Open Access Library Journal
2018, Volume 5, e4559
ISSN Online: 2333-9721
ISSN Print: 2333-9705

The Design and Realization of PKE System Based on ARM9

Tongfei Tu, Suyun Luo

College of Automotive Engineering, Shanghai University of Engineering Science, Shanghai, China
Email: 13222718328@163.com

How to cite this paper: Tu, T.F. and Luo, S.Y. (2018) The Design and Realization of PKE System Based on ARM9. *Open Access Library Journal*, **5**: e4559.
https://doi.org/10.4236/oalib.1104559

Received: April 1, 2018
Accepted: April 16, 2018
Published: April 19, 2018

Abstract

In order to solve the problem that the PKE (passive keyless enter) with a fixed-frequency used in middle and low grade cars was interfered and broken easily, which led to the damage of anti-theft system and even the loss of cars, and in order to ensure the PKE can be used long and be expanded and upgraded in the future, a new, low power consumption and high reliability PKE was designed with the S3C2410 microprocessor which is based on ARM9 and the RF transceiver chip nRF905 which has the function of frequency modulation. As frequency-hopping communication technology was used in the system, the information would not be disturbed or blocked in the communication process, which increased the reliability of the system. With reasonable power-management module, the system power consumption was greatly reduced. Test shows that the new PKE can well meet the practical application.

Subject Areas

Electric Engineering

Keywords

PKE, S3C2410, nRF905, Frequency-Hopping Communication Technology, Low Power Consumption

1. Introduction

With the progress of the times, the development of science and technology, and the increasing demand for automotive quality, more and more high-tech technologies are being used in automobile production. Safety and convenience are very important in the daily use of automobiles. As a new generation of anti-theft technology, the car's keyless entry system (PKE) is developed on the basis of the remote control door lock (RKE), increasing the ability to identify the owner's

identity. At present, the application of this technology has gradually come into the middle and low grade cars from high grade cars. It has gradually entered the middle and low-grade cars from high-end cars. However, in many mid-range and low-end cars, the keyless entry system uses a fixed frequency and is extremely vulnerable to interference and interception of signals from the surrounding environment.

In the system, the "key" uses a button battery as a power source, and its service life is limited. Therefore, the author designed a low-power, high-reliability wireless radio chip nRF905 based on highly scalable S3C2410 microprocessor and easy to implement frequency hopping communication technology.

2. Keyless Enters System Working Principle

The keyless entry system, PKE (passive keyless enter), works as follows: When the driver is close to the sensing area of the PKE system of the car, the key chain or smart card does not have to be taken out, and only by touching the door handle with hand, four drivers can be driven. The door lock motor is unlocked to open the door. Once the driver enters the car, the PKE system will detect if the "key" device is in the car. If the car is in the car, simply press the start button and the car engine will start. When the driver leaves the car, the PKE system will also detect whether the driver's position is near the system. If it is, then only need to press the lock switch on the handlebar, the door will be locked, and then press the lock switch again. The door will be completely locked. The door is not allowed to open from the inside, to ensure the safety of the car [1] [2]. The workflow of the keyless entry system is shown in Figure 1.

3. Keyless Enters the System Overall Design

3.1. Overall Design Idea

The keyless entry system is divided into two parts: the PKE "key" and the vehicle-mounted PKE system. Its block diagram is shown in Figure 2 and Figure 3. In the entire keyless entry system, the main control chip uses low power, high performance, highly scalable ARM9 processor S3C2410, RF transceiver module

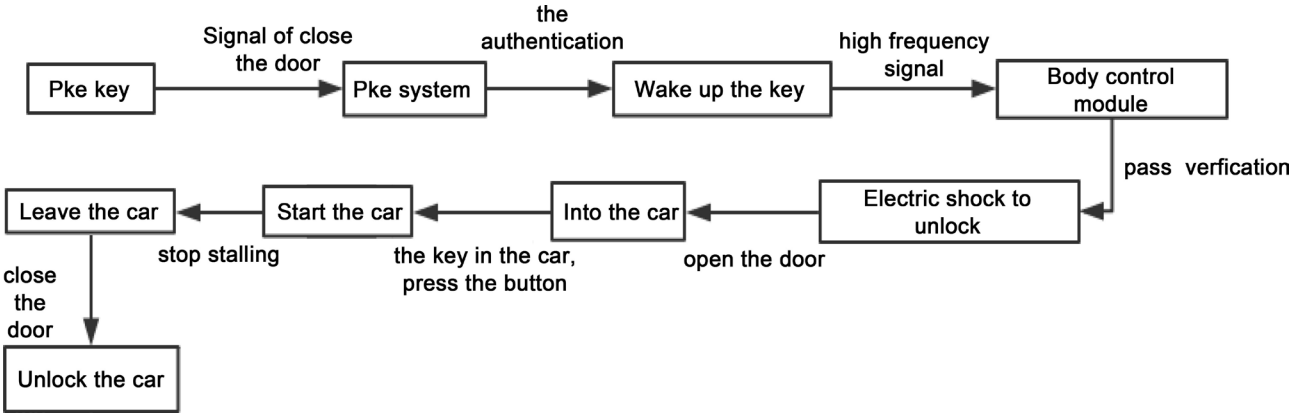

Figure 1. PKE overall work flow chart.

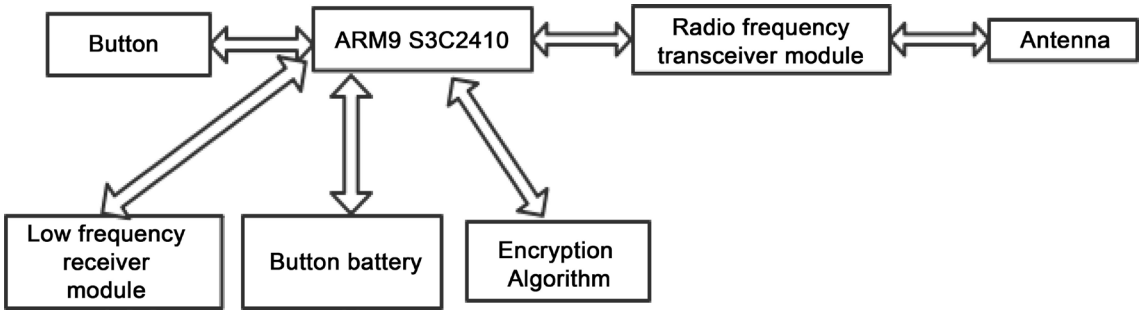

Figure 2. PKE "key" overall block diagram.

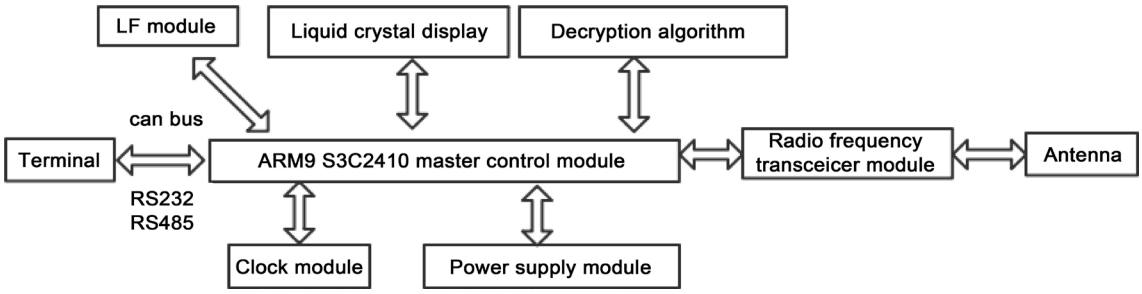

Figure 3. On-vehicle PKE overall block diagram.

uses a single-chip RF transceiver that is easy to implement frequency hopping communication.

The chip nRF905. Uses the SPI bus to communicate between the main control chip and the RF transceiver module. In order to ensure the security and confidentiality of the wireless information transmission process, a coded encryption and decryption technology is used. In addition, the vehicle-mounted PKE system provides CAN. Bus, RS232/RS485 interface to achieve the connection with the terminal equipment.

3.2. Low-Power Design

In the keyless enter system, only when the button in the door handle is pressed, then activate the on-board PKE send a low-frequency signals to PKE "keys", when the signal in the "key" save the id information is consistent, "keys" will be awakened. This process can prevent random noise or other disturbance signal awakens the "key", extend battery life.

On the other hand, the "key" awakened after, will send the corresponding high frequency signal to the on-board PKE, and each time only valid data communication can be done in a very short period time, the rest of the time PKE "key" will remain low power state.

3.3. Hardware Circuit Design

3.3.1. Microprocessor

The S3C2410 processor is a 16/32-bit RISC embedded processor designed by Samsung based on ARM920T processor core. This processor provides a cost-effective, low-power microcontroller solution for handheld devices and

general types of applications. It implements the MMU, AMBA bus and Harvard cache architecture, providing 1.1 MIPS/MHz performance. To reduce the cost of the entire system, the processor integrates many rich components on the chip. For power control logic, S3C2410 has many A kinds of power management scheme, so that each given task has the optimal power consumption [3].

3.3.2. Wireless RF Transceiver Module

The nRF905 is a monolithic radio frequency transceiver integrated chip from Nordic VLSI in Norway. The operating voltage is 1.9 to 3.6 V. It operates on three ISM (industrial, scientific and medical) channels at 433,868,915 MHz, and the conversion time between channels is less 650 μs. nRF905 consists of frequency synthesizer, receiver demodulator, power amplifier, crystal oscillator. It is composed of a modulator and does not need an external SAW filter. It has a built-in complete communication protocol, automatically processes the header and CRC (cyclic redundancy check), and can automatically perform Manchester encoding/decoding by on-chip hardware. Very convenient. In addition, nRF905 has Shock-Burst working mode. Its power consumption is very low. The current is only 11 mA when transmitting at −10 dBm output power. The current when operating in the receive mode is 12.5 mA, built-in power-down mode and standby mode, easy to achieve energy saving. nRF905 current in power-down mode is 2.5 μA, in standby mode. When the crystal frequency is 16 MHz, the power consumption is 32 μA. The nRF905 uses Gaussian frequency shift keying (GFSK) modulation method. Strong anti-interference ability, can well reduce the impact of noise environment on system performance [4]. nRF905 can carry out artificial carrier frequency control, easy to implement frequency hopping communication.

3.3.3. SPI Connection

S3C2410 and nRF905 use SPI interface for two-way communication. nRF905's SPI bus SCK (SPI clock), MISO (SPI output), MOSI (SPI input), CSN (SPI enable). S3C2410 through control TRX_CE, PWR_UP, TX_EN high and low levels of the three pins make the nRF905 in Shock Burst receive mode, Shock Burst transmit mode, power down mode, and standby mode. CD (carrier sense), AM (address match), DR (data ready) for 3 digital output pins, the connection between S3C2410 and nRF905 is shown in **Figure 4**.

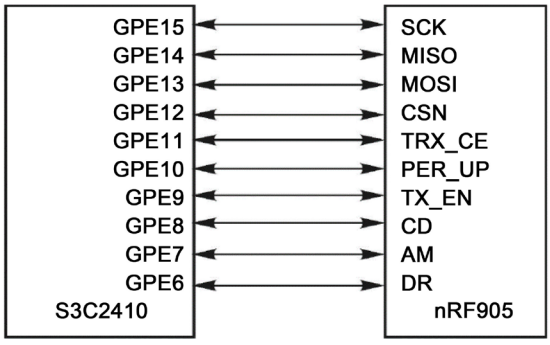

Figure 4. Diagram of connection between S3C2410 and nRF905.

4. Software Design and Implementation of the System

4.1. Wireless Transceiver Process

4.1.1. Launch Mode Process

1) The S3C2410 puts the TRX CE pin of the nRF905 low so that it is in standby mode and communicates with it via the SPI interface to configure the register;

2) When the S3C2410 has data to send to a specified node, the address of the receiving node is written into the nRF905 transmit address register TX-address through the SPI interface;

3) S3C2410 through the SPI interface will send valid data to be written nRF905 send valid data register TX-Payload;

4) The S3C2410 sets the PWR_UP, TRX_CE, and TX_EN pins high so that the nRF905 is in the Shock Burst transmit mode;

5) nRF905 Shock Burst TM internal processing: the wireless system automatically powers up, completes the data packet (adds preamble and CRC check bytes), sends data packets (rate 100 kbps, GFSK modulation, Manchester encoding), data transmission High Data Ready (DR) pin when done;

6) Set the AUTO RETRAN pin high, nEF905 continuously retransmits until TRX CE is set low;

7) After the data transmission is completed, the S3C2410 de asserts the TRX CE pin of the nRF905 so that the nRF905 is again in standby mode.

The program flow chart of nRF905 sending mode is shown in Figure 5.

4.1.2. Receive Mode Flow

1) The S3C2410 puts the TRX CE pin of the nRF905 low so that it is in standby mode and communicates with it via the SPI interface to configure the register.

2) The S3C2410 sets the PWR UP and TRX CE pins of the nRF905 high and the TX EN pin is set low, enabling the nRF905 to enter the Shock Burst receive mode.

3) The nRF905 monitors the frequency information in the air. When it finds and receives the carrier with the same frequency, it receives the data and sets the carrier sense (CD) pin high.

4) When the address of the data packet received by the nRF905 is the local address, the address match (AM) pin is set high;

5) When the nRF905 receives a valid data packet (CRC check is correct), the nRF 905 removes the preamble, address and CRC bits, and the data ready (DR) pin is set high;

6) S3C2410 sets TRX_CE of nRF905 low, making nRF905 back to standby mode.

7) S3C2410 reads valid data at a suitable rate via the SPI interface.

8) After all valid data is read out, the nRF905 sets the data ready (DR) pin and the address match (AM) pin low. The program flow chart of nRF905 receiving mode is shown in Figure 6.

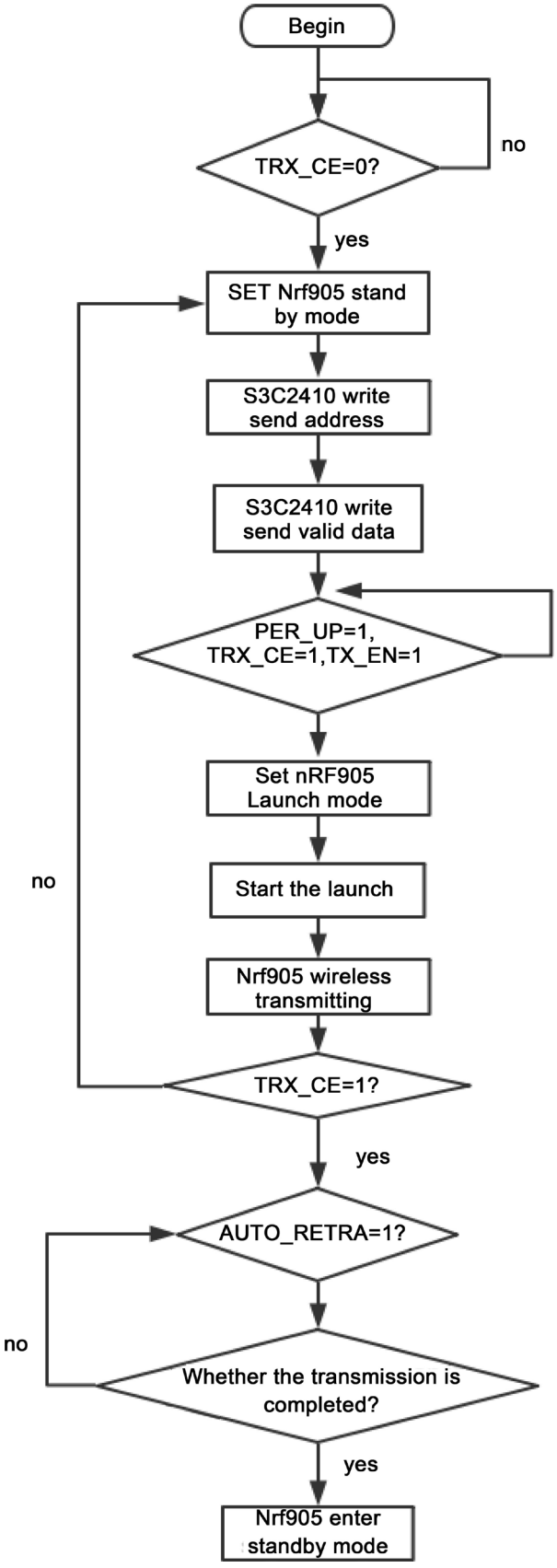

Figure 5. Wireless transmission flow chart.

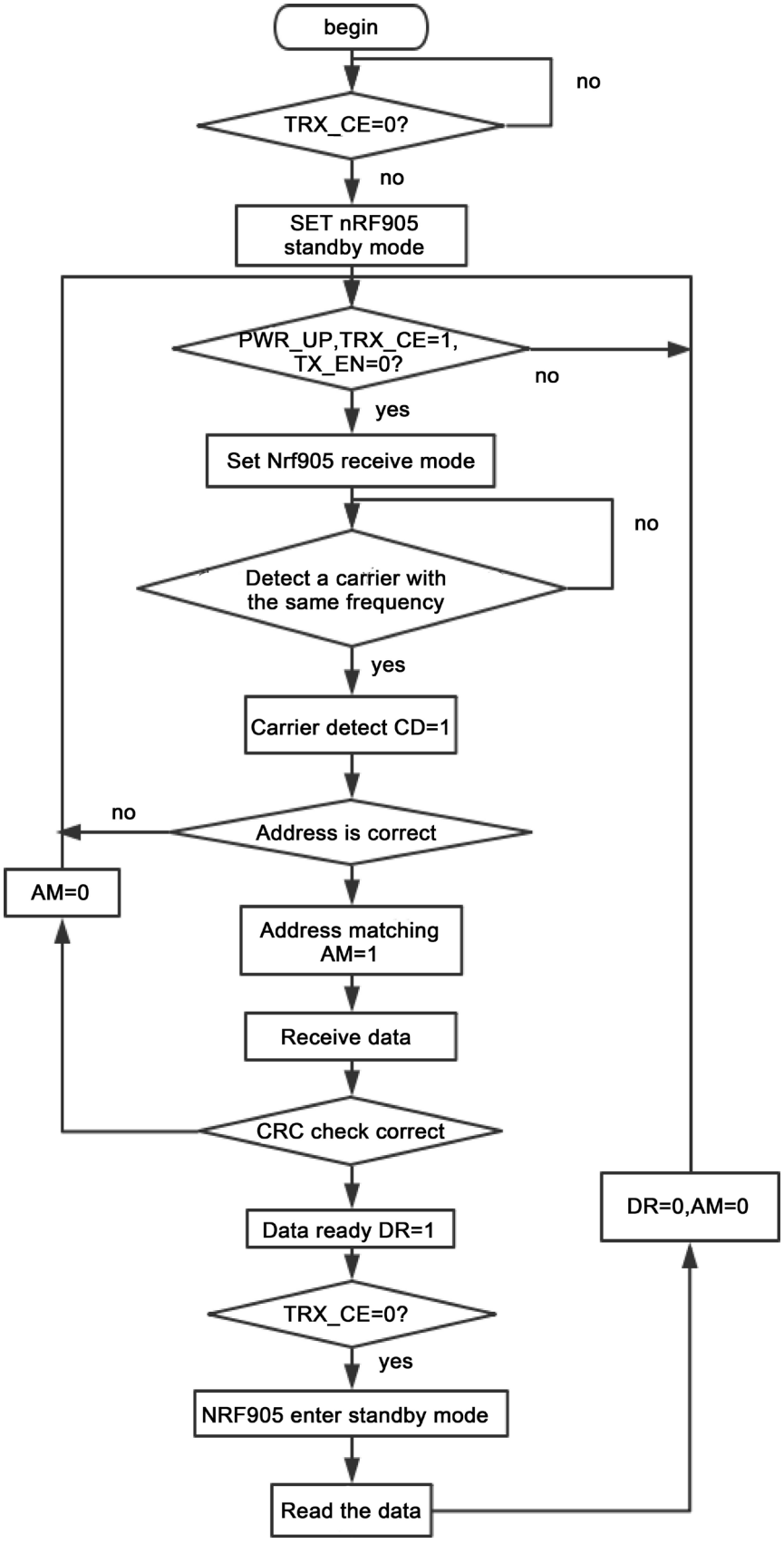

Figure 6. Wireless receive flow chart.

4.2. Radio Frequency Hopping Communication

4.2.1. Wireless Frequency Hopping Communication Design

In keyless entry systems of low-end and mid-range cars, due to the use of fixed carrier frequencies, they are susceptible to interference, interception, and cracking during communication, and the reliability is reduced. However, the interference caused by the system environment only exists within a certain period of time, and interference occurs. The frequency is relatively fixed. Therefore, the use of frequency hopping technology can effectively avoid the interference frequency, and continue to communicate with another less interfered with the frequency. This system uses nRF905 wireless RF chip can achieve artificial carrier frequency control, for frequency-hopping communication Provides good support, and provides a large number of channels. You can use the HFREQ PLL and CH NO pins of the RF configuration register of the.nRF905 to set the frequency in conjunction to achieve frequency hopping, as in Equation (1).

As shown, the subscript d indicates that the binary data stored in the corresponding register is converted to decimal data.

$$\mathrm{FRP} = \left(422.4 + \frac{\mathrm{CH}_{NO_d}}{10}\right) * \left(1 + \mathrm{HFREQ}_{\mathrm{PLLd}}\right) \mathrm{MHZ} \tag{1}$$

The HFREQ_PLL controls the PLL to operate at 433 or 868/915 MHz: when it is "0", it means that it works in the 433 MHz band and the channel difference is 100 kHz; when it is "1", it means that it works in the 868/915 MHz band and the channel difference is 200 kHz. In practical applications, for a certain fixed antenna, only one frequency band allows the chip to perform the best communication performance. Therefore, an antenna can support up to 29 communication channels, when communication is interfered on a channel, able to pass frequency hopping to another channel to continue communication [5].

In this system, nRF905 uses 433 MHz band, Using 5 channels from 420.1 to 440.1 MHz for communication, the spacing between two adjacent channels is 5 MHz. In frequency hopping communication, in order to prevent communication parties from making mistakes during communication, frequency hopping tables are read. Take inconsistent data and make the system chaotic and unable to communicate the problem, improve the reliability of communication, will be used as the handshake frequency of the two parties of the 420.1 MHz. When the system has problems or the communication between the two parties is unsuccessful, immediately return to the handshake frequency from the frequency hopping. The initial value of the table restarts communication [6]. The remaining four channels are used as data channels for frequency hopping communication for transmission. Valid data from the PKE "key" to the car PKE and the confirmation signal of the vehicle PKE data.

4.2.2. Wireless Frequency Hopping Communication Process

If the PKE "key" receives data from the vehicle PKE after the current data channel sends data to the vehicle-mounted PKE, the PKE "key" will end the commu-

nication and go to sleep until the next functional cycle. If not received Car PKE data confirmation signal, PKE "key" will retransmit the frame data to the vehicle PKE; if no data confirmation signal is received after three consecutive retransmissions, the data channel value will be modified so that in the next transmission cycle, PKE The "key" will carry out data communication with the vehicle-mounted PKE on another channel to complete a data channel frequency hopping. After the vehicle-mounted PKE jumps into the data channel, it works in the receiving state and waits for the PKE "key" to send data. If valid data is received, Send a data confirmation signal to the PKE "key", end this communication, and jump back to the handshake channel to wait for the next PKE "key" connection request. If the vehicle PKE does not receive any data of the PKE "key" within the timeout interval, it will Abandon this communication and jump back to the handshake channel. The frequency hopping communication flow chart is shown in Figure 7.

5. Conclusion

This paper presents a low-power, high-reliability keyless entry system. Tests

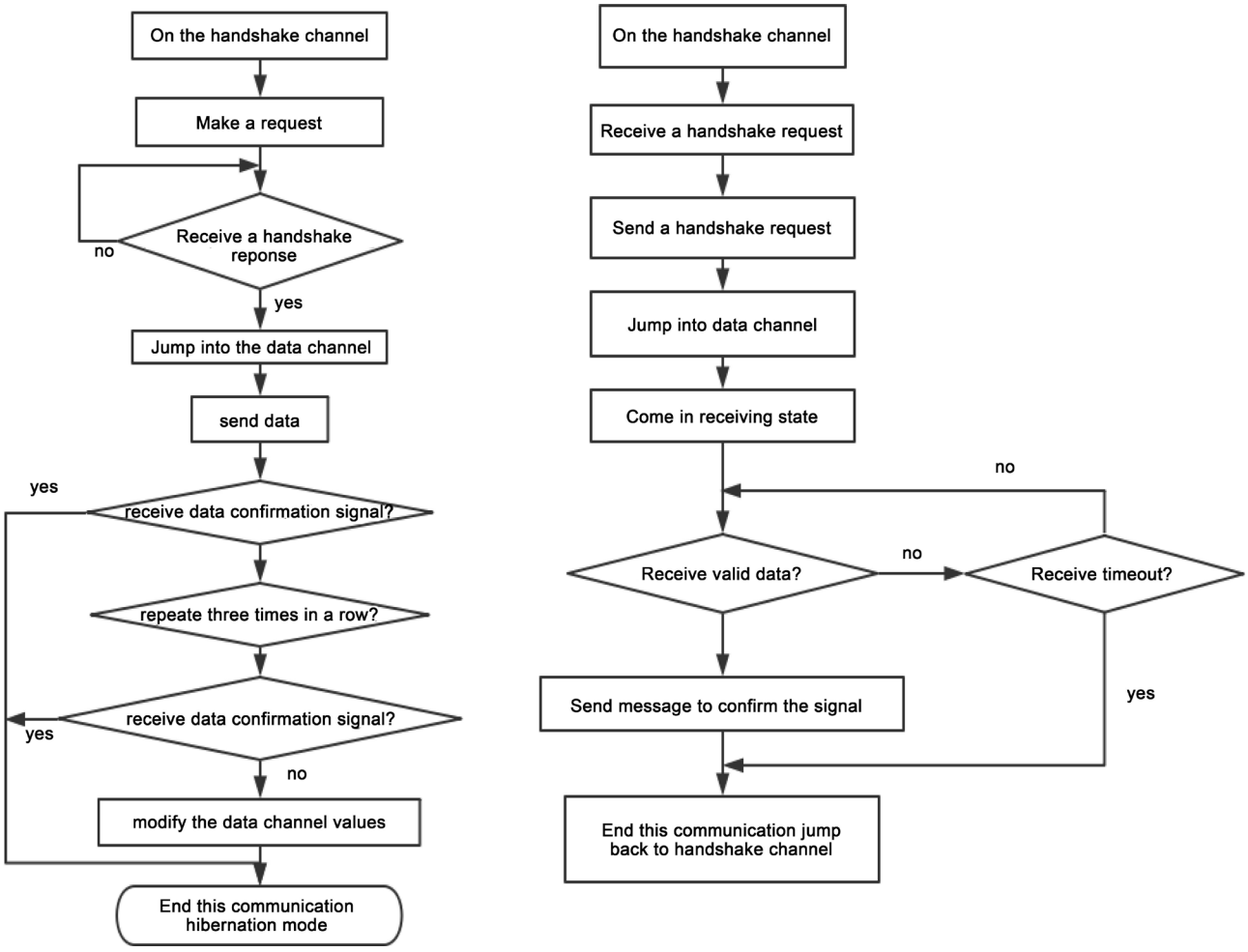

Figure 7. Frequency hopping communication flow chart.

have shown that this system has very low power consumption in standby mode, which can meet the requirements of PKE key for a long time use; meanwhile, the application of frequency hopping communication technology has greatly improved the anti-jamming capability and anti-interception capability of wireless communication systems and ensured the safety of PKE systems' comprehensiveness and reliability. In addition, the reliable communication distance of this system in an open environment can reach 180 m, which can meet the practical application requirements of middle- and low-end car keyless entry systems. Because of the small size, low power consumption, low cost and high performance, the system can be expanded and upgraded to a remote control system with a wireless network. Therefore, the keyless entry system designed this time is worth promoting.

References

[1] Chang, L.-N. and Luo, X.-C. (2009) The PKE (Passive Keyless Entry) Demo Based on uPD780503 and uPD780881. *Global Electonics China*, No. 7, 40-43.

[2] Yang, B. (2010) The Detailed Analysis of PKE Used in Shanghai GM Cars. *Auto Maintenance*, No. 5, 25-27.

[3] Xu, Y.-H., Ma, Z.-M., Wang, L., *et al*. (2010) ARM9 Embedded System Design—Based on S3C2410 and Linux. 2nd Edition, Beijing University of Aeronautics and Astronautics Press, Beijing, 64-69.

[4] Gao, Z.-F. and Zhu, S.-A. (2006) Multipoint Wireless Communication Module on MSP430 and nRF905. *Chinese Journal of Electron Devices*, **29**, 264-267.

[5] Yang, J. (2007) Development and Implementation of Wire-Less RF Data Acquisition System Based on the nRF905. Central South University, Department of Computer Science and Engineering, Changsha, 46-47.

[6] Lin, J. and Li, X.-C. (2010) Design of Wireless Frequency-Hopping Communication System Based on nRF905. *Information Technology*, No. 3, 99-102.