The Safety Analysis on Representative Random Key Pre-distribution Schemes for Wireless Sensor Network

Yang Su-min*, Lu Hong-feng, Cui Jing, Han Yue-xia
Information Engineering Department, Ordance Engineering College 050003, Shijiazhuang
*yangaumin1971@sina.com

Abstract - For wireless sensor network, almost all the key management schemes are improved with the representative E-G and q-Composite key pre-distribution models. Firstly, the author analyzes the key pre-distribution principle of two representative models, and studies the node storage key number, and key pool size, and analyzes the node ability of resistance to captive capacity. Lastly the author utilizes the simulation experiments to verify the analysis validity and correctness, and the deficiency of the E-G and q-Composite key pre-distribution models. The obtained results provide the basis for the design and optimization of WSN safety scheme.

Index Terms - Wireless sensor network, Random key Pre-distribution scheme, Security connectivity, Resistance to captive capacity

1. Introduction

At present, the Wireless sensor network (WSN) is the main way of wireless communication in the digital battlefield, and which is an important technology to obtain data of the opposite army [1]. But the sensors of WSN are deployed in the open area where no one keeps an eye on, and without tamper-proof function itself, so these sensors are vulnerable to information leakage, being tampered, congestion, and black hole threat, therefore the WSN security is much fragile. The Key management is the basis and core to ensure safety of WSN. In the paper the principle of the E-G and q-Composite key pre-distribution models is studied firstly, and the author demonstrates the correlation between the node size and the node storage keys on the condition of ensuring network security. On the other hand the measures to improve the safety of WSN are given. Lastly the author utilizes the simulation experiments to verify the analysis validity and correctness, and the deficiency of the E-G and q-Composite key pre-distribution models, and the experiment results provide the basis for the design and optimization of wireless sensor network safety scheme.

2. The Security Feature Analysis of WSN

The WSN has the generality as same as the traditional wireless network, but it has its particularity which is different from the traditional network.

A. The restricted node energy, limited computing power and storage capacity

Sensor nodes are tiny embedded terminal equipment, which have low cost, limited battery capacity, limited power consumption etc., all of those limit the computational ability and storage capacity of the nodes, so it is difficult to undertake complex computing, and mass storage and long distance communication.

B. The dynamic topology with no centre and self-organizing

WSN is a kind of peer-to-peer network, there is no strict control center. Sensor nodes can join and leave networks at any time, so the network topology is dynamic. Because the node breakdown has no effect on the whole network, network survivability is much strong. The pre-configured infrastructure isn't needed in the process of network deployment. Sensor nodes coordinate their behavior through the layer protocol and distributed algorithm, and nodes can quickly join the network after being started. When sensor nodes are in the work or in the sleep, they can complete state switch, and move position, and join a new node etc.

C. Large-scale network and high density nodes

In order to collect information completely, wireless sensor nodes are layout very densely. The node number is about tens of thousands. Because the sensor nodes often communicate in the way of radio, there will be a large number of redundant nodes. Redundant nodes and a large number of redundant information make the WSN with strong anti-destroying ability, high fault tolerance and high precision.

D. Little physical security guarantee of deployment area

The WSN sensors are usually deployed in the open area where no one keeps an eye on, so they are vulnerable to some physical or artificial damage. In addition, WSN with limited power supply, the wireless channel and distributed control technology will be attacked by the physical damage, depletion attack, active invasion, the black hole attack, flood attack, collision attack, being tampered, forgery attack etc.

E. Lack of relevant prior knowledge for subsequent nodes

In WSN we don't know with which one the subsequent nodes will communicate directly. So the key pre-distribution is aimless, the shared key ratio among nodes is much lower, so the safe connectivity ratio of WSN is little.

Due to almost all the key management schemes are improved with the representative E-G and q-composite key pre-distribution models, so in the paper, the author studies and analyzes their principle and safety, the analysis results can provide reference for the WSN key management algorithm in the process of design and optimization.

3. The E-G Key Pre-Distribution Scheme

A. Algorithm mechanism

The E-G key pre-distribution model [2] is firstly put forward by Eschenauer and Gligor, whose process is composed of three stages:

(1) Key pre-distribution phase: Before deployment, the server generates a key pool with G key and G key identification firstly, each node select $k(k << G)$ different keys from the key pool randomly, which can ensure that any two nodes have shared keys at a certain probability.

(2)The Shared key discovery phase: If two adjacent nodes deployed randomly exist shared keys, we can randomly select one as the their both shared key; Otherwise we enter the third stage;

(3)The establishing key route phase: Both two nodes can establish a key route through other neighbor nodes with shared key after several jumps.

B. Safety performance analysis

In the paper, the secure connectivity and node resistance to captive capacity are used as indicators for evaluating the security of WSN [7]. Security connectivity refers to the network connectivity based on safe routes. Safe routes are established among nodes with shared keys at first, if safe routes can connect all of the nodes into a network, we can consider the network as safe connectivity. Node resistance to captive capacity refers to the probability of no one shared key being threatened after attackers have captured one or more nodes.

(1) Secure connectivity

According to the classical random graph theory, if the shared key probability between any two sensor nodes is p', the relationship between the key pool size G and the storage key number k in each node is as following:

$$p' = 1 - \frac{((G-k)!)^2}{(G-2k)!G!} \tag{1}$$

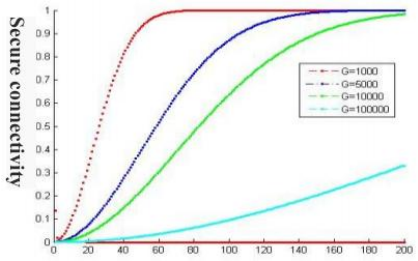

Fig.1 Network connectivity

When G is enough large, we can't calculate formula (1) by the computer. Based on Stirling approximation $n! \approx \sqrt{2\pi} n^{n+1/2} e^{-n}$, the formula (1) is changed as the formula:

$$p' = 1 - \frac{(1-k/G)^{2(G-k+0.5)}}{(1-2k/G)^{(G-2k+0.5)}} \tag{2}$$

Figure 1 shows the secure connectivity with different key pool size and the different storage key in each node. We can see from the curve, when key pool size is 1000, we can guarantee the shared key probability 0.9 between any two nodes, but each sensor node only stores about 50 key. When key pool size is10000, we can guarantee the shared key probability 0.5 between any two nodes, about 75 key need to be stored in each sensor node.

(2) Resistance to captive capacity

In the E-G random key pre-distribution scheme of WSN, the attackers can obtain k keys when capturing one node, the probability to threat other routes is k/G, when nodes are captured, the probability that no one key is threatened is $(1-k/G)^x$, the resistance to captive capacity is $(1-k/G)^x$. Figure 2 shows Resistance to captive capacity with the captured node number under the condition of different key pool size and the different storage keys in each node:

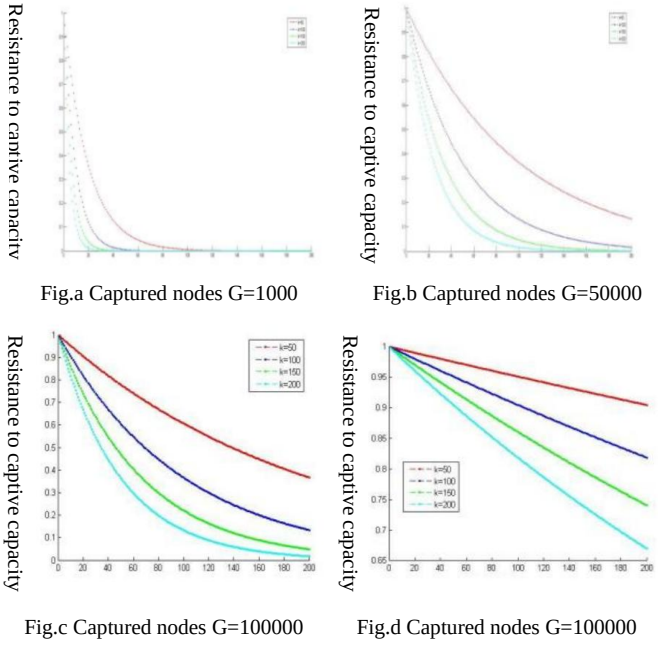

Fig.a Captured nodes G=1000 Fig.b Captured nodes G=50000

Fig.c Captured nodes G=100000 Fig.d Captured nodes G=100000

Fig.2 Resistance to captive capacity with different nodes and different storage keys

From figure 2, we can see that resistance to captive capacity increases gradually with the increase of key pool size and the same storage key number. For example, when G equals 1000, 1000, 10000, 100000 respectively, and $k = 50$, node resistance to captive capacity is 0.07, 0.69, 0.71 and 0.97 respectively. When the node scale is constant, resistance to captive capacity decreases gradually with the increase of node storage key. For example, when $G = 5000, x = 50$, and k equals 50, 100, 150 and 200 respectively, resistance to captive capacity is 0.59, 0.36, 0.14 and 0.23 respectively. So in order to guarantee the security of WSN, under the constant network scale, we should reduce node storage keys in each node as far as possible, so the attackers can get less information about other nodes when one node captured.

4. Q-Composite Key Pre-Distribution Scheme

A. Realizing mechanism

The q-Composite realizing mechanism [3] is the same as the E-G key pre-distribution model. But shared key between neighbor nodes is greater than k for the q-Composite key pre-distribution model. After receiving all the shared keys, if the shared key number between two nodes is more than q , if it is q' , then we make use of all of shared keys q' to generate a shared key K between two nodes, the result is $K = hash(k_1 \| k_2 \| \cdots \| k_{k'}$. Along with the increase of the value of q, the safety degree of q-Composite scheme increases exponentially, but to achieve ideal probability for safe connectivity among nodes, we must reduce the size of the key pool, increase the overlapping degree of shared keys between nodes.

B. Safety performance analysis

(1) Secure connectivity

If the probability of the Shared key with i between any two nodes is $p(i)$, we can select k key for any node from G keys:

$$p(i) = C\binom{G}{k}C\binom{G-i}{2(k-i)}C\binom{2(k-i)}{k-i} \tag{3}$$

When G is enough large, we can't calculate formula (3) by the computer. Based on Stirling approximation $n! \approx \sqrt{2\pi} n^{n+1/2} e^{-n}$, the formula (3) is changed as the formula :

$$p(i) = \frac{((G-k)!)^2 (k!)^2}{G!i!((k-i)!)^2 (G-2k+i)!} = \frac{(1-\frac{k}{G})^{2(G-k+1/2)}}{i!G^i k^{-2i} e^i (1-\frac{i}{k})^{2(k-i+1/2)} (1-\frac{2k}{G}+\frac{i}{G})^{(G-2k+i+1/2)}} \tag{4}$$

When there are at least q Shared keys between any two nodes, the probability of secure connectivity is:

$$p' = 1-(p(0)+p(1)+p(2)+...+p(q-1)) \tag{5}$$

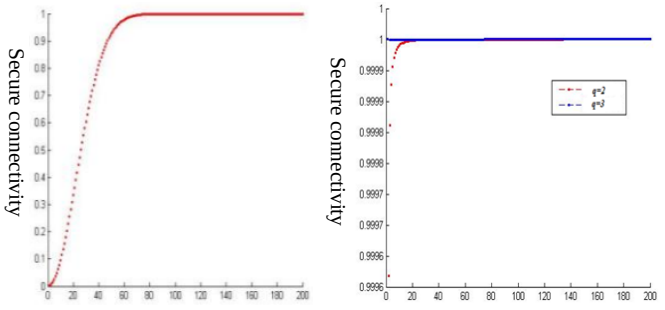

Fig. a Storage key Fig. b Storage key

Fig.3 Network connectivity

Figure 3 shows the secure connectivity when $G = 1000$ and one to three different keys are shared among sensor nodes. On the other side, we can see that the node storage keys decrease fast with the increase of shared key number. With two or three share keys, we can guarantee the shared key probability more than 0.99 between any two nodes with about 15 or so keys being stored in each sensor node.

(2) Resistance to captive capacity

In the q-Composite key pre-distribution scheme in WSN, when nodes are captured, the probability that no one key is threatened is $(1-k/G)^x$, the total probability that any key is threatened is $1-(1-k/G)^x$,when we use the Hash value of i shared keys to generate route key, the probability that no one key is threatened is $(1-(1-(1-k/G)^x)^i) \times p(i)/p$, among $p = p(q)+p(q+1)+p(q+2)+\cdots+p(k)$, the resistance ability to be captured is $\sum_{i=q}^{k}(1-(1-(1-k/G)^x)^i) \times p(i)/p$, Figure 4 shows the simulation results of resistance to captive capacity under various parameters:

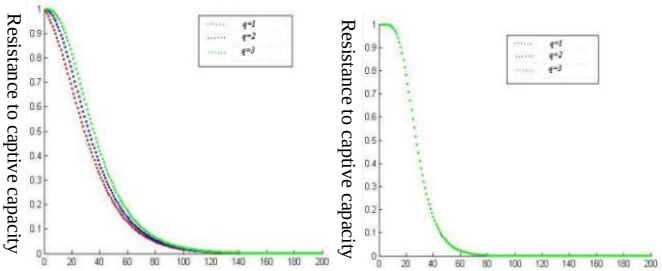

Fig.a G=1000, k=50 Fig.b G=1000, k=100

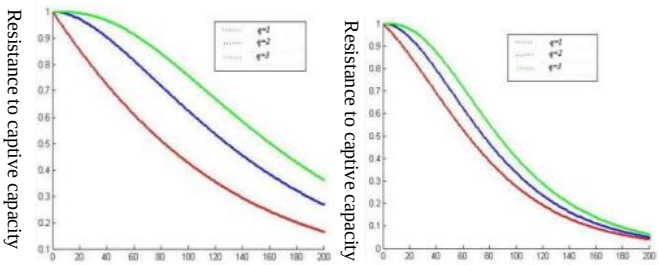

Fig. c G=5000, k=50 Fig. d G=5000, k=100

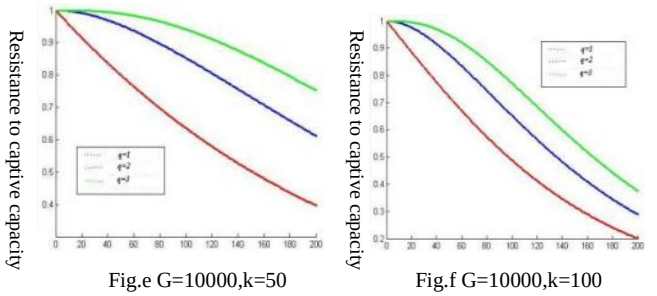

Fig.e G=10000,k=50 Fig.f G=10000,k=100

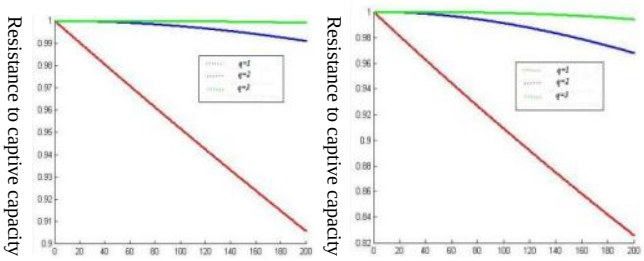

Fig.g G=100000, k=50 Fig.h G=100000, k=50

Fig.4 Resistance to captive capacity with different nodes and different storage keys

From the figure 4, we can see that resistance to captive capacity for q-Composite with more share key increases with the increase of key pool size and the same storage key number. For example, when $k=50, q=2$, and the captured number is 60,and G equals 1000, 1000, 10000, 100000 respectively, resistance to captive capacity is 0.18,0.78, 0.92 and 0.99. When G, k is the same for WSN, the more the number q is, the higher the resistance to captive capacity is. For example, when $G=5000, k=50$, the captured number is 60, the node resistance to captive capacity is 0.65，0.87 and 0.91 for $q=1,2,3$ respectively. The node resistance to captive capacity for $q=2,3$ q-Composite schemes is significantly higher than E-G scheme. In other words, the WSN with q-Composite scheme is safer than the E-G scheme. But we should see that the size of G must be small, so that the overlapping degree between shared keys increases and can ensure that the probability of safe connectivity is more than q. But when G size is too small, more shared keys will be cracked while attackers capture a few nodes.

5. Improvement Measures

Compared with the E-G key pre-distribution scheme, q-composite scheme enhances the security of WSN obviously. But when they have same shared keys, the nodes for q-composite scheme must store more keys than E-G scheme, which increases the possibility of leaking information for the captured nodes. To solve the problem, we can combine the q-composite scheme with polynomial method [4], thus can ensure the WSN security because the polynomial method can't disclose any information when the captured nodes aren't no more than t number. The second we can combine the E-G scheme with the multi-path key enhancement mechanism, j disjoint paths transmit j random value, the receiver generates a shared key by XOR operation on j random value. If an attacker can't get all of the j random value, he can't crack shared key. The third scheme is to establish a random key pre-distribution scheme based on the deployment information [6] when we know the specific geographic information of node deployment information, each node can generate shared key with random selection of the nodes closest to it. With binding shared key and location information, any captured node will not affect the safety of the other nodes. With the above measures we can effectively improve the E-G scheme and q-Composite scheme security.

6. Conclusions

For the security design of WSN, securing keys among sensor nodes is the foundation of the WSN security. In this paper, the author analyzes the performing mechanism and security characters for typical E-G and q-composite random key pre-distribution schemes, and studies the correlation between the key pool size, the node storage keys, and get the quantitative relationship that the resistance to captive capacity as to the captured node numbers, key pool size, and the storage keys in each node, and analyzes the deficiency of two random key pre-distribution schemes, and provides the improvement measures. The simulation results obtained in this paper can be used to optimize constrained WSN node computation, storage, and communication, and has very good guidance significance for designing safe WSN

References

[1] Sinopoli B, Sharp C. Distributed control application within sensor networks. Proceedings of the IEEE Signal Processing Magazine, 2003, 91(8):1235-1246.

[2] Eschenauer L, Gligor V. A Key Management Scheme for distributed sensor networks. Proceedings of 9th ACM Conference on Computer and Communication Security, Washington DC: ACM Press, 2002:41-47.

[3] Chan H W, Perring A, Song D. random key pre-distribution schemes for sensor networks. Pro 2003 IEEE Symp. on Security and Privacy, 2003:197-213.

[4] Blundo C, Santis D.A, Herzberg A, et al. perfectly secure key distribution for dynamic conferences. In Advances in Cryptology-CRYPTO'92, LNCS740, 1992, 471-486.

[5] Liu D, Ning P. Establishing Pair-wise keys in Distributed Sensor Networks. In Proceedings of the 10 the ACM Conference on Computer and Communication Security, 2003, 52-61.

[6] Blom R. An optimal class of symmetric key generation systems. In Proceedings of EUROCRYPT'84, Lecture Notes in Computer Science, 1984, 335-338.

[7] Shen Yulong, Pei Qingqi. Introduction to wireless sensor network security technology, Beijing: Post &Telecom Press, 2010.8.