sensors

MDPI

Article

A Key Pre-Distribution Scheme Based on μ-PBIBD for Enhancing Resilience in Wireless Sensor Networks

Qi Yuan [1,2], Chunguang Ma [1,*], Haitao Yu [3] and Xuefen Bian [4]

1 College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China; yuanqi@hrbeu.edu.cn
2 College of Communication and Electronic Engineering, Qiqihar University, Qiqihar 161006, China
3 College of Tourism, Guilin University of Technology, Guilin 541004, China; albertyht@glut.edu.cn
4 College of Data Science and Technology, Heilongjiang University, Harbin 150080, China; bianxuefen@hlju.edu.cn
* Correspondence: machunguang@hrbeu.edu.cn; Tel.: +86-130-8999-9802

Received: 5 March 2018; Accepted: 10 May 2018; Published: 12 May 2018

Abstract: Many key pre-distribution (KPD) schemes based on combinatorial design were proposed for secure communication of wireless sensor networks (WSNs). Due to complexity of constructing the combinatorial design, it is infeasible to generate key rings using the corresponding combinatorial design in large scale deployment of WSNs. In this paper, we present a definition of new combinatorial design, termed "μ-partially balanced incomplete block design (μ-PBIBD)", which is a refinement of partially balanced incomplete block design (PBIBD), and then describe a 2-D construction of μ-PBIBD which is mapped to KPD in WSNs. Our approach is of simple construction which provides a strong key connectivity and a poor network resilience. To improve the network resilience of KPD based on 2-D μ-PBIBD, we propose a KPD scheme based on 3-D Ex-μ-PBIBD which is a construction of μ-PBIBD from 2-D space to 3-D space. Ex-μ-PBIBD KPD scheme improves network scalability and resilience while has better key connectivity. Theoretical analysis and comparison with the related schemes show that key pre-distribution scheme based on Ex-μ-PBIBD provides high network resilience and better key scalability, while it achieves a trade-off between network resilience and network connectivity.

Keywords: wireless sensor networks; key pre-distribution; partially balanced incomplete block design; combinatorial design; resilience

1. Introduction

Wireless sensor networks have more and more extensive applications due to their properties in lower cost, low power consumption, easy deployment and self-organization [1,2]. Sensor nodes in wireless sensor networks are responsible for monitoring surrounding environment and transmitting the information on-request to base station in one-hop or multi-hop path. A general environment of wireless sensor networks is shown in Figure 1. When sensor networks are deployed in a hostile territory or a special region, they should secure the communication between two sensor nodes by encryption/decryption, safety authentication techniques and others [3–8]. Key management is a core of cryptographic system in WSNs, which is used to protect security in application of WSNs [9–13]. Although study on key management in WSNs becomes more mature, it still has a lot of challenges because of different required network size, wide application background, limited sensor performance and so on [14].

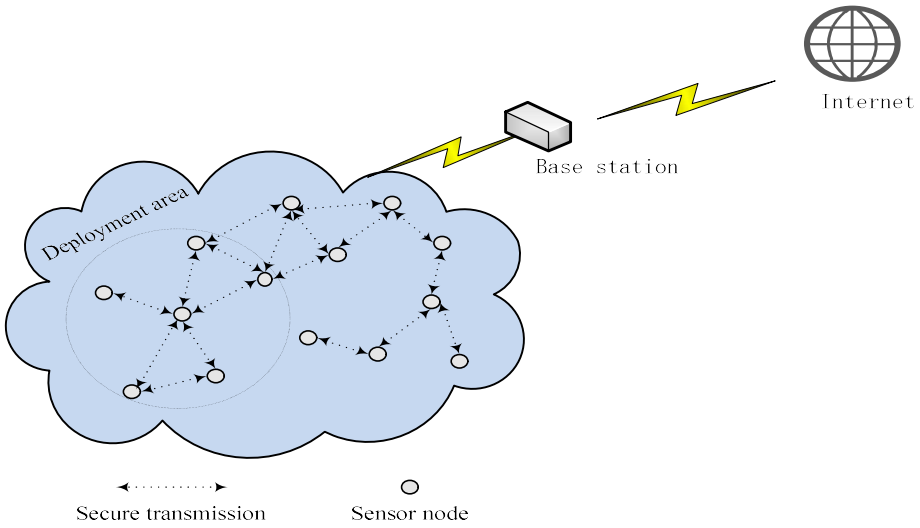

Figure 1. Environment of wireless sensor networks.

Key pre-distribution (KPD) scheme is one of the most extensive research directions of symmetric key management in WSNs [15–17]. A typical KPD scheme contains three phases: key pre-distribution, shared-key discovery and path-key establishment [13,18]. Key pre-distribution is an initialization phase, in which some keys selected from a large key pool are pre-distributed to each sensor to build a key ring. Shared-key discovery is to discover common pairwise keys between two nearby nodes by matching their key rings. In a path-key establishment phase, two nodes try to find one or more intermediary nodes that share common keys with them when the two neighboring nodes have no common pairwise keys. Various metrics of key pre-distribution scheme, such as network scalability, key connectivity, network resilience et al., are used for analyzing the merits and demerits of schemes in WSNs [19,20].

KPD schemes in WSNs are classified into probabilistic KPD scheme and deterministic KPD scheme based on the manner of key selection [6,12,16]. Typical probabilistic KPD schemes include random KPD, Q-composite KPD and polynomial pool based KPD [13]. Probabilistic KPD scheme randomly extracts a number of keys from key pool to form key rings of nodes, and its advantage is easy implementation due to its simple algorithm [21]. However, probabilistic KPD scheme only judges whether a pair of nodes have common keys by the mean of a probability value, and computers key connectivity by probabilistic result. Deterministic KPD scheme constructs key rings with a simple, straightforward model instead of selecting random key, which contributes to implementing shared-key discovery and path-key establishment. However, operations of these two phases, due to the absence of structure in key pre-distribution, are inherently complicated in randomized KDP scheme [20]. Meanwhile, performance metrics, such as scalability and connectivity, can be proven to be deterministic in a deterministic KPD scheme [22]. On the contrary, the deterministic value can not be obtained in a probabilistic scheme.

Combinatorial design theory is usually used for implementing deterministic KPD schemes. Due to the structural features of combinatorial design, metrics of combinatorial KPD scheme can easily be depicted. A general problem on existing combinatorial KPD schemes for WSNs is that construction of combinatorial designs mapped to KPD are complicated in implementation. Therefore, we focus on constructing a simpler combinatorial design applied to KPD scheme of WSNs, while performance metrics of KPD scheme should not be affected. A novel key pre-distribution scheme based on two-dimensional combinatorial design is introduced. Moreover, to enhance resilience and improve scalability, an extended three-dimensional combinatorial KPD scheme is proposed. The main contributions of our work are described as follows:

- A new combinatorial design (μ-PBIBD) is defined based on partially symmetric balanced incomplete block design.
- A μ-PBIBD is constructed in 2-D space, and a key pre-distribution scheme based on 2-D μ-PBIBD is proposed in which blocks are mapped to key rings. That is, shared-keys between nodes can be generated from common points between corresponding blocks. As a result, key connectivity of the proposed scheme depends on the construction of μ-PBIBD.
- To enhance network resilience of 2-D μ-PBIBD scheme, an Ex-μ-PBIBD is constructed by extending μ-PBIBD from 2-D space to 3-D space. Further, a key pre-distribution scheme based on 3-D Ex-μ-PBIBD is presented.
- Performance metrics of the proposed schemes are evaluated by theoretical analyses. Comparing with sBIBD scheme, RD and TD scheme, the results show that the proposed scheme has better scalability and higher resilience.

The remainder of this paper is organized as follows: In Section 2, related works on combinatorial design KPD schemes are introduced. Background knowledge of combinatorial design is described and a new combinatorial design is defined in Section 3. A μ-PBIBD is constructed and KPD scheme based on μ-PBIBD for WSNs is presented in Section 4. Then Section 5 proposes an extended μ-PBIBD based KPD scheme. Performance of the proposed scheme is analyzed and compared with the corresponding schemes in Section 6. Finally, the conclusions are drawn in Section 7.

2. Related Works

Combinatorial design theory is the part of combinatorial mathematics that deals with the existence and construction of systems of finite sets whose the existence have specified numerical properties [23]. Just because of these specified, easy-to-implement, numerical properties of combinatorial design theory, a series of studies on KPD scheme based on combinatorial design theory have been developed rapidly [24–33]. The first deterministic KPD scheme proposed by Comtepe and Yene [1] based on combinatorial design theory, which mapped Balanced Incomplete Block designs (BIBD) and Generalized Quadrangles (GQ) to KPD schemes, made key connectivity up to 1. Because of the difficulty of constructing BIBD and GQ, this KPD scheme supported only limited network size [9,30] and could not ensure keys pre-distribution according to actual demand about wireless sensor networks. Scheme [32] proposed a hybrid design according to complement of each block, i.e., when blocks of combinatorial design assigned to nodes were used up, a random subset of the complementary design blocks was distributed to the new-added nodes as key rings. This scheme supported larger-scale WSNs and improved the resilience of networks. Modiri et al. [30] introduced a new combinatorial design called residual design and mapped it to key pre-distribution scheme. This KPD scheme provided high connectivity while maintaining better scalability and resilience.

Stinson et al. [20,22,24,25] had been studying a series of combinatorial design based KPD since 2004. Lee and Stinson [20] introduced related knowledge of combinatorial set system to deterministic KPD schemes for WSNs. A strongly regular graph in [24] was used to product a network graph that represented whether two nodes share secret keys, and both one-way hash function and modified multi-space Bolm' scheme were introduced to reduce efficiently storage overheads of keys and increase resilience. In schemes [25], Lee defined two basic types of combinatorial designs as "configurations" and "μ-common intersection design" and discussed their influence on the local connectivity and two-hop paths in WSNs. In schemes [20], Lee proposed a general framework to construct KPD schemes based on a transversal design (TD), and represented KPD schemes based on linear polynomials and quadratic polynomials. These schemes provided higher efficiency in a shared-key discovery phase with better connectivity and resiliency. Paterson and Stinson in [22] defined a general class of designs as "partially balanced t-designs", which encompassed almost all of the proposed combinatorial designs used for KPD schemes. This general framework contributed to analyzing proposals of combinatorial KPD schemes and comparing with existing schemes, and easily evaluated which schemes possessed

better performance metrics for a certain application. In [33], taking the problem with the restricted number of sensor nodes in combinatorial KPD into consideration, a universal method was proposed to compute metrics for connectivity and resilience of combinatorial KPD schemes. A deterministic method exploited a resolvable TD to adjust the network size by removing key rings and easily analyzed the properties of the scheme using the framework constructed in [22].

Taking into account the difficulty of implementation of scheme [32], Xia et al. [21] first constructed BIBD with Hadamard matrix, and then mapped it to a KPD scheme in WSNs. Furthermore, the network size of WSNs was doubled by complementary set design and the shared-key intensity was enhanced by key slicing. In [26], based on the divisible core pair-wise balanced design, key rings of nodes were constructed, where common blocks and particular blocks were mapped to key rings of common nodes and key rings of cluster head nodes, respectively. This scheme increased network scalability and had better resilience. Gao et al. [31] proposed a combinatorial design based KDP scheme for two-layer hierarchical WSNs. In this scheme, a key pre-distribution scheme was constructed with orthogonal array. A block associated with keys was assigned to a more capable node, and a random subset of a block associated with keys was allotted to a less capable node. This scheme obtained higher resilience and better tradeoff between performance metrics than some probabilistic schemes.

3. Preliminaries

Combinatorial design theory is the branch of combinatorics which focuses on designing subsets of a finite set to satisfy certain properties [23]. Block design is a type of combinatorial design. In the following section, a brief introduction of definitions and prerequisites of combinatorial design theory used in this paper are given.

3.1. Combinatorial Design

Definition 1 [34]. *Let V be a basic set of v elements (called points) with $V = \{p_1, p_2, \cdots, p_v\}$ and B be a finite set of subsets (called blocks) of V. B is described as $B = \{B_1, B_2, \cdots, B_d\}$ in which $B_1, B_2, \cdots, B_d$ are d subsets of V. Then B is called "block design" of V.*

Definition 2 [32]. *If B is a block design of V that satisfies the following properties:*

(1) Uniformity: Each block in B contains exactly k distinct points.
(2) Regularity: Each point of V exists in exactly r different blocks of B.
(3) Balance: Each pair of points of V exists in exactly λ blocks of B.

B is called "balanced incomplete block design (BIBD)" and denoted as $B(v, d, r, k, \lambda)$. v, d, r, k, λ are parameters of the BIBD that satisfy $dk = vr$ and $\lambda(v-1) = r(k-1)$. In particular, when $d = v$ and therefore $r = k$, a BIBD is called symmetric BIBD (sBIBD) which can be denoted as $sB(v, k, \lambda)$.

Example 1. *Consider $sB(v, k, \lambda) = (7, 3, 1)$ with $V = \{1, 2, 3, 4, 5, 6, 7\}$ and $B = \{B_1, B_2, \ldots, B_7\}$. The blocks in B are: $B_1 = \{1, 2, 3\}$, $B_2 = \{1, 4, 5\}$, $B_3 = \{1, 6, 7\}$, $B_4 = \{2, 4, 6\}$, $B_5 = \{2, 5, 7\}$, $B_6 = \{3, 4, 7\}$, $B_7 = \{3, 5, 6\}$.*

For every prime or prime power $q \geq 2$, there exists a $sB(q^2 + q + 1, q + 1, 1)$. Comtepe et al. [32] defined a mapping from $sB(q^2 + q + 1, q + 1, 1)$ to KPD and proposed a KPD scheme base on sBIBD. In this scheme, each point in V was associated with a distinct random key and each block was used as a key ring, providing the key pool having $v = q^2 + q + 1$ keys and $d = q^2 + q + 1$ key rings each having $k = q + 1$ keys. In sBIBD, each pair of blocks intersected on one point and was mapped to KPD scheme in which each pair of key rings shared one key. As a result, the probability of key shared between each pair of nodes was always 1. When value of q was large, constructing $sB(q^2 + q + 1, q + 1, 1)$ was a NP-problem [32] which limited the size of sensor networks whose keys were pre-distributed. That is, this scheme was only theoretically feasible for a large scale of WSNs.

Definition 3 [20]. *A set system is a tripe (V, G, B), where V is a finite set of cardinality v, G is a partition of V into k parts (called groups) of size q and B is a block design of V with size k of blocks, which satisfies the following properties:*

(1) $|G \cap B| = 1$, *for every $G \in G$ and every $B \in B$.*

(2) *Every two points from different groups occurs in exactly λ blocks of B.*

The tripe (V, G, B) is a transversal design of V which can be expressed as $TD(\lambda, k, q)$. When $\lambda = 1$, it can be written as $TD(k, q)$. A $TD(k, q)$ has the following properties: (1) There are exactly kq points and q^2 blocks; (2) every block contains exactly k points; and (3) every point occurs in exactly q blocks.

Example 2. *Let*

$$V = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\},$$

$$G = \{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{10, 11, 12\}\}, \textit{and}$$

$$\begin{aligned} B = \{&\{1, 4, 7, 10\}, \{1, 5, 8, 11\}, \{1, 6, 9, 12\},\\ &\{2, 4, 8, 12\}, \{2, 5, 9, 10\}, \{2, 6, 7, 11\},\\ &\{3, 4, 9, 11\}, \{3, 5, 7, 12\}, \{3, 6, 8, 10\}\}. \end{aligned}$$

Then (V, G, B) is a TD(4, 3) with a set V of $|V| = kq = 12$ points, $G = \{G1, G2, \cdots, Gk\}$ of $|G| = k = 4$ groups and $B = \{B1, B2, \cdots, Bq^2\}$ of $|B| = q^2 = 9$ blocks.

A $TD(k, q)$, where q is a prime or a prime power, was constructed by Lee et al. in [20] as follows.

Let the point in V be denoted as (a, b), where $a \in \{0, 1, \cdots, k-1\}$, $b \in \mathbb{F}q$ and $2 \leq k \leq q$. The construction of V is

$$\begin{aligned} V = \quad &\{(0,0), (0,1), \cdots, (0, q-1),\\ &(1,0), (1,1), \cdots, (1, q-1),\\ &\cdots\\ &(k-1,0), (k-1,1), \cdots, (k-1, q-1)\}. \end{aligned}$$

A group G of V is

$$\begin{aligned} G = \quad &\{\{(0,0), (0,1), \cdots, (0, q-1)\},\\ &\{(1,0), (1,1), \cdots, (1, q-1)\},\\ &\cdots\\ &\{(k-1,0), (k-1,1), \cdots, (k-1, q-1)\}\}. \end{aligned}$$

For every ordered pair $(i, j) \in \mathbb{F}q \times \mathbb{F}q$, a block of B is defined as

$$B_{i,j} = \{(a, ia + j (\mathrm{mod} q)) | 0 \leq a \leq k-1\}.$$

Then $B = \{B_{i,j} : (i, j) \in \mathbb{F}q \times \mathbb{F}q\}$. This tripe (V, G, B) is a $TD(k, q)$.

Compared with sBIBD scheme proposed by Comtepe and Yener, this transversal design was simple in construction and corresponding KPD scheme was no limit to network size of WSNs.

3.2. μ-Partially Balanced Incomplete Block Design

A PBIBD is a generalization of a BIBD, in which each pair of points does not need to appear the same number of times [34]. The definition of PBIBD is given as follows:

Definition 4. *If B is a block design of V that satisfies the following properties:*

(1) *Uniformity: Each block in B contains exactly k distinct points.*

(2) Regularity: Each point of V exists in exactly r different blocks of B.

(3) Partial Balance: Each pair of points of V exists in different numbers of blocks of B.

B is called "partial balanced incomplete block design (PBIBD)". Further, we refine PBIBD to define a μ-PBIBD.

Definition 5. *Let $F = \{\lambda 1, \lambda 2, \cdots, \lambda\mu\}$ be a set of positive integers. A μ-PBIBD is a pair (V, B), where V is a finite set of v elements (called "points") and B is a set of d k-subsets (called "block") of V, which satisfies the following properties:*

(1) (V, B) is regular, i.e., each point of V appears in exactly r different blocks of B.

(2) (V, B) is uniform, i.e., the number of points in every block is k.

(3) (V, B) is partial balance, i.e., every pair of points appears in λi blocks, for $1 \leq i \leq \mu$.

The μ-PBIBD can be expressed as $\mu - PB(v, d, r, k, \lambda 1, \cdots, \lambda\mu)$, in which parameter r is called the degree of a point in V, k is called the rank of (V, B), and μ is called the class of (V, B).

Theorem 1. *$\mu - PB(v, d, r, k, \lambda 1, \cdots, \lambda\mu)$ exists only if dk = vr.*

Theorem 2. *The number of common points in any two blocks is λi ($1 \leq i \leq \mu$). If μ = 1, a μ-PBIBD will degenerate into a BIBD, in which case any pair of points exists in $\lambda 1$ blocks.*

In particular, when $d = v$ and therefore $r = k$, a μ-PBIBD is called symmetric μ-PBIBD (μ-sPBIBD) which can be denoted as $\mu - sPB(v, k, \lambda 1, \cdots, \lambda\mu)$.

Example 3. *Let V = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15} and $B = \{B_1, B_2, \cdots, B_{15}\}$, where the blocks $B_1, B_2, \cdots, B_{15}$ in B are:*

$B_1 = \{2,3,4,5,6,11\}; B_2 = \{1,3,4,5,7,12\}; B_3 = \{1,2,4,5,8,13\}; B_4 = \{1,2,3,5,9,14\};$
$B_5 = \{1,2,3,4,10,15\}; B_6 = \{1,7,8,9,10,11\}; B_7 = \{2,6,8,9,10,12\}; B_8 = \{3,6,7,9,10,13\};$
$B_9 = \{4,6,7,8,10,14\}; B_{10} = \{5,6,7,8,9,15\}; B_{11} = \{1,6,12,13,14,15\}; B_{12} = \{2,7,11,13,14,15\};$
$B_{13} = \{3,8,11,12,14,15\}; B_{14} = \{4,9,11,12,13,15\}; B_{15} = \{5,10,11,12,13,14\}.$

In this block design, there are 15 blocks and 15 points where each block contains 6 points and each point occurs in 6 blocks. Every pair of points appears in λ_1, λ_2 or λ_3 blocks, where $\lambda_1 = 1$, $\lambda_2 = 2$ and $\lambda_3 = 3$. Then the block design is a μ-sPBIBD which can be denoted as $\mu - sPB(15, 6, 1, 2, 3)$.

4. Key Pre-Distribution Based on μ-sPBIBD

In this section, we construct a basic sPBIBD and describe the mapping from μ-sPBIBD to KPD in WSNs.

4.1. A Construction of 2-D μ-sPBIBD

By combining with $sB(v, k, \lambda)$ and $TD(k, q)$ in Section 3.1, we use the representation of data elements in 2-D space to construct $\mu\text{-}sPB(v, k, \lambda_1, \cdots, \lambda_\mu)$ which can be described as follows.

Let points of V be expressed as (a, b), where (a, b) are coordinate of 2-D space elements for $a \in \{1, \cdots, m\}$ and $b \in \{1, \cdots, n\}$. Then V is a set of cardinality mn, where

$$\begin{aligned} V = \quad & \{(1,1),(1,2),\cdots,(1,n),\\ & (2,1),(2,2),\cdots,(2,n),\\ & \cdots\\ & (m,1),(m,2),\cdots,(m,n)\}, \end{aligned}$$

for every ordered pair $(a, b) \in \{1, \cdots, m\} \times \{1, \cdots, n\}$, a block in V is defined as

$$B_{a,b} = \{(i, b), (a, j) | 1 \leq i \leq m, i \neq a;\ 1 \leq j \leq n, j \neq b\}.$$

Let $B = \left\{B_{a,b} : (a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n\right\}$.
The pair (V, B) has some following properties.

Property 1. *In (V, B), V has mn points, B has exactly mn blocks, and the number of points in each block is exactly $m + n - 2$.*

Proof. Constructed as before, V can be viewed as a 2-D space with the dimension $m \times n$. Therefore, the number of points in V is mn; Each block $B_{a,b}$ in B, where $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, is a set of coordinates of all elements on a row and b column except (a, b) in $m \times n$ 2-D space. Therefore, the number of blocks in B is mn and the number of points in each block is $m - 1 + n - 1 = m + n - 2$. □

Property 2. *In (V, B), every point in V occurs in exactly $m + n - 2$ blocks.*

Proof. According to the aforementioned construction of block, point (a, b) in V should appear in block $B_{a,\overline{b}}$ (where $\overline{b}$ is between 1 and n except b) and block $B_{\overline{a},b}$ (where $\overline{a}$ is between 1 and m except a). Therefore, the number of blocks containing point (a, b) is $m + n - 2$. □

Property 3. *In (V, B), there are three cases on the number λ of blocks in which any pair of points, say (a_1, b_1) and (a_2, b_2), is contained simultaneously. If $a_1 \neq a_2$ and $b_1 \neq b_2$, value of λ should be 2; If $a_1 = a_2$ and $b_1 \neq b_2$, value of λ should be $n - 2$; If $a_1 \neq a_2$ and $b_1 = b_2$, value of λ should be $m - 2$.*

Proof. There are three cases on position relationship between two points in V. One is that, if points (a_1, b_1) and (a_2, b_2) in V lie on the different rows and columns, the two points should occur in blocks B_{a_1,b_2} and B_{a_2,b_1}, and then $\lambda = 2$. Another is that, if points (a_1, b_1) and (a_2, b_2) lie on the same row and different column, the two points should occur in exactly the blocks whose subscript are expressed by other points on the same row except these two points, and then $\lambda = n - 2$. The third is that, if points (a_1, b_1) and (a_2, b_2) lie on the same column and different row, the two points should occur in exactly the blocks whose subscript are expressed by other points on the same column except these two points, and then $\lambda = m - 2$.

Therefore, inferred from the three properties, (V, B) is μ-sPBIBD which can be denoted as $\mu - sPB(mn, m + n - 2, 2, m - 2, n - 2)$. □

4.2. 2-D μ-sPBIBD Based KDP Scheme

A key pool contains keys which will be selected in various ways to form key rings. These key rings need to be pre-distributed to sensor nodes before sensor nodes of WSNs are deployed. When nodes in WSNs transfer messages to their neighbor nodes, secure communications should be guaranteed by the common keys in key rings of communication nodes.

In KPD schemes based on 2-D μ-sPBIBD for WSNs with M sensor nodes, the mapping from 2-D μ-sPBIBD to KPD is described in Table 1. Each point in V can act as a key in the key pool and each block can be viewed as a key ring to distribute a sensor node, meaning that the number d of blocks should satisfy $d \geq M$ and if two blocks have common points, the two nodes which contain respectively the two blocks will have share-keys.

4.2.1. Key Pre-Distribution Phase

In 2-D μ-sPBIBD scheme, keys in key pool are defined as the elements in 2-D space while the corresponding key IDs are expressed by coordinates of the elements in 2-D space. That is, points (1, 1),

$\ldots$, (1, n), $\ldots$, (a, b), $\ldots$, (m, 1), $\ldots$, (m, n) in V are view as key IDs which are associated with keys in key pool. Point (a, b) and the corresponding key $key_{a,b}$ can be represented as a whole $P_{a,b}$, where $1 \leq a \leq m$ and $1 \leq b \leq n$, Then the key pool can be described as a set of $P_{a,b}$. According to the construction of blocks proposed in Section 4.1, mn blocks $B_{a,b}$ are generated, where $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, which can be denoted as $B_{a,b} = \{(P_{a,j}, P_{i,b} | 1 \leq i \leq m, i \neq a; 1 \leq j \leq n, j \neq b\}$. The number of elements in block $B_{a,b}$ is $m + n - 2$. Elements $P_{a,b}$ in block $B_{a,b}$ are distributed as a key ring to a sensor node.

Table 1. Mapping from 2-D μ-sPBIBD to key pre-distribution (KPD).

μ-sPBIBD	KPD	Parameter	Value of Parameter
Basic set (point set)	Key pool	V	$\{(a,b)\|(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n\}$
Basic set size	key pool size	v	mn
Block	Key ring	$B_{a,b}$	$\{(i,b),(a,j)\|1 \leq i \leq m, i \neq a;$ $1 \leq j \leq n, j \neq b\}$
Number of blocks	Number of key rings	d	mn
Block size	Key ring size	k	$m + n - 2$
Number of common points between two blocks	Number of shared keys between two nodes	$\lambda_1, \ldots, \lambda_\mu$	$2, m - 2, n - 2$

4.2.2. Shared-Key Discovery Phase

When a sensor node needs to transmit the message to neighbor nodes, the node broadcasts its key IDs in key ring. The neighbors discover shared-keys with source node by comparing with their key IDs. Property 3 shows that there are three possibilities for the number of shared-keys between the two nodes: 2, $m - 2$ or $n - 2$.

Suppose that two sensor nodes N_i and N_j have s shared-keys, say $key_1, key_2, \cdots, key_s$, where $key_1, key_2, \cdots, key_s \in V$ and value of s is 2, $m - 2$ or $n - 2$, respectively. A session key between the two nodes can be generated from the shared-keys corresponding to common points between blocks. According to [20], a session key $K_{i,j}$ is established by a hash function h,

$$K_{i,j} = h(key_1 || \cdots || key_s || i || j)$$

This approach that computes session key by a hash function of common keys can improve the network resilience [6,20].

If two communication nodes fail to discover their shared-keys in the shared-key discovery phase, then path-key will be established. In 2-D μ-sPBIBD scheme, any pair of nodes can share at least two keys. Therefore, path-key establishment phase will not be considered.

4.3. 3-D Ex-μ-sPBIBD Based KPD Scheme

In combinatorial KPD scheme, the more keys the blocks share, the more blocks are effected by a compromised block [32]. That is, network resilience contradicts with key connectivity [18]. Complete key connectivity inevitably leads to poor resilience in 2-D μ-sPBIBD based KPD scheme. In order to make a trade-off between resilience and connectivity, we propose an extended μ-PBIBD that can improve the resilience by reducing properly connectivity.

As mentioned in Section 4.1, a key pool can be viewed as 2-D space to store keys, in which key IDs are expressed by corresponding row-column coordinates of elements in 2-D space. In this subsection, we extend a key pool from 2-D space to 3-D space in which each key ID can be expressed by corresponding row-column-page coordinate of element in 3-D space. A extending μ-sPBIBD (Ex-μ-sPIBD) based KPD is proposed and KPD in 3-D space is described as follows.

Let V be a set of coordinates of $q \times q \times q$ elements in 3-D space, which can be defined by

$$\left\{ \begin{array}{c} \left[\begin{array}{c} (1,1,1), \cdots, (1,b,1), \cdots, (1,q,1) \\ \cdots \\ (a,1,1), \cdots, (a,b,1), \cdots, (a,q,1) \\ \cdots \\ (q,1,1), \cdots, (q,b,1), \cdots, (q,q,1) \end{array} \right] \\ \cdots \\ \left[\begin{array}{c} (1,1,c), \cdots, (1,b,c), \cdots, (1,q,c) \\ \cdots \\ (a,1,c), \cdots, (a,b,c), \cdots, (a,q,c) \\ \cdots \\ (q,1,c), \cdots, (q,b,c), \cdots, (q,q,c) \end{array} \right] \\ \cdots \\ \left[\begin{array}{c} (1,1,q), \cdots, (1,b,q), \cdots, (1,q,q) \\ \cdots \\ (a,1,q), \cdots, (a,b,q), \cdots, (a,q,q) \\ \cdots \\ (q,1,q), \cdots, (q,b,q), \cdots, (q,q,q) \end{array} \right] \end{array} \right\} \quad (1)$$

A point in set V is denoted as (a, b, c), where $1 \leq a, b, c \leq q$. The blocks in 3-D Ex-μ-sPBIBD are defined as

$$B_{a,b,c} = \{(i,b,c), (a,j,c), (a,b,l) | 1 \leq i \leq q, i \neq a;\ 1 \leq j \leq q, j \neq b; 1 \leq l \leq q, l \neq c\}, \quad (2)$$

where $(a, b, c) \in \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_q$.

Let

$$B = \left\{ B_{a,b,c} : (a,b,c) \in \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_q \right\}.$$

In 3-D Ex-μ-sPBIBD, the number of blocks is q^3 and a block has $3q - 3$ points. Mapping from Ex-μ-sPBIBD to KPD can be described in Table 2.

Table 2. Mapping from 3-D Ex-μ-sPBIBD to KPD.

Ex-μ-sPBIBD	KPD	Parameter	Value of Parameter
Basic set	Key pool	V	$\{(a,b,c) \mid (a,b,c) \in \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_q\}$
Basic set size	Key pool size	v	q^3
Block	Key ring	$B_{a,b,c}$	$\{(i,b,c), (a,j,c), (a,b,l) \mid 1 \leq i \leq q, i \neq a; 1 \leq j \leq q, j \neq b; 1 \leq l \leq q, l \neq c\}$
Number of blocks	Number of key rings	d	q^3
Block size	Key ring size	k	$3q - 3$
Number of common points between blocks	Number of shared-key between nodes	$\lambda_1, \cdots, \lambda_\mu$	$0, 2, q-2$

A key pool is considered as 3-D space in which store $q \times q \times q$ keys. Key IDs in the key pool are represented by row-column-page coordinate (a, b, c) of elements in 3-D space. A Key combining with the corresponding key ID is denoted as a whole $p_{a,b,c}$. A 3-D Ex-μ-sPBIBD is constructed by the approach similar to Section 4.1.

5. Theoretical Analysis

In this section, we analyze some important metrics of μ-sPBIBD based KPD scheme, such as connectivity, scalability and resilience.

5.1. Key Connectivity

Key connectivity is one of important metrics to evaluate the performance of KPD scheme in WSNs. Connectivity represents the ability of secure communication between nodes [26] and can be described by the probability that sensor nodes have shared-keys. If two nodes have no shared-keys, communication between them will use the third node to forward who has shared-keys with the two nodes, which will result in energy waste. Therefore, direct key connectivity can not only secure the networks but also save the communication overhead.

As noted in Section 4.2, KPD scheme based on 2-D μ-sPBIBD guarantees that any pair of key rings has λ_i common keys, which means key connectivity of the proposed scheme can achieve 1. In the following, we study key connectivity of 3-D Ex-μ-sPBIBD scheme in WSNs.

3-D space with dimension $q \times q \times q$ is depicted in Figure 2. Taking N_1 as example, the relation among node, block and 3-D space in 3-D Ex-μ-sPBIBD scheme are descripted as follow. Suppose that N_1 is a sensor node in WSNs. Then a block B_{a_1,b_1,c_1} constructed by Equation (2) is preloaded to N_1 as a key ring. For simplicity, location of N_1 in 3-D space is denoted as (a_1, b_1, c_1).

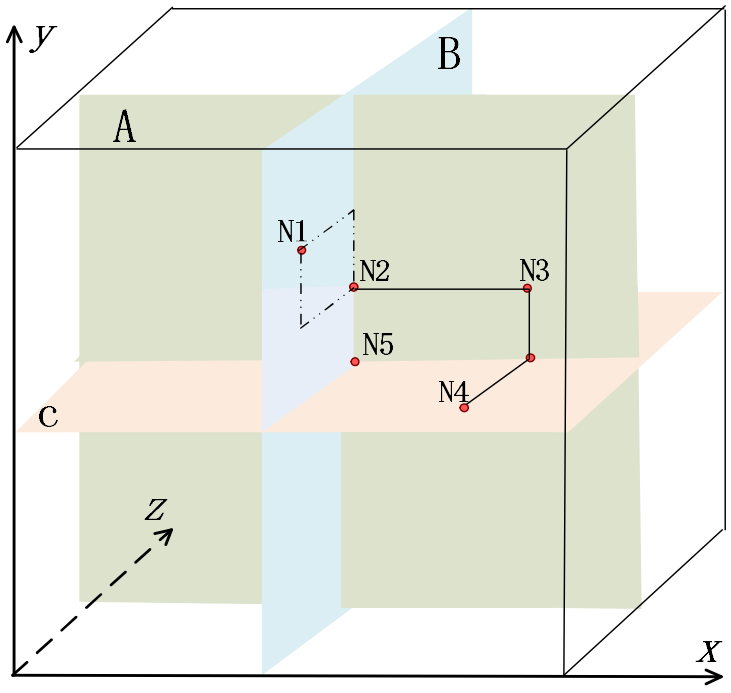

Figure 2. Relation among node, block and shared-key in 3-D Ex-μ-sPBIBD.

If two nodes in 3-D space are coplanar, 3-D Ex-μ-sPBIBD will degenerate into 2-D μ-sPBIBD which has been described in Section 4.1. Therefore, two blocks have 2 or $q-2$ common points, which means the two nodes have 2 or $q-2$ shared-keys. If two nodes are preloaded non-coplanar blocks as key rings, they will have no shared-key and need to use path-key to secure communicate.

Let V be a set of $|V| = v = 6 \times 6 \times 6$ points and be expressed by Equation (1) where $q = 6$. According to Figure 2, nodes are denoted as N_1, N_2, N_3, N_4 and N_5, while the corresponding blocks $B_{3,5,2}$, $B_{3,4,3}$, $B_{5,4,3}$, $B_{5,3,1}$ and $B_{3,3,3}$ can be described as follows.

$$
\begin{aligned}
B_{3,5,2} = \{&(1,5,2),(2,5,2),(4,5,2),(5,5,2),(6,5,2),\\
&(3,1,2),(3,2,2),(3,3,2),(3,4,2),(3,6,2),\\
&(3,5,1),(3,5,3),(3,5,4),(3,5,5),(3,5,6)\}\\
B_{3,4,3} = \{&(1,4,3),(2,4,3),(4,4,3),(5,4,3),(6,4,3),\\
&(3,1,3),(3,2,3),(3,3,3),(3,5,3),(3,6,3),\\
&(3,4,1),(3,4,2),(3,4,4),(3,4,5),(3,4,6)\}\\
B_{5,4,3} = \{&(1,4,3),(2,4,3),(3,4,3),(4,4,3),(6,4,3),\\
&(5,1,3),(5,2,3),(5,3,3),(5,5,3),(5,6,3),\\
&(5,4,1),(5,4,2),(5,4,4),(5,4,5),(5,4,6)\}\\
B_{5,3,1} = \{&(1,3,1),(2,3,1),(3,3,1),(4,3,1),(6,3,1),\\
&(5,1,1),(5,2,1),(5,4,1),(5,5,1),(5,6,1),\\
&(5,3,2),(5,3,3),(5,3,4),(5,3,5),(5,3,6)\}\\
B_{3,3,3} = \{&(1,3,3),(2,3,3),(4,3,3),(5,3,3),(6,3,3),\\
&(3,1,3),(3,2,3),(3,4,3),(3,5,3),(3,6,3),\\
&(3,3,1),(3,3,2),(3,3,4),(3,3,5),(3,3,6)\}.
\end{aligned}
$$

As shown in Figure 2, shared-keys between nodes have three cases. The first case is that, for example, blocks of N_1 and N_2 have two shared-keys, say (3, 5, 3) and (3, 4, 2), and the case are the same as N_1 and N_5, N_3 and N_5, N_3 and N_4, and N_4 and N_5. The second case is that blocks of nodes have $q - 2 = 4$ shared-keys. For example, shared-keys between N_2 and N_3 have (1, 4, 3), (2, 4, 3), (4, 4, 3) and (6, 4, 3). The third case is that blocks of nodes have no share-key in which we should establish their path-key.

Taking nodes N_1 and N_3 as example, we analyze the establishment of path-key between the two nodes. In Figure 2, N_2 has shared-key with N_1 and N_3, and then a secure two-hop path between N_1 and N_3 (i.e., N_1, N_2, N_3) is established.

Taking example for node N_5 in Figure 2, we analyze the connectivity of Ex-μ-sPBIBD scheme. All nodes that are coplanar with N_5 have the share-keys with N_5. Therefore, the number of nodes on plane A, B and C that have share-keys with N_5 is $3q$ $(q - 1)$. The total number of nodes except N_5 in WSNs is $q^3 - 1$. Then direct connectivity of Ex-μ-sPBIBD is given by

$$Con = \frac{3q(q-1)}{q^3-1} = \frac{3q}{q^2+q+1}. \tag{3}$$

Figure 2 illustrates shared relation of blocks and key connectivity of key rings. For simplicity, we replace block with node to illustrate key shared. There are three cases of key-shared between nodes: If two nodes, such as N_4 and N_5, lie on the same plane and have the different row and column subscript, the two nodes should have 2 shared-keys; If two nodes, such as N_2 and N_3, lie on the same plane and have the same row (or column subscript), the two nodes should share $q - 2$ keys; If two nodes, such as N_1 and N_3, are not coplanar, the two nodes should have no direct shared-key.

5.2. Network Scalability

Network scalability reflects flexibility metrics of KPD scheme in WSNs and fails to effect security of network when new nodes join WSNs. Scalability can be expressed as the maximum number of nodes supported by KPD in WSNs. In the combinatorial KPD scheme, blocks are mapped to key rings. Therefore network scalability is equivalent to the number of blocks in combinatorial design.

In 2-D μ-sPBIBD, let the number of points in V be v, v can be decomposed into multiple forms as $m_1 \times n_1$, $m_2 \times n_2, \cdots$. In terms of property 1, if V is described by 2-D spaces with different dimensions, the number of blocks of μ-sPBIBD will also be different which is $m_1 + n_1 - 2$, $m_2 + n_2 - 2, \cdots$, respectively. That is, scalability of KPD scheme based on 2-D μ-sPBIBD varies with the number of the corresponding key rings.

Example 4. *Suppose the number of points in V is 10,000, 10,000 elements can be expressed in the form of 100 × 100, 50 × 200, 25 × 400, 20 × 500, 10 × 1000, 5 × 2000, 250 × 40 and 125 × 80, where the form 100 × 100 results in the minimum number of points in blocks in 2-D μ-sPBIBD.*

Theorem 3. *Let v be expressed as $q \times q$, $m_1 \times n_1$, $m_2 \times n_2 \cdots$. In 2-D space, the form $q \times q$ corresponds to the minimum number of points in block.*

Proof. Suppose that v can be described by two forms such as $q \times q$ and $\frac{q}{e} \times (q \times e)$, where $e, \frac{q}{e} \in \mathbb{Z}^+$ and $e \neq 1$. In both cases, the number of points in blocks are $2q - 2$ and $\frac{q}{e} + (q \times e) - 2$, respectively. Comparing with the number of points in the two blocks, the result is as follow.

$$(2q - 2) - (\frac{q}{e} + (q \times e) - 2) = (-q)\frac{(e-1)^2}{e} < 0$$

As described above, if v can be decomposed into many forms of multiplication of two numbers, the number of points of blocks will be the minimum in the case of v being expressed by a square of a certain number. That is, the corresponding 2-D space should hold the same row and column.

In 2-D μ-sPBIBD, the number of blocks is the same as the number of points in V. Therefore, the number of nodes in WSNs is also v. According to Theorem 3, in our proposed KPD scheme based on μ-sPBIBD, the number of keys in the key pool should be a minimum square of a number, which will lead to shorter key ring size under similar network scalability in WSNs. If the number of sensor nodes of WSNs is n and $n = q^2$, the scalability of WSNs can be described as $\min\{q^2 | q^2 > n, q, n \in \mathbb{Z}^+\}$.

In 3-D Ex-μ-sPBIBD, each point in V is denoted as coordinate of 3-D space which is the same as subscript of each block. As analyzed above, 3-D space should be defined as $q \times q \times q$, and then number of blocks in V is q^3. That is, if the number of nodes in WSNs is q^3, the scalability of WSNs can be described as $\min\{q^3 | q^3 > n, q, n \in \mathbb{Z}^+\}$. □

5.3. Network Resilience

Resilience represents security metrics of KPD against node capture in WSN. Because low performance nodes in WSNs are not equipped with tamper-resistant hardware [35] once one node is captured by an adversary, all of the information stored in the node including key material will be exposed. The adversary may use the captured keys to decrypt communication between other nodes that using the same keys. When the number of compromised sensor nodes reaches a certain value, all keys in the key pool will be exposed and the whole WSNs will be collapsed.

Resilience reflects the extent that the compromised nodes affect the remaining non-compromised nodes when WSNs suffer from attack of node capture. Resilience of WSNs is expressed as $Res(x)$, which denotes the broken probability of a link between two fixed non-compromised nodes when an attacker captures x other nodes [20]. The lower the value of $Res(x)$ is, the stronger the resilience of WSNs will be.

5.3.1. Resilience of 2-D μ-sPBIBD

As noted in Section 5.2, let V be square of q in 2-D μ-sPBIBD. Then two nodes have 2 or $q - 2$ shared-keys. In Figure 3, 2-D space with dimension $q \times q$ is depicted. Taking N_1 in Figure 3a as example, the relation among node, block and 2-D space in 2-D μ-sPBIBD scheme is descripted as follows. Suppose that N_1 is a sensor node in WSNs, a block B_{a_1,b_1} constructed in Section 4.1 is preloaded to N_1 as a key ring in which (a_1, b_1) is a point of V. Then, for simplicity, location of N_1 in 2-D space is denoted as (a_1, b_1).

1. If the number of shared-keys is 2

Suppose that node N_1 and N_2 share two keys. Two blocks corresponding to key rings preloaded to N_1 and N_2 are denoted as B_{a_1,b_1} and B_{a_2,b_2}. As presented in Figure 3, in 2-D space, points in B_{a_1,b_1}

cover orange and blue segments, while points in B_{a_2,b_2} cover green and blue segments. Figure 3a illustrates that B_{a_1,b_1} and B_{a_2,b_2} have common points (a_1, b_2) and (a_2, b_1) which represent key ID of two shared-keys between N_1 and N_2 (for simplicity, in the following analyses, we replace key with key ID).

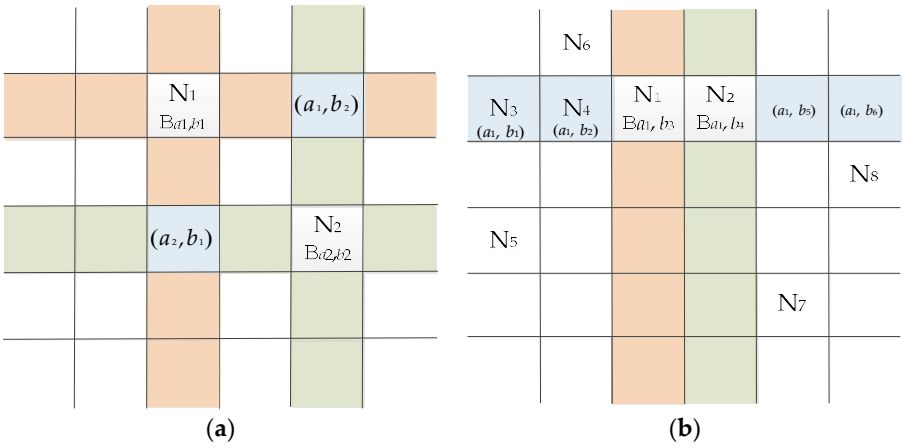

Figure 3. Key distribution and key-shared corresponding to 2-D sPBIBD. (**a**) 2 shared-keys; (**b**) $q-2$ shared-keys.

Resilience is repressed by the probability that communication between N_1 and N_2 will be compromised after x random nodes are captured. Suppose that H_{a_1,b_2} and H_{a_2,b_1} are two sets of blocks including (a_1, b_2) and (a_2, b_1), respectively. From Property 3, we have that

$$\left|H_{a_1,b_1}\right|=\left|H_{a_2,b_2}\right|=2q-2$$

and $\left|H_{a_1,b_1} \cap H_{a_2,b_2}\right|=2$. Then

$$\left|H_{a_1,b_1} \cup H_{a_2,b_2}\right|=2(2q-2)-2=4q-6.$$

To secure the communication between N_1 and N_2, (a_1, b_2) or (a_2, b_1) should not exist in the blocks associated with the x captured nodes. The number of ways of choosing x nodes unrelated to (a_1, b_2) is $\begin{pmatrix} q^2-2q+2 \\ x \end{pmatrix}$. Similarly, the number of ways of choosing x nodes unrelated to (a_2, b_1) is $\begin{pmatrix} q^2-2q+2 \\ x \end{pmatrix}$. Then the number of ways of choosing x nodes unrelated to $\left|H_{a_1,b_1} \cup H_{a_2,b_2}\right|$ is $\begin{pmatrix} q^2-4q+6 \\ x \end{pmatrix}$. Therefore, if x nodes are captured, network resilience, which is represented by the probability that communication with two fixed nodes is broken, can be given by

$$\begin{aligned} Res_1(x) = & \quad 1-\frac{2\begin{pmatrix} q^2-2q+2 \\ x \end{pmatrix}-\begin{pmatrix} q^2-4q+6 \\ x \end{pmatrix}}{\begin{pmatrix} q^2-2 \\ x \end{pmatrix}} \\ & \approx 1-2\left(1-\frac{2q-4}{q^2-2}\right)^x+\left(1-\frac{4q-8}{q^2-2}\right)^x \end{aligned} \tag{4}$$

2. If the number of shared-key is $q-2$

Two blocks will share $q-2$ keys if the two blocks corresponding to two key rings in node N_1 and N_2 have the same row-subscript (or column-subscript). In Figure 3b, blocks B_{a_1,b_3} and B_{a_1,b_4} have

the same row-subscript. Then the common points between B_{a_1,b_3} and B_{a_1,b_4} are all elements in a_1 row except (a_1, b_3) and (a_1, b_4).

As illustrated in Figure 3b, suppose blocks in N_1 and N_2 have the same row (or column). If an attacker captures x nodes, N_1 and N_2 will compromise in the following three cases:

(1) In x captured nodes, there are at last two nodes, such as N_3 and N_4, that the corresponding blocks have the same row (or column) subscript as the blocks in N_1 and N_2.
(2) In x captured nodes, there are one node, such as N_3, that the corresponding block has the same row (or column) subscript as the blocks in N_1 and N_2, and then another node, such as N_5, must be the node that corresponding block has the same column (or row) subscript as block in N_3.
(3) In x captured nodes, if subscripts of blocks in x captured nodes are different with those of N_1 and N_2, x should be greater than or equal to $q-2$ and there are at least $q-2$ captured nodes that column (or row) subscripts of the corresponding blocks are different with those of N_1 and N_2. Meanwhile, column (or row) subscripts of corresponding $q-2$ blocks are different from each other. For example, in Figure 3b, N_5, N_6, N_7 and N_8 are four nodes of x compromised nodes.

Resilience of the first two cases will be given by

$$Res_{2\_1}(x) = 1 - \frac{\begin{pmatrix} q^2-q \\ x \end{pmatrix} + \begin{pmatrix} q-2 \\ 1 \end{pmatrix}\begin{pmatrix} q^2-q \\ x-1 \end{pmatrix}}{\begin{pmatrix} q^2-2 \\ x \end{pmatrix}}. \tag{5}$$

In the third case, the number of ways of choosing x compromised nodes is given by

$$\begin{aligned} Ch(x) = & \begin{pmatrix} q(q-1) \\ x \end{pmatrix} \\ & -\begin{pmatrix} q-2 \\ 1 \end{pmatrix}\begin{pmatrix} (q-1)(q-1) \\ x \end{pmatrix} \\ & +\begin{pmatrix} q-2 \\ 2 \end{pmatrix}\begin{pmatrix} (q-1)(q-2) \\ x \end{pmatrix} \\ & + \\ & \cdots \\ & +(-1)^{\theta}\begin{pmatrix} q-2 \\ \theta \end{pmatrix}\begin{pmatrix} (q-1)(q-\theta) \\ x \end{pmatrix} \\ & +\cdots \\ & (q-1)(q-2) \geq x \geq q-2 \end{aligned} \tag{6}$$

and resilience of the third case will be given by

$$Res_{2\_2}(x) = \frac{Ch(x)}{\begin{pmatrix} q(q-1) \\ x \end{pmatrix}} \tag{7}$$

Then, if two nodes have $q-2$ shared-keys, resilience can be written as:

$$Res_2(x) = Res_{2\_1}(x) + Res_{2\_2}(x) \tag{8}$$

In terms of the construction of μ-sPBIBD, the probability that two blocks share $q-2$ points is given by

$$pro_2 = \frac{2q-2}{q^2-1} = \frac{2}{q+1}. \tag{9}$$

The probability that two blocks share 2 points is given by

$$pro_1 = 1 - pro_2 = \frac{q-1}{q+1}. \tag{10}$$

Finally, resilience of KPD scheme based on μ-sPBIBD can be computed by Equations (4) and (8)–(10). The resilience is expressed as follows:

$$\begin{aligned} Res(x) &= pro_1 \times Res_1(x) + pro_2 \times Res_2(x) \\ &= \frac{q-1}{q+1}\left(1 - 2\left(1 - \frac{2q-4}{q^2-2}\right)^x + \left(1 - \frac{4q-8}{q^2-2}\right)^x\right) \\ &+ \frac{2}{q+1}\left(1 - \frac{\binom{q^2-q}{x} + \binom{q-2}{1}\binom{q^2-q}{x-1}}{\binom{q^2-2}{x}} + \frac{Ch(x)}{\binom{q(q-1)}{x}}\right) \end{aligned} \tag{11}$$

5.3.2. Resilience of 3-D Ex-μ-sPBIBD

Resilience of 3-D Ex-μ-sPBIBD are similar to 2-D μ-sPBIBD. Suppose that x random nodes are captured. Resilience can be analyzed as follows.

1. If the number of shared-keys is 2

Suppose that subscripts of blocks of two nodes have different row and column in the same plane. The two nodes have two shared-keys, say (a_1, b_1, c_1) and (a_2, b_2, c_2). For example, suppose N_1 and N_2 in Figure 2 have two shared-keys and the corresponding points are (3, 5, 3) and (3, 4, 2). H_{a_1,b_1,c_1} and H_{a_2,b_2,c_2} are sets of blocks containing (a_1, b_1, c_1) and (a_2, b_2, c_2), respectively, where $a_1 = a_2$, $b_1 \neq b_2$ and $c_1 \neq c_2$. According to Property 3, we have

$$\left|H_{a_1,b_1,c_1}\right| = \left|H_{a_2,b_2,c_2}\right| = 3q-3$$

and

$$\left|H_{a_1,b_1,c_1} \cap H_{a_2,b_2,c_2}\right| = 2.$$

Then

$$\left|H_{a_1,b_1,c_1} \cup H_{a_2,b_2,c_2}\right| = 2(3q-3) - 2 = 6q-8.$$

In order to ensure the security of a link between N_1 and N_2, key rings of x captured nodes fail to contain the two keys (a_1, b_1, c_1) and (a_2, b_2, c_2). The number of ways of choosing x nodes unrelated to (a_1, b_1, c_1) is $\binom{q^3-3q+3}{x}$. Similarly, the number of ways of choosing x nodes unrelated to (a_2, b_2, c_2) is $\binom{q^3-3q+3}{x}$. Then the number of ways of choosing x nodes unrelated

to $\left|H_{a_1,b_1,c_1} \cup H_{a_2,b_2,c_2}\right|$ is $\begin{pmatrix} q^3-6q+8 \\ x \end{pmatrix}$. Therefore, if x nodes are captured, the probability $Res'_1(x)$ which a link between the two fixed nodes is broken will be given as follows:

$$\begin{aligned} Res'_1(x) &= 1 - \frac{2\begin{pmatrix} q^3-3q+3 \\ x \end{pmatrix} - \begin{pmatrix} q^3-6q+8 \\ x \end{pmatrix}}{\begin{pmatrix} q^3-2 \\ x \end{pmatrix}} \\ &\approx 1 - 2\left(1-\tfrac{3q-5}{q^3-2}\right)^x + \left(1-\tfrac{6q-10}{q^3-2}\right)^x. \end{aligned} \tag{12}$$

2. If the number of shared-keys is $q-2$

If subscripts of two blocks are coplanar and with the same row (or column), their corresponding nodes will have $q-2$ shared-keys. Taking N_2 and N_3 as example in Figure 2, we compute network resilience.

Coplanar two blocks in 3-D Ex-μ-sPBIBD can be viewed as two blocks in 2-D μ-sPBIBD. For simplicity, as analyzed in Section 5.3.1, it is similar to Equations (4)–(7) that the resilience of this case can be given by

$$Res'_2(x) = 1 - \frac{\begin{pmatrix} q^2-q \\ x \end{pmatrix} + \begin{pmatrix} q-2 \\ 1 \end{pmatrix}\begin{pmatrix} q^2-q \\ x-1 \end{pmatrix}}{\begin{pmatrix} q^3-2 \\ x \end{pmatrix}} + \frac{Ch(x)}{\begin{pmatrix} q(q-1) \\ x \end{pmatrix}} \tag{13}$$

In terms of construction of 3-D Ex-μ-sPBIBD, the probability that two blocks share 2 points can be given by

$$pro'_1 = \frac{3q-3}{q^2+q+1}. \tag{14}$$

The probability that two blocks share $q-2$ points can be given by

$$pro'_2 = \frac{3q-3}{q^3-1} = \frac{3}{q^2+q+1} \tag{15}$$

Finally, resiliency of KPD scheme based on 3-D Ex-μ-sPBIBD can be computed by Equations (12)–(15). Resilience can be expressed as follows,

$$\begin{aligned} Res'(x) &= pro'_1 \times Res'_1(x) + pro'_2 \times Res'_2(x) \\ &= \frac{3q-3}{q^2+q+1}\left(1-2\left(1-\frac{3q-5}{q^3-2}\right)^x + \left(1-\frac{6q-10}{q^3-2}\right)^x\right) \\ &+ \tfrac{3}{q^2+q+1}\left(1 - \frac{\begin{pmatrix} q^2-q \\ x \end{pmatrix} + \begin{pmatrix} q-2 \\ 1 \end{pmatrix}\begin{pmatrix} q^2-q \\ x-1 \end{pmatrix}}{\begin{pmatrix} q^3-2 \\ x \end{pmatrix}} + \frac{Ch(x)}{\begin{pmatrix} q(q-1) \\ x \end{pmatrix}}\right) \end{aligned} \tag{16}$$

6. Performance Comparison

In order to better analyze the performance of the proposed method, we compare with other combinatorial design based KPD schemes. Symmetric BIBD scheme [32] is a classical combinatorial design based deterministic key pre-distribution scheme, which mapped a symmetric design with parameters $(q^2+q+1, q+1, 1)$ to KPD scheme. RD scheme [30] constructed a residual design (RD) based on sBIBD with parameters $(q^2+q+1, q+1, 1)$ and was first time that used RD to KPD scheme, which improved the resilience and scalability comparing with sBIBD scheme. TD scheme [20] employed

linear construction and quadratic construction of transversal designs which were expressed as $TD(k, q)$ and $TD(\lambda, k, q)$, respectively, and it offered a lot of flexibility in trading off the various metrics.

In this section, we compare the proposed schemes with sBIBD scheme, RD scheme and linear TD scheme according to different criteria. For the sake of clarity, the parameters of different KPD schemes are listed in Table 3. We can find that metrics of linear TD scheme depend on two parameters k and q, which is different from others combinatorial schemes that only depend on one parameter.

6.1. Network Scalability

According to Table 3, we can obtain network scalability of these schemes. In sBIBD scheme, the key ring size was $k = q + 1$ and the maximum size of network supported by sBIBD scheme was $q^2 + q + 1$. In RD scheme, the key ring size was $k = q$ and the scalability of RD scheme was computed as $(q^2 + q + 1)(q + 1)$. In linear TD scheme, the key ring size was k and the probability that two sensor nodes shared a common key was Pr_1. Then a prime q was chosen such that $q + 1 \leq k/Pr_1$, and the maximum scale of network supported by linear TD scheme was q^2 [20]. In 2-D μ-PBIBD scheme, each node is preloaded with $k = 2q - 2$ distinct keys and the maximum network size that can be supported by 2-D μ-PBIBD scheme is q^2. The key ring size is $k = 3q - 3$ in 3-D Ex-μ-PBIBD scheme which can support network size up to q^3.

Table 3. Parameters of BIBD, RD, TD, 2-D μ-PBIBD and 3-DEx-μ-PBIBD.

Combinatorial Design	Key Pool Size	Number of Key Rings	Key Ring Size
BIBD [3]	$q^2 + q + 1$	$q^2 + q + 1$	$q + 1$
RD [30]	$q^2 + q + 1$	$(q^2 + q + 1)(q + 1)$	q
Linear TD [20]	kq	q^2	k
2-D PBIBD	q^2	q^2	$2q - 2$
3-D EX-PBIBD	q^3	q^3	$3q - 3$

The scalability of μ-PBIBD and Ex-μ-PBIBD are compared with sBIBD, RD and TD schemes when size of key ring increases from 10 to 100 by increments of 10. For linear TD scheme, we analyze the scalability in the case of $Pr_1 = 0.3$ and $Pr_1 = 0.9$. As expected, Ex-μ-PBIBD scheme performs better network scalability than μ-PBIBD scheme. Figure 4 shows that at the same key ring size, scalability of Ex-PBIBD is higher than, PBIBD, BIBD and TD($Pr_1 = 0.9$) scheme, while it is lower than RD and TD($Pr_1 = 0.3$) scheme. When key ring size is up to 100, the network sizes of the schemes in Figure 4 are 1020201, 110224, 40471, 12100, 9901, and 2601, respectively. Although the scalability of Ex-μ-PBIBD scheme is not the best among the above schemes, according to the data in Figure 4, we achieve that the key ring size in Ex-μ-PBIBD scheme can enough support the corresponding network size in practical WSNs.

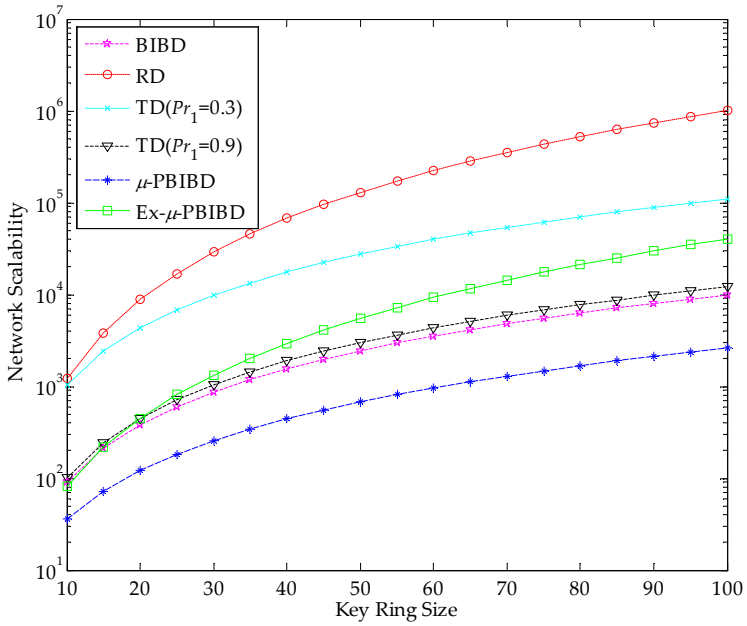

Figure 4. Comparison of network scalability of different KPD schemes at the same key ring size k.

6.2. Key Connectivity

In sBIBD scheme with parameters $(q^2 + q + 1, q + 1, 1)$, the probability of key shared between each pair of nodes was always 1. Thus, direct key connectivity of BIBD scheme is 1.

In RD scheme with parameters $(q^2 + q + 1, (q^2 + q + 1)(q + 1), q(q + 1), q, 1)$, the probability that any pair of blocks come from same class was given by

$$Q_{SC} = \frac{q^2 + q - 1}{(q^2 + q)(q^2 + q + 1) - 1} \tag{17}$$

and the probability of the pair of blocks shared one or more points was computed as

$$P_{SC} = \frac{q^2}{q^2 + q}. \tag{18}$$

The probability that any pair of blocks come from different classes was given by

$$Q_{DC} = \frac{(q^2 + q)^2}{(q^2 + q + 1)((q^2 + q)(q^2 + q + 1) - 1)} \tag{19}$$

and the probability that any pair of blocks shared one or more points was computed as

$$P_{DC} = \frac{q^4 + q - 1}{(q^2 + q)^2}. \tag{20}$$

The formula for Q_{SC}, P_{SC}, Q_{DC} and P_{DC} were given in Ref. [30]. Then key connectivity of RD scheme was expressed as

$$Con_{RD} = Q_{SC} * P_{SC} + Q_{DC} * P_{DC}$$

where Q_{SC}, P_{SC}, Q_{DC} and P_{DC} could be computed using Equations (17)–(20).

The key connectivity of Linear TD scheme was estimated as follows:

$$Con_{TD} = \frac{k}{q + 1} \tag{21}$$

Figure 5 shows key connectivity of the four combinatorial schemes. Any pair of nodes in sBIBD scheme and μ-sPBIBD scheme have at least one common key. Thus the two schemes have complete connectivity property. The connectivity of Linear TD scheme was determined by parameters k and q. In order to compare with the connectivity of Linear TD scheme, the network scale of TD scheme should be the same as that of Ex-μ-PBIBD. Figure 5 shows that at equal key ring size, Ex-μ-sPBIBD scheme has better connectivity than RD scheme when key ring size is more than 13. While it has worse connectivity than TD scheme. We can find that, as key ring size increases, direct connectivity of the proposed scheme decreases in Figure 5. This is due to fact that the probability of key-share tends to $O(1/k)$ when k tends to infinity.

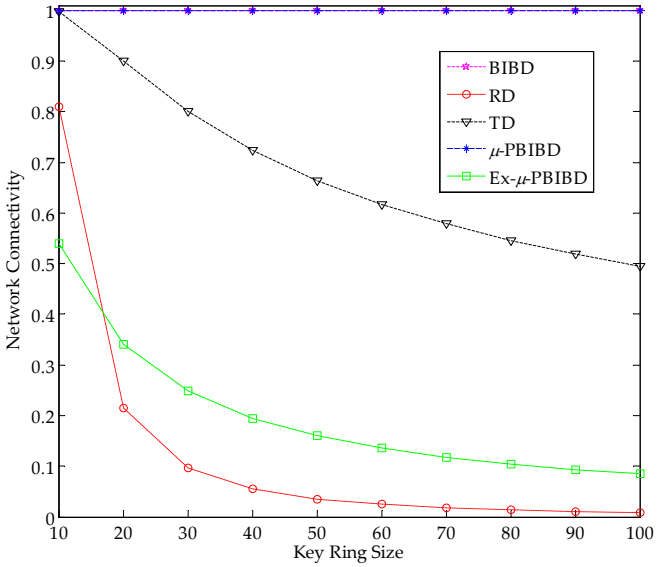

Figure 5. Comparison of key connectivity of different schemes at the key ring size.

6.3. Network Resilience

In this subsection, we discuss network resilience of the five schemes. The network resilience of the sBIBD scheme [32] was calculated as

$$Res_{\mathrm{BIBD}}(x) = 1 - \frac{\binom{q^2}{x}}{\binom{q^2+q+1}{x}} \tag{22}$$

where x represented the number of captured nodes.

In RD scheme, the network resilience [30] was given by

$$Res_{\mathrm{RD}}(x) = \sum_{j=1}^{q^2+q+1} \frac{\binom{q(q+1)}{2}}{\binom{(q^2+q+1)(q+1)}{2}} \left(1 - \frac{\binom{(q+1)(q^2+1)}{x}}{\binom{(q^2+q+1)(q+1)}{x}}\right) \tag{23}$$

where x was the number of captured nodes.

The network resilience of TD scheme in Reference [23] was computed using the following equation:

$$Res_{\mathrm{TD}}(\mathrm{x}) = 1 - (1 - \frac{q-2}{q^2-2})^{x}. \tag{24}$$

In Figure 6, we compare the network resilience of the five schemes at equal number of captured nodes for $k = 24$ and $k = 48$, respectively. In order to compare the performance of TD scheme in a similar setting, we consider two cases of TD schemes which have the same scalability and connectivity as those of our scheme, respectively. According to Figure 6, we can find that Ex-μ-sPBIBD scheme provides the best network resilience against compromised nodes in the five schemes. The figures reflect the fact that the network resilience of Ex-μ-PBIBD scheme hardly substantially declines, as the number of compromised node increases. Comparing Figure 6a with Figure 6b, the higher k is, the better the network resilience is in the case of the same number of captured nodes. That is because the session key between nodes is constructed by shared-keys of key rings between the two nodes. Then more nodes are needed to capture along with the increase of key ring size.

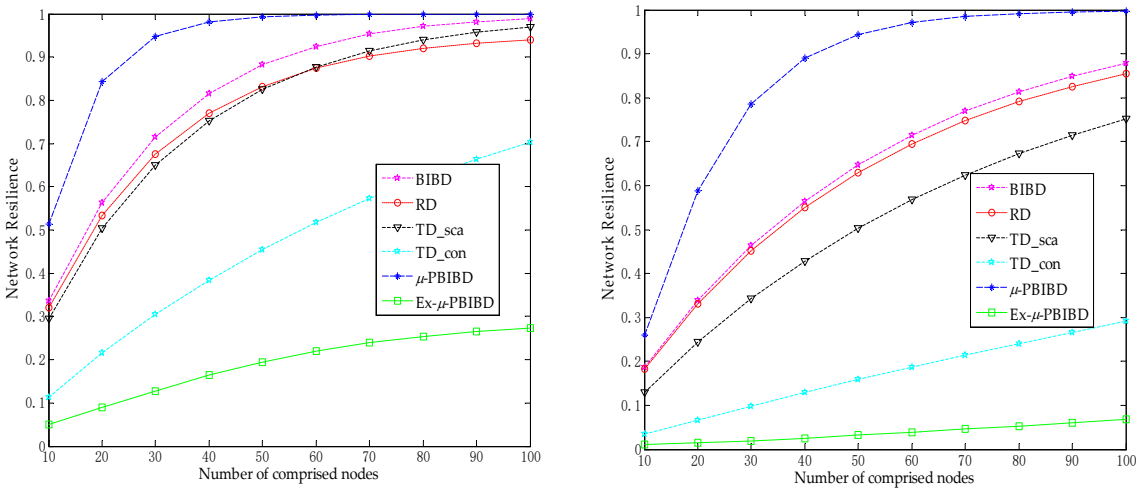

Figure 6. Comparison of resilience of different schemes at the same key ring size. In this figure, resilience is probability of compromised links between two fixed non-compromised nodes versus number of compromise nodes. TD_sca and TD_con are two cases of TD scheme which have the same scalability and connectivity as those of Ex-μ-PBIBD, respectively. (**a**) $k = 24$; (**b**) $k = 48$.

6.4. Additional Analysis

In Ex-μ-sPBIBD scheme, connectivity, scalability and resilience are determined by size of key ring (denoted by k). Thus, choosing the proper parameter k could achieve a trade-off between connectivity and resiliency. Comparing with TD scheme, we should normalize by fixing the size of key ring, k, and key connectivity, Con. Firstly, we computer connectivity of Ex-μ-PBIBD scheme using Equation (3). Next, fixing the size of key ring and the key connectivity, we obtain resilience of TD scheme from Equations (21) and (24) and scalability from Table 3. In Table 4, the parameter choices of schemes are summarized. Then we list the maximum network size (denoted by M) and resilience $Res(x)$ of two schemes. We could select the value of k according to requirement of practical WSN.

Table 4. Performance of schemes for values of k and Con fixed.

Parameter	Linear TD	Ex-PBIBD
$k = 24$ $Con = 0.3$	$M = 6241$ $Res(40) = 0.3915$ $Res(80) = 0.6297$ $Res(100) = 0.7112$	$M = 729$ $Res(40) = 0.1642$ $Res(80) = 0.2533$ $Res(100) = 0.2728$

Table 4. *Cont.*

Parameter	Linear TD	Ex-PBIBD
$k = 36$	$M = 28224$	$M = 2179$
$Con = 0.213$	$Res(40) = 0.2102$	$Res(40) = 0.0587$
	$Res(80) = 0.3762$	$Res(80) = 0.1131$
	$Res(100) = 0.4456$	$Res(100) = 0.1390$
$k = 48$	$M = 82944$	$M = 4913$
$Con = 0.166$	$Res(40) = 0.1290$	$Res(40) = 0.0251$
	$Res(80) = 0.2414$	$Res(80) = 0.0533$
	$Res(100) = 0.2921$	$Res(100) = 0.0677$

7. Conclusions

In this work, we defined a new combinatorial design, termed "μ-PBIBD" and constructed a 2-D μ-sPBIBD. We proposed a basic mapping from 2-D μ-sPBIBD to KPD which could achieve complete key connectivity and a poor network resilience. To enhance network resilience, we extended a set of keys V from 2-D space to 3-D space and proposed an extended 3-D Ex-μ-sPBIBD KPD scheme with better network scalability and high network resilience. The theoretical analysis and performance comparison with the existing schemes show that KPD scheme based on Ex-μ-sPBIBD increases the network scalability and provides the better network resilience.

Author Contributions: Q.Y. conceive and designed the research, and contributed as the lead author of the paper; H.Y. performed the experiments; X.B. analyzed the data; C.M. gave more valuable suggestion of the paper and revised the paper; Q.Y. and H.Y. wrote this paper.

Funding: This work was supported by National Nature Science Foundation of China (No. 61170241, 61472097).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

V	The basic set
p_i	The i point of V
v	The number of points in V
B	The block design of V
B_i	The i block in B
d	The number of blocks in B
k	The number of points in a block (i.e., key ring size)
r	The number of blocks in which a point is contain
λ	The number of blocks in which each pair of elements exist
$B(v, d, r, k, \lambda)$	Balanced incomplete block design with parameter v, d, r, k,λ
q	The order of finite projective plane corresponding to $sB(q^2 + q + 1, q + 1, 1)$
G	A partition of V
μ	The number of cases on the number of blocks in which each pair of points exist
M	the number of senor nodes in WSNs
(a, b)	The point in V in 2-D μ-PBIBD
m, n	The number of row and column when V is viewed as 2-D space
$K_{i,j}$	The session key between nodes Ni and Nj
$Res(x)$	The network resilience when an attacker captures x nodes
pro_1	The probability that two blocks share 2 keys
pro_2	The probability that two blocks share $q - 2$ keys
(a, b, c)	The point in V in 3-D μ-PBIBD
Con	The probability that two blocks have shared-key in Ex-μ-sPBIBD
Ni	The i node in WSNs

References

1. Mahmood, Z.; Ning, H.; Ghafoor, A. A Polynomial Subset-Based Efficient Multi-Party Key Management System for Lightweight Device Networks. *Sensors* **2017**, *17*, 670. [CrossRef] [PubMed]
2. Ge, M.; Choo, K.K.R.; Wu, H.; Yu, Y. Survey on key revocation mechanisms in wireless sensor networks. *J. Netw. Comput. Appl.* **2016**, *63*, 24–38. [CrossRef]
3. Lee, C.C.; Hwang, M.S.; Li, L.H. A new key authentication scheme based on discrete logarithms. *Appl. Math. Comput.* **2003**, *139*, 343–349. [CrossRef]
4. Lee, C.C.; Lin, T.H.; Tsai, C.S. A new authenticated group key agreement in a mobile environment. *Ann. Telecommun. Ann. Telecommun.* **2009**, *64*, 735–744. [CrossRef]
5. Tzeng, S.F.; Lee, C.C.; Lin, T.C. A Novel Key Management Scheme for Dynamic Access Control in a Hierarchy. *Int. J. Netw. Secur.* **2011**, *12*, 178–180.
6. Bechkit, W.; Challal, Y.; Bouabdallah, A. A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 948–959. [CrossRef]
7. Bechkit, W.; Challal, Y.; Bouabdallah, A. A new class of Hash-Chain based key pre-distribution schemes for WSN. *Comput. Commun.* **2013**, *36*, 243–255. [CrossRef]
8. Lee, C.C.; Li, C.T.; Chiu, S.T.; Lai, Y.M. A new three-party-authenticated key agreement scheme based on chaotic maps without password table. *Nonlinear Dyn.* **2014**, *79*, 2485–2495. [CrossRef]
9. Zhan, F.; Yao, N.; Gao, Z.; Tan, G. A novel key generation method for wireless sensor networks based on system of equations. *J. Netw. Comput. Appl.* **2017**, *82*, 114–127. [CrossRef]
10. Fakhrey, H.; Tiwari, R.; Johnston, M.; Al-Mathehaji, Y. The Optimum Design of Location-Dependent Key Management Protocol for a WSN with a Random Selected Cell Reporter. *IEEE Sens. J.* **2016**, *16*, 7217–7226. [CrossRef]
11. Bala, S.; Sharma, G.; Verma, A.K. A survey and taxonomy of symmetric key management schemes for wireless sensor networks. In Proceedings of the Cube International Information Technology Conference, CUBE'12, Pune, India, 3–5 September 2012; pp. 585–592.
12. He, X.; Niedermeier, M.; Meer, H.D. Review: Dynamic key management in wireless sensor networks: A survey. *J. Netw. Comput. Appl.* **2013**, *36*, 611–622. [CrossRef]
13. Raghini, M.; Maheswari, N.U.; Venkatesh, R. Overview on key distribution primitives in wireless sensor network. *J. Comput. Sci.* **2013**, *9*, 543–550. [CrossRef]
14. Pramod, T.C.; Sunitha, N.R. Key pre-distribution schemes to support various architectural deployment models in WSN. *Int. J. Inf. Comput. Secur.* **2016**, *8*, 139–157. [CrossRef]
15. Gandino, F.; Montrucchio, B.; Rebaudengo, M. Key Management for Static Wireless Sensor Networks With Node Adding. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1133–1143. [CrossRef]
16. Gharib, M.; Yousefi'Zadeh, H.; Movaghar, A. Secure Overlay Routing Using Key Pre-Distribution: A Linear Distance Optimization Approach. *IEEE Trans. Mob. Comput.* **2016**, *15*, 2333–2344. [CrossRef]
17. Zha, X.; Ni, W.; Zheng, K.; Niu, X.X. Collaborative Authentication in Decentralized Dense Mobile Networks with Key Predistribution. *IEEE Trans. Inform. Foren. Secur.* **2017**, *12*, 2261–2275. [CrossRef]
18. Zhang, Y.; Liang, J.; Zheng, B.; Chen, W. A Hybrid Key Management Scheme for WSNs Based on PPBR and a Tree-Based Path Key Establishment Method. *Sensors* **2016**, *16*, 509. [CrossRef] [PubMed]
19. Simplício, M.A., Jr.; Barreto, P.S.L.M.; Margi, C.B.; Carvalho, T.C.M.B. A survey on key management mechanisms for distributed Wireless Sensor Networks. *Comput. Netw.* **2010**, *54*, 2591–2612. [CrossRef]
20. Lee, J.; Stinson, D.R. On the Construction of Practical Key Predistribution Schemes for Distributed Sensor Networks Using Combinatorial Designs. *ACM Trans. Inf. Syst. Secur.* **2008**, *11*, 5. [CrossRef]
21. Xia, G.; Huang, Z.; Wang, Z. Key pre-distribution scheme for wireless sensor networks based on the symmetric balanced incomplete block design. *J. Comput. Res. Dev.* **2008**, *45*, 154–164.
22. Paterson, M.B.; Stinson, D.R. A unified approach to combinatorial key predistribution schemes for sensor networks. *Designs Codes Cryptogr.* **2014**, *71*, 433–457. [CrossRef]
23. Zhang, J.; Varadharajan, V. Wireless sensor network key management survey and taxonomy. *J. Netw. Comput. Appl.* **2010**, *33*, 63–75. [CrossRef]
24. Lee, J.; Stinson, D.R. Deterministic key predistribution schemes for distributed sensor networks. In Proceedings of the 11th International Workshop on Selected Areas in Cryptography, SAC2004, Waterloo, ON, Canada, 9–10 August 2004; pp. 294–307.

25. Lee, J.; Stinson, D.R. A combinatorial approach to key predistribution for distributed sensor networks. In Proceedings of the 2005 IEEE Wireless Communications and Networking Conference, WCNC 2005, New Orleans, LA, USA, 13–17 March 2005; pp. 1200–1205.
26. Ma, C.; Zhang, B.Z.; Sun, Y.; Wang, H.Q. Based on pair-wise balanced design key pre-distribution scheme for heterogeneous wireless sensor networks. *J. Commun.* **2010**, *31*, 37–43.
27. Xu, C.; Liu, W. Key Updating Methods for Combinatorial Design Based Key Management Schemes. *J. Sens.* **2014**, *2014*, 134357. [CrossRef]
28. Dargahi, T.; Javadi, H.H.S.; Hosseinzadeh, M. Application-specific hybrid symmetric design of key pre-distribution for wireless sensor network. *Secur. Commun. Netw.* **2015**, *8*, 1561–1574. [CrossRef]
29. Ding, J.; Bouabdallah, A.; Tarokh, V. Key Pre-Distributions From Graph-Based Block Designs. *IEEE Sens. J.* **2016**, *16*, 1842–1850. [CrossRef]
30. Modiri, V.; Javadi, H.H.S.; Anzani, M. A Novel Scalable Key Pre-distribution Scheme for Wireless Sensor Networks Based on Residual Design. *Wirel. Pers. Commun.* **2017**, *96*, 2821–2841. [CrossRef]
31. Gao, Q.; Ma, W.; Luo, W. A Combinatorial Key Predistribution Scheme for Two-Layer Hierarchical Wireless Sensor Networks. *Wirel. Pers. Commun.* **2017**, *96*, 2179–2204. [CrossRef]
32. Çamtepe, S.A.; Yener, B. Combinatorial design of key distribution mechanisms for wireless sensor networks. *IEEE/ACM Trans. Netw.* **2007**, *15*, 346–358. [CrossRef]
33. Henry, K.; Paterson, M.B.; Stinson, D.R. Practical Approaches to Varying Network Size in Combinatorial Key Predistribution Schemes. In Proceedings of the 20th International Conference on Selected Areas in Cryptography, SAC 2013, Burnaby, BC, Canada, 14–16 August 2013; pp. 89–117.
34. Colbourn, C.J.; Colbourn, M.J. *Algorithms in Combinatorial Design Theory*, 1st ed.; Elsevier Science Publishing Company: New York, NY, USA, 1985; p. 69. ISBN 0444878025.
35. Du, X.; Guizani, M.; Xiao, Y.; Chen, H.H. A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 1223–1229. [CrossRef]