Chapter 19
Secure Measuring and Controlling Methods Embedded SM4 Algorithm for Smart Home

Xiangdong Hu, Xiaopeng Qin and Haiming Mou

Abstract Smart home based on the Internet of things is gradually changing our daily life, while it faces such serious problems as secure measuring and controlling to appliances and protection of end user's privacy. To guarantee the safety and reliability of smart home system, a secure measuring and controlling method embedded the domestic SM4 cryptographic algorithm for smart home is proposed in this paper, which integrates such secure mechanisms as access control based on the physical addresses of smartphone terminal or sensor nodes used in measuring and controlling operations, authentication based on the keys used in the encrypted transmission of instructions of measuring, and controlling and abnormal detection based on analysis of data. On such basis, the comparison in performances is carried out by secure measuring and controlling methods embedded domestic SM4 algorithm or typical AES one. The results of test suggest that the proposed secure measuring and controlling methods for smart home is feasible and effective, and the delay time consumed in information processing of the proposed method is only 2.5 % more than the currently pervading ones without secure mechanism. The rate of delay based on the SM4 algorithm is about 4 % less on average than the original AES one embedded in nodes, and SM4 algorithm owns independent intellectual property right with more flexible in realization of system.

Keywords Internet of things · Smart home · Safety · SM4 algorithm · Measuring and controlling

X. Hu (✉) · X. Qin · H. Mou
College of Automation, Chongqing University of Posts and Telecommunications,
Chongqing, China
e-mail: huxd@cqupt.edu.cn

Z. Deng and H. Li (eds.), *Proceedings of the 2015 Chinese Intelligent Automation Conference*, Lecture Notes in Electrical Engineering 336,
DOI 10.1007/978-3-662-46469-4_19

19.1 Introduction

With the rapid development of the Internet of things, more and more smart home are connecting various kinds of household electrical appliances or sensing devices together through local family networks, and easily and efficiently controlling them by technologies such as computer, communication, measurement, and control for a more comfortable living environment [1]. Smart home brings people much convenience while it faces many potential risks of malicious attacks, such as injecting unauthorized control instructions into system or eavesdropping information of monitoring and so on, which will further threaten safe and reliable operations of smart home or users' privacy [2].

The current smart home industry in China is still in its infancy. There are no unified national standards or technical specifications, and its standards in safety are blank. Security problems of smart home based on the Internet of things technology need to be urgently solved to improve people's experience of living [3].

A building method of security-focused smart home embedded domestic SM4 cipher algorithm is proposed in this paper, which is helpful to deal with the potential risks in information security for smart home.

19.2 The System Model of Secure Smart Home

19.2.1 The Composition of Secure Measuring and Controlling System

The composition of secure measuring and controlling system in smart home is illustrated in Fig. 19.1.

The secure measuring and controlling system mainly includes a WiFi gateway, primary or secondary routing nodes, measuring and controlling nodes, and household appliances and devices. Measuring and controlling nodes are the fundamental part of smart home, their main tasks are to sense the environment of home, or to receive commands so as to control corresponding appliances or devices such as air conditioner, digital TV set, refrigerator, curtain, lighter, monitor, alarm, etc. The secure algorithm is stored in nodes, and all communications within the smart home systems are protected by SM4 block encryption algorithm. Moreover, when intrusion detection finds an illegal node or abnormal case, the alarm node will be activated and the host or hostess will receive a notice of alarm about the incident [4].

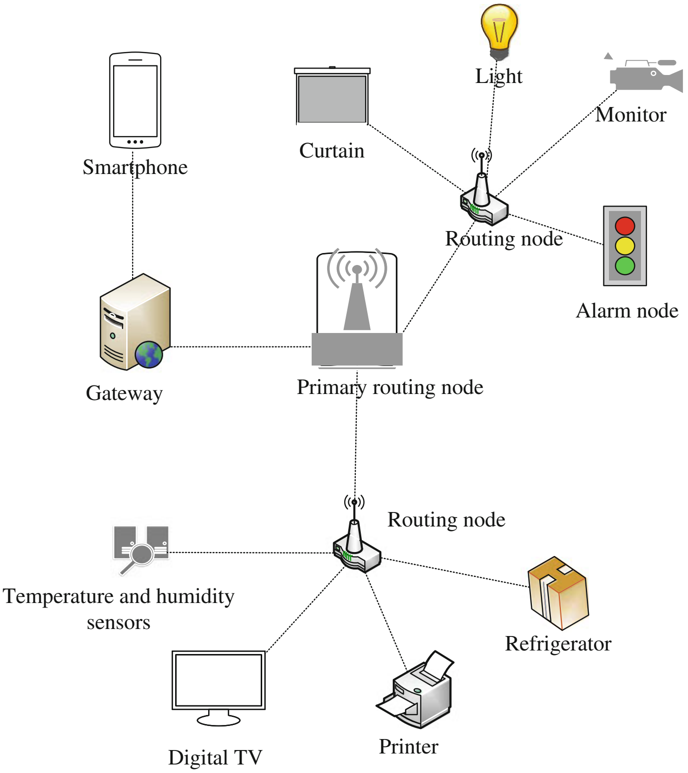

Fig. 19.1 The composition of secure measuring and controlling system in smart home

19.2.2 Security Mechanism

In order to ensure safe and reliable operation of smart home system and to protect users' privacy, here a secure measuring and controlling method embedded SM4 algorithm for smart home is proposed. The involved security mechanism is as follows: First of all, an access authentication is necessary to login system by the authorized user identity and password; Secondly, any node will be examined and verified based on the physical address and the preset key before they can access the network, and the unverified nodes will be excluded; Thirdly, each measuring and controlling instruction or message transmitted between nodes will be encrypted by SM4 cipher algorithm to improve the confidentiality of smart home system [5]; Finally, further security can be reached along with intrusion detection and alarm mechanism.

19.3 Implementation of Secure Measuring and Controlling System and Performance Evaluation

19.3.1 Hardware Implementation of the System

In order to verify the feasibility of smart home characterized in secure measuring and controlling, CC2530 chip is chosen as the core unit and a star topology structure is adopted to set up a simulation platform of secure smart home shown in Fig. 19.2 [6, 7].

As the human–machine interface of secure smart home system, the smartphone terminal based on Android4.0 is mainly responsible for sending measuring and controlling commands and receiving information from nodes including controlling and sensing ones. The WiFi gateway is responsible for two-way Zigbee signal conversion between the smartphone terminal and routing nodes. The routing node is responsible for establishing Zigbee network. The terminal node is used for connecting and controlling various kinds of household equipments. In addition, a simulated malicious terminal mainly acts as illegal invasion node to simulate intrusion behavior [8, 9].

19.3.2 Secure Measuring and Controlling Process

The secure measuring and controlling method is designed into APK (Android Package) software based on Android 4.0 smartphone terminal by dedicated Eclipse V22.3 development tools. The domestic SM4 cipher algorithm is embedded into the control software to compare with the original AES one. The secure measuring and controlling process of smart home is divided into two paths based on different

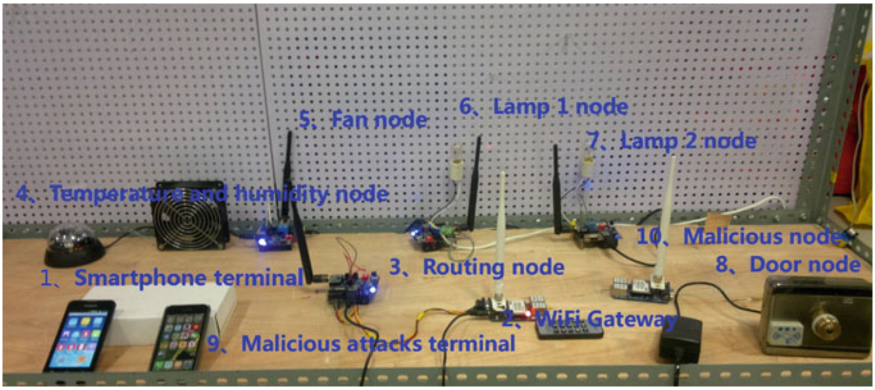

Fig. 19.2 Secure smart home system

functions of nodes: data acquisition and object controlling, as illustrated in Fig. 19.3.

To create a new SM4 function in Java file under Android platform, the statement of SM4 algorithm is: SMS4 sm4 = new SMS4 ().

An example of *key* used in SM4 is:

byte[] *key* = {*0x*01, *0x*23, *0x*45, *0x*67, *0x*89, *0xab*, *0xcd*,*0xef*, 0xfe, *0xdc*, *0xba*, *0x*98, *0x*76, *0x*54,*0x*32, *0x*10}.

An example of the plain text of instruction used in temperature measurement is as follows:

byte [] *temp* = {*0xF*, *0xC2*, *0x01, 0x01*, *0xC4*, *0xFE*}.

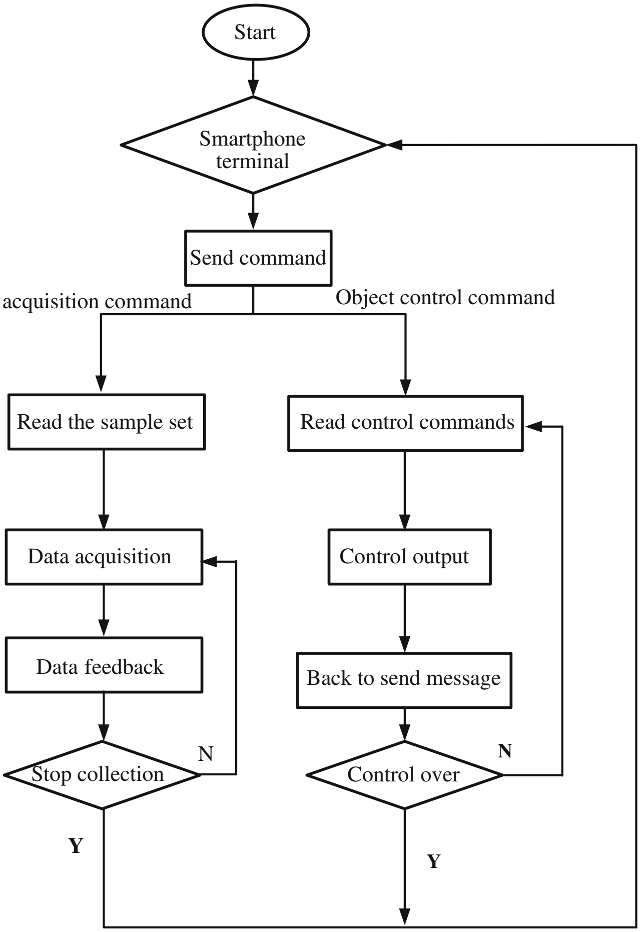

Fig. 19.3 Secure measuring and controlling process for smart home

The statements used in calling the SM4 cryptographic algorithm and sending commands are as follows:

*sm*4.*sms*4 (*temp*, *inLen*, *key*, *outTemp*, *ENCRYPT*);
SendCmd(*outTemp*);

19.3.3 The Performance Test of System

The performance of secure smart home system has been tested by adopting SM4 algorithm, and compared with the embedded AES one.

Secure measuring and controlling instructions in the smart home are similar to such format of data as “EF C1 02 01 C3 FE”. The instruction means to open lamp 2. EF and FE are used as check digit. C1 is the serial number of equipment. 02 is No.2 lamp. 01 means that the lamp will be lighted on. C3 is checksum. The whole instruction is encrypted into 128-bit hexadecimal data by SM4 cipher algorithm. SM4 encryption function used in the smart home system is as follows:

*SM*4. *SMS*4 (*in, inLen, key, out*, *ENCRYPT*)

Correspondingly, SM4 decryption function is:

*SM*4. *SMS*4 *(out, inLen, key*, *in*, *DECRYPT*)

As a contrast, a smart home system embedded AES algorithm is realized in the same way. AES encryption functions: *out* = *Encrypt_Byte* (*in, key*), and AES decryption function is: *in* = *Decrypt_Byte*(*out, key*).

The above two algorithms are called to evaluate the performance of the proposed based on monitoring nodes and controlling ones. The results of test show each of them can protect the system and find abnormal behaviors from nodes, but the time to finish an instruction is different. A detailed evaluation is carried out as follows.

The test is divided into three cases: unencrypted, encrypted based on SM4, and encrypted based on AES. Smartphone terminal sends unencrypted sensing or controlling instruction to nodes every 4 s, and receives the feedback message from nodes which has finished the instruction, all records are stored in LogCat logs. Assuming the timestamp of sending unencrypted instruction as S_i, the timestamp of feedback is R_i, therefore, the delay between sending and receiving operations for an unencrypted instruction can be expressed as T_i:

$$T_i = R_i - S_i \tag{19.1}$$

Similarly, the encrypted test by SM4 or AES algorithm can be done. Let the timestamp of sending encrypted instruction be S_i, the timestamp of feedback is r_i, therefore, the delay between sending and receiving operations for an encrypted instruction can be expressed as t_i:

$$t_i = r_i - s_i \tag{19.2}$$

So one can get the ratio of time delay of encrypted instruction compared to unencrypted one:

$$d_i = \frac{t_i - T_i}{T_i} \tag{19.3}$$

The average ratio of time delay for m–times test can be obtained according to the following formula [10, 11]:

$$\bar{d} = \sum_{i=1}^{m} \frac{d_i}{m} \tag{19.4}$$

The impact of secure mechanism on time delay is plotted in Fig. 19.4 by sampling 50 times. Figure 19.4a, b show the impact of secure mechanism on controlling instruction or sensing one, respectively. They are classified into three kinds of situations: unencrypted case without security mechanism, encrypted case embedded SM4 algorithm, and encrypted case with AES algorithm.

According to Fig. 19.4, the average values of time delay of secure mechanisms is illustrated in Table 19.1 based on 50 sampling values. Table 19.1 shows that the average ratios of time delay are 2.61 and 6.25 % for sensing instructions with a secure mechanism based on SM4 and AES algorithms, respectively. The corresponding results are 2.28 and 7.91 % for controlling instructions. Although the secure mechanisms have little impact on time delay of system, while a secure guarantee is in prospect. Furthermore, the secure mechanism embedded SM4 algorithms have less time delay than one embedded AES algorithm, that is, one can get that the advantages of SM4 algorithm in time delay are 3.64 and 5.63 % for data acquisition and node controlling than the AES in Table 19.1.

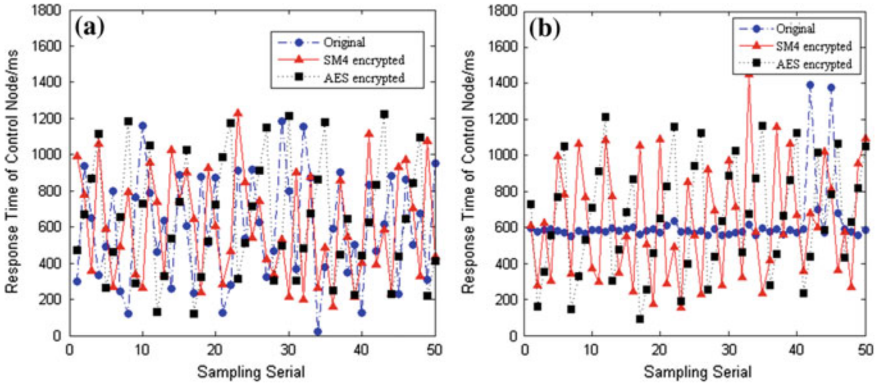

Fig. 19.4 The impact of secure mechanisms on time delay. **a** Control nodes, **b** sensing nodes

Table 19.1 The average impact of secure mechanisms on time delay

	Unencrypted	SM4 encryption		AES encryption	
	t/ms	t/ms	*d*/%	t/ms	*d*/%
Data acquisition	616.7	632.8	2.61	655.3	6.25
Node controlling	594	607.6	2.28	641	7.91

Although AES cryptographic algorithm is built in such Zigbee nodes as CC2530, which is convenient for secure communications between those nodes with the same configuration, it is hard for non-Zigbee nodes such as smartphone terminal, WiFi gateway, and so on. However, the proposed scheme embedded SM4 algorithm could solve this problem by distributing SM4 algorithm in all nodes of smart home, this is helpful to earn its flexibility in realizing the secure measuring and controlling system.

19.4 Conclusions

Smart home brings much convenience to people while it faces some potential risk from malicious attacks. Research on secure smart home is necessary for application and popularization. Secure measuring and controlling methods are proposed for smart home based on nodes embedded SM4 cryptographic algorithm. The secure mechanisms such as access control, encryption of instructions, authentication of devices, intrusion detection, and alarm are helpful to improve information security of smart home and to protect users' privacy. The results of simulation proved that the proposed method is effective and feasible to enhance the security of smart home system. The extra mechanism of security only brings about 2.5 % time delay in processing of instruction. The results show that the proposed methods embedded SM4 algorithm have about 4 % less time-consuming advantage in delay and flexibility of implementation compared to the typical AES scheme, and it does not involve the use of foreign intellectual property rights. This research provides a theoretical path and technical exploration for realization of secure smart home based on the Internet of things.

Acknowledgments This work is supported by the National Natural Science Foundation of China (61170219) and the Basic and Frontier Research Project of Chongqing Municipality (cstc 2013jcyjA40002).

References

1. Liu ZB (2004) X-10 protocol and its applications in smart houses. Microelectron Comput 21 (3):5–8 (in Chinese)
2. Hu XD, Wei QF, Tang H (2010) Model and simulation of creditability based data aggregation for the internet of thing. Chin J Sci Instrum 31(11):2636–2640 (in Chinese)

3. Wu CK (2010) A preliminary investigation on the security architecture of the internet of things. Bull Chin Acad Sci 25(04):411–419 (in Chinese)
4. Zhang XM, Wang GQ, Ding XN (2009) Development of an Internet home automation system. Chin J Sci Instrum 30(11):2423–2427 (in Chinese)
5. Wu J (2013) Research and implementation of hybrid cipher algorithm based on SM4 and Sm2. Softw Guide 12(8):127–130 (in Chinese)
6. Hou J, Wu CD (2009) Research of intelligent home security surveillance system based on Zigbee. Mech Electri Eng Mag 26(01):33–35 (in Chinese)
7. Liu YH, Zhang JX (2012) Smart home based on the Zigbee wireless. Intell Netw Intell Syst 05:122–125
8. Daehwan K, Daijin K (2006) An intelligent smart home control using body gestures. Hybrid Inf Technol 06:439–446
9. Ren XL, Yu HB (2007) Study on security of Zigbee wireless sensor network. Chin J Sci Instrum 28(12):2132–2137 (in Chinese)
10. Hu XD, Han KM, Xu HR (2014) Design and implementation of security focused intelligent household IOT. J Chongqing Univ Posts Telecommun 26(2):171–176 (in Chinese)
11. Jiang J, Liu T, Hu X (2008) Research and implementation of dynamic SMS4 algorithm. Netw Secur Technol Appl 9:92–93 (in Chinese)