A Hexagon-Based Key Predistribution Scheme in Sensor Networks

Guorui Li
College of Computer Science and Technology
Beijing University of Technology
Beijing 100022, China
liguorui@emails.bjut.edu.cn

Jingsha He
School of Software Engineering
Beijing University of Technology
Beijing 100022, China
jhe@bjut.edu.cn

Yingfang Fu
College of Computer Science and Technology
Beijing University of Technology
Beijing 100022, China
fmsik@emails.bjut.edu.cn

Abstract

Sensor networks are widely used in environment exploration and disaster recovery and in military applications due to their self-organization characteristics and distributed nature. As a fundamental requirement for providing security functionality in sensor networks, key management plays a central role in authentication and encryption. In this paper, we present a hexagon-based key predistribution scheme and show that it can improve the key management in sensor network through the use of the bivariate polynomial in a hexagonal coordinate system based on deployment information about expected locations of the sensor nodes. We show that the scheme presented here can improve the probability of establishing pairwise keys between sensor nodes of up to two hops apart by more than 40% over previous schemes.

Keywords and phrases: sensor networks, security, key distribution, hexagon.

1. Introduction

With the development of wireless and microelectronics technologies, it has become possible to deploy a large number of low-cost, high-performance and low-power sensor nodes in a wireless sensor network. These sensor nodes collect environment data such as temperature, humidity and pressure by embedded sensor component and transmit the data to data collectors through wireless links. The characteristics exhibited in a wireless sensor network, such as self-organization, self-healing, distribution and loose coupling, make wireless sensor network suitable for widespread applications in environment data collection, health monitoring and disaster recovering and in a variety of military applications.

Security plays a central role in wireless sensor networks. This is because the confidentiality, integrity and availability of the transmitted data between sensor nodes must be preserved in a hostile environment. As the basic requirement for providing security functionality, key management plays a central role in encryption and authentication. However, due to resource constraints in sensor nodes, many ordinary security mechanisms such as public key-based authentication and key distribution schemes are deemed unpractical, and sometimes infeasible in sensor network.

Eschenauer and Gligor proposed the basic probabilistic key predistribution scheme, in which each sensor node is assigned a random subset of keys from a key pool before the deployment of the network so that any two sensors will have a certain probability to share at least one key [1]. Chan et al. improved the scheme and developed the q-composite key predistribution scheme and the random pairwise key scheme [2]. The q-composite key predistribution scheme is based on the basic probabilistic key predistribution scheme, but it

requires that two sensor nodes share at least q predistributed keys as the basis to establish a pairwise key between the two nodes. In the random pairwise key scheme, random pairwise keys are predistributed between a specific sensor node and a random subset of other sensor nodes. Such a scheme has the property that security compromise to a sensor node doesn't lead to compromise to pairwise keys that are shared between uncompromised sensor nodes. Liu and Ning developed a framework in which pairwise keys are predistributed by using bivariate polynomials [3]. They also proposed two efficient instantiations, a random subset assignment scheme and a grid-based key predistribution scheme, to establish pairwise keys in sensor networks. They also proposed the closest pairwise key predistribution scheme and the closest polynomials predistribution scheme, which take advantage of sensor nodes' expected locations to predistribute appropriate keys to the sensor nodes and thus can improve the performance of key establishment [4]. Chan and Perrig developed PIKE, which facilitates pairwise key establishment using peer sensor nodes as trusted intermediaries [5]. However, all the schemes described above failed to take into account the information on deployment locations and signal propagation. Therefore, they lowered the probability of successful key establishment with an increase in the cost.

In this paper, we propose a hexagon-based key predistribution scheme in sensor networks in which we use the hexagon to simulate the signal propagation. We show that the proposed scheme can greatly improve the probability of successful key establishment by constructing a sensor cellar network to predistribute the key polynomials. The scheme also decreases the cost of pairwise key establishment.

The rest of the paper is organized as follows. In the next section, we introduce the polynomial-based key predistribution scheme. In Section 3, we describe the hexagon-based key predistribution scheme and analyze its performance and security. In Section 4, we mention some related work in sensor network security. Finally, in Section 5, we conclude this paper and discuss some future research directions.

2. The polynomial-based key predistribution scheme

To predistribute pairwise keys, the key distribution server first randomly generates a bivariate t-degree polynomial $f(x,y)=\sum_{i,j=0}^{t} a_{ij}x^i y^j$ over a finite field F_q, where q is a prime number that is large enough to accommodate a cryptographic key. Obviously, $f(x,y)$ exhibits the property of symmetry, i.e., $f(x,y)=f(y,x)$. We assume that each sensor node has a unique integer ID. Then, for each sensor node *i*, the setup server computes a polynomial share of $f(x,y)$, that is $f(i,y)$ and stores it in sensor node *i*. For any two sensor nodes *i* and *j*, node *i* can compute the pairwise key $f(i,j)$ by evaluating $f(i,y)$ at point *j* and node *j* can compute the pairwise key $f(j,i)$ by evaluating $f(j,y)$ at point *i*. From the property of symmetry of $f(x,y)$, $f(i,j)=f(j,i)$. So the pairwise key between nodes *i* and *j* can be established.

In this scheme, each sensor node needs to store a bivariate t-degree polynomial's coefficients, which would occupy $(t+1)log_2 q$ storage space. The security proof in [6] ensures that this scheme is unconditionally secure and t-collision resistant. That is, the coalition of no more than *t* compromised sensor nodes knows nothing about the pairwise keys between any two non-compromised sensor nodes.

3. The hexagon-based key predistribution scheme

3.1. The hexagonal coordinate system

A hexagonal coordinate system provides more benefits than a common rectangular coordinate system in wireless sensor networks. First, when a sensor node transmits data over wireless links, its signal range would form a circle that is centered around its deployment location with the radius being the distance of signal propagation. Therefore, a hexagon can be used to express and simulate the signal range more appropriately than a square can. Second, a hexagon can be used to describe equal distance between two neighboring sensor nodes. In a common rectangular coordinate system, the distance between neighboring sensor nodes differs, which depends on whether the neighboring node is located directly adjacent (in which case the distance is 1 unit) or diagonal (in which the distance is square root of 2 units) to it. Under the hexagonal coordinate system, all adjacent sensor nodes have that same distance which is normally 1 unit.

Without loss of generality, let's label the center of a hexagon 0 in the hexagonal coordinate system. Then all other points in the hexagon are located around hexagon 0 counter-clockwise as shown in Figure 1. According to the numbering rule, the numbers in the

nth circle of the hexagon should be from $\sum_{i=1}^{n-1} 6(i-1)+1$ to $\sum_{i=1}^{n} 6(i-1)$. Consequently, we can determine a hexagon's location and its adjacent hexagons in a hexagonal coordinate system based on the above numbering rule.

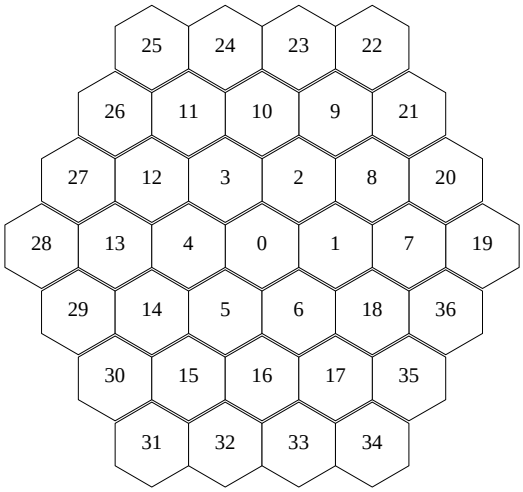

Figure 1. The hexagonal coordinate system

3.2. The scheme

In the hexagon-based scheme, key predistribution is carried out in three phases: predistribution, direct key establishment and path key establishment. The predistribution phase is performed in order to initialize the sensor nodes by distributing bivariate polynomial subset built by key setup server according to the expected locations of the sensor nodes. After deployment, two sensor nodes can successfully establish a direct key between them if they share the same bivariate polynomial. Otherwise, the two sensor nodes should establish path key with the help of other intermediate nodes.

(1) The predistribution phase

A key setup server would partition the target deployment field into m equal sized hexagons according to the hexagonal coordinate system. Then, it builds m different bivariate t-degree polynomials over a finite field F_q and assigns these polynomials to hexagonal coordinate system randomly in order to make sure that each hexagon has a unique bivariate polynomial. For convenience, the key setup server assigns a unique ID to each polynomial.

For each sensor node *i*, the key setup server first determines its home hexagon H_i where the sensor node is expected to locate and discover that six hexagons $\{H_{ij} \mid j=1,...,6\}$ that are adjacent to the sensor node's home hexagon. Then it computes $P_i(ID_i, y)$ and $\{P_{ij}(ID_i, y) \mid j=1,...,6\}$ by evaluating hexagon H_i and $\{H_{ij} \mid j=1,...,6\}$'s corresponding polynomial P_i and $\{P_{ij} \mid j=1,...,6\}$ at sensor node *i*'s ID ID_i. Finally, the key setup server assigns $P_i(ID_i, y)$, $\{P_{ij}(ID_i, y) \mid j=1,...,6\}$ and their corresponding IDs to sensor node *i* and store them into the node in order to build the pairwise keys.

(2) The direct key establishment phase

After deployment, if two sensor nodes want to establish a pairwise key, they first need to identify a shared bivariate polynomial. If they can find out at least one such polynomial, a common pairwise key can be established directly using the polynomial-based key establishment scheme presented in Section 2. In order to find out whether the two sensor nodes hold the shared polynomial, they should exchange their polynomials' IDs. To protect information associated with their polynomials' IDs, the sensor nodes may challenge each other to solve puzzles. Sensor node *i* broadcasts an encryption list, α, $E_{ID_1}(\alpha)$, $E_{ID_2}(\alpha)$, …, $E_{ID_7}(\alpha)$ where $ID_i, i=1,...,7$ is the ID of the polynomials that sensor node *i* holds. If the other sensor node can correctly decrypts one of the $E_{ID_i}(\alpha)$ using one of its own polynomial ID_i, then they share the same polynomial ID_i and can proceed to establish a direct pairwise key using this shared polynomial.

(3) The path key establishment phase

If direct key establishment failed, the two sensor nodes can establish pairwise key in the path key establishment phase. When a source sensor node broadcasts the ID of a destination sensor node, an intermediate sensor node can establish a path key for the two sensor nodes if it holds the pairwise keys with the source and the destination sensor nodes, respectively. Otherwise, the intermediate sensor node would broadcast this message continuously until it discovers a sensor node that shares a pairwise key with the previous sensor node and the destination sensor node respectively. Then the path key can be established along the message broadcast path reversely.

From hexagonal coordinate system we can see

that a sensor node can be an intermediate node in the path key establishment if it is on the path between the source and the destination sensor nodes. We can also see that the path between the source and the destination sensor nodes isn't necessarily unique, which would provide a certain degree of resilience for path key establishment when some intermediate sensor nodes were compromised or damaged. Sometimes we can restrict the length of a path in order to avoid the broadcast storm.

3.3. Analysis

(1) The probability of direct key establishment

Similar to the analysis in [4], the probability of direct key establishment for any sensor node u in the hexagon-based key predistribution scheme is:

$$p_u = \frac{n_u^s}{n_u} = \frac{\sum_{C_j \in S_i} p(C_j, C_i)}{\sum_{\forall j} p(C_j, C_i)}$$

where n_u^s is the average number of sensor nodes that can establish a pairwise key with u directly, n_u is the average number of sensor nodes that u can directly communicate with, and S_i is the set of hexagons of the sensor nodes that share at least one common polynomial with sensor node u.

In the hexagon-based key predistribution scheme, each sensor node takes its deployment hexagon as the center and can share polynomials with sensor nodes deployed in its 19 adjacent hexagons. For example, in Figure 2, all sensor nodes deployed in shaded hexagons can share common polynomial with the sensor node deployed in hexagon 0. Let's assume that the sensor deployment density in hexagon is ϖ and signal propagation distance is d_r, then the probability of direct key establishment in the hexagon-based key predistribution scheme is:

$$p_u = \frac{n_u^s}{n_u} = \frac{19 \cdot \varpi \cdot \frac{3\sqrt{3}}{2} \cdot R^2}{\pi \cdot d_r^2 \cdot \varpi} = \frac{57\sqrt{3}R^2}{2\pi d_r^2}$$

where R is the diameter of the hexagon.

In contrast, the probability of direct key establishment in closest polynomial key predistribution scheme described in [4] is:

$$p_u^{'} = \frac{n_u^s}{n_u} = \frac{13 \cdot \varpi \cdot L^2}{\pi \cdot d_r^2 \cdot \varpi} = \frac{13L^2}{\pi d_r^2}$$

where L is the side length of a square in a common rectangular coordinate system. Each sensor node can only communicate with the sensor nodes deployed in 13 adjacent squares in the common rectangular

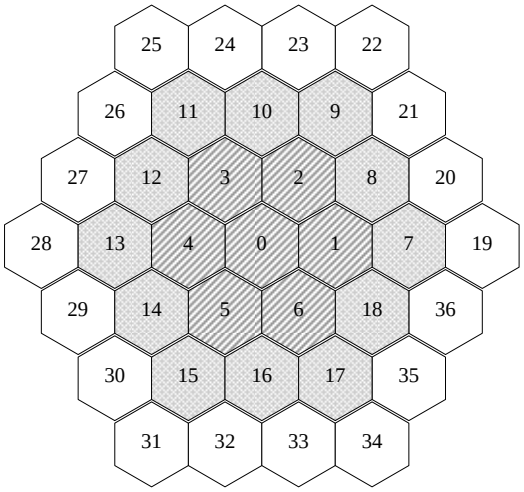

Figure 2. The adjacent hexagons in a hexagon-based predistribution scheme

coordinate system. As shown in Figure 3, only the sensor node deployed in 13 shaded squares can establish direct pairwise keys with the sensor node u deployed in $C_{2,2}$.

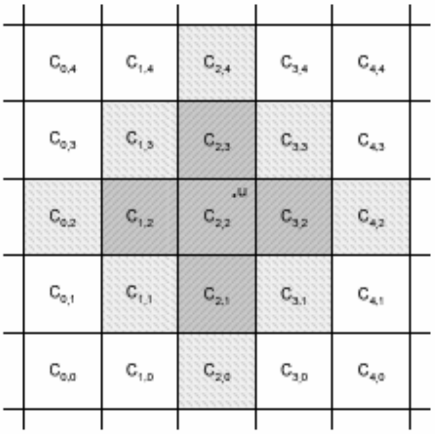

Figure 3. The adjacent squares in a closest polynomial predistribution scheme

To simplify our analysis, we assume that the signal propagation distance in both of these schemes is the minimal distance between a sensor node and those that are within the signal range of the sensor node that can establish a direct pairwise key with the sensor node. Consequently, in the hexagon-based key predistribution scheme, $d_r = 3\sqrt{3}R$ whereas, in the closest polynomial predistribution scheme, $d_r = \sqrt{10}L$. Therefore, the ratio between the probabilities of the two direct key establishment

schemes is:

$$\frac{p_u}{p_u'} = \frac{57\sqrt{3}}{26} \cdot (\frac{R}{L})^2 = \frac{57\sqrt{3}}{26} \cdot (\frac{\sqrt{10}}{3\sqrt{3}})^2 \approx 1.406 .$$

That is, the probability of direct key establishment in the hexagon-based key predistribution scheme is approximately 40% higher than that in the closest polynomial predistribution scheme presented in [4].

(2) The probability of path key establishment

To simplify our analysis, we only discuss the probability of path key establishment between two sensor nodes of two hops away in which it requires only one intermediate node to help establish the path key between the source and the destination sensor nodes. Similar to the analysis above, each sensor node can establish two-hop path key with sensor nodes deployed in its 61 adjacent hexagons in the hexagon-based key predistribution scheme and 41 adjacent squares in the closest polynomial predistribution scheme. So the ratio between the probabilities of two-hop path key establishment based on the two direct key establishment scheme is:

$$\frac{p_u}{p_u'} = \frac{\frac{3\sqrt{3}}{2} R^2 \cdot 61}{41 \cdot L^2} = \frac{183\sqrt{3}}{82} \cdot (\frac{\sqrt{10}}{3\sqrt{3}})^2 \approx 1.432 .$$

That is, the probability of establishing a two-hop path key in the hexagon-based key predistribution scheme is approximately 43% higher than that in the closest polynomial predistribution scheme presented in [4].

3.4. Security analysis

According to the result of the polynomial-based key predistribution scheme, unless more than t polynomial shares of a bivariate polynomial are disclosed, an attacker would not know about the non-compromised pairwise keys established using this polynomial. Thus, the security of the hexagon-based key predistribution scheme depends on the average number of sensor nodes that share the same polynomial. Assume that there are m nodes on average in the signal range of each sensor node, the density of the sensor node deployment can be estimated by $\varpi = \frac{m}{\pi d_r^2}$. Thus, the number of sensor nodes that shares at least one common polynomial in the hexagon-based key predistribution scheme is:

$$N_s = \frac{m}{\pi d_r^2} \cdot \frac{3\sqrt{3}}{2} R^2 \cdot 7 = \frac{21\sqrt{3} m R^2}{2\pi d_r^2} .$$

As long as $N_s \le t$, our scheme is compromise-resistant.

We assume that a fraction p_c of sensor nodes in the network have been compromised. Thus, among N_s sensor nodes that hold the same polynomial shares, the probability that i sensors has been compromised can be estimated to be $P_c(i) = \frac{N_s!}{(N_s - i)! i!} p_c^i (1 - p_c)^{N_s - i}$. Thus, the probability that the bivariate polynomial is compromised is $P_c = 1 - \sum_{i=0}^{t} P_c(i)$. For any pairwise key established between non-compromised sensor nodes, the probability that it is compromised is the same as P_c.

4. Related work

Nowadays, there are many studies in sensor network security, which are mostly on key management, authentication, and vulnerability analysis. Other than the key predistribution scheme presented in [1-6], Perrig et al. developed a security architecture for sensor networks, which includes SNEP, a security primitive building block, and a broadcast authentication technique μTESLA [7]. Liu and Ning extended this technique to a multilevel key chain method to prolong the time period covered by a μTESLA instance [8]. Wood and Stankovic identified a number of DoS attacks in sensor networks [9]. Karlof and Wagner analyzed the vulnerabilities as well as the countermeasures for a number of existing routing protocols [10].

5. Conclusion and future work

In this paper, we presented a hexagon-based key predistribution scheme in which we take advantage of the knowledge regarding sensor nodes' expected deployment locations and establish pairwise keys between the sensor nodes by using the bivariate t-degree polynomial in a hexagonal coordinate system. We showed that the scheme could increase the probability of direct key establishment and that of 2-hop path key establishment by over 40%. Our future work would focus on the development of methods and schemes that can be used to adjust the polynomial distribution by taking into consideration the difference between expected deployment locations and actual

deployment locations of the sensor nodes.

References

[1] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in *Proc. 9th ACM Conference on Computer and Communications Security*, November 2002, pp. 41-47.

[2] H. Chan, A. Perring, and D. Song, “Random key predistribution schemes for sensor networks,” in *Proc. IEEE Symposium on Research in Security and Privacy*, 2003.

[3] D. Liu and P. Ning, “Establishing pairwise keys in distributed sensor networks,” in *Proc. 10th ACM Conference on Computer and Communications Security*, October 2003, pp. 52-61.

[4] D. Liu and P. Ning, “Location-based pairwise key establishments for static sensor networks,” in *Proc. 2003 ACM Workshop on Security in Ad Hoc and Sensor Networks*, 2003, pp. 72-82.

[5] H. Chan and A. Perrig, “PIKE: Peer intermediaries for key establishment in sensor networks,” in *Proc. IEEE Infocom*, 2005.

[6] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, “Perfectly secure key distribution for dynamic conferences,” in *Advances in Cryptology - CRYPTO’92. Lecture notes in Computer Science*, Vol. 740, Springer-Verlog, New York， 1992, pp. 471-486.

[7] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, “Spins: Security protocols for sensor networks,” in *Proc. 7th Annual International Conference on Mobile Computing and Networks*, July 2001.

[8] D. Liu and P. Ning, “Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks,” in *Proc. 10th Annual Network and Distributed System Security Symposium*, February 2003, pp. 263-276.

[9] D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” in *IEEE Computer*, Vol. 35, No. 10, October 2002, pp. 54-62.

[10] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” in *1st IEEE International Workshop on Sensor Network Protocols and Applications*, May 2003.