A Key Management Scheme for IoTs Based on China Remainder Theorem

ZHANG Li
China Academy of Engineering Physics
Institute of Computer Application
Mianyang, China
zhangli1009120@caep.cn

LIU Dong, YANG Yonghui*
China Academy of Engineering Physics
Institute of Computer Application
Mianyang, China
liudong@caep.cn, younphy@163.com

***Abstract*—In order to reach ubiquitous perception in Internet of things, which confusion of network deployment can't generate when information collection, some security problems are considered in IOT, such as key management, privacy protection and data processing. A key management scheme based on Homomorphics Encryption and China Remainder Theorem is proposed, in which a layer network model based on node location is given to deploy network infrastructure. Double key pools are introduced for key management and distribution, which save network overhead and node resource consumption. According to the use of homomorphic encryption for the note privacy information to protect users' privacy and keep the data processing safe. A security network model and pair-key discover probability simulation is given, which shows this scheme have good connectivity and security.**

***Keywords*: Internet of Things (IOT); key management; Homomorphic Encryption(HE); China Remainder Theorem; shared key; key pre- distribution**

I. INTRODUCTION

Internet of things(IoTs)[1] has become one of the strategic heights of the new round of economic and Technological Development in the world. With the rapid development of Internet of things, network scale is constantly expanded. In the process of conveying sensitive information from border sense node to next node, how to protect privacy of information and how to identify each other is not solved currently. However, sensing node conduct resource is limited. The existing network security architecture and key management scheme can not meet the new security requirements.

In the paper[2-4], the Internet of things is divided into 3 layers, namely, sense layer, network layer and application layer. The security requirement analysis is carried out for each layer, and a relatively completely security model is given in this paper. Paper[5] propose a energy-robust high-efficient key management scheme of ID-protection for IoTs, and IoTs system model network model, adversary model and the security requirements of key management schemes are also proposed, but security prove and is not given. Paper[6] propose a key sharing scheme based on repeated adversary game theory, this scheme analyze and adopt game model to provide key-sharing between heterogeneous nodes , but not give the details of network model.

In this paper, a key management scheme based on Homomorphics Encryption theory and China Remainder Theorem is proposed, in which network is divided by applications and locations. Through constructing double key pool matrix to ensure the security of nodes security, node construct secret key list which are generated by key pools, Session key between Node A and B is generated by each secret key with Encryption Homomorphic and China Remainder Theorem. Center-control node distribute session key and secret key to each node, node(not center-control) just need to encrypt data and secret key by primary session key, privacy is protected and resource is enough.

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

II. PREPARE KNOWLEDGE

A. China Remainder Theorem [7]

Set $p_1, p_2, \cdots, p_k$ are k positive integer, which are prime number each other, $k \geq 2$:

$$P = p_1 p_2 \cdots p_k = p_1 P_1 = p_2 P_2 = \cdots = p_k P_k \quad (1)$$

satisfy $P_i = P / p_i$, $i = 1, 2, \cdots, k$,Simultaneously satisfy equations:

$$\begin{Bmatrix} c \equiv y_1 \bmod p_1 \\ c \equiv y_2 \bmod p_2 \\ \vdots \\ c \equiv y_k \bmod p_k \end{Bmatrix} \quad (2)$$

positive integer solution:

$$c \equiv y_1 P_1^{'} P_1 + y_2 P_2^{'} P_2 + \cdots + y_k P_k^{'} P_k \bmod P \quad (3)$$

$P_i^{'}$ Simultaneously satisfy $P_i^{'} P_i \equiv 1 \bmod p_i, i = 1, 2, \cdots, k$ 。

B. Homomorphics Encryption

R L Rivest[8] proposed Homomorphics Encryption in 1978, it is the encryption exchange that allows the direct operation of the cipher text. But because it is not safe to be known, it is improved by Domingo. Encryption technique is used to encrypt the statistical data firstly. The algorithm is the one that can be used to operate the sensitive data and protect its privacy: This technique is based on algebra theory, basic principle as follow：

Assuming E_{k1} and D_{k2} denote encrypt function and decrypt function, that $\{M_1, M_2, L, M_n\}$ denote plaintext elements which are finite sets, and α and β represent Homomorphics Encryption operation on the integer domain, if formula satisfy:

$$\alpha\left(E_{K1}(M_1), E_{K1}(M_2), \cdots, E_{K1}(M_n)\right) = E_{K1}\left(\beta(M_1, M_2, \cdots, M_n)\right) \quad (4)$$

that $\{E_{k1}, D_{k2}, \alpha, \beta\}$ is Homomorphics 。

This paper adopts Homomorphics Encryption operation as follow:

$$E(x) = (x + r * p) \bmod p * q \qquad (5)$$

r is random integer, p, q are large prime number。 $\alpha: E_{K1}(M_1) + E_{K1}(M_2) + \cdots + E_{K1}(M_n)$, $\beta: M_1 + M_2 + \cdots + M_n$, α , β represent ordinary addition operation on integer domain.

III. KEY MANAGEMENT SCHEME

A. *Network model*

According to different applications and network style, the Internet of things is divided into different regions[9]. Assuming each regions has Control Center(CC) ,which collect information from other nodes by GPS network architecture, and compute location such as distance and angle which are used to divide regions. Network model of the Internet of things is shown in figure 1.

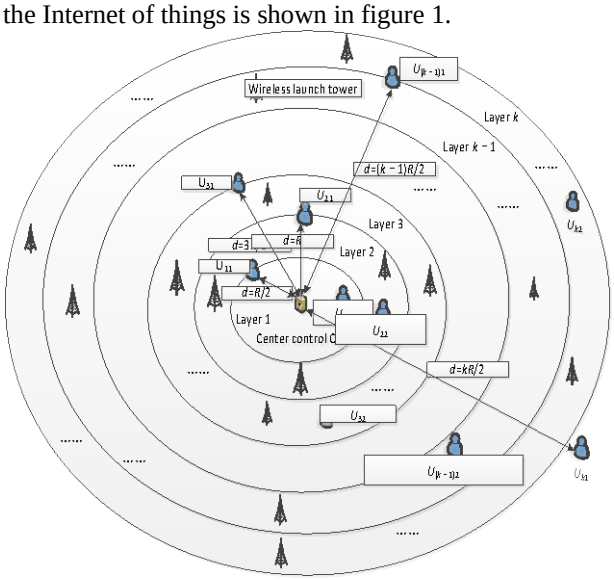

Figure 1 IoTs model based on China Remainder Theorem

The sensing layer of the Internet of things is made up of some resource limited devices, and most of them use wireless technique to exchange information. Consider the communication cost and energy of each node are different, Taking a certain area CC as the center, the distance between CC and node is d, and the longest is R. The node communication area is the entire circular area with the CC as the center and the radius of R. According to the distance between the nodes and the CC, the area is divided into K layer:

Layer 1：d∈(0,R/2];

Layer 2：d∈(R/2,R];

…

Layer K：d∈((K−1)R/2,KR/2]。

In accordance with the above rules, CC distributes the area key and layer key for each node which is used to generate session key. In order to be able to ensure that any two nodes in the same layer can be communicate directly ,intermediate forwarding devices are constructed on these regions, such as a radio transmitter tower or base station. Assume arc length L<R of these nodes is taken to determine the number of the radio transmitting tower in the layer. The communication distance model of different nodes in layer i is analyzed, as shown in Figure 2.

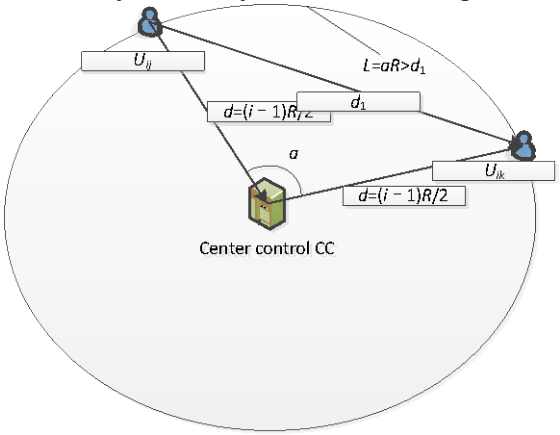

Figure 2 Layer node communication model

Figure 2 show that when d_1>R, nodes can not communicate directly. For layer i, select the largest arc, namely perimeter of a circle which radius is (i-1)R/2. Calculate circumference is 2*pi*(i-1)R/2 ,then the number of transmit devices is pi*(i-1)R/2R, For Layer 1,2,….,k, the number of transmit devices is $\sum_{i=1}^{k} \pi(i-1)/2$.

B. *Scheme design*

a. *Key pool Construction*

M*N matrix is constructed in paper[10],nodes select key from each column of M*N key pool according to hash H(ID) , which is composed of a key ring, but this scheme has not considered the network environment and application and set only one control center to manage and generate key pool. It can not satisfy the IoTs requirement To this end, this paper constructs two T*L matrix, one matrix stores original key, another store private key. $seed_{ij}$ represent the original key for all nodes in the region i, layer j. Another matrix storage node's private key p_{ij} , p_{ij} represent region i, layer j private key, p_{ij} is a large prime, $seed_{ij}, p_{ij} \in \left[-2^{\rho}, 2^{\rho}\right]$ as a security parameter, where the security parameters can be generated according to different application requirements, its key pool matrix (5), type (6):

$$\begin{bmatrix} seed_{11} & seed_{12} & \cdots & seed_{1L-1} & seed_{1L} \\ seed_{21} & seed_{22} & \cdots & seed_{11} & seed_{1L} \\ \vdots & \vdots & & \vdots & \vdots \\ seed_{T-11} & seed_{T-11} & \cdots & & seed_{T-1L} \\ seed_{T1} & seed_{T1} & seed_{T1} & \cdots & seed_{TL} \end{bmatrix}_{T\times L} \qquad (5)$$

$$\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1L-1} & p_{1L} \\ p_{21} & p_{22} & \cdots & p_{11} & p_{1L} \\ \vdots & \vdots & & \vdots & \vdots \\ p_{T-11} & p_{T-11} & \cdots & & p_{T-1L} \\ p_{T1} & p_{T1} & p_{T1} & \cdots & p_{TL} \end{bmatrix}_{T\times L} \qquad (6)$$

Among them, $seed_i$ is generated by the offline server for each region CC, and different regions are generated by different seed key. These key is stored by CC. The whole IoTs Network is divided into T regions: $[seed_1, seed_2, \cdots, seed_T]$, $seed_{ij} = H(seed_i \| dk_{ij})$.

According to above rule, it can guarantee in the same area, the same layer of nodes to obtain the same $seed_{ij}$, and $seed_{ij}$ can not infer $seed_i$; when update these keys, CC need to update the $seed_{ij}$ by $seed_i$.

The above key pool construction based on assuming the number of layer of different application and the number of nodes in different layers are equal, but network style and size is different. Therefore, this paper according to distance of node and CC and direction (by CC selected x, y vertical axis, and then calculate the node and CC axis a x)so as to identify with the change of the node position, x, y vertical axis is selected by CC, increase the difficulty of the opponent guessing attack.

b. Key Distribution

Set DKij= (IDij||dkij) as the identification of nodes Uij, $U_{ij} \in \text{Region}\, i, Layer j$ where ID_{ij} represent the unique number of the node, ID=H (d||a); dkij indicates the location of the node of region i and layer j. CC generates the key steps as follows:

Assume that the node deployment information is DKij, the corresponding private key value is Pij. In the matrix, remove the line i and column j, (7) is used to construct this node's key ring. This construction is to improve the probability that the same layer can be found session key, and to prevent common attacks, as shown :

$$\begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,j-1} & p_{1,j+1} & \cdots & p_{1,L-1} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,j-1} & p_{2,j+1} & \cdots & p_{2,L-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ p_{i-1,1} & p_{i-1,2} & \cdots & & \cdots & \cdots & p_{i-1,L-1} \\ p_{i+1,1} & p_{i+1,2} & \cdots & p_{i+1,j-1} & p_{i+1,j+1} & \cdots & p_{i+1,L-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\ p_{T-1,1} & p_{T-1,2} & p_{T-1,3} & p_{T-1,j-1} & p_{T-1,j+1} & \cdots & p_{T-1,L-1} \end{bmatrix}_{T-1 \times L-1} \quad (7)$$

The construction process of key rings in the scheme is as follows:

Assume distance of nodes Uj and CC is du, $U_j \in layerj$,then the construction of all nodes in the layer is:

(1) CC calculate hash H(IDUj)= B1 B2…BL−1, where Bi denote a decimal number.CC select Seedij from (5) according to the Bi ,i=1,2…,L-1.

(2) CC select pij from column j and line Bi of matrix (7),i=1,2,…,L-1.Then calculate $H(seed_{ij} \| pij)$,i=1,2,… L-1.These values construct node's key ring. It ensures that a certain probability p to find session key, and the probability value is related to the hash value of each node ID.

Set $p(i)$ represent the probability of i session keys in

$$p(i) = \frac{C_{L-1}^{i}(T-1-1)^{L-i-1}}{(T-1)^{L-1}} \quad (8)$$

The probability of different layer session key is 0. Because this paper delete the matrix ranks of nodes in the region i and layer j, $p(i)$ is higher than paper[10], and it can prevent the same area, defend the same layer of common attack. node can not calculate the Seedij and Pij to generate a session key.

The selection mechanism may cause the node to satisfy the distance between different layers less than or equal to R, but there is no session key. In order to make up for the above defects, two methods are adopted in the communication process:

(1) In addition to exchange the necessary identity and regional information, it is also necessary to exchange the information of the distance between the nodes, and when the node is found not satisfy the same layer, and the distance d<R,CC assigned to them session key.

(2) Change the key generation rules, which are selected from two adjacent columns. In this case, a node generate session the key of the probability of P, $0 \le p \le p(1)$

c. Communication protocol

In this paper, communication protocol is based on somewhat Homomorphics Encryption, The realization of protocol as follows:

Region i is divided into A layers. Through the above analysis, it is shown that Seedij and Pij are the same for the same layer node. CC constructs China Remainder formula (9) as follow:

$$\begin{aligned} Y_{i,1} &\equiv seed_{i,1} + p_{i,1}r_2 + 2r_{i,1} \bmod p_{i,1} \\ Y_{i,2} &\equiv seed_{i,2} + p_{i,2}r_2 + 2r_{i,2} \bmod p_{i,2} \\ &\vdots \\ Y_{i,A-1} &\equiv seed_{i,A-1} + p_{i,A-1}r_2 + 2r_{i,A-1} \bmod p_{i,A-1} \\ Y_{i,A} &\equiv seed_{i,A} + p_{i,A}r_2 + 2r_{i,A} \bmod p_{i,A} \end{aligned} \quad (9)$$

Where Pij represent private key of region i and layer j, Seedij is the seed key for the j layer of the region i. By the Chinese Remainder theorem, there exists a value Y, which satisfies the formula (10):

$$Y \equiv Y_{i,1}P_{i,1}P'_{i,1} + Y_{i,2}P_{i,2}P'_{i,2} + \cdots + Y_{i,A}P_{i,A}P'_{i,A} \bmod P_{i,1}P_{i,2}LP_{i,A} \quad (10)$$

CC calculate and broadcast Y to each node within the region, the node uses its own private key Pij to operate as formula(11):

$$\begin{aligned} Y &\equiv Y_{i,j} \equiv seed_{i,j} + 2r_{i,j} \bmod p_{i,j} \\ Y_{i,j} &\equiv seed_{i,j} \bmod 2 \\ r_{i,j} &\equiv Y_{i,j} - seed_{i,j} \bmod p_{i,j} \end{aligned} \quad (11)$$

Where, rij is the layer key which is stored in the node. CC adopt homomorphic encryption with regional key encryption to broadcast L-1 Keys to each node, also include matrix corresponding to the ranks of the coordinate value.

After the completion of the above steps, the adjacent nodes can encrypt the node's key list to each other by the layer key, the other party can find out all the session key

with the same information from the key list. In addition, consider the resource constraints of the device nodes in the scheme, the [11] protocol is used to carry out the key agreement protocol.

d. Key Update

The key update in this paper involves two parts: periodic update and node join/leave update. The update of the program is done by CC. CC has a strong computing power and sufficient resources. When nodes join/leave, Seedij is updated, and the private key Pij is updated. CC updates the source key matrix, each regional CC updates its key to form a new key.

$$\left[seed_1^{'}, seed_2^{'}, \cdots, seed_k^{'} \right] \tag{12}$$

$$\begin{bmatrix} seed_{1,1}^{'} & seed_{1,2}^{'} & \cdots & seed_{1,L-1}^{'} & seed_{1,L}^{'} \\ seed_{2,1}^{'} & seed_{2,2}^{'} & \cdots & seed_{2,L-1}^{'} & seed_{2,L}^{'} \\ \vdots & \vdots & & \vdots & \vdots \\ seed_{T-1,1}^{'} & seed_{T-1,2}^{'} & \cdots & & seed_{T-1,L}^{'} \\ seed_{T,1}^{'} & seed_{T,2}^{'} & seed_{T,3}^{'} & \cdots & seed_{T,L}^{'} \end{bmatrix} \tag{13}$$

CC generates a new key ring for each node according to the new value, and distributes it to each node in the form of the broadcast.

IV. PERFORMANCE ANALYSIS

A. Session key discovery probability

According to the key distribution described in 3.2.2 section, there is a probability of i session key between any two nodes:

$$p(i) = \frac{C_{L-1}^{i}(T-1-1)^{L-1-i}}{(T-1)^{L-1}} \tag{14}$$

Between any two nodes, at least of the probability of a session key:

$$p = 1 - p(0) - p(1) - \cdots - p(t-1) = 1 - \sum_{i=0}^{t-1} p(i) \tag{15}$$

By the formula (14),(15) if T is constant, with the increase of L, p is also increased. When T=128, L=256, t=1, P is 90%, t=3, P is still more than 30%.

Table 1 compares the key distribution scheme of [10],[11] with q-composite in this paper. According to the data from table 1, we can get the ideal probability value by choosing the similar L and T, which is similar to that obtained by using q-composite key pre-distribution method.

Table 1 Session key find probability

Scheme	parameter	p(t=1)	p(t=2)	p(t=3)
[12]	T=128,L=128	0.633 00	0.264 23	0.078 85
	T=256,L=256	0.633 56	0.264 24	0.079 58
[10][11]	T=128,L=128	0.633 56	0.264 24	0.079 58
	T=256,L=256	0.632 44	0.264 24	0.079 57
This paper	T=128,L=128	0.633 57	0.264 24	0.079 59
	T=256,L=256	0.633 48	0.264 25	0.0795 78

B. Network connectivity analysis

According to the probability analysis of session key, the probability of two nodes can be directly established by the security channel from formula(14). In order to facilitate the establishment of a secure channel between two nodes, the probability of a single hop is P1, the probability of two hops is P2. Each node has d neighbor nodes, which can be directly related to the source node IDi and the target node IDj. Thus, the nodes IDi and IDj can be established by a single hop and two hops to build the probability of communication is P1,2:

$$p_{1,2} = 1 - (1 - p_1)\left(1 - p_1^{\,2}\right)^{d} \tag{16}$$

Obviously, the probability P1,2 increases with the increase of the probability P1, and the increase of the number of neighbor nodes. According to the formula (16), it can calculate the probability that the two nodes can build up a secure link directly or indirectly is more than 90%.

In this paper, we can set up the communication distance between nodes, and the nodes can maintain a high session key discovery protocol in the communication range. Because the set of communication distance 2R can be used to reduce the session key discovery probability. Because of the different applications, it can reduce the session key discovery probability, but also can be used as a supplementary to ensure the connectivity of the whole scheme. From the construction process of the above matrix, the matrix is designed to be the base of the maximum number of layers in all regions, so it is convenient for the whole network.

C. Network scalability analysis

In this paper, two key pools matrixs are constructed according to the region and layer. Consider initial deployment can not satisfy requirement. L*T matrix is chosen as the standard and the construction method can satisfy the network scalability. T and L are 128 and 256 are not related to the larger network size, which is mainly limited by the function of the simulation software, but the theoretical analysis from the structure of the process and the key construction process can be known, with the continuous expansion of the network size, the probability advantage will be more obvious.

In this scheme, nodes need to store their own private key Pij, public key PK, region key Seedij and broadcast layer key. The session key discovery process only needs to broadcast its own list of coordinates, the complexity is o(1).Encryption transmission mechanism uses encryption scheme of Gentry. Therefore, this scheme is feasible.

V. SECURITY ANALYSIS

In this paper, an attacker can obtain all key of a specific node if capture this node, and then obtain the communication key of the node and other nodes. Assuming that the K nodes has been captured, and the attacker can obtain the probability of a certain node is P:

$$p = \left(1 - \left(\frac{T-1}{T}\right)^{k}\right)^{L} \tag{17}$$

The result of simulation by matlab as shown in figure 3.

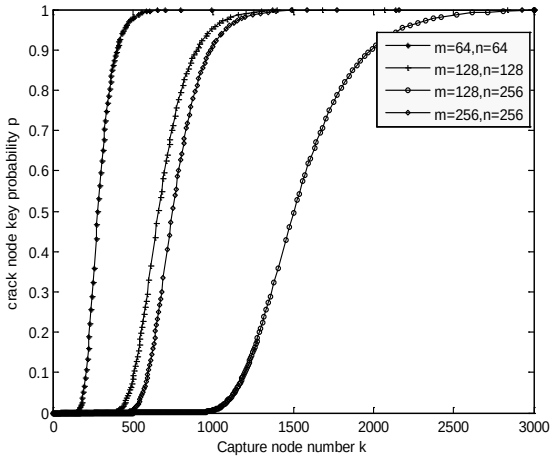

Figure 3 Capture node number and crack node key probability

For the whole network attack, the attacker can obtain the key pool in a certain number of nodes, so as to destroy the perception layer network. If the K node is captured, the attacker can obtain the probability of all keys in the key pool is $P^{'}$. When all the keys are not repeated, the k is m, so the attacker can obtain all the key at least capture m codes, S(k,m) is second Stirling number, then the attacker can obtain the probability of all keys in the key pool:

$$p^{'} = \left(\frac{S(k,T)T!}{T^{k}} \right)^{L} \qquad (18)$$

Where k=m=n=128, $P^{'} \propto 0$,k=1000M=N=128, $p^{'} = 0.0016$。

(1) Anti-collusion attack. The theoretical basis of this paper is the Homomorphics encryption technique and the Chinese remainder theorem. The key pool matrix is generated and updated by CC. The key is generated by the Hash function. The position information of the node is first selected by CC, then the angle and distance are calculated. So the location information of the nodes changes with the position. The key is distributed to the nodes and the nodes are not distributed to the same key. In the process of selecting the key factors, H (Seedij||pij) can effectively prevent the collusion attack. So the adversary can not obtain the key.

(2) The probability of adversary cracked the node's private key and primary key is small. The scheme uses the encryption technique of the encryption and the remainder theorem to encrypt the information. The node is used to decrypt the private key and the primary key. CC need to carry out regular feedback to each node in order to detect the abnormal behavior of the node, and to further enhance the effective way and method of CC detection of abnormal nodes. In order to protect the security of nodes, the node deployment information DK contains the dk (location information), ID (node and CC distance and angle), which are private, although it is easy to obtain the broadcast messages from the same layer encryption, but the adversary can only obtain the number of the area, which can not obtain the specific node number.

(3) The probability of adversary obtain key pools is small. In this paper, we assume that the regional control center as a management center, with sufficient data process capacity and sustainable work ability. CC is responsible for generating, updating and storing the primary key, and processing the data in different regions. Adversary capture node to obtain key ring and through the asynchronous attack and conspiracy attack can obtain the Seedij key matrix and Pij matrix, but because Seedij is composed of Seedi and Dij by Hash, the difficulty of cracking is equivalent to decipher the adversary one-way function. So adversary cannot control the primary key and key matrix updating ability; Consider the characteristics of mobile network equipment, the same equipment ID will change with the deployment of different position, and adversary can not through the deployment of equipment to decipher the adversary information node. Analysis on the crack nodes session key, adversary at least capture the same region, the same layer more than 1000 nodes can obtain extremely low probability of decryption key matrix; Through capturing in different regions and different layer nodes to crack the key matrix can be neglected.

(4) Satisfy the safety of front and back. When the new device node leaves, to ensure communication forward security, CC update the Pij matrix column j and distribute to the region nodes and the layer nodes, because other regions of the node does not relate to the column j, so that it can reduce the update cost.

According to different security requirement, we can set different security levels. For example, we can improve or reduce the security level by changing the parameters p and safety parameters of the R, and the private key Pij can be improved according to different needs.

VI. CONCLUSION

In this paper, a new key management scheme based on China Remainder Theorem is proposed, which is based on node location information. Compared with the existing schemes, the following advantages: (1) According to the max distance of node communication, the radio transmitting tower is calculated. (2)This scheme gives the double key pools to select region key and private key. The node position information and the CC vertical axis of the central control center are selected to ensure the privacy. (3) The probability of node session key discovery has been improved.(4) This scheme give a specific key update protocol, which can satisfy the dynamic key update when the nodes join/leave. (5) The security of the scheme is better than the existing scheme.

REFERENCES

[1] ITU Internet Resports 2005:The Internet of Things [EB/OL]. (2005-07-11).

[2] WANG Jing, Quan Chun-lai, ZHOU Xiang. Research of public security platform software architecture based on internet of things [J]. Computer Engineering and Design, 2011, 32(10): 3374-3377.

[3] BAI Jiao, Quan Chun-lai,GUO zhen. Research of public security platform cloud computing architecture based on internet of things[J]. Computer Engineering and Design, 2011, 32(11): 3696-3701.

[4] Liu Ji hong, Yang Li. Application of Internet of

Things in the Community Security Management [C]//Proceedings of the 3rd International Conference on Computational Intelligence, Communication Systems and Networks. Bali, Indonesia: IEEE Press, 2011: 314-318.
[5] REN Wei, LEI Min, YANG Yu. ID-Protected Power Efficient Robust Key Management Schemes in T2Tol of Internet of Things[J]. Journal of Chinese Computer Systems, 2011, 32(9): 1903-1907.
[6] LI Da-wei, YANG Gen. Secret Sharing scheme of internet of things based on Repeated Game[J]. Journal on Communications, 2010, 31(9A): 97-103.
[7] XI Guo-bao,Chen Hui-fang,Zhao Wen-dao. China Remainder Theorem-Based Secret Sharing Scheme [J]. Journal of Electronics & Information Technology, 2006, 28(12): 2378- 2381.
[8] Rivest R L, Adleman L, Detrouzos M L. On Data Banks and Privacy Homomorphism[M]. New York, USA: Academic Press,1978.
[9] Saber Banihashemian, Abbas GhaemiBafghi. A New Key Management Scheme in Heterogeneous Wireless Sensor Networks[C]//Proceedings of the 12th International Conference on Advanced Communication Technology. [S. l.]: IEEE Press, 2010: 141-146.
[10] Zhang Rui, Liu Ji-qiang, Zhao Jia. An ID-based Key Pre-distribution Scheme for wireless Sensor Networks[J]. Journal of Electronics & Information Technology, 2009, 31(4): 929-932.
[11] ZENG Ping, ZHANG Li, HU Rong Lei. Lightweight authenticated key agreement protocol based on ECC for wireless sensor networks[J]. Computer Engineering and Applications, 2014, 50(2): 65-69.
[12] Chan Hao-wen, Perrig A, Song D. Random Key Pre-distribution Schemes for Sensor Networks[C] //Proceedings of 2003 IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Computer Society, 2003: 197-213.