The Perception Layer Information Security Scheme for Internet of Things based on Lightweight Cryptography

XiangYi Hu[12] LiPing Du[12] Ying Li[12]

[1] Beijing Municipal Institute of Science & Technology Information, Beijing, China
[2] Beijing Key Laboratory of Network Cryptography Authentication, Beijing, China

Abstract

This paper uses the lightweight (simple cryptography, high security and fast speed single-key cryptographic algorithms such as: RC4, RC5, SMS4 etc.) cryptography, and a security single-key management technology to solve the key update management problems of lightweight cryptography. In smart chip of sensor/RFID reader device and encrypt card of the authentication center in the internet of things(IoT), the device authentication, signature/verification and encryption/decryption protocols are established to ensure the device of sensing layer in IoT is credible, and sense information is credible, integral and confidential. Thus, an information security for perception layer of IoT is built.

Keywords: Internet of things (IoT), perception layer, lightweight cryptography, information security

1. Introduction

With the fast development of IoT, the security problem is imminent. Most countries carry out research in this area actively, especially the research on information security of unattended sensing devices (such as sensors, RFID reader and M2M communication equipment, etc). Our country will also carry out the exploratory research in this field, such as in the alternative project collection guide of national 863 plain in 2013, paragraph 4.1: "research on perception layer security scheme of IoT, lightweight encryption technology and authentication mechanism,… research on nodes verification of perception layer…".

The power of sensing device mainly comes from the battery, so the smart chip embedded in such device has the limitations of energy, computing power and storage space which lead to weak computation ability and small storage space. In the small smart chip, if the double key cryptographic mechanism such as RSA algorithms or ECC algorithms is used to build encryption system and security protocol, it is feasible theoretically, but it can not be achieved in practice. The lightweight cryptographic technology (simple cryptographic, high security and fast speed single-key cryptographic algorithms) is the only way to realize the security protocol and system in the smart chip.

This paper uses lightweight cryptography to build the sensing device authentication protocol, sensing information signature/encryption protocol in the smart chip of sensing device of IoT, providing the credibility of sensing devices of perception layer and ensuring reliable transmission, integrity and confidentiality for sensing information, and realizing the information security of perception layer for IoT.

2. The security architecture for perception layer of IoT

2.1. Sensing device end

A smart chip is embedded in the sensing device, and in the smart chip, the encryption system of sensing device is built. That is, the lightweight cryptography, hash algorithm and security protocols of sensing device which include authentication protocol, signature/encryption protocol are written into the smart chip. Also in the initial phase, the identity of smart chip in sensing device, the identity of sensing device and a group of transmission key are written into the smart chip.

Each smart chip in sensing device has the unique ID number, and they are different from each other. One identifier is corresponding to a sensing device and a group of transmission key.

2.2. Authentication center end

In IoT, the authentication center is composed of the authentication server and encryption card. The encryption card is inserted into the PCI interface of authentication server. IoT data center connects to the authentication center, and the data transmission between the data center and authentication center is a double way transmission. In the encryption card, the IoT authentication center encryption system is built. Lightweight cryptographic algorithms, hash algorithms and authentication center security protocols which include sensing device authentication protocol, decryption/verification protocol are written into the encrypt card. Also a group of storage key is initialized in the encryption card in the initial phase. In the key database, all the sensing devices' ID number, all smart chips' ID number and all sensing devices' transmission key cipher SKi (i=1~n, n is the sum of all the sensing devices) are stored.

3. The key management of lightweight cryptography

The security single-key technology is used to build the device authentication protocol, data signature and encryption/decryption protocol for perception layer of IoT.

3.1. The authentication/signature key

The authentication/signature key CK is generated by the hardware random number generator. When the sensing device authentication protocol or signature/encryption protocol is running in the smart chip of sensing device, the random number generator in the smart chip generates a group of random number which the length is NN bytes, and this group random number is as the authentication/signature key CK. When the CK is as the authentication key, CK is used to encrypt the other group random number S to generate the authentication code. When CK is as the signature key, CK is used to encrypt the digest value of sensing information. At the same time, CK is also as the signature key for basic information in the RFID.

3.2. Transmission Key

Transmission key SKi (i=1~n, n is the sum of all the sensing devices in authentication center) is generated by the random number generator in the encryption card of the authentication center during the key initialization. Transmission key SKi (i=1~n) is a group of random number, stored in smart chip of every sensing device. At the same time, in the encrypt card of authentication center, all corresponding sensing device's transmission key SKi (i=1~n) is encrypted by a group of storage key to SKi' (i=1~n), and the cipher SKi' (i=1~n), that is SK1',SK2',…,SKn', along with the corresponding sensing device's ID number

and the smart chip's ID number, are stored in the transmission key database of the authentication center.

3.3. Storage key

Storage key K, is a group of NN bytes random number generated by the hardware random number generator of encryption card in the authentication center. K is a fix single-key, stored in the encrypt card. K is used to encrypt the sensing device's transmission key SKi (i=1~n), and the cipher SK1',SK2'…, SKn' are stored in the transmission key database of authentication server. Simultaneously, storage key K is also used to encrypt the signature key CK of each RFID's sensing information, and the cipher CKi' (i=1~n) are stored in the signature key database of authentication center.

When the sensing device end and authentication end exchange the authentication/signature key CK, the storage key K in the encrypt card of authentication center decrypts the transmission key SKi'(i=1~n) which corresponding to the CK to SKi(i=1~n). And the SKi is used to decrypt the authentication/signature key's cipher CK' to CK.

If the sensing information cipher of RFID needs to be decrypted and verified, the storage key K in the encrypt card of authentication center is used to decrypt the RFID's signature key cipher to CK, and CK is used to decrypt and verity the sensing information cipher of RFID.

4. The Security protocol of perception layer of IoT

4.1. The authentication protocol

1) The authentication protocol in sensing device end. The sensing device authentication protocol in sensing device end follows the following steps:

First, the sensing device generates a group of random number S, and the S is inputted into the smart chip of sensing device;

Second, the smart chip of sensing device generates a group of NN bytes random number as the authentication key CK.

Third, CK is used to encrypt S to get the cipher, that is authentication code 1.

Fourth, the transmission SKi (i=1~n) encrypts the authentication key CK to cipher CK'.

Finally, 5 group of authentication data including: the identity of smart chip of sensing device, the sensing device's identity, random number S, authentication code 1 and the authentication key's cipher CK', are sent to the authentication center.

2) The authentication protocol in authentication center of IoT. When the authentication center receives the authentication data from the sensing device, the sensing device authentication protocol in authentication center of IoT follows the following steps:

First, the authentication center will locate the record in the transmission key database according the identity number of smart chip, and get the transmission key cipher SKi'(i=1~n).

Second, the SKi' is inputted to the encrypt card. The storage key K is used to decrypt the SKi'(i=1~n) to transmission key SKi(i=1~n).

Third, SKi(i=1~n) is used to decrypt the authentication key cipher CK' to CK.

Fourth, the authentication key CK is used to encrypt the random number S to authentication code 2.

Finally, the authentication center will judge the sensing device's credibility by compare the authentication code 1 and authentication code 2.

4.2. The signature protocol

1) The signature/encryption protocol for sensing information. The protocol steps

are as follows:

First, the sensing information collected by the sensing device is transmitted to the smart chip of sensing device, and is computed by hash algorithms to get digest information L1.

Second, a group of NN bytes (NN is the key length) random number generated by the hardware random generator of smart chip is as signature key CK to encrypt the sensing information and digest information L1, getting the cipher of sensing information and L1, that is digital signature.

Third, the transmission key in the smart chip encrypts the signature key CK to cipher CK'.

Finally, the ID number of smart chip of sensing device, the sensing device's ID number, the sensing information cipher, digital signature and the signature key cipher CK', all 5 group signature data are sent to the authentication center.

2) The decryption/verification protocol for sensing information in authentication center. When the authentication center receives the 5 group of signature data from the sensing device, the sensing device decryption/verification protocol in authentication center of IoT will follow the following steps:

First, the authentication center will locate the record in the transmission key database according the identifier of smart chip, and get the transmission key cipher SKi'(i=1~n).

Second, the SKi' is inputted to the encrypt card. The storage key K is used to decrypt the SKi'(i=1~n) to transmission key SKi(i=1~n) in the encrypt card.

Third, SKi(i=1~n) is used to decrypt the signature key cipher CK' to CK.

Fourth, the signature key CK is used to decrypt the sensing information cipher and digital signature to get the plain data of sensing information and digest L1.

Fifth, the hash algorithm is used to compute the sensing information to get digest L2.

Finally, the authentication center will judge the sensing information credibility and integrity by compare the L1 and L2.

3) The signature/encryption protocol of RFID.RFID is an electronic label. There is no CPU chip and no work power in the RFID. The data in RFID is written in advance and read by the RFID reader. The mainly data stored in RFID includes: the ID number B1 for RFID, the basic information LL for corresponding items. (For example, the important information for a bag of milk powder: factory, production time, ingredients, ingredients etc). The signature/encryption protocol of RFID follows the following steps:

First, a group of NN bytes (NN is the key length) random number generated by the encrypt card of authentication center is as signature key CKK for RFID to encrypt B1 and LL.

Second, CKK is used to encrypt the digest of B1 and LL (namely Q1) to get Q1 cipher, which is digital signature.

Third, the storage key K in the authentication center encrypts the signature key of RFID CKK to cipher CKK'.

Fourth, CKK' and the ID number of RFID B1 are stored into the signature key database of the authentication center.

Finally, the ID number of RFID B1, the cipher for B1 and LL, the cipher for Q1 and CKK', all 4 group data are written into RFID.

There are 4 groups of data in RFID:1) the ID number B1 for RFID. 2) the cipher for B1 and LL. 3) the cipher for Q1 which is the digest of B1 and LL, that is digital signature.4) the cipher for signature key CKK, namely CKK'. The 4 groups of data are as the sensing data CL for RFID, CL is written into the RFID in advance.

The signature/encryption protocol for sensing information of RFID reader is the

same as the other sensing device's protocol (As shown in 3.2.1). The only exception is the sensing information CL for RFID is a group of fix information which is written into the RFID.

4) The decryption/verification protocol for RFID sensing information in authentication center of IoT. When the authentication center receives the 5 group of signature data sent from the RFID reader, the RFID decryption/verification protocol in authentication center of IoT will follow the following steps:

First, the authentication center will locate the record in the transmission key database according the identity number of smart chip in RFID, and get the transmission key cipher SKi'(i=1~n).

Second, the SKi' is inputted to the encrypt card. The storage key K is used to decrypt the SKi'(i=1~n) to transmission key SKi(i=1~n) in the encrypt card.

Third, SKi(i=1~n) is used to decrypt the signature key cipher CKK' to CKK.

Fourth, the signature key CKK is used to decrypt the sensing information cipher and digital signature to get the plain data of sensing information CL and digest L1.

Fifth, the hash algorithm is used to compute the sensing information to get digest L2.

Finally, the authentication center will judge the CL's credibility and integrity by compare the L1 and L2. If $L1 \neq L2$,the sensing information CL of RFID is not credible and integrity.

If L1=L2, the CL sent from the RFID reader is credible and integrity. The authentication center of IoT will locate the record in the signature key database according B1 (the ID number of RFID) of CL, and get RFID signature key cipher CKK'. CKK' is inputted to the encrypt card. The storage key K is used to decrypt the CKK' to signature key CKK in the encrypt card. Then CKK is used to decrypt the cipher of RFID basic information LL, also the signature of B1 and LL to get the LL and digest Q1 (the digest for B1 and LL). And the hash algorithm is used to compute the data of B1 and LL to get digest Q2. Finally the authentication center will judge the credibility and integrity for B1 and LL in RFID by compare the Q1 and Q2. If $L1 \neq L2$,the sensing information CL of RFID is not credible and integrity.

5. The advantage of security protocol for perception layer

5.1. Chip based Security

The security protocol is a chip based protocol. Both the sensor end and authentication center end security protocol are performed in the hardware chip. The cryptographic algorithms, keys, security protocol and data are stored in the smart chip of sensor end and encrypt card of authentication center, so the security level for the perception layer encryption system and security protocol of IoT are improved.

5.2. Single-Key Technology

The speed of single-key algorithms is 1000 times faster than the double key cryptographic algorithms in the chip. The security single-key technology resolves the problem of key update and management when single-key algorithms used in the authentication, signature/encryption protocol for sensing devices. Also, this technology reduces the cost of single-key on updating and maintenance, and has the advantage of fast encryption/decryption speed, improves the performance efficiency of perception layer security protocol of IoT.

5.3. Large scale application

Due to large number of sensing devices in IoT, which is 32 times more than the user number in internet, storage space in authentication center of IoT is an important

factor to consider. In the authentication center end of IoT, the storage key is used to encrypt the transmission key of every sensing device or the signature key of every RFID (signature key CKK, used to sign the basic information of RFID LL), and to ensure the storage security of sensing devices' transmission key and RFID's signature key in authentication center. The authentication center does not need to purchase the large number encrypt cards to store the large number transmission key and RFID's signature key, so greatly reduce the construction cost for authentication center. Moreover, both the transmission key of sensing device and signature key of RFID only occupy 16 bytes (according to the key length), the single authentication center of IoT can manage massive (over 300 million) sensing devices.

5.4. Security Keys

The security single-key management technology ensures the security usage of three keys.

1) The original authentication/signature key is in the smart chip of sensing device and not out of the chip. In the chip, the transmission key SKi(i=1~n) is used to encrypt the authentication/signature key CK to generate the key cipher CK', and the CK' is sent to the authentication center. The authentication/signature key transmission security is ensured.

Authentication/signature key has the random characteristics and is one time one variant. It is generated by the hardware random number of the smart chip. The authentication/signature key cipher CK' is also random, and has the characteristics of one-time-one-variant, and has on regularity. The decipher cannot use the CKj'(j=1~M, M is natural) as the decipher condition, that is the "repeat"(using the same single-key to encrypt different plaintext to cipher) to decode the authentication/signature key CKj(j=1~M, M is natural), or decode the transmission key SKi(i=1~n).

2) The transmission key SKi(i=1~n) corresponding to each sensing device is stored in smart chip of sensing device. In authentication center, all sensing devices' transmission key SKi(i=1~n) are stored in the transmission key database as cipher to ensure the storage security of transmission key. All the RFID signature key is stored in the signature key database of authentication center as cipher to ensure the storage key security for all RFID's signature key.

3) The storage key K is generated in the encrypt card and is stored in the encrypt card, so the storage security and running security of storage key is ensured.

Each group of transmission key SKi(i=1~n) is generated by hardware generator during the initialized phase. The transmission key is random and is a group of rules codes. The storage key K is used to encrypt each group of transmission key SKi(i=1~n) to generate the cipher SKi'(i=1~n) which also is random and one time one variant, The SK' is a group of rules codes too. The decipher cannot use the SKi'(i=1~n) as the decipher condition, that is the "repeat"(using the same single-key to encrypt different plaintext to cipher) to decode the transmission key SKi(i=1~n), or decode the storage key K.

5.5. RFID information security

The basic information of RFID LL which is transported in the perception layer is signed and encrypted two times. First, the basic information LL is signed and encrypted to generate the sensing information CL and is written into RFID. Second, when CL is read out of the RFID reader, the signature/encryption protocol in the smart chip sign the CL and encrypt it, then sends it to the authentication center of IoT. In the encrypt card, the cipher data of RFID is decrypted and verified

two times. Thus, the sensing information read from the RFID reader is prevent to be tampered and also to prevent the basic information of RFID to be tampered with or cloned.

6. Conclusions

This paper analyzes the performance of smart chip, and proposes that the light-weight encryption technology is the only way to build the security protocol for perception layer of IoT. This scheme uses the security single-key management technology to solve the update problem for key update of lightweight cryptography. In the smart chip of sensing device end, sensing device authentication protocol for sensing device end and signature/encryption protocol are built. In the encrypt card of authentication center end, sensing device authentication protocol for authentication center end, decryption/verification protocol are built. All these security protocols ensure the sensing device credible, true and not replaced and ensure the sensing information credible, integrate, not be tampered with and confidential. Thus the perception layer information security system of IoT is established and promotes the establishment of our country's smart city.

7. Acknowledgement

This work was financially supported by Program of Network Authentication Lab affiliated to Beijing Municipal Institute of Science & Technology Information (No. PXM2011_178214_000007).

8. References

[1] Hu Xiang-yi, A Method for Device Authentication, Data Integrity and Confidential Transmission in Internet of Thing; China, 201010517919X [P]. 2010-10-25.

[2] Lei Ji-cheng, "Internet of things security technology", "Publishing house of electronics industry", 2012.6

[3] Yang Geng, Xu Jian ,Chen Wei, Qi Zheng-hua, Wang Hai-yong," Security Characteristic and Technology in the Internet of Things," "Journal of Nanjing University of Posts and Telecommunications(Natural Science)", 2010, 30(4)

[4] Sun Jian-hua, Chen Chang-xiang, "Initial study on IOT Security", "Communications Technology", 2012,45(7)

[5] Zang Jin-song, "Safety performance on Internet of Things," "Network and computer security", 2010,(6)

[6] Xiao Yi, "Study on IOT Security Management Technology", "Communications Technology",2011,44(1)

[7] Zhang Heng-yun,"A Study of Protection for Message's Safety on the Internet of Things Sensing layer","Computer Knowledge and Technology", 2011,07(19)