SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2015; **8:**1561–1574
Published online 25 September 2014 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1104

RESEARCH ARTICLE

Application-specific hybrid symmetric design of key pre-distribution for wireless sensor networks

Tooska Dargahi[1]*, Hamid H. S. Javadi[2] and Mehdi Hosseinzadeh[1]

[1] Department of Computer Engineering, Islamic Azad University, Science and Research branch, Tehran, Iran
[2] Department of Mathematics and Computer Science, Shahed University, Tehran, Iran

ABSTRACT

Wireless sensor networks have been established for a wide range of applications in adversarial environments, which makes secure communication between sensor nodes a challenging issue. To achieve high level of security, each pair of nodes must share a secret key in order to communicate with each other. Because of the random deployment of sensors, a set of keys must be pre-distributed, so that each sensor node is assigned a set of keys from a key pool before the deployment. The keys stored in each node must be carefully selected to increase the probability of key share between two neighboring nodes. In this paper, we consider a hybrid key pre-distribution scheme based on the balanced incomplete block design. We present a new approach for choosing key pool in the hybrid symmetric design that improves the connectivity and scalability of the network. We also introduce an extension to the proposed approach to detract memory usage and improve resilience. Experimental results verify the performance and applicability of our approach. Copyright © 2014 John Wiley & Sons, Ltd.

KEYWORDS

wireless sensor network; key pre-distribution; symmetric BIBD; hybrid symmetric design

***Correspondence**

Tooska Dargahi, Department of Computer Engineering, Islamic Azad University, Science and Research branch, Tehran, Iran.
E-mail: t.dargahi@srbiau.ac.ir

1. INTRODUCTION

A wireless sensor network (WSN) is a collection of sensor nodes deployed in an area for several applications of various domains such as military, medical, urban, and biosurveillance systems [1]. These nodes communicate with each other over wireless links to relay the monitored data to a central node (called base station) or to each other. In many applications, WSNs are deployed in unsafe environments. Moreover, as with any radio-based medium, there exists possibility of various attacks in WSN. Therefore, security is an important issue in these networks.

Wireless sensor networks differ from other networks in several aspects; sensor nodes have limited computing capability, limited energy, and memory capacity. Moreover, their location is usually unknown before the deployment. For a secure communication, any two nodes should share a common secret key. There are several key distribution and agreement approaches, known as *key management* schemes, which can be used in such networks.

Various classifications of key management schemes have been addressed by researchers [2–5]. We consider the most common categorization of key management approaches: *self-enforcing*, *pre-distribution*, and *trusted server*, as shown in Figure 1. Because of the random deployment of nodes, 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 [2,3,5].

In the key pre-distribution schemes, keys are assigned to each sensor node from a set of keys called *key pool* by a trusted key distribution center (KDC), before the deployment of the network. So each node has a set of keys called *key chain*. Every pair of nodes, which need to communicate with each other, must share at least a common key from their key chains and have to be in each others radio range. If they do not share a common key directly, they can communicate through a path called *key path* in which each pair of neighboring nodes shares a common key.

Metrics that are usually used to evaluate a key pre-distribution scheme are connectivity, resilience, scalability, and key-chain size. Given any two nodes, connectivity is the probability of key share between them. Resilience refers to the stability of the sensor network against node capture attack. Usually, these two parameters are in conflict [5,6]. Scalability is the ability to support larger network

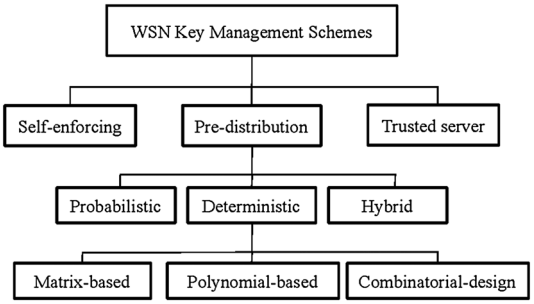


Figure 1. Classification of key management schemes in wireless sensor network.

size [7]. Key-chain size is related to the number of keys in the key chain of a node; key-chain size is tied to the memory capacity of sensor nodes [5].

Key pre-distribution schemes can be divided into three categories (Figure 1): (i) Probabilistic: key chains are chosen from a key pool in a random manner and are assigned to sensor nodes; (ii) Deterministic: key chains are chosen on the basis of a predefined arrangement; and (iii) Hybrid: combination of the probabilistic and deterministic approaches to inherit best of both worlds.

Although various approaches exist in the literature for each of the aforementioned categories, in this paper, our main focus is on hybrid key pre-distribution scheme based on combinatorial design, which is a subset of the deterministic class and its combination with probabilistic approach. In [8], a key distribution scheme based on combinatorial design, called symmetric design, is proposed. Although the symmetric design has many desirable properties, it is not scalable. To support large networks, we need large key pool and therefore larger key chains, which is beyond the capabilities of typical sensor nodes that have limited memory. To remedy this issue, Çamtepe and Yener propose hybrid version of the symmetric and probabilistic designs for a given number of nodes and key-chain sizes [8]. Hybrid symmetric design enhances scalability and resilience of the network while reduces key share probability of the core symmetric design [5].

1.1. Our contribution

In this paper, we propose a hybrid key pre-distribution scheme based on balanced incomplete block design (BIBD); a combinatorial-based design. Our scheme modifies the hybrid symmetric design [8] in order to improve key share probability and scalability yet providing the same resilience against node capture attack. The idea is to use two similar key pools with some different keys in contrast to the hybrid symmetric scheme, which utilizes one key pool and its complement. By this way, our proposed scheme, so-called modified hybrid symmetric (MHS) design, scales to large networks and facilitates the addition of new nodes without the need for key distribution re-organization comparing with the hybrid symmetric design.

We introduce a parameter to specify a desired level of connectivity for various application-specific scenarios. Using this parameter, a network designer can establish a trade-off between connectivity and resilience based on the application requirements. Furthermore, we introduce an extension to the proposed approach to reduce the key-chain size and therefore memory usage, which also enhances resilience.

We emphasize that our main objective in the proposed approach is to improve the scalability of BIBD-based schemes and enhance the key share probability of the hybrid symmetric design.

The rest of the paper is organized as follows. Section 2 presents background that is used throughout the paper. It further discusses the related work and preliminaries. Section 3 provides basic features of our system and adversarial model. Section 4 describes the proposed approach and its analysis in detail. Section 5 compares the performance of the proposed approach with that of hybrid symmetric design. Finally, Section 6 concludes the paper and highlights the future research directions.

2. BACKGROUND AND RELATED WORK

In the last few years, with the increasing use of WSNs in many applications, security and key management issues become an essential concern in such networks. In this section, we focus on some key pre-distribution schemes more related to our work. We follow by explaining a special type of combinatorial design, which is the fundamental basis for our proposed approach.

2.1. Security in wireless sensor network

Security has been a major concern in network design and especially in WSNs. Several applications require some secure infrastructures to protect the exchanged data from malicious activity. According to the security requirements in WSNs and resource constraints in such networks [9], two sensor nodes, which need to establish communication, require some type of secure mechanism among which pairwise schemes have gained interesting attention in the literature [2,4]. Pairwise schemes work as follows: Each node is assigned a set of keys, that is, *key chain*, to be used in communication with other nodes. If two nodes need to establish a secure connection, they have to be within each others radio range and also possess common keys. Moreover, if such direct link does not exist between these nodes, communication is established through a secure multi-hop path. Figure 2 demonstrates an example of such path in a WSN.

Various approaches have been proposed to attain pairwise security in WSNs. One simple solution is to utilize unique pairwise keys for each pair of nodes in the network. The main drawback of such scheme is the memory overhead for large network size because it leads to storing

DOI: 10.1002/sec

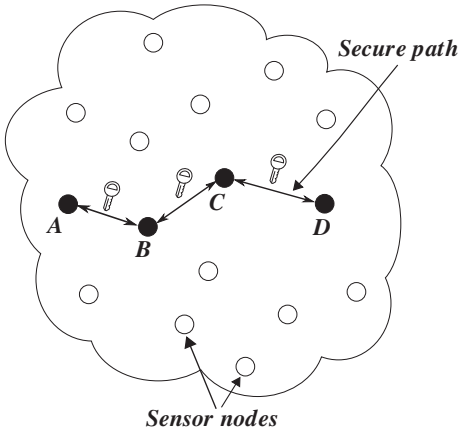


Figure 2. An example of a secure path in wireless sensor network.

$N - 1$ keys in each node where N is the network size. Another disadvantage of this scheme is its scalability. In another interesting approach [10], a randomized key distribution scheme based on random graphs has been proposed in which each pair of nodes is connected to each other with some probability p. As WSNs need sufficient connectivity in order to carry out the planned functionality, deterministic key distribution schemes have been studied in the literature [2,3,5], which seem to enhance the probability of key share.

2.2. Key pre-distribution

A key pre-distribution scheme consists of three phases: *key pre-distribution*, *shared-key discovery*, and *path-key establishment*. In the first phase, a key chain that consists of several keys is assigned to each sensor node by KDC from a key pool. Any pair of nodes, which need to communicate with each other and are in each others radio range, must find at least a common key in the shared-key discovery phase. The two nodes accomplish this phase by exchanging the list of their key identifiers. If they do not share one common key with each other, they may establish a secure path using one or more intermediate nodes, along which each pair of nodes shares a common key. This last phase is the path-key establishment [11].

As mentioned earlier, key pre-distribution schemes can be classified into three categories: probabilistic, deterministic, and hybrid. Several approaches proposed in each classification of key pre-distribution schemes are as follows. The probabilistic approaches have been studied by many researchers among which Eschenauer and Gligor [11] and Chan *et al.* [10] were the first to propose random key pre-distribution schemes in WSNs based on random-graph theory. Qian [12] propose a key pre-distribution scheme in which a hash function is used to improve resilience against node capture attack. These approaches do not guarantee that each pair of nodes has a common key. In [13], Li *et al.* propose a threshold for random key pre-distribution schemes by which they guarantee that each node in the network can establish a secure path with its ℓ-hop neighbors. Catakoglu and Levi [14] propose an uneven key pre-distribution scheme for mobile WSNs, which uses multiple distinct key pools for each generation of nodes that improves resilience of the network.

As shown in Figure 1, deterministic category can be further categorized into *matrix-based*, *polynomial-based*, and *combinatorial-based* schemes [5]. In [15], Blom propose a matrix-based approach for establishing pairwise keys. Chien *et al.* [16] extend Blom's scheme to improve resilience. In the second class of deterministic schemes, polynomial-based key pre-distribution approach proposed by Blundo *et al.* [17]. This scheme uses a bivariate t-degree symmetric polynomial to establish secure connection. In [18], Wang and Chen propose a grid-based pairwise key pre-distribution scheme, which uses multiple polynomials for each row, each column, and each diagonal in the grid.

There are several combinatorial designs such as *block designs*, *transversal designs*, and t-designs [19], which can be used as deterministic approaches for key pre-distribution purpose. Çamtepe and Yener [8] propose *symmetric design* based on BIBD, which provides full connectivity in the network. Bechkit *et al.* [20] propose another key pre-distribution approach based on unital design theory to improve scalability while providing good connectivity.

Several schemes exist in the hybrid category, which inherit benefits of both probabilistic and deterministic schemes to enhance the aforementioned metrics. Matrix-based hybrid approach has been studied in [21] and [22]. Liu *et al.* [23] propose a polynomial pool-based approach, which is a combination of the random scheme proposed by Eschenauer and Gligor with the Blundo's scheme [17]. Çamtepe and Yener [8], Chakrabarti *et al.* [24], and Kavitha and Sridharan [25] propose hybrid designs for key pre-distribution in sensor networks, which employ combinatorial designs.

2.3. Key pre-distribution based on combinatorial design

Various deterministic key pre-distribution approaches have been proposed, which most of them suffer from memory overhead, computation and communication complexity, which increase the energy consumption. Combinatorial designs have been utilized to alleviate these issues.

Çamtepe and Yener [8] propose a key pre-distribution scheme using symmetric BIBD. Another approach based on the symmetric BIBD scheme [8] has been proposed by Srinivasa *et al.* [26] in which multiple key spaces are constructed out of a key pool instead of a single key space. In another study, Lee and Stinson [27] use transversal design for key pre-distribution. Shafiei *et al.* [28] propose a method using expander graphs to deterministically distribute key chains. Addya and Turuk [29] use Steiner triple system, which is a combinatorial design to pre-distribute keys. A triangular partially BIBD-based scheme is proposed by Ruj and Roy [30]. Recently, Ruj *et al.* [31]

use strong Steiner trades for key distribution in static and mobile WSNs, which improve resilience against node capture attack. They also propose a triple-key distribution scheme in which every three nodes share a common key.

The goal of the combinatorial design theory is to partition various elements of a finite set into subsets such that it satisfies certain properties. A particularly interesting combinatorial design is the BIBD. In what follows, we provide some properties of BIBD.

Definition 1. *A (v, k, λ)-BIBD or equivalently (v, b, r, k, λ)-BIBD is a design in which v distinct objects are arranged into b blocks where each block contains exactly k distinct objects and each object occurs in exactly r different blocks such that each pair occurs together in exactly λ blocks. In particular, a BIBD is called symmetric BIBD when $b = v$ and $r = k$.*

A $(q^2 + q + 1, q + 1, 1)$-BIBD is called a *projective plane* of order q, and a $(q^2, q^2 + q, q + 1, q, 1)$-BIBD is considered as an *affine plane* of order q, where $q \geq 2$ [32].

The following theorems are popular theorems in combinatorial design theory. For proof, see [32].

Theorem 1. *For every prime power $q \geq 2$,*

- *There exists a symmetric $(q^2 + q + 1, q + 1, 1)$-BIBD (i.e., a projective plane of order q).*
- *There exists a $(q^2, q, 1)$-BIBD (i.e., an affine plane of order q).*

Definition 2. *A Latin square of order q is a $q \times q$ array of q symbols such that each symbol occurs only once in each row and in each column. Suppose that L_1 and L_2 are two Latin squares of order q. So L_1 and L_2 are Orthogonal Latin Squares if for every $x = L_1(i, j)$ and for every $y = L_2(i, j)$, there exists a unique cell (i, j), which contains (x, y). A set of n Latin squares $(L_1, L_2, \ldots, L_n)$ of order q are Mutually Orthogonal Latin Squares (MOLS) if they are orthogonal in pairs.*

Theorem 2. *Let $q \geq 2$. Then, the existence of each of the following designs implies the existence of the other two designs:*

(1) $q - 1$ MOLS(q);
(2) an affine plane of order q;
(3) a projective plane of order q.

Therefore, an affine plane can be constructed using $q - 1$ MOLS of order q, and then, it can be converted to a projective plane, which is a symmetric $(q^2 + q + 1, q + 1, 1)$-BIBD.

The construction of symmetric (v, k, λ)-BIBD can be summarized as follows:

- Considering N as the number of nodes in the network;
- Finding the minimum prime power q such that $q^2 + q + 1 > N$;
- Generating $q - 1$ MOLS of order q;
- Generating q^2 blocks of affine plane of order q;
- An affine plane is basically a projective plane, which is a symmetric $(q^2 + q + 1, q + 1, 1)$-BIBD.

Çamtepe and Yener [8] propose a so-called symmetric key pre-distribution design based on symmetric (v, k, λ)-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. Each block is generated according to Definition 1 and then assigned to each node as a key chain. Mapping from symmetric BIBD to key pre-distribution is demonstrated in Table I.

The main advantage of their scheme is that it provides full connectivity between any pair of nodes in the network. However, adding more nodes to the network calls for larger key pool and hence relatively large key chains, which reduces the scalability of the scheme. Moreover, memory usage of the approach is considerable when the number of nodes grows. In the case of resilience, because providing higher connectivity leads to lower resilience, symmetric design gains full connectivity at the cost of diminishing the resilience. To address these problems, Çamtepe and Yener [8] proposed a hybrid design according to which the complement of each block is used in order to provide key chains for additional nodes.

Let $D = (v, k, \lambda)$ be a block design with a set $|S| = v$ objects and $B = \{B_1, B_2, \ldots, B_b\}$ of $|B| = b$ blocks in which every block comprises exactly k objects. In a complementary setting, $\bar{D}$ consists of the complement blocks $\bar{B}_i = S - B_i$ for $1 \leq i \leq b$. The block design $\bar{D}$ has parameters $(v, b, b - r, v - k, b - 2r + \lambda)$, where $(b - 2r + \lambda > 0)$ in

Table I. Mapping from symmetric balanced incomplete block design to key pre-distribution.

Symmetric BIBD	Key distribution
Object set (S)	Key pool (KP)
Object set size ($\|S\| = v = q^2 + q + 1$)	Key-pool size ($\|KP\| = v = q^2 + q + 1$)
Blocks	Key chains
Number of blocks ($b = q^2 + q + 1$)	Number of key chains ($b = q^2 + q + 1$)
Number of objects in a block ($k = q + 1$)	Number of keys in a key chain ($k = q + 1$)
Number of blocks containing an object ($r = q + 1$)	Number of key chains containing a key ($r = q + 1$)
Number of shared objects between two blocks ($\lambda = 1$)	Number of shared keys between two key chains ($\lambda = 1$)

BIBD, balanced incomplete block design.

DOI: 10.1002/sec

which $\bar{D} = (v, v-k, v-2r+\lambda)$ is a symmetric design if and only if $D = (v, k, \lambda)$ is a symmetric design.

Consider a sensor network of N nodes, where each node can store at most K keys because of its memory limitations. In hybrid symmetric design approach [8], the largest prime power q is considered in a way that $q + 1 \leq K$. Then, b blocks of size $q + 1$ are generated and assigned to M nodes as key chains, where $M < N$. Among k-subsets of the complementary design, $N - b$ blocks are randomly selected for each of the remaining $N-M$ nodes. The hybrid symmetric design improves scalability and resilience of the network by sacrificing key sharing probability of the core symmetric design [5].

To reduce the memory usage of the symmetric design, Srinivasa *et al.* [26] propose a multiple key-space approach based on symmetric BIBD. For a network of size N, they consider a prime power n such that $n^2 + n + 1 > N$ and construct a symmetric design from key pool P. In this scheme, the nodes are partitioned into k_n groups, and each sensor node belonging to a group is assigned a key chain from the corresponding key space, which is a subset of the key pool P. Therefore, there are k_n key spaces such that each of which contains $m^2 + m + 1$ blocks (key chains), where m is a prime power. As each key space is constructed on the basis of $(m^2 + m + 1, m + 1, 1)$ design, each pair of nodes, which is assigned key chains from the same key space, shares a common key, while the nodes, which are assigned key chains from different key spaces, may or may not share a common key. The values of m and k_n are selected in such a way that the minimum number of additional key chains is generated by the design. The main advantage of this scheme is that it reduces the key-chain size and memory usage compared with the symmetric design. This approach provides the same resilience as the symmetric design yet decreases the probability of key share and scalability.

3. MODEL AND ASSUMPTIONS

This section provides the basic characteristics and assumptions of our scheme. Detailed description is deferred to the next section.

3.1. System model

Suppose a WSN comprises of N sensor nodes randomly deployed in the region of interest. We assume that each sensor node is pre-loaded with a key chain (including key identifiers) according to our proposed scheme, which will be explained in Section 4. We consider a key pre-distribution scheme consists of three phases. In the key pre-distribution phase (as the first phase), the base station or KDC generates two key pools and a number of key chains based on the proposed algorithm and then assigns a key chain to each sensor node before the deployment of the network. After the deployment phase, sensor nodes, which reside in the communication range of each other, perform the shared-key discovery phase. In this phase, each pair of neighboring nodes exchanges the list of their key identifiers to find the shared keys. The last phase is path-key establishment in which two nodes that do not share any common key establish a secure path through other nodes in the network.

3.2. Adversarial model

We suppose that the key pre-distribution phase of our proposed scheme is secure, because it is performed before the deployment of the network. Therefore, an adversary cannot obtain any information about the key pools and key chains from this phase. We also assume that the shared-key discovery phase is attack-free, because we only exchange the key identifiers as explained in [11]. So an attacker cannot access the keys stored in each node without capturing that node. He or she also cannot spoof the identity of the node to communicate with other nodes, without compromising the keys stored in that node. We assume that whenever a sensor node is captured by an attacker, all the keys stored in that node are revoked from other nodes' key chains. To this end, KDC broadcasts a revocation message containing captured keys' identifiers. Consequently, all the links, which were secured with the compromised keys, will be broken. It is worth mentioning that an attacker cannot recognize which nodes are assigned key chains from which key pool after network deployment. Therefore, he or she cannot selectively capture nodes based on a specific key-pool values.

The characteristics of WSNs make such networks vulnerable against various types of attacks. There is no comprehensive solution to resist against all kinds of attacks. Node capture attack is a general and serious attack, which affects security credentials of WSNs and considered as the first step for other kinds of attacks [33–36]. In this paper, we only focus on node capture attack and leave evaluating of the other kinds of attacks for future work.

4. THE PROPOSED APPROACH

We have modified the hybrid symmetric design [8] to address the problem of low key share probability. Let N be the number of nodes in the network. We propose a key pre-distribution scheme to decide on choosing N key chains from two key pools and assign them to sensor nodes. We recall that this key generation phase is performed by the KDC before the deployment of sensor network.

To generate key pools and key chains, 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 (key chains) of size $q+1$, where objects come from object set KP_1, which refers to the first key pool, that is, a set of v keys. Then, we assign these b blocks as well as the corresponding key identifiers to b nodes, where $b < N$. For the remaining $N-b$ nodes, instead of generating complementary design as proposed in [8], we use another symmetric BIBD with the same parameters as the first

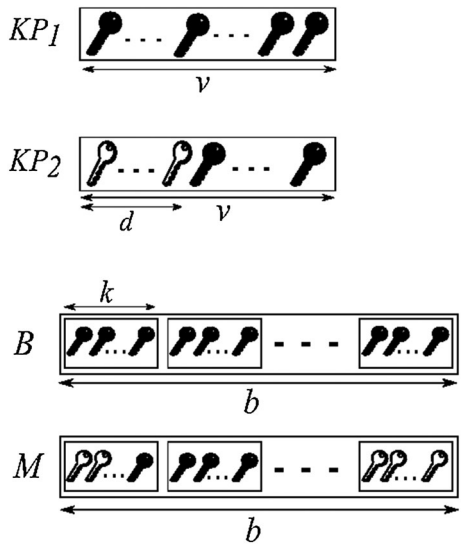


Figure 3. An example of the proposed approach.

symmetric design, but with a new object set KP_2, which refers to the second key pool, that is, a set of v keys. We introduce a parameter, called d, which denotes the number of different keys between KP_1 and KP_2. Thus, KP_2 is constructed in a way that it comprises d different keys from KP_1 and the remaining b-d keys are the same. Finally, we assign $N-b$ blocks randomly selected from the blocks that are generated from KP_2, to the remaining $N-b$ nodes along with the corresponding key identifiers. Our proposed key pre-distribution approach for a sensor network of size N can be summarized in the Algorithm 1. Figure 3 shows an example to clarify the aforementioned algorithm.

Example 1. Consider a network with $N = 10$ nodes. According to Algorithm 1, we set $q = 2$. Then, we construct a $(7, 7, 3, 3, 1)$-symmetric design. Let $KP_1 = \{1, 2, 3, 4, 5, 6, 7\}$ be a set of $v = 7$ objects (keys). We can generate $b = 7$ blocks (key chains) as $B = \{(1, 2, 3), (1, 4, 5), (1, 6, 7), (2, 4, 6), (2, 5, 7), (3, 4, 7), (3, 5, 6)\}$. As it can be observed, each key chain contains $k = 3$ keys, every key appears in $r = 3$ key chains, and each pair of distinct keys exists in $\lambda = 1$ key chain. To generate the second key pool, let $d = 1$ and thus $KP_2 = \{1, 2, 3, 4, 5, 6, 8\}$. Then, we generate $b = 7$ key chains as $M = \{(1, 2, 3), (1, 4, 5), (1, 6, 8), (2, 4, 6), (2, 5, 8), (3, 4, 8), (3, 5, 6)\}$. Finally, we assign key chains from B to seven random selected nodes out of 10 nodes, for example, $(1, 2, 3) \rightarrow node_1$ and $(2, 5, 7) \rightarrow node_2$. Furthermore, the remaining three nodes are assigned key chains from M, for instance, $(2, 5, 8) \rightarrow node_9$.

As the symmetric BIBD guarantees full connectivity of every pair of nodes, when both nodes are assigned key chains selected from the same set of blocks, that is, either M or B, the probability that these nodes share a common key in our approach is 1. On the other hand, for small values of d, each pair of nodes, which is equipped with key chains from different set of blocks, may share a common key with a good probability, that is, P_{MHS}, which will be discussed later. If they do not share a common key directly, they can communicate through a key path. As there is a trade-off between connectivity and resilience, in order to have better resilience, we can choose larger values for d. Therefore, we can state that our proposed approach is application specific, because by choosing appropriate values for d, we can fulfill each applications' requirements in terms of connectivity or resilience.

Algorithm 1: Modified hybrid symmetric design

Input: N
Find the largest prime number q
where $q^2 + q + 1 < N$;
Generate the first symmetric
$(q^2+q+1, q+1, 1)$-BIBD with the following key pool:

- $KP_1 = \{K_1, K_2, \ldots, K_v\}$ containing v objects,

Generate b blocks $B = \{B_1, B_2, \ldots, B_b\}$ from KP_1;
Choose a number d where $0 < d \leq q^2 + q + 1$;
Generate the second symmetric
$(q^2+q+1, q+1, 1)$-BIBD with the following key pool:

- $KP_2 = \{K'_1, K'_2, \ldots, K'_v\}$ containing v objects,
- KP_2 is generated in a way that d keys differ from KP_1 and other keys are the same,

Generate b blocks $M = \{M_1, M_2, \ldots, M_b\}$ from KP_2;
Assign b blocks from B to b nodes $(b < N)$;
Choose $N - b$ blocks from M in a random manner and assign them to $N - b$ remaining nodes.

4.1. Analysis of the proposed approach

In what follows, we provide an analysis of connectivity, scalability, and resilience of the proposed scheme (MHS design) compared with that of hybrid symmetric design. Various notations that are used in this section are summarized in Table II.

4.1.1. Connectivity.

According to the analysis in [8], the probability that any pair of nodes share at least a common key in the hybrid symmetric design is limited to

$$P_{HSYM} \leq Q_{BB} + Q_{HB} + P_H Q_H + Q_{HH} \quad (1)$$

and

$$P_{HSYM} \geq Q_{BB} + 0.5Q_{HB} + P_H Q_H + Q_{HH} \quad (2)$$

Table II. List of notations that are used in the paper.

Variable	Description
N	Number of nodes
q	A prime number that satisfies certain conditions
d	Number of different keys between two considered key pools
P_{HSYM}	Probability of a node having a common key with every other nodes in the hybrid symmetric design
P_{MHS}	Probability of a node having a common key with every other nodes in the modified hybrid symmetric design
P_{OMHS}	Probability of a node having a common key with every other nodes in the optimized modified hybrid symmetric design
KP_i	A set of keys as key pool i
P_{BB}	Probability that a pair of selected key chains is generated from KP_1
P_{MM}	Probability that a pair of selected key chains is generated from KP_2
P_{MB}	Probability that a pair of selected key chains is generated from KP_1 and KP_2
P^*	Certain probability of key share for various scenarios
$\mathcal{A}_c$	Event that the adversary captures c nodes and thus c key chains
C_i	Event that a key chain, which includes key i, is compromised
l_i	Event that link L uses key i to communicate with another node

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,

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

Similar to the hybrid symmetric design, in our approach, considering the set $B \cup M$ of blocks, every pair of blocks (α, β) selected for assigning to a pair of nodes can be one of the following three types:

- Type-BB: $\alpha \in B$ and $\beta \in B$,
- Type-MM: $\alpha \in M$ and $\beta \in M$,
- Type-MB: ($\alpha \in M$ and $\beta \in B$) or ($\alpha \in B$ and $\beta \in M$).

The probability that any pair of blocks from the first symmetric design (in which blocks are generated from KP_1) have one common object is $Pr_{BB} = 1$ (according to the features of symmetric BIBD).

Similarly, the probability that any pair of blocks from the second symmetric design (in which blocks are generated from KP_2) have one common object is $Pr_{MM} = 1$.

Moreover, the probability that any pair of blocks (α, β), where ($\alpha \in B$ and $\beta \in M$) or ($\alpha \in M$ and $\beta \in B$) have at least a common object is $Pr_{MB} = \frac{b-d}{b}$.

Therefore, the probability P_{MHS} that any pair of blocks share one or more objects in the MHS design is

$$P_{MHS} = P_{BB} + P_{MM} + Pr_{MB}P_{MB} \tag{3}$$

where P_i denotes the probability that a pair of selected blocks is in type i for $i \in \{BB, MM, MB\}$. Thus,

$$P_{BB} = \frac{\binom{b}{2}}{\binom{N}{2}} = \frac{b(b-1)}{N(N-1)}$$

$$P_{MM} = \frac{\binom{N-b}{2}}{\binom{N}{2}} = \frac{(N-b)(N-b-1)}{N(N-1)}$$

and,

$$P_{MB} = \frac{\binom{b}{1}\binom{N-b}{1}}{\binom{N}{2}} = \frac{2b(N-b)}{N(N-1)}$$

therefore,

$$P_{MHS} = \frac{b(b-1) + (N-b)(N+b-2d-1)}{N(N-1)} \tag{4}$$

Note that in Equation (4), the probability of key share in our approach depends on the value of parameter d. To compare the two approaches, that is, our proposed approach and the hybrid symmetric scheme, in terms of connectivity, we can state that choosing a specific value for d yields a precise probability of key share in our approach. However, according to Equations (1) and (2), the probability of key share in the hybrid symmetric design is bounded and may not be specific.

Table III. Comparison of the proposed approach and the hybrid symmetric design in terms of the probability of key share.

$N = 800$		$q = 23$			$0.78 \leq P_{HSYM} \leq 1$	
d	50	100	150	200	250	300
P_{MHS}	0.962	0.923	0.884	0.846	0.807	0.769
$N = 1700$		$q = 37$			$0.857 \leq P_{HSYM} \leq 1$	
d	100	200	300	400	500	600
P_{MHS}	0.980	0.960	0.939	0.919	0.899	0.878
$N = 10500$		$q = 101$			$0.981 \leq P_{HSYM} \leq 1$	
d	1 100	2100	3100	4100	5100	6100
P_{MHS}	0.996	0.992	0.989	0.985	0.982	0.978

Table III summarizes the probability of key share results obtained from Equations (1), (2), and (4) for the hybrid symmetric scheme (P_{HSYM}) and the proposed approach (P_{MHS}). We have evaluated the schemes with varying number of nodes: $N = 800, N = 1700, N = 10\,500$, and several values for d.

Our approach is also preferable from another aspect. As it can be seen in Table III, the value of d plays an important role in the connectivity of the network. Small values of d result in higher probability of key share, whereas large values of d lead to lower connectivity. Thus, this parameter can be useful for situations in which a network designer wants to ensure a certain probability of key share (P^*). The following equation can be used to obtain the suitable value for d.

$$d = \frac{(N-b)(N+b-1) - P^*N(N-1) + b(b-1)}{2(N-b)} \tag{5}$$

4.1.2. Scalability.

In the proposed approach, we have considered two key pools of size $v = q^2 + q + 1$ in such a way that they differ from each other in d keys. We select d different objects from KP_1 in an unordered manner and replace them with new objects, where $0 < d \leq q^2 + q + 1$. So we have d-combinations for all d subsets of the KP_1. Therefore, we can support network sizes up to

$$\sum_{d=1}^{v} \binom{v}{d} = 2^{q^2+q+1} - 1 \tag{6}$$

while the maximum network size that the hybrid symmetric design can support is determined in [8] as

$$\binom{v}{k} = \binom{q^2+q+1}{q+1} \tag{7}$$

where $k = q + 1$ is the key-chain size.

Note that our approach outperforms the hybrid symmetric scheme in terms of scalability. The proposed approach supports addition of new nodes after network deployment without a need to re-organizing the network and keys stored in each sensor node. As we explained earlier, we consider two same key pools with d different keys to generate a set of key chains for assigning to each sensor node before the deployment of the network. As it can be realized from Algorithm 1, in MHS scheme, the number of generated key chains is more than the initial number of nodes in the network. Therefore, additional nodes can be deployed at any time assigning a key chain from the remaining set of pre-produced key chains without the need for re-organizing the key pool and key chains. If the number of newly added nodes be more than available key chains, we can simply choose another d keys from the KP_1 and replace them with new keys. Using Algorithm 1, we will be able to generate b new key chains to assign to new nodes without the need for re-keying in previously deployed nodes in the network. We can consider this new key pool as KP'_2, and the same analysis as the previous subsection could be performed. Referring to Equation (4), we can state that this newly added nodes may share a common key with the other existing nodes in the network with a good probability.

4.1.3. Resilience.

We consider resilience as the probability that a link is compromised when an attacker captures c randomly selected nodes and their key chains. Let $\mathcal{A}_c$ denotes the event that the adversary captures c nodes and thus c key chains. We are interested in computing the probability that link L is compromised, which can be defined as follows:

$$Pr(L \mid \mathcal{A}_c) = \sum_{i=1}^{v} Pr(l_i)\, Pr(C_i \mid \mathcal{A}_c) \tag{8}$$

where l_i denotes the event that link L uses key i to communicate with another node and C_i denotes the event that a key chain, which includes key i, is compromised.

In our proposed approach, each key exists in $r = q + 1$ key chains, and two communicating nodes must have a common key i in their key chains. We have two key pools and two key chain sets each of which has $b = q^2 + q + 1$ key chains. Let the number of key chains in the first and the second key chain sets be b_1 and b_2, respectively, where $b_1 = b_2$. So, the probability that a link between two nodes is secured using key i is

$$Pr(l_i) = \frac{\binom{2r}{2}}{\binom{b_1+b_2}{2}} = \frac{\binom{2q+2}{2}}{\binom{2q^2+2q+2}{2}} = \frac{(q+1)(2q+1)}{(q^2+q+1)(2q^2+2q+1)} \quad (9)$$

Moreover, the probability that the key i appears in one or more of c compromised key chains is

$$Pr(C_i \mid \mathcal{A}_c) \leq 1 - \frac{\alpha+\beta+\gamma}{\binom{b_1+b_2}{c}} \quad (10)$$

where

$$\alpha = \binom{b_1+b_2-2r}{c}$$

in which we consider $b_1 + b_2 - 2r$ as the number of key chains that does not contain the key i if the key is selected from the common keys between two key pools.

$$\beta = \binom{b_1-r}{c}$$

in which we consider $b_1 - r$ as the number of key chains that does not contain the key i if the key is selected from the keys, which appears only in KP_1.

and

$$\gamma = \binom{b_2-r}{c}$$

in which we consider $b_2 - r$ as the number of key chains that does not contain the key i if the key is selected from the keys, which appears only in KP_2.

Substituting each variable in Equation (10) with its formula yields

$$Pr(C_i \mid \mathcal{A}_c) \leq 1 - \frac{\binom{2q^2}{c} + 2\binom{q^2}{c}}{\binom{2q^2+2q+2}{c}} \quad (11)$$

Therefore, the probability that a link is compromised when c key chains are captured by an attacker can be computed as

$$\begin{aligned} Pr(L \mid \mathcal{A}_c) &= \sum_{i=1}^{q^2+q+1} Pr(l_i) Pr(C_i \mid \mathcal{A}_c) \\ &= \frac{2q^2+3q+1}{2q^2+2q+1} Pr(C_i \mid \mathcal{A}_c) \\ &\simeq Pr(C_i \mid \mathcal{A}_c) \\ &\leq 1 - \frac{\binom{2q^2}{c} + 2\binom{q^2}{c}}{\binom{2q^2+2q+2}{c}} \end{aligned} \quad (12)$$

which is the upper bound for the resilience of our proposed scheme.

The probability that a link is compromised when an attacker captures x key chains is computed by Çamtepe and Yener in [8] for the symmetric design as

$$Pr(L \mid \mathcal{A}_x) = 1 - \frac{\binom{q^2}{x}}{\binom{q^2+q+1}{x}} \quad (13)$$

Thus, we can state that our proposed approach improves the resilience against node capture attack compared with the symmetric design, because the upper bound for $Pr(L \mid \mathcal{A}_c)$ obtained by our proposed approach in Equation (12) is obviously smaller than that of symmetric design, which is demonstrated in Equation (12).

As regards the resilience and connectivity are orthogonal properties, trade-offs among them must be carefully established. Parameter d establishes such a trade-off as it varies from 0 to $q^2 + q + 1$ because of the need for better probability of key share or better resilience. For small values of d as more keys are shared between the two key pools, the probability of key share increases while the resilience decreases because by compromising a node, more keys from two key pools are affected. However, for large values of d as more keys are different between the two key pools, the resilience increases while the connectivity of the network decreases. Therefore, we can establish a trade-off between connectivity and resilience based on application requirements. This is the application-specific property of our proposed scheme.

Consider a sensor network of size N, where $N > b$ and b denotes the number of generated blocks on each key pool. The proposed approach assigns b blocks, which are generated from the KP_1, to b nodes and then $N - b$ blocks, which are generated from KP_2, to the remaining $N - b$ nodes. Note that, for network sizes that $N - b$ is not large enough, only a few nodes are assigned key chains generated from KP_2. In this case, the proposed approach behaves almost the same as symmetric design [8], and the resilience decreases. However, if the difference between N and b is high, more nodes are assigned keys from KP_2. Therefore, our scheme provides better resilience and outperforms hybrid symmetric design.

For example, assume a network consists of $N = 1500$ nodes. We consider $q = 37$ and generate $b = 1407$ blocks from each key pool. Then, our approach assigns 1407 blocks, generated from KP_1, to 1407 nodes and 93 blocks, which are generated from KP_2, to the remaining 93 nodes. Now, if we assume a network with $N = 1700$ nodes with the same value for q, the approach assigns 1407 blocks from KP_1 to 1407 nodes and 293 blocks generated from KP_2 to the remaining 293 nodes. In the latter case, we provide better resilience as more nodes are assigned keys from the second key pool.

4.2. Optimized modified hybrid symmetric design

As sensor nodes are small devices with limited memory, it is desirable to have a key pre-distribution scheme, which offers low memory usage. In this section, we propose an alteration to the MHS approach—called optimized MHS (OMHS)—in order to reduce memory consumption and improve resilience. This scheme has better performance for large-scale networks compared with MHS and hybrid symmetric schemes.

Consider a network of size N. We select the smallest prime number q such that $q^2 + q + 1 > \frac{N}{2}$ instead of $q^2 + q + 1 < N$ and generate two key pools of size $q^2 + q + 1$ as mentioned in Section 4. As a result, for the same N, we can choose less value for q. Considering key-chain size $k = q + 1$, as q decreases, k also reduces. Therefore, memory consumption is improved.

Since in this approach almost $\frac{N}{2}$ of the nodes are assigned key chains from KP_1 and the remaining nodes are assigned key chains from KP_2, it can provide better resilience than hybrid symmetric and MHS schemes while decreasing the probability of key share. However, connectivity strongly depends on the value of d. Connectivity and scalability of the OMHS scheme can be computed the same as MHS design using Equations (4) and (6). Also, as well as the MHS approach, we can use Equation (5) to obtain an appropriate value for d to ensure a certain probability of key share.

For example, for $N = 10\,500$, we can select $q = 73$ instead of $q = 101$ (which we selected for MHS design). As a result, we will obtain almost 27% decrease in key-chain size ($k = q + 1$) and memory usage. In this case, each key pool contains 5403 keys, and the same number of blocks is generated for assigning to each node. Thus, 5403 nodes are assigned key chains generated from KP_1, and the remaining 5097 nodes are given key chains generated from KP_2. As a result, if C nodes are captured, less fraction of links in the network is compromised, and thus, resilience is improved.

5. EXPERIMENTAL RESULTS

We carried out extensive simulations to evaluate our proposed approach. Numerous validation experiments have been established. However, for the sake of specific illustration, validation results are presented for limited number of scenarios. We adopted 95% confidence level to make sure that, on average, the confidence interval, which is calculated using t-student distribution and standard error, contains the true values around 95% of the time. These simulations allowed us to change parameters d and C (i.e., Number of captured nodes), and check the sensitivity of our schemes to these parameters. We have implemented the hybrid symmetric design along with our proposed approaches (MHS and OMHS schemes).

To compare the schemes, we use the following evaluation metrics:

- *Connectivity:* We use connectivity to refer to the probability that any two neighboring nodes have at least one common key in their key chains. It is one of the most important efficiency metrics in WSNs, because low connectivity can lead to higher energy consumption and network partitioning in some network topologies.
- *Resilience against node capture:* We consider resilience as the fraction of communication links compromised by an attacker if C nodes are captured.

We present our simulation analysis in two subsections. The first subsection evaluates the performance of the MHS scheme, and the second subsection investigates the efficiency of the OMHS approach.

5.1. Modified hybrid symmetric design

Simulation results approve our analytical results, which we obtained for our proposed approach in Equations (4) and (12).

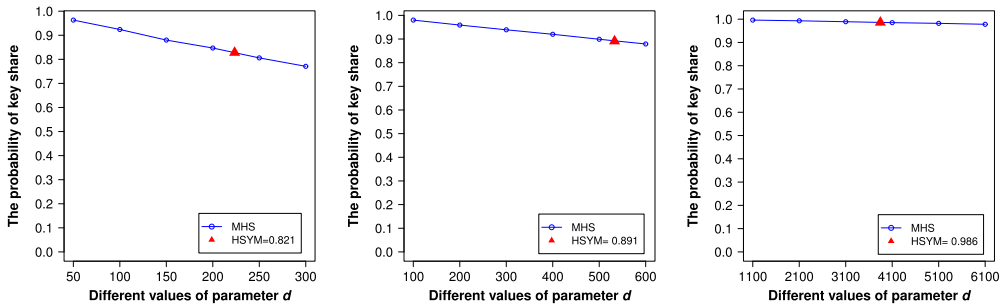
Connectivity - Figure 4 demonstrates connectivity estimated by our scheme (MHS) and the hybrid symmetric design (HSYM) for $N = 800, N = 1700$, and $N = 10\,500$ with different values of d. We consider q in such a way that $q^2 + q + 1 < N$, and therefore, each key-pool size, that is, $| KP | = q^2 + q + 1$ for each network size equals 553, 1407, and 10 303 for $N = 800, N = 1700$, and $N = 10\,500$, respectively. Moreover, the key-chain size, that is, $k = q+1$ is computed as $k = 24, k = 38$, and $k = 102$ for $N = 800, N = 1700$, and $N = 10\,500$, respectively.

Because the connectivity of our approach depends on the values of d, the line shows the probability of key share based on different values of d, while the single point illustrated on each line denotes the probability of key share extracted for the hybrid symmetric design for the same number of nodes and key-chain size. The d^* represents the point that our scheme and the hybrid symmetric scheme have the same level of connectivity.

Note that substituting different values of parameter d in Equation (4) yields the same results obtained from simulation results.

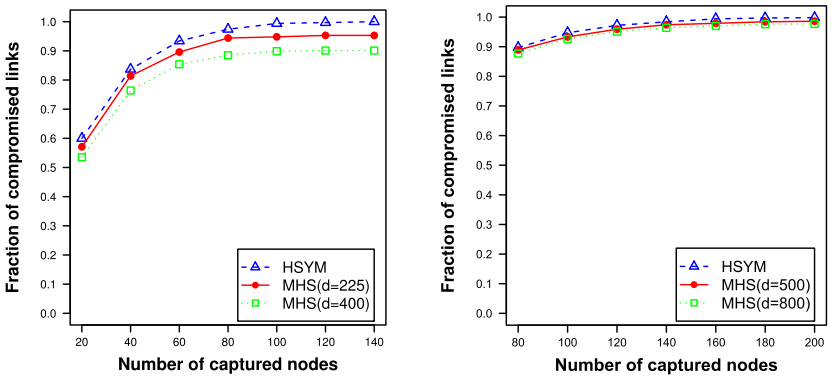
It can be observed that for small network sizes and also small values of d (where $1 < d < d^*$) our scheme outperforms the hybrid symmetric scheme, while for larger network size, both schemes obtain almost the same level of connectivity.

DOI: 10.1002/sec



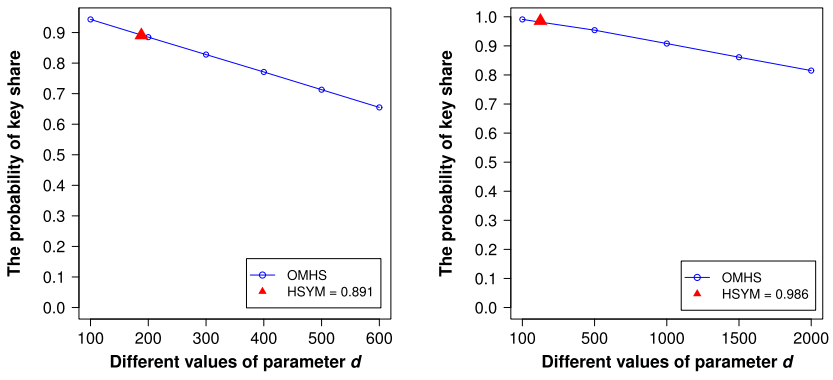
(a) $N = 800$, $d^{\star} = 221$ (b) $N = 1700$, $d^{\star} = 533$ (c) $N = 10500$, $d^{\star} = 3745$

Figure 4. Simulation results for the connectivity of the proposed scheme (modified hybrid symmetric [MHS]) and the hybrid symmetric scheme (HSYM) based on different values of N and d.



(a) $N = 800$ (b) $N = 1700$

Figure 5. Simulation results for the resilience of our scheme (modified hybrid symmetric [MHS]) versus the hybrid symmetric scheme (HSYM) based on different values of N and d.

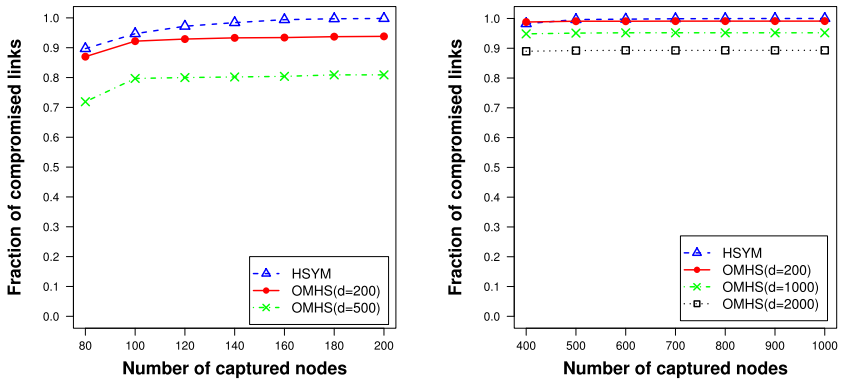


(a) $N = 1700$, $d^{\star} = 188$ (b) $N = 10500$, $d^{\star} = 144$

Figure 6. Simulation results for the connectivity of the optimized modified hybrid symmetric (OMHS) approach versus the hybrid symmetric scheme (HSYM) based on different values of N and d.

Resilience - For resilience evaluation, we assume that C captured nodes are randomly distributed within the deployment region. Figure 5 shows the resilience estimated by our scheme and the hybrid symmetric design for $N = 800$ and $N = 1700$. As can be seen in Figure 5(a), for small network sizes, our approach always has better resilience against node capture attack.

It can be realized that the upper bound for the resilience obtained by our proposed model in Equation (12) conforms to the simulation results.



(a) $N = 1700$ **(b)** $N = 10500$

Figure 7. Simulation results for the resilience of the optimized modified hybrid symmetric (OMHS) approach versus the hybrid symmetric scheme (HSYM) based on different values of N and d.

Notice that for $d = 225$, connectivity of the MHS approach is almost the same as that of HSYM. As d grows, resilience of our approach is improved while connectivity decreases. Figure 5(b) shows resilience of the two schemes for $N = 1700$. Note that for $d = 500$, both resilience and connectivity of our approach are almost the same as HSYM.

As illustrated in Figure 4, in the proposed approach, the probability of key share between each pair of nodes is more than 80% almost always. If an attacker captures all the nodes, which are assigned key chains from one of the key pools (for instance KP_2), the other remaining nodes (to which we assigned key chains from KP_1) can still communicate with each other based on the BIBD features explained in Section 4.1.1. However, as denoted in adversarial model, we believe that an attacker cannot recognize exactly which nodes are assigned key chains from KP_2.

5.2. Optimized modified hybrid symmetric design

In this subsection, we evaluate the OMHS scheme.

Connectivity - Figure 6 shows the connectivity estimated by the OMHS design and the hybrid symmetric design, that is, HSYM, for $N = 1700$ and $N = 10\,500$ with different values of d.

We consider q such that $q^2 + q + 1 > N/2$, and therefore, each key-pool size, that is, $| KP | = q^2 + q + 1$ for each network size equals $| KP | = 871$ and $| KP | = 5403$ for $N = 1700$ and $N = 10\,500$, respectively. Moreover, the key-chain size, that is, $k = q + 1$, is computed as $k = 30$ and $k = 74$ for $N = 1700$ and $N = 10\,500$, respectively.

The plot depicts the probability of key share based on different values of d, while the single point on the line corresponds to the probability of key share extracted for the hybrid symmetric design, for the same number of nodes. The size of key chains used in OMHS scheme is less than that of MHS and hybrid symmetric designs. Note that memory usage is improved at the cost of reduced connectivity.

Resilience - Considering C captured nodes that are randomly distributed within the deployment region, Figure 7 shows the resilience estimated by OMHS and the hybrid symmetric schemes for $N = 1700$ and $N = 10\,500$.

As can be seen in Figure 7, OMHS approach always has better resilience against node capture attack. Notice that for $d = 200$ (Figure 6(a)), connectivity of the OMHS approach is almost the same as that of HSYM. As d grows, resilience of our approach is improved significantly.

6. CONCLUSION

In this work, we present a modification to the hybrid symmetric key pre-distribution scheme [8] to improve scalability, key share probability, and resilience of the WSNs against node capture attack. We illustrated that by considering two similar key pools with some different keys, instead of using complementary design in the hybrid symmetric scheme, we can obtain better results for small size networks. We also presented an extension to the proposed approach, which improves memory usage and resilience for large-scale networks at the cost of reduced key share probability.

The analysis and experimental results show that our proposed MHS design and its optimized version can fulfill application-specific purposes. For applications having high connectivity need, the MHS scheme is preferred, while the OMHS is beneficial in the case of higher resilience need and low memory usage.

Our future work would target to improve other weaknesses of key pre-distribution scheme based on combinatorial design, such as low resilience against some well-known attacks. We will also extend the current work to be deployment-aware.

REFERENCES

1. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: a survey. *Computer networks* 2002; **38**(4): 393–422.
2. Simplício Jr. MA, Barreto PS, Margi CB, Carvalho TC. A survey on key management mechanisms for distributed wireless sensor networks. *Computer Networks* 2010; **54**(15): 2591–2612.
3. Chen C-Y, Chao H-C. A survey of key distribution in wireless sensor networks. *Security and Communication Networks* 2011. Wiley Online Library, DOI: 10.1002/sec.354.
4. Zhang J, Varadharajan V. Wireless sensor network key management survey and taxonomy. *Journal of Network and Computer Applications* 2010; **33**(2): 63–75.
5. Çamtepe SA, Yener B. Key distribution mechanisms for wireless sensor networks: a survey. *Technical Report*, Rensselaer Polytechnic Institute, Troy, New York, 2005.
6. Di Pietro R, Mancini LV, Mei A, Panconesi A, Radhakrishnan J. Redoubtable sensor networks. *ACM Transactions on Information and System Security (TISSEC)* 2008; **11**(3): 13:1–13:22.
7. Pattanayak A, Majhi B. Key predistribution schemes in distributed wireless sensor network using combinatorial designs revisited. *Technical Report*, Cryptology eprint Archive. Report 2009/131, 2009.
8. Çamtepe SA, Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks. *IEEE/ACM Transactions on Networking* 2007; **15**(2): 346–358.
9. Wang Y, Attebury G, Ramamurthy B. A survey of security issues in wireless sensor networks. *IEEE Communications Surveys & Tutorials* 2006; **8**(2): 2–23.
10. Chan H., Perrig A, Song D. Random key predistribution schemes for sensor networks, *Symposium on Security and Privacy*, IEEE, Oakland, California, USA, 2003; 197–213.
11. Eschenauer L, Gligor VD. A key-management scheme for distributed sensor networks, *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ACM, Washington, DC, USA, 2002; 41–47.
12. Qian S. A novel key pre-distribution for wireless sensor networks. *Physics Procedia* 2012; **25**: 2183–2189.
13. Li W-S, Tsai C-W, Chen M, Hsieh W-S, Yang C-S. Threshold behavior of multi-path random key pre-distribution for sparse wireless sensor networks. *Mathematical and Computer Modelling* 2013; **57**(11): 2776–2787.
14. Catakoglu O, Levi A. Uneven key pre-distribution scheme for multi-phase wireless sensor networks, *Information Sciences and Systems*, Springer, Baltimore, USA, 2013; 359–368.
15. Blom R. An optimal class of symmetric key generation systems, *Advances in Cryptology*, Springer, Berlin, 1985; 335–338.
16. Chien HY, Chen R-C, Shen A. Efficient key predistribution for sensor nodes with strong connectivity and low storage space, *Proceedings of the 2nd International Conference on Advanced Information Networking and Applications (AINA'08)*, IEEE, GinoWan, Okinawa, Japan, 2008; 327–333.
17. Blundo C, De Santis A, Herzberg A, Kutten S, Vaccaro U, Yung M. Perfectly-secure key distribution for dynamic conferences, *Advances in Cryptology, CRYPTO92*, Springer, Santa Barbara, California, USA, 1993; 471–486.
18. Wang N-C, Chen H-L. Improving pairwise key predistribution in wireless sensor networks, *Advances in Intelligent Systems and Applications*, Springer, Hualien, Taiwan, 2013; 521–530.
19. Anderson Ian. *Combinatorial Designs and Tournaments*, Vol. 6. Oxford University Press: London, U.K., 1997.
20. Bechkit W, Challal Y, Bouabdallah A, Tarokh V. A highly scalable key pre-distribution scheme for wireless sensor networks. *IEEE Transactions on Wireless Communications* 2013; **12**(2): 948–959.
21. Du W, Deng J, Han YS, Varshney PK, Katz J, Khalili A. A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC)* 2005; **8**(2): 228–258.
22. Lee J, Stinson DR. Deterministic key predistribution schemes for distributed sensor networks, *Selected Areas in Cryptography*, Springer, Kingston, Ontario, Canada, 2005; 294–307.
23. Liu D, Ning P, Li R. Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security (TISSEC)* 2005; **8**(1): 41–77.
24. Chakrabarti D, Maitra S, Roy B. A key pre-distribution scheme for wireless sensor networks: merging blocks in combinatorial design. *International Journal of Information Security* 2006; **5**(2): 105–114.
25. Kavitha T, Sridharan D. Hybrid design of scalable key distribution for wireless sensor networks. *IACSIT International Journal of Engineering and Technology* 2010; **2**(2): 136–141.
26. Srinivasa KG, Poornima V, Archana V, Reshma C, Venugopal KR, Patnaik LM. Combinatorial approach to key generation using multiple key spaces for wireless sensor networks, *Proceedings of the 16th International Conference on Advanced Computing and*

Communications ADCOM 2008, IEEE, Tamilnadu, India, 2008; 279–284.
27. Lee J, Stinson DR. On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs. *ACM Transactions on Information and System Security (TISSEC)* 2008; **11**(2): 1:1–1:35.
28. Shafiei H, Mehdizadeh A, Khonsari A, Ould-Khaoua M. A combinatorial approach for key-distribution in wireless sensor networks, *Proceedings of the IEEE Global Telecommunications Conference GLOBECOM 2008,* IEEE, New Orleans, LA, USA, 2008; 1–5.
29. Addya SK, Turuk AK. A technique for communication of distance node on key pre-distribution in wireless sensor networks. *International Journal of Recent Trends in Engineering and Technology* 2010; **4** (1): 87–92.
30. Ruj S, Roy B. Key predistribution using partially balanced designs in wireless sensor networks. *Parallel and Distributed Processing and Applications* 2007; **4742**: 431–445.
31. Ruj S, Nayak A, Stojmenovic I. Pairwise and triple key distribution in wireless sensor networks with applications. *IEEE Transactions on Computers* 2013; **62**(11): 2224–2237.
32. Stinson DR. *Combinatorial Designs: Construction and Analysis*. Springer: New York, 2004.
33. Cheng Y, Agrawal DP. An improved key distribution mechanism for large-scale hierarchical wireless sensor networks. *Ad Hoc Networks* 2007; **5** (1): 35–48.
34. Conti M, Di Pietro R, Mancini LV, Mei A. Emergent properties: detection of the node-capture attack in mobile wireless sensor networks, *Proceedings of the First ACM Conference on Wireless Network Security*, ACM, Alexandria, VA, USA, 2008; 214–219.
35. Conti M, Di Pietro R, Mancini LV, Mei A. Mobility and cooperation to thwart node capture attacks in manets. *EURASIP Journal on Wireless Communications and Networking* 2009; **2009**: 1-13.
36. Conti M, Di Pietro R, Gabrielli A, Mancini LV, Mei A. The smallville effect: social ties make mobile networks more secure against node capture attack, *Proceedings of the 8th ACM International Workshop on Mobility Management and Wireless Access*, ACM, Bodrum, Turkey, 2010; 99–106.