Applications and Applied Mathematics: An International Journal (AAM)

Volume 14 | Issue 1 Article 11

6-2019

New Approach of Deterministic Key Pre-distribution Scheme Using Triangle Free Quasi Symmetric Designs

Debashis Ghosh
C. V. Raman College of Engineering

Joydeb Pal
National Institute of Technology, Durgapur

Recommended Citation

Ghosh, Debashis and Pal, Joydeb (2019). New Approach of Deterministic Key Pre-distribution Scheme Using Triangle Free Quasi Symmetric Designs, Applications and Applied Mathematics: An International Journal (AAM), Vol. 14, Iss. 1, Article 11.
Available at: https://digitalcommons.pvamu.edu/aam/vol14/iss1/11

Available at
http://pvamu.edu/aam
Appl. Appl. Math.
ISSN: 1932-9466

Vol. 14, Issue 1 (June 2019), pp. 188 - 198

Applications and Applied Mathematics:
An International Journal
(AAM)

New Approach of Deterministic Key Pre-distribution Scheme Using Triangle Free Quasi Symmetric Designs

[1]Debashis Ghosh and [2]Joydeb Pal

[1]Department of Mathematics
C. V. Raman College of Engineering
Bhubaneswar, Orissa – 752054, India
ghoshdebashis10@gmail.com

[2] Research Scholars
Department of Mathematics
National Institute of Technology
Durgapur, West Bengal, India
joydebpal77@gmail.com

Received: September 12, 2018; Accepted: March 29, 2019

Abstract

A wireless sensor network (WSN) consists of tiny autonomous sensor nodes with some constraints. There are organizations having moderately necessitates of these kind of networks. So, security become an indispensable concern in WSN, due to potential adversaries. To overcome the security problem, keys are pre-loaded to the nodes before deployment. Among all key distribution schemes, deterministic key pre-distribution scheme (KPS) using combinatorial design is efficient regarding security aspect. In this paper, a deterministic approach, based on combinatorial design, for key assignment before the network deployment has been presented. Here the quasi-symmetric design which is of triangle-free is being used to present the new KPS for sensor networks. Due to this approach each sensor node either will contain a key-chain or will communicate through a key-path. This will improve the resiliency and achieve the sufficient level of security in the network. This design can also be used when a large number of nodes are being deployed in WSN.

Keywords: Triangle-free Quasi-symmetric designs; Sensor network; Key pre – distribution scheme; Resiliency

MSC 2010 No.: 05B05, 94C30

1. Introduction

Recent advances in wireless communications for civilian as well as military operations, have paved the way for the proliferation of WSN. The distributed adhoc sensor networks which are collection of inexpensive sensor devices having low battery power, low computational speed, low storage capacity and others limited resources. Because of these constraints and wide area of sensitive applications, security becomes a challenging issue for sensor networks see Zhou et al. (2008). As a consequence, it is infeasible to use traditional pairwise key establishment techniques based on the complex arithmetic of large integers given by Chakrabarti et al. (2006). Therefore, a scheme has called for to intercommunicate among the sensor nodes and relay the massage to its base station securely, known as KPS. Over the last two decades, a sequence of research work dealt with key distributions for WSN and many solutions have been proposed keeping various aspect in mind. Based on the assignments of keys to sensor nodes, researchers have categorized the key pre-distribution approach to the problem of key establishment, prior to deployment, into three categories: probabilistic see Du et al. (2005), Eschenauer & Gligor (2002) and Liu & Ning (2003), for deterministic see Blom (1984), Camtepe & Yener (2007), Dong et al. (2008), Hazra et al. (2015), Lee and Stinson (2004), Pietro et al. (2004), Ruj and Roy (2007) and Shafiei et al. (2008) and for hybrid see Camtepe & Yener (2007), Chakrabarti et al. (2006), and Modh et al. (2015). Here, we present a deterministic key pre-distribution scheme for WSN.

Key pre-distribution scheme is a means of specifying which node stores which key-rings according to previous arrangement of keys before deployment. These schemes essentially involve a trade-off between the competing requirements of low memory usage, high network connectivity and resilience against adversaries who capture nodes and steal the keys stored in nodes. This scheme consists of three phases, key distribution, shared key discovery, and path key establishment. Every sensor node is initially loaded with a fixed number of keys and assigned to a unique key identifier. After the deployment of the distributed sensor nodes, the shared-key discovery phase takes place, where any two nodes in wireless communication range exchange their list of key identifiers to each other, and look for their common keys. If they share one or more common keys, they can pick a set of keys for cryptographic communication. The path-key establishment phase takes place if there is no common key between a pair of nodes. Then a sequence of nodes constitute the path. To establish a secure path with node B_j, a node B_i needs to find a path between itself and the node B_j such that any two adjacent nodes in the path have common key. Thus, messages from the node B_i can reach to the node B_j securely.

The key pre-distribution scheme based on combinatorial designs determines how many chosen keys to designate to key chain before the sensor network deployment. This scheme becomes an emerging research area due to the arrangement of elements of finite sets into subsets satisfying various properties. Eschenauer & Gligor proposed the basic random key pre-distribution scheme in Eschenauer & Gligor (2002). In this scheme, two nodes will compute pair wise key only if they share a certain number common keys, which is pre-specified. Then each node will be pre-loaded with a key ring of k keys randomly selected from a large pool S which is deduced by the key derivation function. After the deployment step, if two neighbors share at least one key, they establish a secure link and compute their session secret key which is generated from the common key. Otherwise, if neighboring nodes do not have common keys, they should determine secure paths which are composed of successive secure links. This basic approach is CPU and energy efficient but it requires a large memory space to store the key ring. Moreover, if the network nodes are progressively corrupted, the attacker may discover a large part or the whole global key pool. Hence, a great number of links will be compromised. In the year 2004, Camtepe & Yener suggested the deterministic key pre-distribution scheme using projective planes, generalized quadrangle and symmetric BIBD and analyze the security and connectivity properties like scalability and resiliency of the scheme in Camtepe and Yener (2007). By that time, Lee and Stinson have also used the concept of Transversal Design for key pre-distribution in WSN, independently given in Lee & Stinson (2004). On studying and simulating the scheme provided by Lee & Stinson, can be chosen to vary the resilience, connectivity and storage requirements of the KPS. They also describe how the resilience of the scheme can be increased by combining a transversal design with Blom's method in Blom (1984), to construct a KPS, which they term as **multiple space scheme**. Chakrabarti, Roy, and Maitra provide a new scheme, where they randomly choose x number of blocks and merged to form a new node in Chakrabarti et al. (2006). They have chosen the blocks in such a way that there will be no inter node connectivity. As they have chosen randomly, for some cases they could not avoid the occurrence of inter node connectivity. After forming a number of nodes they revised their scheme by introducing $MOVE$ function to increase connectivity between different pairs in the network. $MOVE$ increases the connectivity by exchanging blocks between maximum linked pair with zero linked pair. Later various combinatorial objects are being used to design KPS to develop security and performance in load distribution, such as Partially balanced incomplete block designs and Reed-Solomon codes were suggested in 2007 by Ruj & Roy, Orthogonal arrays and 3-designs were suggested in 2008 by Dong et al. and many more. Beside these schemes and to reduce hops and hence potential risks from node capture, it is more important to have connected networks that cannot be guaranteed by random schemes. So we opt for deterministic protocols for security applications in networks that ensure high connectivity.

Here we have designed a KPS scheme based on combinatorial designs. The pioneering work of Camtepe & Yener proposes a deterministic pairwise KPS with the help of combinatorial objects such as symmetric designs and generalized quadrangles. There Balanced Incomplete Block Designs are mapped to obtain efficient key distribution schemes. They have shown that the combinatorial approach produces better connectivity with smaller key-chain sizes. Further study in this context can be found in Du et al. (2005), Lee and Stinson, (2004), Shafiei et al. (2008) or Zhou et al. (2008).

On the other hand, combinatorial design theory is an arrangement of a set of elements under some specific rules. Such rules are pre-defined by the parameters of design theory see Ghosh & Dey (2015) and Shrikhande & Sane (1991). Designs are analyzed by the study of these parameters. As of application in this area, each node need not be stored the keys of all other nodes and hence the storage overhead of the network be reduced.

The remainder of this paper is organized as follows: Section 2 devoted to the mathematical foundation and established the relation between combinatorial design and key distribution model. Also some previous works relevant to KPS scheme are reviewed in this section. In Section 3, we introduce our suggested scheme with relevant phases using triangle-free quasi-symmetric design. In the succeeding subsection we address the security issues. Finally in section 4, we conclude with future Plan.

2. Mathematical Foundation

The subject combinatorial design found its application initially in the design of experiments in statistics in the year 1930. Then the rapid advances in design theory can be attributed in large degree to its impetus from application in coding theory and communication. Also combinatorial design techniques have been used in numerous other areas such as Boolean function, authentication code, cryptography etc. with deep interactions with geometry, algebra, number theory and graph theory. For detail on these areas where combinatorial designs have been used, one can refer Cameron and Lint (1991) and Colbourn and Dinitz (2007).

2.1. Quasi-symmetric 2-Design

Combinatorial objects become a rich field of practical application in wireless communication. Balanced Incomplete Block Design (BIBD) is one such among them.

Definition 2.1.1.

A 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 BIBD (v, b, r, k, λ) or 2-design is an incidence structure which satisfies the following conditions:

(1) $|X| = v, |A| = b$.
(2) Each subset in A contains exactly k varieties.
(3) Each variety in X occurs in r many blocks.
(4) Each 2-subset of varieties in X is contained in exactly λ blocks in A.

A BIBD (v, b, r, k, λ) design can be represented by an incidence matrix $M = (m_{ij})$ of dimension $v \times b$ with entries 0 and 1, where $m_{ij} = 1$, if the i^{th} variety is in the j^{th} block, and 0 otherwise. The parameters are related by themselves as $\lambda(v-1) = r(k-1)$ and $bk = vr$.

For $0 \leq x < k$, x is called the block intersection number, if there exists $B, B' \in A$ such that $|B \cap B'| = x$. A symmetric design is a 2-(v, k, λ) design such that $b = \lambda_0 = v$ and $r = \lambda_1 = k$ and any 2 blocks intersect in λ points. Now a slight generalization in the above definition will be sufficiently broad to include all symmetric designs. That generalization has been done in Fisher's inequality by $b \geq v$.

Definition 2.1.2.

A 2-design with exactly two intersection numbers is said to be quasi-symmetric 2-design.

We denote these intersection numbers by x and y, and assume to be $0 \leq x < y < k$. Here we will consider the proper quasi-symmetric design, i.e., both the intersection numbers are positive and not equal. So, for an example of quasi-symmetric design is symmetric design with some new additional blocks, where the blocks are intersecting either at λ points or nowhere. Again let D be a multiple of a symmetric 2-(v, k, λ) design. Then D is a quasi-symmetric 2-design with $x = \lambda$ and $y = k$ Ghosh & Dey (2015). For details reading on design theory, we refer to Shrikhande (1986).

Example 2.1.1.

For simplicity we consider the following parameter of design

- $v = 22$
- $k = 6$
- $\lambda = 5$
- $r = 21$
- $b = 77$

With $x = 0$ and $y = 2$ as intersection numbers. Then, the computer search result gives the blocks as,

$A = \{123456;\ 12789a;\ 12bcde;\ 12fghi;\ 12jklm;\ 137bfi;\ 138cgk;\ 139dhl;$
$13aeim; 147chm;\ 148bil;\ 149efk;\ 14adgj;\ 157dik;\ 158ehj;\ 159bgm;\ 15acfl;$

$167egl; 168dfm; 169cij; 238bhm; 16abhk; 237cil; 238bhm; 239egj; 23adfk;$
$247bgk; 248cfj; 249dim; 24aefl; 257efm; 258dgl; 259chk; 25abij; 267dhj;$
$268eik; 269bfl; 26acgm; 3478de; 349abc; 34fglm; 34hijk; 357agh; 3589fi;$
$35bekl; 35cdjm; 3679km; 368ajl; 36bdgi; 36cefh; 458akm; 4579jl; 45bdfh;$
$45cegi; 467afi; 46bejm; 46cdkl; 5678bc; 4689gh; 569ade; 56fgjk; 56hilm;$
$78fhkl; 78gijm; 79behi; 79cdfg; 7abdlm; 7acejk; 89celm; 8abefg; 89bdjk;$
$8acdhi; 9afhjm; 9agikl; bckikm; bcghjl; defijl; deghkm\}.$

Quasi-symmetric designs are also represented by the block graph Γ. Here vertices of Γ are the blocks of the design and two vertices are adjacent if they have y number of common verities. The parameters of $\Gamma(b, a, c, d)$ are related with the parameters of quasi-symmetric design Shrikhande (1986) as

$$a = \frac{\mathrm{k(r-\ 1)\ +\ x(1-\ b)}}{\mathrm{(y-\ x)}},$$
$$c = a + \mu_1\mu_2 + \mu_1 + \mu_2, \quad d = \ a + \mu_1\mu_2,$$
$$\mu_1 = \frac{r - \lambda - k + x}{y - x},$$
$$\mu_2 = \frac{x - k}{y - x}.$$

Let M and N denote the incidence matrix and adjacency matrix of the design respectively. Then with the help of these, a matrix P can be formed as

$$P = \begin{pmatrix} 0 & M \\ M' & N \end{pmatrix}.$$

Consider the complement of strongly regular graph $\Gamma(b, a, c, d)$, denoted by $\overline{\Gamma}$, is again a strongly regular graph with parameters $(b,\ b - a - 1,\ b - 2a + d - 2,\ b - 2a + c)$. A strongly regular graph Γ is said to be triangle-free iff $c = 0$, i.e., the graph contains no cycle of length 3. A quasi-symmetric design is said to be triangle-free, if the complement of Γ i.e., $\bar{\Gamma}$ does not contain a triangle or equivalently the design has no three mutually disjoint blocks.

Theorem 2.1.1. [Shrikhande (1986)]

Let D be a quasi-symmetric design $(\mathrm{v, b, r, k}, \lambda)$ with block intersections x and y $(\mathrm{x} \neq \mathrm{y})$. Let M and N be the incidence matrix and adjacency matrix of the design D. Let 1_{v} and 0_{b} be row vectors of all 1's and 0's respectively. Then, P will represent a strongly regular graph if and only if D has parameters,

$$\mathrm{v = y(y^2 + 3y + 1)}, \qquad \mathrm{b = (y^2 + 2y - 1)(y^2 + 3y + 1)}, \ \ \mathrm{r = (y + 1)(y^2 + 2y - 1)},$$
$$\mathrm{k = y(y + 1)}, \qquad \lambda = \mathrm{y(y + 1) -\ 1}, \qquad \mathrm{x = 0}, \qquad \mathrm{y}, \qquad (\mathrm{y} \geq 1).$$

Moreover, the only strongly regular graph P so obtained are so-called "Negative Latin Square graphs" $\mathrm{NL_y(y^2 +\ 3y)}$ with parameters $\mathrm{((y^2 +\ 3y)^2,\ y(y^2 +\ 3y\ +\ 1),\ 0,\ y(y\ +\ 1))}$.

Example 2.1.2.

Consider the design D with parameters $(v, k, \lambda, b, r) = (22, 6, 5, 77, 21)$ is a quasi-symmetric design as in **Example 2.1.1.** Its corresponding parameter of the strongly regular graph is:

$$b = (\mathrm{y}^2 + 3\mathrm{y})^2 = 100,\ \mathrm{a} = \mathrm{y}(\mathrm{y}^2 + 3\mathrm{y} + 1) = 22,\ \mathrm{c} = 0, \mathrm{d} = \mathrm{y}(\mathrm{y} + 1) = 6.$$

Since it contains no cycle of length 3, so this also represents a triangle-free strongly regular graph. The figure of which is given below in Figure 1.

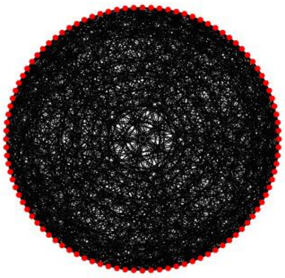

Figure 1: A Figure of tf-SRG

Here we are interested with the set of parameters of triangle-free quasi-symmetric designs to represent the key distribution scheme. A quasi-symmetric design here refers to 2-design with precisely two block intersection numbers 0 and y.

2.2. Correspondence between Quasi-symmetric designs and Key Distribution.

Once the network size (denoted by b) and the number of keys per node (denoted by k) are specified, the centre chooses a regular, uniform design of rank k, say (X, A), having exactly b blocks. The design (X, A) is used as the key ring space. The key ring space is used as a key pre-distribution scheme for a network having b nodes. Let the sensor nodes be denoted by $V_1, V_2, \ldots, V_b$. Let

$$X = \{x_i | 1 \leq i \leq v\}$$

and

$$A = \{A_j \, | 1 \leq j \leq b\}.$$

The v points in X have $1 - 1$ correspondence with a set of v keys, as follows: For $1 \leq i \leq v$, a key, denoted by K_i, is chosen uniformly at random from some specified key-space, say S (e.g. $= \{0, 1\}^{256}$). Then, for each j, $1 \leq j \leq b$, the sensor node V_j receives the set of k keys

$$\{K_i : i \in A_j\}.$$

Here, each point x_i work as the key identifier for K_i and each block A_j identify the key set that is assigned to the node V_j. Such scheme is familiar with Eschenauer & Gligor (2002), where key ring space is the subset of all k – subset from X. The variation of our model is the non-existence of 3 mutually disjoint blocks i.e., the complement of the block graph does not contain any triangle, which reduces the storage overhead of the said network. Thus the correspondence between the design and KPS given in the following table.

Table 1. Corresponding between design and KPS

Quasi-symmetric designs	**Key distribution**
Point set	Key space S

Point set size v	Key space size ($\lvert S \rvert$)
Block	Key ring
# blocks (b)	# key-chain or # key ring, # nodes
# points in a block	# K_i in key-chain
# blocks that a point is in	# key-chains that a key is in
Two blocks adjacent for y points in common	Two nodes communicate for y keys are common

The effectiveness of a sensor network can be explained by the following two aspects:

- The connective probability $p_{connect}$, which is defined by the probability that any pair of sensor nodes shares a link i.e., they have exactly y common keys. By this the effectiveness of the sensor network is measured.
- The probability $fail(1)$, this is defined by 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 networks. Such probability is defined by,

$$fail(1) = \frac{\text{the losted connectivies}}{\text{the connectivities remains}},$$

Given two nodes have at least y common keys; they use all their common keys to compute their pairwise key, by means of an appropriate key derivation function.

3. New Scheme

For the key distribution among the sensor nodes, the combinatorial design has been implemented, known as quasi-symmetric 2-design, which is a slight generalization of symmetric design. Let (X, B) be a combinatorial design with $|X| = v$ and every block B'in B containing k number of elements of X. If any pair of elements of X occurs in λ number of blocks, then it is called 2 - (v, k, λ) design. If in addition, any pair of blocks intersect one of two distinct number of points of X, say x and y, then it is known as quasi-symmetric 2-design. Here we consider the quasi-symmetric design having non-trivial intersection number, i.e., $y > x \geq 0$.

Lemma 3.1. [Shrikhande & Sane (1991)]

Let (x, B) be a non flag of a triangle-free quasi-symmetric design D and suppose $\alpha(\mathrm{x}, \mathrm{B})$ is the number of blocks on x not meeting B. Then,

$$\alpha(x, B) = r - m\lambda$$

for any integer m, its value is restricted by $2 \leq \mathrm{m} \leq \mathrm{y} + 1$.

Theorem 3.2.

Let D be a quasi-symmetric design with block intersection numbers 0 and y. Suppose D has no three mutually disjoint blocks. Then the parameters of D can be expressed as follows:

$$\mathrm{v} = \mathrm{y}(\mathrm{y}^2 + 3\mathrm{y} + 1), \qquad \mathrm{b} = (\mathrm{y}^2 + 2\mathrm{y} - 1)(\mathrm{y}^2 + 3\mathrm{y} + 1),$$

$$\mathrm{r} = (\mathrm{y} + 1)(\mathrm{y}^2 + 2\mathrm{y} - 1), \qquad \mathrm{k} = \mathrm{y}(\mathrm{y} + 1), \qquad \lambda = \mathrm{y}^2 + \mathrm{y} - 1.$$

Remark 3.3.

The above D become a triangle-free quasi-symmetric 2-Design. With the help of this design we can construct a key pre-distribution scheme.

Consider the sensor network having b number of nodes and therefore b numbers of key–chains are there. Each key-chain can store at most k number of keys coming from a key-pool X. Since each key presents in r number of blocks. But we establish the link among the nodes for exactly y keys are common.

3.1. Algorithm 1

Following algorithm describe the triangle-free quasi-symmetric designs.

Require: Choose y an integer ≥ 2

- Calculate $v = y(y^2 + 3y + 1)$.
- Calculate $k = y(y + 1)$.
- Calculate $b = (y^2 + 2y - 1)(y^2 + 3y + 1)$.
- Establish $r = v - 1$ and $\lambda = k - 1$.
- Calculate $\mu_1$and μ_2.
- Calculate $a = b + \mu_1\mu_2 - 2$.
- Calculate $c = a + \mu_1\mu_2 + \mu_1 + \mu_2$.
- Establish the link between the two nodes provided they have y number of common keys.

3.2. Storage Overhead

When using the proposed triangle-free quasi-symmetric design based version matching with strongly regular graph of uniform rank k, each node is pre-loaded with one key ring corresponding to one block from the design. Hence, each node is pre-loaded with $y(y + 1)$ number of keys. The memory required to store keys is, then, $l \cdot y(y + 1)$ where l is the key size.

3.3. Network Scalability

From construction, the total number of possible key rings when using the triangle-free quasi-symmetric design based scheme is $b = (y^2 + 2y - 1)(y^2 + 3y + 1)$, this is then the maximum number of supported nodes.

3.4. Session Key Sharing Scheme

When using the mapping of quasi-symmetric design, we know that each key is used in exactly $y(y^2 + 3y + 1)$ key rings among the $(y^2 + 2y - 1)(y^2 + 3y + 1)$ possible key rings. Let us consider two nodes x_1 and x_2 selected randomly. The node x_1 is pre-loaded with a key ring $A_{x_1}$of $y(y + 1)$ different keys and that of x_2 is pre-loaded with a key ring $A_{x_2}$of same number of keys. Now these pair of nodes may have no common key or they have y number of keys in common. Therefore, the nodes will be adjacent, provided they have y number of keys in common. Now from the idea of strongly regular graph, two adjacent nodes have exactly c common neighbors. Again, $\bar{\Gamma}$ represents triangle-free quasi-symmetric designs with above parameters also generate a negative Latin square graph where two adjacent nodes have no common neighbor, since triangle-free strongly regular graph does not contain any cycle of length 3. On the other hand, for two non-adjacent nodes have $y(y^2 + 4y + 2)$ number of common neighbours. These will help to construct the key-path.

Each key is contained in $v - 2$ other key rings. Knowing that each pair of keys occur together in exactly $(y^2 + y - 1)$ blocks, we find that the blocks containing $y\ + 1$ different keys of A_{x_1} are completely disjoint. Hence, each node shares exactly one key with $y^3 + 3y^2 + y - 2$ nodes among the $y^3 + 3y^2 + y - 1$ other possible nodes. Therefore, the number of links established for a node is $y(y\ + 1)$. Let $p_{connect}$ be the probability of any two nodes sharing exactly y keys to form a secure connection. Then

$$p_{connect} = \frac{y(y\ +\ 1)}{b}.$$

3.5. Resiliency against random node compromise.

Security is the major issue of wireless sensor network. Security problem incorporated in WSN due to various constrained as storage capacity, low computational power, large number of nodes in the network, wireless type of communication etc. Here, we have tried to evaluate a new scheme in terms of its resilience against node collusion and selective node capture attack. But resiliency contradicts to the probability of key share because as many blocks are effected, as the number of more keys are shared among the nodes when a block is compromised. If a node is directly involved in node collusion, e.g., because of being captured by an outside adversary or reprogrammed to do harm to the whole network, we say the node is compromised. Mathematically this can be calculated as

$$fail(1) = \frac{Number\ of\ links\ broken\ when\ s\ nodes\ are\ compromised}{\frac{(N-s)(N-s-1)}{2}},$$

where, N is the size of the network. In case of selective node capture attack, the attacker comprises those nodes whose keys have not already been compromised. Amid shared key discovery phase only node identifiers are broadcasted, key identifiers are not exchanged. Hence attacker at any stage cannot know which key identifiers are present in which node. Thus attacker cannot gain any information using this attack. The Table 2 gives a list of value of probability $p_{connect}$ and $fail(1)$ of our scheme.

Table 2. Comparison for various numbers of nodes

y	b	v	k	s	$p_{connect}$	$fail(1)$
4	667	116	20	7	0.2121	0.00064
5	1394	205	30	11	0.2386	0.00034
6	2585	330	42	16	0.2615	0.00020
7	4402	497	56	27	0.3456	0.00015

8	7031	712	72	37	0.3809	0.00011

4. Conclusion

All key management techniques have their own benefits as well as shortcomings. In this paper, a new highly scalable key pre-distribution scheme for WSN has been proposed. We make use, for the first time, of the triangle-free quasi-symmetric design to improve the resiliency. We showed that a basic mapping from quasi-symmetric designs to key pre-distribution allows achieving extremely high network scalability while improving the key sharing probability. We proposed then an enhanced quasi-symmetric design based construction which gives birth to a new key management scheme providing high network scalability and good key sharing probability. We conducted analytic calculation and showed that our approach enhances significantly the network scalability when providing good overall performances. As future work, we plan to deepen the analysis of our parameter choice in order to suggest values given the best trade-off. Furthermore there is lot of chances in this field so that constrained resources of wireless sensor network can be efficiently used and network utilization can be improved.

Acknowledgement

Second named author is thankful to DST-INSPIRE for financial support to pursue his research work.

REFERENCES

Blom, R. (1984). An optimal class of symmetric key generation systems, In Proceeding of EUROCRYPT, pp. 335 – 338.

Blundo, C., Santis, A. D., Herzberg, A., Kutten, A., Vaccaro, U., and Yung, M. (1992). Perfectly secure key distribution for dynamic conference, Advances in Cryptology-CRYPTO, LNCS Springer – Verlag, Vol. 740, pp. 471 – 486.

Cameron, P. J., and Van Lint, J. H. (1991). Designs, Graphs, Codes and their links, Cambridge University Press, pp. 105 – 116.

Camtepe, S. A., and Yener, B. (2007). Combinatorial design of key distribution mechanisms for wireless sensor networks, ACM Trans. on Networking, Vol. 15, No. 2, pp. 346 – 358.

Chakrabarti, D., Maitra, S., and Roy, B. K. (2006). A key pre-distribution scheme for wireless sensor networks merging blocks in combinatorial design, Int. J. Inf. Sec., Vol. 5, No. 2, pp. 105 – 114.

Colbourn, C. J., and Dinitz, J. H. (2007). Handbook of Combinatorial Designs, 2nd ed. CRC Press, Chap: Quasi-symmetric Designs, M. S. Shrikhande, pp. 578 – 582.

Dong, J. W., Pei, D. Y., and Wang, X. L. (2008). A class of key pre-distribution schemes based on orthogonal arrays, J. Computer Science and Technology, Vol. 23, No. 5, pp. 825 – 831.

Du, W., Deng, J., Han, Y. S., Varshney, P., Katz, J., and Khalili, A. (2005). A pairwise key pre-distribution scheme for wireless sensor networks, ACM Transactions on Information and System Security, Vol. 8, No. 2, pp. 228 – 258.

Eschenauer, L., and Gligor, V. D. (2002). A key-management scheme for distributed sensor networks, In Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington DC, USA, pp. 41 – 47.

Ghosh, D., and Dey, L. K. (2015). On some parametric classification of Quasi-Symmetric 2-Designs, Tamkang Journal of Mathematics, Vol. 46, No. 3, pp. 269 – 280.

Hazra, P., Giri, D., and Das, A. K. (2015). Key-Chain-Based Key pre-distribution protocols for securing wireless sensor networks, in International Conference on Mathematics and Computing (ICMC 2015), Springer Proceedings in Mathematics and Statistics.

Lee, J., and Stinson, D. R. (2004). Deterministic Key pre-distribution schemes for Distributed Sensor Networks, In Proc. 11th International Workshop, SAC, pp. 294 – 307.

Liu, D., and Ning, P. (2003). Establishing pairwise keys in distributed sensor networks, In Proceedings of the 10th ACM Conference on Computer and Communications Security, Washington DC, USA, pp. 52 – 61.

Mitra, S., Mukhopadhyay, S., and Dutta, R. (2014). A group-based deterministic key pre-distribution scheme for wireless sensor network, International J. of Wireless and Mobile Computing, Vol. 7, No. 5, pp. 435 – 447.

Modh, A., Dabhi, M., and Mishra, L. N. (2015). Wireless network controlled robot using a website, android Application or simple hand gestures, Journal of Computer Network, Vol. 3, No. 1, pp. 1 – 5.

Pietro, R. Di, Mancini, L. V., Mei, A., and Panconesi, A. (2004). Connectivity Properties of Secure Wireless Sensor Networks, In Proc. of the 2nd ACM SASN workshop, pp. 53 – 58.

Ruj, S., and Roy, B. (2007). Key pre-distribution schemes using partially balanced designs in wireless sensor networks, In ISPA, Lecture Notes in Computer Science 47, pp. 431 – 445.

Shafiei, H., Mehdizadeh, A., Khonsari, A., and Ould-Khaoua, M. (2008). A Combinatorial Approach for Key-Distribution in Wireless Sensor Networks, In Proc of the IEEE "GLOBECOM”.

Shrikhande, M. S. (1986). A survey of some problems in combinatorial designs: A matrix approach, Linear Algebra Appl., Vol. 79, pp. 215 – 247.

Shrikhande, M. S., and Sane, S. S. (1991). Quasi-symmetric designs, London Math. Soc. Lecture Notes 164, Cambridge University Press.

Zhou, Y., Fang, Y., and Zhang, Y. (2008). Securing wireless sensor networks: A survey, IEEE Communications Surveys and Tutorials, Vol. 10, No. 1 – 4, pp. 6 – 28.