Random Cooperative Key Pre-Distribution Scheme in Wireless Sensor Networks

https://doi.org/10.3991/ijoe.v14i11.9505

Xiaojuan Zhao
Hunan Urban Construction College, Hunan, China
xiaojuanzhao2401@126.com

Abstract—To cope with the security challenges brought by the popularization of wireless sensor network (WSN), a new random key pre-distribution scheme for WSNs based on the grid deployment theory of Blom mechanism is proposed. The core idea is to divide the network area where the nodes are into different types of hexagonal grids and nodes in different grids use different ways to create keys. Theoretical analysis and simulation results show that the scheme has better connectivity, local security and global security. In view of the existing storage consumption problems, a deterministic key establishment scheme is proposed based on the irregular network model. The simulation results show that the effective coding mechanism introduced optimizes the storage consumption in the network range. It also has a higher security threshold and absolute connectivity, and the enemy's ability to resist capture attacks is stronger.

Keywords—WSN, security, key management, key pre-distribution

1 Introduction

A sensor is a "output signal device or device that is made up of a sensitive element and a conversion element, and can be measured in a sense according to a certain rule". A sensor is a technology that collects information about physical objects or processes. From a technical level, sensors are the devices that can convert parameters or events in the physical world into devices that can measure and analyze signals. Sensors are directly connected to the controller and processing stations to transmit the collected data through wireless transmission to the disposal station. Wireless sensor is composed of a large number of micro sensor nodes and these nodes constitute a mobile wireless self-organizing network to achieve the function of acquiring the related information of the objects. The University of California at Los Angeles, in collaboration with the Rockwell Science Center, proposed the concept of wireless integrated network sensors and studied the devices of low power sensors. In 2003, the Massachusetts Institute of Technology proposed WSN and published in the Journal of Technical Review. WSN is formed in the case that when many sensors monitor a large area of physical environment in collaboration. Sensor nodes are often responsible for not only collecting data and analyzing internal networks, but also responsible for integrating their own data and other node data. These nodes can communicate with each other, or the nodes communicate directly with the base station. With the gradual deepening of the application of the Internet of things, higher requirements for its security are also put forward.

The importance of sensors is not only reflected in the wired environment, but also in almost any environment of WSN and is applied in a very wide range of fields. For example, it is applied in cotton textile processing field, mechanical power field, aeronautics and astronautics field, bioclone medicine industry field and energy saving and emission reduction environment field, and also widely used in household appliances. With the electronic hardware circuit becoming cheaper and miniaturized, WSN has a very wide application prospect. Compared with traditional network, WSN has the characteristics of limited sensor node storage capacity and computing power, fast change of network structure, complex topology, and lack of unified identification and coding. The security of WSN needs key management, security routing, node authentication, and intrusion detection. Among them, key management is the core of WSN security. The traditional computer network is established based on the existing standard. The energy of WSN is the main problem for the design of all nodes and the use of resources, and it cannot be directly contacted with the sensor nodes. Many protocols and mechanisms in WSN are proprietary solutions, and most of them adopt multi-hop routing in link communication. The standard-based solutions are progressing very slowly. How to find a multi-hop path from a sensor node to the base station is one of the most important challenges that WSN faces, which has attracted great attention from the academic community.

2 Literature review

In WSN, there are two structure models of distributed and layer cluster. In the distributed structure, the functions, energy and structure of each node are the same, and each node is homogeneous. In the layer cluster structure, the division of responsibilities of nodes is different. According to the different capabilities of the nodes, the nodes are arranged to perform different functions. The nodes of different functions are called base stations, cluster heads and common sensing nodes, respectively. Cluster heads are special nodes selected according to certain algorithms and protocols. The layer cluster model is suitable for the occasions with larger network scale. The multi-level message is applied to integrate and reduce the communication amount, reduce the energy consumption of node communication and reduce the communication distance of nodes. Compared with distributed structure, it has a higher transmission efficiency and longer life cycle. The structure of WSN typically includes many common sensor nodes, receiving points, public networks, management nodes and end users. In the target sensor area, many small intelligent and inexpensive sensor nodes are randomly dispersed. These sensor nodes cooperate with each other through a wireless connection, and form a network for communication to collect, transmit and analyze the data in the environment. WSN carries out the deployment of nodes in a mobile and self-organizing way, ensuring that the network obtains information in the real world and carries out ubiquitous control in a multi-hop network protocol. Nodes transmit data that have been collected along the WSN link path. Until the data is transmitted to the direction of the sensor node, the data is transmitted to the final node and received, and the finally received node is called the sink node. The sink node is essentially based on a cooperative modulator between a sensor node and end users, and it can be regarded as a gateway node of a network. The sink node acts as a gateway with high processing capability and communicates directly with task management nodes. The Internet or satellite constitute a public network to complete the connection between the sink node and the task management node. Once the end user receives data from the task management node, it immediately executes some processing behavior on the received data.

Based on the collaborative effort between a large number of sensor nodes distributed in the region of interest, these coordinated sensor nodes cooperate with other nodes in the WSN based on some network topology to meet the requirements of the application. Each sensor node monitors the local environment and processes and stores the collected data locally so that the other sensor nodes in the network use these messages. To provide an economical and feasible scheme for extensive applications, Kumar and Pais (2018) proved that WSN is a good alternative and the WSN structure must be able to accept the node with limited computing power and limited power in WSN. Gateway nodes can share and load the loads on wireless sensor nodes and prolong the lifetime of network work [1].

Gharib et al. (2016) pointed out that the dense pre-allocation scheme can enable any two nodes in the network to establish a shared key directly. When the number of the captured nodes is not more than the threshold value, the entire network is secure [2]. The main idea of the scheme is to produce an open matrix G on the finite field, N is the number of nodes, and any $\lambda+1$ column of matrix G is linearly independent. At the same time, a secrecy symmetric matrix D of $(\lambda+1) * (\lambda+1)$ is generated randomly, and $N*(\lambda+1)$ matrix $A=(D*G)^T$ is calculated, in which $(D*G)^T$ is a transposed matrix of $(D*G)$. $K= (D*G)$ is a symmetric matrix, that is, $K_{ij}=K_{ji}$. Assuming that each legitimate node stores the k-th line in the matrix A and the k-th column in the corresponding matrix G, when the node i and node j are to generate the shared key, two nodes exchange the corresponding column values of the G matrix, and the matrix multiplication operation is conducted to independently calculate the key K_{ij} and K_{ji}.

Yavuz et al. (2017) proposed the WSN key pre-distribution and dynamic allocation strategies, and put forward a key allocation strategy based on the combination of pre-distribution and dynamic distribution of keys, which use a constructed key management tree to complete distributed and centralized management [3]. The key management tree uses the following model: a remote control device HomeHost is used to manage the network. The nodes in the network are divided into common nodes and base stations with special functions. These base stations divide the network into groups of different levels. For each group, the base station establishes secure communication with sensor nodes or high level base stations and HomeHost to form a key management tree. Then, through the key management tree, a secure communication between neighboring base stations and neighbor nodes can be established.

Arora et al. (2016) proposed a key management scheme based on deployment information for WSN, which adopts identity encryption algorithm. First, a network grouping model is established to deploy the sensor network by dividing the network deployment area into several sub regions. Then, the identity-based cryptosystem is used, and bilinear mapping is used to complete mutual authentication and pairwise key establishment among nodes [4]. The scheme has higher security, but the node authentication and pairing key establishment process use asymmetric cryptosystems, so the computation cost is great.

Zahurul et al. (2016) proposed a dynamic key agreement scheme based on edge key for sensor networks. First, the key pre-distribution stage generates a polynomial for each edge of all the sub-regions of the network, which is called the edge key. Secondly, for each node, the four-side polynomial key components corresponding to the four edges of the node in the node are stored. Therefore, the nodes in the adjacent region can establish the shared key by storing the same edge polynomials. The shared key is found to establish the pair key by using the shared polynomials among the nodes, and the path key establishment stage is calculated by using the multi-hop path and the pair key is established [5]. Although the scheme reduces the storage cost of nodes, the computation and communication overhead is large. As a result, a key management scheme based on node location for partition is put forward. By using the known node deployment information, the network nodes are divided into several logical groups, and the key is assigned to each node system from a structured key pool.

Olofsson et al. (2016) proposed a group-based node deployment model for WSN. In the model, nodes are deployed in groups, so that the location of nodes in the same group is close after deployment. Based on this idea, two key pre-distribution schemes are proposed: management scheme based on hash key and polynomial-based management scheme. First, a group-based node deployment model is proposed. Nodes in the network are divided into n deployment groups and each group has m nodes. Thus, the probability of nodes in the same deployment group becoming neighbor nodes is relatively high, and at the same time, a spanning group is formed between different deployment groups [6].

Wei et al. (2017) proposed a key pre-distribution scheme based on the communication range [7]. The main idea is that the neighbor nodes refer to two nodes in each other's communication range, and the non-neighbor nodes are not necessary to store the shared key. Therefore, the node A takes the m keys randomly from the key pool S first. And for the neighbor node of the node A, the k shared keys are taken from the A node randomly, then a key is taken from the key pool, so that each node has a key, and the node in the communication range has a shared key. Therefore, the communication between neighbor's node is guaranteed, and there is no too many useless keys.

The communication capability of WSN is limited so that nodes can only communicate directly with neighbor nodes. The typical way of communication is to communicate in multi-hop mode. At the same time, data processing technology such as data fusion is usually used to optimize network performance. Therefore, in view of the characteristics of WSN, Khasawneh et al. (2017) put forward a universal hierarchical key system. Each node preserves four types of ciphers: individual cipher (the individual key between each node and the base station), the group cipher (the key shared among all nodes), the cluster cipher (the key shared between each node and all its neighbor nodes), and a dual key (a separate key between each node and all its neighbors) [8]. In WSN, the individual key is generated first. The cluster key is generated and updated through the dual key, and the group key is generated and updated through the cluster key. Therefore, the key is how to establish and update the dual key.

The key management scheme with obvious advantages will be applied in terms of application background and demand. At the same time, the existing key pre-distribution schemes have different problems for different requirements, such as poor network connectivity, uneven loss of nodes, and low security performance. Therefore, it is necessary to further study the key pre-distribution scheme of WSN.

3 Method

3.1 Multi-key space scheme based on Blom mechanism

Based on the idea of multi-key space scheme and combinatorial design theory, the scheme of group key pre-distribution is optimized and a scheme of WSN multi-key space based on Blom mechanism is proposed. The collection grid i contains a complete key grid j and 6.5 key grid j. A key grid is evenly distributed in two adjacent set grids, and the size of the communication radius between nodes is determined by the size of the collection grid in the region. If the size of the collection grid is L in a certain range and the communication radius is R between the nodes, in order to ensure the normal communication of the nodes in the adjacent collection grid, it is necessary to satisfy the case of $L \geq 2R$.

For different collection grids and key grids, the key pool is also different and is determined, so there is no intersection of the key pool between different grids. When q satisfies the prime number of $q^2+q+1 \geq N$, a symmetric balanced incomplete block design $(q^2+q+1, q+1, 1)$ can be generated by q-order finite projection space. In the process of design, the number of keys generated by the network is q^2+q+1, and the number of keys in a single node is $q+1$, in which the nodes in the collection grid create their respective communication keys through the multi-key space scheme.

3.2 Performance analysis

According to the design idea, a collection grid is made up of a complete and 6.5 key grids. The nodes in different aggregate meshes are referred to as inter-group links, and in contrast, nodes in the same collection grid are called intra-group links. At the same time, the node C is set randomly in a triangle in the collection grid i. Therefore, when the distance from the node to the corresponding side is x and the communication radius between the nodes is r, the arched area falling in the adjacent grid is shown in Formula (1).

$$ds = \left(l - \frac{2\sqrt{3}}{3} x \right) * dx \cdot \tag{1}$$

The average area of the arched area can be obtained as shown in Formula (2).

$$s' = 6\int_0^r \left(l - \frac{2\sqrt{3}}{3} x \right)\left(r^2 \cos^{-1}\frac{x}{r} - x\sqrt{r^2 - x^2} \right)/ sdx \cdot \tag{2}$$

Therefore, the proportion of arbitrarily random nodes in adjacent sets can be approximately expressed as Formula (3).

$$P = s' / \left(\pi r^2\right). \tag{3}$$

Supposing that there are two nodes in WSN, namely n_i and n_j, if they are neighbor nodes, they are represented by event $A(n_i, n_j)$. If the key sharing is needed, they are represented by event B (n_i, n_j). Then the local connectivity rate is:

$$P_{local} = \Pr\left(B\left(n_i, n_j\right) \middle| A\left(n_i, n_j\right)\right). \tag{4}$$

If the link occurs only in the same grid for generating the key, then the node connectivity in the same set of keys is:

$$P_1 = 1 - \frac{\left(\frac{w}{t}\right)\left(\frac{w-t}{t}\right)}{\left(\frac{w}{t}\right)^2}. \tag{5}$$

The connectivity among random nodes in a network is calculated as:

$$P_{local} = \left(1 - p\right) \times p_1 + 1 \times p. \tag{6}$$

3.3 Simulation analysis

It is assumed that there is a maximum of 250 storage space between nodes, and the scheme is deployed in a region of 1000M * 1000M. There is R_{max}=50M between WSN nodes, each node has 60 adjacent nodes, and the local area is 100% connected. By computing, it is obtained that d=20, $P_{required}$=0.4, and side length L=100M. There are 72 inter-group links in the deployed area, the number of nodes in the link is 176, and there are 44 nodes in each link in the key network, and q=8.

The connectivity between random nodes in the network can be expressed as: when L=2R, p=0.35. And assume that the maximum space capacity of each node is S_{max}=250, then there is t*(λ+1)+(q+1)=250. Then, the simulation results of connectivity between local area networks are shown in Figure 1.

When t=3 and the value of ω needs to be less than or equal to 42, the value of P_{local} will be greater than or equal to $P_{required}$. When t=4, the connectivity of this scheme is between 0.98 and 0.61; when t=3, the connectivity of this scheme is between 0.785 and 0.485. However, a higher hop connectivity rate is not necessary because the connectivity between nodes can be improved by finding multiple paths. Simulation analysis shows that this scheme has good performance in connectivity. The simulation of local security and global security is shown in Figure 2 and Figure 3, respectively.

Figure 2 shows that, when the node part is captured, the ratio of the reference plan link is greatly increased linearly. When all the nodes are captured, the ratio of the reference plan link affected when being captured is 20%, whereas the ratio of the link in the proposed scheme is about 1%. Compared with the reference plan, when the 100 nodes are all captured, the ratio of links affected is only half of that of the reference plan. Even if the number of nodes captured is increasing, the advantages of the proposed scheme still exist.

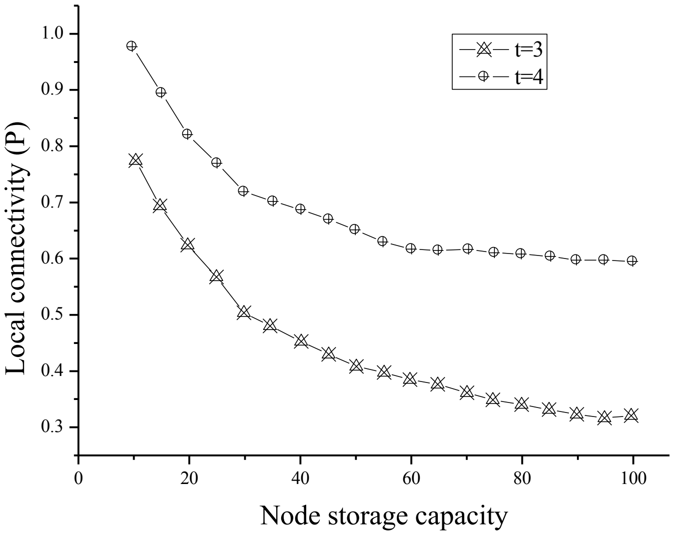

Fig. 1. The simulation results of connectivity between local area networks

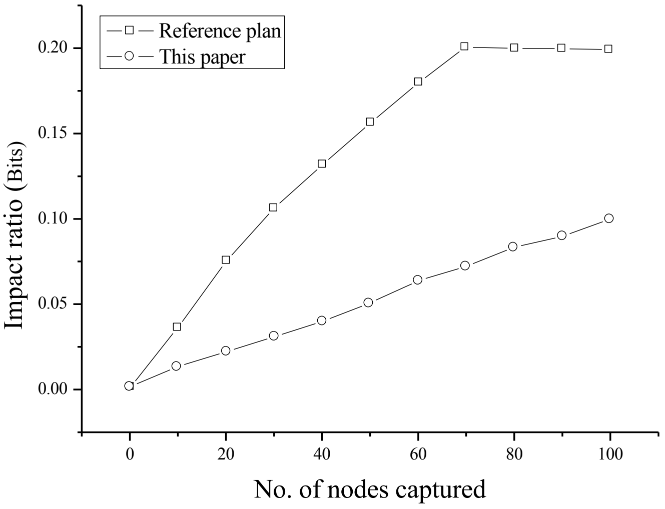

Fig. 2. The simulation of local security

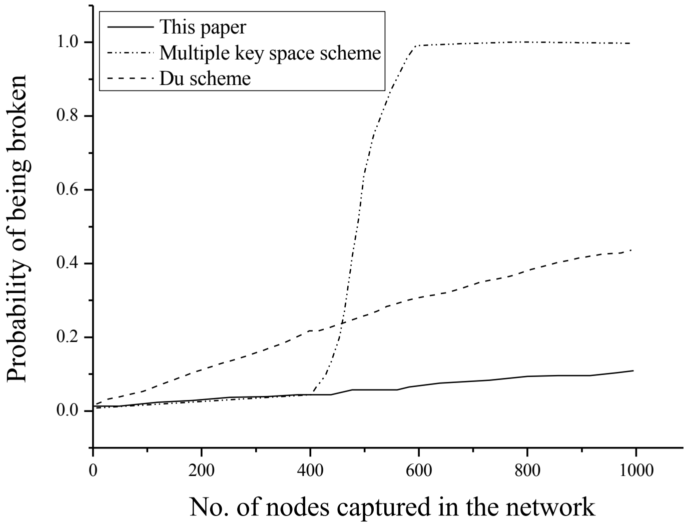

Fig. 3. The simulation of global security

The simulation results of Figure 3 show that when the number of nodes captured in the network reaches 400, the security of the global network of the three schemes is compared, and the Du's scheme is the worst. In the scheme proposed by Du et al., the probability of any link being captured is rising and the ratio of the link affected by this scheme is only about 5%. Even when all 1000 nodes are captured in any link, the probability of captured attacks relative to the Du's scheme has already exceeded 70%, and the probability of the captured attack of the multi-key space scheme is about 42%, but the link of the scheme proposed here is only about 10%.

4 Results

4.1 Deterministic key establishment scheme based on LU matrix

The steps of polynomial pre-distribution based on LU matrix are as follows:

Step 1: in the key pre-distribution phase, the server first generates a large polynomial pool, the polynomial pool is composed of t-order symmetric binary polynomials, and each polynomial on the finite field GF(q) has its own identifier.

Step 2: the arrangement of symmetric matrices is replaced by binary polynomials, and the generated binary polynomial matrices are arranged in the form of m*m.

Step 3: apply the decomposition technique of LU matrix to the decomposition of polynomial pool. This method decomposes the symmetric polynomial matrix K into an upper m*m triangular matrix L and a lower m*m triangular matrix U. The efficient allocation of the zero element of the matrix can save the storage rate among the nodes.

Step 4: before the node is deployed, the upper triangular matrix L is decomposed into several row vectors L_{ni}, i=1,2,...,N, and the lower triangular matrix U is decomposed into a number of column vectors U$_{ni}$, i=1,2,...,N. Then randomly assign to the i-th node in the i-th column of the matrix L and the matrix U, and finally save the identifier of the row and column vector of the node.

4.2 Performance analysis

The Blundo scheme is a shared key algorithm based on finite field polynomials, which has good security tolerance. The LU matrix scheme utilizes the security properties of finite field polynomials to provide better performance against capture attacks. Supposing that the two schemes have the same storage capacity of K, then the simulation results are shown in Figure 4. The result diagram shows that when k=200 and the number of the captured nodes is more than 100, the longitudinal axis shows an increasing trend. When the number of nodes captured is more than 350, the communication probability between the nodes not captured is 1. When the number of the captured nodes is less than 200, the probability of communication between the nodes not captured is 0. When the number of captured nodes is 200, the probability of communication between the nodes not captured is increased, the instantaneous network communication will be leaked, and the probability of communication between the nodes not captured is 1. The probability of communication between the LUKM nodes is 1. Compared to the LU matrix scheme, the Blundo scheme needs to sacrifice more capacity to store nodes, thereby increasing the security of the network. The Blundo scheme is more secure and reliable in the network application, and the nodes also have a good tradeoff between the storage S of capacity and the security threshold T of the network.

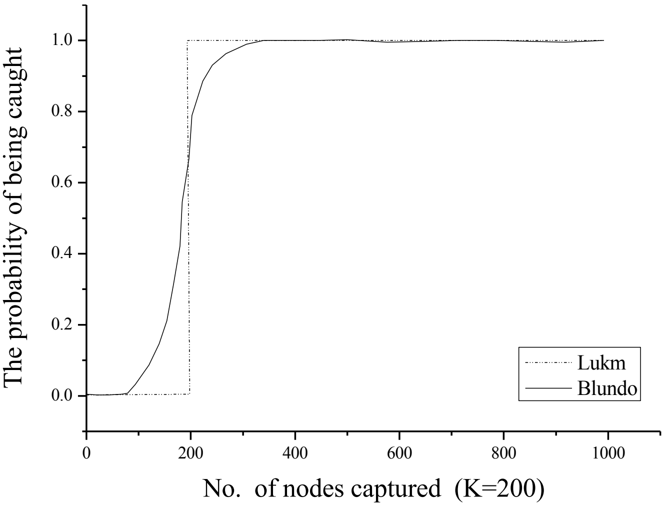

Fig. 4. Anti-capturing feature of the scheme

The storage savings simulation diagram of the LU matrix scheme can be obtained from the consumption formula of the entire network's memory consumption and saving part of memory, as shown in Figure 5. The simulation diagram shows the influence of the order of polynomial and the number of nodes on saving the storage of network space. At the same time, it also shows that if we want to reduce the burden on the network effectively, three different methods should be used to control the size of the network and reduce the class of polynomials. The zero element in the matrix can be counted and allocated reasonably, because the wireless sensor has its own special properties. Compared with the vast majority of WSNs, the LU matrix scheme can reach about 78% in the storage space. Therefore, the LU matrix scheme is an effective application for WSNs.

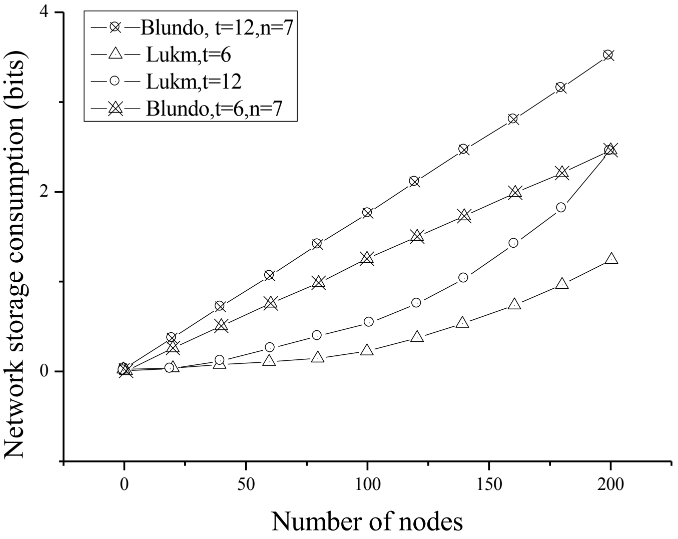

Fig. 5. Network storage consumption

Assuming that the number of nodes N is 200, the polynomial magnitude q is 135, the value of polynomial order t is 6 and 12, and the size of node group n is 5 and 7. When the node group n is equal to 7, regardless of the order of the polynomial, the overall performance of the Blundo scheme is continuously reduced due to the excessive consumption of storage. With the decrease of polynomial order, the overall performance superiority of LU matrix scheme is revealed. Even if the order of polynomials is the same, when the node group of the Blundo scheme is larger, the storage consumption of the LU matrix scheme between the networks is still lower than that of the Blundo scheme. However, when the node group n is equal to 5, regardless of the size of the polynomial order, the storage cost of the Blundo scheme is better than that of the LU matrix scheme, but the security performance is not high. But when the order of polynomial increases, the performance of network storage becomes the primary problem. Therefore, the main problem is to solve the trade-off between security tolerance and the storage and consumption of nodes in the network.

The storage consumption between the networks can calculate the savings ratio of the number of nodes stored in the LU matrix scheme at different times, as shown in Table 1.

Table 1. The savings ratio of storage consumption for LU matrix scheme

The number of nodes N	The order of polynomials T	Storage consumption	Storage savings	Saving ratio
100	6	$0.375*10^5$	$1.125*10^5$	75.59
100	12	$0.515*10^5$	$1.95*10^5$	76.87
200	6	$1.23*10^5$	$3.85*10^5$	78.43
200	12	$2.23*10^5$	$7.25*10^5$	77.26

5 Conclusion

Based on the brief introduction to WSN security, a new hexagonal multi-key space scheme is proposed in view of the offset property between the two factors of network connectivity and security in the existing schemes. This method relies on the high connectivity rate of the group deployment strategy and the high anti-capture capability of the multi-key space. The simulation analysis shows that the scheme not only greatly improves the connectivity of the network, but also effectively enhances the ability of the network to resist the attack of the enemy. Compared with the proposed scheme, it improves in terms of network connectivity, storage overhead, node capture resistance and communication energy, but when the scale of the network is increasing, the overall performance is decreasing.

The decomposition technique of LU matrix is applied to the decomposition technique of a polynomial pool in a finite field. The scheme uses polynomial pools and polynomials to replace the previous key pool and symmetric matrix. The results show that the scheme is replaced by the former key pool to a polynomial pool. For the upper triangular matrix L of the LU matrix and the lower trigonometric matrix U, the part of the zero element is very effective for reducing the storage consumption of the nodes. The simulation results show that the new key determination scheme is efficient for the anti-capture between nodes and the saving of node storage, and the saving rate of storage is over 78%. However, if the network size is large, the connectivity performance of the network will decrease.

6 References

[1] Kumar, A., & Pais, A. R. (2018). A new hybrid key pre-distribution scheme for wire-less sensor networks. Wireless Networks, (8): 1-15.

[2] Gharib, M., Yousefizadeh, H., & Movaghar, A. (2016). Secure overlay routing using key pre-distribution: a linear distance optimization approach. IEEE Transactions on Mobile Computing, 15(9): 2333-2344. https://doi.org/10.1109/TMC.2015.2486758

[3] Yavuz, F., Zhao, J., Yagan, O., & Gligor, V. (2017). K-connectivity in random k-out graphs intersecting erdős-rényi graphs. IEEE Transactions on Information Theory, 63(3): 1677-1692. https://doi.org/10.1109/TIT.2016.2634422

[4] Arora, V. K., Sharma, V., & Sachdeva, M. (2016). A survey on leach and other's rout-ing protocols in wireless sensor network. Optik, 127(16): 6590-6600. https://doi.org/10.1016/j.ijleo.2016.04.041

[5] Zahurul, S., Mariun, N., Grozescu, I. V., Tsuyoshi, H., Mitani, Y., & Othman, M. L., et al. (2016). Future strategic plan analysis for integrating distributed renewable genera-tion to smart grid through wireless sensor network: malaysia prospect. Renewable & Sustainable Energy Reviews, 53: 978-992. https://doi.org/10.1016/j.rser.2015.09.020

[6] Olofsson, T., Ahlén, A., & Gidlund, M. (2016). Modeling of the fading statistics of wireless sensor network channels in industrial environments. IEEE Transactions on Signal Processing, 64(12): 3021-3034. https://doi.org/10.1109/TSP.2016.2539142

[7] Wei, W., Song, H., Li, W., Shen, P., & Vasilakos, A. (2017). Gradient-driven parking navigation using a continuous information potential field based on wireless sensor network. Information Sciences, 408(C): 100-114. https://doi.org/10.1016/j.ins.2017.04.042

[8] Khasawneh, A., Latiff, M. S. B. A., Kaiwartya, O., & Chizari, H. (2017). A reliable en-ergy-efficient pressure-based routing protocol for underwater wireless sensor net-work. Wireless Networks, 1-15.

7 Author

Xiaojuan Zhao works as associate professor at Hunan Urban Construction College, Hunan, China

Article submitted 09 September 2018. Resubmitted 13 October 2018. Final acceptance 27 October 2018. Final version published as submitted by the author.