Research on Secure Transmission Scheme in Wireless Sensor Network

Ying Li, Xiangyi Hu, Liping Du, Jianwei Guo
Beijing Municipal Institute of Science & Technology Information,
Beijing Key Laboratory of Network Cryptography Authentication
Beijing, China
shai_wang@hotmail.com

***Abstract*—In order to achieve secure communication in WSN, a lightweight encrypting transmission scheme based on symmetric cryptographic algorithm is proposed. In the scheme, a combined secret key generation algorithm is used to generate one-time secret key, hardware encrypt device is used to distribute symmetric secret keys and establish secure transmission protocol. The experiment results show that the scheme is with high execute speed and low energy consumption, and clearly superior to popular protocols.**

Keywords-wireless sensor network; transmission; symmetric cryptographic algorithm

I. INTRODUCTION

In recent years, wireless sensor network as an important branch of the Internet of Things (IoT) is gradually applied in many fields, such as smart home, intelligent buildings, intelligent transportation, environmental monitoring, etc.. Along with the development of WSNs in sensitive industries and intelligent home, the collected information more and more involved in business secrets and personal privacy. The Cluster of European Research Projects on the Internet of Things (CERP-IoT) developed in 2009 its Strategic Research Agenda (SRA), in which security and privacy technologies are described as important IoT enabling technologies [1] .

In order to secure the confidentiality of information, some security measures need to take, of which the most effective one is to transmit data in cipher text. A few security measures popular in internet security system can still play a role in the WSNs after adjustment according to the requirement of WSNs. In WSNs most of the nodes are deployed in unattended environment, with limited hardware resources (finite energy and narrower communication bandwidths), hence the transmission protocol applied on the nodes must be with feathers of high speed and low energy consumption [2].

The most popular trusted transmission protocol in Internet is SSL protocol in which both of symmetric cryptography and asymmetric cryptography are used. In SSL protocol, a CA center must be established first to achieve distribution and verification of certificate, public key and private key. When protocol works, several rounds of consultations run to determine encryption key (symmetric key). In these consultations all data is encrypted by certificate, public key and private key to ensure safety. After consultations, encryption key is used to encrypt transmitted data.[3] SSL protocol is not suitable for WSN applications for its disadvantage of high complexity, long consultations process and more additional data. In 2007, the concept of lightweight CA was put forward [4], in which the amount of communication of consultations is reduced while the safety is preserved through the pre-distribution of part of public key and fusion of certificate and public key. However, even if further simplified, three rounds of challenge-response are still required to generate a session key in consultations and a large amount of calculations are inevitable in the process of public key generation[5]. In Some scheme, the public-private key pair can be pre-stored in the security chip to shorten the time of encryption and decryption by leaving out public key generation [6], and the secret key can be generated randomly and send attached to transferring data after encrypted with the public key to omit consultation process. But because of the disadvantages of asymmetric cryptography, such as high complexity is, long packet length, the scheme can't meet the requirement of WSNs. Symmetric cryptographic have inherent advantages in encryption and decryption, but the key management is difficult to solve which limits its usage.

In this paper, a transmission scheme based symmetric cryptosystem is proposed. The mainly research of the scheme is to achieve distribution and management of symmetric secret keys through using encryption devices and secret key generation algorithm, and establish the lightweight transmission protocol to secure the confidentiality of data transmitted in WSNs. Section 4 analyzes the scheme and section 5 points out the future research directions.

II. SECRET KEY GENERATION AND MANAGEMENT

In secure transmission encryption is the most effective way and in encryption technology key management is the core problem to solve. In public key cryptosystem, the encryption key PK (public key) and decryption key SK (private key) is inconsistent, and it's very difficult to deduce SK from PK which make it easy to distribute and manage the secret key and to establish secure protocol[7]. Symmetric encryption algorithm is clearly superior to asymmetric encryption algorithm on the speed of encryption and decryption. For example, 3DES, mainstream symmetric algorithm, is 100 times faster than mainstream asymmetric algorithm of RSA when implemented by computer program.[8] If implemented by electronic circuit, 3DES can be even one thousand times faster than RSA. Whereas, how to manage symmetric key is always a difficult problem to achieve [9]. In the article, hardware encryption devices and

Published by Atlantis Press, Paris, France.

key generation algorithms are utilized to solve the problems of secret key distribution and management which make it possible to apply symmetric cipher mechanism in WSNs.

The core idea of secret key generation and management is: key elements of each node are generated by the management center, stored in the sensor node end and management center. While data transferring , a one-time secret key is produced by key generation algorithm from key elements. Key elements stored in sensor nodes are various and a large number of secret keys are produced by selected and combined from key elements of 256 bytes.

A. *Key elements generation and pre-storage*

Hardware equipment is generally used to store secret key efficiently and encrypt data by digital circuit[10]. In the solution, hardware equipment is applied to generate and pre-store key elements: an encrypt card with standard PCI is plugged in management center, and a security chip in sensor end.

In the Initialization process of sensor nodes, 256 bytes random sequence are produced as key elements by encryption card deployed in management center. In sensor end, The random sequence is pre-stored in security chip which is embedded in sensor through the interface of 7816 or standard SD. In management center, they are saved in a database after encrypted to cipher text by storage secret key stored in encryption card.

B. *Symmetric key generation algorithm*

The principle of the symmetric key generation algorithm is that a secret key aggregate on a big scale is generated by given key elements of a small scale according to a special formula. Symmetric key elements are a set of 256 elements of byte type, each of them occupies one byte. All the elements construct a 16*16 matrix, described as A, as follow:

$$A = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,15} \\ a_{1,0} & \cdots & \cdots & a_{1,15} \\ \cdots & \cdots & \cdots & \cdots \\ a_{15,0} & a_{15,1} & \cdots & a_{15,15} \end{bmatrix} \quad (1)$$

Assume M_i ($0 \le i \le 15, 0 \le M_i \le 15$) and N_i ($0 \le i \le 15, 0 \le N_i \le 15$) are both sets of 16 elements, and element value is in the range of 0 to 15. M and N are generated by Hardware random number generator and participate in the process of key generation as important parameters.

$$R[i] = A[M[i], N[i]] \quad (2)$$

Assume R_i ($0 \le i \le 15, 0 \le R_i \le 15$) is a set of 16 elements of byte type, and it is just the secret key what we intend to get. Here a simply model is given: according to (2), each element of R_i can be calculated According to M_i as row offset and N_i as column offset. Because M_i and N_i are produced by randomizer every time, R_i varies every time. Through symmetric key generation algorithm, the large-scale key management can be simplified to the management of small-scale key elements [11].

III. SECURE TRANSMISSION SCHEME

A. *Transmission system architecture*

In the article, transmission system architecture consists of two parts: management center and sensor end. A security chip is embedded in sensor end in which key elements, the transmission protocol and a specific cryptographic algorithm are pre-stored.

Data is acquired in sensor node and transmitted to management center and the management center received transmitted data and decrypted it to clear text. The manage center contains key database, log database and encryption card. Encryption card is used to store cryptographic algorithms, transmission protocols and storage key, key databases to store secret key elements in cipher text and log database to store the log of encryption and decryption information of transmitted data.

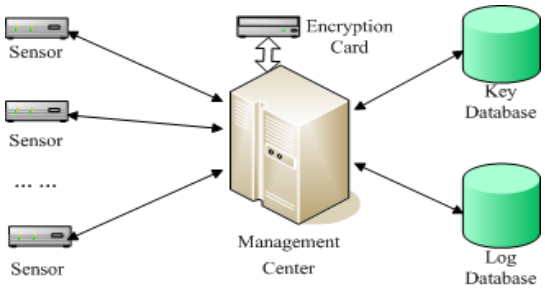


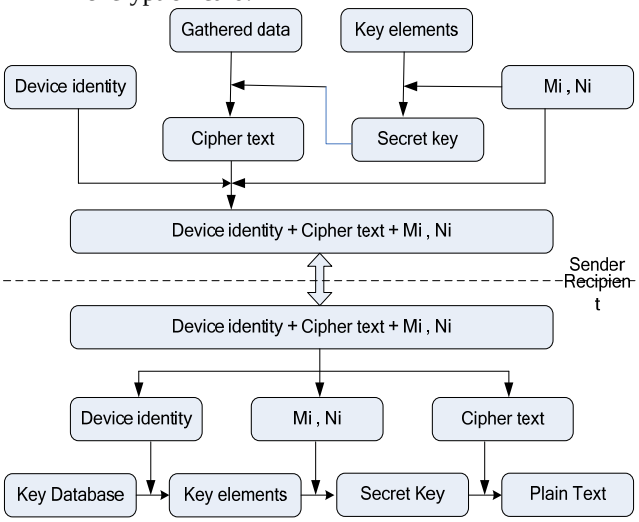
Figure 1. System architecture

B. *Transmission protocol*

When transmission protocol runs, gathered data is encrypted by security chip in sensor node end before transmitted in WSNs. When the server-side receive the cipher text, it's decrypted by encryption card to clear text. The protocol described as follows:

- Data is gathered by sensors and input into security chip plus device identity of sensor as D1.
- Mi and Ni is generated by Hardware random number generator in security chip;
- Mi and Ni is input into secret key generation algorithm to produce encryption secret key R1;
- Input data D1 is encrypted to cipher text S1 with R1.
- The device identity, Mi, Ni and S1 are combined into encryption result L1.
- Sensor gets L1 from security chip and sends it to management center.
- Management center receives L1 and splits it into device identity, Mi, Ni and data cipher text S1;
- The cipher text of Secret key element is taken out from key database by device identity.

- In encryption card, encryption key R2 is generated with secret key elements, Mi, Ni and secret key generation algorithm.
- In encryption card, S1 is decrypted to clear text D2 by the secret key R2.
- Management center get clear text D2 from encryption card.



Transmission protocol

In the implementation, a data fingerprint can be attached to gathered data to ensure the correctness and integrity of the transmission data.

IV. ANALYSIS

In this article, we will compare the scheme with the simplified transmission protocol based on light weight CA Center mentioned above, recorded as T-3DES and T-RSA. In the experiment, a SZD-35 SDKey produced by Haitai Company is employed within which RSA and 3DES cipher algorithms are fixed. In the initial process, public key of RSA and symmetric key elements of 3DES are written into secret key files of SDKey.

- T-RSA Scheme: Symmetric cryptography 3DES is used to encrypt gathered data and secret key of 3DES is encrypted by public key of RSA. In CA center, the corresponding private key which will be used to decrypt secret key is found by device identity. The transmitted data generated by the sensor end consists of device identity, the cipher text of gathered data and the cipher text of secret key.
- T-3DES Scheme: Symmetric cryptography 3DES is used to encrypt gathered data and the secret key is generated by control parameters Mi and Ni. In the management center, the corresponding secret key elements are also located by device identity. The transmitted data generated by the sensor end consists of device identity, the cipher text of gathered data and the control parameters of Mi and Ni.

Sensors of WSN have some notable features of small space and low energy. In the scheme, the security operation is implemented in security chips in which there is enough memory to store variable cipher algorithm, security protocol and pre-stored data, so the testy emphasis on computational speed and additional communications bandwidth of scheme which decide the additional energy consumption.

A. *Computational speed*

According to the energy consumption formula W = U * I * t, in which U is node current voltage, I is operating current in turning off the wireless module, t is the desired time for encryption or decryption operations, when sensor node is in a steady state, computational speed determines how much energy is consumed in the encrypting process.

Resume four groups of data gathered by sensor will be encrypted, the lengths of them are respectively 16 bytes, 32 bytes, 48 bytes and 64 bytes. The execute times of encryption are shown in table 1.

TABLE I. EXECUTE TIME

Scheme name	Length of clear text			
	16 bytes	*32 bytes*	*48 bytes*	*64 bytes*
T-3DES	0.499971	0.571125	0.648391	0.752066
T- RSA	60.14415	60.1787	60.1279	60.7031

The unit of execute time is ms

B. *Additional communication bandwidth*

According to the literature, The energy consumption in the radio transmitting is described as formula: , [12] EFM 3 * 10-12.it is clearly seen that, given a certain distance, the energy consumption of radio transmission is proportional to communication bandwidth.

The both of cryptographic algorithms used in the experiments are based on packet encryption, which means when plaintext length is less than the packet length (secret key length), the plain text must be made up until its length equals to packet's before encrypted. In the experiments, secret key length of 3DES is of 16 bytes, and the key length of RSA is of 128bytes. Sensor device identity is 8 bytes in length. In order to reduce the communication bandwidth, control parameters Mi and Ni can be compressed into 8 bytes. So, according to the description above, the additional transmitted data length after encryption are shown as Figure 3.

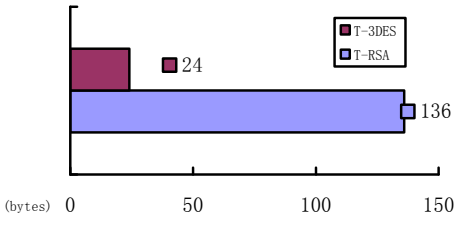


Figure 2. Additional data length

C. *Security analysis*

In cryptography, in order to guarantee the security, the key can't be unchanged for a long time. In CA center

implementation, key pairs of sensors are demanded to update every three months or earlier. However, due to a large number of sensors access to network, it‘s very difficult to update the key pairs. So the key pairs will not change which makes the protocol unsafe. In the scheme proposed in this paper, secret key is one-time key and can meet the requirement of security.

From above analysis it can be known that the energy consumption in computational speed of T-RSA is nearly 100 times to that of T-3DES while the energy consumption in additional communications bandwidth of T-RSA is 6 times to T-3DES’s, at the same time due to ease of maintenance T-3DES is more secure than T-RSA. Thereby, compared with schemes based on asymmetric cryptographic algorithm like T-RSA, the scheme put forward in this paper is more suitable for wireless sensor networks.

V. CONCLUSION

In this paper a lightweight transmission scheme is presented. Some experiment has been done and experimental results show that compared with popular transmission technology, the scheme is applicable to the wireless sensor network for the advantage of fast speed, low energy consumption and high security. Now this scheme has been applied successfully in some case. Next performance test will be carried out for WSN with large-scale nodes.

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

[1] Huanshen Ning, Qunyu Xu, 2010,” Research on Global Internet of Things' Developments and It's Lonstruction in China”, ACTA ELECTRONICA SINICA, vol.38(11),PP 2590-2599 .

[2] Huanshen Ning, Qunyu Xu, 2010,” Research on Global Internet of Things' Developments and It's Lonstruction in China”, ACTA ELECTRONICA SINICA, vol.38(11),PP 2590-2599

[3] Stephen A.Thomas. SSL & TLS Essentials Securing the Web. Wiley Computer Publishing John Wiley &Sons,Inc.,2000.

[4] Xiaolei DONG, Licheng WANG, Zhenfu CAO.”New public key Authentication with lite certification authority” [EB/OL]. http://eprint.iacr.org/2006/154.

[5] Yun Pan,Licheng WANG, Zhenfu CAO,Jian Li.” Lite-CA based key pre-distribution scheme in wireless sensor network”. “JOURNAL ON COMMUNICATIONS”, 2009, 30(3),PP130-134

[6] Xiaoyu Yuan,Qishan Zhang.” The Key Question Analysis of RSA Digital Signature Algorithm Based on Smart Card”,” ACTA ELECTRONICA SINICA”, 2004, 32(11) ,PP1897-1900

[7] Xiaofeng Chen,Yumin Wang,” A survey of public key cryptography”,” JOURNAL OF CHINA INSTITUTE OF COMMUNICATIONS” , 2004, 25(8),PP109-117

[8] Du Lijian Tang Xiaoyan Li Shourong,” Comparative Studies of Information Encryption Algorithms”,” NETWORK SECURITY TECHNOLOGY & APPLICATION”, 2006, (8),PP88-89

[9] D.G. Feng, Computer Communication Network Security, Tsinghua University Press, Beijing, 2001.

[10] K.J Zhou and X.L. Zuo , “Network Data Security System Based on Des and RSA”, Computer Engineering and Applications, North China Computing Technology Institute, Beijing, 1998.9, pp.12-13.

[11] Guifen Zhao, Xiangyi Hu, Ying Li, Liping Du. Implementation and testing of an identity-based authentication system. 2009 ISECS International Colloquium on Computing, Communication, Control, and Management, Sanya, 2009.8. pp. 424 - 427.

[12] Ning Jin, Daoyuan Zhang, Jianqiao Gao, Zhaofeng Wang, ”A Study on the Application of Symmetric Ciphers and Asymmetric Ciphers in Wireless Sensor Networks”. ” Chinese Journal of Sensors and Actuators”, 2011, 24(6).PP874-878