JACET Journal of Advances in Computer Engineering and Technology, 1(3) 2015

Hybrid Key Pre-distribution Scheme for Wireless Sensor Network Based on Combinatorial Design

Hamid. Haj Seyyed Javadi[1], Mohaddese. Anzani[2]

Received (2015-09-19)
Accepted (2015-10-17)

Abstract **- Key distribution is an important problem in wireless sensor networks where sensor nodes are randomly scattered in adversarial environments. Due to the random deployment of sensors, a list of keys must be pre-distributed to each sensor node before deployment. To establish a secure communication, two nodes must share common key from their key-rings. Otherwise, they can find a key- path in which ensures that either two neighboring nodes have a key in common from source to destination. Combinatorial designs are powerful mathematical tools with comprehensive and simple structures. Recently, many researchers have used combinatorial designs as key pre-distribution scheme in wireless sensor networks. In this paper we consider a hybrid key pre-distribution scheme based on Balanced Incomplete Block Design. We consider a new approach for choosing key-rings in the hybrid symmetric design to improve the connectivity and resilience. Performance and security properties of the proposed scheme are studied both analytically and computationally. The obtained results show that our scheme provides better resilience than symmetric design.**

Index Terms **- Wireless sensor networks, Key pre-distribution, Symmetric BIBD.**

1- shahed university(hamid.h.s.javadi@gmail.com)
2- shahed university(anzani@shahed.ac.ir)

I. INTRODUCTION

A wireless sensor network (WSN) is a collection of sensor nodes which is used in critical applications within several fields including military, medical and industrial sectors. These sensors have limitations in computing power, memory and battery power. In a WSN, sensor nodes need to communicate with each other for data processing and secure communication. For a secure communication, any two nodes should share a common secret key. Key agreement is one of the most challenging aspects of key-distribution, in a sensor network. There are three types of key agreement schemes: self-enforcing, pre-distribution, and trusted server. Due to the lack of trusted infrastructure and resource constraints, key pre-distribution schema seems to be the best solution which is used in most of the research studies. All the key Pre-distribution schemes have three phases: 1) Pre-distribution; in the first phase, a large pool of keys with their ID is generated. Then, to each sensor node, a subset of key-pool (key-ring) with their ID is assigned. 2) shard-key discover; this phase is performed after the deployment of sensor nodes. Each pair of nodes that are in the radio frequency to communicate with each other, by exchanging their key identifiers, they must find at least one shared-key between them. 3) Path-key establishment; if the two nodes that must communicate with each other, they do not have a shared key, they may establish a secure path using one or more intermediate nodes along which each pair of nodes share a common key. The key pre-distribution in a wireless sensor network can be done using three methods: (1) Probabilistic (2) Deterministic (3) Hybrid. In the

first method, the keys are selected randomly from a key-pool and stored on each sensor node. In this way it is possible that two nodes are not directly able to communicate with each other. In the second method, key- rings are selected from the key-pool, using a predetermined manner. In the third method, both probabilistic and deterministic methods are used. The probabilistic section of this method, helps to improve the scalability and flexibility whereas, its deterministic section, improves the key connectivity.

The first Probabilistic key pre-distribution scheme proposed by Eschenauer and Gligor [7]. Based on this scheme, Chan et al. [6] proposed a q-composite random key pre-distribution scheme, which increases the security of communication between two nodes. In this scheme, two nodes can establish a secure link only if they share at least q keys. In [11], Qian proposed a key pre-distribution scheme in which a hash function is used to improve resilience against node capture attack. Li et al. in [10] proposed a threshold for random key pre-distribution schemes that each node in the network can establish a secure path with its l-hop neighbours. In [3], Blom proposed a λ-secure key pre-distribution scheme where each node stores a row of a secret matrix and a column of a public matrix. Blom's scheme is a deterministic scheme where any pair of nodes can share a common secret key.

Combinatorial designs are the other methods used to design a deterministic key pre-distribution. In [4], Camptepe and Yener presented a deterministic key pre-distribution approach based on combinatorial scheme, to decide the number of keys and which keys are assigned to each key-ring, before deploying sensor networks. In this scheme has been used the Balanced Incomplete Block Designs(BIBD) and Generalized Quadrangles (GQ), to obtain the efficient key distribution schemes. Lee and Stinson in [9] used Transversal Design (TD) as a deterministic KPS. Ruj and Roy in [12] proposed a scheme using Partially Balanced Incomplete Block Design (PBIBD). Bechkit et al. in [2] proposed another key pre-distribution approach based on Unital design theory.

The hybrid schemes which inherit benefits of both probabilistic and deterministic schemes have been studied by several researchers. Camtepe and Yener [4], Chakrabarti et al. [5] and Kavitha and Sridharan [8] proposed hybrid designs for key pre-distribution in sensor networks which employ combinatorial designs.

1.Our Contributions

In this paper we provide a new approach for key pre-distribution in wireless sensor networks to improve the resilience of the SBIBD scheme [4] and also to enhance the connectivity of the Hybrid Symmetric design [4]. In our proposed approach we use the same key- pool to construct the blocks of base symmetric design and remaining blocks in contrast to the hybrid symmetric scheme, which utilizes one key- pool and complement of blocks.

This paper is organized as follows: In Section II, we consider the background of combinatorial design and related work of key pre-distribution based on combinatorial design. In section III, we provide a basic model of our scheme. In Section IV, we describe our proposed approach. In Section V, we present our analysis and comparison with hybrid symmetric scheme and symmetric design. Finally in Section VI we conclude.

II. BACKGROUND ON COMBINATORIAL DESIGNS

1. Preliminaries

A set system or design is a pair (X; A), where A is a set of subsets of X, called blocks. The elements of X are the points. The degree of a point x ϵ X is the block numbers contain x.

The size of the largest block is called the rank of a set system. Balanced Incomplete Block Design (BIBD) or (v; b; r; k; λ)-BIBD is a set system with the following properties:

1. | X |= v, | A |= b,
2. Each block of A contains exactly k elements,
3. Each elements occurs in exactly r blocks,
4. Each pair of elements comes in exactly λ blocks of A.

In a (v; b; r; k; λ)-BIBD, we have: λ (v -1) = r(k - 1) and bk = vr. Especial type of BIBD is called symmetric Design or symmetric BIBD denoted by (v; k; λ)-SBIBD. In SBIBD we have b = v and therefore r = k [13]. In a Symmetric Design every block has k = r elements, every element appears in r = k blocks, every pair of elements appears in λ blocks and every pair of blocks intersects in λ elements.

A Projective plane is a finite set of points and lines in which every pair of lines has just one intersection point and a unique line covers every pair of points. Projective plane is a kind

of SBIBD with parameters (q^2+q+1; q+1; 1)

which means q+1 points on each line has q^2+q + 1 points and q^2 + q + 1 lines [13].

Another class of block designs is Latin square with order q which is a q×q array such that each of the q symbols occurs exactly once in each column and row. Latin squares A and B

of order q are orthogonal if all entries of A join B are distinct. Latin square A1; A2;… ; Ar are Mutually Orthogonal Latin Squares (MOLS) if they are orthogonal in pairs.

2. Key pre-distribution based on combinatorial

In [4] Camtepe and Yener proposed a symmetric key predistribution design based on symmetric BIBD with parameters (q^2 + q + 1; q + 1; 1) in which q is a prime power that q^2 + q + 1 > N, where N is the number of nodes in the network. The main advantage of their scheme is that it provides full connectivity between any pair of nodes in network but it is not scalable. To support large networks, we

need a large key- pool and therefore larger key-rings which are beyond the memory limitation of sensor nodes.

To improve these problems, Camtepe and Yener [4] proposed a hybrid design which the subsets of complementary design blocks are used to construct key-rings for additional nodes.

Let D = (v; k; λ) be a block design with a set |S| = v objects and B = {B1; B2; …;Bb} blocks in which every block has k objects. In a complementary design, D has complement blocks Bi = S - Bi for $1 \leq i \leq b$. The block design D has parameters (v; b; b-r; v -k; b-2r + λ) where b - 2r + λ > 0 [1, Theorem 1.1.6]. D = (v; k; λ) is a symmetric design if and only if D = (v; v - k; b - 2r + λ) is a symmetric design [1, Corollary 1.1.7].

In this approach for the network with N nodes where nodes can store K keys because of its memory limitations, the largest prime power q is considered in a way that q +1 < K. Then

b of N blocks are generated by base symmetric design and N -b blocks are randomly selected among k-subsets of the complementary design blocks. The hybrid symmetric design decreases the probability of key share of the base symmetric design.

III. NETWORK MODEL

In this work, we assume that N sensor nodes are distributed in an adversarial environment. We suppose that each sensor node

is preloaded with a key-ring. We consider a key pre-istribution consists three phases: in the key pre-distribution phase, the base station generates a number of key rings based on the

our proposed algorithm and assigns a key ring to each sensor node before deployment of the network. Then the shared-key discovery phase takes place. In this phase, each pair of nodes

in wireless communication range try to find the common keys. If there is no common key between a pair of nodes in wireless communication range, the path-key establishment takes place. In this phase, two nodes look for a secure path to communicate each other.

IV. OUR PROPOSED APPROACH

In this work we have modified the hybrid symmetric design to solve the problem of low key share probability. Let N be the number of nodes in network, therefore N key-rings are required. To generate a key-pool and key-rings, we first find the largest prime number q such that q^2 + q + 1 < N and use symmetric BIBD with parameters (q^2+q+1; q+1; 1) to generate b blocks of size q+1. We assign these b blocks

to b nodes where b < N. For the remaining N -b nodes, instead of using the subsets of complementary design blocks, we repeat the blocks of base symmetric BIBD design. Therefore, we have a BIBD design with parameters (q2 + q + 1; 2(q^2 + q + 1); 2(q + 1); (q + 1); 2).

It results from the following Theorem:

Theorem 1: (Sum Construction [13, Theorem 1.30]) Suppose that there exists a (v; k; λ 1)-BIBD and a (v; k; λ 2)-BIBD. Then there exists a (v; k; λ 1 + λ 2)-BIBD.

Our proposed approach can be summerized in the Algorithm I.

Example 2: Consider a network with N nodes. Assume that nodes can store at most K = 3 keys in their key-rings.

Therefore, we can choose q = 2 and construct symmetric design (7; 3; 1). We can generate b = 7 blocks as B =

{{1; 2; 3}; {1; 4; 5}; {1; 6; 7}; {2; 4; 6}; {2; 5; 7};{3; 4; 7}; {3; 5; 6}}. Remaining N - b = 3 blocks are selected at random among blocks of B (repeat the blocks). The blocks

H = {{1; 4; 5}; {2; 4; 6}; {3; 5; 6}} can be

assigned to remaining three nodes.

Algorithm I: Modified Hybrid Design

Require: N {Total number of nodes}

1. Find the largest prime number q such that $(q2 + q + 1) < N$;
2. Generate the base Symmetric Design with parameters$(q2 + q + 1; q + 1; 1)$:
   •v objects $P = \{a_1, a_2,...,a_v\}$;
3. Generate b blocks $B = \{B_1, B_2,..., B_b\}$ of size $q + 1$ from the base Symmetric Design;
4. Randomly select $N - b$ blocks among of blocks Of B and assign them to $N - b$ remaining nodes (we repeat the blocks of B).

V. ANALYSIS

In this section we analyse the connectivity and resilience of the proposed scheme compared with that of hybrid symmetric design and symmetric BIBD in[4] .

1. Connectivity

We consider connectivity as the probability that any pair of nodes shares at least a common key. As the symmetric BIBD has full connectivity between every pair of nodes and

selected nodes in our approach are from same key- pool, the probability that these nodes share a common key in our approach is 1. Note that the probability that any pair of nodes share at least a common key in the hybrid symmetric design in [4] is:

$$\text{QBB} + 0.5\text{QHB} + \text{PHQH} + \text{QHH} \leq \text{PHSYM}$$

and

$$\text{PHSYM} \leq \text{QBB} + \text{QHB} + \text{PHQH} + \text{QHH}$$

where

$$Q_{BB} = \frac{b(b-1)}{N(N-1)};$$

$$Q_{HB} = \frac{2b(N-b)}{N(N-1)};$$

$$Q_{H} = \frac{(N-b)(N-2b)}{bN(N-1)};$$

$$Q_{HH} = \frac{(b-1)(N-b)^2}{bN(N-1)};$$

and

$$P_H = 1 - \frac{\binom{q^2-q-1}{q+1}}{\binom{q^2}{q+1}}.$$

Comparing our proposed approach and hybrid symmetric scheme, in terms of connectivity, we can state our proposed approach has better connectivity than hybrid symmetric approach.

Table I, summarizes the computational results of the probability of key share for the hybrid symmetric scheme and the our proposed approach.

TABLE I
Comparison of the proposed approach and hybrid symmetric in terms of connectivity

Key-ring size	Our proposed approach		Hybrid symmetric design	
	N	P_c	N	P_c
24	800	1	800	0.8929
42	1800	1	1800	0.8902
68	4557	1	4557	0.9010
102	10500	1	10500	0.9861

2. Resilience

In terms of resilience, we are interested in the probability that a link is compromised when an attacker captures x randomly selected nodes and their key-rings. This probability can be defined as:

$$P(L \mid C_x) = \sum_{\forall j} P(l_j \mid l) P(D_j \mid C_x)$$

where C_x denotes the event that x nodes are captured, l_j denotes event that a given link is secured with key j and D_j denotes the event that a key-ring which includes key j is compromised.

In our proposed approach we have a BIBD design with parameters (v; 2b; 2r; k; 2_) =(q^2+q+1; 2(q^2+q+1); 2(q+1); (q+1); 2). A key can appear in 2r blocks of 2b blocks. So, the probability that a link between two nodes is secured using key j is

$$P(l_j \mid l) = \frac{\binom{2r}{2}}{\binom{2b}{2}}$$

The probability that the key *j* appears in one or more of *x* compromised blocks is

$$P(L \mid C_x) = \sum_{j=1}^{q^2+q+1} P(l_j \mid l) P(D_j \mid C_x)$$

$$= \frac{(2q^2 + 3q + 1)}{2q^2 + 2q + 1} P(D_j \mid C_x)$$

$$\Rightarrow P(D_j \mid C_x) = 1 - \frac{\binom{2q^2}{x}}{\binom{2(q^2+q+1)}{x}}$$

Note that, resilience computed by Camtepe and Yener in [4] for the symmetric Design is

$$P(L \mid C_x) = 1 - \frac{\binom{q^2}{x}}{\binom{q^2+q+1}{x}}$$

It is clear that our proposed approach improves the resilience against node capture with the symmetric design.

In Table. II, we summarize the results of the probability that a link is compromised when an attacker captures some nodes.

We implemented the symmetric BIBD, hybrid symmetric design and our proposed approach. The simulations to evaluate our proposed approach approve our analytical results. Our proposed approach is compared with hybrid symmetric design for connectivity in Figure 1. As the connectivity coverage of both SBIBD and our proposed approach are the same (full connectivity), we have just drawn the connectivity of our proposed approach.

It is shown that the our proposed approach has better connectivity than hybrid symmetric design.

In Figure 2 we compare the resilience of our proposed scheme with symmetric BIBD and hybrid symmetric design for N = 00 and N = 1800. We select q in such a way that $q^2 + q + 1 <$ N and therefore key-ring size is computed as k = 24 and k = 42, respectively. We can see in Figure 2 (a), for small network size, our approach always has better resilience against node capture. Figure 2 (b) shows that for N = 1800 the resilience of our proposed approach is almost the same symmetric BIBD and hybrid symmetric design.

TABLE II
COMPARISON OF DIFFERENT SCHEMES IN TERMS OF RESILIENCE

	SBIBD-KP				
Key-ring size	30	50	70	90	110
24	0.7454	0.9022	0.9639	0.9872	0.9954
42	0.5260	0.7140	0.8285	0.8978	0.9395
	Our Proposed approach				
Key-ring size	30	50	70	90	110
24	0.6748	0.8396	0.9097	0.9406	0.9542
42	0.5245	0.7114	0.8253	0.8946	0.9366
	Hybrid Symmetric-KP				
Key-ring size	30	50	70	90	110
24	0.7493	0.8862	0.9517	0.9854	0.9935
42	0.5223	0.7262	0.8350	0.8856	0.9341

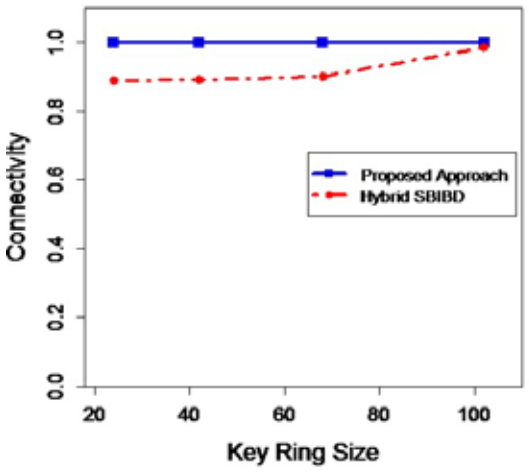

Fig. 1. Connectivity Comparison. Direct secure connectivity of our proposed scheme is compared with Hybrid Symmetric design and Symmetric design. Figure shows that our proposed scheme has better connectivity than Hybrid Symmetric design.

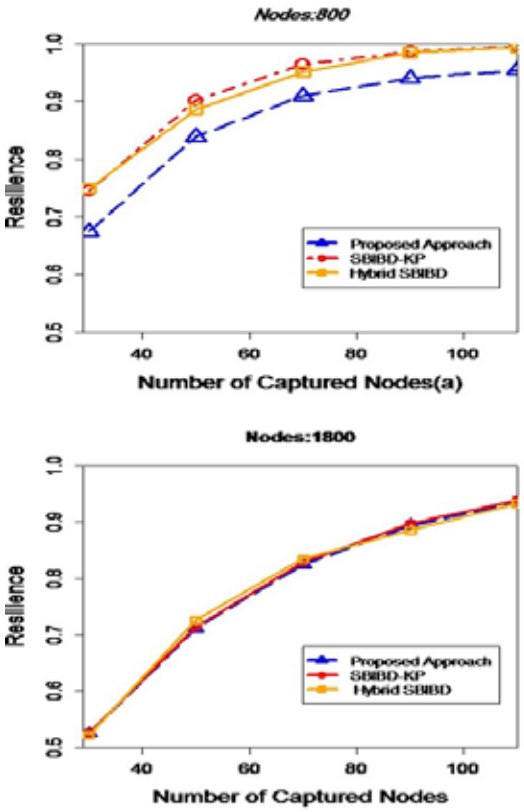

Fig. 2. Resilience Comparison. (a) . Solution results show that for small networks, our proposed approach has better resilience against node capture. (b) Resilience of the our proposed scheme is compared with Hybrid Symmetric design and Symmetric BIBD for the key-ring size k =42. For compromised nodes number greater than 70, the our proposed approach has the same resilience with both schemes.

VI. CONCLUSION

In this work, we present a modification to the hybrid symmetric design [4] to improve the key share probability and resilience of the wireless sensor network. We show that by considering same key-pool, instead of using complementary design in the Hybrid Symmetric scheme, we can achieve better results for networks. We illustrate our proposed approach has full connectivity and provides a better network resilience with the symmetric design and hybrid symmetric design.

REFERENCES

[1] I. Anderson, Combinatorial Designs: Construction Methods. Chicester, U.K.: Ellis Horwood, 1990.

[2] W. Bechkit, Y. Challal, A. Bouabdallah, and V.Tarokh,A highly scalable key pre-distribution scheme for wireless sensor networks. IEEE Transactions on Wireless Commu-nications, 12 (2): 948-959, 2013.

[3] R.Blom, An Optimal Class of Symmetric Key Genera-tion Systems. In Proceeding of Eurocrypt, Advanceds in Cryptology, Springer, 335-338, 1985.

[4] S. A. Camtepe, and B. Yener, Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. IEEE/ACM Transactions on Networking, 15: 346-358, 2007.

[5] D. Chakrabarti, S. Maitra, and B. K. Roy, A Key predistribution Scheme for Wireless Sensor Networks: Merging Blocks in Combinatorial Design. Int. J. Inf. Sec., 105-114, 2006.

[6] H. Chan, A. Perring, and D. Song, Random Key predistribution Schemes for Sensore Networks. In Proceeding of IEEE Symposium on Security and Privacy, 197-213,2003.

[7] L. Eschenauer, and V. D. Gligor, A key-management scheme for distributed sensor networks. In Proceeding of the 9th ACM Conference on Computer and Communications security, 41-47, 2002.

[8] T. Kavitha, and D. Sridharan. Hybrid design of scalable key distribution for wireless sensor networks. IACSIT International Journal of Engineering and Technology, 2 (2): 136-141, 2010.

[9] J. Lee, and D. Stinson, A Combinatorial Approach to Key predistribution for Distributed Sensor Networks. IEEE Wireless Communications and Networking Conference (WCN' 05), IEEE Communication Society, 1200-1205, 2005.

[10] WS. Li, CW. Tsai, M. Chen, WS. Hsieh, and CS. Yang, Threshold behavior of multi-path random key predistribution for sparse wireless sensor networks. Mathematical and Computer Modelling, 57 (11): 2776-2787,2013.

[11] S. Qian, A novel key pre-distribution for wireless sensor networks. Physics Procedia, 25: 2183-2189, 2012.

[12] S. Ruj, and B. Roy, Key pre-distribution Using Partially Balanced Designs in Wireless Sensor Networks. 5th International Symposium (ISPA), Springer, 431-445, 2007.

[13] D. Stinson, Combinatorial designs: Construction and Analysis. Springer, 2004.