A novel based-node level Security strategy in wireless sensor network

Zheng Yue-Feng
BoDa College of Jilin Normal University
Si ping ,China
Email: bdxy1627@163.com

Han Jia-Yu
College of Computer Science and Technology, Jilin University
Key Laboratory of SymComputation and Knowledge Engineering, Ministry of Education, Jilin University,
Chang Chun, China
Email: hanjy0821@mails.jlu.edu.cn

Chen Zhuo-Ran
BoDa College of Jilin Normal University
Si Ping ,China
Email:czr_czr@126.com

Li Zheng (Corresponding author)
Computer Department of Jilin Normal University
BoDa College of Jilin Normal University
Si Ping ,China
Email:lst783@126.com

***Abstract*—In Wireless Sensor Networks,Security is very important, especially in the networks which require high security. This paper raises a method to establish key distribution scheme, based on node layer security system, which combines with the group key distribution and identification of encryption. This method can make the two nodes carry on communication in a secure environment when identified, at the same time, communication in the safe environment between groups can also be guaranteed. The results show that the ability of resistance to attack, Sybil attack, node increases the attack, the node replication attacks can effectively be stopped. At the same time, further illustrates that the adoption of this security strategy for wireless sensor network security enhancement.Simulation results show that, the structure of security system we proposed is safe and feasible.**

Key words- WSNs; network security; cryptography

I. INTRODUCTION

Wireless Sensor Networks (WSNs) in the military, environmental monitoring, earthquake and climate prediction, the exploration of deepwater, underground and outer space, and many other aspects has a wide range of application prospects [1]. However, its security is also facing the huge challenge, especially in the field which requires high security [2] [3]. To prevent eavesdropping and attack, there are many security schemes which are using point to point communication have been proposed [4]. However, due to node's computing ability, communication ability, storage ability and other aspects limited, the node cannot rely on itself to decide the security algorithm, and should rely on the security key-pair and intelligent routing to transmit information safely.

This paper introduces the risk and trust mechanism; ensure that the system can make a crucial decision during sharing information between nodes.

II. THE EXISTING SECURITY ALGORITHM ANALYSIS

In recent years, the methods of key-establishment in Wireless Sensor Network have been studied extensively. The simplest way is that we preset the same key in every node, and use this key to communicate between each pair of nodes [4]. However, this approach has a fatal flaw. Once a node has been captured, the network is in a state of paralysis. A relatively simple solution is to set the same key between the node and other nodes which might communicate with the node. Then, if a node has been captured, it will not affect the other nodes' security in the network. But, with the expansion of network scale, because of the node's storage capacity is limited, this method is not suitable for Wireless Sensor Networks.

Multiple methods have been proposed which based on the plans which mentioned above. Like the methods based on group [5] or based on the location [6], these methods are prominent especially in the large-scale network. However, these programs are using the technology of symmetric key encryption, ignoring the asymmetric key usage. It is generally believed that, limited in computing ability leads to that the asymmetric key cannot be applied to Wireless Sensor Networks. At the earliest, Neal Koblitz and Victor Miller are separately proposed the idea that elliptic curve can be applied to cryptography [7]. It has some characteristics like high security, small key size, and good flexibility, and it received widespread international attention. It can be proved that, the key establishment and key management schemes which are based on the elliptic curve encryption scheme are feasible.

At present, establishing the security key is widely used, which is guaranteed by encryption algorithm based on the

978-1-4673-1931-7/12/$31.00 ©2012 IEEE

identification. IBC [8] (identity based cryptography) is first presented by Shamir, it is similar to the traditional public key encryption algorithm, but it added the random public key generator. It can be guaranteed that the unique string or other short code can be considered as the public key. IBC perfectly solved a problem about storage space which is occupied by the key information during its establishing process is a very good solution to establish the key information in the process of storage space, a 16 bit address can be stored in 216=65536ID.

III. THE SECURITY ARCHITECTURE BASED ON THE NODE LAYER

Based on the analysis above, this paper uses node distribution which is based on group, after distribution, the node in group is fixed relatively. Each node in the group preset unique key information.

A definition of model

The finite field arithmetic is the basis of the Elliptic Curve Arithmetic [9]; the domain is composed of a set and some operational component which is defined on the set. If the set F is a finite set, then we call the domain as finite domain. The number of element in finite field is called the order of the limited domain.

Definition 1.1

P is a prime, there is a finite field F if and only if q = Pm, where p is called the features of domain F, m is a positive integer.

The domain F is called the prime field when it meets M=1;

The domain F is called the extension field when it meets M>=2; If q satisfies the requirements and q has already been identified, then only a q order finite domain is existed. We use Fq to represent the q order finite domain.

Definition 1.2

Assume P is a prime number, and t is an arbitrary integer, t mod p represents the remainder w of t divide p (0 ≤ w≤ P), the set, which is consisted by the entire W, is denoted as Fp.

Definition 1.3

E Fp denoted by Elliptic Curve y2=x3+ax+b(mod p), p is a prime here, a and b are two non-negative integer which is smaller than p and satisfied by 4a3+27b2(mod p)≠0, moreover, x,y,a,b ∈Fp, then the point(x,y), which meet this formula, and a infinite point O consist the Elliptic Curve E.

In this paper, the G1, G2 represent the order q subgroup in the range of Elliptic Curve E, ê is G1 x G1→G2, H is a hash function and an encryption function in G1, h is a hash function and a public encryption function, A and B are the Node group, x and y are Individual nodes, IDA is the value ID of GA, IDx is the value of ID of node x, Kx:A is the key which is used by the communication between GA and node x,Kxy is the shared key which is used by the communication between node x and node y, and mA is the master key of GA.

Elliptic curve discrete logarithm problem ECDLP is defined as follows: give prime P and elliptic curve E, for Q=kP, determine all the positive K which is smaller than P in the situation that P, Q is known. Thus it can be proved that it is rather easy to calculate Q if known K and P, and it is a little difficult to calculate K if known Q and P, and until now no effective method to solve this problem, so the encryption algorithm of elliptic curve owns a high security. Nodes P, Q in the E (P, Q) elliptic curve constitute a node pair with some nodes. Usually P, Q linear independent, otherwise, e linear independence, and E (P, Q) =1.

B elliptic curve algorithm (ECC) comparison with RSA algorithm

Elliptic curve public key system is a strong competitor to replace RSA. Compared with RSA, Elliptic curve encryption method has the following advantages:

(1) Higher safety performance, such as the ECC with 160 bits and the RSA, DSA with 1024 bits has the same security strength;

(2)Small amount of calculation, fast processing speed, ECC is faster than RSA or DSA at the speed of processing the private key (encryption and signature).

(3)Small storage space, the key size and system parameters of ECC are smaller than RSA and DSA, so the occupied storage space is much smaller, which is suitable for using in wireless sensor;

(4)The low requirements of bandwidth, which makes ECC, have extensive application prospects.

These characteristics of ECC make it replace the RSA and become the public key encryption algorithm which is generally used. For example, the designers of SET protocol have put it as the default public-key cryptography of the next generation of SET protocol.

TABLE 1 THE COMPARISON OF ECC AND RSA/DSA AT SECURITY INTENSITY

The time to Crack (MIPS year)	RSA/DSA Key size	ECC Key size	RSA/ECC Key size ratio
104	*512*	*106*	*5：1*
108	*768*	*132*	*6：1*
1011	*1024*	*160*	*7：1*
1020	*2048*	*210*	*10：1*
1078	*21000*	*600*	*35：1*

C The key establishing based on group

Set node artificially or automatically in some scene, or know the key nodes of fixed position [5]. In this paper, assume that the nodes cannot be moved after distribution, and don't need to add extra positioning equipment, the key information used by each group is unique. So, the node containing the Ga key information can set up couple keys with the nodes within the Ga node, and transport the information securely.

1) Authorization keys and node key initialization

Each group of all nodes preset an independent license key; every main authorization keys can generate key information for each authorization key (p, E/Fp, G1, G2, E). Following a group of nodes distribution, authorization node random selects ma as the safe key of the Ga.

In this stage, assuming that each group has its own unique identity value Ida and each node in the group has a unique identity value-IDx. Authorization node can provide each node which is in the group a unique key Kx: A based on its identity (Kx: A = maH (IDx)). Each node in the group except Kx: A, still be preset the basic information (p, E/Fp, G1, G2, ê, H, h, IDA). Because of the complexity of the elliptic curve discrete algorithm, the captured node will not get the group key mA. Here is the reason: E is a elliptic curve defined in the Fp, P ∈ E (Fq). Q is also a node in elliptic curve, it is difficult to find an integer d (0 < = d < = n), making the Q = dP. That is to say, because of Kx:A = maH (IDx),and with Kx:A and IDx are known to us, it is difficult to find a ma.

Random selected a node x in Ga preset an adjacent group Gb corresponding key Kx: AB, Kx: AB = mambH (IDx). The number of preset the keys which correspond the adjacent group among the node is relevant to network scale, if the network layer is i, then among the nodes, the number of preset keys which correspond the adjacent group is 2i + 2. See chart 1-1.

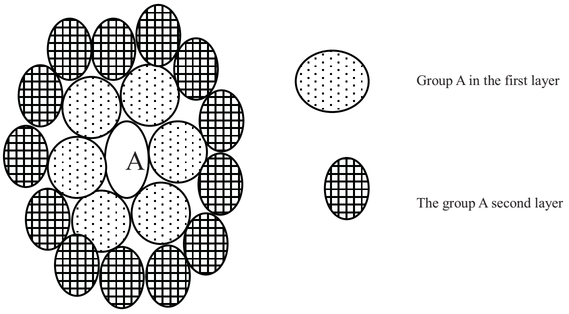

Figure 1-1sensor network layer

2) for key establishing

Key pair between adjacent nodes is divided into two ways to establish: first, establishing key pair in the same group: the nodes of establishing key pair are in the same group; Second, establishing key pair between groups, the nodes of establishing key pair are in the different groups. Key pair ê (P, Q) needs to preset the private key information Kx:A in the source node. Public key information IDy has been preset in destination node. Because of the symmetry of key pair, the private key pair information Kx:A of the destination node and the public key information IDx of the source node will produce the same results.

Establishing key pair in the group: node x broadcasts its identity value IDx, group identity value IDA and random variables nx, and waits for the response of neighbor node in a certain range. After receiving the broadcast, node y first discriminate that whether node x and node y are in the same group. If they are in the same group, node y broadcast its identity IDy value and random variables ny. Calculate and check public key values. Because of the communications are in the group, so the group identity values are the same, there is no need to return values. For node x, through the public key to calculate the information between two nodes whether matched. Through verification, node y can establish key pair with node x.

Establishing key pair between groups: Be similar to establishing key pair in the group, node x broadcasts its identity value IDx, group identity value IDA and random variables nx. After the node y from another group (GB) received IDA, node y known that node x is in the different group, then node y detect that whether there is a key Ky:BA corresponding with group A. If there is anyone, return IDy, IDB, ny and a validation public key. After receiving the return value, node x detects whether there is a key Kx:AB corresponding with group B. If there is anyone, return the corresponding validation information. Then node x and node y establish a key pair between groups.

IV. Security strategy

Current safety algorithm was mostly focused on the data link layer, the transport layer, the application layer on the way through encrypted data to ensure the security of the network. This paper used the simple, suitable for wireless sensor network security strategy to ensure the security.

A illustrates

This paper puts forward the security strategy which is divided into the following several parts: node, components, connections, transmission. Two nodes establish a safe passage through a connection, and the process of connection through transmission to realize, the nature of the each components using properties to indicate.

1)Node and components

Node has two attributes: their own identity and groups' identity. Own identity value can determine the only one node when in the establishment of the key process, while group identity value can only determine a group. Node is represented by lowercase letters, group identity is represented by subscript value, xA represents a certain node in groups. Component is some of components which are used for processing information by a sensor node. Such as: internal clock, motion sensor, thermometer, etc. Components is represented by uppercase letters and a number, xAT1 represents thermometer T1 in node x of group A.

2) Connection

A pair of node has multiple connection lines through different ways, this paper use direction and trust to describe the connection. Direction that describes the connection is divided into symmetrical connections and non-symmetric connection, symmetrical connection nodes can be said to two direction transmission, which can make the sender and also can be the receiver; Asymmetric connection said that the direction of transmission is unique; a node only can be as the sender or recipient. Trust represents the credibility when a node completes the transmission not be captured. In this paper, we use the arrow with pointing to represent the direction, and use uppercase letters with a superscript to represent trust.

3) Transmission

Transmission is described by brisk index which is a number between 0 and 1, the higher index the more important the information is. Use alpha, beta, gamma. with a superscript to display risk index. Risk index has been set up in the early network distribution, but as the network changes and security policy changes, the risk index may change.

After the above instructions, we can make the following definition: node x in group A, and node y in group B carry out α transmission, risk index is 0.2, and with J type way which trust is 0.4 to transmit.

B application strategy

This paper of security strategy on the intrusion detection effects obviously, suppose an intrusion detection systems contain several detection mobile node, the node distributes in different area. If a node detects the mobile, it sends out a warning signal, and identifies mobile happened area, and transfers it to the base station. Each area has a base station. Nodes can communicate with nodes which are in the adjacent area directly, and communicate with nodes which are not in the neighboring area indirectly.

The base station in the areas can provide security strategy, all the nodes in area form a group, and the components of nodes include a clock (C1) and a mobile detector (M1). The base station contains a clock and mobile testing receiver R1. Transmission includes two operations; one is α0.2 which is synchronization time with low risk, and the other one is β0.5 which is intrusion detection with the high risk. The way of connection between node and base station in group is the same as the way of connection between nodes, both of them use symmetry connection. Without loss of generality, we do not set trust series between the groups firstly, unified regulation of 0.4. This means that if the distance between the group is 1, then BT (A, B) = 1, the risk factors we allowed is 0.41 = 0.4; When BT (A, B) = 2, the biggest risk factor is 0.42 = 0.16.

Intrusion detection is a high risk transmission, intrusion notice is more important than gaining energy efficient routing, because before test, we can't know that whether a node is captured in the next group. Node A connects base station Za through transmission J, such as the trust level is 2.0, transmission risk is 0.5, and therefore transmission is feasible. At the same time, transmission is asymmetrical, so the node does not need to receive any introduction information from transmission.

The attacker often captures a certain node between adjacent groups to bypass the intrusion detection. For example, attackers captured node m which is closer to node x, use node m to intercept intrusion detection information from node x. The m in group B is legal node, x will establish the connection after carrying on the certification, but t (A, B) = (Fx) BT (A, B) =0.4. Because of the transmission needs that trust level is greater than or equal to 0.5, so the system do not establish a connection, the attack fails.

V. RESISTANCE TO ATTACK.

In Wireless Sensor Networks, the typical attacks conclude Sybil attack, node increases the attack, and the node replication attacks, the scheme proposed in this paper can prevent these attacks.

A Sybil attack

Sybil attack is an attack nodes camouflage multiple legal identities in a site, using such legal identity and the nodes in network to communicate. Compared with the node replication attacks, Sybil attacks do not produce multiple intrusion nodes, and a certain attack node generates a plurality of legal identity. The scheme we proposed can effectively prevent the attack of Sybil, because the attack nodes don’t have the information that key generate key pair, so they can’t establish key pair, thus they can’t communicate with the legal node within the network normally.

B node increasing attack

Node increasing attack differs from the node replication attacks, it is not a copy node, but adds a unique node. In order to establish key pairs, attack node must occupy the key information, such as the main key (mA). The existing methods generally allow that the master key in the independent nodes exists in a short period of time, but the plan in this paper does not allow the master key existing in the node. No master key, the attacker may have partial key information (such as IDA, IDx, Kx:A etc.). Even they get IDx and Kx:A, they can’t derive the mA shows by the property of the key pair .

C node replication attacks

Node replication attacks refer to attacking nodes capture one or a plurality of existing nodes, copy (or modify) node information to the illegal nodes, and put the illegal nodes into the network. The simple method is difficult to detect the node replication attacks, especially the nodes are in the distant distribution, and attacking node will intercept the transmission data, effect routing, and even affect the trust mechanism based reputation. This project will eliminate the node replication attacks. If node X in group A were captured, replication node, X’, if the group where the node X’ in and group A were not shared key, then, X’ can’t establish the key pair with other nodes in the group. In order to establish the key pair, attack nodes have no choice but to put the X’ into the group which share the key with group A, but the possibility of doing this is very small in a large scale network, Moreover, the node which communicate with the node X will receive the request for communicating. When the two nodes exist with the same identity, the two nodes will be further authentication, after this, the system find the illegal node X’, the node replication attacks failed.

REFERENCE

[1] Akyildiz F, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor network: A survey. Computer Networks, 2002, 38(4): 393−422.

[2] Carman DW, Kruus PS, Matt BJ. Constraints and approaches for distributed sensor security. Technical Report, #00-010, NAI Laboratories, 2000.

[3] Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks. Communications of the ACM (Special Issue on Wireless Sensor Networks), 2004,47(6):53.57.

[4] Wa Fubao, Shi Long, Ren Fengyuan. Self-Localization Systems and Algorithms for Wireless Sensor Networks. Journal of software , 2005,16(5): 857-868.

[5] Su Zhong, Lin Chuang, Feng Fujun, Ren Fengyuan. Key Management Schemes and Protocols for Wireless Sensor Networks. Journal of software, 2007,18(5):1218-1231.

[6] Wang Wei, Li Ping, Han Bo. Research on Routing Protocol of Wireless Sensor Networks. Industrial Control Computer,2005,18(1):26-27.

[7] Gu Yonghao, Liu Yong. Fast Algorithm of elliptic curve parameters generated. 20th National Computer Security Academic Exchange memoir, 2005-08

[8] Zhang YC, Liu W, Lou WJ, Fang YG. Location-Based compromise-tolerant security mechanisms for wireless sensor networks. IEEE Journal on Selected Areas in Communications, 2006,24(2):247-260.

[9] A. Cilardo, L. Coppolino, N. Mazzocca. Elliptic Curve CryptographyEngineering. Proceeding of the IEEE. 2006, 94(2):395~401

[10] Zhang Nan, Zhang JianHua, Wu Bing, Chen Jianying, Fu Chunchang. Based on elliptic curve cryptography digital signature. Journal of Southwest University for Nationalities (Natural Science Edition). 2007, 33(1):166-168.

[11]The Education Department of Jilin province science and technology research projects and funding (2012397)