Research Journal of Applied Sciences, Engineering and Technology 5(19): 4722-4726, 2013
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: September 27, 2012 Accepted: December 13, 2012 Published: May 10, 2013

Research on Lightweight Information Security System of the Internet of Things

[1, 2]Ying Li, [1, 2]Li Ping Du, [1, 2]JianWei Guo and [1, 2]Xin Zhao
[1]Beijing Municipal Institute of Science and Technology Information, Beijing, China
[2]Beijing Key Laboratory of Network Cryptography Authentication, Beijing, China

Abstract: In order to improve the security of information transmitted in the internet of things, this study designs an information security system architecture of internet of things based on a lightweight cryptography. In this security system, an authentication protocol, encryption/decryption protocol and signature verification protocol are proposed and implemented. All these security protocol are used to verify the legality of access device and to protect the confidentiality and integrity of transformation data. This study analyzes the security and performance of the system.

Keywords: Internet of things, security, symmetric cryptographic algorithm

INTRODUCTION

The widely use of the internet of things can bring the convenience to people's life, improve the efficiency of work and promote the development of the national economy at the same time. But it muse also be noted that the huge security risk the internet of things brings to us. The risk brought about by the information and network becomes more urgent and complex in the internet of things. Therefore, the security issues of the internet of things will inevitably become an important factor to constraint the comprehensive development of the internet of things. The urgent problem faced is how to build a secure and reliable internet of things.

The internet of things is a large-scale information system which is composed of the sensing layer, network layer and application layer. To these three logical layers, many targeted cryptographic means and solutions have been promoted. But the internet of things is a whole application and the each layer's independent security cannot provide the reliable security by simple addition. Moreover, compared with the internet, the security of the internet of things has its own features which are as follows:

- The number of sensors and terminals in the internet of things is in large-scale
- The processing capability of the terminal devices is limited

Li *et al*. (2010) have a study on secure system architecture of iot. Liu and Hou (2011) have a study of protection for messege's safety on the internet of things. Wu (2010) study a preliminary investigation on the security architecture of the internet of things. Li (2011) study the research of internet of things security issues. Ning and Xu (2010) have a research on global internet of things' developments and it's lonstruction in china. Yang *et al*. (2010) study the security characteristic and technology in the internet of things. The security architecture of the internet of things at the technical level can be improved from the two aspects which include authentication and access control and data encryption. In recent years, according to the characteristics of the internet of things, the future development developed by the EU project research group on the internet of things clearly shows that the research direction on the security and privacy of the internet of things is the energy efficient security algorithms and low cost, safe and efficient security authentication equipment. In this case, we proposed a lightweight information security system design for internet of things based on the symmetric encryption algorithm, combined symmetric key technology and cryptographic chip technology according to the characteristics of the internet of things, as well as the advantage of symmetric cryptographic algorithm in computational complexity and power consumption. This design scheme can authenticate the server and access equipment in the system and ensure the reliability of the server end and the legitimacy of access equipment. In addition, it can protect the security, integrity and non-repudation of information transmitted between the access equipment and server.

This study designs an information security system architecture of internet of things based on a lightweight cryptography. In this security system, an authentication protocol, encryption/decryption protocol and signature verification protocol are proposed and implemented. All these security protocol are used to verify the legality of

Corresponding Author: Ying Li, Beijing Municipal Institute of Science and Technology Information, No. 138 Xizhimenwai Street, Beijing 100044, China

access device and to protect the confidentiality and integrity of transformation data. This study analyzes the security and performance of the system.

SYSTEM ARCHITECTURE

From the architecture of the internet of things, the total security demand is combination of the sensing layer, network layer and application layer. Namely, not only the each layer's security of internet of things, but also the overall security should be paid attention to. In other words, the security system of internet of things must be designed in a holistic manner and passing through three levels to ensure the confidentiality, integrity and authenticity of information in the internet of things. In this study, an information security system for internet of things is proposed, which guarantees the information security of sensing layer, network layer and application layer by authenticating the sensor, verifying the sensing information's integrity and encrypting the transmission information.

The information security system of internet of things is composed of sensor (the security chip accessed to the sensor), data center (the security component deployed in the application server) and authentication center. The system architecture is as follows:

In Fig. 1, on the sensor devices the security chip is deployed and in the security chip security protocols are put. The sensor device calls the security protocols in the connected security chip to realize the security operations. The operations include sensor device authentication (mutual authentication), upload the data signature and encrypted data (mutual signature and verification) functions etc. The security chip may be connected to the sensor device by the standard interface of 7816 or SD card. The detailed information is showed in Fig. 2. The circuit board is the development board for sensing equipment and the red box section in the circuit is the embedded security chip.

In data center, a security module is deployed to be called by the application server, which is a bridge between the data center and authentication center. The data center receives the data uploaded from the sensors, sends part of the data which need to be handled by security operation to authentication center through security module and receive the result returned from the module. Simultaneously, the data center can get the security operation data from the authentication center by the security module and forward it to the sensor to initiate a security request.

The authentication center is built in the system background. The key seeds and security log are stored in authentication center. The authentication center's functions is to distributes the key, store the terminal key seeds, record the log and exception information and execute the security mission according to the security operation received from the security module, including

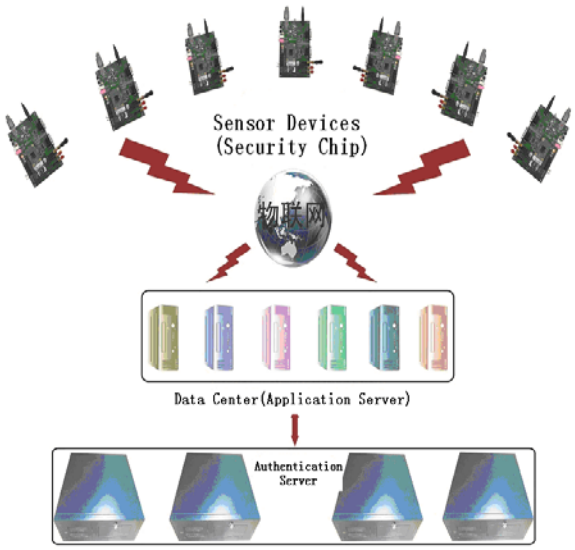

Fig. 1: The information security architecture of internet of things

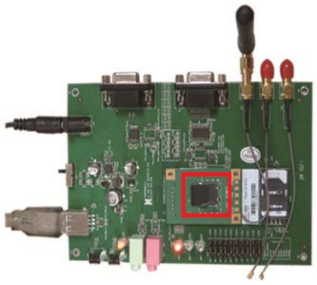

Fig. 2: The sensor end in security system

the mutual authentication, signature and signature verification, encryption and decryption.

SECURITY PROTOCOL

Because of the constraints of sensor's computation capacity and energy in the internet of things, only the faster symmetric cryptographic algorithm and Hash technology and corresponding lightweight security protocol are used in the internet of things. The security protocol in the internet of things is based on the symmetric cryptographic algorithm SM1 and Hash algorithm SM3 which are simple and practical. Also these algorithms take up less space, have small amount of computation and faster speed, all these are very suitable for the terminal equipment of internet of things which demands low power operation.

The security protocols for information security system of internet of things are stored in the terminal's security chip and encrypt card of authentication center. The core of security protocols use a key generate algorithm, the combined symmetric key technology, to realize the equipment authentication, data signature and

verification. The CSK technology has advantage of faster speed and less space which can ensure the core protocols to run in the chip.

The combined symmetric key: The core of CSK is creating the small size of key seed at first. And with the participation of time stamp and random number, a large-scale set of keys can be generated through a kind of mapping which combine and compute the key among the collection of key seeds. The same key seeds with different time stamp and random number can get the different key, which ensure the key is changed each time. Through the CSK technology, the large-scale key management can be simplified the management of small-scale key seeds.

Authentication protocol: The identity authentication in the sensing layer of internet of things is very important. The terminals of internet of things generates the identity authentication information on time and upload it to the server. If the server does not accept the authentication code from the sensor, a judgement can be made that the sensor is be stolen or damaged. When the authentication code is received, it will be authenticated by the authentication center. If the authentication is failed, the server can confirm one of conditions appeared as follows: the sensor device is damaged, the information is loss, the sensor is illegal or the information sent by the sensor is incredible. If the authentication success, the sensor's working state is normal and the information transmitted is credible.

The signature/encryption and signature verification/decryption protocol of upload data: The digital signature and verification mechanism can ensure the transmitted, received or stored data is integrated and not to be tampered with. The tampered data can be discovered timely. It is very important in the information security building of internet of things to protect the data integrity which sent by sensor terminals.

In the internet of things, when the sensor node uploads the data collected to the server, the data signature to the collected information can be computed to avoid the malicious tampered. When the server received the uploaded information from the sensor node, the signature of information can be re-calculated to judge whether the information has been tampered with. If the signature verification failed, the information has been tampered with and the information is not credible.

The non-repudiation of data can be realized by confirming the identity of data sender. The digital signature mechanisms can not only guarantee the integrity of the information transmitted, but also confirm the identity of the sender and prevent the sender's repudiation. Thus, The digital signature and signature verification of uploaded data are implemented by the sensor nodes and authentication center to enhance the anti-repudiation of transmitting information.

The network layer of internet of things realizes the transmission and communication of information. In order to protect the security of data transmitted over the network, at first the transmission reliability of network must be improved, secondly, the transmitted data must be encrypted and transmitted in the way of cipher text, so as to improve the security of the data during transmission.

The digital signature/encryption and signature verification/decryption protocol of control instructions: In the internet of things, the data center can control the sensor behavior or change the status of senor devices by sending the operation instructions to the sensor devices. If the instruction data is intercepted, the information may be leaked and hackers can even change the control demand to the sensor device and disrupt the operation of sensor devices. So, the control instruction data is needed to be protected in the ways, such as data encryption, integrity check and non-repudiation check.

When the data center sends the control instructions to the sensor devices, the authentication center will sign and encrypt the sent data firstly, then the digital signature, data cipher and corresponding data will be sent to the sensors. The sensor devices decrypt and verify the received data by the security chip. Through the verification the sensor can judge whether the operation instruction is correct and perform the corresponding control operation according to the correct instructions.

SYSTEM SECURITY ANALYSIS

Hardware encryption device: Hardware encryption device as a universal key storage and management equipment can effectively ensure the security of the key storage. Hence, in the implement of transmission protocol, hardware cryptographic devices of same encryption mechanism are set on both ends of the communication in this article, e.g., encryption card is set on authentication center and security chip on sensor ends. The Hardware encryption device of strong anti-attack ensure the security of pre-stored data used in transmission protocol.

Lightweight security protocol: Limited to the computing capability and energy of sensor devices, only lightweight algorithms and protocols, such as symmetric encryption algorithm, HASH algorithm and lightweight security protocols based on the above algorithm, can be used in the sensor devices. The protocols put forward in this study based on symmetric

ciphers SM1 and Hash technology SM3 is simple and practical, which possess a property of rapid execute speed and little space and meet the requirement of large scale subsequent security tasks in the Internet of Things.

Lightweight security protocol is stored and proceed in the chip of hardware encryption device, which possesses a property of rapid speed and higher security.

Symmetric key management: In the security protocol of system, a symmetric cryptographic algorithm SM1 is used to encrypt and decrypt data. The management of symmetric ciphers key, such as distribution, store, update, is recognized difficult to resolve. In this study, this problem is solved by usage of hardware encryption device. Key data seeds and key generate algorithm is pre-stored in security chip, the generating process of Symmetric ciphers key is also proceed in security chip. One-time Symmetric ciphers key is generated by key generate algorithm in the effect of time and random factor. Using hardware encryption device ensures the security of Symmetric ciphers keys and key generate algorithm which generates one-time key make key update Not necessary.

Audit log: When Information security systems is running, the system will write into the log database of authentication center the day-to-day behavior, emergencies, anomalies recording, which make system management staff find abnormal reasons easily.

Sensors device authentication logs and data signature verification logs are also stored in a database table of authentication center. System managers can view the logs by management platform to observe the operation of the system and sensor devices.

SYSTEM PERFORMANCE TESTING

In the process of Laboratory testing, the test content is focus on performance of the authentication center, because compared with the internet, the internet of thing access so more nodes that generates a very high level of the number of security tasks need to be handled. So, the execution speed of the authentication center is crucial for the security of the Internet of Things. In the other hand, the performance of sensor devices is not included in the test content because in the sensor device end, low complexity and low power consumption is more concerned about instead of the execute speed of security protocol. Test environment as shown in Table 1.

In the database of authentication center, the simulation data of 30 millions sensor device are stored.

Test Method: security subsequent tasks are sent to the authentication center 5 times by the data center. Each time 20000 authentication or signature verification requests are sent and completion times are recorded in seconds. The test data are shown as Table 2.

Table 1: Test environment

Terminal	Authentication center	Data center
Hardware Environment	Intel 1.86 *4/2G/250GB+1 TB, domestic encryption card	Intel 2.33G*2/ 2GB/ 250GB
Operating System	Windows 2003	Windows 2003
Software Environment	SQL Server 2000	JDK 1.5, Tomcat 5.0

Table 2: Test data

Task style	Authentication	Signature verification
Completion time1:	39.42	48.17
Completion time1:	39.30	47.36
Completion time1:	39.46	46.33
Completion time1:	40.08	47.78
Completion time1:	39.39	44.19
Average completion time:	39.53	46.77

The test results show that the average completion time of 20000 authentications by Security authentication center is 39.53 seconds and that of 20000 signature verifications is 46.77 sec.

CONCLUSION

In this article, information security system for the Internet of Things is designed, with lower construction cost, high efficiency and less maintenance related to regular implements. In which Lightweight protocols of chip level is used to protect data transmitted over network ,symmetric encryption mechanisms is used to improve the efficiency of the system and the scale of management equipment and a combination key generation techniques to solve symmetric key distribution and management problems.

According to laboratory tests, System can accomplish 20000 subsequent authentications within 40 sec and 20000 subsequent signature verification within 50 sec, it means, a day 72 million authentication tasks or 43.2 million signature verification tasks can be completed. In addition, the speed of system can be Substantial increased by using advanced hardware device. With above data, a authentication center can manage the number of ultra-large-scale (10 million level) sensing device and the system can manage the scale sensing devices. To test and improve the system is important future research directions.

ACKNOWLEDGMENT

The authors wish to thank the helpful comments and suggestions from my director and colleagues in Beijing Key Laboratory of Network Cryptography Authentication. This work is supported by the Program of Network Authentication Lab affiliated to Beijing

Municipal Institute of Science & Technology Information (No. PXM2011_178214_000007).

REFERENCES

Li, Z., 2011. The reserch of internet of things security issues. Netw. Comput. Secur., 10: 57-59.

Li, G., Y. Bo and S. Yan, 2010. Study on secure system architecture of IOT. China Inform. Secur., 12: 73-75.

Liu, J. and Y. Hou, 2011. A study of protection for messege's safety on the internet of things. Microcomput. Appl., 32(1): 15-19.

Ning, H. and Q. Xu, 2010. Research on global internet of things' developments and it's lonstruction in China. Acta Electron. Sinica, 38(11): 2590-2599.

Wu, C., 2010. A preliminary investigation on the security architecture of the internet of things. Bull. Chinese Acad. Sci., 25(4): 411-419.

Yang, G., J. Xu, W. Chen, Z. Qi and H. Wang, 2010. Security characteristic and technology in the internet of things. J. Nanjing Univ. Post. Telecommun. Nat. Sci., 30(4): 20-29.