International Journal of Security and Its Applications
Vol.9, No.11 (2015), pp.313-322
http://dx.doi.org/10.14257/ijsia.2015.9.11.29

A Key Pre-distribution Scheme Based on Deployment Information

Shulan Xia[1], Jilin Wang[2]*, Ru-gang Wang[2]

[1]*College of Electrical Engineering,*
Yancheng Institute of Technology, Yancheng 224051, Jiangsu, PR China;
[2]*College of Information Engineering, Yancheng Institute of Technology,*
Yancheng, 224051, Jiangsu, PR China
xslnj@126.com

Abstract

A scheme of grouping key distribution based on polynomial protocol is proposed and experimentally demonstrated. The grouping idea is ingeniously used in the design of key distribution. The performance is experimental demonstrated by comparing with kinds of random key pre-distribution schemes. The results show that it can not only guarantee the key connected rate but also strengthen the security performance of the network, and this scheme is very suitable for static underwater acoustic communications network.

Keywords*: Communication network; Grouping; Key distribution; Network connectivity*

1. Introduction

The network nodes of underwater acoustic communication are randomly deployed in an unknown area, in this case, the neighbors are unknown, and it is very difficult to set up the entire network in advance for all possible security key, so the secure key establishment process is the core problem in security management. Pre-shared key is the easiest kind of key establishment process, and the required key in node communication is stored in the network nodes by the Key Distribution Center prior to deployment. Because the scheme of key pre-distribution in the system is almost completed prior to the deployment, and it is generally based on a simple and efficient symmetric encryption algorithm, widely used in distributed, self-organizing wireless communication networks [1-4].

In this paper, the key pre-distribution mechanism will be studied in the underwater acoustic communication network environment. And the typical random key pre-distribution scheme is analyzed, a method of grouping key distribution based on polynomial protocol is proposed and experimentally demonstrated, and its feasibility is demonstrated in a static simulation of underwater acoustic communication network.

2. Key Distribution Scheme Evaluation Standard and Key-Pre Distribution Protocol

2.1. Key Management

Encryption technology is an important part of all network security architecture, and key management is one of the key issues. The security of the encryption system mainly depends on the use of secret key. Once the key has been obtained by an attacker, and the security of the whole system will be threatened.

* Jilin Wang[2] is the corresponding author.

ISSN: 1738-9976 IJSIA

In underwater acoustic communication networks, because the nodes are deployed in open areas, sensor nodes are likely to be the attacker to capture, so the attacker can easily obtain key information. Key management includes key generation, distribution, update and destruction. In underwater acoustic communication network key distribution is very important, because in most cases, impossible to know in advance what will be the neighbor nodes, *i.e*., which nodes need to share the same pair of keys.

2.2. Key Distribution Scheme Evaluation Standard

At present, the following key distribution scheme evaluation standard:

(1) Scalability: there are more than thousands of the nodes. With the expansion of the scale, computation, storage and communication overhead of key agreement required will increase, the key management schemes and protocols must be able to adapt to the different scale of the network, have the ability to support large scale network.

(2) Efficiency: the storage, processing and communication capabilities of network nodes are very limited, so we must give full consideration to efficiency, mainly as follows:

1) Storage space: the storage space will be saved the key;
2) Processing time: the number of processing cycles for establishment of key;

3) The amount of communication: the amount of information transmission has been required in the process of generating key;

4) Key connectivity: the probability of two or more sensor nodes store the same key

(3) Resilience: the ability to resist damage or captured nodes. Survivability can be said when some nodes are damaged, the probability of the other node key is exposed. Survivability is better, the lower the mean link damage.

(4) The dynamic changes of network: dynamic changes including the nodes join and leave dynamically. Due to attack, the power is exhausted and unable to work node, node scheme must ensure that leave cannot continue to be important in the data network. At the same time must be extended support network, but also can ensure the new node cannot be added to the network transmission of secret information.

2.3. Key-pre Distribution Protocol

Key-pre distribution protocol: random key pre distribution is a key establishment protocol mainly terrestrial wireless sensor networks, node communication required key by key distribution center in the network is stored in the nodes before deployment. The principle of the agreement is the average degree of the network node exceeds a certain threshold value, a random graph with high probability of connectivity. The average value of each node is established when the safety link in the network than with high probability connected network security required link threshold, will form a security network connectivity. Key pre distribution scheme is established based on the most complete security system deployment, and the general symmetric encryption algorithm based on simple and efficient, so it is widely used in distributed, self-organizing wireless communication networks. But the random key distribution mechanism requires storage cost is very high, and with the increase of the number of nodes in the network, the node needs to store the key with the exponential growth of [5]. And because the random key distribution, can only be applied to meet the network structure model of random graphs. If the non dense or node density of nodes in a network, so as to establish some key nodes cannot be successfully completed, and will lead to non connected network.

3. Typical Random Key pre-Distribution Scheme

3.1. Eschenauer-Gligor Scheme

The basic random key pre-distribution scheme is firstly proposed by Eschenauer and Gligor [6], this scheme is based on probability and random graph theory, when the average of safety link established in the network is over the necessary safety link threshold with high probability network connectivity, and a secure connectivity network is formed. The scheme will be analyzed through the three sections.

(1) Process of node key pre-distribution prior to deployment.

The random key pool will be constructed, it contains the S kinds of different keys (S is large enough), and each key has a unique identifier ID. The k key will be extracted at random from the key pool in each node, and the keys will be saved to the memory, and then the extracted keys back into the key pool. So that, the k keys and key chain with identifier can be formatted in each node. According to Erdos random graph theory, the probability that the key can be shared by two nodes is given by [7].

$$p = 1 - \frac{((S-k)!)^2}{((S-2k)!S!)} \quad (1)$$

(2) Phase of shared key discovery, it occurs after completing node deployment.

Two adjacent nodes can exchange the key identifier, the identifier is retrieved based on its own secret key string to determine whether the same key. If two neighbors have at least one same key, then select one as the shared key. Thus, there is a secure link in the figure of key shared between two neighbors.

(3) Phase of shared key indirect negotiation.

If there is no public key between two nodes, it can be negotiation to share key through a third party as an intermediary neighbors with the public key of the two nodes, the process is known as shared key indirect negotiation phase, this process can ensure normal communication across the network.

Since $k << S$, between any two neighboring nodes exist only in a probabilistic public key, which is the two neighbor nodes exist only in a probabilistic safety chain, this probability is the probability of network security connectivity p. For the Eschenauer-Gligor scheme, the key goal is to design a suitable S and k, so that the p can reaches a predetermined expectations, making the network's key sharing Pictured connected graph, thus ensuring the security of the entire network communication.

3.2. Random Key Pre-Distribution Model of q-Composite

The Eschenauer-Gligor scheme only requires two neighbor nodes to share a common key, so the secure link can be established if the node simply stores small kinds of keys, it can reduce the node's storage overhead, but the node is weak against external attacks. To enhance the node anti-attack capability, the Eschenauer-Gligor scheme was extended, and the q-composite random key pre-distribution scheme is proposed by Chan, Perrig and Song [8]. The scheme and the basic model is in a similar procedure, only requires the number of adjacent nodes is larger than q public key to establish a secure communications link. In all the shared key information received, if the shared key between two nodes quantity exceeds q, is a q', then all q' share the key generation with a key k, $k = hash(k_1 \| k_2 \| ... \| k_{q'})$, where the hash is a public ha Greek function. Similarly, in the q-composite scheme

probability of network connectivity is based on probability theory and random graph theory calculations, is given by

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

Where p(i) is extracted from the S-key pre-distribution of k to the node, the two neighbor nodes have the probability with the i same key. According to the total probability Equation, any two nodes can directly establish a shared secret with probability.

$$p = 1 - (p(0) + p(1) + ... + p(q-1)) \quad (3)$$

The key agreement scheme overhead of q-composite is basically the same as the Eschenauer-Gligor scheme, and the only difference is, q-composite scheme requires more than once a hash computed shared key. However, the energy consumption of the hash computation is relatively small, and broadcast key identifier shared key discovery phase only once, this part of the overhead is not.

From the above analysis, improved the value of q can improve the resistance to attack networks and shared key number q difficulty exponentially. But in order to ensure network connectivity, namely secure network shared key between any two points more than the probability q to achieve the desired probability value p, it is necessary to reduce the size of the entire key pool to increase the shared key between nodes degree of overlap. Narrow key pool will have a negative effect, the enemy captured a few key nodes can get a lot of space, it will seriously affect the security of the network. So for the use of this program network, its security and connectivity is a contradiction. The experimental results show that when q = 2 can achieve optimal network performance.

4. Key Pre-Distribution Scheme Converged Packet Design

4.1. Ideas of Grouping Design

Polynomial-based key pre-distribution scheme has a safe threshold, and it has better anti-attack capability than the key pre-distribution scheme based on random probability. Initially, an approach based on the finite field GF (q) symmetric polynomial key pre-distribution is proposed by Blundo[9], and then the scheme is further optimized by Liu and Ning[10-11], and it constructs on t-order symmetric binary polynomial at randomly over a finite field GF (q) .

$$f(x, y) = \sum_{i,j=0}^{t} a_{ij} x^i y^j (\mathrm{mod}\, q) \quad (4)$$

Where q is sufficiently large primes, before node deployment, the polynomial can pre-distributed for each node, the node i, and distribution f(i, y), for node j, the pre-distribution f(j, y). After node deployment, it should be calculated to go through polynomial shared key, calculated as follows: node i for j compute node j for i calculated by the symmetry of a polynomial $f(i, j) = f(j, i)$, this result is the node i and j shared key. T-order polynomial $f(x, y)$ having a safety threshold t, as long as the number of nodes to be captured is not more than t, then the secure communication network is not affected, and by capturing the nodes does not pose a

threat to the network node, when the node to be captured is greater than the safety threshold, network security will decline rapidly.

In order to improve network security, while achieving better connectivity probability of key network nodes, in this paper introduces the polynomial grouped on the basis of calculations designed is introduced to make up for the lack of programs based on polynomial. The basic idea of grouping nodes is to deploy the entire region into a plurality of nodes distributed grids, and each grid corresponds to a node deployment groups, each group of nodes deployed deploy only to the group corresponding to the grid area. Assumed that the wireless sensor network has n nodes and it is divided into g groups, each group has n_g nodes. Each group is assigned a unique identifier for GD, each member of the group node is assigned node identifier for ND, within different groups the same node identifier range is used, while in the same group is relatively unique identifier for each node. Thus, any node has a globally unique identifier for network expansion $D = GD \| ND$. For example, a 1000 wireless sensor network nodes, all nodes are divided into 10 groups, each with 100 nodes, each group GD assign 0-9 for each group node allocation ND 0 to 99, any node in group 2 as a network identifier node 6 can be expressed as D=2| |6. Actual operation is expressed in binary form. And random key is the scheme of the program in the same node for each node before deployment is assigned a unique node identifier, but random key pre-distribution scheme in the node identifier is randomly assigned, and the scheme for each node identifier where the group related to it is easier to determine whether the same set of nodes.

Assuming a 3×3 square region of the deployment region shown in Figure 1, and each node within the grid can obey binomial distribution. Network Control Center does not directly distribute keys to the node, but distributed in GF (q) on randomly generated symmetric binary polynomial to the node. Node deployment, the system in GF (q) can generate on randomly binary symmetric S-containing symmetrical polynomial pool, k polynomial can be drawn out to every node. If a node's key capacity is m, each node distributes k polynomial, as the amount of each key polynomial t +1, then m = k (t +1).

After node deployment, if two neighbors have the same polynomial, directly establish a shared key, if two neighbors have no same polynomial, third-party neighbor nodes with the same polynomial can be found to establish a shared key indirect negotiations.

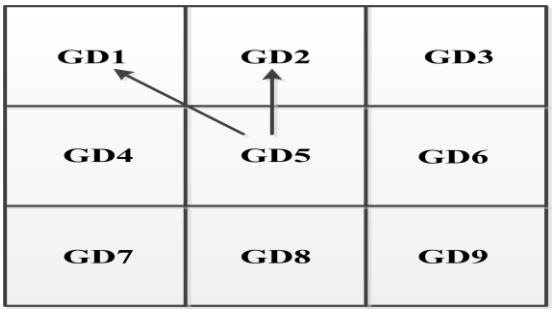

Figure 1. Nodes Grouping Deployment

Grouping deployment can achieve some better results, such as the following:

(1) The network connectivity is not reduced, at the same time the storage information in each node can be reduced, which is particularly important for the sensor nodes.

(2) It can greatly enhance the network's ability to resist the adversary captures nodes.

(3) The impact for betraying local area network key is limited by using grouping deployment.

4.2. Key Management Scheme and Implementation Process

4.2.1. Initialization: First, g number of the symmetrical bivariate polynomial $f_i(x, y)$ can be randomly generated according to number of the network packets, and then all the nodes divide into some groups, a unique identifier D is assigned and stored in the node, at the same time, and the private shared polynomial and the neighbor 8 groups corresponding polynomial can be loaded to the node of each group.

4.2.2. Shared Key Discovery: At this stage, it is assumed to the node a broadcasts its own identifier Da to the neighbor b, after receiving the broadcast, the node b estimates the identifier Da whether or not they are in the same group, if in the same group, they will be calculated and stored for $K_{ab} = f_b(GD_a)$, and its own identifier D is transferred to the node a, after receiving identifier D, they will be calculated and saved for $K_{ab} = f_b(GD_b)$, where K_{ab} is the link-shared key, then the two nodes complete the process of establishing shared key.

If two nodes are different groups, the node b can estimate whether it is one of neighbors based on the group number, if it is the neighbor group, it is determine to use the appropriate polynomial according to its group number, and then, the own identifier D is transferred to the node a, after received the request, the node b will put the D into polynomials in this group, and can obtain the shared key.

4.2.3. Security Link Establishment : After completing the shared key, if the two nodes obtain the shared key, the key is used as two nodes communicate key for the future, if two nodes needed to communicate have no the same key, the two nodes need to find a safe path between nodes by using intermediate nodes. The method is as following, first, the source node sends target node identifier D to the neighbors with shared key, and each neighbor will find out the nodes with shared key. If it is the target node, then the security path is established, otherwise it continues broadcasting to its neighbors, until a safe path is obtained. The source node generates a key after the establishment of safe path, and the key will be sent to the target node through this secure link.

5. Analysis of Performance

5.1. Analysis of Connectivity

In this scheme, it assumes that n is the mumble of nodes in a static underwater acoustic communication network, and it were divided into g groups, there are ng nodes in each groups, P is a probability of shared key between two nodes, and m represents the number of the key pair in each node. For node A and B, node A does not share any key, and node B is different group of two nodes.

$$P_{share} = 1 - P(A) = 1 - P(A \mid B) \times P(B) \quad (5)$$

Considering the most secure connectivity probability, the probability is obtained:

$$P(A \mid B) = (1 - m / (n - n_g))^2 \quad (6)$$

$$P(B) = (\frac{n/n_g}{2}) \times n_g^2 / (\frac{n}{2}) = (n - n_g)/(n-1) \quad (7)$$

According to Eq. (6) and (7), Eq. (5) is simplified.

$$P_{share} = 1 - (n - n_g - m)^2 / ((n - n_g)(n-1)) \quad (8)$$

When the network is large scale, and it can be considered as $n \approx n-1$, then according to $n_g = n/g$, Eq. (8) can be shown:

$$P_{share} = 2m/n + 1/g - g/(g-1) \times (m/n)^2 \quad (9)$$

For random key pre-distribution scheme, the minimum safe node connectivity probability p can obtained by using p=m/n, in general, for the larger network, m << n, so $1/g - g/(g-1) \times (m/n)^2$ can be guaranteed to be a positive. Thus, the scheme can be obtained that secure connectivity probability is greater than random key pre-distribution scheme.

5.2. Analysis of Calculating Load

Between neighbors the main computing shared key overhead is O(t) times modular multiplication. Respect to symmetric encryption algorithm, the polynomial modular multiplication is an expensive larger operation, and it should also take into account two points: the calculation of shared key discovery polynomial is done only once, and it does not need to be calculated after obtaining the shared key. Relative to the same modular multiplication, the computation is still relatively small by using asymmetric encryption algorithm.

5.3. Analysis of Node Anti-capture Capability

In the random key pre-distribution scheme, the betrayed node key is likely to lead to other nodes key exposure, and affect other nodes communicate securely, it great harms to network security. And in this scheme, if multiple nodes are captured, it will only disclose this group or adjacent groups sharing key pair, and it does not affect other groups in the network nodes. In this paper, network simulation tool OMNeT + + is used as the primary experimental platform, Figure 2, is the capturing probability versus different numbers of captured nodes under conditions of n=1000, m=200.

From the Figure 2 we can see that the capturing probability increase as the numbers of captured nodes. The capturing probability of a communication link is less than the probability of the E-G and q-composite scheme in the network. And the network security is fully guaranteed by using polynomial-based key computing in aspect of anti-capture. Theoretical analysis and experimental results show that the scheme proposed in this paper can not only ensure network connectivity, but also improve the network's anti-attack capability. The network security, connectivity and the load in the static underwater acoustic communication can reach a good balance by using the designed scheme.

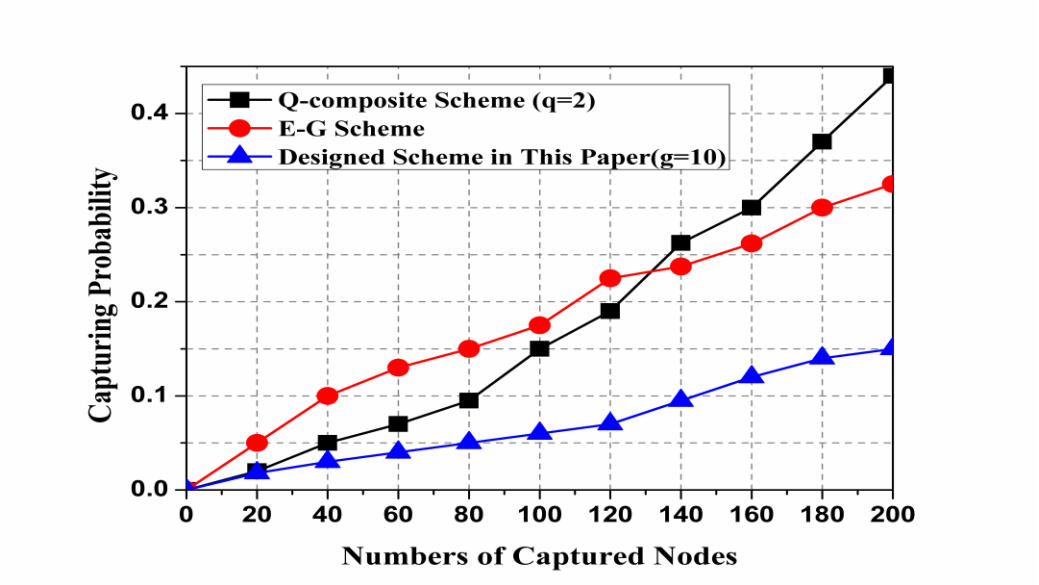

Figure 2. Capturing Probability Versus Different Numbers of Captured Nodes

6. Conclusion

The E-G and q-composite scheme of typical random key management protocol is analyzed, and it shows that they are difficult to achieve network security and connectivity dual optimization. In this paper, the design scheme of grouping based on polynomial key distribution protocol is proposed and experimentally demonstrated. The experimental results show that the capturing probability of a communication link is less than the probability of the E-G and q-composite scheme as increasing the captured number of nodes in the network. The network security can be improved, and network connectivity can be ensured. From these analyses, we can see that this solution is very suitable for static underwater acoustic communications network.

Acknowledgements

This work is supported by the Yancheng Institute of Technology Talents Project of China and the National Basic Research Program of China (973 program) under contract No. 2010CB327803.

References

[1] S. Verma . “Analysis of a New Random Key Pre-distribution Scheme Based on Random Graph Theory and Kryptograph”, Mobile Communication and Power Engineering. Springer Berlin Heidelberg, 92013).
[2] S . Yi, C Yongfeng, T Liangrui. “A multi-phase key pre-distribution scheme based on hash chain”, Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on. IEEE, (**2012**), pp. 2061-2064.
[3] H. Zhao, J. Hu, J . Qin, *et al*. “Hashed Random Key Pre-distribution Scheme for Large Heterogeneous Sensor Networks” Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, (**2012**), pp. 706-713.
[4] E . Khan, E. Gabidulin, B. Honary. “Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks”. IET wireless sensor systems, vol.2, no.2, **(2012),** pp.108-114.
[5] R. Dupont, A Enge. “Provably secure non-interactive key distribution based on pairings”, Discrete Applied Mathematics, vol.154 ,no.2, **(2006)**, pp.270-276.

[6] L. Eschenauer, V D Gligor. "A key-management scheme for distributed sensor networks".,Proceedings of the 9th ACM conference on Computer and communications security., Washingtion, DC, USA., June **(2002)**, pp. 4-6.
[7] J. Spencer,The strange logic of random graphs, Springer-Verlag Berlin and Heidelberg GmbH & Co. K, **(2001).**
[8] H. Chan, A. Perrig, "Song D. Random key predistribution schemes for sensor networks"., Proceedings 2003 IEEE Symposium on Security and Privacy: May 11-14, Berkeley, California, USA.
[9] C. Blundo, A. De Santis, A Herzberg. "Perfectly-secure key distribution for dynamic conferences", Advances in cryptology—CRYPTO'92: 12th Annual International Cryptology Conference, California, USA, **(1992)** Aug., pp. 16-20.
[10]] D. Liu, P. Ning. "Establishing pairwise keys in distributed sensor networks", Proceedings of the 10th ACM conference on Computer and communications security., Washingtion, DC, USA.**,(2003)** Oct., 12-15;
[11] M. A. Simplício Jr, P S L M Barreto, C B Margi, *et al*. "A survey on key management mechanisms for distributed Wireless Sensor Networks", Computer Networks, vol.54, no.15,**(2010)**, pp.2591-2612,.

Authors

Xia Shulan She received MS from Nanjing University of Science and Technology, China, in 2011.Now She is Associate professor in College of Electrical Engineering, Yancheng Institute of Technology, China. She current research interests include electronic technology and information processing.

Wang Jilin He received MS from Southeast University, China , in 2004.Now he is full professor in College of Information Engineering, Yancheng Institute of Technology, China. His current research interests include signal and information processing.