Key Pre-distribution Schemes based on Symplectic Geometry for Wireless Sensor Networks *

Shangdi Chen† Huihui Wei

College of Science, Civil Aviation University of China, Tianjin, 300300, China

Abstract Key distribution is paramount for wireless sensor networks (WSNs). The design of key management schemes is the most important aspects and basic research field in WSNs. A key distribution scheme based on symplectic geometry over fields is proposed, a 2-dimensional subspace in symplectic geometry represents a node, all 2s-dimensional non-isotropic subspaces represent key pool, and guarantees every pair of nodes has shared key, so as to improve the networks connectivity. The performance analysis shows that the scheme has good connectivity and higher resilience to node compromise compares with other key pre-distribution schemes.

Keywords Key pre-distribution; Symplectic geometry; Wireless sensor network.

MSC 2010 05B25, 11E57, 94A60, 94A62

1 Introduction

Recent advancements in micro-electro-mechanical systems and low power and highly integrated electronic devices have led to the development and wide application of wireless sensor networks (WSNs)[1]. WSNs which integrate wireless communication technology, sensing technology and computer technology are considered as one of the most important technologies in the 21th century.

*Supported by the National Natural Science Foundation of China(No.61179026), and the Fundamental Research Funds For The Central Universities(No.3122014K015 and No.3122013K001).

†Corresponding author. E-mail address: 11csd@163.com; sdchen@cauc.edu.cn

1.1 Wireless Sensor Networks

A WSN[2,3] is an ad hoc network consisting of spatially distributed sensor nodes that autonomously gather data and use wireless communication to transmit the information that they collect. The typical characteristics of a WSN are:

1. *Highly constrained nodes.* The nodes are very small battery-powered devices and are highly constrained with respect to memory storage and power. They are thus limited in their computational and communication ability.

2. *Lack of central control.* Once deployed, most WSNs do not feature any central control node. Thus all network functionality must be achieved through co-operation between the nodes.

3. *Requirement to form a network to a sink.* In most WSNs the assumption is that the sensor nodes will take readings and then attempt to communicate this data back to a sink, which is a more powerful device that will periodically connect to the WSN and request data. The location of this sink in the network is typically not fixed (it could, for example, be a portable laptop).

4. *Hop-based communication.* Most WSNs use radio communication to connect between nodes. The constrained nature of the nodes means that in most cases the communication range of a node will be much smaller than the network diameter. Thus nodes communicate by hopping, meaning that a node passes data to a node within range, who then passes it onto a node within its range, etc.

5. *Dynamic network structure.* It is generally assumed that WSNs are highly dynamic. Nodes are often assumed to regularly sleep to conserve battery power. Nodes expire once their battery is drained. In some WSNs the nodes are mobile, although in most current applications they are static.

6. *Nodes vulnerable to compromise.* The constrained nature of sensor nodes mean that strong security protection such as tamper-resistance is usually not viable. Thus it is normally assumed that sensor nodes can be fairly easily captured and that any sensitive information (such as keys) that is stored on them is likely to be exposed.

Sensor networks consist of many tiny and inexpensive sensing devices, which have low battery power, low computation speed, limited memory capability and limited resources, and are scattered randomly in large numbers over a target area.

Sensor networks are increasingly used in numerous fields such as military, medical and industrial sectors. They are more and more involved in several sensitive applications which require sophisticated security services. Due to the resource limitations, existing security solutions for conventional networks could not be used in WSNs. So, the security issues become one of the main challenges for the resource constrained environment of WSNs.

Key management is a corner stone service for many security services such as confidentiality and authentication which are required to secure communications in WSNs. The establishment of secure links between nodes is a challenging problem in WSNs. Unfortunately, public key based solutions, which provide efficient key management services in conventional networks, are unsuitable for WSNs because of resource limitations.

1.2 Key Pre-distribution Schemes for WSNs

Key management problems in WSNs have been extensively studied in the literature and several solutions have been proposed. According to the key distribution method of nodes, the key pre-distribution schemes (KPSs) for WSNs can be divided into probabilistic key management schemes and deterministic key management schemes.

Probabilistic key pre-distribution scheme is a key pre-distribution scheme model of probability results. In this scheme, keys are drawn randomly from a key pool and placed in the sensor nodes prior to deployment which ensure that the probability of any two nodes have shared key is higher than a certain value. The set of keys in a node is called a *key chain*. Random key pre-distribution schemes have the following two kinds:

1. Basic random key pre-distribution schemes.

   The study of KPSs for WSNs began in the paper by Eschenauer and Gligor[5] in 2002. They proposed a basic random key pre-distribution scheme with computational security and "good" connectivity of nodes. The KPS for WSN can be thus regarded as consisting of the following three stages:

   (a) *Key pre-distribution.* Each node is pre-loaded with a key ring of k keys randomly selected from a large key pool denoted by S. After the deployment step, each node exchanges with each of its neighbors the list of key identifiers that it maintains in order to identify the common keys.

   (b) *Shared key discovery.* If two nodes within communication range of one another wish to deploy a cryptographic service, they first

need to determine if they have any keys in common. The default method is to broadcast their node allocations to one another, but more efficient techniques can sometimes be found. If they have key identifiers in common then a session key can be generated from the common keys associated with these identifiers by means of a suitable key derivation function.

(c) *Path-key establishment.* If two nodes fail to identify common keys during shared key discovery, then they need to find a secure path between one another by employing intermediate nodes which can. Obviously, the shorter this secure path the better.

In the basic random key pre-distribution scheme, there exists a mathematical relationship among the probability p of shared keys between two nodes, the key pool S and the key ring length k:

$$p = 1 - \frac{\left(1 - \frac{k}{|S|}\right)^{2\left(|S|-k+\frac{1}{2}\right)}}{\left(1 - \frac{2k}{|S|}\right)^{\left(|S|-2k+\frac{1}{2}\right)}}.$$

2. q-composite random key pre-distribution scheme

Based on the basic Eschenauer-Gligor scheme, Chan, Perrig, and Song[7] proposed a q-composite random key pre-distribution scheme, which increases the security of key setup such that an attacker has to compromise many more nodes to achieve a high probability of compromising communication. The relationship among the probability p of shared keys between two nodes, the key pool S and the key ring length k as follows:

$$p = 1 - \sum_{i=0}^{q-1} \frac{C\left(|S|, i\right) C\left(|S| - i, 2(k-i)\right) C\left(2(k-i), (k-i)\right)}{C^2\left(|S|, k\right)}.$$

Deterministic key pre-distribution schemes ensure that each node can establish a pair-wise key with all its neighbors. The main drawback of this scheme is the non scalability because the number of the stored keys is equal to the network size which is very restrictive.

Camtepe and Yener[8] proposed a new deterministic key pre-distribution scheme based on symmetric balanced incomplete block design (SBIBD), they introduced a mapping from the SBIBD to the pool based on key distribution. The scheme has total secure connectivity because each pair of two key rings shares exactly one common key.. However, the SBIBD

scheme does not scale to very large networks. Indeed, using key rings of $n+1$ keys we can generate only n^2+n+1 key rings.

Blundo et al.[9] proposed several schemes which allow any group of t parties to compute a common key while being secure against collusion between some of them. These schemes focus on saving communication costs while memory constraints are not placed on group members. When $t=2$, one of these schemes is actually a special case of Bloms scheme[10], which uses one key space for all nodes to make sure that any pair can compute its pairwise key in this key space.

Liu[11] proposed a key pre-distribution scheme based on polynomial. Lee and Stinson[12] proposed a key pre-distribution scheme by using regular graphs. These models can establish key path effectively and ensure the network security. However, the probability of dual key establishing between sensor nodes is low, which costs higher communication overhead.

Chakrabarti et al.[16] provided a scheme where they randomly choose x number of blocks which merged to form a new node. They chose the blocks randomly, so for some cases they could not avoid the occurrence of inter node connectivity.

Aldar[17] introduced a graph theoretical framework to study the fundamental tradeoffs between key storage, average key path length and resilience of key pre-distribution schemes for wireless sensor networks. Based on the proposed framework, a lower bound on key storage and an upper bound on the compromising probability are given.

S Khalid et al.[18] evaluated various existing deterministic, probabilistic and hybrid type of key pre-distribution and dynamic key generation algorithms for distributing pair-wise, group-wise and network-wise keys. In addition, they proposed a key pre-distribution scheme using combinatorial design and traversal design which improve the resiliency and achieve sufficient level of security in the network.

In this paper, we first use symplectic geometry over finite field to construct a key pre-distribution scheme for wireless sensor networks. A 2-dimensional subspace in symplectic geometry represents a node and the 2s-dimensional non-isotropic subspaces orthogonal to the 2-dimensional subspace represent the keys.

Then we study and compare the connectivity and security of our scheme with respect to existing schemes. We study the security of such a network in terms of a parameter, which consider the proportion of nodes disconnected, when m nodes are compromised. We show that our design results in much better connectivity and security compared to [5], [12], [13], [16].

1.3 Organization

This paper is organized as follows. Section 2 presents the mathematical structures that are used in this paper. Section 3 we present our new key pre-distribution scheme. Section 4 we discuss the connectivity and security of our scheme and compare our scheme with several other existing ones. Section 5 we conclude with some open problems.

2 Symplectic Geometry

Assume that $\mathbb{F}_q$ is a finite field with q elements, where q is a prime power. Let

$$K = \begin{pmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{pmatrix}$$

be a $2\nu \times 2\nu$ matrix over $\mathbb{F}_q$. The $2\nu \times 2\nu$ matrices T over $\mathbb{F}_q$ such that $TK\,{}^tT = K$ form a group with the matrix multiplication as its composition, where ${}^tT$ denotes the transpose of T. This group is called the symplectic group of degree 2ν over $\mathbb{F}_q$, and denoted by $Sp_{2\nu}(\mathbb{F}_q)$, i.e.

$$Sp_{2\nu}(\mathbb{F}_q) = \{T \in GL_n(\mathbb{F}_q) | TK\,{}^tT = K\}.$$

Let $\mathbb{F}_q^{(2\nu)}$ be the 2ν-dimensional row vector space over $\mathbb{F}_q$. An action of $Sp_{2\nu}(\mathbb{F}_q)$ on $\mathbb{F}_q^{(2\nu)}$ defined as follows:

$$\begin{array}{rcl} \mathbb{F}_q^{(2\nu)} \times Sp_{2\nu}(\mathbb{F}_q) & \rightarrow & \mathbb{F}_q^{(2\nu)} \\ ((x_1, x_2, \cdots, x_{2\nu}), T) & \mapsto & (x_1, x_2, \cdots, x_{2\nu})T. \end{array}$$

The vector space $\mathbb{F}_q^{(2\nu)}$ together with the action of $Sp_{2\nu}(\mathbb{F}_q)$ is called the *2ν-dimensional symplectic space* over $\mathbb{F}_q$.

Let P be an m-dimensional vector subspace of $\mathbb{F}_q^{(2\nu)}$, we also use the same symbol P to denote the $m \times 2\nu$ matrix with rank m over $\mathbb{F}_q$. An m-dimensional subspace P is called a subspace of type (m, s), if the rank of $PK\,{}^tP$ be $2s$. In particular, subspaces of type $(m, 0)$ are called m-dimensional *totally isotropic subspace*, and subspaces of type $(2s, s)$ are called $2s$-dimensional *non-isotropic subspace.*

The following theorems will be used in the later proof process and Theorem 2.1-2.5 are adopted from [15].

Theorem 2.1 *There exists subspace of type (m, s) in 2ν-dimensional symplectic space $\mathbb{F}_q^{(2\nu)}$, if and only if $2s \leq m \leq \nu + s$. Moreover, a subspace of type (m_1, s_1) contained in a given subspace of type (m, s), if and only if $\max(0, \alpha) \leq \min(\beta, \gamma)$, where $\alpha = m_1 - s - s_1$, $\beta = m - 2s$, $\gamma = m_1 - 2s_1$.*

Theorem 2.2 *The number of all subspaces of type (m, s) in 2ν-dimensional symplectic space $\mathbb{F}_q^{(2\nu)}$ is denoted by $N(m, s; 2\nu)$, then*

$$N(m,s;2\nu) = q^{2s(\nu+s-m)} \frac{\prod_{i=\nu+s-m+1}^{\nu}(q^{2i}-1)}{\prod_{i=1}^{s}(q^{2i}-1)\prod_{i=1}^{m-2s}(q^i-1)}.$$

Theorem 2.3 *The number of all subspaces of type (m_1, s_1) in 2ν-dimensional symplectic space $\mathbb{F}_q^{(2\nu)}$ contained in a given subspaces of type (m, s) is denoted by $N(m_1, s_1; m, s; 2\nu)$, then*

$$\begin{aligned} & N(m_1,s_1;m,s;2\nu) \\ = & \sum_{k=\max(0,\alpha)}^{\min(\beta,\gamma)} \frac{\prod_{i=k-\alpha+1}^{s}(q^{2i}-1)\prod_{i=\beta-k+1}^{\beta}(q^i-1)}{\prod_{i=1}^{s_1}(q^{2i}-1)\prod_{i=1}^{\gamma-k}(q^i-1)\prod_{i=1}^{k}(q^i-1)} q^{2s_1(k-\alpha)+(m_1-k)(\beta-k)}. \end{aligned}$$

Theorem 2.4 *Let $0 \le m \le n$, then the number of m-dimensional vector subspaces in $\mathbb{F}_q^{(n)}$ is denoted by $N(m, n)$, then*

$$N(m,n) = \frac{\prod_{i=n-m+1}^{n}(q^i-1)}{\prod_{i=1}^{m}(q^i-1)}.$$

Let v be an arbitrary non-zero vector, a vector u in 2ν-dimensional symplectic space $\mathbb{F}_q^{(2\nu)}$ is orthogonal to vector v, if $uKv^t = 0$. Let $P^\perp$ denote the dual subspace of P, i.e.,

$$P^\perp = \{y \in \mathbb{F}_q^{(2\nu)} \mid yKx^t = 0, \text{for all} x \in P\}.$$

Obviously, $P^\perp$ is a $(2\nu - m)$-dimensional vector subspace of $\mathbb{F}_q^{(2\nu)}$.

We call P is orthogonal to Q, if $P \subseteq Q^\perp$.

Theorem 2.5 *Suppose that P is a subspaces of type (m, s) in 2ν-dimensional symplectic space $\mathbb{F}_q^{(2\nu)}$, then the dual subspace of P is a subspaces of type $(2\nu - m, \nu + s - m)$.*

Theorem 2.6 *Suppose that P is a subspaces of type (m, s) in 2ν-dimensional symplectic space $\mathbb{F}_q^{(2\nu)}$, then the number of all subspaces of type (m', s') orthogonal to P is $N(m', s'; 2\nu - m, \nu + s - m; 2\nu)$.*

Proof. Let P be a subspaces of type (m, s) in 2ν-dimensional symplectic space $\mathbb{F}_q^{(2\nu)}$. Without loss of generality, let

$$P = \begin{pmatrix} I^{(s)} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I^{(s)} & 0 & 0 \\ 0 & I^{(m-2s)} & 0 & 0 & 0 & 0 \\ s & m-2s & \nu+s-m & s & m-2s & \nu+s-m \end{pmatrix}.$$

Assume that Q is a subspace of type (m', s') orthogonal to P, then $Q \subseteq P^{\perp}$. In addition, $P^{\perp}$ is a subspaces of type $(2\nu - m, \nu + s - m)$.

Then we need to calculate the number of all subspaces of type (m', s') in 2ν-dimensional symplectic space $\mathbb{F}_q^{(2\nu)}$ contained in a given subspaces of type $(2\nu - m, \nu + s - m)$, that is, $N(m', s'; 2\nu - m, \nu + s - m; 2\nu)$.

3 The Construction of Key Pre-distribution Schemes

Let q be a power of prime number, and $\mathbb{F}_q^{(2\nu)} (\nu \geq 5)$ be the 2ν-dimensional row vector symplectic space over $\mathbb{F}_q$. There are $\frac{q^{2\nu}-1}{q-1}$ 1-dimensional subspaces in 2ν-dimensional symplectic space $\mathbb{F}_q^{(2\nu)}$. We choose the smallest q such that $n \leq \lfloor \frac{q^{2\nu}-1}{2(q-1)} \rfloor$.

Choice of parameter

Nodes Let n be the total number of nodes that the network can support. The nodes of the senor network are denoted by $P_1, P_2, \cdots$, and P_n, respectively.

There are $N(2, 2\nu)$ 2-dimensional subspaces in 2ν-dimensional symplectic space $\mathbb{F}_q^{(2\nu)}$. Since $n << N(2, 2\nu)$, we take n distinct 2-dimensional subspaces, which are denoted by $W_1, W_2, \cdots, W_{n-1}$ and W_n, and assign W_i to the node P_i, $i = 1, 2, \cdots, n$.

Key pool Let s be a fixed integer, $1 \leq s \leq \nu$. Each subspace of type $(2s, s)$ in 2ν-dimensional symplectic space $\mathbb{F}_q^{(2\nu)}$ represents a key, the set of all subspaces of type $(2s, s)$ in symplectic space $\mathbb{F}_q^{(2\nu)}$ is a key pool, so the size of the key pool is $N(2s, s; 2\nu)$.

Key chains For each sensor assign keys to sensor P_i corresponding to the subspaces of type $(2s, s)$ orthogonal to the subspace W_i, so the key chain in the node P_i is the set of all the subspaces of type $(2s, s)$ orthogonal to W_i in symplectic space $\mathbb{F}_q^{(2\nu)}$.

We use (P_i) to denote the set of all keys of a node P_i, i.e. (P_i) is the key chain of the node P_i. The set of shared keys of two nodes P_i and P_j is denoted by $(P_i) \cap (P_j)$. We also let $r_i = |(P_i)|$ and $\lambda_{ij} = |(P_i) \cap (P_j)|$.

Additional, we also note that $(P_i) \cap (P_j)$ is the set of all subspaces of type $(2s, s)$ orthogonal to the subspace $W_i + W_j$ in symplectic space $\mathbb{F}_q^{(2\nu)}$.

4 Analysis of Our Scheme

This section analyzes our scheme, calculating the number of keys required for each node, the number of shared keys in two nodes, the connectivity and security of the network.

4.1 Memory requirement

The following Lemmas 4.1 and 4.2 help us to calculate the number of keys in each node.

Lemma 4.1 *If W_i is a subspace of type $(2, 0)$, then the number of keys in node P_i is $N(2s, s; 2\nu - 2, \nu - 2; 2\nu)$.*

Proof. If W_i is a subspace of type $(2, 0)$, then the keys in node P_i are the subspaces of type $(2s, s)$ orthogonal to the subspace of type $(2, 0)$. Hence the number of keys in node n_i is $N(2s, s; 2\nu - 2, \nu - 2; 2\nu)$ by Theorem 2.6.

Lemma 4.2 *If W_i is a subspace of type $(2, 1)$, then the number of keys in node P_i is $N(2s, s; 2\nu - 2, \nu - 1; 2\nu)$.*

Proof. If W_i is a subspace of type $(2, 1)$, then the keys in node P_i are the subspaces of type $(2s, s)$ orthogonal to the subspace of type $(2, 1)$. Hence the number of keys in node P_i is $N(2s, s; 2\nu - 2, \nu - 1; 2\nu)$.

From Lemmas 4.1 and 4.2 it follows that:

Theorem 4.1 *The number of keys in node P_i is r_i, then $r_i = N(2s, s; 2\nu - 2, \nu - 2; 2\nu)$ or $N(2s, s; 2\nu - 2, \nu - 1; 2\nu)$.*

The following Lemmas 4.3, 4.4 and 4.5 help us to calculate the number of keys in common between any two nodes P_i and P_j.

Lemma 4.3 *If both W_i and W_j are subspaces of type $(2,0)$, $i \neq j$, then $W_i + W_j$ is a subspace of type $(3,0)$, $(3,1)$, $(4,0)$, $(4,1)$ or $(4,2)$.*

Proof. From our construction, we know that for any W_i, W_j, $i \neq j$, then $W_i \neq W_j$. By the dimension formula, $\dim(W_i + W_j) \geq 3$. It means that $W_i + W_j$ may be a subspace of type $(3,0)$, $(3,1)$, $(4,0)$, $(4,1)$ or $(4,2)$.

Since $Sp_{2\nu}(\mathbb{F}_q)$ acts transitively on each set of subspaces of the same type, without loss of generality, we can determine the types of $W_i + W_j$ according to the matrix representations of W_i and W_j.

1. If

$$W_i = \begin{pmatrix} \overbrace{1\ 0\ 0\ \cdots\ 0}^{\nu} & \overbrace{0\ \cdots\ 0}^{\nu} \\ 0\ 1\ 0\ \cdots\ 0 & 0\ \cdots\ 0 \end{pmatrix},$$

$$W_j = \begin{pmatrix} \overbrace{1\ 0\ \cdots\ 0}^{\nu} & \overbrace{0\ 0\ 0\ \cdots\ 0}^{\nu} \\ 0\ 0\ \cdots\ 0 & 0\ 0\ 1\ \cdots\ 0 \end{pmatrix},$$

then $W_i + W_j$ is a subspace of type $(3,0)$.

2. If

$$W_i = \begin{pmatrix} \overbrace{1\ 0\ 0\ \cdots\ 0}^{\nu} & \overbrace{0\ \cdots\ 0}^{\nu} \\ 0\ 1\ 0\ \cdots\ 0 & 0\ \cdots\ 0 \end{pmatrix},$$

$$W_j = \begin{pmatrix} \overbrace{1\ 0\ \cdots\ 0}^{\nu} & \overbrace{0\ 0\ 0\ \cdots\ 0}^{\nu} \\ 0\ 0\ \cdots\ 0 & 0\ 1\ 0\ \cdots\ 0 \end{pmatrix},$$

then $W_i + W_j$ is a subspace of type $(3,1)$.

3. If

$$W_i = \begin{pmatrix} \overbrace{1\ 0\ 0\ \cdots\ 0}^{\nu} & \overbrace{0\ \cdots\ 0}^{\nu} \\ 0\ 1\ 0\ \cdots\ 0 & 0\ \cdots\ 0 \end{pmatrix},$$

$$W_j = \begin{pmatrix} \overbrace{0\ 0\ 1\ 0\ \cdots\ 0}^{\nu} & \overbrace{0\ \cdots\ 0}^{\nu} \\ 0\ 0\ 0\ 1\ \cdots\ 0 & 0\ \cdots\ 0 \end{pmatrix},$$

then $W_i + W_j$ is a subspace of type $(4,0)$.

4. If

$$W_i = \begin{pmatrix} \overbrace{1\ 0\ 0\ \cdots\ 0}^{\nu} & \overbrace{0\ \cdots\ 0}^{\nu} \\ 0\ 1\ 0\ \cdots\ 0 & 0\ \cdots\ 0 \end{pmatrix},$$

$$W_j = \begin{pmatrix} \overbrace{0\ 0\ 1\ \cdots\ 0}^{\nu} & \overbrace{0\ 0\ \cdots\ 0}^{\nu} \\ 0\ 0\ 0\ \cdots\ 0 & 0\ 1\ \cdots\ 0 \end{pmatrix},$$

then $W_i + W_j$ is a subspace of type $(4,1)$.

5. If

$$W_i = \begin{pmatrix} \overbrace{1\ 0\ 0\ \cdots\ 0}^{\nu} & \overbrace{0\ \cdots\ 0}^{\nu} \\ 0\ 1\ 0\ \cdots\ 0 & 0\ \cdots\ 0 \end{pmatrix},$$

$$W_j = \begin{pmatrix} \overbrace{0\ \cdots\ 0}^{\nu} & \overbrace{1\ 0\ 0\ \cdots\ 0}^{\nu} \\ 0\ \cdots\ 0 & 0\ 1\ 0\ \cdots\ 0 \end{pmatrix},$$

then $W_i + W_j$ is a subspace of type $(4,2)$.

Lemma 4.4 *If W_i and W_j are subspaces of type $(2,0)$ and $(2,1)$, respectively, then $W_i + W_j$ is a subspace of type $(3,1)$ or $(4,1)$.*

Proof. Similar to Lemma 4.3, we can prove that $W_i + W_j$ is a subspace of type $(3,1)$ or $(4,1)$.

1. If

$$W_i = \begin{pmatrix} \overbrace{1\ 0\ 0\ \cdots\ 0}^{\nu} & \overbrace{0\ \cdots\ 0}^{\nu} \\ 0\ 1\ 0\ \cdots\ 0 & 0\ \cdots\ 0 \end{pmatrix},$$

$$W_j = \begin{pmatrix} \overbrace{1\ 0\ \cdots\ 0}^{\nu} & \overbrace{0\ 0\ \cdots\ 0}^{\nu} \\ 0\ 0\ \cdots\ 0 & 1\ 0\ \cdots\ 0 \end{pmatrix},$$

then $W_i + W_j$ is a subspace of type $(3,1)$.

2. If

$$W_i = \begin{pmatrix} \overbrace{1\ 0\ 0\ \cdots\ 0}^{\nu} & \overbrace{0\ \cdots\ 0}^{\nu} \\ 0\ 1\ 0\ \cdots\ 0 & 0\ \cdots\ 0 \end{pmatrix},$$

$$W_j = \begin{pmatrix} \overbrace{0\ 0\ 1\ \cdots\ 0}^{\nu} & \overbrace{0\ 0\ 0\ \cdots\ 0}^{\nu} \\ 0\ 0\ 0\ \cdots\ 0 & 0\ 0\ 1\ \cdots\ 0 \end{pmatrix},$$

then $W_i + W_j$ is a subspace of type $(4,1)$.

Lemma 4.5 *If both W_i and W_j are subspaces of type $(2,1)$, $i \neq j$, then $W_i + W_j$ is a subspace of type $(3,1)$ or $(4,2)$.*

Proof. Similar to Lemma 4.3, we can prove that $W_i + W_j$ is a subspace of type $(3,1)$ or $(4,2)$.

1. If

$$W_i = \begin{pmatrix} 1 & \overbrace{0 & \cdots & 0}^{\nu} & \overbrace{0 & 0 & \cdots & 0}^{\nu} \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix},$$

$$W_j = \begin{pmatrix} 1 & \overbrace{1 & \cdots & 0}^{\nu} & \overbrace{0 & 0 & \cdots & 0}^{\nu} \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix},$$

then $W_i + W_j$ is a subspace of type $(3,1)$.

2. If

$$W_i = \begin{pmatrix} 1 & \overbrace{0 & \cdots & 0}^{\nu} & \overbrace{0 & 0 & \cdots & 0}^{\nu} \\ 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix},$$

$$W_j = \begin{pmatrix} 0 & \overbrace{1 & \cdots & 0}^{\nu} & \overbrace{0 & 0 & \cdots & 0}^{\nu} \\ 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \end{pmatrix},$$

then $W_i + W_j$ is a subspace of type $(4,2)$.

From Lemmas 4.3, 4.4 and 4.5 it follows that:

Theorem 4.2 *The number of keys in common between any two nodes P_i and P_j are listed as follows in the Table 1:*

W_i	W_j	$W_i + W_j$	$\lambda_{i,j} = \lvert(P_i) \cap (P_j)\rvert$	s and ν
		(3, 0)	$N(2s, s; 2\nu - 3, \nu - 3; 2\nu)$	$s \leq \nu - 3$
		(3, 1)	$N(2s, s; 2\nu - 3, \nu - 2; 2\nu)$	$s \leq \nu - 2$
(2, 0)	(2, 0)	(4, 0)	$N(2s, s; 2\nu - 4, \nu - 4; 2\nu)$	$s \leq \nu - 4$
		(4, 1)	$N(2s, s; 2\nu - 4, \nu - 3; 2\nu)$	$s \leq \nu - 3$
		(4, 2)	$N(2s, s; 2\nu - 4, \nu - 2; 2\nu)$	$s \leq \nu - 2$
(2, 0)	(2, 1)	(3, 1)	$N(2s, s; 2\nu - 3, \nu - 2; 2\nu)$	$s \leq \nu - 2$
		(4, 1)	$N(2s, s; 2\nu - 4, \nu - 3; 2\nu)$	$s \leq \nu - 3$
(2, 1)	(2, 1)	(3, 1)	$N(2s, s; 2\nu - 3, \nu - 2; 2\nu)$	$s \leq \nu - 2$
		(4, 2)	$N(2s, s; 2\nu - 4, \nu - 2; 2\nu)$	$s \leq \nu - 2$

Table 1: The number of shared keys in nodes P_i and P_j

Theorem 4.3 *If m nodes are compromised, and $m < q^{2s}$, then no nodes will be disconnected.*

Proof. Let $P_1, P_2, \cdots, P_m$ be the m nodes which are compromised, then the keys in the m nodes becomes fully ineffective which can't be used by other nodes. Let P_t be an uncompromised node.

From table 1, there are at most λ keys in common between two nodes P_i and P_j $(i, j = 1, 2, \cdots, m, i \neq j)$, where

$$\lambda = N(2s, s; 2\nu - 3, \nu - 2; 2\nu) = \frac{\prod_{i=\nu-s-1}^{\nu-2}(q^{2i} - 1)}{\prod_{i=1}^{s}(q^{2i} - 1)} q^{2s(\nu-s-1)}.$$

In addition, by Theorem 4.1, there are at lest μ keys in the node P_t, where

$$\mu = N(2s, s; 2\nu - 2, \nu - 2; 2\nu) = \frac{\prod_{i=\nu-s-1}^{\nu-2}(q^{2i} - 1)}{\prod_{i=1}^{s}(q^{2i} - 1)} q^{2s(\nu-s)}.$$

Since $m < q^{2s}$, $m\lambda < \mu$. Hence the network will be security.

We now demonstrate this Theorem with the following example.

Example 4.1 *We compare our scheme with Samiran-Sushmita's scheme, as exhibited in the following table 2.*

Our scheme				Samiran-Sushmita's scheme[13]		
n	q	s	$m < q^{2s}$	n	q	$m < \frac{q+1}{4}$
683	4	1	$m < 16$	870	59	$m < 15$
1640	3	2	$m < 81$	1980	89	$m < 22$
10923	4	2	$m < 256$	13572	233	$m < 59$

Table 2: compare our scheme with Samiran-Sushmita's scheme

Analyzing the data in the table 2, it is clear to see that our scheme has more compromise nodes with closing numbers of nodes under the situation of network security, so it has a better connectivity.

4.2 Connectivity

Two nodes within communication range can exchange information securely, if they have a common key. In most probabilistic schemes, this is not

possible, since key chains are chosen randomly. In our scheme, any two nodes share at least one key, which has full connectivity and reduces delays occurring in multihop communications.

We compare the connectivity with several other existing ones, as exhibited in the following table 3.

Schemes	E-G[5]	C-Y[8]	L-D[12]	C-M-R[16]	PBIBD[6]	Samiran[13]	Our
Connectivity	No	Yes	No	No	Yes	Yes	Yes

Table 3: Comparison of the connectivity for different schemes

4.3 Security

If a node is captured by the enemy, then the information stored in the node is no longer safe. Once the node P_i is captured which stores the shared keys between node P_i and P_j, the connection between P_i and P_j will be destroyed. Define the loss probability:

$$fail(1) = \frac{\text{the number of nodes disconnected}}{\text{the total number of nodes}}.$$

This paper studies the security of the wireless sensor networks by measuring the proportion of nodes disconnected, when m nodes are compromised, and it is defined as follows.

$$fail(m) = 1 - (1 - fail(1))^m.$$

We compare the proportion of nodes disconnected with several other existing ones, as exhibited in the following table 4.

Schemes	Lee-Stinson[12]		Samiran-Sushmita[13]		Our scheme			
n	1187	1187	1980	1980	1640	1640	10923	10923
m	15	20	15	20	15	20	20	40
fail(m)	0.1732	0.2874	0.1081	0.1837	0.1281	0.1788	0.0354	0.1378

Table 4: The proportion of nodes disconnected in different schemes

Clearly, our scheme works best when it is a large network with ten thousands of nodes. In addition, the sensor nodes are consist of a 2-dimensional subspace in a symplectic space, this structure increases the security of the network. In most of the existing schemes, the global connectivity of WSN are only about 0.6, but in this paper, the global and local connectivity are 1, so it can ensure high network security connectivity when reducing the number of shared key between adjacent nodes appropriately.

5 Conclusion

Wireless sensor networks are increasingly widespread, their security problems draw more and more people's attention, where the key pre-distribution is the most important safety problem in wireless sensor networks. Because wireless sensor nodes have resource constraints, traditional key distribution method is unsuitable for wireless sensor networks. In the current scenario, the existence of a shared key and the key path length can not be guaranteed in some random pre-distribution schemes based on probabilities, it is difficult to support large-scale networks.

In this paper, the characteristic and the research actuality of wireless sensor networks are described, and the existing random-based key pre-distribution schemes, such as Eschenauer-Gligor scheme and Chan-Perrig-Song scheme are discussed. We present the deterministic pre-distribution scheme based on symplectic spaces which ensure the establishment of keys between neighboring nodes to have higher probability, and solve the security problems in the original schemes.

References

[1] A. Perrig, J. Stankovic, D Wagner. Security in sensor networks, Communications of the ACM, **6**(2004): 53-57.

[2] L. M. Sun. Wireless Sensor Networks, Tsinghua University Press, 2005.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam. A survey on sensor networks, IEEE Communications, **8**(2002): 102-114.

[4] H. Chan, A. Perrig. Security and privacy in sensor networks, IEEE Computer, **10**(2003): 103-105.

[5] L. Eschenauer, V. Gligor. A key management scheme for distributed sensor networks, Proceedings of 9th ACM Conference on Computer and Communication Security, (2002): 41-47.

[6] S. Ruj, B. Roy. Key pre-distribution using partially balanced designs in wireless sensor networks, Proceedings of ISPA, Niagara Falls, Canada, (2007): 431-445.

[7] H.Chan, A.Perrig, D.X.Song. Random key pre-distribution schemes for sensor networks, In: Proc of 2003 IEEE Symp on Research in Security and Privacy. New York : ACM Press, (2003): 197-213.

[8] S. A. Camtepe, B. Yener. Combinatorial design of key distribution mechanisms for wireless sensor networks, In: Proc of the 9th European Symp on Research in Computer Security. Berlin: Springer, (2004): 293-308.

[9] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-secure key distribution for dynamic conferences, Lecture Notes in Computer Science, (1993): 471-486.

[10] R. Blom. An optimal class of symmetric key generation systems. Advances in Cryptology: Proceedings of EUROCRYPT 84 (Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, eds.), Lecture Notes in Computer Science, Springer-Verlag, (1985): 335-338.

[11] D. Liu, P. Ning. Establishing pair-wise keys in distributed sensor networks, In: Proc of the 10th ACM Conf on Computer and Communications Security. New York: ACM Press, (2003): 52-61.

[12] J. Lee, D. R. Stinson. Deterministic key pre-distribution schemes for distributed sensor networks, In: Proc of the 11th Int Workshop on Selected Areas in Cryptography. Berlin: Springer, (2004): 1-14.

[13] S. Bag, S. Ruj. Key Distribution in wireless sensor networks using finite affine plane, IEEE computer society, (2011): 436-441.

[14] G. M. Xia, Z. G. Huang, Z. Y. Wang. A key pre-distribution scheme for wireless sensor networks based on the symmetric balanced incomplete block design, Computer Research and Development, **1**(2008): 154-164.

[15] Z. X. Wan. Geometry of Classical Groups over Finite Field, Lund: Student literature, 1993.

[16] D. Chakrabarti, S. Maitra, B. Roy. A key pre-distribution scheme for wireless sensor networks: Merging blocks in combinatorial design, Lecture Notes in Computer Science, **11**(2005): 89-103.

[17] A. C. Chan. A graph theoretic approach for optimizing key pre-distribution in wireless sensor networks, National University of Singapore, **11**(2013): 1-16.

[18] S. Khalid, F. Ahmad, M. R. Beg. Secure key pre-distribution in wireless sensor networks using combinatorial design and traversal design based key distribution, Department of Computer Science and Engineering, Integral University, **11**(2005): 100-106.