VOL 3 (2019) NO 1

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

A Hybrid Key Pre-Distribution Scheme for Securing Communications in Wireless Sensor Networks

Mojtaba Jamshidi[#], Hamid Bazargan[*], Abdusalam Abdulla Shaltooki[#], Aso Mohammad Darwesh[#]

[#] *Department of Information Technology, University of Human Development, Sulaimani, Iraq*
[*] *Department of Electrical, Computer and IT Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran*
E-mail: jamshidi.mojtaba@gmail.com, h.bazargan@qiau.ac.ir, Salam.abdulla@uhd.edu.iq, aso.darwesh@uhd.edu.iq

***Abstract*— Wireless Sensor Network (WSN) is a type of ad hoc networks which consist of hundreds to thousands of sensor nodes. These sensor nodes collaborate to surveillance environment. WSNs have a variety of applications in military, industrial and other fields and they are fit to study environments that presence of human being is costly or dangerous. Sensor nodes have memory, energy and processing limitations. According to sensors' limitations and also increasing use of these networks in military fields, establishing a secure WSN is very important and challenging. Applying Key Predistribution Schemes (KPSs) is one of the effective and useful mechanisms to provide security in WSN. In this paper, a hybrid KPS is proposed that support three various keys, primary pairwise, polynomial, and ordinary. The proposed scheme has been implemented using J-SIM simulator and its performance has been evaluated in terms of maximum supportable network sizes and resiliency against node capture attack, by performing some experiments. Simulation results have been compared with Basic, q-Composite, RS, Cluster-Based, QS, and Double-Key Hash schemes. The compared results showed that the proposed scheme has a better resiliency against links disclosing via enemies.**

***Keywords*— Wireless Sensor Network, Security, Key Management, Cryptography, Pairwise Keys**

I. INTRODUCTION

Wireless sensor networks (WSN) have a variety of applications in industrial, health and specifically in military fields. They are fit to study environments that presence of human being is costly or dangerous. Generally, after nodes deployment and finalizing the mission, it's not possible to collect and reuse sensor nodes, therefore the cost for each sensor node should be low. Concerning tiny size and also low cost of implemented sensor nodes, there will be many serious limitations like storage capacity, processing power, radio range, energy. According to these limitations and also unattended sensor nodes deployment, the nature of wireless communication, and also increasing use of WSN in militaries domains, establishing a secure WSN is very important and challenging which many researchers focus their studies on this field [1-3]. Already, many attacks have been taking place against WSNs. One of the most common and dangerous attacks against WSN is eavesdropping attack which discovers information transmitted in the network's links. Applying KPSs and cryptography is one of the effective and promising mechanisms to protect against such threats [4][5]. In KPS, nodes establish keys (private, group, public) with neighboring or Base Station (BS) nodes after deployment in a specific environment, then encrypt data with these keys and transmit them. In this case, the enemy will not be able to decrypt data, unless has the keys [6][7].

Many of key management schemes [8-19] for WSN has been proposed. For example, in [8], a master key based pre-distribution scheme has been proposed. In this scheme, before node distribution in the environment, a master key will be load into sensor nodes' memory. After distribution of nodes in the environment, every two nodes can establish a pairwise key using this master key and a random number. This method has infinite scalability and less memory overhead. Of course, this method has a considerable problem, when a master key has been captured by the enemy, all the pairwise keys will be disclosed.

In SPIN scheme [10], when two neighboring nodes, like u and v, want to establish a pairwise key, they send a request to BS. The base station receives the request and generates a unique pairwise key and sent it to them. This scheme has a high resiliency but lack of scalability remains as its main disadvantage because when the number of nodes increases, base station becomes a bottleneck.

In [12] a random key pre-distribution scheme has been proposed. In this scheme, each node is given a key ring (contains $r>0$ keys) from a key pool. After node distribution in the environment, each two neighbor nodes have a common key in their key rings; they can establish a pairwise

key using that key. This scheme is scalable but in addition to low connectivity degree, its security is vulnerable.

In [14] a *t*-degree polynomial-based key pre-distribution scheme has been proposed which its mechanism is same [12], but instead of using ordinary keys, *t*-degree two variables polynomial keys have been used. This scheme has a high level of security until the enemy has captured less than *t* pairwise keys or (nodes). But if the enemy captures more than *t* pairwise keys, therefore, the polynomial will be exposed and a huge part of network communication will be disclosed.

In this paper, a hybrid key pre-distribution scheme based on three primary pairwise keys, polynomial keys, and ordinary keys to securing communications in WSNs has been proposed. The proposed scheme holds a promising amount of connectivity degree while has a good resiliency against node capture and exposing communication links.

The rest of this paper is organized as follows. Section II presents related work, system assumption, symbols, and the proposed scheme. Section III presents the simulation results. The paper is concluded in Section IV.

II. Material And Method

In this section, we first present some existing key management schemes in WSNs. Then, we present the preliminaries of the proposed scheme, including system assumptions and symbols. Finally, the proposed scheme is presented.

A. *Related Work*

In [9] LEAP scheme has been proposed which supports establishing four type of keys including individual key, pairwise key, cluster key and group key. In [10] SPINS scheme with the participation of Base Station(BS) has been proposed. In this scheme each node *u* has a private key $K_{u.BS}$ with BS. When two nodes *u*, *v* need a pairwise key, they sent their request to BS. Upon receiving these request, BS generates a pairwise key, encrypt it with $K_{u.BS}$ and $K_{v.BS}$ separately, then send it to *u* and *v*.

In [11] a pair-wise key pre-distribution scheme has been proposed which before deployment of sensor nodes in the environment, for every two nodes *u* and *v*, a unique pairwise key has been generated and will be load in their memory. This scheme provides a high level of security but it is costly and not scalable because each node needs to hold *n*-1 pairwise keys in its memory to communicates with all other nodes in the network.

Eschenauer and Gligor [12] have proposed a random key pre-distribution scheme which referred as the base scheme for most of the other scheme. In this scheme, communication keys are implemented in three phases: (1) Key pre-distribution, (2) Shared key discovery, and (3) path-key establishment.

Chan and Perrig in [13] proposed the q-composite scheme in order to optimize the base scheme [12]. This scheme uses at least *q* (*q*>1) common keys between two neighbor nodes with a hash function to establish a pairwise key. Thus, when *q* equals 1 this scheme is equivalent to the base scheme [12]. Simulation results have demonstrated that this scheme has more resilience against disclosing of communication links when enemy discovered a small number of nodes. But its resilience will be less than the base protocol if a large number of nodes has been discovered by the enemy.

In [14] a polynomial-based key pre-distribution scheme has been proposed. To pre-distribute pairwise keys, the Key Setup Server (KSS) randomly generates a bivariate *t*-degree polynomial, $f(x.y) = \sum_{i,j=0}^{t} a_{i,j} x^i y^j$ over a finite field f_q, where *q* is a prime number that is large enough to accommodate a cryptographic key, such that it has the property of $f(x.y) = f(y.x)$. Each bivariate *t*-degree polynomial consume $O(t + 1)\log q$ storage space. Node *u* can compute the common key $f(u.v)$ by evaluating $f(u. y)$ at point *v*, and node *v* can compute the same key $f(v.u) = f(u.v)$ by evaluating $f(v. y)$ at point *u*. This scheme has no communication overhead for establishing pairwise keys. A security proves in [14] guarantees that this scheme is *t*-collusion resistant, meaning that while less than (*t*+1) computed keys from polynomial is not discovered by enemy, the polynomial will not be disclosed, otherwise if the number of discovered keys become more than *t*, then the polynomial will be disclosed and also the entire keys generated by this polynomial will be discovered by enemy.

In [15] a key pre-distribution scheme has been proposed which uses a mobile sink node to establish secure communication links with other sensor nodes. This scheme is based on polynomial keys and *q*-composite scheme.

In [17] an effective key pre-distribution scheme using dual hash keychain mechanism has been proposed. In this scheme, there are two types of key pools: Upward key and downward key.

In [18] a clustering based key pre-distribution scheme has been proposed. In this scheme, all nodes clustered according to their position. Moreover, a scheme has been proposed to distribute keys between inner cluster nodes and cluster controller nodes.

B. *System Assumptions and Symbols*

First, it is necessary to describe considered assumptions for the proposed scheme. Sensor network contains *N* nodes that are randomly distributed in the considered environment. Sensor nodes are fixed that do not have mobility. Each node has a unique ID. The network is homogeneous. It means that all nodes are identical in terms of hardware and software resources. Nodes' transmission range has been considered identical and equal to *r*. It is assumed that sensor nodes are not hardware resistant and the enemy can access their confidential information if capture them. It also assumes that the network is insecure and nodes may be captured by the enemy. A node captured by the enemy is called malicious node or compromised node and the rest of the nodes in the network are called normal. Three key pools exist: S_1 contains n_{S1} primary pairwise keys, S_2 contains n_{S2} ordinary keys, and S_3 contains n_{S3} polynomial keys. Also, each key has a unique ID.

The symbols used in this paper can be found below:

- R_1, R_2, and R_3 are selected key rings from pools S_1, S_2, and S_3 respectively. These key rings are loaded into each sensor node.
- K_i^j Represent a key with identifier *i* from pool S_1.

- K_k^2 represent a key with identifier k from pool S_2.
- $K_j^3(x.y)$represent a polynomial key with identifier $_j$ from pool S_3.
- $PK_{u.v}^1$ is the primary pairwise key between nodes u and v.
- $PK_{u.v}^2$ is the secondary pairwise key established between nodes u and v.
- F is a pseudorandom number generator function.
- CN is the number of captured nodes by the attacker.
- t is the degree of bivariate polynomials.

C. *The Proposed Scheme*

Here we have to explain the proposed scheme. The proposed scheme is a hybrid of schemes [11-13], pair-wise key pre-distribution, random key pre-distribution, and polynomial-based key pre-distribution. The proposed scheme consists of three phases: virtual deployment, distribution of ordinary and polynomial key materials, and nodes deployment and links establishment. In the following, details of these three phases are described.

1. The first Phase (Virtual Deployment)

This phase takes place before deployment of sensor nodes in the network environment. In this phase, initially for each node u, d virtual neighbor nodes are selected randomly from among the other nodes and are recorded in the node u's neighboring table. In the proposed scheme, each node has a neighboring table, Fig. 1, which records information about its neighboring nodes. The identifier of each neighbor node v is recorded in field *NodeID* and the established pairwise key with v is recorded in field *PairwiseKey*.

NodeID	PairwiseKey

Fig. 1. The structure of the neighboring table in the proposed scheme.

In this phase, after selecting d neighbors for each node u, for each neighbor, a random primary pairwise key is selected from key pool $S_1$and stored in its neighboring table.

Key pool S_1 contains the $n_1 = \frac{N \times d}{2}$ primary pairwise key. The ring size of the selected key for pool S_1 (i. e. R_1) is equal to d. Details of this phase of the proposed scheme, for each node u, described as follows:

1. Selecting node v randomly as a virtual neighbor node, in the condition that node v's neighboring table does not complete (each neighboring table can store at most d member). node u also can be considered as a neighbor node for v.
2. Selecting a random pairwise key ($PK_{u.v}^1$) from pool S_1 for nodes u and v and store it in the neighboring table of these two nodes.
3. Repeat steps 1 and 2 while neighborhood table is completed for node u (it must contain d different neighbors).

This phase of the proposed scheme, drawn from the scheme [11] in which, for each node u, N-1 primary random pairwise key selected and loaded into node u. But in the proposed scheme, each node u, only loads d key (corresponding to d virtual neighbor nodes that are chosen randomly) in its memory (d <<N). The primary pairwise keys will be the most powerful type of keys because even if attacker possible to capture a node and extract a primary pairwise key, any other links between some other nodes will be disclosed by that key.

Note that after the actual deployment of nodes in the network environment, a primary pairwise key such as $PK_{u.v}^1$ can be used only if nodes u and v become real neighbors, otherwise it is eliminated from nodes memories.

Clearly, the degree of connectivity that has been achieved by using primary pairwise key is low, because the probability that actual node neighbors, be the same virtual neighbors, is low. Therefore, we have to use another pairwise key (secondary pairwise keys).

2. The Second Phase (Distribution of Ordinary and Polynomial Key Materials)

In this phase, for each node u, R_2 keys from pool S_2 randomly and R_3 keys from pool S_3 particularly are chosen and loaded to its memory. Also, a master key, K_m, and function F are loaded into the memory of all nodes. The size of poolS_3, R_3, and also selecting polynomial keys for each sensor node is in such a way that number of using of each polynomial keys by whole network nodes will not exceeds of t. Therefore in the polynomial key predistribution process, each keyK_j^3will be eliminated from the poolS_3in condition that the choosing times of key K_j^3 reach t.

We set the total number of t-degree polynomial keys equal to $n3 = \left\lfloor \frac{N \times R_3}{t} \right\rfloor$ in the pool S_3. With this approach, however, the amount of connectivity that obtained by using the polynomial keys are low, but polynomials will never disclose. To increase the degree of connectivity, the ordinary keys are used.

3. Third Phase (Nodes Deployment and Links Establishment)

After the implementation of the first and second phases, nodes are deployed in the network environment and then try to discover or establish pairwise keys with their neighbors. Initially, in this phase, each node by sending a "Hello" message along with a list of its key identifiers in key rings R_2 and R_3, can be aware of actual neighbors and also try to establish a secure link with any of its neighbors. At this stage, the "Hello" message and the list of key identifiers encrypted with master key K_m in order to prevent the attacker to access to messages, if he was existing from the start in the network. In this way, each node u is aware of its neighbors and their key rings. Then, node u will run one of the following steps on priority, for each of its neighbors, such as v:

1. If v is a virtual neighbor of u, both of them use primary pairwise key $PK_{u.v}^1$ to establish a secure link.
2. If v and u nodes have a common polynomial key, such as $K_j^3(x.y)$, node u obtains the pairwise key $PK_{u.v}^2$ by computing $K_j^3(u.y)$ at point v. Node v also obtains same pairwise key $PK_{v.u}^2$ by computing $K_j^3(v.y)$ at point u. Notice that $PK_{v.u}^2 = PK_{u.v}^2$ (derived from basic scheme [14]).

3. If nodes v and u have q>0 common ordinary keys in their keyring R_2 (such as $K_1^2.K_2^2.....K_q^2$), the pairwise key will be computed as below (derived from basic scheme [13]):

$$PK_{u.v}^2 = F(u.v.K_1^2.K_2^2.....K_q^2)$$

Thus, the proposed scheme establishes pairwise keys between sensor nodes in a way that resists against node capture attack and disclosure of their links.

III. The Simulation Results

In this section, we evaluate the performance of the proposed scheme. The proposed scheme has been implemented in J-SIM simulator [21] and its performance has been compared with performance of Basic [12] ،q-Composite [13] ،RS [14] ،Strong-Key [16] ،QS [15] ، Cluster-Based [17] ، Double-Key Hash [18] ،EPKP [19] MSKPD [20] scheme. Common assessment metrics include:

- **Maximum supportable network sizes**: the maximum number of nodes that can be found in the network so that the desired degree of connectivity, such as p, has been established in the network.
- **Resiliency**: the fraction of compromised links between non-captured nodes.

The simulation model is derived from [14] and it is as follows:

- network size is100 * 100 meters.
- N node randomly will be deployed in the network.
- The number of keys in key pool S_2 is equal to n_2=10000.
- Radio range of all nodes is also considered to be 10 meters.
- Desirable network connectivity is p.
- We assume that attacker can capture CN nodes and can extract their material.

Experiment 1:
The aim of this experiment is evaluating the effect of the number of nodes captures, CN, on the resiliency of the proposed scheme and compare results with other existing schemes. In this experiment, the total number of nodes N = 1000, the number of captured nodes has been changed from 100 to 700 and the connectivity degree has been considered p = 0.33. To reach that connectivity degree, in the proposed scheme we considered, d=30, R_2=48, and R_3=3. The polynomial degree has been assumed equal to t=49. For RS scheme, key pool size equal to 43, key ring size equal to 4 and the polynomial degree has been considered to be equal to t=49. For the other compared algorithms also size of key ring has been considered to be equal to 200.

The results in Fig. 2 show that the effectiveness of the proposed scheme is always better than Basic and q-Composite schemes. But as long as the number of captured nodes is low, the RS and QS schemes perform better than other schemes in terms of resiliency, because these schemes only use polynomial keys and the attacker needs to capture many nodes to be able to discover polynomials.

But with the discovery of one (or more) polynomials, most of the links will be disclosed. As is clear from the results, as long as the number of captured nodes is less than or equal to 400, RS scheme has better performance than the proposed scheme. Since polynomials have been discovered by the attacker, when the number of captured nodes exceeds 500 or more, the disclosed Links in RS scheme strongly grows and will be much more than the proposed scheme. But in the proposed scheme, the use of polynomial keys has been controlled, therefore never be disclosed by the attacker.

On the other hand, in the proposed scheme, also primary pairwise keys have been used. capturing these keys by the attacker, could not help him discover other links. Hence, the efficiency of the proposed scheme outperforms the other compared scheme in terms of resiliency against node capture attack (except Cluster-Based scheme). Of course, when the number of captured nodes exceed 700, the performance of the proposed scheme is better than the Cluster-Based scheme. It is also necessary to note that the Cluster-Based scheme is applicable only for Cluster-Based networks and it doesn't work well in other topologies.

Experiment 2:
The aim of this experiment is evaluating the performance of the proposed scheme in terms of maximum supportable network sizes and comparing the results with some other schemes. In this experiment, for the proposed scheme, parameters d=30, R_2=50, R_3=3 has been set. The degree of polynomials t=40 has been considered. In RS scheme, keyring size=2 and degree of polynomial t=99 has been considered. For Basic scheme also the keyring size has been set to 200. Overall, keyring size at all three schemes almost set to 200. Fig. 3 shows the results of the experiment.

The results show that maximum supportable network sizes for all three schemes are equal since they have almost same key rings and therefore the probability of link establishment will be equal as well.

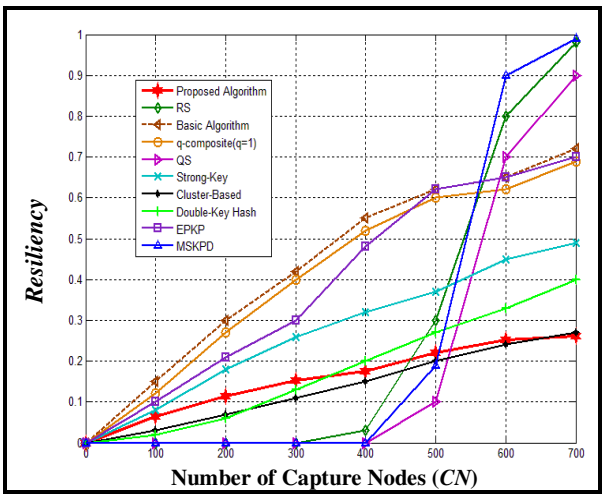

Fig. 2. The fraction of compromised communication between non-compromised nodes (Resiliency) versus the number of captured nodes (N=1000 and p =0.33)

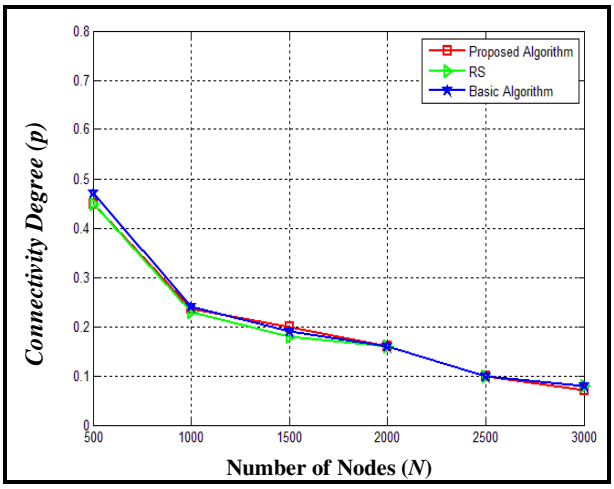

Fig. 3. Maximum supportable network sizes

IV. Conclusion

In this paper, a hybrid key management scheme to establish pairwise keys and secure link keys in wireless sensor network has been proposed. The proposed scheme uses primary pairwise keys, polynomial and ordinary keys. The proposed scheme has been implemented using JSIM simulator and its performance has been evaluated in terms of maximum supportable network sizes and resiliency against node capture attack, by performing some experiments. Simulation results have been compared with Basic, q-Composite, RS, Cluster-Based, QS, and Double-Key Hash schemes. The compared results showed that the proposed scheme has a better resiliency against links disclosing via attackers.

References

[1] M. Jamshidi, A. A. Shaltooki, Z. D. Zadeh and A. M. Darwesh, "A Dynamic ID Assignment Mechanism to Defend Against Node Replication Attack in Static Wireless Sensor Networks", JOIV: International Journal on Informatics Visualization, Vol. 3, No. 1, 2019.

[2] M. Jamshidi, E. Zangeneh, M. Esnaashari and M. R. Meybodi. "A lightweight algorithm for detecting mobile Sybil nodes in mobile wireless sensor networks", Computers & Electrical Engineering, Vol. 64, pp. 220-232, 2017.

[3] A. Andalib, M. Jamshidi, F. Andalib and D. Momeni, "A Lightweight Algorithm for Detecting Sybil Attack in Mobile Wireless Sensor Networks using Sink Nodes", International Journal of Computer Applications Technology and Research, Vol. 5, No. 7, pp. 433 – 438, 2016.

[4] H. S. Jangwan and A. Negi, "A Swarm Optimization Based Power Aware Clustering Strategy for WSNs. International Journal on Advanced Science, Engineering and Information Technology, Vol. 7, No. 1, pp. 250-256, 2017.

[5] G. Padmavathi and D. shanmugapriya, "A survey of attacks, security mechanisms and Challenges in Wireless sensor networks", International Journal of Computer Science and Information Security (IJCSIS), Vol. 4, No. 1 & 2, 2009.

[6] Y. Xiao, V. K Rayi, B. Sun and et. al.,"A survey of key management schemes in wireless sensor networks", Computer Communications, Vol. 30, pp. 2314–2341, 2007.

[7] 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.

[8] B. Lai, S. Kim, I. Verbauwhede, "Scalable session key construction protocol for wireless sensor networks", IEEE workshop on Large Scale RealTime and Embedded Systems LARTES, 2002.

[9] S. Zhu, S. Setia, S. Jajodia, "LEAP: efficient security mechanisms for large- scale distributed sensor Networks". 10th ACM conference on computer and communications security, October 2003.

[10] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, J.D. Tygar "SPINS: security protocols for sensor networks", 7th annual ACM/IEEE international conference on mobile computing and networking, pp. 189–99, July 2001.

[11] H. Chan, A. Perrig and D. Song, "Random Key Predistribution Schemes for Sensor Networks", IEEE Security and Privacy Symposim, 2003.

[12] L. Eschenauer and V. Gligor, "A Key Management Scheme for Distributed Sensor Networks", 9th ACM Conference on Computing and Communication Security, Washington, DC, USA, November 2002.

[13] H. Chan, A. Perrig and D. Song, "Key distribution techniques for sensor networks", IEEE Symposium on Security and Privacy, pp. 197-213, berkely, California, May 2003.

[14] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks", 10th ACM conference on Computer and communications security CCS03, 2003.

[15] A. Rasheed and N. Rabi, Mahapatra. "Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor networks." IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 1, pp. 175-184, 2011.

[16] J. Zhang and et al., "A Strong Key Pre-Distribution Scheme for Wireless Sensor Networks", International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009.

[17] N. Mittal and N. Ramon, "Cluster-based key predistribution using deployment knowledge." IEEE Transactions on dependable and secure computing, Vol. 7, No. 3, pp. 329-335, 2010.

[18] J. Zhang, T. Jianwei and L. Jian, "Key Distribution using Double Keyed-hash Chains for Wireless Sensor Networks." International Journal of Security & Its Applications, Vol. 7, No. 5, 2013.

[19] K. Mu and L. Li, "An Efficient Pairwise Key Predistribution Scheme for Wireless Sensor Networks", Journal of Networks, Vol. 9, No. 2, pp. 277-282, 2014.

[20] J. Zhang, W. Xuerui and L. Jian, "An Efficient Key Predistribution Protocol for Wireless Sensor Networks via Combinatorial Design", International Journal of Security and Its Applications, Vol. 9, No. 6, pp. 135-146, 2015.

[21] J-SIM Simulator, https://sites.google.com/site/jsimofficial/, December 25, 2016.