Design of High Security Wireless Guarding System for Automobiles

Guru Pavan Kumar Potu, K Sham Prasad
Nalanda Institute Of Engineering And Technology
Jawaharlal Nehru Technological University Kakinada
Andhra Pradesh, India

Abstract **– The radio frequency identification technology and the Global Mobile Communication Network are combined to propose an automatic wireless guarding system which reduces the rate of theft of vehicles. The system could identify the vehicle owner quickly and then realized the function of keyless entry and keyless start-up by using micro controller which is interfaced with RFID and GSM module. These interfaced modules along with vibration sensors, helps in monitoring function for the vehicles. GSM module already predefined for controlling the vehicle's states remotely, using the micro controller instructions, sets and dismisses the prevention of messages or calls. Comparing with the traditional system, this system extends the level of reliability and security along with better owner identification. Hence using these two modules unity can be achieved between safeguard and remote control system.**

Keywords – automatic wireless guarding; RFID; GSM network; Remote control

A. Introduction

As the national economy has been developing quickly, the human's utilization of the vehicles also has increased. But, the development of the technology made the crime commitment of automobiles theft easier and frequent. Hence, an anti-theft system is widely used to restrict such consequences. *But the chip one and the network one are the developing directions of the auto-guard technology.* RFID technology has the ability to identify the objectives and receive the data automatically through radio frequency waves as it has passive, contactless, secured and convenient properties. GSM is the most widely used and enhanced tool in mobile communication system. It ensures the information transmission so real-time, security and reliable that realizes the long distance control [1].This paper deals with the design of an automatic wireless secured system for automobiles.

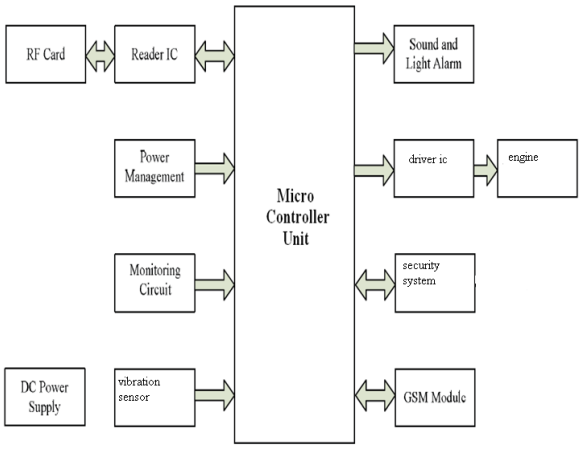

Figure 1. System structure.

B. RFID

This part of the block diagram is consists of three parts as antenna, tag and reader. RFID works under the principle that the signals to be sent into the carrier signal with a particular frequency after encoding are put by the user. These carrier signals are sent through the antenna. Based on the received pulse signals along with the tag that are sent by the user, the circuit starts working on it as modulating, decrypting or decoding. After this it makes command distinguish by working on the request, passwords or permissions. If the received command is read type then the controlling logic circuit will get the message from memory. After encrypting, encoding and modulating, the message will be sent to reader by the antenna in the chip. And then after demodulating, decoding and decrypting the reader sends the message out to the centre of message system to manipulate data. If it is write command of message modification, the control logical circuit originated inner charge pump pulls the working voltage up and hence the E^2PROM content can be modified.

For the automobile to start up in the right way, the ignition switch needs to be inserted with the right identification code. If the ignition switch is turned off, the reader has to send a 13.56MHz charged pulse signal to the tag. This signal will charge the capacitor in the control logic circuit as soon as received. The responder is now able to send the specific code to the reader which is transmitted between the antenna of the reader and the antenna of the tag. The control part encodes the received signal and compares it with the codes of the microcontroller. IF both are same then the engine and the ignition will start up immediately by the operation of the control unit. Even if a single bit is different, then alarm will be raised.

C. Mobile Communication

The module GSM is designed using an isolated operating system, RF process, baseband process and the function module providing standard interfaces which integrated RF chips of GSM, baseband chips, memory and amplifier on the same circuit board. The microcomputer is made to communicate with GSM module by MAX232 serial port and also use the standard AT instructions to control GSM module to realize all kinds of communication, for example, sending message, and making telephone and GPRS dial internet. Just because of low cost and well real time application long range control is realized as the function of sending message.
to rewrite the soft [10]. As a result, the radio technology at present can be replaced completely. So the practical value and the market prospect are considerable.

III. Hardware Design

A. Control Circuit

The microcontroller used here is an 8 bit, the ST Company made STM8AF51AA. Its main features are high reliability, high robustness and low cost. And it is designed for automobile especially. Inside of the chips are E^2PROM with real data and varieties of communication interfaces, such as CAN2.0B, USARTL, INUART LIN2.1, SPI, and I^2C. Its operation speed reaches 10 MIPS (16 MHz).The monitoring circuit is made up of infrared sensors and vibration sensors of which the first one is the finished product component in the type of CS9803GP and later is the finished product component in the type CHT-ZD01 [2]. The actuator is the relay. For drive

interfacing of CAN bus, the PCA82C250 is adopted [3].The power transfer modules are LM7805 and ASM1117. The voltage 12V is pulled down to 5V and then down again to 3.3V to supply MF RC 522 using IC 7805 and ASM 1117 simultaneously as three kinds of voltages 12V, 5V and 3.3V are needed. The power management chip is MAX 708. This chip will save the message with the previous state into E^2PROM immediately, once the power is down, so that it is convenient to read when the power is on. It also helps in providing a reset pulse to avoid program flying when the power voltage is low.

B. RF interface Circuit

Mifare card of NXP Company is the general trend of the market recently. MF RC522 is a read–write base chip with low power consumption and contactless character which is applied for "three instruments" especially. It is a highly integrated reader for contactless communication and protocol at 13.56 MHz. It supports all the levels of ISO14443A and three kinds of interfaces, the SPI, I^2C and serial UART. It can communicate with any MCU and associate with PC directly in the way of RS232 and RS485.In that case, it makes terminal design more flexible than ever [4-5]. The connection of external pins can be checked at the moment of reset, as the MF RC522 supporting a variety of digital interfaces. MF RC522 requires two extra pins I^2C and EA to connect with low level and high level, besides the four universal SPI signal wires (clock wire SCK, input data wire MOSI, output data wire MISO and strobe wire NSS).

The two pins won't take part in the transmission of SPI bus, but only set the digital interface of MF RC522 in SPI way. In addition, CS signal keeps low level when the data flow in; otherwise it will be at high level. The hardware circuit connection of MF RC522 and STM8AF51AA in the SPI way is shown in Fig.2.

C. GSM Interface Circuit

The GSM Module selected in this system is the GSM 900/1800 MHz network double band module made in Simcom Company. This module has the ability to analyze baud rate automatically and improve the performance of electronic public service along with energy save function, embedded TCP/IP and transparent mode belongs to the series of GPRS in three frequencies (900/1800/1900). The peripheral circuit of SIM300DZ mainly consists of the communication interfaces of SIM cassette and module, such as SIM-CLK and SIM I/O, which are the communication wires of module clock and data, SIM-RST and VCC, which are the reset and the power supply. Here, the RXD and TXD are included in the peripheral circuit of SIM300DZ which are connected with the serial port of MCU. The transportation between MCU and GSM through the very two channels is done through the AT instructions [6]. In addition, the voice system channel and MIC channel are included in GSM module. The AT instructions are applied to the voice and microphone of the monitoring system as these channels are switched by MCU. The transmitting ports IN+ and IN is also included which are with the dual tone multi frequency (DTMF) signals. A DTMF signal is sent out to the multi frequency decode chip to analyze and produce Q signal through IN+ and IN-, when the user communicates with the phone equipped in the car and if the button is pressed. The MCU decides how to operate according to the Q signal at this point.

IV. Software Design

The control software of this auto-guard system has to complete sensor signal detection, identification, sending short

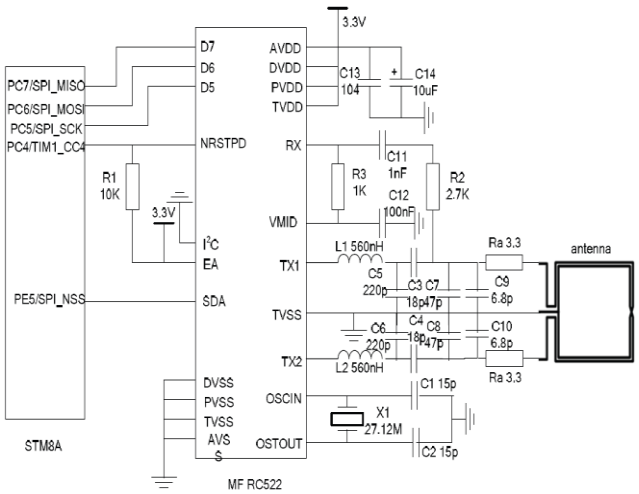

Figure 2. Circuit of the RF interface.

message, the control of the main components of the automobile and sound-light alarm. The system will be in the state of low power after initializing and standby after opening interrupt. When the interrupt takes place, it will end the corresponding process of interrupt event in the interrupt service subroutine by idle mode and set the corresponding flag bit at 1. After being interrupted, according to the state of the flag bit, the routine will execute their process programs. The auto-guard system program modules mainly include control module, identification, GSM manipulating and alarm module etc using the modularization program.

A. The Process of Main Program

The software design module is the core of the system. It includes the calling and setting of initialized function of related equipments. In its main function, the other modules related function can be called to complete the program. The way of using the polling is the basic idea. Every function module's small loop can be called in a big loop and the watchdog is set in each key position in case of the system's crash. Main process is shown in Fig.3.

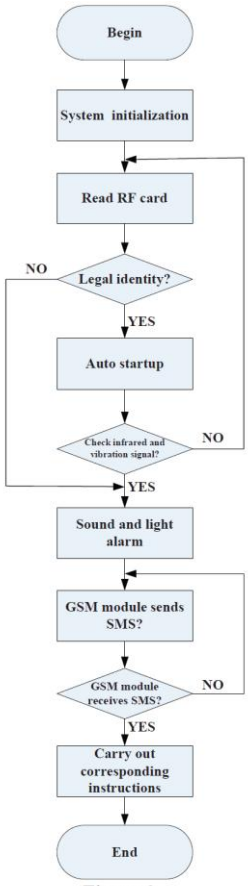

Figure 3
Flow chart of main program.

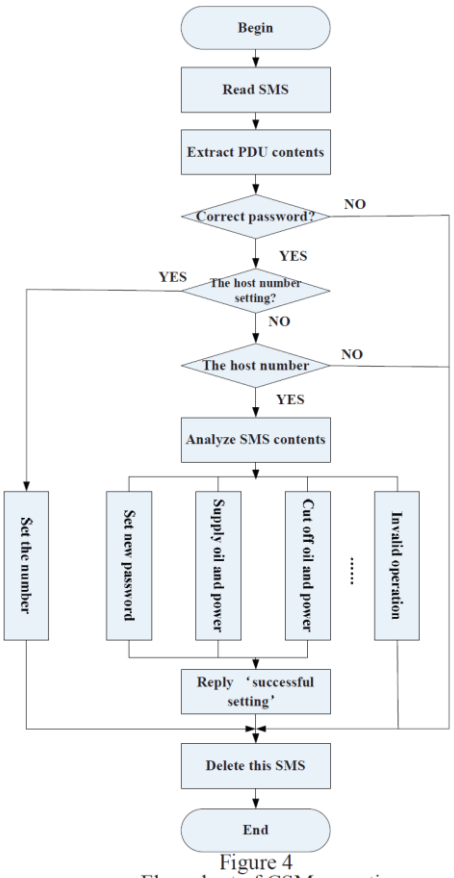

Figure 4
Flow chart of GSM operation.

B. Personal Identification Process

Initially, MF RC522 will be initialized by STM8A. After setting the registers; to achieve the communication with Mifare card; the MF RC522 can receive the commands of MCU and implement the operation. Hence the appropriate operation will be done by Mifare card according to the commands received. The IC card is accessed by STM8A not only through several simple codes but also a series of operation that mainly includes: (1) asking for making up; (2) preventing overlap (preventing the data error caused by overlapping); (3) selecting card; (4) password identification; (5) read-write. A certain order is to be followed by these procedures of Mifare card STM8A. When there is Mifare card into the available range of the antenna, the reading program will perform the operations above to read the unique 64 bit ID from the card and compare it to the one in E^2PROM to identify the user [7-8].

C. GSM Operation Process

In this issue, GSM part is the most important and difficult point. When a new message to the SIM is detected by serial port, it will be activated. The AT+CNMI command will be called by initialization so that the module can send +CMTI :< mem><index> to STM8A automatically. And the <index> represents the position of new message in the memory of SIM. It is convenient to read. It is the CMTI received or not that decides the activation of GSM by the system.

The flow chart of the task is shown in Fig4 [9]. First, the PDU of message will be read by a special array through AT+CMGR=<index>/v/n command will be sent out to module. So the message which in the <index> of memory in SIM card will be sent out in the form of +CMGR: <start>, [<alpha>], <length> <CR> <LF> <pdu> OK. It is convenient to read PDU in the way of looking for by pointer. Second, the telephone number of sender and password and content of UD will be picked up from PDU. So the operation type will be chosen according to the key words, such as "password setting", "user number", "oil and power supply" and "oil and power stop". The PDU (Protocol Data Unit) codes of these key words are saved in a fixed array and will be compared with the received codes by "strncmp" function to get the appropriate operation type.

V. Conclusion

This system has the ability of combined advantage usage of RFID and GSM properties together. A contactless, security and convenient RFID key is the key of the automobile. The long-range monitor and grading responses could be realized by the mobile phones of users, which made the alarm cover a broad range. The microcontroller for vehicle was adopted, which enhanced the reliability and the capability of anti interference. The above mentioned advantages meet the requirements of auto-guard system, and hence a better effect was made in practice and even easy to extend functions. The GPS module can be added if the function of position tracking is needed. If the Internet of things is to be entered, we only need to rewrite the soft [10]. As a result, the radio technology at present can be replaced completely. So the practical value and the market prospect are considerable.

REFERENCES

[1] Huaqun Guo,Cheng H.S.,Wu Y.D.,Ang J.J.,Tao F.,et al.,"An automotive security system for anti-theft," Proceedings of the Eighth
International Conference on Digital Object Identifier,pp.421-426, Mar. 2009.
[2] Hui Song,Sencun Zhu,Guohong Cao,"SVATS:a sensor-network-based vehicle anti-theft system," Proceedings of The 27th Conference on Computer Communications,pp.2128-2136,May,2008.
[3] Yang Wang,Xian-Jun Gao,Zhang Gang,"A study on M_n coding for guarding against theft and remote control device of an automobile," Proceedings of International Conference on Vehicle Electronics,pp.294- 297,1999.
[4] Khangura K.S.,Middleton N.V.,Ollivier M.M.,"Vehicle anti-theft system uses radio frequency identification,"Proceedings of IEEE
Colloquium on Vehicle Security Systems,pp.1-7,Oct. 1993.
[5] Hirano M.,Takeuchi M.,Tomoda T.,Nakano K.-I.,"Keyless entry system with radio card transponder [automobiles],"Proceedings of IEEE Transactions on Industrial Electronics,vol.35,no.2,pp.208-216, May 1988.
[6] Wan Lili,Chen Tiejun,"Automobile anti-theft system design based on GSM,"Proceedings of International Conference on Advanced Computer Control,pp.551-554,Jan. 2009.
[7] Jayendra G.,Kumarawadu S.,Meegahapola L.,"RFID-based anti-theft auto security system with an immobilizer," Proceedings of International Conference on Industrial and Information Systems,pp.441-446, Aug. 2007.
[8] Guo Hongzhi,Chen Hong,Ji Guohuang,Zhou Xin,"The vehicle passive keyless entry system based on RFID,"Proceedings of the 7th World Congress on Intelligent Control and Automation,pp.8612-8617,Jun. 2008.
[9] Zhixiong Liu,Guiming He,"A vehicle anti-theft and alarm system based on computer vision,"Proceedings of IEEE International Conference on Vehicular Electronics and Safety,pp.326-330,Oct. 2005.
[10] Karimi H.A.,Krishnamurthy P.,"Real-time routing in mobile networks using GPS and GIS techniques," Proceedings of the 34th Annual Hawaii International Conference on,pp.11,Jan. 2001.