Key pre-distribution using combinatorial designs for wireless sensor networks

Wangke YU, Shuhua WANG
Shaoxing University
School of Mathematics and Information
Shaoxing, Zhejiang, 312000
P. R. China
Corresponding author:ywkyyy@163.com

Abstract: The main requirement in wireless sensor networks is not only the security but also the energy efficient security due to limited resources. In large scale deployment scenarios, there is no priory knowledge of post deployment network configuration since nodes may be randomly scattered over a hostile territory. Thus, shared keys must be distributed before deployment to provide each node some keys. For large sensor networks it is infeasible to store a unique key for all other nodes in the keys of a sensor node. Consequently, for secure communication either two nodes have a key in common in their keys and they have a wireless link between them, or there is a path, among these two nodes where each pair of neighboring nodes on this path have a key in common. We review and examine the appropriateness of combinatorial designs as a tool for building key pre-distribution schemes suitable for such environments. A scalable key pre-distribution scheme based on combinatorial designs is presented. Performance and simulation results show that the combinatorial approach produces better connectivity with smaller key sizes. An important advantage of our schemes is that we can increase the scalability of the network.

Key–Words: key pre-distribution scheme, wireless sensor networks, combinatorial designs, orthogonal arrays, rational normal curves, security

1 Introduction

Security in Wireless Sensor Networks (WSN) is important for the applications where the confidentiality and integrity of the sensed data is critical. Secure data transfer among wireless sensor nodes can be achieved by securing each of the links used in the communication path via a secret key to be used for the message encryption. Establishing shared keys among sensor nodes after the deployment is one of the main research areas in the literature. Due to the limited computational and power resources of the wireless sensor network, proposed key establishment protocols [1] are mostly based on key pre-distribution which has a low cost of computation. Besides, there are recent studies [2] evaluating the public key establishment in wireless sensor network even though the computational cost is relatively higher. However, these key establishment protocols have been evaluated independently from the underlying network structure and the main purpose is to establish shared keys among all sensor pairs for the possibility of communicating after the deployment. If the network configuration requirements are also considered, assumptions added to the analysis of these protocols may not be applicable or their costs may not be acceptable for some wireless sensor network applications. For example, high network density assumptions made for the key pre-distribution protocols may not be practical due to the wireless medium efficiency. Besides, high network density requirement increases the total system cost per square area and it may not be acceptable for some large scale wireless sensor network applications targeting large area coverage.

When sensor networks are used in a hostile setting, confidentiality and authenticity of communication among the sensor nodes should be provided. While fulfilling these security requirements, fast and energy efficient methods should be used. Although there are some recent works to make public key cryptography practical to be used sensor nodes, symmetric cryptography and hash-based solutions are still more efficient for providing security in sensor networks [3]. These solutions necessitate pair-wise keys distributions among the sensor nodes prior to beginning of secure communication. The problem of distribution of keys to large number of sensor nodes is an active research field. Key pre-distribution schemes [4] are shown to provide practical and efficient solutions. In such schemes, redundant amount of keys are stored in nodes memory before deployment and a matching algorithm is processed between neighboring node pairs after the deployment. As a result of this match, some of the stored keys are used in secure communication of neighbors. If two neighboring nodes share a key, then a secure link exists between those nodes. Due to probabilistic nature of the scheme, some neighboring nodes may not share a key [5].

Combinatorial structures are natural objects on which to model many aspects of symmetric key management. For a survey of their contributions to key establishment, see [6]. In order to construct deterministic key pre-distribution schemes for wireless sensor network, using orthogonal arrays is another strategy in this area. In this paper, we shall construct a class of key pre-distribution schemes by means of a special type of orthogonal arrays.

Symmetric key establishment almost always involves a trusted third party, which we will term a key management authority, at some stage in the process. In some environments this key management authority is online. In such cases the third party is often referred to as a key distribution center, But There is no trusted infrastructure in our scheme.

2 Wireless Sensor Networks

A wireless sensor network is an ad hoc network formed from a collection of low-powered sensor nodes which gather data and use wireless communication to transmit the information they collect. Wireless sensor networks represent an emerging computing platform that blends sensing, computation, and communication to provide a new tool in interfacing with physical environments. Wireless sensor networks consist of a large number of tiny and inexpensive computer platforms that are deeply embedded in their environments. These platforms are capable of sensing the environment, processing information onboard, and communicating with each other and with a network server through multi-hop wireless links. They must reliably operate unattended for extended periods of time, under stringent resource constraints in energy, communication bandwidth, memory capacity, and processing power. The number of nodes can vary between dozens to thousands, depending upon the applications [7]. Wireless sensor network is best suited to applications where some form of environmental monitoring is required, but where the scale and hostility of the environment does not lend itself to the deployment of a few expensive monitoring devices. Examples include seismic data gathering, remote habitat monitoring, gathering of ecological data, forestry welfare, agriculture, disaster relief operations and military intelligence gathering. The typical characteristics of a wireless sensor network are [8-11]:

(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 wireless sensor network do not feature any central control node. Thus all network functionality must be achieved through cooperation between the nodes.

(3) Requirement to form a network to a sink: In most wireless sensor network 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 be connected to the wireless sensor network and request data. The location of this sink in the network is typically not fixed.

(4) Hop-based communication: Most wireless sensor network 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, which then passes it onto a node within its range, etc.

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

(6) Nodes vulnerable to compromise: The constrained natures 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 stored on them is likely to be exposed.

We will make three restrictions on the type of wireless sensor network of being considered in this paper:

- Homogeneous nodes: We will assume that all nodes have the same capabilities and constraints.

- Communication structure: We will assume that the main aim of any communication in the wireless sensor network is to send data from a node to the sink. We will thus not attempt to set up fully connected sub-networks or establish group keys.
- No mobility: We will assume that nodes are not mobile after deployment. In fact, many of the solutions discussed here are also appropriate for mobile nodes.

An important issue that affects key predistribution scheme design is that wireless sensor network vary in the extent to which the location of nodes is known prior to deployment. We will thus classify wireless sensor network as following [11-13]:

1) Uncontrolled if the location of sensors cannot be predicted before deployment. This is the default wireless sensor network scenario and assumes that the application environment is in such a hostile that nodes cannot be positioned in any controlled way. For example, they may be released from the air over a disaster site.

2) Partially controlled if some information about the location of sensors is known before deployment. This might be the case when sensors are strategically released from the air in batches.

3) Fully controlled if the precise location of sensors is known before deployment. This is likely to be the case, for example, when sensors are deployed in a grid in a vineyard to monitor ground humidity.

We will generally assume that a wireless sensor network is uncontrolled [14], however we will discuss key pre-distribution scheme for other types of wireless sensor network. There has been some debate about the practicality of using public key cryptography to implement security services in a wireless sensor network [15]. While this may indeed become more practical, the case for designing solutions that only use symmetric cryptography remains strong. Symmetric cryptography is still preferred in many modern applications which are not as resource constrained as wireless sensor network because of the efficiency gains and the unique problems posed by management of public keys. Perhaps more compellingly, it is likely that as soon as public key cryptography is practical on a given sensor node technology, even more constrained sensor technology will be being developed where it is not. In this paper we assume that a fully symmetric solution is required.

3 Combinatorial Designs

In this section, we discuss the orthogonal array and rational normal curves [6, 16-23].

3.1 Orthogonal Arrays

Definition 1 *Let $k \geq 2$ and $n \geq 1$ be integers. An orthogonal array $\mathrm{OA}(k, n)$ is an $n^2 \times k$ array, A, with entries from a set X of cardinality n such that, within any two columns of A, every ordered pair of symbols from X occurs in exactly one row of A.*

Note that an $\mathrm{OA}(2, n)$ exists trivially for all integers $n \geq 1$ .We give a more general definition now.

Definition 2 *Let t, v, k, and λ be positive integers such that $k \geq t \geq 2$. A $t-(v, k, \lambda)$ orthogonal array is a pair (X, D) such that the following properties are satisfied.*

- *X* is a set of v elements called points.
- *D* is a λv^t by *k* array whose entries are chosen from the set *X*.
- Within any *t* columns of *D*, every *t*-tuple of points is contained in exactly λ rows.

An orthogonal array (X, D) is a simple orthogonal array if all the rows in *D* are different. An orthogonal array (X, D) is a linear orthogonal array if $X = \mathbb{F}_q$ for some prime power *q* and the rows of *D* form a subspace having dimension $\log_q |D|$. It is clear from the definitions that a linear orthogonal array is necessarily simple.

Theorem 3 *Let l and n be positive integers, and let q be a prime power. Let M be an $l \times n$ matrix of elements from $\mathbb{F}_q$ such that every set of t columns of M is linearly independent. Define D to be the $q^l \times n$ matrix whose rows consist of all the linear combinations of the rows of M. Then $(\mathbb{F}_q, D)$ is a linear $t-(q, n, \lambda) - \mathrm{OA}$, where $\lambda = q^{l-t}$.*

Proof: Choose *t* columns of *D*, say the ones labeled $c_1, \ldots, c_t$. Let $y_1, \ldots, y_t$ be an arbitrary *t*-tuple of elements of $\mathbb{F}_q$. We want to determine the rows *i* of *D* such that $D(i, c_j) = y_j$ for $1 \leq j \leq t$.

A row of *D* is constructed as RM, where $R = (r_1, \cdots, r_l) \in (\mathbb{F}_q)^l$. Let c_j denote the *j*th column of M for $1 \leq j \leq n$. We want to determine all vectors R such that:

$$Rc_{i_j} = y_{i_j}, \quad 1 \leqslant j \leqslant t$$

The column vectors $c_{i_1}, \ldots, c_{i_t}$ are linearly independent by assumption. Therefore, $Rc_{i_j} = y_{i_j}$ is a system of t independent linear equations in l unknowns, and it has a solution space of dimension $l-t$. The number of solutions R is q^{l-t}, as desired. □

We present an important corollary of Theorem 3.

Corollary 4 *Let $l \geq 2$ be a positive integer, and let q be a prime power. Then there exists a*

$$2-(q,(q^l-1)/(q-1),q^{l-2})-\mathrm{OA}.$$

Proof: Excluding the zero vector, there are $q^l - 1$ distinct l-tuples of elements of $\mathbb{F}_q$. Each l-tuple has $q-1$ nonzero scalar multiples, so the $q^l - 1$ nonzero vectors are partitioned into $q^l - 1/(q-1)$ subspaces each of dimension equal to one. Arbitrarily pick one vector from each subspace, and let these vectors be the columns of *M*. The results then can be obtained by Theorem 3. □

Theorem 5 *Let q be an odd prime power. For $a, b \in \mathbb{F}_q$, define $f_{a,b} : \mathbb{F}_q \to \mathbb{F}_q$ by the rule*

$$f_{a,b}(x) = (x+a)^2 + b.$$

Then, the $q^2 \times q$ array $D = (d_{i,j})$, where $(d_{i,j}) = f_{a,b}(j)(i = (a,b) \in (\mathbb{F}_q)^2, j \in \mathbb{F}_q)$, is a $2-(q,q,1)-$ OA.

Proof: Let $(x_1, x_2) \in \mathbb{F}_q$ and $(y_1, y_2) \in \mathbb{F}_q$. We need to show that there is exactly one ordered pair $(a, b) \in (\mathbb{F}_q)^2$ such that

$$(x_1 + a)^2 + b = y_1$$

and

$$(x_2 + a)^2 + b = y_2.$$

Subtracting the two equations, we can obtain uniquely by

$$a = \frac{y_1 - y_2}{2(x_1 - x_2)} - \frac{x_1 + x_2}{2}.$$

The unique b can be thus obtained. □

Example 1: Suppose we take $q = 5$ and $l = 2$ in Corollary 4. Each pair of columns of the following 12 matrix is linearly independent over $\mathbb{Z}_5$:

$$\begin{pmatrix} 0\,1\,1\,1\,1\,1 \\ 1\,0\,1\,2\,3\,4 \end{pmatrix}.$$

By theorem 3, we obtain the following $2-(5,6,1)-$ OA:

$$\begin{pmatrix}
0\,0\,0\,0\,0\,0 \\
0\,1\,1\,1\,1\,1 \\
0\,2\,2\,2\,2\,2 \\
0\,3\,3\,3\,3\,3 \\
0\,4\,4\,4\,4\,4 \\
1\,0\,1\,2\,3\,4 \\
2\,1\,2\,3\,4\,0 \\
3\,2\,3\,4\,0\,1 \\
4\,3\,4\,0\,1\,2 \\
0\,4\,0\,1\,2\,3 \\
2\,0\,2\,4\,1\,3 \\
3\,1\,3\,0\,2\,4 \\
4\,2\,4\,1\,3\,0 \\
0\,3\,0\,2\,4\,1 \\
1\,4\,1\,3\,0\,2 \\
\vdots\,\vdots \\
4\,0\,4\,3\,2\,1 \\
0\,1\,0\,4\,3\,2 \\
1\,2\,1\,0\,4\,3 \\
2\,3\,2\,1\,0\,4 \\
3\,4\,3\,2\,1\,0
\end{pmatrix}.$$

□

Example 2: Following $2-(3,3,1)-$ OA is constructed by Theorem 5:

$$\begin{array}{rcc}
 & & 0\;1\;2 \\ \hline
f0,0 & : & 0\;1\;1 \\
f0,1 & : & 1\;2\;2 \\
f0,2 & : & 2\;0\;0 \\
f1,0 & : & 1\;1\;0 \\
f1,1 & : & 2\;2\;1 \\
f1,2 & : & 0\;0\;2 \\
f2,0 & : & 1\;0\;1 \\
f2,1 & : & 2\;1\;2 \\
f2,2 & : & 0\;2\;0
\end{array}.$$

This orthogonal array is not linear. This can be seen, for example, by observing that the sum of the first two rows is $(1, 0, 0)$, which is not a row of the array. □

$\mathrm{OA}(t, k, v)$ is an orthogonal array (OA) of index 1, order v, degree k and strength t, and an orthogonal array of index λ, denoted by $\mathrm{OA}_\lambda(t,k,v)$, is a $\lambda v^t \times k$ array with entries from a set of v symbols, in which all possible combinations of t symbols appear exactly λ times as rows in every $\lambda v^t \times k$ array. Here we mainly concern with the existence of an $\mathrm{OA}_\lambda(t,k,v)$ with a nested $\mathrm{OA}_u(t,k,w)$. We refer to such a nested OA as an $\mathrm{OA}_{(\lambda,u)}(t,k,(v,w))$. It is easy to see that in an $\mathrm{OA}_{(\lambda,u)}(t,k,(v,w))$ the index u of the sub-array cannot exceed the index λ of the larger array. Whenever $\lambda = u$ we simply write it as $\mathrm{OA}_\lambda(t,k,(v,w))$. In particular, if $\lambda = u = 1$, then the notation $\mathrm{OA}(t,k,(v,w))$ is employed.

So far, We now introduce asymmetric nested orthogonal arrays.

Definition 6 *An asymmetric nested orthogonal array:*

$$\mathrm{NOA}((N,M),k,(s_1 \times s_2 \cdots \times s_k, r_1 \times r_2 \cdots \times r_k),g),$$

where $r_i \le s_i$, with strict inequality for at least one i, $1 \le i \le k$, and $M < N$,is an asymmetric orthogonal array, $\mathrm{OA}(N,k,s_1 \times s_2 \times \cdots \times s_k, g)$ which contains an $\mathrm{OA}(M,k,r_1 \times r_2 \times \cdots \times r_k, g)$ is a sub-array.

For example, consider the following array. Note that the definition 6 does not preclude the possibility of existence of an asymmetric nested orthogonal array where in the smaller orthogonal array is a symmetric orthogonal array, nested within a larger asymmetric orthogonal array. The array displayed in transposed form:

$$\begin{bmatrix} 0&0&0&0\\ 0&0&1&1\\ 1&0&0&1\\ 0&1&0&1\\ 1&1&0&0\\ 1&0&1&0\\ 0&1&1&0\\ 1&1&1&1\\ 2&0&0&0\\ 2&1&0&1\\ 2&0&1&1\\ 2&1&1&0\\ 3&0&0&1\\ 3&1&0&0\\ 3&0&1&0\\ 3&1&1&1 \end{bmatrix}.$$

The first 8 rows of this array form a orthogonal array $\mathrm{OA}(8,4,2,3)$ while all the 16 rows represent an asymmetric orthogonal array $\mathrm{OA}(16,4,32,3)$. We continue to call such arrays the asymmetric nested orthogonal arrays. We now describe some methods of constructing of asymmetric nested orthogonal arrays.

Theorem 7 *The existence of an $\mathrm{OA}(N,k,2,2u)$, where $u \ge 1$ is an integer, implies the existence of an*

$$\mathrm{NOA}((tN,2mN),k{+}1,(t^1{\times}2^k,(2m)^1{\times}2^k),2u{+}1),$$

where $t \ge 2$ is an even integer and $1 \le m \le t$ is an integer.

Example 3: Considering A to be an $\mathrm{OA}(4,3,2,2)$, taking $t = 6$, $m = 2$ and following the above method of construction, one obtains an $\mathrm{OA}((24,16),4,(48,32),3)$ which is displayed below in transposed form:

$$\begin{bmatrix} 0000 & 0011 & 0101 & 0110\\ 1111 & 1100 & 1010 & 1001\\ 2222 & 0011 & 0101 & 0110\\ 3333 & 1100 & 1010 & 1001\\ 4444 & 0011 & 0101 & 0110\\ 5555 & 1100 & 1010 & 1001 \end{bmatrix}.$$

The first 16 rows of the above array form an asymmetric $\mathrm{OA}(16,4,32,3)$ and the full array is an $\mathrm{OA}(24,4,48,3)$. Next, consider an asymmetric orthogonal array $A = \mathrm{OA}(N,k,s_1 \times s_2 \times \cdots \times s_k, g)$, where $g \ge 2$. Write A as

$$A = \begin{bmatrix} a_1^{'} & A_1^{'}\\ a_2^{'} & A_2^{'}\\ \vdots & \vdots\\ a_{s_1}^{'} & A_{s_1}^{'} \end{bmatrix},$$

where, for $1 \le i \le s_1$, a_i is an N/s_1 vector with each element equal to i. Clearly, each $A_i (1 \le i \le s_1)$ is an $A = \mathrm{OA}(N/s_1, k-1, s_2 \times \cdots \times s_k, g-1)$. Define $u = N/s_1, v = t/s_1, v = t/s_1, b = (0,1,\ldots,t-1)'$ and $A^* = [A_1^{'} : A_2^{'} : \cdots : A_{s_1}^{'}]'$. Consider the matrix B given by $B = [b \otimes 1_u \vdots 1_v \otimes A^*]$, where $\otimes$ stands for the product of matrices. Then, one can easily see that B is an asymmetric nested array $A = \mathrm{OA}((N/S_1,N),k,(t \times s_2 \times \cdots \times s_k, s_1 \times s_2 \times \cdots \times s_k),g)$, where the first N rows of B form the smaller array, which is an $A = \mathrm{OA}(N,k,s_1 \times s_2 \times \cdots \times s_k, g)$. $\square$

3.2 Rational Normal Curves

Definition 8 *If a curve C in $PG(n, \mathbb{F}_q)$ to be the image of the map,*

$$PG(1, \mathbb{F}_q) \to PG(n, \mathbb{F}_q),$$
$$(x_0, x_1) \mapsto (x_0^n, x_0^{n-1}x_1, \ldots, x_1^n).$$

The curve C consists of the following $q+1$ points:

$$((1, \alpha, \alpha^2, \ldots, \alpha^n)|\alpha \in \mathbb{F}_q) \cup (0, 0, 0, \ldots, 0, 1).$$

We call the image of the curve C under any projective transformation a rational normal curve. Now,we introduce some theorems [6, 23, 24].

Theorem 9 *Let $t \geq 5$ is an integer and $q \geq t-1$ is a prime power. The number of the rational normal curves in $PG(n, \mathbb{F}_q)$ is*

$$q^{n(n+1)/2-1} \prod_{i=3}^{n+1} (q^i - 1).$$

Theorem 10 *Let $t \geq 5$ is an integer and $q \geq t-1$ is a prime power. there exists a $t - (v, b, k, \lambda_r, 0)(3 \leqslant r \leqslant t-1)$ design as well where*

$$v = (q^{t-2} - 1)/(q-1),$$
$$k = q+1,$$
$$b = q^{(t-3)(t-2)/2-1} \prod_{i=3}^{t-2} (q^i - 1),$$
$$\lambda_1 = q^{(t-2)(t-3)/2-1} \prod_{i=2}^{t-3} (q^i - 1),$$
$$\lambda_2 = q^{(r+t-3)(t-r-2)/2} q^{r-2} \prod_{i=1}^{t-r-2} (q^i - 1) \prod_{i=1}^{r-2} (q - i),$$
$$2 \leqslant r \leqslant t-3,$$
$$\lambda_{t-2} = (q-1)^{t-4} \prod_{i=1}^{t-4} (q-i),$$
$$\lambda_{t-1} = \prod_{i=2}^{t-3} (q-i).$$

We study the intersection of any two the rational normal curves now. Let C be a fixed rational normal curves, C' be a rational normal curves, and the set $P \subset C$ with $r = |P|$. Define $\mu_C^{'}(P) = \#\{C^{'} \cap C = P\}$.

Hence the number $\mu_C^{'}(P)$ does not depend on the special curve C and the special set P, it depends only on the number $r = |P|$. We write $\mu_C^{'}(r)$ instead of $\mu_C^{'}(P)$.

Note that $\mu_C^{'}(t) = 0$. By the recursion formula

$$\mu_C^{'}(r) = \lambda_r - \sum_{m=1}^{t-r-1} \binom{k-r}{m} \mu_C^{'}(r+m) - 1,$$
$$1 \leqslant r \leqslant t-1.$$

Define $\mu_C(r)$ for $1 \leqslant r \leqslant t-1$ to be the number of rational normal curves which intersect with C at r points, and the number μ_C to be the number of rational normal curves which have nonempty intersection with C. Then we have

$$\mu_C(r) = \binom{k}{r} \mu_C^{'}(r)$$

and

$$\mu_C = \sum_{r=1}^{t-1} \mu_C(r) = \sum_{r=1}^{t-1} \binom{k}{r} \mu_C^{'}(r).$$

4 Key Pre-distribution Scheme

4.1 Network Model

In this paper, we assume that a large number of resource-limited sensor nodes are randomly scattered around an adversarial area.

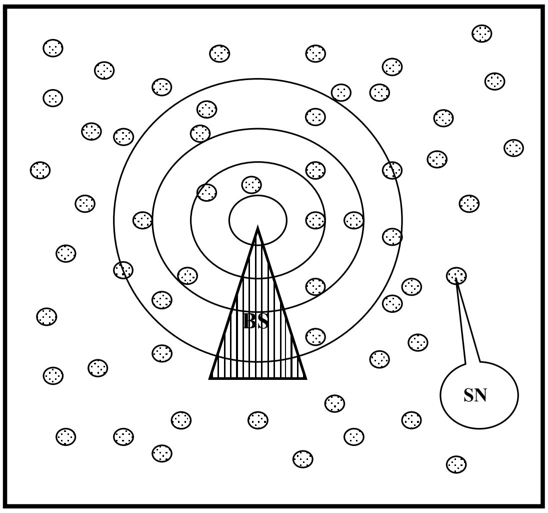

Figure 1: Network model

Examples of such networks can be military or environmental applications in which a large number of sensors are dropped from an airplane to an adversarial or hazardous environment.A realistic model of a wireless sensor network would consist of a large number of sensors and several base stations. Network model of our scheme is shown in Fig. 1. In Fig. 1, sensor nodes (SN) have identical processing, storage, battery life, and communication resources. Once deployed, each sensor node receives messages from another sensor node or base station (BS). The base station works as the system administrators and are responsible for generating keys for all nodes in the network. Two sensor nodes are neighbors if they are physically located within each others signal range. It may be possible for a sensor to have a long transmission. Sensor nodes communicate with each other to exchange application data.

A set system (I, B) consists of a set *I* of *v* elements and a collection *B* of blocks of *I*. The degree of $x \in I$ is the number of blocks of *B* containing *x* and (I, B) is regular if all points have the same degree. The rank *k* of (I, B) is the size of the largest block in *B* and we say that (I, B) is uniform if all blocks have the same size. The wireless sensor network chooses a key pre-distribution scheme defined on the *n* nodes $N = \{N_1, N_2, \dots, N_n\}$ in the network. Following, this key pre-distribution scheme can de modeled by a set system (I, B), where $I = \{x_i : 1 \leqslant i \leqslant v\}$ is a set of v key identifiers and $B = \{B_j : 1 \leqslant j \leqslant n\}$ is a set of *n* node allocations. For each key identifier x_i, the key management authority randomly selects a key K_i. The wireless sensor network then associates each node N_j in the network with a node allocation B_j and issues N_j with the key $L_j = \{K_i : x_i \in B_j\}$. Note that the association of N_j with B_j need not be a secret, however the instantiation of B_j by L_j must be.

4.2 Construct Design

We can construct a $5-(v, b, k, \lambda_1, \lambda_2, \lambda_3, \lambda_4, 0)$ design to a sensor network containing keys in a big keypool. There are b sensor nodes in each cluster, each node containing k keys.

Consider the case of $5-(v, b, k, \lambda_1, \lambda_2, \lambda_3, \lambda_4, 0)$ first, where

$$v = q^2 + q + 1,$$

$$k = q + 1,$$

$$b = q^5 - q^2,$$

$$\lambda_1 = q^4 - q^2,$$

$$\lambda_2 = q^3 - q^2,$$

$$\lambda_3 = q^2 - 2q + 1,$$

$$\lambda_4 = q - 2.$$

Hence,

$$\mu'_C(4) = q - 3,$$

$$\mu'_C(3) = 3q - 6,$$

$$\mu'_C(2) = \frac{1}{2}q^3 - q^2 + \frac{7}{2}q - 4,$$

$$\mu'_C(1) = \frac{1}{3}q^4 + \frac{1}{2}q^3 - \frac{11}{6}q^2 + 2q - 1.$$

It follows that

$$\mu_C(1) = \frac{1}{3}q^5 + \frac{5}{6}q^4 - \frac{3}{4}q^3 + \frac{1}{6}q^2 + q - 1,$$

$$\mu_C(2) = \frac{1}{4}q^5 - \frac{1}{4}q^4 + \frac{5}{4}q^3 - \frac{1}{4}q^2 - 2q,$$

$$\mu_C(3) = \frac{1}{2}q^4 - q^3 - \frac{1}{2}q^2 + q,$$

$$\mu_C(4) = \frac{1}{24}q^5 - \frac{5}{24}q^4 + \frac{5}{24}q^3 + \frac{5}{24}q^2 - \frac{1}{4}q,$$

$$\mu_C = \sum_{r=1}^{4} \mu_C(r) = \frac{5}{8}q^5 + \frac{7}{8}q^4 - \frac{7}{8}q^3 - \frac{3}{8}q^2 - \frac{1}{4}q - 1.$$

We can construct a nested orthogonal array

$$\text{NOA}((Nt/s_1, N), k, (t \times s_2 \cdots s_k, s_1 \times s_2 \cdots s_k), g)$$

from the

$$\text{OA}(N, k, s_1 \times s_2 \times \cdots \times s_k, g),$$

where $g \geq 2$, is available and suppose t is a positive integer such that $s_1 | t$, in Theorem 7.

4.3 Key Pre-distribution Scheme

The correspondences between the parameters of a combinatorial design $5-(v, b, k, \lambda_1, \lambda_2, \lambda_3, \lambda_4, 0)$ and the related key pre-distribution scheme for a wireless sensor network are summarized. We assume that the number of network nodes is N.

(1) **SA:** Select the appropriate prime q, let $N \leq b$:

- Size of the key pool: v.
- Number of keys per node: k.

(2) **SB:** Select the appropriate prime q, let $N > b$:

- Size of the key pool: $v + v_a$.
- Number of keys per node: $k + k_a$.

where v_a is the number of additional key for the key pool; k_a is the number of additional key for each sensor node.

Next, we construct a $\mathrm{NOA}((N, M), k, (s, r), g)$ design to a sensor network containing keys in a big key-pool. There are N sensor nodes, each node containing k keys. The correspondences between the parameters of a combinatorial design $\mathrm{NOA}((N, M), k, (s, r), g)$ and the related key predistribution scheme **(NOAS)** for a wireless sensor network are summarized.

- Network size: N.
- Size of the key pool: $\left\lceil \frac{M \times s}{r \times g} \right\rceil$.
- Number of keys per node: k.

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. If two nodes fail to identify common keys during shared key discovery, then they need to find a secure path between one another that employs intermediate nodes. Obviously, the shorter this secure path is the better.

4.4 Performance Evaluations

In order to evaluate the performance of our scheme, various simulations are performed. We used the well-known metrics such as local connectivity and the probability of links being affected.

1). Local Connectivity

Local connectivity can be referred as the probability of two neighboring nodes sharing at least one key space, in other words, having a direct secure link. Local connectivity can also be defined as the average number of secure neighbors of a node. Fig. 2 shows local connectivity values [23].

$$p = \frac{\mu_C}{b-1}$$

Hence, the probabilities of SA and SB in one hop are more than 0.6, and the probability of SA more than SB. Even for smaller number of keys per node, we achieve very good local connectivity.

In Fig. 3, the probabilities of SA and NOAS in one hop are more than 0.5, and the probability of SA more than NOAS. Even for smaller number of keys per node.

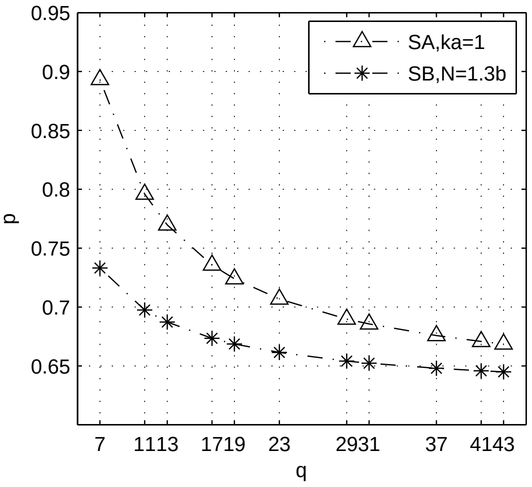

Figure 2: Local connectivity with SA and SB

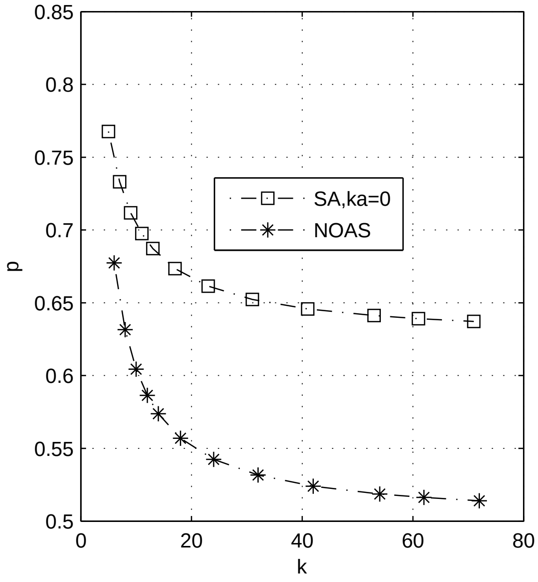

Figure 3: Local connectivity with SA and NOAS

2). Probability of Links Being Affected

The effectiveness of a wireless sensor network can be explained by the probability $fail(1)$. If a sensor node is detected as being compromised, then all the keys it possesses should no longer be used by any node in the sensor network. Suppose the sensor nodes N_i and N_j have at least one common keys. If all the common keys of the pair of N_i and N_j are contained in the compromised sensor node, then N_i and N_j are no longer communicate directly, i.e., the link between

N_i and N_j is lost. And the probability of links being affected is defined in [23]:

$$fail(1) = \frac{\sum_{r=1}^{t-1} \binom{k}{r} \lambda_r \mu_C^{'}(r)}{\sum_{r=1}^{t-1} \binom{k}{r} \mu_C^{'}(r)}.$$

In Fig. 4 we simulated $fail(1)$ values of our scheme. Fig. 4 shows that when being equipped with different number of q, the two schemes of this paper have different $fail(1)$, and all $fail(1)s$ are less than 0.12. Generally, we expect $fail(1)$ as small as possible, since it measures the resilience of the sensor network, when a random sensor node is compromised. So our schemes have high resiliency.

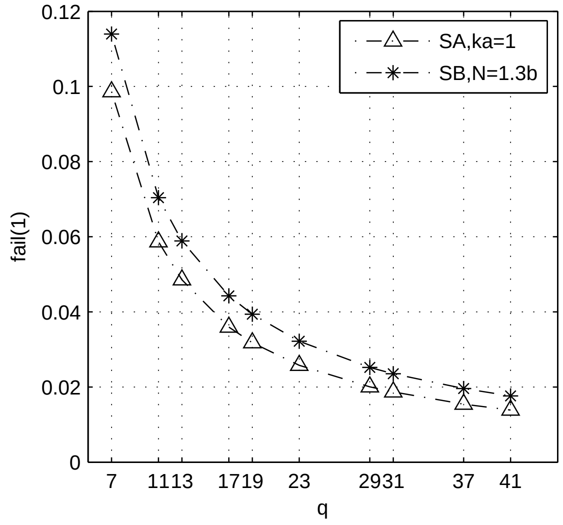

Figure 4: $Fail(1)$ values of our scheme

3). Computation Overhead

Since communication is the most energy-consuming activity, we will analyze and discuss it in more detail. While designing our scheme, we have tried to minimize the communication as much as possible. This also helps in reducing the computation overhead. Fig. 5 shows the number of nodes that can be supported using our scheme.

Note that the graph is drawn on logarithmic scale because the number of nodes that can be supported increases exponentially with respect to the number of keys used. Our scheme is inherently able to support a large number of nodes with a small number of keys using combinatorial designs.

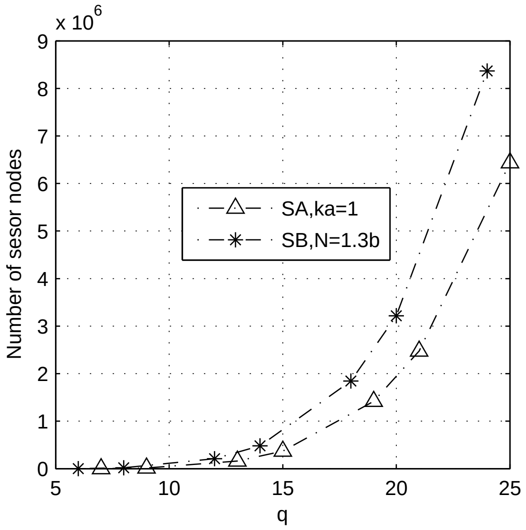

Figure 5: Number of nodes that can be supported

5 Conclusion

In the present paper, we present three random key pre-distribution schemes for sensor networks. In our schemes, we used some combinatorial designs approach, in which each node has its own distinct key spaces. Secure links between nodes are established through neighbor nodes or base station. Performance and simulation results show that these new schemes based on combinatorial designs produce high secure connectivity and substantially strong node capture resiliency while consuming minimal memory.

Acknowledgements: This work was supported by Zhejiang Provincial Natural Science Foundation of China (No. LQ12F02007).

References:

[1] Y. Xiao, V. K. Rayi, B. Sun, and M. Galloway, A survey of key management schemes in wireless sensor networks, *Computer Communications*, 30(11), 2007, pp.2314-2341.

[2] H. Y. Lin, D. J. Pan, X. X. Zhao et al, A rapid and efficient pre-deployment key scheme for secure data transmissions in sensor networks using lagrange interpolation polynomial, *International Journal of Security and its Applications*, 2(3), 2008, pp.49-55.

[3] K. M. Martin, M. B. Paterson, An application-oriented framework for wireless sensor network key establishment, *Electronic Notes in Theoretical Computer Science*, 192(2), 2008, pp.31-41.

[4] A. Unlu, A. Levi, Two-tier, location-aware and highly resilient key predistribution scheme for wireless sensor networks, *Proceedings of Visions of Computer Science-BCS International Academic Conference*, London, UK, 2008, pp.355-366.

[5] J. Lee and D. R. Stinson, On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs, *ACM Transactions on Information and Systems Security*, 11(2), 2008, pp.1-35.

[6] D. Y. Pei, Authentication codes and combinatorial designs, Chapman Hall/CRC, 2006.

[7] A. Boukerche, H. A. B. Oliveira , E. F. Nakamura et al, Secure localization algorithms for wireless sensor networks, *IEEE Commun. Mag.*, 46(4), 2008, pp.96-101.

[8] J. Albath, S. Madria, Secure Hierarchical Aggregation in Sensor Networks, *In Proceedings of IEEE Wireless Communications and Networking Conference*, 2009.

[9] O. Garcia-Morchon, H. Baldus, The ANGEL WSN Security Architecture, *2009 Third International Conference on Sensor Technologies and Applications*, pp.430-435.

[10] Y. W. Palaniswami, M. Hoesel, L. V.Doumen et al, Energy-Efficient link-layer jamming attacks against wireless sensor network mac protocols, *ACM Trans. Sensor Netw*, 5(1), 2009, pp.1-38.

[11] K. Ssu, W. Wang, W. Chang, Detecting Sybil attacks in Wireless Sensor Networks using neighboring information, *Comput. Netw.*, 53(7), 2009, pp. 3042-3056.

[12] P. S. Sausen, M. A. Spohn, A. Perkusich, Broadcast routing in wireless sensor networks with dynamic power management and multi-coverage backbones, *Information Sciences*, 180(5), 2010, pp.653-663.

[13] J. Yoo, L. Yan, S. Lee, et al, A 5.2mw self-configured wearable body sensor network controller and a 12w wirelessly powered sensor for a continuous health monitoring system, *IEEE Journal of Solid-State Circuits*, 45(1), 2010, pp.178-188.

[14] Y. D. Lee, W. Y. Chung, Wireless sensor network based wearable smart shirt for ubiquitous health and activity monitoring, *Sensors and Actuators B: Chemical*, 140(2), 2009, pp.390-395.

[15] R. Steele, A. Lo, C. Secombe et al, Elderly persons' perception and acceptance of using wireless sensor networks to assist healthcare, *International Journal of Medical Informatics*, 78(2), 2009, pp.788-801

[16] R. Mukerjee, P. Z. G. Qian, C. F. J. Wu, On the existence of nested orthogonal arrays, *Discrete Math*, 308, 2008, pp.4635C4642.

[17] T. Wu, J. Yan, R. Liu et al, Optimization of microwave-assisted extraction of phenolics from potato and its downstream waste using orthogonal array design, *Food Chemistry*, 133 (4), 2012, pp. 1292-1298.

[18] X. Wang, Y. Tang, Y. Zhang, Orthogonal arrays for estimating global sensitivity indices of non-parametric models based on ANOVA high-dimensional model representation, *Journal of Statistical Planning and Inference*, 142(7), 2012, pp. 1801-1810

[19] M. V. M. Nguyen, Some new constructions of strength 3 mixed orthogonal arrays, *Journal of Statistical Planning and Inference*, 138(1), 2008, pp. 220-233

[20] J. Yin, J. Wang, L. Ji et al, On the existence of orthogonal arrays OA(3,4,4n+2), *Journal of Combinatorial Theory, Series A*, 118(1), 2011, pp. 270-276

[21] L. Ji, J. Yin, Constructions of new orthogonal arrays and covering arrays of strength three, *Journal of Combinatorial Theory, Series A*, 117,(3), 2010, pp. 236-247

[22] K. Y. Chan, C. K. Kwong, H. Jiang et al, A new orthogonal array based crossover, with analysis of gene interactions, for evolutionary algorithms and its application to car door design, *Expert Systems with Applications*, 37(5), 2010, pp. 3853-3862

[23] D. Y. Pei, J. W. Dong, C. M. Rong, A novel key pre-distribution scheme for wireless distributed sensor networks, *Science China (Information Sciences)*, 53(2), 2010, pp. 288 - 298.

[24] D. Y. Pei, A problem of combinatorial designs related to authentication codes, *Journal of Combinatorial Designs*, 6, 1998, pp. 417-429