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

Jian Wei Guo, Na Yan, Jia Yu Chen and Shiyu Li

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.1

KEYWORDS

Internet of Things (IoT), Perception Layer, Lightweight Cryptography, Information Security

INTRODUCTION

With the rapid development of IoT application, the security problem of network solution is imminent, all countries actively carry out this research, especially the research of information security such as sensors, RFID reader and Sliteral communication equipment. Our country will also carry out exploratory

1JianWei Guo ,Na Yan, Jia Yu Chen, Shiyu Li, Beijing Institute of Science and Technology Information, Beijing Key Laboratory of Network Cryptography Authentication, Beijing, 100044.
research in this field, for example, in the 2013 National 863 Alternative Project Solicitation Guide, section 4.1, soliciting projects: "Research on the perceptual Layer security system, lightweight encryption technology and authentication mechanism, ... The identification of perceptual layer nodes, ... Because the power source of the sensor is mainly from the micro-battery, the intelligent chip embedded in the device has the limitation of energy, computing power and storage space, namely: weak computing ability and small storage space. In this small size smart chip, if the use of dual-key cryptography such as RSA or ECC algorithm, the establishment of encryption systems and various security protocols, theoretically feasible, in fact, cannot be achieved. In the smart chip can only use the lightweight password (simple password, high security, fast operation of the single key password algorithm) technology to achieve. Therefore, we propose a lightweight password, in the network sensor device intelligent chip to establish a sensor authentication protocol, sensor information signature and encryption protocol, to ensure that the network sensing layer of equipment credibility, to ensure that the sensor information transmission reliable, complete and confidential, to realize the information security of the perceptual layer of the Internet.

ARCHITECTURE OF PERCEPTUAL LAYER INFORMATION SECURITY IN IOT

Information Security Architecture For Networked Sensing Devices

Embed a smart chip in the sensor device, in this smart chip, the encryption system of the sensing device is built, i.e., the security protocol to the lightweight password, the digest algorithm and the sensor device includes: The Sensor Device authentication protocol, the signature and the encryption protocol, and the writing data: the identification of the intelligent chip of the sensor end, Identification of the sensing device and a set of transport keys.

Each sensor-side smart card chip has a unique identification, 22 different, a set of sensor-end smart chip identification corresponds to a sensor device and a set of transmission keys.

Information Security Architecture At The End of The Object-networking Authentication Center

In the IoT Authentication Center by authentication server and the encryption card hardware equipment, the authentication server PCI interface inserts the encryption card, the Thing Network data center and the Thing Network Authentication Center connection, the thing Network data center and the Thing network Authentication Center data is the bidirectional transmission, in the encryption card chip, Establishing the encryption system at the end of the Internet
Authentication Center, that is: writing the lightweight cipher algorithm, the digest algorithm, the network Authentication Center end Security protocol includes: IoT authentication protocol, decryption and signature verification protocol, and write data: A set of storage keys. The data is written in the transmission key database of the Internet Authentication Center, which corresponds to the identification of the intelligent chip of the whole sensor device, the identification of the sensing device and the ciphertext of the transmission key ski (i=1~n, the sum of the number of sensing devices).

KEY MANAGEMENT FOR LIGHTWEIGHT PASSWORDS

The device authentication protocol, digital signature and encryption/decryption protocol for the perceptual layer of IoT are established by using the security single key management technology.

Authentication or Signature Key

The authentication or signature key is CK, and the Sensing Device authentication protocol on the sensing device side, or when the signature and encryption protocol is running, the random number generator in the smart card chip of the sensor device generates a set of NN bits (the length of the nn= key) in real time, using the random number of the group as the authentication or signature key CK, When the CK as the authentication key, using CK to encrypt another set of random number s to generate authentication password, when CK as the signature key, using CK to the sensor device end of the sensor information signature and encryption. At the same time, CK is also the signature key of the basic information in RFID.

Transport Key

The transmission key is ski (I=1~n, n is the sum of all sensor devices for the corresponding authentication center), in the process of key initialization, a random number generator in the encryption card chip of the authentication center is used to generate a set of random numbers of NN bits (the length of nn= key), and the random number of the set is a set of transmission key ski (i= n), each input into the corresponding sensor device end of the smart card chip, at the same time, in the Authentication Center-end encryption card chip, using a set of storage keys, all the corresponding sensor device end of each group of transmission key SKi (I=1~N) respectively encryption to generate ciphertext, namely: SKi ' (i=1~n) after output encryption card chip, and transmits the key ski (i=1~n) to ciphertext: SK1 ', SK2 ' skn ' form, respectively, with the corresponding transmission key ski (I=1~N) the sensor device end of the smart card chip identification, and its
sensing device identification, together stored in the Authentication Center-end authentication server in the transport key database.

**Store Key**

The storage key is K, in the process of key initialization, the storage key is in advance of the random number generator in the encryption card chip of the authentication Center end. A random number that generates a set of NN bits (the length of the nn= key), which is used as a set of stored key k and stored in an encryption card chip, which stores the key K as a fixed set of keys, The storage key k is used to encrypt the transmission key Ski (i=1–n) of the sensing device end, which is stored in the transfer key database at the authentication center, after the Cheng Mi-wen is SK1 ', SK2 ', ... skn. and using the storage key K to encrypt the signature key ck of each RFID inside sensor information, encrypt Cheng Mi-wen namely: CK', store in the signature key database of the authentication Center end.

When the sensing device end is authenticated or the signature key CK is exchanged at the Authentication Center end, in the Authentication Center end encryption card chip, uses the storage key K to the authentication center side corresponding encryption CK's transmission key ciphertext ski ' (i=1–n) decrypts the plaintext, then uses the decrypted transmission key Ski (i=1–n), The ciphertext that will receive the authentication or signature key sent from the sensing device is decrypted into plaintext: CK.

If the ciphertext of the sensor information in the RFID is decrypted and the signature is verified, in the authentication Center end of the encryption card chip, the use of storage key K to authenticate the center end of the RFID signature key, namely: CK' decrypted into plaintext is: CK, and then use CK to the RFID sensor information in the ciphertext to decrypt and signature verification.

**SECURITY PROTOCOL FOR PERCEPTUAL LAYER OF IOT**

**Perceptual Layer Authentication Protocol**

1. SENSOR EQUIPMENT AUTHENTICATION PROTOCOL

Sensor Device authentication protocol for sensing equipment, generating another set of random numbers by the sensor device, set: The group random number S, the random number of input sensor device end smart card chip, smart card chip random number generator, generate a set of NN bits (nn= key length) random number, the random number as the authentication key CK, Using CK to encrypt the random number s, the ciphertext of the random number S is: Authentication password 1, then, in the sensor device end of the smart card chip, using the transmission key Ski (i=1–n) to encrypt the authentication key CK
Cheng Mi-wen namely: CK ', finally, the sensor device end smart card chip identification, sensing equipment identification, random number S, Authentication password 1 and authentication key ciphertext CK ' This 5 set of authentication data, one concurrent to the authentication Center end.

(2) AUTHENTICATION PROTOCOL FOR SENSING EQUIPMENT AT THE CENTER END OF IOT AUTHENTICATION

The authentication protocol of the sensing equipment at the end of the IoT Authentication Center, when the certification center end receives the authentication data sent by the sensing device, the authentication center is positioned in the transmission key database according to the identification of the smart card chip, and then the ciphertext of the transmission key in the record is: SKi ' (i=1~n), Enter the encryption card chip in the authentication center, and in the encryption card chip, use the storage key K to decrypt SKi ' (i=1~n) into plaintext namely: SKi (i=1~n), with SKi (i=1~n) to the received authentication key ciphertext Calvin "decrypted into plaintext, namely: CK, Using CK to encrypt random number s to generate authentication password 2, is it the same by comparing authentication password 1 and authentication password 2? To determine whether the sensor device is trustworthy.

Perceptual Layer Digital Signature Protocol

(1) SIGNATURE AND ENCRYPTION PROTOCOL OF SENSING INFORMATION

At the sensing device end, the sensing information collected by the sensing device is fed into the smart card chip of the sensor device. In the sensor-side smart card chip, the digest algorithm is used to "digest" the sensor information to get the "digest" information L1 of the sensing information, which generates a set of nn bits by the random number generator in the smart card chip of the sensing device (NN = The random number of the key, the random number as the signature key CK, to encrypt the sensor information and "Digest" information L1, to get the sensing information ciphertext and L1 ciphertext that is: digital signature, and then use the sensor device end of the smart card chip transmission key, The signature key CK is encrypted Cheng Mi-wen namely: CK ', finally, the identification of the smart card chip, the identification of the sensing device, the ciphertext of the sensing information, the digital signature of the sensing information and the ciphertext of the signature key are the 5 sets of signature data, which are sent to the authentication center side.

(2) THE SENSOR INFORMATION DECRYPTION AND SIGNATURE VERIFICATION PROTOCOL OF THE CENTER END OF IOT AUTHENTICATION
When the IoT Authentication Center receives 5 signature data sent from the sensing device, first, according to the identification of the smart card chip of the sensing device, locating the record in the transmission key database, and then inputting the ciphertext of the transmission key in the record as: SKi (i=1~n) into the encryption card chip of the authentication Center end. And in the encryption card chip, use storage key K to decrypt SKi (i=1~n) into plaintext: SKi, using SKi (i=1~n) to decrypt the ciphertext of the received signature key into plaintext: CK, decrypt the ciphertext of the sensing information and the digital signature of the sensing information with CK. Get the clear text of the sensing information and the "abstract" information of the sensing information L1, then use the abstract algorithm to "digest" The sensing information, get the "abstract" information L2 of the sensing information, by comparing L1 and L2 is the same? To verify that the sensor information transmitted from the sensing device is reliable and complete.

(3) RFID SIGNATURE AND ENCRYPTION PROTOCOL

RFID is an electronic tag, no CPU chip, no working power, the data in the RFID is written in advance and read by the RFID reader. RFID is mainly stored in the data: RFID logo B1, corresponding items of the basic information Il (such as: a bag of important information: production plants, production time, milk powder ingredients, etc.).

RFID signature and encryption protocol, in advance by the Thing Network authentication Center end encryption card chip random number generator, a random number that generates a set of NN bits (the length of the nn= key) is used as the RFID signature key Ckk to encrypt B1 and LL, while encrypting B1 and LL's "digest" Information Q1, The Q1 cipher is the digital signature, using IoT Authentication Center End storage key K, the RFID signature key Ckk encryption Cheng Mi-wen that is: Ckk ', and Ckk ' and the corresponding RFID logo B1 stored in the Internet Authentication Center of the signature key database, finally, RFID logo B1, B1 and LL's ciphertext, Q1 ciphertext, and Ckk ' 4-group data are written to RFID.

There are four groups of data stored in RFID: ①rfid's logo B1, ②B1 and LL's ciphertext, ③B1 and LL's "digest" Information Q1 cipher: digital signature, ④ Signature Key Ckk ciphertext is: Ckk ', set these 4 sets of data: RFID sensor information cl, in advance to write CL RFID.

The signature and encryption protocol of the RFID Reader End Sensing information is the same as the signature and encryption Protocol of the Sensing information of other sensing devices (see: 3.2. 1). RFID reader only read the RFID sensor information CL, is a prior to writing RFID fixed information.
(4) THE RFID SENSOR INFORMATION DECRYPTION AND SIGNATURE VERIFICATION PROTOCOL AT THE CENTER END OF IOT AUTHENTICATION

When the authentication Center receives 5 sets of signature data sent by the RFID Reader, first of all, according to RFID Card reader smart card chip identification, in the transmission key database to locate the records should be identified, and then the record of the transmission key ciphertext is: SKi ' (i=1~n) input authentication Center end of the encryption card chip. And in the encryption card chip, use storage key K to decrypt SKi ' (i=1~n) into plaintext: SKi (i=1~n), using SKi (i=1~n) to decrypt the ciphertext of the received signature key into plaintext, namely: CK, decrypt the ciphertext of the sensing information and the digital signature of the sensing information with CK, The "abstract" information L1 of the sensing information (i.e. CL) and the sensing information is obtained, then the "summary" of CL is obtained by using the abstract algorithm, and the "abstract" information of CL is L2 by comparing L1 and L2. To confirm RFID reader-side transmission of the RFID sensor information CL is trustworthy, complete, if L1≠L2, the RFID sensor information CL is not credible, incomplete.

If the L1=L2, RFID reader-side transmission to the CL trusted, complete, then in the Internet Authentication Center, and then according to CL RFID identification B1, in the Internet Authentication Center of the signature key database location. The ciphertext that corresponds to the signature key of the RFID is: CkK ' , and input encryption card chip, using storage key K to CkK' decryption into plaintext namely: CkK, with CkK the RFID basic information ll's ciphertext, as well as B1 and LL's digital signature declassified, get ll's clear text, while, get B1 and LL's " Abstract "Information Q1, then use the summary algorithm to B1 and LL" Summary, get "digest" information Q2, by contrast Q1 and Q2 is the same? To confirm the RFID inside the logo B1 and the basic information of the RFID ll is intact, has not been tampered with.

THE ADVANTAGES OF THE PERCEPTUAL LAYER INFORMATION SECURITY PROTOCOL

1. This security agreement is done in the chip hardware at both ends of the sensor terminal and the IoT Authentication Center. is a "chip-level" security protocol, and the cryptographic algorithm, key and security protocol software and data are stored in the chip hardware at both ends, thus improving the security level of the perceptual layer encryption system and security protocol of IoT.

2. in smart chip, because of the single key cipher algorithm plus, the decryption speed is 1000 times faster than the two-key cipher algorithm, and the security single Key management technique is used to solve the problem that the key-cipher algorithm is in the authentication of the sensor equipment, or in the signature and encryption protocol, which reduces the cost of the maintenance of
the single key update. It plays the advantage of fast encryption and decryption, and improves the operation efficiency of the security protocol of the perceptual layer of IoT.

3. Because of the large number of networked sensing devices, is the Internet user Volume 32 times, in the Thing Network authentication Center end, uses the storage key respectively to encrypt each sensor device end transmission key, or each RFID signature key (for the RFID inside basic information II signature key Ckk), Ensure storage security for all sensor-side transmission keys stored at the center end of the IoT authentication system, to ensure that the storage of all corresponding RFID signature keys is stored securely at the center end of the IoT authentication, and that there is no need to purchase a large number of encryption card devices to store a large number of transmission keys and RFID signature keys, Can greatly reduce the construction cost of the certification center. At the same time, the corresponding sensor device end transmission key or RFID signature key, only 16 bytes (according to the key length) around storage space, the single Thing network authentication center can manage a large amount (more than 300 million) sensing equipment.

4. Security single Key management technology to ensure the safe use of three kinds of keys.

A. The plaintext of the authentication or signature key is not the smart card chip hardware of the sensor device. In the sensor-end smart card chip, use the transmission key Ski (i=1~n) to encrypt the authentication or signature key CK, generate the authentication or signature key ciphertext that is: CK', and send CK' to the authentication Center end, to ensure the authentication/signature key transmission Exchange security.

The authentication or signature key is generated by a random number generator in the smart card chip of the sensor device. With randomness, one change, belong to a group of garbled, with the transmission key will each generation of authentication or signature key, respectively encrypted ciphertext generated by the randomness, one change, also belong to a set of garbled, irregular. The ckj (j=1~m, M is the natural number) as the deciphering condition-"duplicate" (using the same single key to encrypt multiple different plaintext messages Cheng Mi-wen messages) to decipher the authentication or signature key ckj (j=1~m, M Natural), or to decipher the transmission key Ski (i=1~n).

B. The corresponding transmission key ski (i=1~n) for each sensor device is stored in the sensor-side smart card chip. At the end of the certification center, the corresponding transmission key ski (i=1~n) in the whole sensor device is stored in the transmission key database of the authentication center in ciphertext form, which ensures the storage security of the corresponding transmission key in the authentication center of all sensor devices. All corresponding RFID signature key, is stored in the form of ciphertext in the authentication center of the signature key database, to ensure that all corresponding RFID signature key in the authentication center of the storage security.
C. Storage key k is generated in the chip of the encryption card and stored in the encryption card chip to ensure storage and operation security of the key K.

Each set of transport key Ski (i=1~n) is a key initialization of the produced by random number generator, all have randomness, and belong to a set of garbled characters, using storage key K respectively to encrypt each group of transmission key Ski (I=1~N) generated transmission key ciphertext ski ' (i=1~n), also has randomness, One change, also belong to a set of garbled. The SKi ' (i=1~n) is unable to decipher the transmission key: SKi (I=1~n), or to decipher the storage key K.

D. In the perceptual layer transmission of the basic information of the RFID II, was carried out two times signature and encryption, the first time is the basic information II signed and encrypted, the generated sensor information CL and write RFID, to prevent rfidli data leakage, was tampered with or cloned. When the sensor information in the RFID CL is read by the RFID Reader, then by the RFID Card Reader's smart card chip signature and encryption protocol, signed and encrypted into a ciphertext after the transmission to the network authentication center, in the encryption card chip, the RFID ciphertext data two decryption and signature verification, thus, Prevent the RFID reader from reading the sensor information was tampered with.

CONCLUSIONS

By analyzing the performance of the Smart chip, the scheme it is proposed that the intelligent chip embedded in the IoT sensing device can only use the lightweight encryption technology to establish the security protocol of the perceptual layer, and adopt the security single key management technology to solve the key update problem of the lightweight password, and realize the intelligent chip in the sensor device of the IoT. The Sensor Equipment authentication protocol, signature and encryption protocol are established, and the authentication protocol, decryption and signature verification protocol of the Authentication Center end are established, and the sensing equipment of the sensing layer of the object-connected network is trusted, true and not replaced. To ensure that the sensor information is reliable, intact, tamper-proof and safe-keeping, the information security system of the perceptual layer is established to escort the construction of "intelligent city" in China.

ACKNOWLEDGMENTS

REFERENCES