*Available online www.jocpr.com*

**Journal of Chemical and Pharmaceutical Research, 2014, 6(7):498-502**

**Research Article**

**ISSN : 0975-7384**
**CODEN(USA) : JCPRC5**

# A lightweight secure smart home SMS control scheme

**Youchan Zhu* and Jing Qiu**

*North China Electric Power University, China*

**ABSTRACT**

*In Smart home, it's an important way for people to control their household equipment by Short Message Service (SMS). But its security has been worrying, for this, designed a SMS service scheme, which based on traditional SMS, data encryption, and data signature etc. In addition, proposed random verification code, two authentications, delayed sending, and failures retransmission mechanism etc. Results show that the scheme can provide a secure and reliable communication environment.*

**Key words:** Smart Home; SMS; random verification code; replay attacks

## INTRODUCTION

Smart home[1] is an important part of the Internet of Things, currently, is also a hot field. Smart home is a highly safe, reliable, comfortable, automatic, intelligent home environment, using the cabling, network communications, multimedia, automatic control, data mining etc. A variety of devices in Smart home (such as audio, video, lighting, curtain, air condition, security system, digital cinema system, network appliance, and three tables cc, etc.) can be connected together to provide appliance control, lighting control, curtain control, mobile phone remote control, indoor and outdoor remote control, anti-theft alarm, environmental monitoring, HVAC (Heating, Ventilation and Air Conditioning) control, infrared repeater, and programmable timing control and so on.

The Smart home system can be divided into four layers[2]: the perception layer, transport layer, processing layer, and application layer. The perception layer is mainly composed of various types of sensors and other monitoring equipment which employed to collect data from the environment; the transport layer is to build up a bridge between the perception layer and the processing layer through sophisticated communication technologies, safety and reliability is critical to this layer; the processing layer includes a variety of data processing techniques, such as statistics, data mining[3] and so on, aiming at finding out user's habits and anticipating the changes in the environment, therefore, this layer is the core of intelligence; the application layer supports communication between users and Smart home systems through applications.

As the result of the popularity of smart mobile phones, people begin inseparable with mobile phones, which also makes mobile phones become a significant part of Smart home systems. SMS is still an important way for people to communicate, unfortunately, but the SMS technology does not provide a built-in support for any security feature[4][5], besides, GSM and CDMA network are unreliable. This paper proposed a self-SMS-service platform for Smart home based on information security technologies and home intelligent terminals to achieve the information exchange between persons and things, named as SSMS. The solution provides an easy way for users to query or control their family devices by SMS; and it has simple, practical, inexpensive, secure and reliable features.

## DESIGN THE BASIC ARCHITECTURE OF SSMS

In order to facilitate the description here, give some directions as follows: PE: mobile phone; HE: home intelligent terminal; SMSC: Short Message Service Center; MDs: monitoring devices.

Figure1 shows the basic architecture of SSMS. MAC is a random verification code between PE and HE, which can used to generate a session key. MAC Before the first communication, PE should be registered in HE, and then HE would generate a MAC for PE to set up. MAC is updated after each communication to enhance the system's security; by this way, the replay attack can be prevented. Compared with the key distribution scheme based on trusted third party, this scheme is more convenient, while eliminating the third party system's bottlenecks and safety hazards[6][7]. HOME is a sign of one home. As is shown in the Figure1, HE is the system server, therefore, different homes have different servers, and this design greatly simplifies the Smart home system, saving unnecessary overhead, can achieve the Smart home control independence.

The system requires a special SMS application. The application can ask the user to do an authentication before data exchange, of course, it can receive the traditional short message, besides, and it provides some measures to process the message sending to self-SMS-service system.

Since the SMSC only needs to transmit messages without other operations, so no changes.

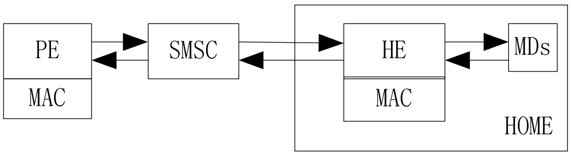

**Figure 1 the basic architecture of SSMS**

**SMS CONTENT PACKAGING FORMAT**

Figure2 is the SMS content packaging format. The "signature" occupies 32 characters to provide message integrity; in order to distinguish SMS categories, such as "authentication", "control command", "system error", etc, "type" is designed, which occupies 1 character; "commands" are a series of instructions, "X:Y" is the form of an instruction, X represents parameter, and Y represents value, use "&" to connect multiple instructions, there is no limit "commands" length. Note that format described here only propose the content of messages, before the final transmission, data encryption is indispensable.

| 32 | 1 | |
|---|---|---|
| signature | type | commads |

**Figure 2 SMS content packaging format**

**DATA SEGMENTATION**

An SMS can be sent to a mobile phone with maximum payload of 140 octets which defines the upper bound of an SMS to be 160 characters using 7-bit encoding[7][9]. It is also possible to encode SMS using 8-bit or 16-bit encoding, which decreases the maximum message length to 140 and 70 characters[8]. Here, since that SMS content is encrypted and encoded into a string of English characters, we chose 7-bit encoding; however, it's necessary to divide a message text into several fragments, none bigger than 160 characters. Figure3 shows the format for division, T records the total number of data fragments, S records the sequence number, G records the group number, and C is the cipher text. As is illustrated in the Figure4, T and S apply 2 characters, G applies 6 characters, and the rest of space is given for C.

Both PE and HE can maintain a queue of messages waiting to be sent. The fragments that belong to a same group will be sent once. Before the feedback information received, next group need to wait. If one group has something wrong with transmission, the group will be required to retransmit, however, the maximum of attempts is 3. The process consists of two algorithms: Packet and Depacket.

Packet(x). The Packet algorithm takes one parameter x as input and outputs a list of fragments, each fragment is encapsulated into a format as the Figure3.

Depacket(List x). The Depacket algorithm takes a List x as input. The algorithm can restore the original information in accordance with T, S, and G.

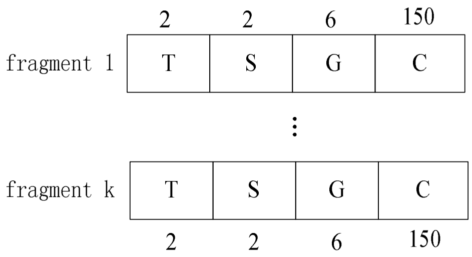

**Figure 3 the format for division**

## KEY PROCESS

There are five fundamental algorithms: Generate, H, Signature, Encrypt, and Decrypt.
Generate(). The Generate algorithm takes no input and outputs a MAC.
H(x). The H algorithm takes one parameter x as input and outputs a session key.
Signature(x). The Signature algorithm takes one parameter x as input and outputs a digital signature.

Encrypt(x,y). The Encrypt algorithm takes x and y as input, and x is the key, y is the plaintext. The algorithm can encrypt y and produce a cipher text.

Decrypt(x,y). The Decrypt algorithm takes x and y as input, and x is the key, y is the plaintext. The algorithm can decrypt y and produce a plaintext.

SMS authentication process is listed as follows:
(1) PE computes K1=H(MAC) to generate session key;
(2) PE computes S1= Signature(M1) and C1= Encrypt(K1, M1), M1=S1 + authentication mark + Id: user's id & Password: user's password, then packages these data and sends to HE;
(3) HE computes K2=H(MAC);
(4) HE computes M2= Decrypt(K2,C1) to get S1, authentication mark, Id and Password;
(5) HE computes S2= Signature(M2), and verifies whether S1=S2, if this is true, HE would verify whether Id and Password are available, if this is available, HE would start a timer for PE; If no operation is performed within the prescribed time, the identity will expire. However, an operation can reset the timer.
(6) HE computes MAC=Generate(), and computes S3= Signature(MAC) and C3= Encrypt(K2, MAC), then packages these data and sends to PE;
(7) PE computes K3=H(MAC);
(8) PE computes M3= Decrypt(K3,C3) to get S3, and MAC;
(9) PE computes S4= Signature(MAC), and verifies whether S3=S4, if this is true, PE would update its MAC.

After SMS authentication process, users can send instructions to HE to control MDs. The process is described as follows:
(1) PE computes K1=H(MAC) to generate session key;
(2) PE computes S1= Signature(M1) and C1= Encrypt(K1, M1), M1=S1 + control mark + commands, then packages these data and sends to HE;
(3) HE computes K2=H(MAC);
(4) HE computes M2= Decrypt(K2,C1) to get S1, control mark and commands;
(5) HE computes S2= Signature(M2), and verifies whether S1=S2, if this is true, HE would control MDs using commands and collect the results;
(6) HE computes MAC=Generate(), and computes S3= Signature(M3) and C3= Encrypt(K2, M3),M3=S3+ MAC + results, then packages these data and sends to PE;
(7) PE computes K3=H(MAC);
(8) PE computes M4= Decrypt(K3,C3) to get S3, MAC, and results;
(9) PE computes S4= Signature(M4), and verifies whether S3=S4, if this is true, PE would update its MAC and show results.

## SENSITIVE DATA STORAGE

Some sensitive data is stored in PE and HE. This will bring some security threats, so these sensitive data will be encrypted; the key seeds are kept by users without storage.

## SECURITY ANALYSIS

In this paper, PE needs to register in HE, and a MAC would be generate for both of them to communicate. Taking into account the unreliability of GSM and CDMA network[11], the scheme also proposed data segmentation, delayed sending, failures and mistakes retransmission mechanism.

Figure4 shows the security architecture of SSMS, including twice authentication, random verification code, data encryption, data signature, data segmentation, delayed sending, and failures and mistakes retransmission etc.

Twice authentication: One is the random verification code and another is user's password.

Random verification code: A code which used to generate a session key. Its random feature can prevent replay attacks. This code can be very short, so can greatly save bandwidth.

Data encryption: Encrypt the communication data and sensitive data stored in PE to ensure the security of data.

Data signature: Signature the communication data to ensure the integrity of data.

Failures and mistakes retransmission, and delayed sending: Ensure the reliability of communication.

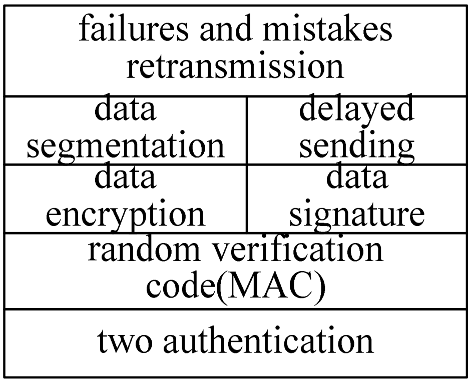

**Figure 4 the security architecture of the system**

The following assumptions are several methods of attacks, indicating the resilience of the scheme:
(1) Fake PE request HE

Fake PE doesn't have correct MAC, user's id and password, besides fake PE doesn't register in HE, so this attack is not established.

(2) Replay attack
The MAC will be updated after each data exchange, so that historical data can not be validated by the system, replay attacks is not established.

(3) Data leakage caused by PE's loss
Sensitive data stored in PE has been encrypted, so a user who doesn't have the key can't get those sensitive data. In addition, message authentication process asks users to enter password before data exchange, so one without correct password also can't control household equipment. The owner can update the MAC and password in HE to prevent those possible attacks.

## EXPERIMENTAL SECTION

The following settings are of the testing system:
(1) Used SHA-256 as H(x);
(2) Used AES-256 as encryption algorithm;
(3) Used MD5 as digital signature algorithm;
(4) Used two Lenovo A380e mobile phones as test equipment, operating system: Android OS 4.3, Dual-core, frequency: 300-1190.4 MHZ, RAM: 512M.

Test data is "TV:open&Geyser:open", and then tried to intercept, tamper, and replay those communication data.

Testing system has shown good ability to ensure the security of data.

Table1 shows the performance of the testing system and system using RSA-1024. The time is the average time-consuming. Compared with the system using RSA-1024, the advantages of the scheme proposed in this paper are very obvious.

The system using RSA-1024 needs at least 1064 bytes to store public key and private key; however, testing system only needs 12 bytes to store MAC, greatly reducing the storage space. Therefore, this scheme is lightweight and secure, and suitable for Smart home systems.

**Table1 the performance of the testing system and system using RSA-1024**

| | keygen | encrypt | decrypt | signature |
|---|---|---|---|---|
| system using RSA-1024 | 456ms | 2ms | 8ms | 1.5ms |
| testing system | 1ms | 1ms | 1ms | 1ms |

## CONCLUSION

Compared with mobile phones communicate with web servers to control home devices, the scheme proposed in this paper provides a direct way to communicate with the home intelligent terminal. The home intelligent terminal acts as a server and a controller. This design meets the distributed nature of Home Networking, simplifies the system architecture, and reduces the system cost. At the same time, random verification code, twice authentication, delayed sending, failures and mistakes retransmission, data encryption, data signature, and data segmentation form the security architecture of the system, enhancing the security of the system. This scheme has a very important significance in Smart home security control.

## REFERENCES

[1] Saad al-sumaiti A, Ahmed M H, Salama M M A. *Electric Power Components and Systems*, **2014**, 42(3-4): 294-305.
[2] Zhang Y H, Huang R. *Advanced Materials Research*, **2013**, 753: 3120-3124.
[3] Gao Y Z, Wei L Y. *Applied Mechanics and Materials*, **2014**, 475: 1150-1153.
[4] Mukhopadhyay A, Maulik U, Bandyopadhyay S, et al. *A Survey of Multi-Objective Evolutionary Algorithms for Data Mining: Part-II*[J]. **2014**.
[5] Pereira G C C F, Santos M A S, De Oliveira B T, et al. *Journal of Systems and Software*, **2013**, 86(3): 698-706.
[6] De Santis A, Castiglione A, Cattaneo G, et al. *An extensible framework for efficient secure SMS[C]//Complex, Intelligent and Software Intensive Systems (CISIS), 2010 International Conference on. IEEE*, **2010**: 843-850.
[7] Lisonek D, Drahansky M. *Sms encryption for mobile communication[C]//Security Technology*, **2008**. *SECTECH'08. International Conference on. IEEE*, **2008**: 198-201.
[8] Saxena N, Chaudhari N S. *Journal of Systems and Software*, **2014**.
[9] Agoyi M, Seral D. *SMS security: an asymmetric encryption approach[C]//Wireless and Mobile Communications (ICWMC),* **2010** *6th International Conference on. IEEE,* **2010**: 448-452.
[10] Lisonek D, Drahansky M. *SMS encryption for mobile communication[C]//Security Technology*, **2008**. *SECTECH'08. International Conference on. IEEE*, **2008**: 198-201.
[11] Nanda A K, Awasthi L K. *A Proposal for SMS Security Using NTRU Crypto system[M]//Quality, Reliability, Security and Robustness in Heterogeneous Networks. Springer Berlin Heidelberg,* **2013**: 706-718.