Using Residual Design for Key Management in Hierarchical Wireless Sensor Networks

Vahid Modiri
Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
va_modiri@srbiau.ac.ir
Hamid Haj Seyyed Javadi*
Department of Mathematics and Computer Science, Shahed University, Tehran, Iran
h.s.javadi@shahed.ac.ir
Amir Masoud Rahmani
Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
rahmani@srbiau.ac.ir
Mohaddese Anzani
Department of Mathematics and Computer Science, Shahed University, Tehran, Iran
anzani@shahed.ac.ir

Received: 25/Nov/2019 Revised: 16/Dec/2019 Accepted: 08/Feb/2020

Abstract

Combinatorial designs are powerful structures for key management in wireless sensor networks to address good connectivity and also security against external attacks in large scale networks. Many researchers have used key pre-distribution schemes using combinatorial structures in which key-rings, are pre-distributed to each sensor node before deployment in a real environment. Regarding the restricted resources, key distribution is a great engagement and challenging issue in providing sufficient security in wireless sensor networks. To provide secure communication, a unique key should be found from their stored key-rings. Most of the key pre-distribution protocols based on public-key mechanisms could not support highly scalable networks due to their key storage overhead and communication cost that linearly increasing. In this paper, we introduce a new key distribution approach for hierarchical clustered wireless sensor networks. Each cluster has a construction that contains new points or that reinforces and builds upon similar ideas of their head clusters. Based on Residual Design as a powerful algebraic combinatorial architecture and hierarchical network model, our approach guarantees good connectivity between sensor nodes and also cluster heads. Compared with similar existing schemes, our approach can provide sufficient security no matter if the cluster head or normal sensor node is compromised.

Keywords: Wireless sensor networks; Key pre-distribution; Residual Design; Hierarchical network model.

1- Introduction

A wireless sensor network (WSN) is a group of a majority of sensor nodes with limited resources such as storage capacity, energy, computational resources, and radio transmission range. We focus on the mechanisms of organizing secret keys between sensor nodes known as the key management problems. Some researches focused on the key management problem [1-6]. The key pre-distribution scheme (KPS) is a practical way to handle key management problems in wireless sensor networks where a set of specified keys is-preloaded in the nodes before deployment. There are three types of random, deterministic, and hybrid for key pre-distribution schemes. In random schemes, key-rings are randomly chosen from the main key-pool. In deterministic key pre-distribution schemes, key-rings are pre-loaded to sensor nodes based on a particular arrangement. In hybrid schemes both the mentioned methods are used. Combinatorial designs are one of the most important approaches used to consider a deterministic KPS. Based on combinatorial design, some approaches were introduced, e.g., [7-13]. All of these proposed schemes considered in a flat network. In such networks, all of the available sensor nodes have the same specifications such as battery life, memory capacity, and computational power. However, flat networks are suitable in terms of efficiency and simplicity for sensor applications. Effective hierarchical key management is required to improve these parameters. Some researchers provided “hierarchical architecture” as their chosen architecture for wireless sensor networks [14-17].

* Corresponding Author

Table 1: Residual Design for (7,3,1)-SBIBD

$c_1 = \{4,5,6,7\}$	$c_2 = \{2,3,6,7\}$	$c_3 = \{2,3,4,5\}$	$c_{4=}\{1,3,5,7\}$	$c_5 = \{1,3,4,6\}$	$c_6 = \{1,2,5,6\}$	$c_7 = \{1,2,4,7\}$
{4,5}	{2,3}	{2,3}	{1,3}	{1,3}	{1,2}	{1,2}
{6,7}	{6,7}	{4,5}	{1,5}	{1,4}	{1,5}	{1,4}
{4,6}	{2,6}	{2,4}	{1,7}	{1,6}	{1,6}	{1,7}
{5,7}	{2,7}	{2,5}	{5,7}	{4,6}	{2,6}	{2,4}
{4,7}	{3,7}	{3,4}	{3,7}	{3,4}	{2,5}	{2,7}
{5,6}	{3,6}	{3,5}	{3,5}	{3,6}	{5,6}	{4,7}

Recent researches show that in the comparison between the two main architectures, hierarchical architecture has better scalability and performance in large-scale wireless sensor network.

In a hierarchical WSN, each node is assigned a role of either Cluster Head (CH) or Cluster Node (CN), considering its capabilities. In each cluster, the node with more capability and resource is considered as CH. The CNs of each cluster collect data, communicate with their neighboring nodes directly or via a multi-hop communication path, and finally, send collected data to their resource-rich CH. In this paper, we present a secure architecture for sensor nodes by proposing a new hierarchical key management method. In our approach, we take advantage of combinatorial designs, and in particular Residual Design [11], for deterministic key pre-distribution. The structure of Residual Design allows each CN to share a common key with its CH, which makes direct communication of each CH with its CNs.

We conduct both analytical and experimental evaluations, considering different criteria: network scalability, connectivity, and resilience against nodes attacks. Network scalability is the maximum number of cooperating nodes supported in a WSN. Network connectivity is the probability of sharing at least a unique key between any two neighboring nodes. Network resiliency is the ability to resist of the network against the compromising of sensor nodes. We show that our approach improves network security and scalability, while provides a reasonable key share probability between the sensor nodes. The structure of this paper is organized as follows. We discuss the background and related works in section 2. The model and assumptions are presented in section 3. Our new approach named RDH is proposed in section 4. Analytical analysis and the simulation of different schemes are compared in part 5. The experimental results are provided in section 6. In the last Section, conclusion and future work directions are outlined.

2- Background and related works

2-1- Background

Definition 1. In a set system $(\mathrm{X},\ \mathcal{A})$, the set X consists of v elemets and $\mathcal{A}$ is subsets of X known as blocks. The combinatorial design theory is the technique of arranging members of $\mathcal{A}$ into words, arrays, or subsets based on predefined rules. Balanced Incomplete Block Design (BIBD) is one such design. In $(\mathrm{v}, \mathrm{k}, \lambda)$ -BIBD or $(\mathrm{v}, \mathrm{b}, \mathrm{r}, \mathrm{k}, \lambda)$-BIBD, there are v elements repeated r times in total b blocks of length k. Every two points exist in exactly λ of b blocks. In BIBD, we have: $\mathrm{bk} = \mathrm{vr}$ and $\lambda(\mathrm{v} - 1) = \mathrm{r}(\mathrm{k} - 1)$.

A BIBD is symmetric $(\mathrm{v}, \mathrm{k}, \lambda)$-SBIBD when $\mathrm{b} = \mathrm{v}$ and consequently $\mathrm{r} = \mathrm{k}$ [18].

Definition 2. Let (V, B) be a symmetric BIBD with $\mathrm{V} = \{\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{v}\}$ and $\mathrm{B} = \{\mathrm{B}_1, \mathrm{B}_2, \dots, \mathrm{B}_\mathrm{v}\}$. For any i, the blocks $\mathrm{B}_1 \backslash \mathrm{B}_\mathrm{i}, \mathrm{B}_2 \backslash \mathrm{B}_\mathrm{i}, \dots, \mathrm{B}_\mathrm{i} \backslash \mathrm{B}_{\mathrm{i}-1}, \mathrm{B}_{\mathrm{i}+1} \backslash \mathrm{B}_\mathrm{i}, \dots, \mathrm{B}_\mathrm{v} \backslash \mathrm{B}_\mathrm{i}$ are constructing a $(\mathrm{v} - \mathrm{k}, \mathrm{v} - 1, \mathrm{k}, \mathrm{k} - \lambda, \lambda)$-BIBD of the point set $\mathrm{X} \backslash \mathrm{B}_\mathrm{i}$. This generalization is called Residual Design [11]. To construct Residual Design or RD structure with the symmetric BIBD $(q^2 + q + 1, q + 1, 1)$, the point set of each class forms a BIBD with parameters$(v, b, r, k, \lambda) = (q^2, q^2 + q, q + 1, q, 1)$.

Example 3. Consider (7,3,1)-SBIBD with the following blocks: $B_1 = \{1,2,3\}$, $B_2 = \{1,4,5\}$, $B_3 = \{1,6,7\}$, $B_4 = \{2,4,6\}$, $B_5 = \{2,5,7\}$, $B_6 = \{3,4,7\}$, $B_7 = \{3,5,6\}$. Then over the point set $C_1 = \{4,5,6,7\}$, the RD sets $B_2 \backslash B_1 = \{4,5\}$, $B_3 \backslash B_1 = \{6,7\}$, $B_4 \backslash B_1 = \{4,6\}$, $B_5 \backslash B_1 = \{5,7\}$, $B_6 \backslash B_1 = \{4,7\}$, $B_7 \backslash B_1 = \{5,6\}$ are the blocks of a $(4,6,3,2,1) - \mathrm{BIBD}$. The remaining blocks can be observed in table 1.

In Residual Design, each class C_i consists of the elements $X \backslash B_i$.

2-2- Related works

For the sake of blindness in the topology of the hierarchical network before the deployment, we have to store keys into memories of sensor nodes via a pre-distribution scheme before deployment. Symmetric approaches are good for wireless sensor networks due to their low resource requirements such as resource and energy consumptions [19].

In [6], Eschenauer and Gligor proposed the RKP approach as the basic random key pre-distribution scheme. In this scheme, a random key-ring of size k is pre-loaded in each sensor node. In [7], Chan et al. proposed an enhancement of RKP for the network resiliency called q-composite. In this algorithm, two adjacent sensor nodes can establish a connection if there would be at least q common keys. In [8], Camptepe and Yener introduced symmetric key pre-distribution designs using parameters $(q^2+q+1, q+1,1)$-SBIBD. Their basic approach had full connectivity but the resilience was not good enough.

Then they provided a hybrid design. In the hybrid design, the complement of each block is generated and the key-rings of extra nodes were provided from those blocks. In the hybrid design, the resilience and also the scalability was improved. Lee and Stinson [9] use the transversal design (TD) for key pre-distribution. In the q-composite scheme, if two nods have $q \geq q'$ keys in common, they can communicate. In [14], Javanbakht et al. proposed a key pre-distribution scheme for a clustered heterogeneous WSN using transversal designs denoted by TDH. Zhang et al.[10] proposed a secure efficient hierarchical key management scheme (SEHKM) for wireless sensor networks. They introduced an assistant node near the cluster head to improve the resiliency and reduce the usage of the resources. In [11], Modiri and Anzani proposed a robust highly scalable key pre-distribution approach based on a new combinatorial algebraic named Residual Design or RD. In RD, good results in terms of connectivity and also very high network scalability are achieved. Also, they introduced a new modification of RD called RD* to improve the resilience of their first scheme.

Anzani and Modiri in [12] proposed the merging hybrid symmetric design to solve the connectivity problem of hybrid symmetric design presented in [8]. They achieved better connectivity results compared with similar related schemes. In MGHS, d blocks of SBIBD were merged instead of constructing a complimentary design in the main scheme.

In [15], Cheng et al. proposed an improved key distribution mechanism for hierarchical and large scale wireless network models. This approach with low communication overhead denoted as IKDM used a bivariate polynomial key-generation mechanism to guarantee that each two clusters can communicate via a unique pairwise key. In [16], Zhang et al. proposed a model in hierarchical networks based on the probability of nodes capture. Depend on nodes attack probabilities, the arrangement of hierarchical nodes could be changed, so that the nodes with smaller probability, tends to be located as cluster heads. The key management scheme uses the mechanism of Exclusion Basis Systems to update the key-rings among clusters.

Albakri et al.[17] introduced a deterministic hierarchical clustered key distribution scheme based on polynomials. They find a pairwise key between any nodes in a cluster and also between the sink node and each cluster heads. In this scheme, to reduce the risk of security attacks, a novel probabilistic feature is used.

3- Model and assumptions

3-1- Network model

Wireless sensor networks are classified as being either flat or hierarchical configuration. In flat architecture, almost entire nodes play the same role, whereas, in a hierarchical sensor network, their roles are different.

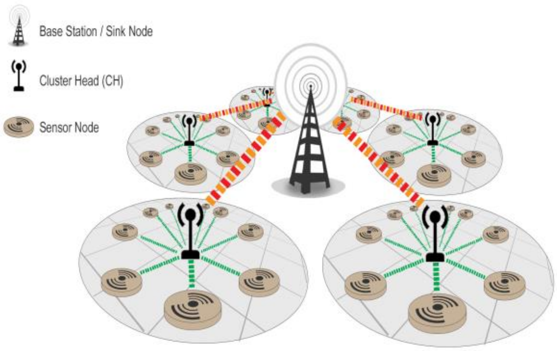

Figure 1: Hierarchical wireless sensor network architecture in our network model. We have q^2+q+1 clusters each consists of a cluster head and q^2+q sensor nodes.

In several aspects such as energy constraints and high network scalability, the hierarchical network model has more operational benefits. In many applications of wireless sensor networks, connectivity between all sensors is not prerequisite and wireless sensors just transmit data to the nodes with similar capabilities [20, 21]. In this work, we concentrate on highly scalable wireless sensor networks in hierarchical network architecture. In figure 1., our network model is illustrated. The architecture has three types of wireless sensor nodes: Sink Node or Base Station (BS), Cluster Head (CH), and Cluster Node (CN).

Sink node: Sink node or base station is a powerful device at the top or in the center of the network. It has unlimited resources such as memory storage, communication power, computation, and a high range of radio transmission to access entire nodes in the network.

Cluster head: Cluster heads have more powerful resources and wider radio transmission range than a normal sensor node. They can transmit data between their members and the sink node.

Sensor node: Sensor nodes are cheaper and have lower resources. They have limited battery power, data processing capability, memory size, and also not wide radio transmission range.

In our model, any sensor node can communicate with its cluster head directly; also may communicate with its sibling in the related cluster headset. In the deployment, the sensor network is partitioned into several clusters known by their cluster heads. The clustering process is performed by some existing clustering algorithms [22, 23]. In this model, each cluster is composed of a cluster head and a set of sensor nodes. As shown in Fig. 1, the sensor nodes directly send data to the related cluster head and also would communicate with other sensor nodes inside the current partition.

Algorithm 1: RDH

```
Require: $N$ {Total number of nodes}
  1. Find the minimum prime power $q$ that satisfies$(q^2+q+1)^2 \geq N$.
  2. Generate the base symmetric design with parameters$(q^2+q+1, q+1, 1)$.
      • $v$ objects $P = \{a_1, a_2, ..., a_v\}$.
      • $b$ blocks $B = \{B_1, B_2, ..., B_b\}$ of size $q+1$.
  3. Generate $c' = (q^2+q+1)$ blocks for classes $c_i$ and $b' = (q^2+q+1)(q^2+q)$ blocks for
constructing internal members of Residual Design from the base symmetric design:
      • Blocks $C_i = P \backslash B_i$ where $i = 1, \ldots, q^2+q+1$.
      • Blocks $B_{ij} = B_i \backslash B_j$ where $i, j = 1, \ldots, q^2+q+1$.
  4. Assign $C_i$ blocks to cluster heads and $B_{ij}$ to sensor nodes.
```

4- Our proposed approach

Considering the hierarchical network model and the Residual Design(RD), we propose a secure scalable key distribution approach for clustered hierarchical wireless sensor networks based on Residual Design. We denote our new approach as RDH. Clusters of the WSN are built based on the RDH algorithm in the offline area. The clustering procedure in our key pre-distribution approach is based on the distribution of the required key-rings on cluster heads and cluster nodes before deployment.

This process is performed in 2 phases: the key pre-distribution phase and shared-key discovery phase. In the key pre-distribution phase, we decide on choosing N secure key-rings from a key pool and pre-load them into cluster heads and also all sensor nodes before they are deployed. Given a wireless network size N, we consider the minimum power q in which $(q^2+q+1)^2 \geq N$ to construct a $(q^2+q+1, q+1, 1)$-SBIBD. Based on this SBIBD, we construct the Residual Design with $c' = (q^2+q+1)$ classes in which the block set $C_i = \{P \backslash B_i\}$ of size q^2 is assigned to each class. Each class has (q^2+q) blocks $B_{ij} = \{B_i \backslash B_j\}$ inside, therefore all classes could generate totally $b' = (q^2+q+1)(q^2+q)$ blocks of size q. Then the blocks C_i are assigned to c' cluster heads and also the blocks B_{ij} are assigned to $b' = N - c'$ Cluster nodes.

The construction algorithm of our proposed approach for hierarchical wireless sensor networks is described in the Algorithm 1.

After the key pre-distribution phase, the nodes are randomly deployed in the environment and the (q^2+q+1) clusters are built. Clusters are built based on different criteria such as location, mission type, and communication range [24].

In the shared key-discovery phase, any two cluster heads or any sensor node and its cluster head must find at least a common key in their radio transmission range by exchanging the list of their key identifiers. There is no eavesdropping in this concept but as will be explained in the next sections, we try to increase the resiliency against compromising nodes.

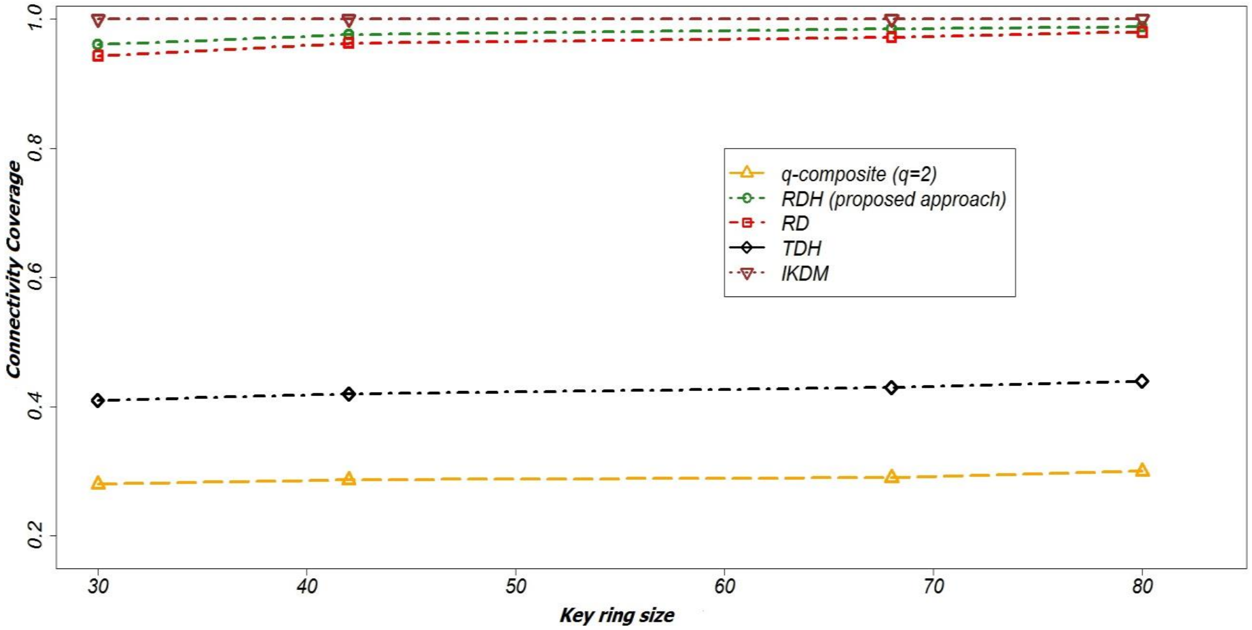

Figure 2: Connectivity Comparison. The connectivity of our scheme (RDH) is compared with classic RD, q-composite, IKDM and hierarchical TD (TDH)

5- Analysis

In this section, a theoretical analysis of important metrics of our proposed approach including scalability, connectivity, and resilience will be presented. In our proposed approach, the Residual Design (RD) is used as a key pre-distribution scheme. After deployment, the properties of RD would help us to calculate these metrics

5-1- Scalability

In our proposed approach we have considered q^2+q+1 clusters of size q^2 in such a way that they differ from q keys. Each cluster has q^2+q sensor nodes. Therefore the maximum network size that can be supported is:

$$(q^2+q+1)(q^2+q)+(q^2+q+1)=(q^2+q+1)^2 \qquad (1)$$

5-2- Connectivity

To compute the connectivity, at first we determine the key share probability for each cluster.

According to the structure of the RD scheme, every sensor node has common keys with its corresponding cluster head node. Therefore, the probability that any sensor node and it's cluster head node have a common key is

$$P_{CHi-Si}=1$$

Every sensor node in a cluster has common keys with q^2 other nodes. Therefore the probability that any pair of sensor nodes has at least a common key is

$$P_{Si}=\frac{q^2}{q^2+q}$$

It shows that the more increase in parameter q, the more in the connectivity of the network. Therefore by increasing the q, the above limit goes to 1. In the RD scheme [11], the probability of key share between two nodes is

$$\frac{q^2}{q^2+q} * Q_{SD} + \left(\frac{q-1}{q^2+q} \times \frac{q^2+1}{q^2+q} + \frac{q^2}{q^2+q} \times \frac{q^2-q+1}{q^2+q}\right) * Q_{DC} \qquad (2)$$

where

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

and

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

In the q-composite scheme [7], two nodes must share at least q common keys to be able to establish a secure link. The connectivity probability of q-composite scheme is calculated as:

$$p_c = p(q)+\ldots+p(k)$$

where

$$p(i) = \frac{\binom{p}{i}\binom{p-i}{2(k-i)}\binom{2(k-i)}{k-i}}{\binom{p}{k}^2}$$

According to the analysis in [14], the connectivity between two nodes in TDH scheme is:

$$\frac{\sum_{j=1}^{c} n_j \times Pr_j}{N}$$

where Pr_j is connectivity for each cluster, n_j is the number of sensor nodes in cluster j, and c is the number of clusters.

In [15], each pair of nodes has a unique pairwise key, therefore the network has full connectivity in IKDM.

5-3- Security Analysis

Node capture attack is a serious threat in wireless sensor networks. The resilience is the ability to resist of the network against the compromising of sensor nodes. In our proposed approach, according to the structure of cluster heads and communication between them, after compromising of any cluster head, nothing would happen for the secure communication between other cluster heads and sensor nodes. Compromising any cluster head leads to deleting the connection between sensor nodes corresponding to this cluster and base station.

To calculate the resilience, we consider the probability that a link in a cluster is compromised when an attacker capture x nodes in a cluster. This probability can be defined as

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

In our proposed approach, each key exists in $r = q+1$ nodes and two communicating nodes must have a common key j in their key-rings. So the probability that a link is secured with key j is

$$P(l_j) = \frac{\binom{q+1}{2}}{\binom{q^2+q}{2} - \frac{q^2+q}{2}} = \frac{1}{q^2+q-2}$$

The probability that the key j appears in one or more of x compromised nodes is:

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

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

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

The probability of compromising a secure link is computed by Camptepe and Yener in [8] for symmetric design as:

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

In [6], the authors proved that the resilience of q-composite scheme is

$$\sum_{i=q}^{k} (1-(1-\frac{k}{p})^x)^i \times \frac{p(i)}{p_c}.$$

In the RD scheme [11], the resilience of network against node capture is

$$(q^2+q+1)\frac{\binom{q^2(q+1)}{2}}{\binom{(q^2+q+1)(q^2+q)}{2}}\left(1 - \frac{\binom{q^4+q^3+q^2+q}{x}}{\binom{(q^2+q+1)(q^2+q)}{x}}\right). \quad (3)$$

The resistance of the network against the capture node in IKDM[15] depends on degree the of bivariate symmetric polynomials.

6- Experimental Results

In this section, we compare our work to the related works based on scalability, connectivity, and network resilience.

For numerical results, we used the C# programming language to provide a simulation tool. Then we produce our comparing graphs with the R programming language. Figure 2 shows that the connectivity estimated by our proposed approach (RDH), q-composite scheme [7], RD scheme [11], and proposed scheme in [14] (TDH) for different key-ring size. It can be observed that our proposed approach has better connectivity than the other related schemes.

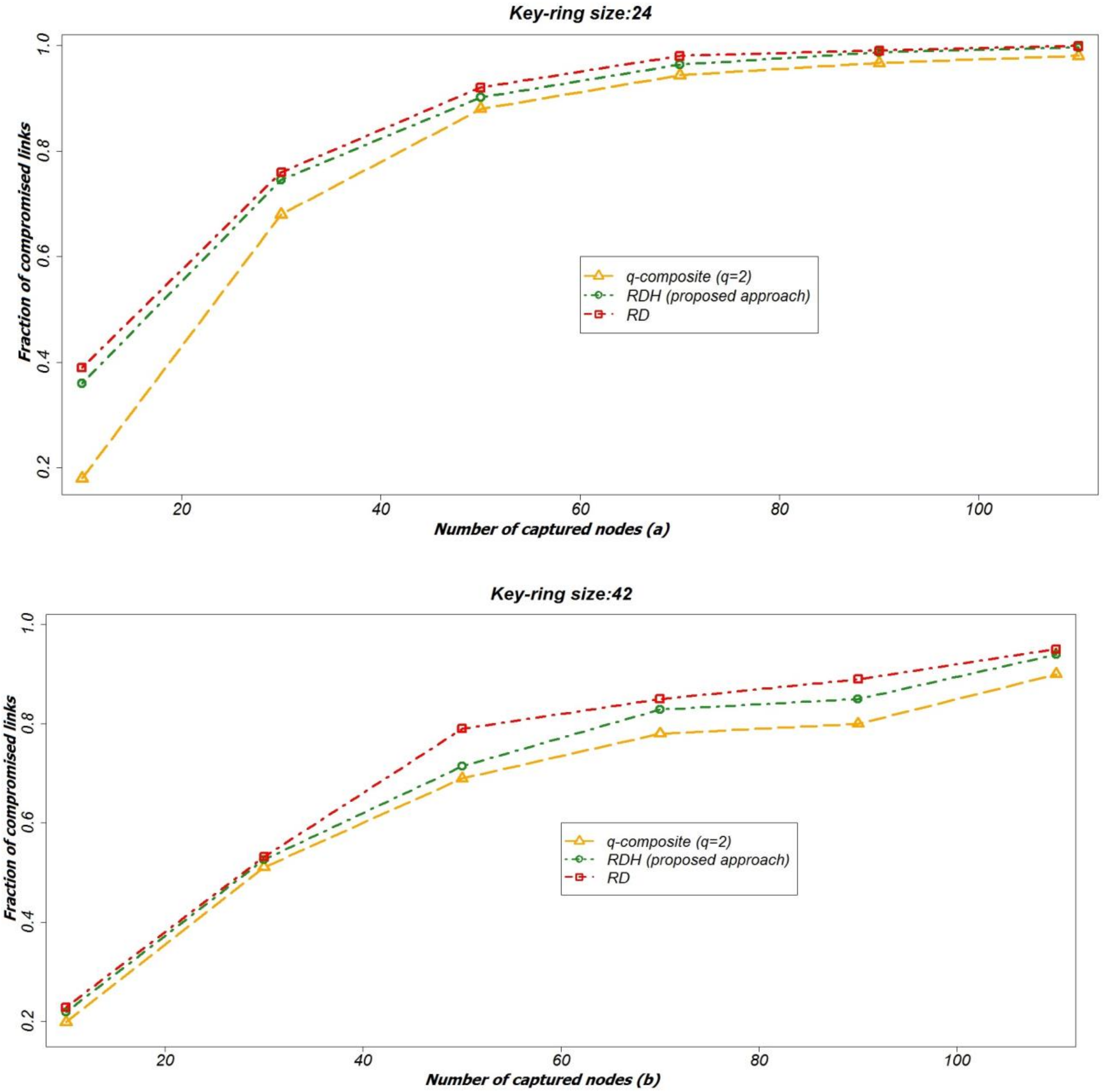

Figure 3: Security behavior Comparison. The network resilience of our new approach (RDH) is compared with classic residual resign (RD) and q-composite design. Simulation results are computed for the same key-ring size k = 24 in (a) and k = 42 in (b)

It shows that by increasing the key-ring size our proposed approach has full connectivity. Figure 3 compares the resilience against node capture attack for key-ring sizes $k = 24$ and $k = 42$. The figure shows that for an equal key ring size, the resilience of our proposed approach is better than the RD scheme. It also has the same resilience with the q-composite scheme for compromised nodes numbers greater than 100.

7- Conclusion

In this paper, we provide a novel proper key distribution approach for large-scale clustered hierarchical wireless sensor networks based on Residual Design. We show that the proposed architecture in wireless sensor networks is more convenient for hierarchical scalable network forms. The analysis and numerical results show that our proposed RDH design has the best connectivity coverage and also scalability rather than other similar schemes. Also this approach provides good security against all types of sensor nodes capture no matter if the cluster head or sensor node is compromised.

Our future work would target to improve low resilience against some other types of attacks. We will also focus on the models based on the Internet of Things (IoT) in this idea.

References

[1] C. Boyd, A. Mathuria, and D. Stebila, Protocols for authentication and key establishment. Springer, 2003.

[2] I. Memon, "A secure and efficient communication scheme with authenticated key establishment protocol for road networks," Wireless Personal Communications, vol. 85, no. 3, pp. 1167-1191, 2015.

[3] I. Memon, I. Hussain, R. Akhtar, and G. Chen, "Enhanced privacy and authentication: An efficient and secure anonymous communication for location based service using asymmetric cryptography scheme," Wireless Personal Communications, vol. 84, no. 2, pp. 1487-1508, 2015.

[4] 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, 2010.

[5] J.-W. Dong, D.-Y. Pei, and X.-L. Wang, "A class of key predistribution schemes based on orthogonal arrays," Journal of Computer Science and Technology, vol. 23, no. 5, pp. 825-831, 2008.

[6] 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, 2002, pp. 41-47.

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

[8] S. A. Çamtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," IEEE/ACM Transactions on networking, vol. 15, no. 2, pp. 346-358, 2007.

[9] 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, 2008.

[10] X. Zhang and J. Wang, "An efficient key management scheme in hierarchical wireless sensor networks," in 2015 International Conference on Computing, Communication and Security (ICCCS), 2015: IEEE, pp. 1-7.

[11] 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, 2017.

[12] 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, 2018.

[13] S. Ruj and B. Roy, "Key pre-distribution using partially balanced designs in wireless sensor networks," International Journal of High Performance Computing and Networking, vol. 7, no. 1, pp. 19-28, 2011.

[14] 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, 2014.

[15] Y. Cheng and D. P. Agrawal, "An improved key distribution mechanism for large-scale hierarchical wireless sensor networks," Ad Hoc Networks, vol. 5, no. 1, pp. 35-48, 2007.

[16] Y. Zhang and P. Li, "Key management scheme based on nodes capture probability for wireless sensor networks," in 2018 Chinese Control and Decision Conference (CCDC), 2018: IEEE, pp. 5470-5475.

[17] A. Albakri, L. Harn, and S. Song, "Hierarchical key management scheme with probabilistic security in a wireless sensor network (WSN)," Security and Communication Networks, vol. 2019, 2019.

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

[19] T. Kavitha and R. Kaliyaperumal, "Energy Efficient Hierarchical Key Management Protocol," in 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 2019: IEEE, pp. 53-60.

[20] S. Zhao, K. Tepe, I. Seskar, and D. Raychaudhuri, "Routing protocols for self-organizing hierarchical ad-hoc wireless networks," 2003.

[21] B. Liu, Z. Liu, and D. Towsley, "On the capacity of hybrid wireless networks," in IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428), 2003, vol. 2: IEEE, pp. 1543-1552.

[22] G. Gupta and M. Younis, "Performance evaluation of load-balanced clustering of wireless sensor networks," in 10th International Conference on Telecommunications, 2003. ICT 2003, 2003, vol. 2: IEEE, pp. 1577-1583.

[23] J. Li and R. Levy, "Fair and Secure Clustering Scheme (FSCS) clustering protocol," In Technical report, 2005.

[24] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," IEEE Transactions on mobile computing, vol. 3, no. 4, pp. 366-379, 2004.

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

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

Amir Masoud Rahmani was born in 1974 in Iran. He received his B.S. in computer engineering from Amir Kabir University, Tehran, in 1996, the M.S. in computer engineering from Sharif University of technology, Tehran, in 1998 and the PhD degree in computer engineering from Islamic Azad University (IAU), science and research branch, Tehran, in 2005. His research interests are in the areas of distributed systems, ad hoc and wireless sensor networks and evolutionary computing.

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