The Improved Key Exchange Protocol Based on Public Key Certificates

Cuijie Zhao*, Guozhen Wang
Information Science and Technology, Pearl River College, Tianjin Finance and Economics University
tianjin,13212087537
*Corresponding author, e-mail: zhaojie810809@126.com

Abstract

We propose mutual authentication and session key exchange protocols based on certificates for the Internet of Things. We also propose an improved version for the conventional certificate-based systems. Our protocol is efficient, it requires fewer messages and only one session key. It gives use a new method to deal with such as preventing tampering and preventing interference security problems. In designing the security protocol proposed here, the low computational power of the wireless sensors nodes and the low bandwidth of the wireless networks are considered. It is good as low computational complexity and cannot be forged.

***Keywords**: intemet of things (IOT), sensor, key exchange protocol, certificate, authentication*

1. Introduction

IOT is known as the third wave of the information industry following the computer and the Internet [1]. It brings many benefits for people while it also brings the increasingly prominent issues of privacy.

From the information collection, transmission and application point of view, the IOT is divided into three layers structure [1], the bottom layer is perceptual layer for data perception, the second layer is the network layer for data transmission, and the last layer is the application layer. In perception layer network, the safety protection ability is poor because of its technical characteristics, and the security level is relatively low compared to the core network [2].

2. Analysis of Sensor Network Security Technology

For many sensor networks, security is very important. Sensor network system not only needs to face the harsh environment, but also face active, intelligent opponent, so the sensor networks need to battle with positioning, sabotage, subversion. On other occasions, security requirements although not obvious, but still very important [3].

2.1. The Safety Barrier of Sensor Network

We usually said sensor network refers to a special network, The constituted process of the sensor network have more constraints and limitations than traditional network. These constraints lead to the existing security technology can not be applied to sensor networks easily.

2.1.1. Limited Resources

All the security protocols and security techniques need to rely on some resources, including data storage, code memory, energy and bandwidth. But for wireless sensor, because of its own limitation, the operation or storage resources are very limited.

1) Memory capacity constraints

The sensor nodes are miniature device, only a small amount of memory used to store the code. So based on this point, when we build safe and effective mechanism we need to control the length of the security mechanism code according to store capacity. For example, a Mica sensor node only has 128KB code storage capacity, 4KB data

Received September 10, 2013; Revised November 20, 2013; Accepted December 3, 2013

storage capacity. TinyOS code accounts for about 4KB. Therefore, all the security code must be very small.

2) Energy restriction

For wireless sensor, the ability restriction largely reflected on the energy constraint. Generally the battery powered sensor nodes once were arranged in a sensor network that would be difficult to be replaced because of high operating cost, and would be not easily charge up again because of high sensor costs, so we must save the battery energy, and prolong the lifetime of the sensor nodes, so prolong the lifetime of sensor network. Because of energy restriction, when we increase encryption function or add a security protocol we should also consider whether the energy constraint is beyond wireless sensor energy range. When we increase the security capacity for sensor node, we must consider the influence that security capacity effect on the node lifetime.

2.1.2. Unreliable Communication

For the wireless sensor network another important threat is unreliable communication. Sensor network security relies on the defined security protocol, and the defined security protocol relies on the communication.

1) Unreliable transmission

The packet routing of sensor network is a wireless connection routing, so it is not reliable. Channel error code and high congestion nodes packet loss may damage the packet. The reliable wireless communication channel also will damage the packet. The high channel bit error rate force software to use some networking source handle error. If the agreement has not appropriate error handling capacity, it may lose security grouping key, such as the encryption key [4].

2) Collision

Even if the channel is reliable, communication industry still may not be reliable, the reason is that the broadcast characteristic of sensor network [5]. If the packet collisions appear in the transmission way, the packet transmission will fail. In the high density sensor network, collision is one of subject matter.

3) time delay

Multi hop routing, network congestion, and node disposal will cause large network delay, thus to achieve synchronization between the sensor nodes is very difficult[6]. The synchronization problem has great influence on the sensor safety, security mechanism depends on critical incident reporting and encryption key block.

2.1.3. Sensor Network Unattended

According to the specific function of sensor network, sensor nodes may be in the unattended state a long time. The longer sensor node unattended time is, the greater the security attack possibility [3]. For unattended sensor nodes exist following three threats:

1) Expose to physical attacks.

Sensor nodes may be arranged in the attacker open and bad weather environment. The possibility of sensor nodes in such an environment suffered from physical attacks is much higher than typical computer.

2) Remote administration.

Sensor network remote management virtually can not detect tampering and physical maintenance. The typical example is that the sensor node used for remote detection may lose contacts with friendly forces.

3) The lack of central management point.

A sensor network should be a distributed network without central management point, which will improve the sensor network vitality. however, if the design is not reasonable, can also lead network organization to difficult, inefficient and fragile state.

3. Key Management

In order to realize the protection of perceptual information, usually we can use key management technology to ensure the security of the system. The perceptual layer key management system faced with two problems: the first one is how to build and adapt the IOT architecture through multiple network unified key management system; the second one is how to use reasonable method to improve relevant key management perception layer problem, which includes a key production process, key distribution process and key updating process [3].

Usually there are two different ways to generate the key management system: one is the centralized mode, this mode usually make the Internet as the center to manage, and have specific organization for the perceptual layer management, often can coordinate the internet key distribution center to manage the key. Once network perception layer access to the Internet, through the key distribution center interacts with the gateway node, finish key management for network aware nodes; The other one is the distributed management approach to the IOT perception layer. This way have a relatively high requirement to sink node and gateway, But the key management has great cost and overhead, because of energy consumption of the edge nodes and the hierarchical algorithm. The following is introductions to the key technology.

3.1. The Public Key Cryptosystem

The concept of public key cryptosystem is proposed by Diffie and Hellman [7] in 1976, Also known as asymmetric cryptosystem. Different from the original private-key cryptosystem, public key cryptosystem based on unidirectional and irreversible mathematical function, using of asymmetric encryption algorithm, the greatest feature is two keys separating the encryption and decryption. A public key for encryption key, a private key for decryption key, both sides of communication without prior exchange or negotiation shared key can secure communication security; On the other hand, analysis private key from public key and cipher text, it is not possible in the calculation. In public key system, each user has a key pair (Pku, Sku), where Pku is an open parameter, called the public key of the user; and Sku kept secret by users themselves, called the private key of the user. In general, the private key Sku is randomly generated, and the public key Pku is injective function check on Sku.

it is a one-way function, so all users can't get any information from the Pku public key corresponding to the private key of Sku. Thus, public key cryptography facilitates key management and distribution; also facilitate communication encryption and digital signature.

3.2. The Public Key Cryptosystem Based on Certificate

Public-key cryptosystem based on the certificate of public key authentication is realized by a digital certificate, is the identity of a user with his public key together, first by an authority trusted to verify the identity of the user, then the identity and the corresponding public key certificate of combining digital signature, to demonstrate the validity of the certificate [8]. The widely used is Public Key Infrastructure (PKI) key certificate management platform.

In the PKI system, the distribution and use of public key certificate to realize, contains the signature public key certificate, identity information of ID users and the authority of the certificate. Because the certificate can't be forged, certificates can be placed in a directory for participants to access, users can also directly to the certificate is sent to the other users. Certificate Authority (CA) plays an important role in the public key system, CA is responsible for the management of certificate of all users in the system including the people, all kinds of application and host.

The following is CA features: certificate, certificate update, and certificate revocation and certificate verification. The core function of CA is the issuance and management of digital certificate, in particular to:

(1) receives the validated end-user application for digital certificates;

(2) To determine whether to accept the end user of the application of digital certificates --certificate of approval;

(3) Issued, refused to issue digital certificates issued to applicants --certificate;

(4) The digital certificate to receive, the end user update request --certificate update;

(5) Query, receiving end user digital certificate revocation;

(6) To produce and publish certificate revocation list;

(7) Archiving of digital certificate;

(8) The key file;

(9) Historical data archiving.

4. Exchange Security Protocol Based on Public Key Certificate

Diffie-Hellman key exchange protocol is used to establish a shared secret between A and B. It makes use of the exponential function in a Q order finite field GF (q) calculations were compared with the calculated log in the same area of difficulty. If y=a^{x} mod q, for any 1<x<q-1 where a is the GF (q) a fixed basic element, then x=log$_{a}$y mod q is to base a discrete logarithm of y. we select a random number x$_{A}$ from the integers 1, 2... Q-1, x$_{A}$ are confidential, and sends them $y_A = \alpha^{x_A} \bmod q$ to B. Also, choose a random number x$_{B}$ in B, and sends y$_{B}$ to A. A and B can calculate $k_s = \alpha^{x_A x_B} \bmod q$ as their key. A need calculated ski by x$_{A}$ $k_s = y_B^{x_A} \bmod q = \left(\alpha^{x_B}\right)^{x_A} \bmod q$, B can got $k_s = y_A^{x_B} \bmod q$ in a similar way. No one knows that x$_{A}$ or x$_{B}$ values except A and B, so that other people must calculate ks from y$_{A}$ and y$_{B}$.

Assume that B is A's neighbor node, Cert$_{A}$ and Cert$_{B}$ are certificates, respectively for node A and node B. Assume the existence of a trusted certificate authority (CA), in a wireless network contract, each node of the A provide a certificate, the certificate contains node A identity, the expiration date, the certificate authority's signature and certificate authority private key SCA. The certificate is used to verify the information, such as the public key in the certificate to prove that it is created by the special organization and belong to this organization. H ( ) is a one-way Hash function. The cut-off date of Certificate is defined by the Date, p$_{B}$ as the node of B public key, IDx is node X's identifier, $\left[h\left(ID_B, P_B, Date_B\right)\right]S_{CA}$ means to sign the $h\left(ID_B, P_B, Date_B\right)$ using the CA private key. Symbolic interpretation as shown in Table 1:

Table 1. Symbol Description

symbol	Meaning
CA	A trusted certification authority
SCA	The private key of certificate authority
Certx	The certificate of Node X
IDx	the identity of Node
yx	The Public value of node X
XA	The secret value for node A
Datex	The expiration date of the certificate
H()	A single Hash function
PX	The public key Node X

The certificate of Node A and B are show in (1) and (2).

$$Cert_B = \left\{ID_B, P_B, y_B, Date_E, \left[h\left(ID_B, P_B, y_B, Date_B\right)\right]s_{CA}\right\} \quad (1)$$

$$Cert_A = \left\{ID_A, y_A, Date_A, \left[h\left(ID_A, y_A, Date_A\right)\right]s_{CA}\right\} \quad (2)$$

$y_A = \alpha^{x_A} \bmod N$ and $y_B = \alpha^{x_B} \bmod N$ are public value node A and node B of the Diffie-Hellman key exchange method, a and N are open to the public, while x$_{A}$ and x$_{B}$ is the Diffie-Helkman key exchange method in secret. the specific process is shown in Figure 1, The encryption and authentication process is shown in Figure 2.

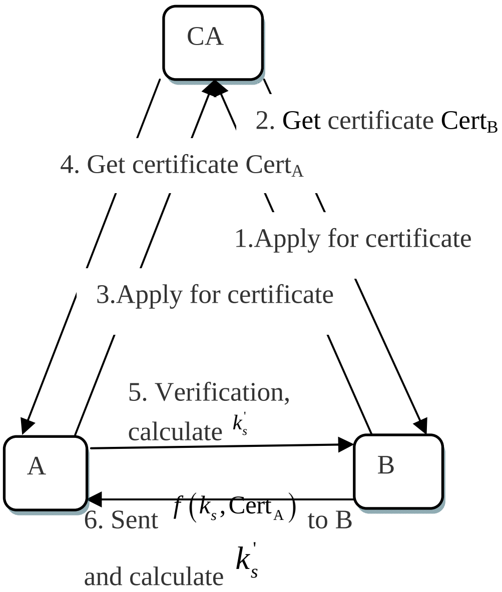

CA
2. Get certificate Cert_B
4. Get certificate Cert_A
1.Apply for certificate
3.Apply for certificate
5. Verification, calculate k_s'
A
B
6. Sent $f(k_s, \text{Cert}_A)$ to B and calculate k_s'

Figure 1. The Communication Process between Node A and Node B

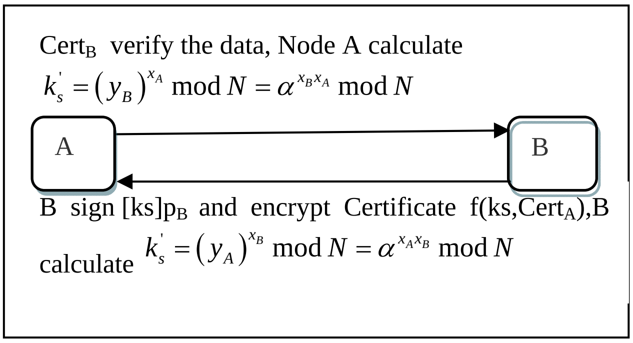

Cert_B verify the data, Node A calculate
$k_s' = (y_B)^{x_A} \bmod N = \alpha^{x_B x_A} \bmod N$
A
B
B sign $[ks]p_B$ and encrypt Certificate $f(ks, \text{Cert}_A)$,B calculate $k_s' = (y_A)^{x_B} \bmod N = \alpha^{x_A x_B} \bmod N$

Figure 2. The Encryption and Authentication Process

If node B will communicate with node A
A<-B: Cert_B
Node A need to calculate the following formula:

$$k_s' = (y_B)^{x_A} \bmod N = \alpha^{x_B x_A} \bmod N \tag{3}$$

If node A will communicate with node B.

$$A \to B : [k_s]\, p_B,\ f(k_s, Cert_A) \tag{4}$$

Node B needs to calculate the following formula.

$$k_s' = (y_A)^{x_B} \bmod N = \alpha^{x_A x_B} \bmod N \tag{5}$$

If the communication between node B and node A.

$$A \leftrightarrow B$$

It can be encrypted using the session key ks’ on the transmission of a message.

In the above protocols, generating and using a two session key ks and ks’. The introduction of another session key for the purpose of ks’ is to forgery prevention certificate was leaked after the. But the generation of this protocol drawback is that each key in the process of consultation session keys are the same. For security reasons, each key agreement are generating the same key is not safe. This is similar to the dynamic password, only changing the session key to ensure and improve the security of the system.

5. The Optimization of the Security Key Management Protocol Based on Public Key Certificate

Exchange process generated session key in Diffie-Hellman keys are the same, which makes great risk exists in the interaction process. The main factors of this defect is the two open values of y_A and y_B Diffie-Hellman key exchange process, because the two public factor has already been certification credible CA signature, resulting in the late key negotiation process in which two factors cannot be changed.

The different between optimization schemes and the above scheme is mainly for key negotiation process different leads to different session keys.

Assume that B is A's neighbor, $Cert_A$and $Cert_B$ respectively for node B and node A of the certificate, the specific process is shown in Figure 3:

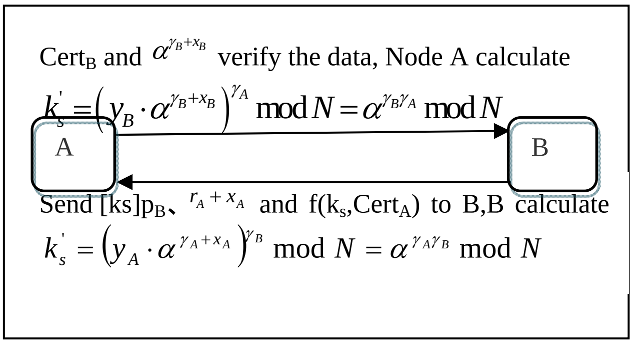

$Cert_B$ and $\alpha^{\gamma_B+x_B}$ verify the data, Node A calculate
$k_s' = (y_B \cdot \alpha^{\gamma_B+x_B})^{\gamma_A} \bmod N = \alpha^{\gamma_B\gamma_A} \bmod N$
A
B
Send [ks]p_B、 $r_A + x_A$ and f(k_s,$Cert_A$) to B,B calculate
$k_s' = (y_A \cdot \alpha^{\gamma_A+x_A})^{\gamma_B} \bmod N = \alpha^{\gamma_A\gamma_B} \bmod N$

Figure 3. The Communication Process between Node A and node B

The certificate of Node A and B are show in (6) and (7).

$$Cert_A = \{ID_A, y_A, Date_A, [h(ID_A, y_A, Date_A)]s_{CA}\} \tag{6}$$

$$Cert_B = \{ID_B, p_B, y_B, Date_B, [h(ID_B, p_B, y_B, Date_B)]s_{CA}\} \tag{7}$$

$y_A = \alpha^{x_A} \bmod N$ and $y_B = \alpha^{x_B} \bmod N$ are public value node A and node B of the Diffie-Hellman key exchange method, a and N are open to the public, while x_A and x_B is the Diffie-Helknan key exchange method in secret.

If node B will communicate with node A.

A<-B: $\alpha^{\gamma_B + x_B}$, $Cert_B$ (8)

Node A need to calculate the following formula:

$$k_s' = (y_B \cdot \alpha^{\gamma_B+x_B})^{\gamma_A} \bmod N = \alpha^{\gamma_B\gamma_A} \bmod N \tag{9}$$

If node A will communicate with node B.

A->B: $r_A + x_A$, $[k_s]p_B$, $f(k_s, Cert_A)$ (10)

Node B needs to calculate the following formula:

$$k_s^{'} = \left(y_A \cdot \alpha^{\gamma_A + x_A}\right)^{\gamma_B} \bmod N = \alpha^{\gamma_A \gamma_B} \bmod N \tag{11}$$

If the communication between node B and node A.

$A \leftrightarrow B$

It can be encrypted using the session key $k_s^{'}$ on the transmission of message.

The node B generate a random number r_B, calculated value of $r_B + x_B$, and broadcast $a^{r_B + x_B}$ and certificate. Here $a^{r_B + x_B}$ broadcast instead of $r_B + x_B$, mainly for A can save the computation of $a^{r_B + x_B}$. After receiving data transmission by node B, node A generates a random value r_A, at the same time, the node A verify the reliability of node B through node B certificate $Cert_B$ contained of y_B, If the situation is to generate the session key. Next, the node A generates a random session key k_s, encrypted cipher text and the $r_A + x_A$ and $f(k_s, \mathrm{Cert}_\mathrm{A})$ transmit to node B. So far, the node B verifies the node A, and calculates the session key $k_s^{'}$. Only when the node A and node B built this session key $k_s^{'}$, can guarantee the security of encryption information transfer between node A and node B. The Adversary of node B in the optimized scheme is unable to obtain the secret value x_A in the node A, at the same time, each session key process generates a different session keys.

In the optimization scheme node A certificate did not encrypted, because the secret information in the certificate does not contain anode. That is to say, if the node in the A secret value Ax not leaked, so no adversary can forge the node A illegal attack. Node A and node B to communicate with each other in order to calculate the same session key $k_S = \alpha^{\gamma_A + x_A} \bmod N$ at the same time transfer certificate and key exchange parameters. The pass back and forth the encrypted identity information is used to verify the session key has been tampered with, the session key can be used to encrypt the message, in order to guarantee the transmission security communication channel message can be established in a node A and node B. Our scheme is more efficient is mainly reflected in the key negotiation process with only a session key for node A, need to have the operation ability is mainly embodied in the calculation of the session key, and The computational complexity depends on the number of modular exponentiation related to the r_A.

Due to the low computing power of wireless sensor nodes and low bandwidth of wireless network, further optimize the management protocol design. The certificate of Node A and B are show in (12) and (13).

$$Cert_A = \{ID_A, y_A, Date_A, \left[h\left(ID_A, y_A, Date_A\right)\right] s_{CA}\} \tag{12}$$

$$Cert_B = \{ID_B, y_B, Date_B, \left[h\left(ID_B, y_B, Date_B\right)\right] s_{CA}\} \tag{13}$$

If node B will communicate with node A.

$$A \leftarrow B : \alpha^{\gamma_A + x_A}, Cert_B$$

Node A need to calculate the following formula:

$$k_s^{'} = \left(y_B \cdot \alpha^{\gamma_B + x_B}\right)^{\gamma_A} \bmod N = \alpha^{\gamma_B \gamma_A} \bmod N \qquad (14)$$

If node A will communicate with node B.

$$A \rightarrow B : r_A + x_A, Cert_A, f\left(k_s, [ID_A, ID_B]\right) \qquad (15)$$

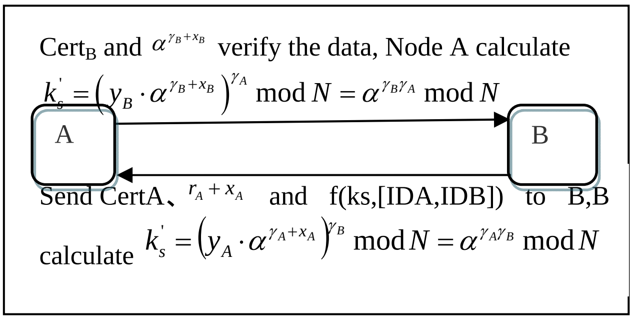
Node B needs to calculate the following formula:

$$k_s^{'} = \left(y_A \cdot \alpha^{\gamma_A + x_A}\right)^{\gamma_B} \bmod N = \alpha^{\gamma_A \gamma_B} \bmod N \qquad (16)$$

If the communication between node B and node A.

$$A \leftrightarrow B : f\left(k_s, [ID_A, ID_B]\right) \qquad (17)$$

The communication process between nodes After further optimization is shown in Figure 4:



Cert$_B$ and $\alpha^{\gamma_B + x_B}$ verify the data, Node A calculate $k_s^{'} = \left(y_B \cdot \alpha^{\gamma_B + x_B}\right)^{\gamma_A} \bmod N = \alpha^{\gamma_B \gamma_A} \bmod N$

Send CertA、$r_A + x_A$ and f(ks,[IDA,IDB]) to B,B calculate $k_s^{'} = \left(y_A \cdot \alpha^{\gamma_A + x_A}\right)^{\gamma_B} \bmod N = \alpha^{\gamma_A \gamma_B} \bmod N$

Figure 4. The Communication Process between Nodes after Further Optimization

6. Conclusion

We propose a security protocol based on certificate than the use of symmetric cryptography for key exchange protocol is more secure and more effective.

The session key Ks' generated before optimization scheme of drawback is that each key negotiation process is the same. For security reasons, each key agreement are generating the same key is not safe. This is similar to the dynamic password, only changing the session key to ensure and improve the security of the system.

Different optimization schemes in the above scheme is mainly for key negotiation process different will produce different session key. The certificate will be similar to what we usually said the password, that is to say if the certificate was leaked, then the adversary can through this similar to the password credentials to imitate the users of illegal behavior.

In the proposed protocol, node A and node B exchange certificates and other Diffie-Hellman parameters to calculate a common session key $k_s = \alpha^{r_A r_B} \bmod N$. The encryption and identity information exchange to authentication and verification of a shared session key role. Ks' can be used to encrypt the session key is exchanged through wireless channels A and E information. Our protocol advantage lies in the amount of information it requires less and only need a session key. Computation node is mainly reflected in the calculation of the session key by $r_A r_B$ computing mode screen operation corresponding to.

We propose an authentication session key for use in a variety of wireless sensor network node to node exchange protocol. Communication between two nodes should be protected each other neighbor nodes in wireless sensor network, which means that the session key exchange between them should not be exposed to other neighbor nodes in the network. When the need for mutual authentication and session key exchange these two aspects will be used when node to node communication security protocol. One side of which is communication between nodes and the wireless network, and on the other hand reflected in the communication between different nodes.

The nodes A and B are in different networks. That is to say, A's neighbor is the same B, neighbor nodes in B is C, A and B want to mutual authentication and shared the same session key when you need to use the Daffier-Hellman key exchange mechanism.

After initialization, node A and node B were certified through each other's certificate. At the same time, the visiting network also need to node A authentication, A and Diffie-Hellman parameter passed to the node, its role is to provide a communication neighbor node E and node B safely through its neighbor nodes in F mode.

In the node to a security protocol node, no secure information transmission of wireless sensor nodes to different network, which means that no one can simulate wireless sensor node. In addition, secret communication between two different nodes can also be guaranteed. Once in each set up a secure channel, node and the network without encryption operation can be appropriate to alleviate.

References

[1] Yang Geng, Xu Jian, Chen Wei. Security features and key technology of the Internet of things. *Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition).* 2010; 30(04): 20-29.

[2] Wang He, Yang Hua, Gao Fubing. Security. *Sichuan ordnance Journal of Internet of things*. 2011; (11): 90-91.

[3] Akyildiz IF, Su W, Sankarasubramansiam Y, Cayirci E. A Survey on Sensor Networks. *IEEE Communications Magazine*. 2002; 40(8): 104-112.

[4] Hao Wenjiang. Technical security issues of. *Network information security of Internet of things*. 2010; (01): 49-50.

[5] Dirk H. RFID Security and Privacy: Concepts, Protocols, and Architectures. Berlin: Springer. 2008: 107-137.

[6] Juels A. RFID Security and Privacy: A Research Survey. *Selected Areas in communication,* 2006; 24(2): 381-394.

[7] Fu Rong. Network research and implementation of security and privacy protection platform sharing, Beijing Jiaotong University. 2011.

[8] Diffie W, Hellman M. New Direction in Cryptography. *IEEE Transaction on Information Theory.* 1976; 6(22): 644-654.

[9] Kohnfelder LM. Towards a Practical Public-key Cryptosystem. MIT B.S. Thesis, MIT Department of Electrical Engineering. 1978.