{n+1}\right)^j\left(1-\frac{t}{n+1}\right)^{j-i} \\ &= \sum_{j=0}^{x}\binom{x}{j}\left(\frac{n+1}{n^2+n+1}\right)^j\left(1-\frac{n+1}{n^2+n+1}\right)^{x-j}\sum_{h=\lambda+1}^{j}\binom{j}{i}\left(\frac{t}{n+1}\right)^j\left(1-\frac{t}{n+1}\right)^{j-i} \end{aligned} \tag{14}$$

From formula (12) and (14), we can get

$$P(L_{brocken} \mid C_x) = \sum_{j=0}^{x} \binom{x}{j} \left(\frac{n+1}{n^2+n+1}\right)^j \left(1-\frac{n+1}{n^2+n+1}\right)^{x-j} \sum_{h=\lambda+1}^{j} \binom{j}{i} \left(\frac{t}{n+1}\right)^j \left(1-\frac{t}{n+1}\right)^{j-i} \quad (15)$$

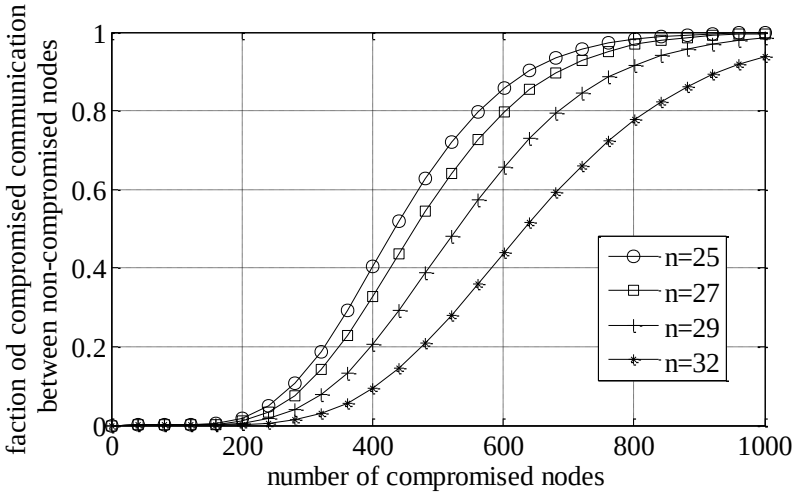
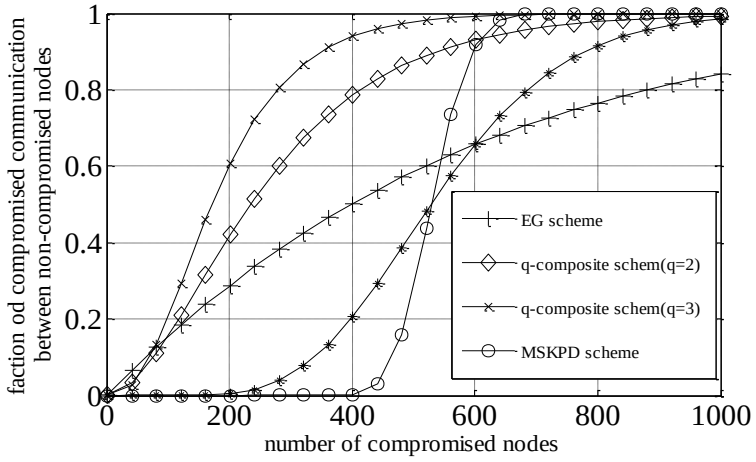
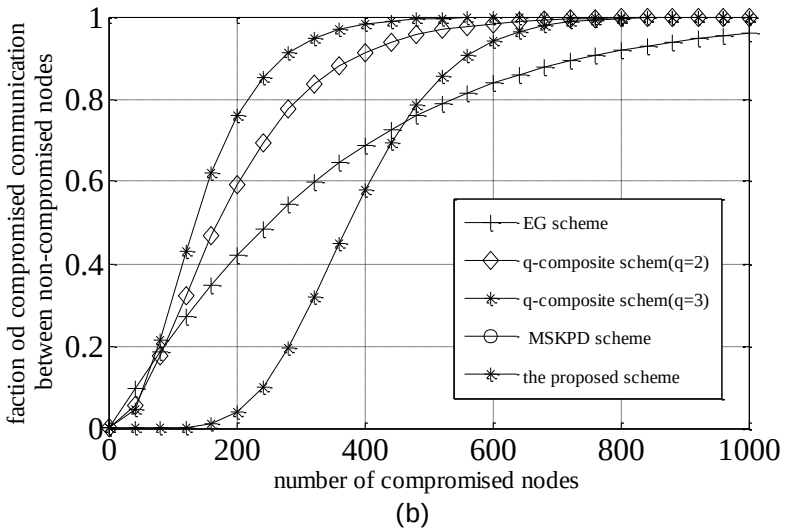


Figure 3. Fraction of Compromised Communication between Noncompromsied Nodes versus Number of Compromised Nodes

4.2.2 Comparison with Related Work: Here, To access how much is the improvements gained by the proposed scheme, we compare our scheme with EG scheme [7], *q*-composite scheme (for *q*=2, 3) [8], and MSKPD scheme[9]. Figure 4 (a)(b) clearly shows that our scheme has better security performances than that of EG schemes, *q*-composite scheme and MSKPD scheme. Taken as an example, the case in which P_{local} =0.5, when an adversary compromise 400 sensor nodes compromised, about be 75% of links compromised between non-compromised sensors in EG scheme will be disclosed, 93.1% in *q*-composite (*q*=2), 99.2% in *q*-composite (*q*=3), 99.5% in MSKPD scheme while there will only be 20% in our scheme.



(a)



(b)

Figure 4. Security of Comparison of EG Scheme, *q*-composite Scheme, MSKPS Scheme and our Scheme under the Same amount of Storage per Node with the Local Connectivity (a) P_{local} =0.34 (b) P_{local} =0.5

4.3. Storage and Communication Overhead

Storage overhead of our scheme is reasonable. Each sensor node of our scheme is associates with *t* key spaces, and for each key space, the node is loaded with the corresponding row of its matrix *M*. In addition, each node needs to remain the IDs of the key space. Assume the keys are chosen from a finite field F_q and the IDs of sensor nodes are chosen from a finite field $\mathrm{F}_{q'}$. Thus, the overall storage overhead is $t((\lambda+1)\log q+\log q')$bits; In terms of communication overhead, in the shared key discover phase each need to disclose of a list of *t* IDs to its neighbor nodes. Then the communication overhead of each node is $t\log q'$.

5. Conclusion

In this paper, an efficient new key management scheme based on Matrix and combinatorial design was proposed. The proposed approach uses finite projective plane to distribute the key space. With properties of the combinatorial design, the proposed scheme has a high local connectivity. The effectiveness of the proposed scheme has been demonstrated through analysis and comparison with other scheme.

References

[1] T. Arampatzis, J. Lygeros and S. Manesis , “A survey of applications of wireless sensors and wireless sensor networks”, Proceeding of the 2005 IEEE International Symposium on Control and Automation, Limassol, Cypru, **(2005)** June 27-29, pp. 719-724.
[2] D. Puccinelli and M.Haenggi, “Wireless sensor networks: applications and challenges of ubiquitous sensing”, Circuits and Systems Magazine, IEEE, vol. 5, no. 3, **(2005)**, pp. 19-31.
[3] K. Romer and F. Mattern, “The design space of wireless sensor networks”, Wireless Communications, IEEE, vol. 11, no. 6, **(2004)**, pp. 54-61.
[4] M. A. Simplício Jr., P. S. L.M.Barreto, C. B. Margi and T C. M. B. Carvalho, “A survey on key management mechanisms for distributed Wireless Sensor Networks”, Computer Networks, vol. 54, no. 15, **(2010)**, pp. 2591-2612.
[5] Y. Xiao, V. K. Rayi, B. Sun, D. Xiaojiang, F. Hue and M. Gallowaya, “A survey of key management schemes in wireless sensor networks”, Computer communications, vol. 30, no. 11, **(2007)**, pp. 2314-2341.

[6] R. Szewczyk Perrig, V. Wen, D. E. Culler and J. D. Tygar, "SPINS: security protocols for sensor networks", Wireless Networks, vol. 8, no. 5, **(2002)**, pp. 521–534.
[7] L. Eschenaure and V. D. Gligor, "A key-management scheme for distributed sensor networks", Processing of the 9th ACM Conference on Computer and Communications, **(2002)**, pp. 41-47.
[8] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks", Processing of 20003 IEEE Symposium on Security and Privacy, **(2003)**, pp. 197-213.
[9] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz and A. Khalili, "A pairwise key predistribution schemes for sensor networks", ACM Transactions on Information and System Security, vol. 8, no. 2, **(2005)**, pp. 228-258.
[10] R. Blom, "An optimal class of symmetric key generation systems", Proceedings of Advances in cryptology, **(1985)**, pp. 335-338.
[11] D. Liu, P. Ning and R. Li, "Establishing Pairwise Keys in Distributed Sensor Networks", ACM Transactions on Information and System Security, vol. 8, no. 1, **(2005)**, pp. 41-77.
[12] A. Rasheed and R. N. Mahapatra, "Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor networks", IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 1, **(2011)**, pp. 176-184.
[13] F. Delgosha and F. Fekri, "A multivariate key-establishment scheme for wireless sensor networks", IEEE Transactions on Wireless Communications, vol. 8, no. 4, **(2009)**, pp. 1814-1824.
[14] H. Dai and H. Xu, "Key Predistribution Approach in Wireless Sensor Networks Using LU Matrix", IEEE Sensors Journal, vol. 10, no. 8, **(2011)**, pp. 1399-1409.
[15] S. A. Campete and B. Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks", Proceedings of Computer Security, **(2004)**, pp. 293-308.
[16] S. A. Camtepe and B. Yener "Combinatorial design of key distribution mechanisms for wireless sensor networks", IEEE/ACM Transactions on Networking, vol. 15, no. 2, **(2007)**, pp. 346-358.
[17] J. Lee and D. K. Stinson, "Deterministic key predistribution schemes for distributed sensor networks", Proceedings of the 11th Int'l Workshop, **(2005)**, pp. 293-307
[18] J. Lee and D. K. Stinson, "A combinatorial approach to key predistribution for distributed sensor networks", Proceedings of IEEE Wireless Communication Network Conference, **(2005)**, pp. 1200-1205.
[19] W. Du, Y. S. Han and P. Varshney, "A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge", IEEE Transactions Dependable Secure Compute, vol. 3, no. 1, **(2006)**, pp. 62-77.
[20] D. Liu and P. Ning, "Location-based pairwise key establishments for static sensor networks", Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, **(2003)**, pp. 72-82.
[21] D. Liu and P. Ning, "Improving key predistribution with deployment knowledge in static sensor networks", ACM Transactions on Sensor Networks, vol. 1, no. 2, **(2005)**, pp. 204-239.
[22] B. Zhou, S. Li, Q. Li, X. Sun and X. Wang, "An Efficient and Scalable Pairwise Key Pre-distribution Scheme for Sensor Networks Using Deployment Knowledge", Computer Communications, vol. 32, no. 1, **(2009)**, pp. 124-133.

