A Lightweight and Security Key Management for WSN

XIE Bin
China Academy of Engineering Physics
Institute of Computer Application
Mianyang, China
ideaxb@caep.cn

ZHANG Li*, JIN Yuquan, HUANG Dan
China Academy of Engineering Physics
Institute of Computer Application
Mianyang, China
zhangli1009120@caep.cn

***Abstract*—Sophisticated key management schemes and protocols, whose main objective is to provide secure and reliable communication. But the design of it meets some challenges in wireless sensor networks, whose intrinsic properties make it difficult. In this paper, a lightweight and high security key management based on ECC and ElGamal was proposed. In the scheme，the key pool is structured by the Hamilton algorithm ,in which a layer network model is given，each lay has a servicer and control center, and session key was generated by ElGamal key agreement. The performance and simulation analysis shows, this scheme was superior to the traditional key pre-distribution schemes, not only computation cost and communication cost could be decreased, but good network connectivity，suitable for wireless sensor networks.**

***Keywords*：wireless sensor networks; communication protocol; Hamilton algorithm; key management ; security**

I. INTRODUCTION

Wireless sensor network (WSN) is a kind of typical distributed mobile network. Its resource is limited, the node energy, computing power and storage capacity are small. The traditional key management scheme is not suitable for WSN. Therefore, it needs to find a safety and efficient key management scheme to meet the requirements of WSN.

In recent years, commonly used key management schemes adopt public key cryptography for node identification, and the communication use of symmetric cryptography. In these schemes, the security of the key distribution process and identity authentication process is ensured by the public key cryptosystem, while the security of the communication is completed by the symmetric cryptography. These schemes depend on the storage capacity and computing power of the nodes. So this limits the size of the network.

The contents of this paper are as follows: second. The research work of this paper is described. The third section describes the key management scheme based on ECC. The network is divided into 3 layers, each layer follows different communication protocols, each node holds its own private key and identity information. The key distribution mechanism is used to realize the key distribution. The fourth section gives a comparison of the resource consumption and the scheme of the relevant documents, analyzes the connectivity of the network, the security analysis of the key agreement protocol is carried out. The fifth section gives the conclusion.

II. RELATION WORK

The research about the key management method in WSN mainly focuses on two aspects: one is pre distribution method for symmetric key, the other is management method based on public key. The former contains two types, one is based on the primary key and the other is based on the key pair. All nodes in the system based on the master key are assigned a key before deployment. When any two nodes want to communicate,

Funding support by Laboratory of Network Security and trusted software CAEP *2012A0403021,J-2014-ZD-03.*

they use the master key to calculate the session key which is used to guarantee the security of communication. Assuming that the system based on the key pair contains N nodes, each node in the system needs to save N-1 key pairs. Resource requirements increase with the expansion of the network. In this case, the application of this kind of key management method becomes worse and worse. In order to balance the security and the storage capacity, scholars have given a number of solutions, such as the random key pre distribution method[1,2], the polynomial key pre distribution method[3]and the key pre distribution method based on network deployment knowledge[4].

The random key pre distribution method was first used in WSN networks by Eschenauer and Gligor. This method consists of three phases. Phase I: Key pre distribution process. Before deployment, the server first generates P keys which are stored in a key pool and generates a unique identifier for each key. Then Each node randomly selects k keys from the key pool, where k<<P.

Phase II: Shared key discovery process. After the deployment of the system, if there are some shared keys between two adjacent nodes, then they randomly select one as the matching key; otherwise go to Phase III.

Phase III: Key path establishment process. If there is no direct shared key between two nodes, then they need to use the nodes that have been built a key path with them to build a new key path.

Chan et al. improved the method and gave the q-composite random key pre distribution method [5]. In this method, a node needs to select m keys from the key pool before deployment and if any two adjacent nodes want to establish a matching key, they at least need to share q keys.

The key negotiation protocol including two parties is given by Diffle and Hellman, which is named D-H algorithm. Using the D-H algorithm and the key construction method given by Shamir, researchers have proposed many key agreement protocols which are based on identity.

In 2001, Boneh et.al designed an encryption method based the identity by using the bilinear pairing[6]. However, these protocols can’t meet the perfect security of the front and back. The protocol given by Shim satisfies the two securities, but is vulnerable to the man in the middle attack[7]. An effective key agreement protocol given by McCullagh et.al can’t resist the key disclosure attack[8]. The security of the protocol proposed by Chen et al has been proved using random oracle model, but this protocol also does not meet the forward/backward security [9].

This paper gives a WSN network model, where ECC is used as authentication for its low computational complexity, AES ECB mode is used for key distribution and information transmission, and the Hamilton algorithm is used to build the key pool. This model uses ECC algorithm to solve the following problems of the node: low computational power, small storage capacity, Power shortage and limited communication range.

III. Key management scheme

A. *Network model*

WSN is divided into three layers: management layer, service layer, user layer. The management layer has the characteristics of strong energy, powerful computing ability, sufficient storage space and communication range, called the control center (S); service layer has a strong energy, computing power and a certain amount of storage. User layer, huge amount of the user sensor nodes (Uij), computing power, energy, storage and communication range is limited.

B. *Key Initialization*

This scheme is divided into three stages (1)Establishment of the system parameters;(2) Initialization phase of node information ;(3) Initialization phase of the regional key.

This scheme uses elliptic curve cryptography. The elliptic curve equation in prime number is $E: y^2 = \left(x^3 + ax + b\right) \bmod p$,

$E:\{a,b,G,N,P\}$ is curve parameter. Where G is the basis of the elliptic curve, N is the order of G. Use $G=(x_G,y_G)$ to represent G, set system private key S. The system public key is sG, $sG=(x_S,y_S)$, $s\in Z_P$. System parameters are managed and updated by the offline key distribution center.

Second stage：Initialization of information

This stage is performed before the node is deployed. Assume that the wireless sensor network has a T * M sensor nodes. Divide the whole network into M regions. Let U be any unit (including control center, server, common sensor node). Its full identity information is shown in Table 1.

Node ID_u

Region number	identification	Serial number

Table 1 node identification information

Node key initialization: public key uID_usG, private key u, which $u\in Z_P$ is a random selection of nodes.

Third stage：Key Initialization。

The initialization of the region key is performed before the node is deployed. AES encryption algorithm is adopted to transmit, each 128 bit for group packet encryption, ECB encryption method . The symmetric key K of each node is stored 128 bit.

C. Key agreement and communication protocol

Figure 1 show that user A and user B communication process:

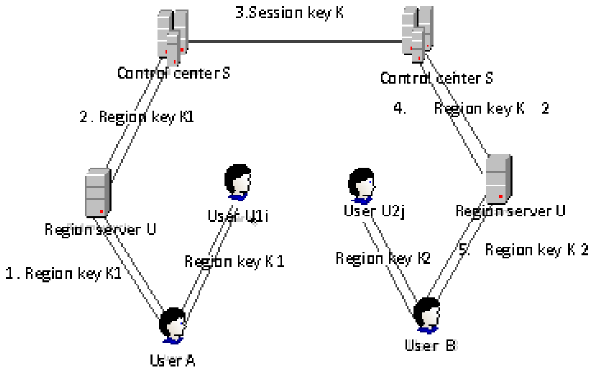

Figure 1 Communication process

Communication protocol shown as follows:

$1: A\rightarrow B: ID_A \| R_A \| (x_1ID_A, y_1R_A)$

$2: B\rightarrow A: ID_B \| R_B \| E_K(R_A \| ID_A \| bsGy_2 \| (x_1ID_B, y_1R_B))$

$3: A\rightarrow B: E_K(R_B \| ID_B \| asGy_2)$

$4: B\rightarrow A: E_K(L \| start)$

$5: A\rightarrow B: E_K(M \| ID_A \| L)$

Table 2 Key agreement protocol

A private key：a ,public key：$aID_AsG, R_A=F_AsG$, F_A is randomly generated。

B private key: b ,public key：$bID_BsG, R_B=F_BsG$, F_B is randomly generated. $a,b,F_A,F_B\in Z_P$.

l is communication clock,l+1 by communication ,if l<L, update key.

Start represent begin of the communication, the session key is K.

The encryption key E_K is extracted from x_2, y_2 as the signature key.

Agreement procession as follows：

1 A calculate $abID_BsG\cdot ID_B^{-1}=absG=(x_1,y_1)$,encrypt ID_A,R_A;

2 B calculate $baID_AsG\cdot ID_A^{-1}=basG=(x_1,y_1)$,verify ID_A,R_A, calculate $(x_2,y_2)=F_AF_BsG=F_AR_B=F_BR_A$ and $bsGy_2$.

3 A calculate $(x_2,y_2)=F_AF_BsG=F_AR_B=F_BR_A$, decrypt and verify $ID_B,R_B, bsG=bsGy_2\cdot y_2^{-1}$.

4 B verify $asG=asGy_2\cdot y_2^{-1}$,send land start.

5 A send plaintext M,L and identity information。

D. Key pool generation

There are T * M nodes in WSN, which are divided into M regions, each region include T nodes. In the initialization phase, the server stores the identity information of all nodes in the region, then the server uses the random number of each node, and each node is set up, and the number is randomly sorted by Hamilton algorithm.

E. Key Update

The key update is also divided into three stages: 1、periodic update key;2、nodes join/leave; 3、system key update.

In this scheme, according to the ECC protocol, the node's own private key S and the session key are randomly selected from the data domain Z_P.

A.1 Period Update

The key and identity of the node in this scheme is only for each node, which can be used to update the n bit in the identity ID.

B.1 *Node join*

Process of node join is shown in figure 2：

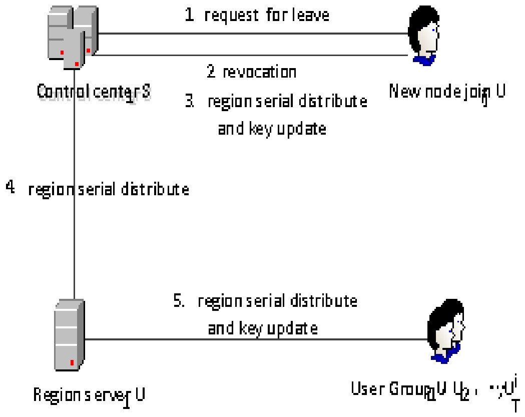

Figure 2 region node join

When a new node is added, control center checks the identity of the node, assuming that the node is U11, for the following communication:

$1:U_{1J} \rightarrow S_1 : ID_{U_{1J}} \parallel join \parallel \left(x_{S1} ID_{U_{1J}}, y_{S1} R_{1J} \right)$

$2:S_1 \rightarrow U_{1J} : ID_{S_1} \parallel R_{S1} \parallel E_{KS} \left(R_{1J} \parallel ID_{U_{1J}} \parallel csGy_{S2} \parallel \left(x_{S1} ID_{S_1}, y_{S1} R_{S1} \right) \right)$

$3:U_{1J} \rightarrow S_1 : E_{KS} \left(R_{S1} \parallel ID_{S_1} \parallel dsGy_{S2} \right)$

$4:S_1 \rightarrow U_1 : jion \parallel ID_{U_{1J}} \parallel Time$

If the new node is added, the application process is as follows:

$1:U_1 \rightarrow U_{11} : jionID \parallel Time$

$2:U_{11} \rightarrow U_1 : ID_{U_{11}} \parallel \left(x_1 ID_{U_{11}}, y_1 R_{11} \right)$

$3:U_1 \rightarrow U_{11} : ID_{U_1} \parallel R_1 \parallel E_K \left(R_{11} \parallel ID_{U_{11}} \parallel bsGy_2 \parallel \left(x_1 ID_{U_1}, y_1 R_1 \right) \right)$

$4:U_{11} \rightarrow U_1 : E_K \left(R_1 \parallel ID_{U_1} \parallel asGy_2 \right)$

$5:U_1 \rightarrow U_{11} : E_K \left(L \parallel start \parallel K_1 \right)$

The verification process follows the protocol 1, the symbolic meaning is as follows：

Where the area server is U_1, the private key is b, a node in the area is U_{11},the private key is a. The private key of the control center is c, $R_{S1} = F_{S1} sG$. The encryption key E_K is extracted from the session key.

C.1 *Node leave/revocation*

Process of node join is shown in figure 3：

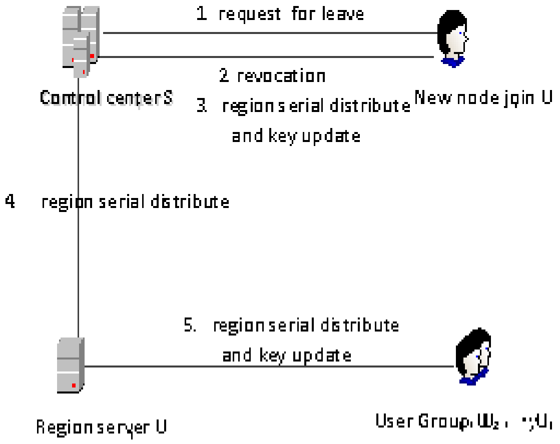

Figure 3 node leave

When node leave, control center checks the identity of the node, assuming that the node is U1J, for the following communication:

$1:U_{1J} \rightarrow S_1 : E_{K_1} \left(leave \parallel ID_{U_{1J}} \right)$

$2:S_1 \rightarrow U_{1J} : ID_{S_1} \parallel \left(x_{S1} ID_{S_1}, y_{S1} R_{S1} \right)$

$3:U_{1J} \rightarrow S_1 : ID_{U_{1J}} \parallel R_{1J} \parallel E_{KS} \left(R_{S1} \parallel ID_{S_1} \parallel dsGy_{S2} \parallel \left(x_{S2} ID_{U_{1J}}, y_{S2} R_{1J} \right) \right)$

$4:S_1 \rightarrow U_1 : DeleteID_{U_{1J}} \parallel Time$

where leave represent request，The encryption key is extracted from the session key, The verification process follows the protocol 1.

Then region server update region key and broadcast to region nodes.

3.5.4 System parameter update

When the key system used for a period of time, in order to prevent the opponent plaintext exhaustive method and aggressive behavior. It also need for regular System parameters to update.

IV. Analysis

A. *Performance analysis*

Set network is M*T ,M region and each region T nodes.

A.1 *Storage*

Control center S stores all control centers in WSN, identity of all nodes and public key .Control center is responsible for forward the cross regional communication messages, the region key pool is required to store. Storage complexity is O (M+T).

Server U stores the area key pool, node identity and public key information. Storage complexity is O(T).

Node Uij store the identity public key information and the regional key and the area control center. Storage complexity is O(3).

B.1 Calculate complexity

Compare Tseng scheme [10] ,this scheme with Steiner scheme, every two nodes have exchange key for communication. The region key is generated by the combination of these keys, so the key is stored in a user node, which is more than previous two schemes. When a new node is added, [10] and this scheme only needs to update the region key, and only the number of nodes in the region has changed ,not effect other regions. In the Tseng scheme and Steiner scheme, a new key is generated, and the time complexity is O (MT).

Table 3 Scheme time complexity compare

Scheme	region node key storage	User node Key storage	Join/leave complexity	Communication complexity
Steiner	o(MT)	o(MT)	o(MT)	o(MT)
Tseng	o(1)	o(1)	o(MT)	o(MT)
This scheme	o(1)	o(1)	o(1)	o(1)

Table 3 gives a comparison of the time complexity of different schemes. Can be seen in the Tseng scheme, the user node only stores region key, and in the Steiner scheme, each two nodes have exchange keys for communication. In the above two schemes, the region key is generated by the combination of the key. Therefore, the key information stored in the user node is significantly less than the Tseng scheme and Stentiner scheme. When a new node is added, the program will only need to update the area code and the regional key, and have no effect on other regions. In the other two schemes, a new region key must be generated and distributed to all the remaining nodes. When nodes leave, the Tseng scheme and Stentiner scheme have to generate a new group key and distribute it to all nodes, and this scheme only needs to cancel and update the identity of the nodes and update the corresponding region number and key.

In order to further describe the network characteristics of the user node of the Internet of things. Compared with [1,2,4,11,12], q-Composite scheme, PIKE scheme, LEAP scheme, E-G scheme, CPKS scheme. In E-G scheme, user node need store K key rings for the shared key discovery. Therefore, the computation complexity and storage complexity of the nodes is O(m). In q-Composite scheme, user nodes randomly select keys from key pool to generate secret key which is similar to the E-G scheme, the node computation complexity and storage complexity is also O(m). PIKE scheme, LEAP scheme and CPKS scheme are also analyzed, and the comparison results are shown in Table 4.

Table 4 Performance and protocol analysis

Scheme	Calculate complexity	Communication complexity	Storage complexity
CPKS	0	0	o(c)
E-G	o(k)	o(2)	o(k)
q-Composite	o(m)	o(2)	o(m)
PIKE	o(2)	$o\left(\sqrt{n}\right)$	$o\left(\sqrt{n}\right)$
LEAP	$o\left(d^2/N\right)$	$o\left(\log N\right)$	$o\left(d+L\right)$
This scheme	o(2)	o(2)	o(2)

As can be seen from table 4,user node in this scheme only needs to carry out the calculation of two times, the 3 communication and storage of public key and private key, compared with the traditional key management scheme, the communication cost and storage cost are greatly reduced.

B. Simulation analysis

A.1 Communication cost

In order to compare communication cost between the two sides in different regions, the probability of A and node B in the same area is P, and the cost of communication is $\lg q$.

In this scheme, the nodes in the same area need to be at least 3 session communication, and the nodes in different regions need at least 16 session communication. Therefore, the communication cost of the node is expected to

$E(p) = 3p\log_2 q + 16p\log_2 q$, and the unit is KB, and the communication cost of the network nodes is simulated by taking different probability P. Simulation results are shown in Figure 4.

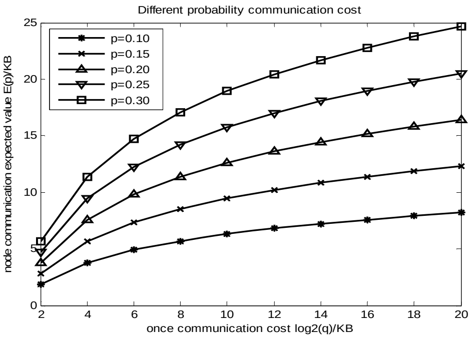

Figure 4 Different probability communication cost

As can be seen from Figure 7, with the increase of probability, the communication cost of the nodes value of the expected is increased. Expected value of the node communication is different with the change of the communication area.

B.1 Network connectivity

If there are T nodes in the region, the packet loss rate is L, which is based on the assumption that the expected value of the node key update cost is $E(q) = 2TL\lg q + T(1-L)\lg q$. By comparing different T values, using MATLAB programming, the simulation results are shown in Figure 5.

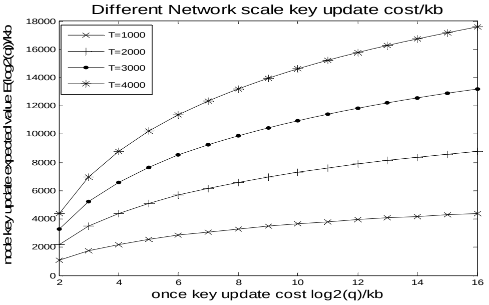

Figure 5 Network key update cost

Fig. 5 simulation results show that, with the increase of the number of network nodes, the cost of node key update is increased. But the magnitude of the increase is polynomial order. not cause too much impact on the connectivity of the whole network.

C. Security Analysis

In this paper, the key agreement protocol satisfies the security forward/backward and PKG security. That is, when a node joins or leaves, the regional key is updated by the server, the session key of each node is updated, so the new node and the node can not get the key and session key. Since each node automatically generates its own secret key when the key is negotiated, the PKG can't calculate the session key. In addition, the protocol can resist common intermediate person attack, replay attack, meet the known key security, unknown key share security and other security.

V. Conclusion

In this paper, a key management scheme and communication protocol based on elliptic curve cryptography is proposed. This model can provide simple, secure key agreement, identity authentication and update method. Because of the calculation of the elliptic curve, the storage capacity of nodes in the communication process is very small. Compared with the traditional key management scheme. The protocol used in this scheme has a higher security, any node in the attack, the impact is only itself and its corresponding link information, the other nodes and links in the network will not be affected. In the next step, the research work will focus on the specific algorithm and implementation of the WSN environment.

References

[1] Eschenauer L，Gligor V. A key management scheme for distributed sensor networks. In:Proc.of the 9th ACM Conf. on Computer and Communications Security. New York:ACM Press,2002,41-47.

[2] Chan H，Perrig A，Song D. Random key predistribution schemes for sensor networks. In：Proc. of the 2003 IEEE Symp. On Security and Privacy. Washington： IEEE Computer Society,2003,197-213.

[3] LIU D, NING P. Establishing pairwise keys in distributied sensor network[A]. Proceedings of the Conference on Computer and Communications Security'03[C]. ACM Press, Washington DC 2003.51-61.

[4] Liu D，Ning P. Location-Based pairwise key establishments for static sensor networks. In：Proc.of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks. New York：ACM Press,2003,72-82.

[5] Chan H，Perrig A，Song D. Random key predistribution schemes for sensor networks. In：Proc. of the 2003 IEEE Symp. On Security and Privacy. Washington： IEEE Computer Society,2003,197-213.

[6] BONEH D，FRANKLIN M. Identity based encryption from the Weil pairing[A]. Advances in Cryptology—Crypto 2001[C]. Berlin ：Springer-Verlag，2001,213-229.

[7] SHIM K. Efficient ID-based authenticated key agreement protocol based on the Weil pairing[J]. IEE Electronics Letters,2003, 39(8): 653-654.

[8] MCCULLAGH N，BARRETO P. A new two party identity-based authenticated key agreement[A]. Proceedigs of the RSA Conference 2005[C]. Berlin：Springer-Verlag，2005：262-274.

[9] CHEN L,KULDA C. Identity based authenticated key agreement protocols from pairing[A].Proceedings of 16th IEEE Computer Security Foundations Workshop[C]. New York,2003,219-233.

[10] Teng Y M，Yang C C，Liao D R. A secure group communication protocol for ad hoc wireless networks[C]//Advances in Wireless Ad Hoc and Sensor Networks and Mobile Computing. Springer,2007:385-390.

[11] Chan H，Perrig A. PIKE:Peer intermediaries for key establishment in sensor networks. In:Proc,of the IEEE INFOCOM 2005.Piscataway: IEEE Communication Society,2005,524-535.

[12] Zhu S，Setia S，Jajodia S. LEAP:Efficient security mechanisms for large-scale distributed sensor networks. In:Proc.of the 10th ACM Conf. on Computer and Communications Security. New York: ACM Press,2003,62-72.