远距离有源 RFID 系统①

李新春，于永鑫

(辽宁工程技术大学 电子与信息工程学院，葫芦岛 125105)

摘　要：针对现有 RFID 系统中的不足，设计了一种基于 ZigBee 技术的有源 RFID 系统。阐述了有源 RFID 系统的硬件设计原理，分别给出了读写器和有源标签软件设计架构，并通过研究 Z-Stack 协议完成阅读器与有源标签之间的通信。采用 TI 公司的 CC2591 功率放大芯片，增大了读卡器与标签的通信距离。并通过增加休眠时间和减少通信流量完成了标签的低功耗设计。最终实现了远距离、多节点的有源 RFID 系统的设计。

关键词：RFID；ZigBee；Z-stack 协议栈；阅读器；有源标签

Active RFID System Based on ZigBee Technology

LI Xin-Chun, YU Yong-Xin

(School of Electronic and Information Engineering, Liaoning Technical University, Huludao 125105, China)

Abstract: For the lack of existing RFID systems, to design an Active RFID systems based on ZigBee technology. This paper elaborates hardware design of active RFID systems, respectively gives software architecture of reader and active tag, and completes the communication between reader and active tag by studying the Z-Stack protocol. TI's CC2591 power amplifier chip is adopted, increasing the communication range of reader and tag. And low-power design is achieved by increasing in sleep time and reducing communication flows. Ultimately the long-range, multi-node active RFID system is realized in this paper.

Key words: RFID; ZigBee; Z-stack protocol stack; reader; active tag

RFID(射频辨识系统)是一种非接触式的自动识别技术[1]，它通过射频信号自动识别目标对象并获取相关数据。典型的 RFID 系统由电子标签(Tag)，读写器(Reader)以及管理系统等组成。主要应用于门禁管理、物流管理、车辆管理、自动控制、防盗系统等多种场合。但现有的 RFID 技术存在数据安全性不高、识别距离短、设备成本高以及读写系统工作灵活性不强等问题。为推广 RFID 技术的使用，RFID 的发展应满足一下要求：

(1) 低成本：现有的 RFID 读卡器需要上万元，很难满足大众群体的需求。

(2) 远距离：对于大型机构如物流、小区车辆管理、公车管理、不停靠收费站等都需要远距离识别。

(3) 移动性：数据可无线传输到管理系统，系统组网简单，可用于临时应急方案。

(4) 可扩展性：在系统不做大的改动的情况下，能够自动地进行软件升级和功能扩张。

(5) 保密性：确保用户的信息不被泄漏或盗取。为了解决 RFID 技术的上述问题，本文提出了一种基于 ZigBee 技术[2]的远距离有源 RFID 系统。

1　系统框架及硬件设计

1.1 系统工作原理

与典型 RFID 一样，系统由电子标签，读写器和服务器管理系统组成，如图 1 所示。

电子标签为智能有源 RFID 电子标签，标签内不仅存储着物体的具体信息，还集成有相应的传感器，可以对周围环境进行监测，并把数据与自己的信息一

① 基金项目:安徽省教育厅自然科学基金(2005KJ004ZD)
收稿时间:2011-03-21;收到修改稿时间:2011-04-29

起传到服务器。有源标签本身有发送数据的自主权，减轻了读写器的负担，增大了标签与读写器之间的距离，减少了读写器的个数。读写器之间可以通过 ZigBee 协议构成无线传感器网络，读写器之间可以协调工作；通过多跳方式把数据传到服务器，扩大了网络覆盖面积。服务器可以通过调用数据库中存储的进入网络的标签的信息，对物体进行定位，跟踪或触发相应事件，实现人与人或人与物的交互。

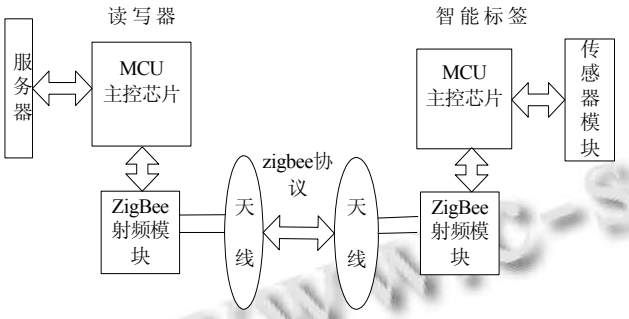

图 1 系统原理图

1.2 硬件的设计原理

结合目前市场上 ZigBee 射频芯片的性能、价格，本系统采用 Chinpcon 公司的 CC2430。C2430 芯片是高度集成的解决方案[3]，仅需很少的外部元件，且所选用元件均为低成本，可支持快速、廉价的 ZigBee 节点的构建。由于技术成熟，这里就不给出 CC2430 的具体内部结构图和它的外围电路图，请参阅其技术手册[4]。

读写器采用 RS232 串口与服务器相连，使用了宽电压范围的 SP3232E 电平转换芯片，它的电压范围在 3.3 到 5V。电源模块采用 LM1117 低压差电压调节器，采用具有固定电压输出 3.3V 型号的 LM1117-3.3，用 5V 适配器为读卡器供电。

CC2430 内部集成了 8～14 位 ADC，简化了标签的硬件电路设计。电池使用纽扣式电池供电，有利于减小标签体积。标签的天线基于 1/4 波长单端 PCB 印制天线理论设计[5]，天线直接印制在 PCB 板上，使得标签紧凑小巧。

为了增大读卡器与标签的通信距离，减少路由个数，我们使用 TI 公司推出的用于 2.4GHz 射频前端集成芯片 CC2591[6]。CC2591 专门用于低功耗、低电压无线传输系统，集成了输出功率高达+22dBm 的功率放大器，及可以将接收灵敏度提高+6dB 的低噪声放大器，从而能大大提高设备的通信范围。CC2591 使得在空旷场地的传输距离提高到 400 米至 800 米，比原来提高 15 倍。CC2591 外围电路图如图 2 所示。

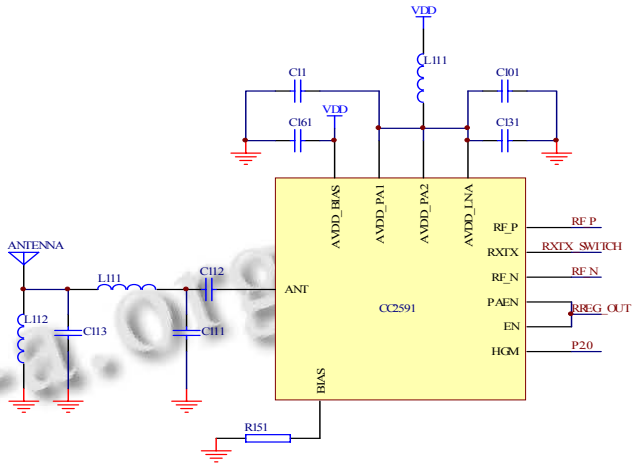

图 2 CC2591 外围电路图

与 CC2430 的通信接口包括 RF_P，RXTX，RF_N，PAEN，EN，HGM。其中 RF_P、RF_N 必须与 CC2430 的 RF_P、RF_N 连接，分别映射到系统协议栈内部接口和寄存器。PAEN，EN 使能端接 CC2430 的 RRFG_OUT，RXTX 接到 CC2430 的 RXTX_SWITCH，HGM 可接任意普通 I /O 口。电源引脚的电容为滤波电容，同时与电感 L111 构成射频负载。CC2591 和天线之间的 C111，C112，C113 和 L112 L111 网络相匹配，整个结构满足 RF 输入/输出匹配电阻(50Ω)的要求，同时 C112 为芯片内部的 PA 及 LAN 提供直流偏置。R151 是偏置电阻，为 CC2591 内部提供一个精确的偏置电流。

2 系统软件架构

2.1 读写器与标签的通信

读写器与标签通信，首先必须有 ZigBee 网络存在。这就需要系统中读写器（一般与服务器直接串口相连）将网络建立起来，并负责地址的分配和成员的加入、节点设备数据的更新、设备关联表的维护。标签发现网络，就会请求加入网络。入网成功后，标签就与其中读写器建立父子关系，时刻保持通信。为了降低标签功耗，标签具有定时休眠的功能。

本系统采用 Z-stack 协议栈[3]来完成网络的建立及路由或标签的入网，从而建立通信链路。

2.1.1 网络形成

读卡器上电后，将扫描 DEFAULT_CHANLIST 指定的通道，最后在其中之一形成网络(根据 ZDAPP_CONFIG_PAN_ID 的值)。然后调用 ZDO 层的初始化设备函数 ZDOInitDevice(0)设置 NV 网络状态：networkStateNV=INITDEV_NEW_NETWORK_STAT;最终触发网络初始化函数，设置网络初始化事件；ZDO 层任务事件处理函数对网络初始化事件进行处理,调用 ZDO_StartDevice()函数，将改变设备状态为协调器启动：devState = DEV_COORD_STARTING；然后调用 NWK 层网络形成请求函数：NLME_Network-FormationRequest();NWK 层通过调用 MAC 和 PHY 层相关功能函数执行一些列网络形成动作，最终形成网络。

2.1.2 标签加入网络

标签在上电初始化以后，经过初始化设备、设置 NV 网络状态、触发网络初始化函数、设置网络初始化事件、启动设备后将改变设备状态为发现网络：devState = DEV_NWK_DISC；调用 NWK 层发现网络请求函数：NetworkDiscoveryRequest();然后 NWK 层通过调用 MAC 和 PHY 层相关功能函数执行一些列发现网络动作，发送发现网络消息至 ZDO 层。ZDO 层接收到该消息后，修改设备状态为正在加入网络：devState = DEV_NWK_JOINING； NWK 层通过调用 MAC 和 PHY 层相关功能函数执行一些列请求加入网络动作，并发送加入网络指示消息至 ZDO 层。ZDO 层任务事件处理函数将执行处理加入网络函数：ZDApp_ProcessNetworkJoin()；修改设备状态为终端设备：devState = DEV_END_DEVICE。设置 ZDO 状态改变事件： osal_set_event(ZDAppTaskID, ZDO_STATE_CHANGE_EVT)；最终加入已有网络，与读卡器进行通信。

2.2 读写器与有源 RFID 标签的软件流程图

读写器设备初始化后首先要检测是否有网络存在，这决定了读写器是作为网络的协调器还是路由器，来完成相应的功能。标签设备初始化后，首先加入网络，再执行设备程序，完成传感器数据采集等功能。在它休眠醒来或数据发送完成后，要检测一下是不是已经离开网络。如果标签远离与它通信的读写器，它将通过孤点方式再次申请加入网络，与新的读写器建立通信。读写器与有源 RFID 标签的具体工作流程如图 3 所示。

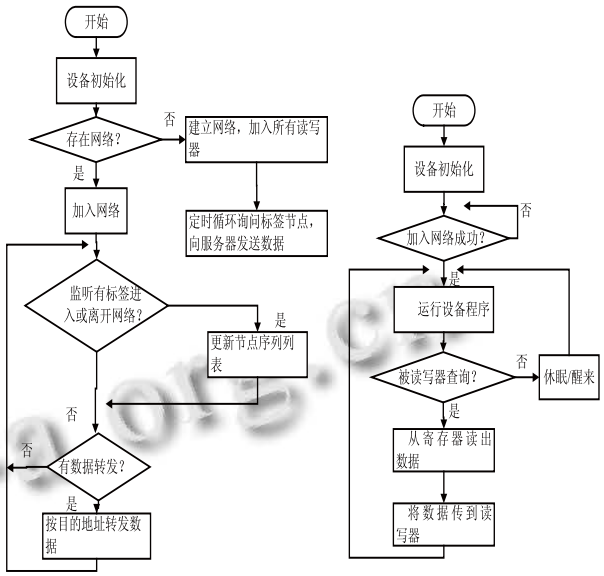

图 3　读写器与有源 RFID 标签的具体工作流程

2.3 低功耗设计

由于标签是有源 RFID，低功耗设计是非常重要的。在设计中，主要采用增加休眠时间还减少通信流量两种方法来实现的。标签在休眠时的功耗将近为唤醒时的千分之一，在保证监控的真确性的前提下，增长休眠时间是低功耗设计的一个重要手段。设计中用定时器 1 作为定时休眠，休眠时间为 10s。具体实现：

```
__interrupt void T1_ISR(void)
{ IRCON &= ~0x02; //清中断标志
 counter++;
 if(counter == 250)
  {counter = 0;timetemp = 10; }//10 秒到
 PowerMode(3);  }//进入休眠模式 3
```

为了减少标签的通信流量，标签会记录上一次的状态(如温度变化)，根据状态是否变化来决定是否传输数据。具体实现：

```
if(oldstate!=newstate)
{zb_SendDataRequest(0xFFFE,REPORT_CMD_ID
, 2, pData,0,AF_ACK_REQUEST,0);} //发送数据请求
else{PowerMode(3);}}//进入休眠模式 3
```

3　测试结果

在测试时，我们模拟仓库管理系统。将标签中写

(下转第 177 页)

片的无线传感器网络。

参考文献

1 DHananjay L, Manjeshwar A, Herrmann F, Biyikglou UE, et al. Measurement and CharActerization of Link Quality Metrics in Energy Const rained Wireless Sensor Networks. Global Telecomm unications Conference (GLOBEC OM'03), 2003.1:446–452.

2 Sivagami A, Pavai K, Sridharan D, et al. Energy and link quality based routing for data gathering tree in wireless sensor networks under TinyOS-2.x. Internatonal Journal of Wireless & Mobile Networks, 2010,2(2):47–60.

3 Heinzelman W, Chandrakasan A, Balakrishnan H. Energy Efficient communication ptotocol for wireless microsensor networks. Hawaii: the 33rd Annual Hawaii International Conference on System Sciences, 2000,3005–3014.

4 Younis O, Fathmy S. Heed: A hybrid, energy efficient, Distribute lustering approach for ad-hoc sensor networks. IEEE Trans. on Mobile Computing, 2004.

5 刘明,曹建农,陈贵海,陈力军,王晓敏,龚海刚.EADEEG:能量感知的无线传感器网络数据收集协议.软件学报,2007,18(5):1092–1109.

6 孙佩刚,赵海,罗玎玎,等.无线传感器网路链路通信质量测量研究.通信学报,2007,28(10):14–22.

7 Couto DSJD, Aguayo D, Bicket J, Morris R. A High-Throughtput Path Metric for Multi-Hop Wireless Routing. Wireless Networks, 2005,11(4): 419–434.

8 Felemban E, Lee G, Ekici E, et al. MMSPEED: Multipath Multi-Speed Protocol for Qos of Reliability and Timeliness in Wireless Sensor Networks. Mobile Computing, 2006,5(6): 738–754.

9 Hamdaoui M, Ramanathan P. A dynamic priority assignment technique for streams with(m,k)firm deadline. IEEE Trans. on Computers, 1955,44 (4):1443–1451.

10 Chen JM, Lin RZ, Li YJ, et al. LQER: A Link Quality Estimation based Routing for wireess Sensor Networks. Sensors, 2008,8:1025–1038.

(上接第 180 页)

入了物体的具体信息（我们这里写入一个 ID 号），并在标签上设计了温度传感器电路，用来实时监测物体周围环境信息。读卡器与计算机相连，通过串口显示标签的信息。串口显示如图 4 所示。

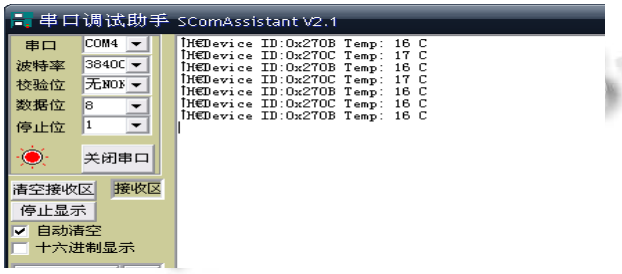

图 4 测试显示结果

4 结语

本文基于 ZigBee 技术设计了一种工作频段为 2.4GHz 的有源 RFID 系统。改善了目前 RFID 系统识别距离短，组网不灵活，抗干扰能力差的缺点。详细地介绍了整个系统的开发流程。但是此系统中标签价格仍然昂贵，只适合于贵重物体跟踪等少数场合。随着技术水平的不断提高，生产出价格低廉，集成度更高的射频芯片，使得芯片体积更小，价格更低，此系统便可以得到广泛应用。

参考文献

1 蒋浩石,张成,林嘉宇.无线射频技术及其应用和发展趋势.电子技术应用,2005,(5):1–4.

2 顾瑞红,张宏科.基于 ZigBee 的无线网络技术及其应用.电子技术应用,2005,(6):1–3.

3 高守玮,杨灿.ZigBee 技术实践教程.北京:北京航空航天大学出版社,2009.

4 cc2430 Data Sheet. http://www.ti.com/cc2430.

5 段艳敏.UHF 频段 RFID 天线的小型化设计与分析.成都:西南交通大学,2010.

6 cc2591 Data Sheet. http://www.ti.com/cc2591.