ORIGINAL RESEARCH PAPER
Pages: 271-282

Survey of Effective Combinatorial Design Schemes in Wireless Sensor Networks Security

NafisehMasaeli[1], Hamid Haj SeyyedJavadi[2] and Seyed Hossein Erfani[3]
[1,3]Department of Computer Engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran
[2]Department of Mathematics and Computer Science, Shahed University, Tehran, Iran
st_n_masaeli@azad.ac.ir; h.s.javadi@shahed.ac.ir;h_erfani@azad.ac.ir
Corresponding author*: h_erfani@azad.ac.ir*

DOI: 10.22070/jce.2021.14655.1189

***Abstract*- Wireless sensor networks (WSNs) are made up of thousands of small sensor nodes that are capable of detecting, calculating, and transferring data via networks. Although there are certain resource limits, wireless transmission is still an effective way to transport information. The secure transfer of data is critical in a WSN. Key management techniques have been established for the purposes of security. Key pre-distribution is one of the key management methods used to assign keys to the devices before deploying them in the wireless sensor networks. The challenges of these schemes include memory consumption due to limited device resources, scalability, connectivity, and resilience against node capture attacks. Combinatorial designs with neutrality characteristics, which are based on mathematical structure and impose low computational overhead and communication overhead, are used in key pre-distribution and information security of wireless sensor networks. In this paper, some key pre-distribution methods based on the combinatorial designs are reviewed. Finally, comparison of performance parameters is illustrated in tables. Suggestions to improve future research are considered as well.**

***Index Terms*-**combinatorial designs, key management, key pre-distribution, security, wireless sensor networks.

I. INTRODUCTION

Wireless sensor networks consist of a large number of sensors randomly distributed throughout the environment. Wireless sensor networks have no fixed infrastructure; therefore, key distribution is one of the information security challenges of these networks. Symmetric and asymmetric key encryption methods have been proposed to enhance the security of the communication channel; but asymmetric key

Manuscript received day-Month-year and revised day-Month-year, P- ISSN:2322-4088
Accepted on day- month-year *E- ISSN: 2322-3936*

cryptography requires considerable computing resources and is not suitable for scenarios with limited resources[1, 2]. Another method of distributing keys is using a key distribution center (KDC). Each node must share a unique symmetric key with the KDC to distribute and authenticate it, which increases the number of security packets sent and the bottlenecks around nodes close to KDC. The security of these schemes depends on the security of the KDC. This method requires a fixed infrastructure with secure servers, often unavailable. Key pre-distribution (KPS) refers to how the keys are distributed across nodes before deployment in the environment [3, 4]. There is a key pool in key pre-distribution patterns that contains all the keys used in the network. Before deployment, a key chain from the key pool assigns to each node. If two neighboring nodes have a common key, they can communicate securely using cryptographic methods. Therefore, key selection should be done to improve the possibility of sharing at least one common key between two neighboring nodes. If two nodes do not share a key, they communicate via the key path [5-8]. There are different key pre-distribution methods, with their own set of features and functions. One of the weaknesses of key pre-distribution patterns is their limitation of scalability [3, 9]. The capacity to manage keys in large networks with many nodes is referred to as scalability. The amount of memory required to hold the keys equals the storage overhead. The storage of keys in each node has a memory constraint; thus simple calculations are required to consume fewer resources. Connectivity is one of the essential parameters in key pre-distribution. The ability to communicate directly or in multiple hops between two nodes is referred to as a connection. Another crucial measure in evaluating the performance of key pre-distribution patterns is resilience to captured nodes. The discovery of keys and certificates stored in nodes results in information exposure and network capture [1, 2, 10, 11]. The goal of this paper is to study some key pre-distribution approaches in fog computing and wireless sensor networks that are based on combinatorial design strategies, as well as to estimate evaluation factors including scalability, memory overhead, network connectivity, and resilience against node capture attacks. In the second part of this article, the work done in key pre-distribution is reviewed. In the third part, several key pre-distribution methods based on combinatorial designs are reviewed. In the fourth part, the results obtained from the presented methods are evaluated. In the fifth part, the results are summarized.

II. RELATED WORK

Key pre-distribution schemes in networks can be classified into three categories: probabilistic, deterministic, and hybrid[12]. In the random method; the keys are randomly selected from a key pool and stored on each node. In this method; the two nodes might not be directly discovered. Eschenauer and Gligo (EG) is the first random distribution scheme [10, 13]. After that; the basic design was generalized, and the q-

composite scheme was proposed [14, 15]. Deterministic key pre-distribution methods are designed to increase network connectivity. There are many deterministic key pre-distribution schemes, such as the Blom design [16] and the Blundo design [17]. In the hybrid method; the keys are assigned to each node using both random and deterministic methods. The random method improves scalability and resiliency against node capture, while the deterministic method improves network connectivity. Hybrid design improves scalability and resiliency against node capture. Two simple ways of key pre-distribution are the single key pattern and the pair key pattern. The single key pattern assigns a common key to all nodes. As a result, two nodes can communicate with each other. Although this technique has a small memory overhead, it has a high resiliency against node capture. Each pair of nodes is given a unique key that they can use to communicate with others in the pair key pattern. The network resiliency in this scenario is high. Because each node in a network with $n$nodes must keep $n-1$ keys, this value grows linearly in large networks, and storage is unfeasible due to the nodes' limited memory. Because these two methods are inefficient, key pre-distribution schemes should have minimum storage space and high resiliency. A key pool of keys and identifiers is generated during the EG key pre-distribution phase. For each node, $k$keys are chosen randomly from the key pool without being placed [10]. To find the common key; the two neighboring nodes exchange and compare the list of key identifiers in their key chains during the key discovery phase. They can choose one of their shared keys as their private communication key to communicating with each other; the key path establishment phase occurs if no common key exists between neighboring nodes. If the key pool has p keys and the key chain length is k; the probability of network connectivity is $1-\frac{(P-k)!^2}{(p-2k)!P!}$. In the q-composite key pre-distribution method [14], when two nodes share at least q common keys, they can compute a private key to communicate with each other. This approach provides more resiliency than EG, and the probability of network connectivity decreases because q keys must share instead of having one. Blom matrix-based method [18] is not for key distribution in sensor networks, but many key distribution schemes are made using the Blom method. Blundo method [17] is based on symmetric polynomials. This polynomial is used to calculate the common key among sensor nodes. The probability of key sharing in this scheme is one. When the degree of the polynomial is t, each node saves $t+1$ keys. It will not obtain any information about the keys of the unoccupied nodes if the $s \leq t$ nodes are compromised, but by capturing $t+1$ node or more, all the keys can be easily compromised. The finite generalized quadrangle (GQ) method's network connectivity is complete; however it is not scalable [16]. Liu et al. method [19] is a hybrid of the random EG method [10] and the deterministic Blundo method [17]. In this method, two-variable polynomials are stored on each node instead of the key. Table I summarizes the major notations used in this paper.

Table I. LIST OF MAIN NOTATIONS.

Notations	Description
q, p	Prime numbers
X	The set of pairs of points, $X = Z_k \times Z_q$
$TD(k, q)$	A transversal design, $2 \leq k \leq q$
$TD_{total}(q)$	Set of $TD(k, q)$
$\mathcal{H}_{total}(q)$	Set of $H^k(q)$groups, $2 \leq k \leq q$
$\mathcal{H}^k(q)$	Set of $H_x^k(q)$ groups, $x \subseteq \mathbb{Z}_k$
$H_x^k(q)$	The group of $TD(k, q)$
$\mathcal{A}_{total}(q)$	Set of $A^k(q)$ blocks
$\mathcal{A}^k(q)$	Set of $A_{(i,j)}(q)$ blocks
$A_{(i,j)}(q)$	The block of$TD(k, q)$, $(i, j) \in \mathbb{Z}_q \times \mathbb{Z}_q$
$\mathcal{H}^q(q)$	The largest groups of
$\mathcal{A}'_{total}(q)$	Set of blocks of the residual TD

III. KEY PRE-DISTRIBUTION SCHEMES BASED ON COMBINATORIAL DESIGN SCHEMES

A. Combinatorial Designs Types

Combinatorial design schemes are one of the methods used in designing a deterministic key pre-distribution pattern [16, 20]. In this section, some combination designs are briefly introduced.

Definition 1: A design is a pair $(X, \mathcal{A})$ such that $X = \{x_1, x_2, \cdots, x_v\}$ is a set of points and $\mathcal{A} = \{B_1, B_2, \cdots, B_b\}$ is a nonempty subset of X called a block. $\mathcal{A}$ block design is called simple if there are no duplicate blocks.

Definition 2: An incompletely balanced block design is represented by either (v, k, λ) or (v, b, r, k, λ). Let v, k, and λ be positive integers, $v > k \geq 2$. Suppose X is a set with v elements. $A = \{B_1, B_2, \cdots, B_b\}$ is a subset of the Xcalled balanced incompletely block design (BIBD). The arrangement v of a separate object in $b$blocks for each $1 \leq i \leq b$; the subset B_i so that each block contains exactly k distinct objects and $k < v$. Each object $x \in X$ exists exactly in a different block r, r is a subset of B_i, $1 \leq i \leq b$ [21].

For general block designs, each pair $x, y \in X$is assigned a number λ_{xy}, if λ_{xy} is the same for all pairs of elements X, then λ represents this common size and is called a balanced design because each block contains $k < v$ elements.

Definition 3: A BIBD is called asymmetric design or an SBIBD when $b = v$ or $r = k$. This scheme is represented as (v, k, λ)-SBIBD. For each power of the prime number $q \geq 2$, there is an asymmetric

scheme $(q^2+q+1, q+1, 1)$ [11]. Each block contains $r = k$ elements; Each element occurs in $r = k$blocks; each pair of members appears in the λ blocks; both blocks are the same in λ.

Definition 4: Transversal design, $TD(k, q)$, contains k groups with size q and is also displayed in triplicate (X, H, A). X contains a set with points kq. $\mathcal{H}$ contains a set of groups. $\mathcal{A}$ contains a set of blocks; Each group $H \in H$ and each block $A \in \mathcal{A}$ are in the same member, $|H \cap A| = 1$. Both blocks are common to a maximum of one member. Each pair of points x_1 and x_2 from different groups occurred in one block $\mathcal{A}$ [22].

Definition 5 : Assume that (X, A) is asymmetric (v, k, λ)-BIBD, and let $A_0 \in A$. Define $Res(X, A, A_0) = (X \backslash A_0, \{A \backslash A_0 : A \neq A_0\})$. $Res(X, A, A_0)$ is called a residual BIBD [9, 11, 23].

B. Application of Combinatorial Designs in Wireless Sensor Networks

In the Naive unital-based key pre-distribution (NU-KP) method, a uniform key pre-distribution model is proposed by Bechkit et al. [24]. The uniform design is $(q^3+1, q^2(q^2\text{-}q+1), q^2, q+1, 1)$. So $q^2(q^2\text{-}q+1)$ are key chains, and the size of each key chain equals $q+1$. The key pool has the size of q^3+1. To increase the probability of a common key and high scalability, a uniform key pre-distribution pattern is presented as t-UKP. In this method; the design of the blocks is uniform, and in each node, a separate block t is preloaded. Different values of t lead to different results; therefore, $t = \sqrt{q}$ is considered to increase scalability and key sharing probability. A pre-distribution scheme for hierarchical wireless sensor networks has been proposed by Javanbakht et al. [25]. The groups and blocks in $TD(k, q)$ are allocated to cluster heads (CHs) and cluster members, respectively. On the other hand; the cluster heads communicate with each other using the BIBD. The Dargahi et al. method [26] proposed a key pre-distribution pattern based on combinatorial and hybrid designs. The key chain in this model is selected from two different key pools and is suitable for small networks. The Residual Method (RD-KP) [27] is a key pre-distribution pattern using combinatorial design schemes. In this method, a new residual design is made by SBIBD with parameters $(q^2+q+1)(q^2+q)$. The length of the key chain in this pattern equals $k = q+1$, and the size of the key pool is $v = q^2+q+1$. $N = (q^2+q+1)(q^2+q)$ is the number of nodes supported in this design. Each key is in the $q^2(q+1)$ block. Merging hybrid symmetric design (MGHS) [28] is a deterministic key pre-distribution that improves network connectivity and resilience against node capture attacks. The sensor nodes are connected directly or multi-hop. In the key pre-distribution phase; the key chains generated at the base station are distributed on the nodes before being deployed in the network; then the key construction step is performed by the sensor nodes. During this phase, each pair of keys that are in communication with each other try to find a common key, and if none

exists, a key path is constructed between them. To establish a stable communication channel in fog networks, Bahrami et al. [23] scheme is built on SBIBD and the residual scheme. The cloud layer, fog layer, and end node layer make up the hierarchical network. Direct or multi-hop communication is used between nodes. The fog layer has two simulated layers, one of which is attached to the end nodes directly. The cloud layer is in direct communication with the base station layer, which is situated above the CH layer and has more resources and capabilities. The key pool containing $p^2 + p + 1$ blocks are created using SBIBD in the pre-distribution phase, and $(p^2 + p + 1)^2$ blocks are created using the residual design. As a result, CHs are assigned $p^2 + p + 1$ blocks, whereas end nodes are assigned $(p^2 + p + 1)(p^2 + p)$ blocks. Transversal design and residual theorem (TD-R) [29] is a key pre-distribution approach. The transversal design and the residual TD schemes are used to assign keys to each node based on. In the TD-R, $TD_{total}(q) = \cup_{k=2}^{q} TD(k, q)$ is constructed using the $TD(k, q)$ scheme. $TD_{total}(q)$ contains a set of groups called $H_{total}(q)$ and a set of blocks called $A_{total}(q)$. Moreover, the set of groups equals $H_{total}(q) = \cup_{k=2}^{q} H^k(q)$. Thus, $H^k(q) = \{H_x^k(q): 0 \leq x \leq k\text{-}1\}$ and $H_x^k(q) = \{x\} \times Z_q$. $A_{total}(q)$ blocks are constructed based on the $A_{total}(q) = \cup_{k=2}^{q} A^k(q)$. So that $A^k(q) = \{A_{(i,j)}(q): (i, j) \in Z_q \times Z_q\}$ and $A_{(i,j)}(q) = \{(x, (ix + j) \bmod q): x \in Z_k\}$. As a result, $TD_{total}(q)$ is a set of $TD(k, q)$ for all k in the range 2 to q , $2 \leq k \leq q$. Also using the residual TD theorem; the blocks $A_{total}(q)$ are reconstructed as $A'_{total}(q) = A_{total}(q) \backslash A_{(i,j)}(q)$. Table II shows the evaluation parameters in the key pre-distribution schemes.

IV. EVALUATION PARAMETERS OF SCHEMES

The methods of Javanbakht et al. [25], MGHS [28], Bahrami et al. [23], and TD-R [29] are investigated in this section using evaluation parameters such as memory overhead, scalability, network connectivity, and resilience to node capture.

A. Memory Overhead

The resource limit in wireless sensor networks is one of the fundamental issues in establishing a key management scheme. $TD(k, q)$ groups are allocated to cluster heads in Javanbakht et al. [25], so the qkey is preloaded on each CH node. The BIBD is used by the CHs to communicate with one another. As a result, each CH node has the $p + 1$ key preloaded. Consequently, each CH has $p + 1$ BIBD keys and q keys of $TD(k, q)$ preloaded; therefore; the total number of keys on each CH node is $q + p + 1$. End nodes are allocated $TD(k, q)$ blocks (cluster members). The blocks have a key chain length of k. As a result, each end node has exactly k keys preloaded. k has a maximum value of q, $2 \leq k \leq q$. SBIBD

blocks are combined with parameters $(p^2 + p + 1, p + 1,1)$in the MGHS method [28] to generate key chains. The blocks' key chains have a length of $p + 1$. In Bahrami et al. [23]; the key chain of the c_i class is preloaded on each node $c_i = X\backslash B_i$. According to BIBD; the length of the block key chain in Xis $p^2 + p + 1$ and in B_i is $p + 1$. Using the residual theorem; the common keys between B_i and Xare recovered from X, resulting in a key chain length of p^2 in each fog node. The end nodes' key chain length is p because the key chain length of the blocks in BIBD is $p + 1$, and the two separate BIBD blocks have precisely one thing in common. One common key is eliminated as a result of the residual theorem. The number of fog nodes and end nodes in the TD-R model is q^2(q-1) and q^4(q-1)^2, respectively. The number of end nodes is given by the formula $|N_e| = q^4$(q-1)^2. The A'_{total}(q)the key chain is pre-distributed to the end nodes, with q keys in each end node.

B. Scalability

Blocks are assigned to end nodes in Javanbakht et al. [25], resulting in q^2 end nodes. The BIBD is used by the CHs to communicate with one another, hence the number of fog nodes is $p^2 + p + 1$. In the MGHS method [28]; the size of the network is N; $q^2 + q + 1 < N$. SBIBD generates $b = q^2 + q + 1$ key chains and assigns them to bnodes using the parameters $(q^2 + q + 1, q + 1,1)$. Merged blocks, on the other hand, are used for N-b nodes. dis the number of merged blocks used to build the residual key chains, where d is the number of merged blocks $2 < d < q + 1$. If d-s blocks have exactly one common key for $0 \leq s \leq$ d-s, then the new set size is $k' =$ d$(q + 1)$-$(s + 1)$d $+ \frac{(s+1)(s+2)}{2}$. The set of new objects is identical to the main pool if $d = q + 1$ and $s = 0$. To produce the remaining N-b key blocks, d blocks from the symmetric BIBD blocks are randomly chosen and combined to form a new set A. The remaining N-b blocks are then chosen at random from the new Aset's k subset. BIBD blocks are assigned to fog nodes in Bahrami et al. [23], and the total number of fog nodes is $p^2 + p + 1$. New blocks based on the residual theorem are constructed and assigned to the end nodes by eliminating the BIBD blocks' shared keys; consequently; the number of end nodes equals $(p^2 + p + 1)(p^2 + p)$. In the TD-R scheme, the number of fog nodes and end nodes is q^2(q-1) and q^4(q-1)^2, respectively. The TD-R supports large networks with a large number of nodes.

C. Network Connectivity

The possibility of a shared key among nodes that links different parts of the network is referred to as

TABLE II. THE EVALUATION PARAMETERS IN THE KEY PRE-DISTRIBUTION SCHEMES.

Patterns	Scalability	Memory	Connectivity	Resiliency	Description
BIBD [21]	✓	✓	✓	✓	Based on block design
TD [22]	✓	✓	✓	✓	Based on BIBD
NU-KP [30]	-	-	✓	-	Based on BIBD
Javanbakht et al. [25]	✓	✓	✓	✓	Based on TD and BIBD
Dargahi et al. [26]	✓	-	✓	-	Based on BIBD
RD-KP [27]	✓	✓	✓	-	Based on BIBD
MGHS [28]	✓	✓	✓	✓	Based on BIBD
Bahrami et al. [23]	✓	✓	✓	✓	Based on BIBD and residual design
TD-R [29]	✓	✓	✓	✓	Based on TD and residual design

network connection. The probability of key sharing between the end nodes and the cluster headers is equal to 1 in Javanbakht et al.[25], $|H \cap A| = 1$. The cluster headers in this method communicate with each other using the BIBD scheme. Increasing or decreasing the number of clusters has no effect on reducing or increasing the probability of key sharing. In the MGHS method [28]; the key sharing probability is more than 85%, which means that nodes can communicate directly. The probability of object sharing between each pair of blocks in $B \cup H$ is investigated, where B is a set of symmetric design blocks and H is a set of randomly selected blocks from the k subset of the new object set A. For each block pair (α, β) of the set $B \cup H$. There are three types of modes (type BB: $\alpha \in B$ and $\beta \in B$, type HH: $\alpha \in H$ and $\beta \in H$, type HB:($\alpha \in H$and $\beta \in B$) or ($\alpha \in B$and $\beta \in H$)).

The probability of each block pair (α, β) equal to $Q_{BB} = \frac{b(b-1)}{N(N-1)}$, $Q_{HB} = \frac{2\,b(N-b)}{N(N-1)}$ and $Q_{HH} = \frac{(N-b)(N-b-1)}{N(N-1)}$. The probability of P_{MGHS} each pair of blocks sharing one or more objects is $P_{MGHS} \geq Q_{BB} + \frac{2}{3}Q_{HB} + Pr_{HH}Q_{HH}$ and $P_{MGHS} \leq Q_{BB} + Q_{HB} + Q_{HH}$. The probability of key sharing, according to Bahrami et al. [23] is $\frac{p^2}{p^2+p-1}$. The BIBD key chains are allocated to CHs so that they can communicate directly. Since each CH has a common key with its members, two nodes from two different clusters can communicate with each other via CHs. The TD-R scheme [29] allocates groups and blocks $TD_{total}(q)$ to cloud nodes and fog nodes, respectively. Because the cloud and fog nodes have the same key $|H \cap A| = 1$; the network connectivity between them is maintained completely. As a result, they can interact directly. In the TD-R model; the $H_{total}(q)$ groups and the $A'_{total}(q)$ blocks are allocated to the cloud node

TABLE III. COMPARISON OF THE EVALUATION PARAMETERS OF SCHEMES.

Patterns / **Attributes**	**Javanbakht et al.** [25]	**MGHS** [28]	**Bahrami et al.**[23]	**TD-R** [29]
Key size in each end nod	q	$p+1$	q	q
Key size in each fog node	$q+p+1$	-	p^2	q
Number of fog nodes	p^2+p+1	-	p^2+p+1	$q^2(q-1)$
Number of end nodes	q^2	$(p^2+p+1)^2$	$(p^2+p+1)(p^2+p)$	$q^4(q-1)^2$
Connection between cloud and fog nodes	-	-	1	1
Connection between cloud and end nodes	-	-	1	$1-(\frac{q-t}{q})^k$
Connection between fog nodes	1	-	1	$\frac{k}{q+1}$
Connection between fog and end nodes	1	-	1	$\frac{k}{q+1}$
Connection between end nodes	1	$P_{\text{MGHS}} \geq Q_{BB}+\frac{2}{3}Q_{HB}+Pr_{\text{HH}}Q_{HH}$ $P_{\text{MGHS}} \leq Q_{BB}+Q_{HB}+Q_{HH}$	$\frac{p^2}{p^2+p-1}$	≤ 1
Resiliency	-	$(p^2+p+1)\frac{((p+1)\binom{k'-1}{p})}{\binom{(p^2+p)(p^2+p+1)}{2}}$	$\frac{\binom{p+1}{2}}{\binom{(p^2+p)(p^2+p+1)}{2}}$	-

and the end nodes, respectively. The number of groups $H^q(q)$ equals qand the length of the key chain $A'_{\text{total}}(q)$ is k. The probability that the key is not on the cloud equals $\frac{q-t}{q}$ if t is the number of groups in each cloud node. As a result, the probability of a shared key between the cloud node and the end nodes equals $1-(\frac{q-t}{q})^k$. Both blocks $A_{\text{total}}(q)$ have a maximum of one common key, $|A_i \cap A_j| \leq 1$. The authors in [22] and [31] claim that the probability of having a common key between two neighboring nodes in the $TD(k,q)$ equals $\frac{k}{q+1}$. $k=q$ is the maximum network connection for each $TD_{\text{total}}(q)$.The network connection increases with each $TD_{\text{total}}(q)$, with qremaining constant as k rises. The network connection increases when q is at its peak where the number of nodes is almost constant and has not changed, or the number of nodes has increased.

A. Resiliency

According to Javanbakht et al. [25], the number of broken links divided by the total number of uncompromised nodes equals the resiliency against node capture. The resistance increases as the number of clusters grows, but this has no impact on network connectivity improvement. The probability of compromising the link in the case of node capture, according to the MGHS method [28], is $(p^2 + p + 1)\frac{((p+1)\binom{k'-1}{p})}{\binom{(p^2+p)(p^2+p+1)}{2}}$, where k' is the size of set A. By merging the blocks and establishing a new block, reducing network connectivity in the symmetrical design has been solved. According to BIBD, d blocks are fused. The parameter d determines network connectivity. Low-value d results in high network connectivity, whereas a high-valued results in increased resiliency. Due to the distinction of the keyspace in the Bahrami et al. [23] model, node capture in a cluster head does not affect cluster members. $\frac{\binom{p+1}{2}}{\binom{(p^2+p)(p^2+p+1)}{2}}$ is the probability that any link between the two compromised nodes will be broken. At minimum one group of the set $H^q(q)$ is preloaded into each cloud node in the TD-R scheme. The number of preloaded groups on each cloud node determines its resiliency. A cloud node is made up of tgroups and has tq keys. $\frac{t}{q}$ represents the ratio of the number of groups assigned on each cloud node to the total number of groups. Table III compares the approaches of Javanbakht et al. [25], MGHS [28], Bahrami et al. [23], and TD-R [29].

V. CONCLUSION

Key pre-distribution is one of the most crucial steps in the key management process, which is used to solve the key deployment problem. In key pre-distribution, combinatorial design schemes can be used to design deterministic key pre-distribution. The evaluation results of these designs show that removing the condition of full network connectivity improves the resiliency against node capture attacks, but the constant length of the key chain still poses scalability challenges. Future research could concentrate on methods to improve resiliency against node capture attacks by employing combinatorial design schemes. In addition, a model for updating and distributing keys can be provided as part of future research. It is also possible to include a new approach in which scalability, network connectivity, resilience to node capture attacks, and other network evaluation parameters are independent of the parameters.

REFERENCES

[1] J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," *Journal of network and computer applications*, vol. 33, no. 2, pp. 63-75, Mar. 2010.

[2] C. Y. Chen and H. C. Chao, "A survey of key distribution in wireless sensor networks," *Security and Communication Networks*, vol. 7, no. 12, pp. 2495-2508, July 2014.

[3] M. Anzani, H. H. S. Javadi, and A. Moeni, "A deterministic key predistribution method for wireless sensor networks based on hypercube multivariate scheme," *Iranian Journal of Science and Technology, Transactions A: Science*, vol. 42, no. 2, pp. 777-786, July 2018.

[4] H. Haj Seyyed Javadi and M. Anzani, "Hybrid Key pre-distribution scheme for wireless sensor network based on combinatorial design," *Journal of Advances in Computer Engineering and Technology*, vol. 1, no. 3, pp. 33-38, Apr. 2015.

[5] K. Alhamazani et al., "An overview of the commercial cloud monitoring tools: research dimensions, design issues, and state-of-the-art," *Computing*, vol. 97, no. 4, pp. 357-377, Apr. 2015.

[6] M. Ali et al., "SeDaSC: Secure data sharing in clouds," *IEEE Systems Journal*, vol. 11, no. 2, pp. 395-404, June 2015.

[7] B. Guan, J. Wu, Y. Wang, and S. U. Khan, "CIVSched: A communication-aware inter-VM scheduling technique for decreased network latency between co-located VMs," *IEEE trans. cloud computing*, vol. 2, no. 3, pp. 320-332, July 2014.

[8] S. H. Erfani, H. H. Javadi, and A. M. Rahmani, "A dynamic key management scheme for dynamic wireless sensor networks," *Security and Communication Networks*, vol. 8, no. 6, pp. 1040-1049, Apr. 2015.

[9] V. Modiri, H. H. S. Javadi, A. M. Rahmani, and M. Anzani, "Using Residual Design for Key Management in Hierarchical Wireless Sensor Networks," *Information Systems & Telecommunication*, p. 53, Feb. 2020.

[10] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," *in Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 41-47, Nov. 2002.

[11] D. Stinson, Combinatorial designs: constructions and analysis. Springer Science & Business Media, 2007.

[12] N. S. Esfehani and H. H. S. Javadi, "A survey of key pre-distribution schemes based on combinatorial designs for resource-constrained devices in the IoT network," *Wireless Networks*, vol. 27, no. 4, pp. 3025-3052, May. 2021.

[13] J. Dong, D. Pei, and X. Wang, "A key predistribution scheme based on 3-designs," *in International Conference on Information Security and Cryptology*, pp. 81-92: Springer, Sept. 2007.

[14] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," *in 2003 Symposium on Security and Privacy*, *IEEE*, pp. 197-213, May. 2003.

[15] P. Schaffer, K. Farkas, A. Horvath, T. Holczer, and L. Buttyan, "Secure and reliable clustering in wireless sensor networks: a critical survey," *Computer Networks*, vol. 56, no. 11, pp. 2726-2741, July 2012.

[16] S. A. Camtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," *in European symposium on research in computer security*, pp. 293-308: Springer, 2004.

[17] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," *in Annual international cryptology* conference, pp. 471-486: Springer, May. 1992.

[18] R. Blom, "An optimal class of symmetric key generation systems," *in Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 335-338: Springer, Dec. 1984.

[19] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, no. 1, pp. 41-77, Feb. 2005.

[20] I. Anderson, Combinatorial designs: construction methods. Ellis Horwood Chichester, 1990.

[21] A. Pattanayak and B. Majhi, "Key Predistribution Schemes in Distributed Wireless Sensor Network using Combinatorial Designs Revisited," *IACR Cryptol. ePrint Arch.*, vol. 2009, pp. 131, 2009.

[22] J. Lee and D. R. Stinson, "A combinatorial approach to key predistribution for distributed sensor networks," *in IEEE Wireless Communications and Networking Conference*, vol. 2, pp. 1200-1205, Oct. 2005.

[23] P. N. Bahrami, H. H. Javadi, T. Dargahi, A. Dehghantanha, and K. K. R. Choo, "A hierarchical key pre-distribution scheme for fog networks," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 22, pp. e4776, Aug. 2019.

[24] W. Bechkit, Y. Challal, and A. Bouabdallah, "A new class of Hash-Chain based key pre-distribution schemes for WSN," *Computer communications*, vol. 36, no. 3, pp. 243-255, Feb. 2013.

[25] M. Javanbakht, H. Erfani, H. H. S. Javadi, and P. Daneshjoo, "Key predistribution scheme for clustered hierarchical wireless sensor networks based on combinatorial designs," *Security and Communication Networks*, vol. 7, no. 11, pp. 2003-2014, Jan. 2014.

[26] T. Dargahi, H. H. Javadi, and M. Hosseinzadeh, "Application specific hybrid symmetric design of key pre-distribution for wireless sensor networks," *Security and Communication Networks*, vol. 8, no. 8, pp. 1561-1574, Sept. 2015.

[27] V. Modiri, H. H. S. Javadi, and M. Anzani, "A novel scalable key pre-distribution scheme for wireless sensor networks based on residual design," *Wireless Personal Communications*, vol. 96, no. 2, pp. 2821-2841, June 2017.

[28] M. Anzani, H. H. S. Javadi, and V. Modirir, "Key-management scheme for wireless sensor networks based on merging blocks of symmetric design," *Wireless Networks*, vol. 24, no. 8, pp. 2867-2879, Apr. 2018.

[29] N. Masaeli, H. H. S. Javadi, and S. H. Erfani, "Key pre-distribution scheme based on transversal design in large mobile fog networks with multi-clouds," *Journal of Information Security and Applications*, vol. 54, pp. 102519, Oct. 2020.

[30] W. Bechkit, Y. Challal, A. Bouabdallah, and V. Tarokh, "A highly scalable key pre-distribution scheme for wireless sensor networks," *IEEE trans. wireless communications*, vol. 12, no. 2, pp. 948-959, Feb. 2013.

[31] J. Lee and D. R. Stinson, "On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs," *ACM Transactions on Information and System Security (TISSEC)*, vol. 11, no. 2, pp. 1-35, May. 2008.