

A Novel Scalable Key Pre-distribution Scheme for Wireless Sensor Networks Based on Residual Design

Vahid Modiri¹ · Hamid Haj Seyyed Javadi² · Mohaddese Anzani²

Published online: 20 June 2017

© Springer Science+Business Media New York 2017

Abstract Key distribution is one of the most challenging security issues in wireless sensor networks. To achieve a high level of security, each pair of nodes must share a secret key in order to communicate with each other. Recently, many researchers have used combinatorial designs as key pre-distribution scheme in wireless sensor networks. In this paper, we describe a new construction of a design in combinatorial algebraic called residual design and use it for key establishment. This is the first time for application of residual design. Our approach is a highly scalable key management scheme for wireless sensor networks which provides a good secure connectivity. We show that the basic mapping from residual design to key pre-distribution has an extremely high network scalability while this mapping does not have high resilience. Therefore, we present a new approach for key pre-distribution based on residual design that improves the resilience of the network while maintaining connectivity and high scalability. We also explain that the computational cost and storage overhead is low. Performance and security properties of the proposed scheme are studied both analytically and computationally to compare our scheme to main existing schemes. The obtained results show that at equal key-ring size, our scheme provides better scalability with high connectivity and resilience.

Keywords Wireless sensor networks · Key pre-distribution · Security · Residual design

✉ Hamid Haj Seyyed Javadi
h.s.javadi@shahed.ac.ir

Vahid Modiri
va_modiri@srbiau.ac.ir

Mohaddese Anzani
anzani@shahed.ac.ir

¹ Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran

² Department of Mathematics and Computer Science, Shahed University, Tehran, Iran

1 Introduction

A wireless sensor network (WSN) is a collection of sensor nodes that have very limited storage capacity, energy and computational capabilities. WSNs have many applications such as military, environmental and habitat monitoring, vehicle monitoring, and industrial process control. Nodes in WSNs sense, process and communicate with each other over wireless links to relay the monitored data to a base station [1]. In such applications, security becomes essential since the WSN is prone to malicious attackers.

Secure communication between a pair of sensor nodes requires privacy, integrity and authentication. Therefore, any two nodes should share a common secret key. There are several key distribution and agreement approaches, known as *key agreement approaches* problem, which can be used to set-up secret keys between communicating nodes. The key agreement has been studied in general network structures [2].

Three types of key agreement schemes have been classified as *trusted server*, *self-enforcing*, and *key distribution*. There are many different types of key distribution schemes in wireless sensor networks. One of these types are mechanisms based on public-key algorithms. Public-key algorithms such as Elliptic Curve Cryptography (ECC) and RSA have high computation overhead and consume high energy in each sensor node. Power resources and limited computation of sensor nodes, makes it undesirable to use these types of algorithms. Sensor nodes may need a lot of seconds up to minutes to execute all steps of public-key algorithms and this time may increase the vulnerability of Denial of Service (DoS) attacks.

In addition, wireless sensor networks may not have good public-key infrastructure (PKI) for key distribution. Public keys should be distributed into nodes via the base station, which produces high communication overhead.

Since there is no fixed infrastructure and network configuration is unknown prior to deployment, key pre-distribution scheme (KPS) is the best solution which is used in several research studies [3, 4].

In pre-distribution schemes, a list of keys (*key-ring*) is stored into sensors before the deployment, which keys are randomly drawn from a *key-pool*.

KPSs can be random, deterministic and hybrid. In random schemes, key-rings are chosen from a key-pool in a random manner and are assigned to sensor nodes. In deterministic schemes, key-rings are chosen based on deterministic methods to provide better key connectivity between nodes. Hybrid schemes are the combination of both deterministic and random approaches to inherit best of both worlds.

A few approaches have been proposed to provide pairwise security in WSNs. A simple way is to store $N - 1$ secret pairwise keys in each node where N is network size. This scheme has full resilience against node capture, but it is impractical for networks with extremely large amount of nodes.

Eschenauer and Gligor [5] proposed a randomized key pre-distribution scheme for distributed WSNs. This approach consists of three phases: *key pre-distribution*, *shared-key discovery*, and *path-key establishment*. In the key distribution phase, a large key pool is generated and every sensor node is loaded with a fixed number of keys chosen randomly from this key pool along with their key identifiers. Then the shared-key discovery phase takes place, where two nodes in their wireless communication range, exchange the list of key identifiers from their own key-rings to find a common key. The path-key establishment phase takes place if there is no common key between a pair of nodes in a wireless

communication range. Then two nodes try to communicate with each other through a multi-hop path.

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 connection only if they share at least q keys.

Qian [7] proposed a key pre-distribution scheme in which a hash function is used to improve resilience against node capture attack. Li et al. in [8] proposed 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 neighbours.

Blom [9] 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.

In [10], a polynomial-based key pre-distribution scheme is proposed for group key pre-distribution. Blundo et al. use a bivariate t -degree symmetric polynomial to establish secure connection.

Combinatorial designs are the other methods used to design a deterministic key pre-distribution. Camtepe and Yener [11] proposed a deterministic key pre-distribution scheme by using the finite Generalized Quadrangles (GQ) and Symmetric Balanced Incomplete Block Design (SBIBD). The main advantage of this scheme is full connectivity coverage. However, the SBIBD scheme does not scale to very large networks. Lee and Stinson [12] used transversal designs (TD) which provide better resilience. Other works like are those of Ruj and Roy [13] who used Partially Balanced Incomplete Block Design (PBIBD) and of Chakrabarty et al. [14] who used merging blocks for deterministic key pre-distribution.

Ruj et al. [15] proposed a trade-based key management scheme. In combinatorial trade, there exist unique secret pairwise keys between connected nodes.

Bechkit et al. [16], proposed another key pre-distribution approach based on Unital design to improve scalability while providing good connectivity. Also, they proposed a modified unital-based key pre-distribution scheme in order to improve the network scalability.

The hybrid schemes which inherit benefits of both probabilistic and deterministic schemes have been studied by several researchers. Liu et al. [17] proposed an approach where nodes are pre-loaded with bivariate polynomials instead of keys. This approach is a combination of the random scheme proposed by Eschenauer and Gligor [5] with the Blundo's scheme [10]. Camtepe and Yener [3] and Kavitha and Sridharan [18] proposed hybrid designs for key pre-distribution in sensor networks which employ combinatorial designs. Dargahi et al. [19] proposed a key pre-distribution scheme based on combinatorial and hybrid designs. In this scheme, key-rings are selected from two key pools and are assigned to sensor nodes before the deployment of sensor network [20]. Presented key management in wireless sensor networks based on multiple key encryption methods.

1.1 Our Contributions and Organization of This Work

As pointed out, energy resources and limited computation of sensor nodes usually make it impractical to use public key algorithms, such as Diffie–Hellman and elliptic curve key agreement.

In this paper, we focus on combinatorial constructions for deterministic key pre-distribution schemes. For comparison of different schemes, many important criteria such as

“scalability”, “connectivity”, “resilience”, “storage overhead”, “communication overhead” and “computation overhead” are considered.

The contributions of our work can be summarized in the following points:

- We introduce, for the first time, the use of residual design theory as an important algebraic architecture, in key pre-distribution for WSNs. We show that the basic mapping from residual design to key pre-distribution is an extremely scalable scheme while providing good connectivity.
- We propose a modified residual based key pre-distribution scheme in order to increase the network resilience while maintaining a good scalability.
- We evaluate and compare our new scheme against main existing approaches considering different criteria. The simulated results and comparison with the mentioned approaches show that, our novelty provides better scalability with high resilience and connectivity.

This paper is organized as follows. In Sect. 2, we provide a brief overview to combinatorial design theory. In Sect. 3, we introduce our key distribution scheme and show how to map the residual design to key distribution. We present our analysis and computational results in Sect. 4. Finally in Sect. 5, we conclude.

2 Background on Combinatorial Designs

2.1 Preliminaries

A set system or design is a pair (X, \mathcal{A}) where X is a set of v elements (points) and \mathcal{A} is a finite set of subsets of X called blocks. The degree of a point $x \in X$ is the number of blocks containing x . The rank of a set system is the size of the largest block and (X, \mathcal{A}) is said to be uniform of rank k if all blocks have the same size k . A Balanced Incomplete Block Design (BIBD) is one of such designs. In the following we provide some properties of BIBD.

Definition 1 A (v, k, λ) -BIBD or equivalently (v, b, r, k, λ) -BIBD is an arrangement of v distinct objects 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.

Also in a (v, k, λ) -BIBD, we have: $\lambda(v-1) = r(k-1)$ and $bk = vr$. In particular, a BIBD is called *symmetric BIBD* when $b = v$ and therefore $r = k$ [21]. Symmetric (v, k, λ) -BIBD is denoted by (v, k, λ) -SBIBD.

A $(q^2 + q + 1, q + 1, 1)$ -BIBD with $q \geq 2$ is called a *projective plane* of order q and a $(q^2, q^2 + q, q + 1, q, 1)$ -BIBD is called an *affine plane* of order q where $q \geq 2$. For every prime power $q \geq 2$ there exists a $(q^2 + q + 1, q + 1, 1)$ -SBIBD (i.e., a projective plane of order q) and also a $(q^2, q, 1)$ -BIBD (i.e., an affine plane of order q) [21].

2.2 Related Works

There are several key pre-distribution schemes which use combinatorial techniques. Camtepe and Yener [3] proposed symmetric key pre-distribution designs based on (v, k, λ) -SBIBD with parameters $(q^2 + q + 1, q + 1, 1)$ in which q is a prime power such

that $q^2 + q + 1 \geq N$ where N is the number of nodes in the network. The proposed mapping from symmetric BIBD to key pre-distribution allows to construct $q^2 + q + 1$ key-rings from key pool of $q^2 + q + 1$ keys such that each key-ring contains $k = q + 1$ keys and each two key-rings shares exactly one common key. The main advantage of this scheme is that it provides full connectivity between any pair of nodes in the network. Since providing higher connectivity leads to lower resilience, symmetric design does not ensure a perfect network resilience. Therefore, they proposed a hybrid design according to which the complement of each block is used in order to provide key-rings for additional nodes. In hybrid design, the large prime power q is considered in a way that $q + 1 < k$. Then b of N blocks of size $q + 1$ are generated by base symmetric design. $N - b$ blocks are randomly selected among k -subset of the complementary design blocks. The hybrid design improves scalability and resilience of underlying symmetric design.

Ruj et al. [15] proposed a trade-based key pre-distribution scheme denoted Trade-KP. A $t - (v, k)$ Steiner trade (also called combinatorial trade) consists of collections $T = \{T_1, T_2\}$ where $T_i, (i = 1, 2)$ is a collection of k -elements blocks chosen from a finite set X such that each t -set chosen from X occurs in precisely the same number of blocks of T_1 , as those of T_2 . A $2 - (v, k)$ Steiner trade $T = \{T_1, T_2\}$ is said to be strong, if any block in T_1 intersects any block of T_2 in at most two elements. They proposed a new construction of strong steiner trade to establish pairwise keys in sensor networks. For a prime power q , they construct sets of k -subsets ($k \geq 4$), T_1 and T_2 from X . A k -subset of T_1 is represented by t_{ij}^1 , such that, $t_{ij}^1 = \{(x, (xi + j) \text{ mod } q) : 0 \leq x < k\}$, where $0 \leq i, j < q$. A k -subset of T_2 is represented by t_{ij}^2 , such that, $t_{ij}^2 = \{(x, (x^2 + xi + j) \text{ mod } q) : 0 \leq x < k\}$, where $0 \leq i, j < q$. This construction results in a $2 - (qk, k)$ strong Steiner trade. For mapping, each block of the set of blocks $T_1 \cup T_2$ selected for a key-ring is such that the size of key-ring is k ($0 < k \leq q$) and the scalability of the scheme is $2q^2$.

Bechkit et al. [16] proposed a unital-based key pre-distribution scheme denoted NU-KP. Given a finite set X of v points, a Unital design is a 2-design $(q^3 + 1, q^2(q^2 - q + 1), q^2, q + 1, 1)$. They proposed a basic mapping from unital design to key pre-distribution in which $b = q^2(q^2 - q + 1)$ key-rings of size $k = q + 1$ are generated from a key pool of $q^3 + 1$ keys. In order to enhance the key sharing probability while maintaining high network scalability, they presented a new unital-based key pre-distribution scheme denoted t-UKP. In this scheme, unital design blocks are generated and each node is preloaded with t disjoint blocks. In their combinatorial approach, choosing the t parameter may produce different results. In order to maintain a high key sharing probability and high scalability, they proposed to choose $t = \sqrt{q}$. The t-UKP scheme with $t = \sqrt{q}$ is denoted UKP*.

2.3 Residual Design

There are a number of easy constructions which can create new BIBDs once given the existence of a symmetric design. The relation between affine and projective planes can be generalized to other block designs. If B_0 is any block of (v, b, r, k, λ) -BIBD, then any two elements that do not belong to B_0 must occur together in λ of the remaining blocks, while any two elements of B_0 must be together in $\lambda - 1$ of the remaining blocks. It follows that the blocks $B \setminus B_0$ form a BIBD when B ranges through the remaining blocks. We shall refer to these as the residual design of the original with respect to the block B_0 . We can start with a symmetric balanced incomplete block design. The design resulting from the following theorem is known as a residual design [22].

Theorem 2 Let (V, B) be a symmetric BIBD with $B = \{B_1, B_2, \dots, B_v\}$ and $V = \{x_1, \dots, x_v\}$. Then for any i ,

$$B_1 \setminus B_i, B_2 \setminus B_i, \dots, B_{i-1} \setminus B_i, B_{i+1} \setminus B_i, \dots, B_v \setminus B_i$$

are the blocks of a $(v - k, v - 1, k, k - \lambda, \lambda)$ -BIBD of the point set $X \setminus B_i$.

Example 3 Consider $(7, 3, 1)$ -SBIBD with the blocks $B_1 = \{1, 2, 3\}, B_2 = \{1, 4, 5\}, B_3 = \{1, 6, 7\}, B_4 = \{2, 4, 6\}, B_5 = \{2, 5, 7\}, B_6 = \{3, 4, 7\}, B_7 = \{3, 5, 6\}$.

Then,

$B_2 \setminus B_1 = \{4, 5\}, B_3 \setminus B_1 = \{6, 7\}, B_4 \setminus B_1 = \{4, 6\}, B_5 \setminus B_1 = \{5, 7\}, B_6 \setminus B_1 = \{4, 7\}, B_7 \setminus B_1 = \{5, 6\}$. Clearly $B_i \setminus B_1$ for $i = 2, \dots, 7$, are the blocks of a $(4, 6, 3, 2, 1)$ -BIBD over the point set $\{4, 5, 6, 7\}$.

Suppose that a design D has the parameters $(v - k, v - 1, k, k - \lambda, \lambda)$ for some v, k and λ . One can ask whether there exists a (v, k, λ) -design of which D is a residual? The following theorem would answer this question [22].

Theorem 4 Suppose that D is a $(v - k, v - 1, k, k - \lambda, \lambda)$ -BIBD. If $\lambda = 1$ or $\lambda = 2$, there is a (v, k, λ) -design of which D is the residual.

2.4 Network Model

In this work, we construct the residual design foundation by the symmetric BIBD with parameters $(q^2 + q + 1, q + 1, 1)$. Let the i th class of residual design constructed from the point set $X \setminus B_i$ be denoted by C_i and $B_j \setminus B_i$ be denoted by B_{ij} for $i = 1, \dots, v$ and $j = 1, \dots, i - 1, i + 1, \dots, v$ respectively. Since in this work, key-rings are preloaded before node's deployment, it is necessary that classes be specified.

2.5 Construction

Using symmetric design with parameters $(q^2 + q + 1, q + 1, 1)$ to construct residual design, we consider some following properties.

Property 1 The point set of each class in our approach forms a BIBD with parameters $(v, b, r, k, \lambda) = (q^2, q^2 + q, q + 1, q, 1)$.

Proof This property results of Theorem 2. □

Property 2 Given the key-ring size $k = q + 1$ and the key pool size $v = q^2 + q + 1$, residual design can support the network size up to $N = (q^2 + q + 1)(q^2 + q)$.

Proof Since each of classes in residual design forms $(q^2, q^2 + q, q + 1, q, 1)$ -BIBD and the number of classes is exactly $q^2 + q + 1$, we can support totally $(q^2 + q + 1)(q^2 + q)$ sensor nodes. □

Property 3 The common point set of two classes has $q^2 - q$ elements.

Proof This can be shown by proving that any class C_i formed by remaining elements of $X \setminus B_i$. Consider blocks B_i and B_j in symmetric design which have $q + 1$ keys in key-ring. Then $X \setminus (B_i \cup B_j)$ has $(q^2 + q + 1) - (2q + 1)$ elements and therefore two classes C_i and C_j have $q^2 - q$ common elements. □

Property 4 Each block constructed in residual design is repeated q times.

Proof Since each element in symmetric BIBD occurs in exactly $q + 1$ different blocks and each block in residual design is constructed from $B_i \setminus B_j$, each block in residual design is repeated q times. □

Property 5 In residual design, each key appears in exactly $q^2(q + 1)$ blocks.

Proof According to residual design, each key j appears in all but $q + 1$ classes. This means that key j is coming in the point set of q^2 classes ($(q^2 + q + 1) - (q + 1) = q^2$). Since each object in point set of any class appears in $q + 1$ blocks of this class, there exist $q^2(q + 1)$ blocks containing key j . □

3 Combinatorial Design to Key Distribution

In this section we explain how residual designs are used to distribute pairwise keys to sensor nodes.

3.1 Mapping from Residual Design to Key Distribution

Consider a distributed wireless sensor network of N sensor nodes, where each sensor has a key-ring of K keys coming from a key pool P . As expressed before, we focus on an especial type of symmetric BIBD with parameters $(q^2 + q + 1, q + 1, 1)$ in which q is a prime power. Camtepe and Yener [11] proposed a symmetric design to key distribution based on $(q^2 + q + 1, q + 1, 1)$ -SBIBD. In this scheme, for a prime power $q, b = q^2 + q + 1 \geq N$ blocks are constructed. Then each generated block is assigned to each sensor node as a key-ring. Since symmetric designs guarantee that any pair of blocks have $\lambda = 1$ object in common, their scheme has full connectivity between any pair of nodes in the network. Contrary of full connectivity, adding more nodes to the network reduces the scalability of the scheme. Our basic approach is highly scalable since a great number of blocks can be generated with parameter q .

In this work, we start by developing a simple scalable key pre-distribution scheme based on residual design. We propose a basic mapping to decide on choosing key-rings from a key set of key-pool and assign them to sensor nodes before deployment (see Table 1).

Algorithm I: Residual Design

Require: N {Total number of nodes}

1. Find the minimum prime power q such that $(q^2 + q + 1)(q^2 + q) \geq N$.
 2. Generate the base Symmetric Design with parameters $(q^2 + q + 1, q + 1, 1)$.
 - v objects $P = \{a_1, a_2, \dots, a_v\}$.
 - b blocks $B = \{B_1, B_2, \dots, B_b\}$ of size $q + 1$.
 3. Generate $b' = (q^2 + q + 1)(q^2 + q)$ blocks for constructing Residual Design from the base Symmetric Design:
 - Blocks $B_{ij} = B_i \setminus B_j$ where $i, j = 1, \dots, q^2 + q + 1$.
 4. Assign blocks to specified nodes.
-

Table 1 Mapping from residual design to key pre-distribution

Residual design	Key pre-distribution
Point set ($ S $)	Key pool (KP)
Object set size ($ S = q^2 + q + 1$)	Key pool size ($ KP = q^2 + q + 1$)
Blocks	Key-rings
Number of blocks ($(q^2 + q + 1)(q^2 + q)$)	Number of key-rings
Size of a block ($k = q$)	Size of a key-ring

First, we consider the minimum prime power q in a way that $(q^2 + q + 1)(q^2 + q) \geq N$ to construct $(q^2 + q + 1, q + 1, 1)$ -SBIBD. This symmetric design can be used to construct residual designs (Theorem 2). We use residual designs which has $q^2 + q + 1$ classes where each class has q^2 elements to generate totally $b = (q^2 + q + 1)(q^2 + q)$ blocks of size q . Then the generated blocks are assigned to N sensor nodes as key-rings, where $b \geq N$. The construction algorithm is summarized in Algorithm I.

3.2 Analysis of the Proposed Approach

In this section, we provide an analysis of storage overhead, computation overhead, communication overhead, connectivity, scalability and resilience of the proposed scheme that we denote by RD-KP. The notations used in present paper are summarized in Table 2.

3.2.1 Communication Overhead

Communication overhead or multi-hop communication is the maximum indirect path length between 2 nodes. In our approach, this path length depends on the length of key-ring of the nodes that is $q + 1$. Therefore, the average key path length is $O(q)$.

Table 2 List of used notation

Notation	Definition
N	Total number of nodes in the network
N_{RD}	Number of supported sensor nodes in RD-KP
N_{RD^*}	Number of supported sensor nodes in RD*-KP
q	A prime number which satisfies certain conditions
B_i	i -th block of symmetric design
C_i	i th class of residual design constructed from point set of $X \setminus B_i$
B_{ij}	The resulting blocks of $B_j \setminus B_i$
x_{ij}	The j -th element of class i
P_{SC}	Probability that a pair of selected blocks is from same class
P_{DC}	Probability that a pair of selected blocks is from different classes
P_{RD}	Probability that a node have a common key with other nodes in RD-kp

3.2.2 Computation Overhead

In pre-distribution mechanisms, base stations execute most of computations of algorithm. In our proposed scheme, each node needs maximum time of $q + 1$ for computation. It means the average computation overhead of RD-KP would be estimated as $O(q)$.

3.2.3 Storage Overhead

By using our proposed approach based on residual design of order q , each node is assigned a key-ring corresponding to a block of design. So, each node has to store $q + 1$ disjoint keys. Therefore, memory required to store keys is $l(q + 1)$ where l is the key size.

In Table 3, we compared storage overhead, computation overhead and communication overhead of different key pre-distribution schemes rather than RD-KP.

3.2.4 Scalability

Scalability is the maximum size that the network can support. Following from the Property 2, the scalability of the wireless network would be $N = (q^2 + q + 1)(q^2 + q)$.

3.2.5 Connectivity

In wireless sensor networks the connectivity is the probability that two nodes share at least a common key. We consider blocks B_{ij} and $B_{i'j'}$ of residual design. Any pair of selected blocks can be either one of the following two types:

1. Type SC: $i = i'$, that is both of the blocks belong same class (e.g. C_i). In this case, each block has common keys with q^2 other blocks.
2. Type DC: $i \neq i'$, that is two blocks belong to different classes C_i and $C_{i'}$.

Proposition 5 The probability P_{SC} that any pair of blocks from same class has at least a common key is $\frac{q^2}{q^2+q}$.

Proof Since each class has $q^2 + q$ blocks and following from the definition of Type 1, we have $P_{SC} = \frac{q^2}{q^2+q}$. □

Proposition 6 The probability Q_{SC} that any pair of blocks is Type-SC is

Table 3 Key pre-distribution schemes in terms of overheads

Schemes	Storage overhead	Computation overhead	Communication overhead
Fully pairwise key scheme	$n - 1$	0	0
EG scheme	$O(q)$	$O(q)$	$O(q)$
q-Composite scheme	$O(q)$	$O(q)$	$O(q)$
BIBD scheme	$O(q)$	$O(q)$	0
Hybrid symmetric design	$O(q)$	$O(q)$	$O(q)$
RD	$O(q)$	$O(q)$	$O(q)$

$$Q_{SC} = \frac{\binom{q^2 + q}{2}}{\binom{(q^2 + q)(q^2 + q + 1)}{2}}$$

Proposition 7 *The probability Q_{DC} that any pair of blocks is Type-DC is*

$$Q_{DC} = \frac{\binom{q^2 + q}{1} \binom{q^2 + q}{1}}{\binom{(q^2 + q)(q^2 + q + 1)}{2}}$$

The blocks distribution state of type DC can also be categorized in 3 cases:

1. In each class C_i there exists one block that has no common key with blocks of class C_j (Clearly this block is the result of $B_j \setminus B_i$).
2. There exist $q - 1$ blocks in class C_i which all q objects are in common point set of classes C_i and C_j .
3. There exist q^2 blocks in class C_i which $q - 1$ objects are in common point set of classes C_i and C_j .

Property 6 *There exist exactly $q - 1$ blocks of class C_i in class C_j .*

Proof Since the common point set of every two classes in our approach is $q^2 - q$, the number of blocks consisting q elements of these $q^2 - q$ elements is $\frac{q^2 - q}{q} = q - 1$. □

Property 7 *The number of blocks of any class C_j that are in common with any of the $q - 1$ blocks of case 2 is $q^2 + 1$.*

Proof Since each class contains $q(q + 1)$ blocks and also according to the case 2 of common objects, we have

$$q(q + 1) - (q - 1) = q^2 + 1.$$

□

Proposition 8 *Let B_{ij} be one of the $q - 1$ blocks of class C_i satisfying case 2 and block $B_{i'j'}$ of different class, then the probability that B_{ij} and $B_{i'j'}$ have at least one common key is*

$$\frac{q - 1}{q^2 + q} \times \frac{q^2 + 1}{q^2 + q}$$

Proof It follows from Properties 6 and 7. □

Property 8 *The number of blocks of any class C_j that are in common with any of the q^2 blocks of case 3 is $q^2 - q + 1$.*

Proof We have easily

$$(q - 1)(q + 1) - (q - 1) + 1 = q^2 - q + 1.$$

□

Proposition 9 *Let B_{ij} be one of the q^2 blocks of class C_i satisfying case 3 and block $B_{i'j'}$ of different class, then the probability that B_{ij} and $B_{i'j'}$ have at least one common key is*

$$\frac{q^2}{q^2 + q} \times \frac{q^2 - q + 1}{q^2 + q}.$$

Proof It follows from Property 8. □

Proposition 10 *The probability P_{DC} that any pair of blocks from different class has at least a common key is*

$$P_{DC} = \frac{q - 1}{q^2 + q} \times \frac{q^2 + 1}{q^2 + q} + \frac{q^2}{q^2 + q} \times \frac{q^2 - q + 1}{q^2 + q}.$$

Proof It follows from Propositions 8 and 9. □

Theorem 11 *The probability P_{RD} that any pair of blocks shares one or more objects in residual design is expressed as follows:*

$$P_{RD} = \frac{q^2}{q^2 + q} * Q_{SC} + \left(\frac{q - 1}{q^2 + q} \times \frac{q^2 + 1}{q^2 + q} + \frac{q^2}{q^2 + q} \times \frac{q^2 - q + 1}{q^2 + q} \right) * Q_{DC}.$$

Proof It follows from Propositions 5, 6, 7 and 10. □

3.2.6 Resilience

Network resilience is the ability to adapt correctly in the face of nodes attacks and stress issues. In this section we consider the probability that a link is compromised when an attacker captures x nodes. For simplicity we define some notations as follows:

- C_x : event that x nodes (key-rings) are captured;
- D_j : event that a block including key j is compromised;
- l_j : event that a given link is secured with key j ;
- l : event that a given link is secured;
- L_j : event that a link secured with key j is compromised;
- L : event that a link is compromised.

According to the definition of resilience and the above notations we are interested in finding the value of $P(L | C_x)$.

The probability that a given link is secured with key j is expressed as:

$$P(l_j | l) = \frac{\binom{q^2(q+1)}{2}}{\binom{N_{RD}}{2}} = \frac{\binom{q^2(q+1)}{2}}{\binom{(q^2+q+1)(q^2+q)}{2}}$$

Also, the probability that x compromised blocks include key j can be defined as:

$$P(D_j | C_x) = 1 - \frac{\binom{N_{RD} - q^2(q+1)}{x}}{\binom{N_{RD}}{x}} = 1 - \frac{\binom{q^4 + q^3 + q^2 + q}{x}}{\binom{(q^2+q+1)(q^2+q)}{x}}$$

Clearly, the probability that a given link secured with j is compromised when x nodes are captured is:

$$P(L_j | C_x) = P(l_j | l)P(D_j | C_x).$$

Finally, in residual design, the probability that a link is compromised when an attacker captures x nodes can be written as:

$$P(L | C_x) = \sum_{j=1}^{q^2+q+1} \frac{\binom{q^2(q+1)}{2}}{\binom{(q^2+q+1)(q+1)}{2}} \left(1 - \frac{\binom{q^4 + q^3 + q^2 + q}{x}}{\binom{(q^2+q+1)(q+1)}{x}} \right)$$

4 Modified Residual Design

In this section we propose modified residual design in order to improve resilience while maintaining high network scalability. According to the last section, any block constructed from residual design is repeated totally q times. Therefore two nodes may have same key-ring. In this new approach, we remove repeated blocks. In other words, each pair of nodes is assigned with distinct key-rings. Therefore, we need a greater q rather than the basic approach to generate the same amount of blocks. We denote the modified residual design by RD*-KP. For any prime power of q , the parameters of different schemes are summarized in Table 4.

4.1 Key Pre-distribution

Before the deployment step, we generate blocks of residual design, where each block corresponds to a key-ring. Contrary to the basic approach that two nodes can be preloaded

Table 4 Parameters of SBIBD, UKP, RD-KP, RD*-KP

Design	v	b	r	k
Symmetric BIBD	$q^2 + q + 1$	$q^2 + q + 1$	$q + 1$	$q + 1$
NU-KP	$q^3 + 1$	$q^2(q - q + 1)$	q^2	$q + 1$
RD-KP	$q^2 + q + 1$	$(q^2 + q + 1)(q^2 + q)$	$q^2(q + 1)$	q
RD*-KP	$q^2 + q + 1$	$(q^2 + q + 1)(q + 1)$	$q(q + 1)$	q

with one block, we preload each node with disjoint blocks. It means that each two nodes share between zero and $q - 1$ keys.

After the deployment step, each two neighbours exchange the identifiers of their keys in order to determine the common keys. Otherwise, when neighbours do not share any key, the path key establishment phase takes place.

The RD*-KP, enhances the network resilience since the attacker has to compromise more keys to break a secure link. Moreover, the connectivity in this approach is similar to basic approach. Also we show that this approach maintains a high network scalability although it remains lower than that of the basic approach.

4.2 Theoretical Analysis

In this section, we analyze some important properties of the modified residual design. The connectivity, storage overhead, computation overhead and communication overhead is similar to residual design. We evaluate scalability and resilience against node capture.

4.2.1 Scalability

Since each block of residual design is repeated q times and each node is preloaded with disjoint blocks from the $(q^2 + q + 1)(q^2 + q)$ possible blocks of the residual design, it is obvious that the maximum number of nodes that we can support is equal to

$$N_{RD*} = \frac{(q^2 + q + 1)(q^2 + q)}{q} = (q^2 + q + 1)(q + 1).$$

4.2.2 Resilience

In our new proposed approach, each key exists in $q(q + 1)$ key-rings and two communicating nodes must have a common key i in their key-rings. With the same method of residual approach, we can evaluate the resilience of the new approach. The probability that a link between two nodes is secured using key i is:

$$P(l_i | l) = \frac{\binom{q(q+1)}{2}}{\binom{N_{RD*}}{2}} = \frac{\binom{q(q+1)}{2}}{\binom{(q^2 + q + 1)(q + 1)}{2}}.$$

Moreover, the probability that the key i appears in one or more of x compromised key-rings is:

$$P(D_i | C_x) = 1 - \frac{\binom{N_{RD*} - q(q+1)}{x}}{\binom{N_{RD*}}{x}} = 1 - \frac{\binom{(q+1)(q^2 + 1)}{x}}{\binom{(q^2 + q + 1)(q + 1)}{x}}.$$

Therefore, the probability that a link is compromised when x key-rings are captured by an attacker is computed as:

$$P(L|C_x) = \sum_{j=1}^{(q^2+q+1)} \frac{\binom{q(q+1)}{2}}{\binom{(q^2+q+1)(q+1)}{2}} \left(1 - \frac{\binom{(q+1)(q^2+1)}{x}}{\binom{(q^2+q+1)(q+1)}{x}} \right).$$

We can state that our proposed approach improves the resilience compared with the residual design since the probability $P(L|C_x)$ obtained by our proposed approach is obviously smaller than that of residual design which is demonstrated in Sect. 3.

4.3 Performance Comparison

In this section, we compare the two proposed approaches to existing schemes considering different criteria.

4.3.1 Scalability

In Fig. 1a we compare the scalability of the proposed schemes against SBIBD-KP, UKP* and Trade-KP methods. In the SBIBD scheme [11] with order q , the key-ring size is $k = q + 1$. This scheme is used for generating the maximum number of $q^2 + q + 1$ key-rings. Combinatorial trade [15] consists of collection union $T = T_1 \cup T_2$, where T_i is a collection of q^2 blocks of size k . The key-ring size is $4 \leq k \leq q$ and the number of supported sensors is exactly $N = 2q^2$. A proper choice for k in Trade-KP can be $k = q - 1$ where q is a prime power. In unital-based key pre-distribution [16] of order m , where each node is preloaded with $t(m + 1)$ distinct keys, there would be at least

$$\frac{m^2(m^2 - m + 1) - ((t - 1)(m^2 - 1)(m + 1) + t)}{t}$$

key-rings, where t is the t-UKP parameter.

In UKP* scheme the parameter t is selected as $t = \sqrt{m}$. The figure shows that at equal key-ring size, the RD-KP scheme greatly enhances the scalability compared to the other schemes. Additionally, RD*-KP scheme has a higher network scalability than UKP*, Trade-KP and SBIBD-KP. We then plot in Fig. 1b the required key-ring size when using the same schemes. The figure shows that at equal network size, the RD-KP and RD*-KP schemes allow to reduce the key-ring size rather than the other schemes.

4.3.2 Connectivity

In Fig. 2 we compare the network security coverage of different 6 schemes. SBIBD scheme ensures a perfect key sharing probability. In Trade-KP scheme [15], the fraction of nodes directly connected is $\frac{k(k-1)}{2(2q^2-1)}$ where $4 \leq k \leq q$ and q is a prime power. The same as the last subsection, we choose the key-ring size $k = q - 1$. In q-composite scheme [6], two nodes must share at least q common keys to be able to establish a secure link. The connectivity probability of q-composite scheme [23] is calculated as:

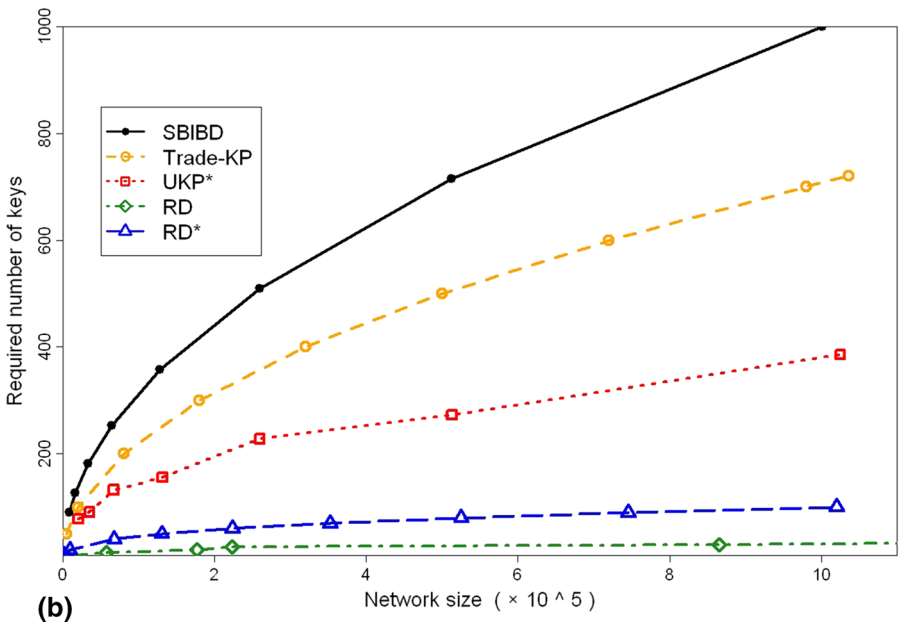
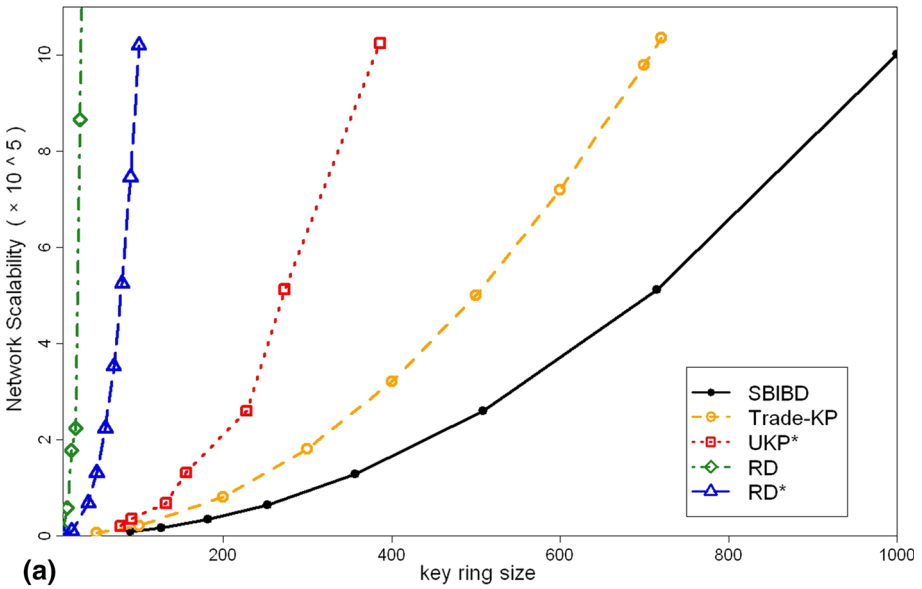


Fig. 1 Network scalability and required key-ring size. **a** Scalability of RD-KP and RD*-KP is compared with SBIBD, Hybrid Symmetric, Trade and UKP*-KP key pre-distribution schemes. RD-KP achieves a high network scalability and RD*-KP would provide better network scalability to UKP*-KP, Trade and SBIBD key pre-distribution schemes. **b** In reverse, the required key-ring size of RD-KP and RD*-KP is compared with SBIBD, Hybrid Symmetric, Trade and UKP*-KP key pre-distribution schemes at equal network size

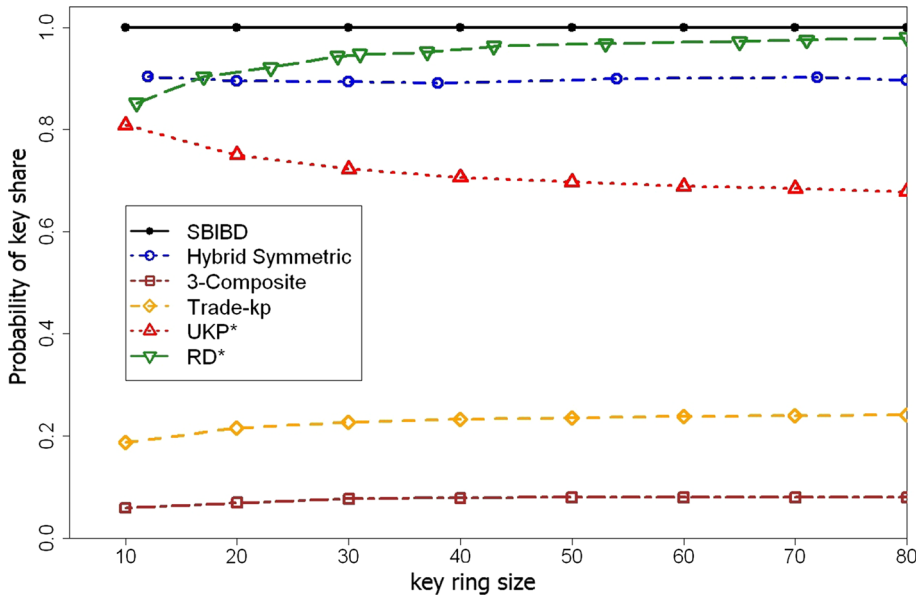


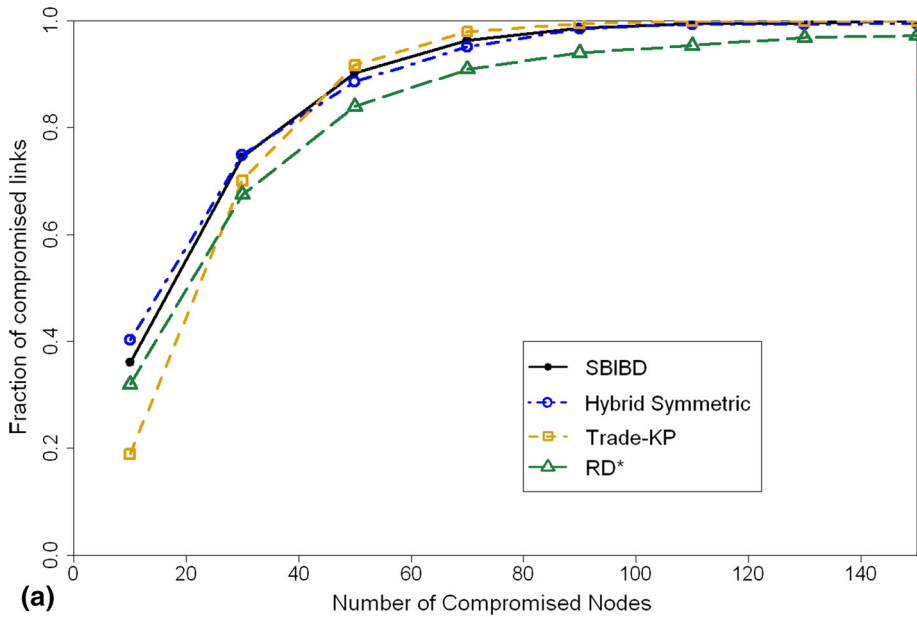
Fig. 2 Connectivity comparison. Direct secure connectivity of RD*-KP is compared with SBIBD, Hybrid Symmetric, 3-Composite, Trade and UKP*-KP key pre-distribution schemes. The figure shows that the 3-Composite and Trade schemes provide a bad secure connectivity coverage compared to other schemes. In addition the figure shows that RD*-KP scheme gives very good probability of connectivity

$$1 - \sum_{i=0}^{q-1} \frac{\binom{n-k}{k-i} \binom{k}{i}}{\binom{k}{n}}$$

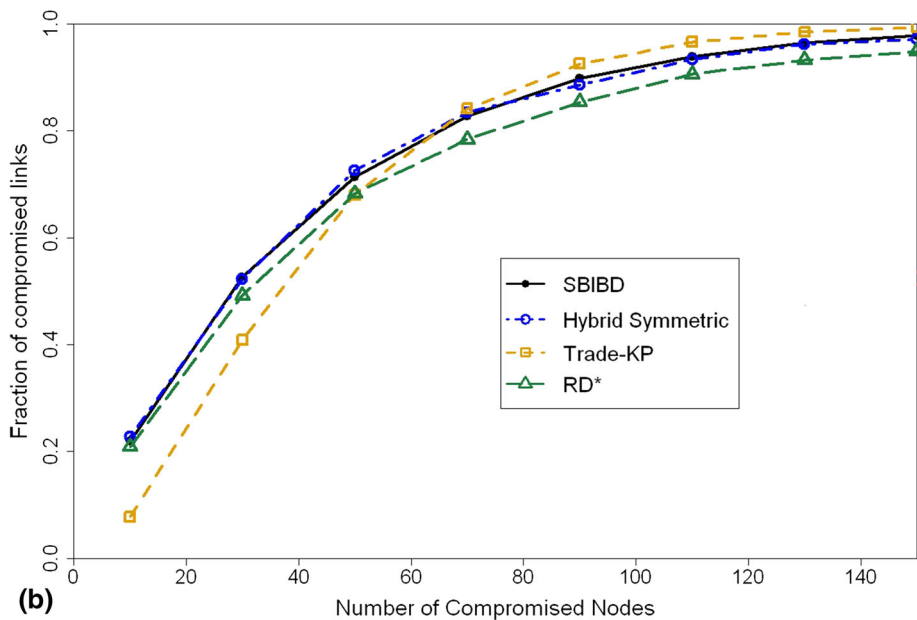
In t-UKP the secure connectivity coverage [16] is given by:

$$1 - \left(1 - \frac{(m+1)^2}{(m^3+m+1)} \right)^t$$

In Hybrid Symmetric Design, the key-ring size is $k = q + 1$ and we simulated this scheme for a network with $N = (q^2 + q + 1) + 0.2(q^2 + q + 1)$ nodes. Indeed, $0.2(q^2 + q + 1)$ nodes are loaded from complementary blocks. As the connectivity coverage of both RD-KP and RD*-KP approaches are the same, we've just drawn the connectivity of RD*-KP. The obtained results show that RD*-KP scheme gives a better connectivity coverage rather than UKP* and also rather than Hybrid Symmetric Design for the key-ring sizes greater than 17. Additionally, our proposed schemes are much better than 3-composite and Trade-KP. Although the RD*-KP connectivity coverage is greater than 0.851 for the key-ring sizes greater than 10, this metric is lower compared to SBIBD-KP.



(a)



(b)

Fig. 3 Resilience Comparison. **a** Resilience of RD*-KP is compared with SBIBD, Hybrid Symmetric and Trade key pre-distribution schemes. They are compared with the same key-ring size $k = 24$. RD*-KP provides a good resilience compared to SBIBD, Hybrid Symmetric and Trade schemes for compromised nodes number >27 . **b** Resilience of RD*-KP is compared with different schemes with the same key-ring size $k = 42$. For compromised nodes number >50 , RD*-KP has advantage in terms of resilience

4.3.3 Resilience

We compare the proposed RD* scheme against those of the Trade-KP, SBIBD and Hybrid Symmetric ones. In Fig. 3a all four schemes are compared at equal number of compromised nodes for key-ring size of $k = 24$. In Fig. 3b we plot the network resilience for key-ring size of $k = 42$. Here, we provide deeper details for $k = 42$. In [16] the resilience of Trade-KP is expressed as

$$1 - \frac{\binom{2q^2 - 4q + 2}{x} + 4(q - 1)\binom{2q^2 - 4q + 2}{x - 1}}{\binom{2q^2}{x}}$$

Here, choosing $k = q - 1$, q would be 43.

In [3], author proved that the resilience of SBIBD-KP scheme is

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

where q is a prime power. For key-ring size of 42, q would be 41. We simulated the resilience of Hybrid Symmetric Design scheme for $q = 41$ and $N = 1.2(q^2 + q + 1) = 2070$ nodes. The analysis shows that for the equal key-ring size, the resilience of RD*-KP

Table 5 Comparison of different schemes in terms of connectivity and scalability

Key-ring size	SBIBD-KP		Hybrid Symmetric-KP	
	Number of nodes	P_c	Number of nodes	P_c
30	931	1	931	0.8929
42	1807	1	1807	0.8902
68	4557	1	4557	0.9010
80	6481	1	6481	0.8961
Key-ring size	Trade-KP		UKP*	
	Number of nodes	P_c	Number of nodes	P_c
30	1922	0.226	16,471	0.727
42	3698	0.232	72,010	0.709
68	9522	0.239	557,039	0.687
80	13,122	0.240	1,097,421	0.681
Key-ring size	RD-KP		RD*-KP	
	Number of nodes	P_c	Number of nodes	P_c
30	865,830	0.943	28,861	0.943
42	3,263,442	0.963	77,701	0.963
68	22,019,556	0.972	323,817	0.972
80	41,996,880	0.980	524,961	0.980

Table 6 Comparison of different schemes in terms of resilience

KRS-CNN	10	30	50	70	90	110
<i>SBIBD-KP</i>						
24	0.3607	0.7454	0.9022	0.9639	0.9872	0.9954
42	0.2191	0.5260	0.7140	0.8285	0.8978	0.9395
<i>Hybrid Symmetric-KP</i>						
24	0.4026	0.7493	0.8862	0.9517	0.9854	0.9935
42	0.2270	0.5223	0.7262	0.8350	0.8856	0.9341
<i>Trade-KP</i>						
24	0.1892	0.7013	0.9171	0.9799	0.9955	0.9990
42	0.0777	0.4086	0.6805	0.8419	0.9259	0.9666
<i>RD*-KP</i>						
24	0.3200	0.6748	0.8396	0.9097	0.9406	0.9542
42	0.2088	0.4919	0.6829	0.7844	0.8542	0.9066

is better than SBIBD-KP and Hybrid Symmetric Design. It also gives a better resilience than Trade-KP for compromised nodes number (CNN) greater than 50.

4.4 Discussion

Assess our work, in this section we compare our approach against other schemes. In Tables 5, 6 we provide numerical results comparing scalability, connectivity coverage and resilience of the six schemes (SBIBD-KP, Hybrid Symmetric-KP, Trade-KP, UKP*, RD-KP and RD*-KP) at equal key-ring size. Using RD-KP and RD*-KP schemes, we have the maximum number of supported nodes in network scalability. For Example, Give KRS = 80, RD-KP would generate nodes more than 6000 times the SBIBD-KP and more than 35 times the UKP*. We can observe that our plan obviously better than the other three schemes SBIBD-KP, Hybrid Symmetric-KP and Trade-KP in terms of network resilience. As an example, for KRS = 42 and CNN = 90, the resilience of RD*-KP = 0.8542, SBIBD-KP = 0.8978, Trade-KP = 0.9259 and Hybrid Symmetric-KP = 0.8856. Additionally, our proposed schemes increase the probability of network connectivity over three methods Hybrid Symmetric-KP, Trade-KP and UKP*. For instance, in both RD-KP and RD*-KP, we maintain a high connectivity coverage over 0.943.

5 Conclusion

In this work, we designed a scalable key pre-distribution scheme in WSNs using a combinatorial design. We used for the first time the residual design theory as an important combinatorial algebraic architecture. We provided a mapping from residual design to key pre-distribution in WSNs. We achieved an extremely high network scalability and have advantage over other key pre-distribution schemes in terms of connectivity. The computational cost of RD-KP is less than or equal the similar symmetric key management algorithms. We then proposed modified residual design key pre-distribution scheme. Although the modified approach allows to reach same connectivity with the first scheme, analysis and numerical results in our simulations show that the optimized approach provides a better network resilience while giving lower network scalability against residual design key pre-distribution scheme at equal key-ring size.

References

1. Rathnayaka, A. J. D., & Potdar, V. M. (2011). Wireless sensor network transport protocol: A critical review. *Journal of Network and Computer Applications*, 36, 1–13.
2. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1990). *Handbook of applied cryptography*. New York, NY: CRC Press.
3. Camtepe, S. A., & Yener, B. (2007). Combinatorial design of key distribution mechanisms for wireless sensor networks. *IEEE/ACM Transactions on Networking*, 15, 346–358.
4. Ghen, C. Y., & Chao, H. C. (2011). A survey of key distribution in wireless sensor networks. *Security and Communication Networks*, 7, 2495–2508.
5. Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. In *Proceeding of the 9th ACM conference on computer and communications security* (pp. 41–47).
6. Chan, H., Perrig, A., & Song, D. (2003). Random key pre-distribution schemes for sensor networks. In *Proceeding of IEEE symposium on security and privacy* (pp. 197–213).
7. Qian, S. (2012). A novel key pre-distribution for wireless sensor networks. *Physics Procedia*, 25, 2183–2189.
8. Li, W. S., Tsai, C. W., Chen, M., Hsieh, W. S., & Yang, C. S. (2013). Threshold behavior of multi-path random key pre-distribution for sparse wireless sensor networks. *Mathematical and Computer Modelling*, 57(11), 2776–2787.
9. Blom, R. (1985). An optimal class of symmetric key generation systems. In *Proceedings of Eurocrypt, advances in cryptology* (pp. 335–338). Springer.
10. Blundo, C., Santis, A. D., Herzberg, A., Vaccaro, U., & Yung, M. (1992). Perfectly-secure key distribution for dynamic conferences. In *Proceeding, advances in cryptology (CRYPTO 92)* (pp. 471–486).
11. Camtepe, S. A., & Yener, B. (2004). Combinatorial design of key distribution mechanisms for wireless sensor networks. In P. Samarati, P. Y. A. Ryan, D. Gollmann, & R. Molva (Eds.), *ESORICS, volume 3193 of lecture notes in computer science* (pp. 293–308). Springer.
12. Lee, J., & Stinson, D. (2005). A combinatorial approach to key pre-distribution for distributed sensor networks. In *IEEE wireless communications and networking conference (WCN' 05), IEEE communication society* (pp. 1200–1205).
13. Ruj, S., & Roy, B. (2007). Key pre-distribution using partially balanced designs in wireless sensor networks. In *5th international symposium (ISPA)* (pp. 431–445). Springer.
14. Chakrabarti, D., Maitra, S., & Roy, B. K. (2006). A key pre-distribution scheme for wireless sensor networks: Merging blocks in combinatorial design. *International Journal of Information Security*, 5, 105–114.
15. Ruj, S., Nayak, A., & Stojmenovic, I. (2013). Pairwise and triple key distribution in wireless sensor networks with applications. *IEEE Transactions on Computers*, 62(11), 2224–2237.
16. Bechkit, W., Challal, Y., Bouabdallah, A., & Tarokh, V. (2013). A highly scalable key pre-distribution scheme for wireless sensor networks. *IEEE Transactions on Wireless Communications*, 12(2), 948–959.
17. Liu, D., Ning, P., & Li, R. (2005). Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 8(1), 41–77.
18. Kavitha, T., & Sridharan, D. (2010). Hybrid design of scalable key distribution for wireless sensor networks. *IACSIT International Journal of Engineering and Technology*, 2(2), 136–141.
19. Dargahi, T., Javadi, H. H. S., & Hosseinzade, M. (2015). Application-specific hybrid symmetric design of key pre-distribution for wireless sensor networks. *Journal of Security and Communication Networks*, 8, 1561–1574.
20. Zhang, J., & Varadharajan, V. (2010). Wireless sensor network key management survey and taxonomy. *Journal of Network and Computer Applications*, 33, 63–75.
21. Stinson, D. (2004). *Combinatorial designs: Construction and analysis*. Berlin: Springer.
22. Wallis, W. D. (1988). *Combinatorial designs*. Pure and applied mathematics series. New York: CRC Press.
23. Kendall, E., Kendall, M., & Kendall, W. S. (2012). A generalised formula for calculating the resilience of random key predistribution schemes. In *IACR Cryptology ePrint Archive* (p. 426).



Vahid Modiri is currently pursuing the Ph.D. degree in Computer Science at the Department of Computer Engineering, Islamic Azad University, Science and Research. He received the B.S. degree in Computer Science at Iran University of Science and Technology and the M.S. degree in Computer Science from the Islamic Azad University North Tehran branch. His main research focuses on key management in wireless sensor networks and wireless security.



Hamid Haj Seyyed Javadi received the B.S., M.S. and Ph.D. degrees in Amir Kabir University. He has been working as a full-time faculty member and Associate Professor of Shahed University. His research interests are ad-hoc network technologies, sensor network technology, distributed operating systems, and heuristic Algorithm.



Mohaddese Anzani received her M.S. degree in Mathematics from Shahed university, Tehran, Iran. She is currently pursuing the Ph.D. degree in Computer Science at Shahed University, Tehran, Iran. Her research interests include key management in wireless sensor networks and wireless security.