基于 μC/OS-Ⅱ和 GPRS 的无线 RFID 读写器的研究与开发

王延政,李瑞祥,王立青

(上海理工大学 光电信息与计算机工程学院,上海 200093)

摘 要:针对目前 RFID 读写器无法随身携带,实现远程的 IC 卡读写操作的问题,采用 GPRS 无线网络作为数据传输的载体,实现了无线 RFID 读写器的开发。采用 μC/OS-Ⅱ嵌入式实时操作系统作为读写器终端的软件平台,在 ARM7 系列微处理器 LPC2148 上实现了对 IC 卡的发行、加值、消费、操作记录查询与汇总、数据采集以及无线传输。采用动态密钥加密算法很好地保证了 IC 卡的数据安全。应用结果表明,该 RFID 读写器运行稳定可靠、响应速度快、安装及操作方便、便于携带,具有一定的实用性和推广价值。

关键词:μC/OS-Ⅱ;GPRS;LPC2148;动态密钥

中图分类号:TP368 **文献标识码**:A **文章编号**:1674-7720(2011)07-0022-03

The study and development of wireless RFID reader based on μC/S-Ⅱ and GPRS

Wang Yanzheng, Li Ruixiang, Wang Liqing

(School of Optical-Electrical and Computer Engineering, Shanghai University of Science and Technology, Shanghai 200093, China)

Abstract: View the problem that the present RFID reader can not be carried easily and remote read and write operations, using GPRS wireless data transmission network as a carrier, to achieve a wireless RFID reader development. Embedded real time operating system μC/OS-Ⅱ as a reader terminal software platform achieves the IC card issuing, value-added, consumption, operating records check and summary, data acquisition and wireless transmission, based on LPC2148 of ARM7 family microprocessor. Dynamic key encryption algorithm ensures a good IC card data security. The application results show that the RFID reader is stable and reliable, fast response, easy to operate, easy to install, easy to carry with some practicability and promotional value.

Key words: μC/OS-Ⅱ; GPRS; LPC2148; dynamic-key

传统的 RFID 读写器多采用有线接入的方式实现与数据中心(上位机)的通信,即使部分 RFID 读写器终端实现了无线的数据传输,但也多是采用短距离的无线通信方式,最终还是要经过现场的有线设备实现与数据中心的通信,无法满足远距离、跨区域、便携式的 RFID 读写器的应用需求。本文介绍的无线 RFID 读写器的开发是以提高系统的稳定性、便携性、安全性为目标,采用嵌入式系统的设计思想,硬件方面使用功能强大的 ARM 处理器 LPC2148,外扩 GPRS 无线模块实现终端数据的实时上传。LPC2148 丰富的 IO 口资源使其能够外扩更多的外设,保证了终端功能的实现。软件方面引入实时多任务嵌入式操作系统 μC/OS-Ⅱ,进行多任务的调度,在提高系统稳定性的同时降低了系统的开发难度。

1 GPRS 简介

通用分组无线业务 GPRS (General Packet Radio Service)是在现有 GSM 系统上发展起来的一种新的承载业务,目的是为 GSM 用户提供分组形式的数据业务,而不需要利用电路交换模式的网络资源,从而提供了一种高效、低成本的无线分组数据业务。GPRS 充分利用共享无线信道,实现了与标准 Internet 的无缝连接,采用 IP Over PPP 实现数据终端的高速、远程接入。无线 GPRS 网络所具有的永远在线、按流量计费、传输速率高以及

支持 X.25 和 IP 协议等突出特点，特别适合于 RFID 读写器系统这样间断、突发性的数据传输。

2 读写器硬件组成

2.1 硬件系统原理

IC 卡无线手持机的硬件系统结构框图如图 1 所示。图中，LPC2148 为终端的主控单元，通过 GPIO 口与 IC 卡读卡芯片 MF RC500 相连实现对 IC 卡的读写；通过串口 1(URRT1)与 GPRS 模块 MC55 相连实现 GPRS 数据传输；系统外扩一块 I²C 接口的 E²PROM 芯片 24C256，用于存储终端设置参数以及暂存 IC 卡用户在本机的交易信息；通过 LPC2148 自带的 USB 接口实现上位机对读写器相关参数的设置以及交易信息的离线上传。

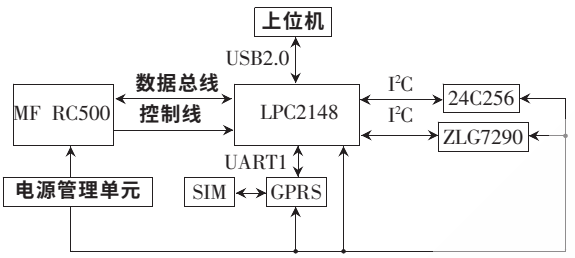

图 1 硬件系统结构框图

2.2 读写器的微处理器

手持机终端系统的核心部分是由 LPC2148 及其外围电路构成的最小系统电路。LPC2148 是基于一个支持实时仿真和嵌入式跟踪的 32/16 bit ARM7 TDMI-S CPU 的微控制器，并带有 32 KB 和 512 KB 嵌入的高速 Flash 存储器。较小的封装和很低的功耗使得 LPC2148 特别适用于 POS 机等小型的应用场合。LPC2148 提供多达 45 个高速 GPIO 口以及 USB2.0 全速设备控制器，使其成为本系统设计的理想选择。

2.3 读写器的 IC 卡读写模块

IC 卡读写模块选用 Philips 公司 Mifare 卡专用读卡芯片 MF RC500 及其相关的外围电路、射频天线等，实现手持机与 IC 卡之间的数据通信。MF RC500 是应用于 13.56 MHz 非接触式通信中高集成读卡 IC 系列之一，利用了先进的调制和解调概念，在 13.56 MHz 下，完全集成了所有类型的被动非接触式通信方式和协议，并支持 ISO14443A 所有的层。

2.4 匹配电路及天线的设计[1]

MF RC500 是一个单独的读卡器集成电路，在本系统中，MF RC500 与 Mifare 卡之间的数据交互是通过 RF 天线来完成的。参照 MF RC500 数据手册，采用直接匹配的天线，即可实现该读写器与 Mifare 卡之间的数据通信和能量传递，其推荐的工作距离可达 100 mm。直接匹配天线的匹配电路如图 2 所示，主要包括：

(1)EMC 滤波：Mifare 系统的工作频率为 13.56 MHz，由石英振荡器发生，但它同时也产生高次谐波。为了符合国际 EMC 规定，13.56 MHz 中的 3 次、5 次和高次谐波要被良好地抑制。本系统使用如图 2 所示的 $L1$、$L2$、$C11$、$C13$ 组成的低通滤波器来实现 EMC 滤波。

(2) 接收电路：MF RC500 的内部接收部分使用了一个新的接收概念，即使用卡响应的副载波负载调制所产生的两个边频带，由图 2 中的 $R9$、$R10$、$C9$、$C10$ 组成接收电路。

(3)阻抗匹配：在图 2 中由电容 $C11$ 和 $C13$ 组成，电容的值由天线本身和环境因素来决定，本系统 $C11$、$C13$ 均取 47 pF。该部分电路主要是为了实现滤波和天线之间的阻抗匹配，以使天线的性能达到最佳。

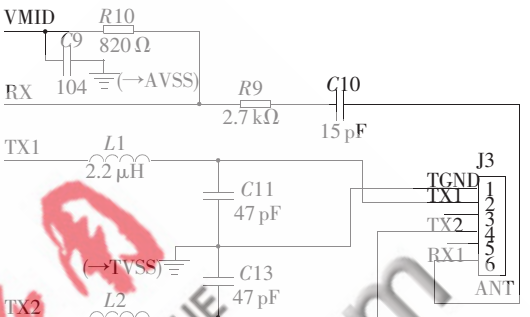

图 2 直接匹配天线的匹配电路

2.5 读写器无线传输模块

系统的无线数据传输通过内嵌有 TCP/IP 协议的 GPRS 模块来实现。目前市场上提供的 GPRS 无线模块有 WAVECOM 公司的 Q2403B，SIEMENS 公司的 MC35i、MC39I，摩托罗拉公司的 G20 等。结合本系统的实际应用，选用了 SIEMENS 的 Sim300。Sim300 是新一代的 900 MHz/1 800 MHz 双频自动选择的无线模块，内嵌有 TCP/IP 协议栈，无需微处理器的支持即可实现基于 TCP/IP 的数据传输。其支持标准的 AT 命令及增强的 AT 命令监护数据模式，功能强大，操作灵活方便。微处理器可以通过标准串口接口 RS232 与 Sim300 通信，为用户提供了标准的 AT 命令接口，为数据传输提供了快速、可靠、安全的传输通道，用户可以很方便地进行实际应用的二次开发设计。

2.6 读写器人机交互的实现

手持终端人机交互通过外扩的一块 I²C 接口的数码管驱动及键盘扫描管理芯片 ZLG7290，配以 8 bit 共阴数码管和 16 个按键实现。ZLG7290 是广州周立功单片机发展有限公司研发的数码管驱动及键盘扫描管理芯片，具有 I²C 总线串行接口，能够提供键盘中断、驱动 8 bit 共阴数码管和 64 个按键扫描等功能，并且支持 10 种数字和 21 种字母的译码显示功能。

3 读写器软件设计

读写器的软件采用 μC/OS-Ⅱ嵌入式实时操作系统作为系统的软件平台，在 μC/OS-Ⅱ系统下实现对读写器终端的控制管理。μC/OS-Ⅱ具有较高的可靠性和稳定性，提供了多任务管理功能。系统的各单元部分以单独的任务线程设计，在减少了软件设计的复杂度的同时也增强了软件系统的稳定性。

3.1 μC/OS-Ⅱ嵌入式实时操作系统的移植

要将μC/OS-Ⅱ实时操作系统移植到处理器上，处理器必须满足以下条件[2]：

(1)处理器的编译环境能够产生可以重入的C代码。

(2)用C语言就可以打开或关闭中断。

(3)处理器支持中断处理，并能产生定时中断。

(4)处理器支持能够容纳一定数量的硬件堆栈。

(5)处理器具有将寄存器、堆栈指针读出和存储到堆栈中的指令。

对于ARM7系列的微处理器LPC2148及其开发环境ADS1.2的编译器，完全能够满足上述条件，可以确保μC/OS-Ⅱ在LPC2148上的移植成功。移植工作包括：

(1)用#define设置一个常量的值(OS_CPU.H)。

(2)声明10个数据类型(OS_CPU.H)。

(3)用#define声明3个宏(OS_CPU.H)。

(4)用C语言编写6个简单的函数(OS_CPU_C.C)。

(5)编写4个汇编语言函数(OS_CPU_A.ASM)。

3.2 无线数据传输的软件实现

Sim300中内嵌了TCP/IP协议，并且以AT指令的形式给控制模块提供接入GPRS网络进而接入Internet的API接口。由于该GPRS模块具有自动拨号功能，因此在进行无线数据传输时，不需要通过AT拨号指令连接Internet。读卡器系统在传输数据时对数据准确性的要求相对较高，因此，本设计采用TCP的方式实现读写器终端与系统数据中心之间的数据传输。读写器终端在与数据中心进行数据传输时用到的AT指令如下：

(1)建立TCP连接

AT+CIPSTART="TCP","61.13.48.9","2020"

连接数据中心服务器，此处61.13.48.9是服务器的IP地址，2020是端口号。连接成功的返回值是：CONNECT OK。

(2)向服务器发送数据

AT+CIPSEND

>Hello everyone! <Ctrl+Z>

向服务器发送字符串Hello everyone!。发送成功返回值为：OK。

(3)关闭连接

AT+CIPCLOSE

断开与数据中心服务器之间的连接，操作成功返回值为：OK。

(4)关闭移动场景

AT+CIPSHUT

操作成功返回值为：OK。

当服务器端有数据传输到GPRS模块时，数据会通过模块与LPC2148之间的串口接口直接转发给MCU，不需要AT指令操作。

由于该GPRS模块具有上电自动拨号的功能，在程序设计时就不再考虑终端拨号上网的实现。

3.3 MF RC500驱动软件的设计

MF RC500的驱动程序主要是MCU对MF RC500的控制以实现MF RC500与IC卡之间的数据交互，并把相关的数据结果返回给MCU。MCU通过MF RC500与IC卡的数据交换过程如下：

(1)由读写器的MCU发送指令给MCM(MF RC500)。

(2)MCM执行指令，并将其转换为射频信号发送给IC卡。

(3)IC卡接收到来自MCM的指令后，按指令完成其内部的各种处理，并回送应答信号/数据给MCM。

(4)MCM接收卡回送的射频信号，并将其转换为数字信号输出给MCU，MCU读取MCM接收到的应答/数据，即可完成与IC卡的数据交换。

MF RC500实现对IC卡读写的程序流程如图3所示。

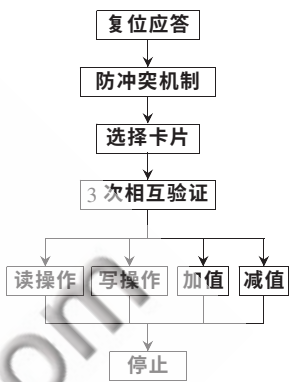

图3 MF RC500读写IC卡的程序流程图

3.4 动态密钥加密算法

动态密钥的的基本思想是在保持系统主密钥不变的情况下，每读一次用户卡就使用本次通信中产生的数据A动态地改写用户卡的密钥一次，以此来确保用户卡密钥不断更新，从而不被破解。数据A可以是当前通信时间、操作机具体标识或者随机数的组合。其具体的设计和实现可以参考文献[2]。

本文介绍的利用GPRS无线网络作为数据传输载体，以ARM7系列微处理器LPC2148作为主控单元的无线RFID读写器，具有通用性强、功耗低、便于携带、安装方便等特点。采用μC/OS-Ⅱ多任务实时操作系统，使得读写器终端的稳定性和可靠性均得到了较大的提高，同时程序的模块化设计有利于终端功能的升级与扩展。应用结果表明，该RFID读写器运行稳定可靠、响应速度快、安装和操作方便、便于携带，具有广泛的应用前景。

参考文献

[1] 谢高生，易灵芝，王根平.动态密钥在Mifare射频IC卡识别系统中的应用[J].计算机测量与控制，2009，17(4)：725-726.

[2] LABROSSE J J.嵌入式实时操作系统μC/OS-Ⅱ(第二版)[M].邵贝贝译.北京：北京航空航天大学出版社，2003.

(收稿日期：2010-12-03)

作者简介：

王延政，男，1986年生，硕士研究生，主要研究方向：嵌入式系统及无线数据传输。

李瑞祥，男，1967年生，讲师，主要研究方向：嵌入式系统。

王立青，男，1984年生，硕士研究生，主要研究方向：嵌入式系统。