文章编号：1672-2892(2010)01-0118-05

基于跳频通信的汽车智能防盗器设计

李新超，李继凯

(茂名学院 计算机与电子信息学院，广东 茂名 525000)

摘 要：为解决现有普通汽车电子防盗器采用固定频率通信容易被破解及复制的问题，利用具有载波频率调制功能的射频收发芯片 nRF905 设计了一款新的防盗器，该防盗器在通信过程中不断改变通信频率，使信息无法被干扰或截获，防盗器很难被复制、破解，通过通信方案的优化和程序设计增加了跳频通信的可靠性，增加的双向通信功能使车主能及时掌握汽车状况及报警信息，并通过多传感器检测电路的设计增加了防盗器的可靠性，经测试达到了良好的防盗效果。

关键词：汽车防盗器；nRF905 芯片；跳频通信；通信可靠性

中文分类号：TN914.413 文献标识码：A

Intelligent car anti-theft device design based on frequency hopping communication

LI Xin-chao，LI Ji-kai

(College of Computer and Electronic Information，Maoming University，Maoming Guangdong 525000，China)

Abstract: In order to solve the problem that the existing anti-theft device was easily to be cracked and reproduced when communicating at a fixed-frequency, a new anti-theft device was designed on nRF905 which had the function of frequency modulation. Since the communication frequency was kept changing, the information could not be interfered or intercepted, and the anti-theft device was difficult to be reproduced and cracked. Through the communications program optimization and program design, the reliability of the frequency-hopping communications was improved. The car owner could gain prompt access to car conditions and alarm information through the two-way communication function. The multi-sensor detection circuit design could improve the reliability of the anti-theft device. The new anti-theft device has been tested to have a good effect，so it has good prospects of application.

Key word: car anti-theft device ;nRF905 ;frequency-hopping communication ;communication reliability

随着社会经济的发展，人们生活水平的提高，汽车已逐步进入家庭，而如何有效防止汽车被盗也成为车主比较关心的问题。目前在汽车防盗器中，普通的电子遥控防盗器由于价格便宜占有很大的市场分额。但普通的电子遥控防盗器多为固定载波频率通信，容易被干扰、截获和破解[1]。有报道说一般的遥控锁在 30 s 内就可被专用的解码器复制，1 min 内就可破解。普通的电子遥控防盗器多为单向通信，车主可以遥控汽车上锁、解锁，但汽车信息不能及时反馈给车主。

针对普通电子防盗器的不足，我们将军事通信中应用的跳频通信技术应用到汽车智能遥控防盗器的设计中。在通信过程中不断改变双方的通信频率，使信息传递难以被跟踪、干扰或截获、破解，将有效提高防盗系统的安全性和可靠性。

1 系统总体方案设计

系统由车载终端、人持终端两部分构成。车载终端主要完成人机控制指令的接收执行，执行汽车上锁解锁指令，并完成对汽车防盗信息的检测发送；人持终端主要完成车主对汽车的上锁、解锁的控制指令的发送，并接收车载终端发来的汽车相关报警信息及指令执行情况信息。系统功能结构如图 1 所示。

收稿日期：2009-08-10；修回日期：2009-09-24

基金项目：茂名学院科研基金资助项目(203259)

2　系统的电路设计与实现

2.1 车载终端的电路设计

车载终端主要完成汽车防盗信息的监测并将汽车异常状况信息发送给车主，接收执行人持终端控制指令如对汽车上锁解锁等，针对目前防盗器主要依赖振动传感器检测盗窃信息存在不可靠的问题[2]，设计了多信息融合的传感器电路，通过监测车门、车窗、车座位来提高防盗器的可靠性，增加的备用电源管理功能保证防盗器在主电源线被剪的情况下仍能正常工作，主要由主控 MCU 模块、无线跳频通信模块、汽车门窗监测、电源监控、振动检测、车内是否有人监测模块构成。

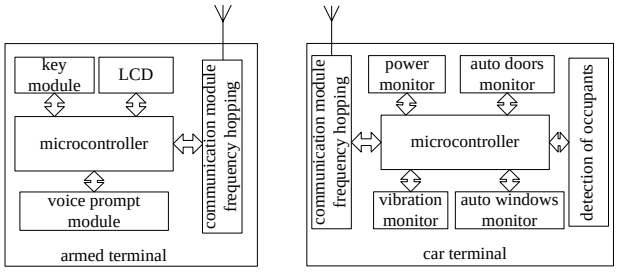

Fig.1 Structure diagram of the car anti-theft system
图 1 系统总体结构框图

2.1.1 主控 MCU 模块电路

主控 MCU 主要负责整个系统的协调控制，传感器信息的检测处理，跳频通信模块的配置、信息发送接收等，采用 C8051F340 实现。C8051F340 是美国 Cygnal 公司的混合信号系统级集成芯片，具有与 8051 兼容的高速 CIP-51 内核，片内集成了数据采集和控制系统中常用的模拟、数字外设及其他功能部件，内部时钟频率可达到 48 MHz[3]。具有增强型的 SPI 接口，可方便实现对 nRF905 的控制。

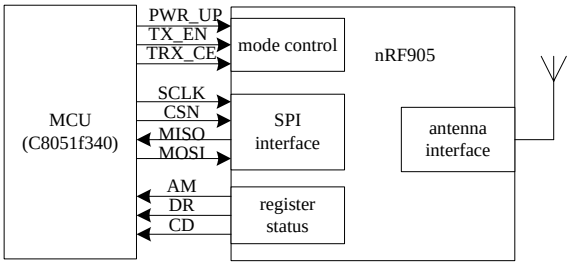

Fig.2 Interface circuit of nRF905 with microcontroller
图 2 nRF905 与单片机接口电路

2.1.2 跳频通信模块硬件电路

跳频通信模块硬件电路采用 Nordic 公司推出的单片射频收发器芯片 nRF905 实现，其功耗非常低，以–10 dBm 的输出功率发射时电流只有 11 mA，在接收模式时电流为 12.5 mA，传输距离大于 100 m。工作于 433/868/915 MHz 3 个 ISM 频道(可以免费使用)。nRF905 可以自动完成处理字头和循环冗余码校验的工作，可由片内硬件自动完成曼彻斯特编码/解码，使用 SPI 接口与微控制器通信，配置非常方便，性能可靠，并可以实现人工载波频率控制，具有 128 个可选频点，频点间隔 100 kHz，频点切换时间为 650 μs，可快速实现频点切换[4]。使用该芯片可构成无线跳频通信的收发模块，模块电路及单片机接口电路如图 2，通过 PWR_UP,TRX_CE 和 TX_EN 与单片机连接实现工作模式配置。通过 CD,AM,DR 进行载波检测、地址检测、中断检测，通过 SPI 接口与单片机通信实现载波频率、通信指令数据格式的配置及数据的接收。

2.1.3 车门车窗监测模块

通过将光电检测二极管置于车门车窗关口，当车门或门窗没有锁紧时，对应的光电检测电路会检测到相关信息[5]，在车内无人时车载终端通过汽车主控接口通知汽车微处理系统启动自动关门关窗电路，并提醒车主车门或车窗没有锁好，在防盗状态下车门车窗被打开则发出报警信号。

2.1.4 车内有无人检测模块

通过放置在汽车座位下的应变电阻设计的压力测量装置，判断车内是否有人，如车内无人，车防盗锁系统未启动，则延时 1 min 自动上锁；若汽车防盗锁启动状态下，如若有人，即有可能是有人盗车，防盗器立刻进行报警。

2.1.5 车外振动检测模块

车外振动检测用来检测当车处于防盗状态时，是否有人对汽车进行碰撞，如有则报警。它采用了振动传感器 Z04B[6]，它是一种高灵敏振动模块，能检测极其微弱的震动波；安装简便，不受任何角度限制；抗干扰性好，对外界声响无反应，具有抗雷电及鞭炮干扰能力，输出为瞬态脉冲，用来构成可靠的汽车振动检测模块。

2.1.6 电源测控模块

设计了备用电源管理功能，在汽车主电源被剪断时，备用电源供电并将该情况反馈给车主，提高防盗系统的安全性和可靠性。

2.2 人持终端的电路设计

人持终端完成对汽车的上锁、解锁等控制指令发送，并接收车机发来的汽车相关信息，如振动情况、车门车窗开关情况信息，并发出语音提示。由主控单片机电路和跳频通信模块、人机接口模块构成，其中主控单片机电

路和跳频通信模块与车载终端部分相同。

人机交互接口模块电路主要由按键电路完成人操作指令的发送，采用 LCD 液晶显示电路使操作更为方便，采用 ISD1820 设计语音提示电路进行报警提示及车载终端指令执行情况提示。

3 系统的软件设计与实现

3.1 nRF905 的配置过程及跳频通信的实现

3.1.1nRF905 的配置过程

如图 2 所示，nRF905 通过 CPU 控制 nRF905 的 3 个引脚 PWR_UP,TRX_CE 和 TX_EN 的高低电平来决定其 4 种工作模式(如表 1 所示)，通过 nRF905 的 CD,AM,DR 三个引脚进行载波检测、地址检测、中断检测，在表 1 中的前两种模式下，MCU 通过 SPI 接口配置 nRF905 的 5 个内部寄存器(状态寄存器、射频配置寄存器、发送地址寄存器、发送数据寄存器、接收数据寄存器)。其中状态寄存器包含数据准备好引脚状态信息和地址匹配引脚状态信息；射频配置寄存器包含收发器配置信息，如频率和输出功能等；发送地址寄存器包含接收机的地址和数据的字节数；发送数据寄存器包含待发送的数据包的信息，如字节数等；接收数据寄存器包含要接收的数据的字节数等信息。

表 1 nRF905 的工作模式

Table 1 nRF905 operational modes

PWR_UP	TRX_CE	TX_EN	operating modes
0	X	X	Power-down and SPI-Programming
1	0	X	Standby and SPI-Programming
1	1	0	Radio Enabled-ShockBurst TX
1	1	1	Radio Enabled-ShockBurst RX

3.1.2 nRF905 的无线收发过程

1) 发射模式设置及过程

a) 上电以后 MCU 首先配置 nRF905 模式，先将 PWR_UP,TX_EN,TRX_CE 设为(10X)配置模式。

b) MCU 通过 SPI 将 RF 寄存器的频率配置数据，配置数据移入 nRF905 模块。

c) 当 MCU 有数据需要发往规定节点时，接收节点的地址(TX-address)和有效数据(TX-payload)通过 SPI 接口传送给 nRF905。

d) MCU 设置 TRX_CE,TX_EN 为高启动传输。

e) nRF905 内部处理：无线系统自动上电、数据包完成(加前导码和 CRC 校验码)、数据包发送(1000kbps,GFSK,曼切斯特编码)。

2) 接收模式

a) 上电以后 MCU 首先配置 nRF905 模式，先将 PWR_UP,TX_EN,TRX_CE 设为(10X)配置模式。

b) MCU 通过 SPI 将 RF 寄存器的频率配置数据，配置数据移入 nRF905 模块。

c) 设置 TRX_CE 高，TX_EN 低来选择 RX 模式，nRF905 监测空中的信息。

d) 当 nRF905 发现和接收频率相同的载波时，载波检测(CD)被置高。

e) 当 nRF905 接收到有效的地址时，地址匹配(AM)被置高。

f) 当 nRF905 接收到有效的数据包(CRC 校验正确)时，nRF905 去掉前导码、地址和 CRC 位，数据准备就绪(DR)被置高。

g) MCU 设置 TRX_CE 低，进入 standby 模式(待机模式)。

h) MCU 可以以合适的速率通过 SPI 接口读出有效数据。

i) 当所有的有效数据被读出后，nRF905 将 AM 和 DR 置低。

3.1.3 跳频的实现

nRF905 可以实现人工载波频率控制，只需要修改 nRF905 的 RF 工作频率寄存器的 CH_NO 和 HFREQ_PLL 就可以选择不同的载波频率，实现跳频。位变量 HFREQ_PLL 为 0，表示工作在 430 MHz 频段，频道差为 100 kHz；为 1，则表示工作在 868/915 MHz 频段，频道差为 200 kHz。因此共有 1 024 种通信频率。通信频率(H)为 H=(422.4+(CH_NO)$_{10}$/10)×(1+HFREQ_PLL)。

例如 CH_NO=(001001100)$_2$=(76)$_{10}$，HFREQ_PLL=0，则 H=(422.4+76/10)×(1+0)=430.0 MHZ。

本系统统一设置为工作频段为 430 MHz，频道差为 100 kHz，每一个频点间隔为 100 kHz，随机数产生于 0~128 之间，跳频带宽为 12.8 MHz，完成一次跳频时间 T≤800 μs[4]。

3.2 基于跳频通信遥控防盗器的可靠性设计及系统实现

3.2.1 生成随机跳频表增强安全性

为了增加安全性，每对密码锁除具有唯一对应的 32 位加密地址外还增加了一一对应的随机跳频表，第一次使用时，将车机、人机对应的设置开关打开，人持终端可以产生一个随机的跳频表，并将该跳频表通过握手频率发送给车载终端，经返回校验无误时将该跳频表存储在掉电保护的非易失 FLASH 存储器中，关闭设置开关，在保证两机有一一对应的跳频频率表的同时又很好地保护了频率表的安全性，只要双方按照事先约定的与跳频表对应设置一致的 CH_NO 和 HEFREQ_PLL 的数值便可实现跳频通信，增加了无线通信的可靠性、安全性。

3.2.2 设定握手及出错、丢包回归频率，保证通信可靠

跳频通信的一个突出问题就是尽管可靠性高，但一旦通信双方通信错误，引发跳频表读取数据不一致，系统将发生混乱，无法通信。为解决这一问题，提高防盗器安全性和可靠性，系统设定了一个固定频率作为握手频率，人机和车机之间的通信是先从一个双方设定的握手频率来进行握手连接，该频率仅携带目标地址和握手请求或应答信号，即使被截获也不影响系统的安全性。当系统出现问题双方通信不成功时，马上回到握手频率，从跳频表初始值重新开始通信。在一次指令信息传输进行过程中屏蔽中断，保证信息的可靠传输。

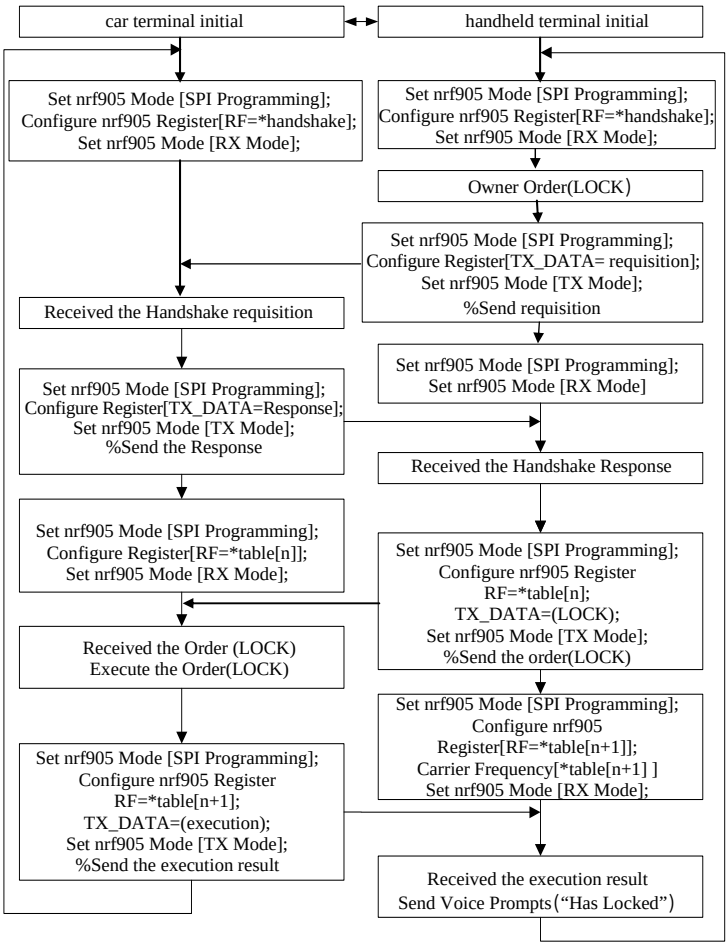

Fig.3 Flowchart of the anti-theft device

图 3 防盗器工作流程图

3.2.3 系统工作过程

系统上电初始化跳频表后，人机和车机都通过设定系统的工作模式(Set nRF905 Mode)，配置 nRF905 的寄存器(Configure Register)，使其工作在握手频率，接收模式(RX Mode)。当其中一端收到中断请求时(车主指令/报警信息等)，便发起握手请求，握手完成后，进行两次跳频通信过程，完成信息的发送及反馈，在发送过程中，发送方发出握手请求或指令后等待响应或反馈的时间不超过 200 ms，否则便认为通信出错，发起方重新发起请求。以车主发出上锁指令为例，系统整个工作过程如图 3，其他车主指令发送、车载报警信息的发送过程类似。

4　结论

经测试该系统在小区内的可靠通信距离可达到 150 m，满足一般汽车防盗器的实际应用要求，采用跳频通信保证了防盗器不易被截获破解，通过通信方案的优化设计，保证了跳频的通信可靠性，进一步提高了防盗器的安全性和可靠性。将该系统简化外围电路设计后也可用于摩托车防盗及其他防盗系统。

参考文献：

[1] 房颖,魏冬至. 汽车防盗系统综述[J]. 科学之友, 2007(11):100-102.
[2] 莫长江. 汽车 GSM 语音防盗系统设计[J]. 信息与电子工程, 2008,6(3):223-225.
[3] 新华龙电子. C8051F340 中文手册[Z]. 新华龙电子公司, 2007.
[4] 迅通科技. nRF905 手册[Z]. 迅通科技公司, 2006.

[5] 肖莹慧,欧阳君. 基于多信息融合技术的智能汽车防盗报警系统研究与设计[J]. 计算机与数字工程，2009,37(3)：114-116
[6] 王莉莉,吕芳. 汽车防盗报警装置的设计[J]. 机械工程与自动化, 2008(6):171-172.

作者简介：

李新超(1980-)，男，河南省南阳市人，硕士，实验师，从事生物医学电子学研究. email:2005lixin@163.com.

李继凯(1963-)，男，河南省原阳市人，硕士，副教授，从事生物医学电子学研究.

(上接第75页)

作者简介：

李　娟(1984-)，女，江苏省丰县人，在读硕士研究生，主要研究方向为信号与信息处理.email: sisisusan12@126.com.