Design of Smart Lock Control System with Function of Active Authentication

JIANG Cun-bo[1,a], KONG Xiang-li[1,b], JIAO Yang[1,c] and Chen Xiao-qin[1,d]

[1]Department of Information Science and Engineering, Guilin University of Technology, Guangxi 541006, China

[a]jiangcunbo@163.com, [b]1654646724@qq.com, [c]496003921@qq.com, [d]149833896@qq.com

Keywords: Embedded system; Intelligent control; Wireless authentication; GSM

Abstract: The smart lock control device has functions of active wireless authentication and GSM remote unlocking. A smart key can match with 8 locks. A smart lock can have 8 keys. When the intelligent lock receives unlocking request, it will send an encrypted authentication request packet on its own initiative. After receiving request packet, the key checks the correctness of lock ID, determines the corresponding PD(password dictionary), obtains the password by PI(dynamic password index), and deciphers the message. Secondly, the key compares lock address with the source address to determine whether to transmit a reply packet. The lock adopts the same way to judge legitimacy of the key. Moreover, it adds lock ID and overtime certification. After identity authentication, the control system performs unlocking operation. Mobile phone can achieve remote unlocking by using dynamic authentication codes. Verified by experimental tests and application, the system can meet the design requirements in function and security.

Introduction

The following situations are often encountered in daily life. We often wish to be able to open the door by door handle directly when carrying articles to home.We usually hope that a key can open multiple locks at home. At public place, in order to improve security, we hope door or lock could record the unlocking key number and time. Features of this intelligent lock is in the following. (1) A key can open multiple locks in the home and the door can record unlocking key number and unlocking time. (2) The function of opening the door with handle directly is realized by active wireless identity authentication.(3) The function of remote unlocking is realized by GSM short message based on dynamic authentication.

Overall structure and hardware design

Overall structure

A smart lock consists of the lock body module, intelligent control module, communication and alarm module, and the active identification card (smart key). Overall structure is shown in figure 1.

The system uses processor ARM as controller and accomplishes lock state identification and monitor through switch state detection circuit, including the handle switch, the counter lock switch, the locking switch, the pressure switch on the door, etc. If there is a unlocking request and two-way authentication is passed, the system will perform unlocking operation, give a sound and light hint and record unlocking information. If there is a illegal status, the system will give both local and remote alarm.

In order to ensure safety and reliability of the system, power supply adopts two methods. One of ways is adopting external power when external power is normal , the other is adopting rechargeable batteries when external power can’t provide electricity. Smart key only uses one button battery, which can keep normal work about 1 year with special working mechanism where there is 1 000 ms dormant state and 5 ms awakened state in a cycle.

GSM and voice alarm module

Chip SIM900A is used in short message module where pin TXD and pin RXD is respectively connected with pin RX1 and pin TX1 of processor ARM, and pin POWER controls GSM module to turn on or turn off. The digital audio files is converted into analog audio files by the DAC on ARM. Audio power amplifier LM4871 drives output signals to the speaker.

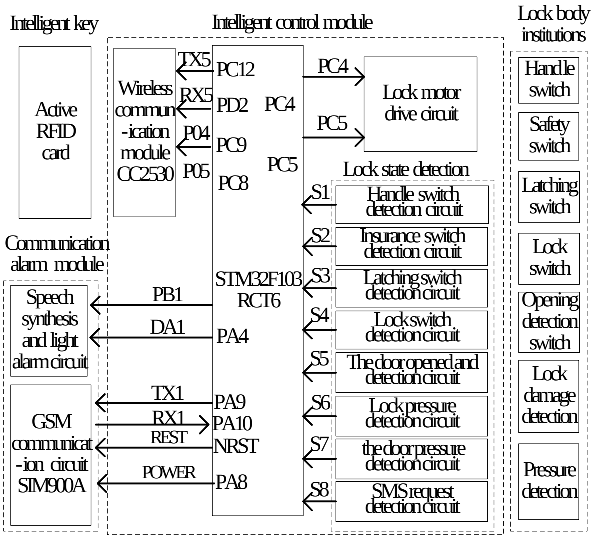
Intelligent key
Intelligent control module
Lock body institutions
Active RFID card
Wireless commun-ication module CC2530
TX5
RX5
P04
P05
PC12
PD2
PC9
PC8
PC4
PC5
STM32F103RCT6
Lock motor drive circuit
Lock state detection
S1
S2
S3
S4
S5
S6
S7
S8
Handle switch detection circuit
Insurance switch detection circuit
Latching switch detection circuit
Lock switch detection circuit
The door opened and detection circuit
Lock pressure detection circuit
the door pressure detection circuit
SMS request detection circuit
Handle switch
Safety switch
Latching switch
Lock switch
Opening detection switch
Lock damage detection
Pressure detection
Communication alarm module
Speech synthesis and light alarm circuit
PB1
DA1
PA4
GSM communication circuit SIM900A
TX1
RX1
REST
POWER
PA9
PA10
NRST
PA8

Figure 1 Overall structure

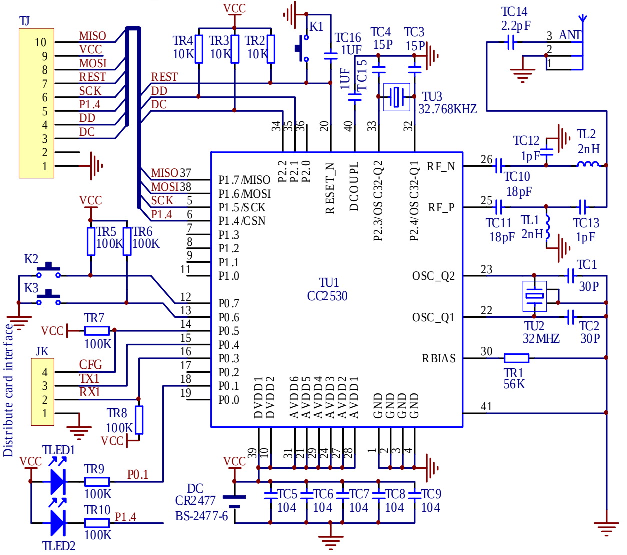

Figure 2 Smart key

RF communication module and smart key circuit design

Circuit design of RF communication module is the same as the design of intelligent key where TI company chip CC2530 is selected for RF communication. Referred to official design, intelligent key circuit is shown in figure 2 in which the card interface is used to communicate wit issuing card device.

The dashed frames express that there are no switch buttons used to unlocking and no battery button in RF communication module. RF communication module is connected to ARM processor through serial interface USART5 and is controlled by the processor, while CC2530 on the intelligent key works independently.

Software design

Packet format

Authentication request packet and reply packet use fixed format with 18 bytes. The packet format is shown in table 1.

Table 1 Authentication packet format

Function	Message header			Data fields					
	Destination address	Function code	Cipher key word	Source ID	Source address	Destination ID	Sending time	Communication distance	Check word
The number of bytes	1	1	1	4	1	4	3	1	2
Character	DA	FC	PI	SID	SA	DID	T	RSSI	FCS
Instructions	Broadcast address or receiving device address	Distinguish in function of a message	Fields used to find the key from a PD (password dictionary)	Message sending device ID	The address of message sending device	The message receiver ID	Time of sending the message	CC2530 automatic calculation	CC2530 automatic generation
Encryption	No encryption			8 byte encryption Encryption algorithm : $Y = X \oplus P_{ENC}$				No encryption	
18 bytes in total									

DA is filled in broadcast address 0xFF in request message while lock address in reply message. FC is filled in 0x05 in request message while 0x06 in reply message. PI is a 6 bit random number produced by sending device. Only the data domain is encrypted whose size is 8 bytes(64 bit).

Encryption and decryption

In order to reduce power consumption by reducing the number of packet bytes in RF communication, there is not using AES co-processor built in CC2530 to encrypt and decrypt the packet. Intelligent lock system only encrypts message field {SA, DID, T}.

Encryption and decryption process are as follows.

(1)The intelligent lock device randomly generates password dictionary with 128 groups of 64 bit random number which is configured to the intelligent key with the key address when the card issuing device is allocating keys.

(2) The sending device produces a 7 bit random number to fill in the PI field and applies PI to choose a set of 64 bit word from the PD as cipher. Then it encrypts the data domain of X, including SA, DID and T, and transmits the encrypted packet. The encryption algorithm is $Y = X \oplus P_{ENC}$.

(3)The receiving device uses the PI field of the received packet to choose a set of cipher which is employed to decrypt the message domain of Y, including SA, DID and T, and judge the legitimacy. The decryption algorithm is $X = Y \oplus P_{DEC}$.

(4)Time T which is a time stamp is produced by the real time clock of intelligent lock.

Data structures and storage

An intelligent key can manage eight locks and each lock can be up to eight keys authorized. Smart key stores the attribute sets of registered locks and lock stores the attribute sets of keys authorized. When key information is matched with lock information in bidirectional authentication process, the system will performs unlocking operation. Data structure of attributes is shown in table 2.

Table 2 Data structure of lock/key attributes

	Key attributes in a lock					Lock attributes in a key				
Attributes	KID	KA	LID	LA	RSSI	LID	LA	KA	LPDI	RSSI
Meaning	Key ID	Key address	Lock ID	Lock address	Distance	Lock ID	Lock address	Key address	Password dictionary index of lock	Distance
The number of bytes	4	1	4	1	1	4	1	1	1	1
	11 bytes					8 bytes				

Attributes of smart key are described by structure {KID, KA, LID, LA, RSSI}. KID and LID respectively express 4 bytes key ID and lock ID which are configured when leaving factory. KA and LA respectively express 1 byte key address and lock address. RSSI can reflect the valid distance between key and lock. The key stores attribute sets of registered locks. Attributes of the lock are described by structure {LID, LA, KA, LPDI, RSSI}. LPDI expresses 3 bit PD storage index.

8 groups of lock attribute sets are stored in CC2530F256RHAR internal Flash which has 256k bit storage capacity. First address of the storage space is 0x3C800. The intelligent lock stores key attributes information and unlocking information in outside EEPROM memory. Information recorded is {4 bytes key ID, 3 bytes time T}.

Active authentication

The authentication process is as follows.

Lock control device detects the unlocking request and sends unlocking request packet to intelligent key. In the authentication request packet, SID is filled in LID, DA is filled in broadcast address, and T is filled in the current time. Then the message is encrypted.

Intelligent key needs one authentication to complete certification of lock identity after receiving request packet. First of all, the key judges that whether there is a LID in lock attribute sets matching with SID and then determines whether to send a reply packet or not. If it exists, the key continues to seek LA and KA and find decryption key P_{DEC} through PI and PD. Next, the key decrypts request message to obtain the time stamp T and finally transmits an authentication reply packet. In the reply message, SID is filled in LID, DA is filled in LA, and SA is filled in KA.

Intelligent lock needs four groups of authentication to complete the certification of key identity after receiving reply packet. Firstly, the lock needs to judge whether SID matches with KID. Secondly, the lock decrypts message and judges whether SA matches with KA. Thirdly, whether DA and LA match. Fourthly, whether the reply message is timeout according to T. If the key Passes the four authentication, the lock control system will perform unlocking operation.

Lock security

Intelligent door security includes operation security and authentication security. If lock system identifies a illegal operation through detecting switches and identifying the state, it will give a local sound and light alarm and a remote SMS notification. Authentication security is realized by the mechanisms of packet encryption, authentication information matching and time constraint.

Lock actively sends request packet where 64 bit field {SA, DID, T} is encrypted and PI randomly generated by sending device is 7 bit. There are eight lock attribute sets and PDs in the intelligent key which need 3 bit binary number to find one PD. So comprehensive password valid binary digits have 74 bit. If speculation method is applied to crack the packet, the number of guess is up to 2^{74}. Moreover, in order to enhance the ability against attack during authentication process, authentication process should be finished within lifecycle(time constraints).

Lifecycle refers that the intelligent key response time Tack should comply with the formula: $Tack + Tc \le Treq + Td \le 1Sec,$ Wherein Tc represents one-way RF communication delay, Ty represents the time key uses to generate reply packet, Treq represents request packet sending time, and Td represents delay time from sending request packet to receiving response packet calculated by intelligent lock.So such authentication methods can meet security need of average family smart locks.

Program design

Intelligent lock control software is to realize issuing card, lock state detection, authentication, packet encryption and decryption, unlocking control and anti-theft alarm, etc. Figure 4 shows the main program flow chart.

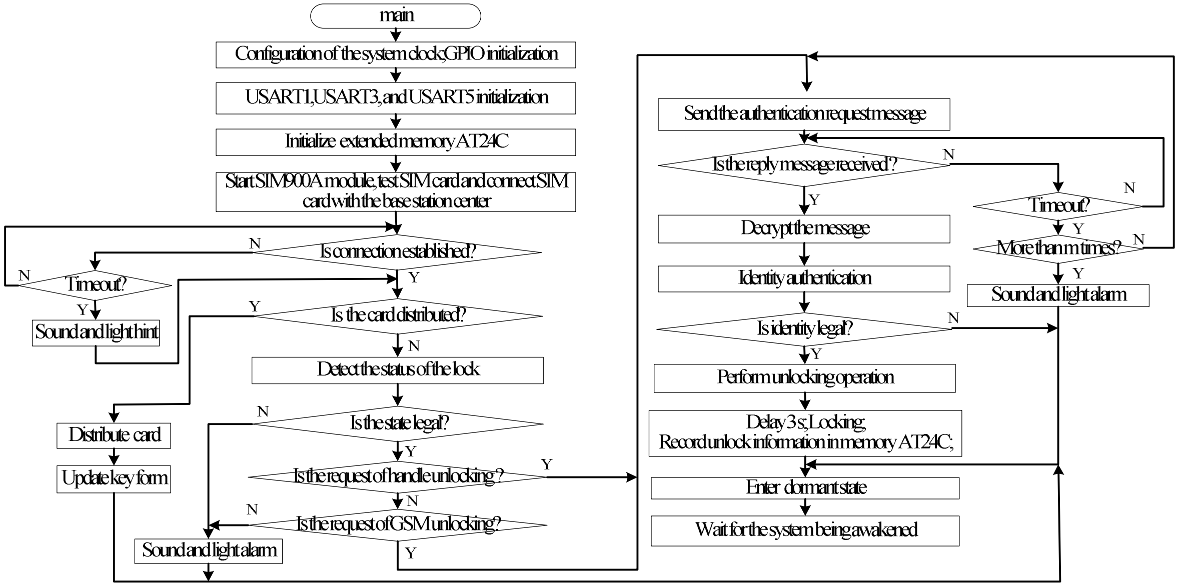
main
Configuration of the system clock;GPIO initialization
USART1,USART3,and USART5 initialization
Initialize extended memory AT24C
Start SIM900A module, test SIM card and connect SIM card with the base station center
Is connection established?
N
Y
Timeout?
N
Y
Sound and light hint
Is the card distributed?
Y
N
Distribute card
Update key form
Detect the status of the lock
Is the state legal?
N
Y
Is the request of handle unlocking ?
Y
N
Is the request of GSM unlocking?
N
Y
Sound and light alarm
Send the authentication request message
Is the reply message received ?
N
Y
Timeout?
N
Y
More than m times?
N
Y
Sound and light alarm
Decrypt the message
Identity authentication
Is identity legal?
N
Y
Perform unlocking operation
Delay 3 s;Locking;
Record unlock information in memory AT24C;
Enter dormant state
Wait for the system being awakened

Figure 3. Main program flow chart

Experimental test

Experiments include: (1)The authentication between lock and key when the handle is used to open the door directly. Test the response time from the press of handle to driving motor to open the door. Test the authentication between lock and key. Test the distance between lock and key in which the door can open. (2) Whether the door could give an alarm when destroyed. Test that when the door is broken, removed, and counter locked, whether the door sends mobile phone a notification message. (3) A key authorized by multiple locks can open doors with different address. (4)Mobile phone remotely controls unlocking.

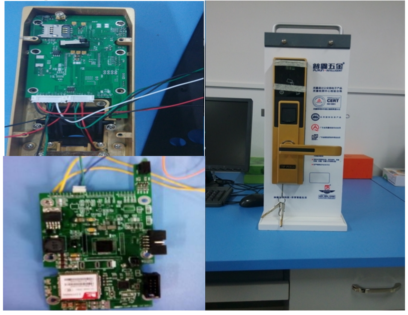

Figure 4 Smart lock photos

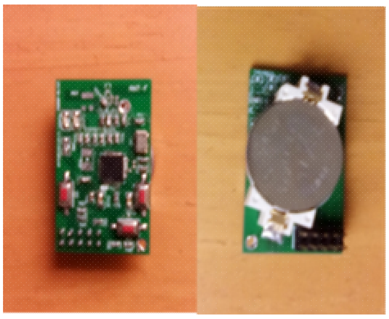

Figure 5 Smart key photos

The test results show that the response time to open the door can meet requirements of users. If ID and address don’t match, door handle can’t open the door directly. Distance between key and lock in which door could open is from 0.5 meter to 1 meter on condition that there is no obstruction. When the door is destroyed by violence, it will give a sound and light alarm and send a notification to cell phones. A key can open multiple locks. Only the phone bound to the lock can remotely open the door while other phones can not perform the above operation.

Conclusion

This paper designs a kind of smart lock control system with functions of active identity authentication and GSM wireless remote unlocking which can meet the demand of ordinary households and offices. At the same time, it is more convenient to use. It can also meet the requirement of security through password dictionary matching, dynamic cipher key word, and time limitation.

Acknowledgment

This work was financially supported by National Natural Science Foundation of China (51167004), Natural Science Foundation of Guangxi (2015GXNSFBA139250), Patent Support Project of Science (KY2015ZL100) and Construction of Key Laboratory of Guilin University of Technology.

References

[1]Zhong Zhao-hui. Design of Wireless Smart Lock System Based on ZigBee[D]. Zhejiang: Hangzhou University of Electronic Science and Technology master's degree thesis, 2013.

[2]He Wen-cai, Yang Wei, Liu Pei-he. Design and realization of remote access control system based on SIM900A module[J]. Network Security Technology & Application Vol.12-13 (2014).

[3]Zhong Zhao-hui, Cheng Zhi-qun. Study on System for Smart Lock Based on ZigBee[J]. Electrical Measurement & Instrumentation Vol.49(9):91-96(2012).

[4]Bai Yan, Lou Yan-hang. Design of Smart Home Based on ZigBee[J]. Intelligence Application Vol. 12:60-61(2014).

[5]Ni Long, He Jun-Ping, Lin Liao-jun. Development of an Interactive Wireless Automobile Intelligent Key System[J]. Computer Measurement & Control. Vol.5:1136-1138(2010).