

基于 ZigBee、GPRS 和 TCP/IP 协议的无线网关设计*

项雷军

(华侨大学 信息科学与工程学院, 福建 厦门 361021)

摘要: 针对 ZigBee 无线传感器网络的远程监控技术的实现, 设计一个将 ZigBee 协议与 TCP/IP 协议有机融合在一起的无线网关。系统运行时, 互联网中的远程服务器可通过网关对 ZigBee 无线传感器网络所有节点进行监控。此网关设计方案成本低廉且易于实现, 可以为无线传感器网络在诸多领域的应用开发提供设计参考。

关键词: ZigBee; 无线传感器网络; C8051F120; GPRS; TCP/IP 协议; 网关

中图分类号: TP212.9; TN925.93

文献标识码: A

文章编号: 1674-7720(2013)08-0051-04

Design of the wireless gateway based on ZigBee, GPRS and TCP/IP protocols

Xiang Leijun

(College of Information Science and Engineering, Huaqiao University, Xiamen 361021, China)

Abstract: Aiming to solve the remote monitoring problem of wireless sensor network (WSN) based on the ZigBee protocol, the gateway that merges ZigBee protocol and TCP/IP protocol together has been designed in detail. All the nodes of the ZigBee-based wireless sensor network can be monitored by the remote server through the gateway when the system is running normally. This design scheme of the gateway can achieve easily and has only low cost, then may be used as a design reference for the application development of wireless sensor network in many fields.

Key words: ZigBee; wireless sensor network (WSN); C8051F120; GPRS; TCP/IP protocol; gateway

随着无线通信技术、传感器技术和计算机网络技术的不断发展, 无线传感器网络作为一种多学科交叉技术得到了学术界和工业界的广泛关注。ZigBee 技术是一种具有近距离、低速率、低功耗、双向数据传输、可以自组网等特点的高可靠个域网无线通信标准^[1-2]。在工业控制、医疗健康、农业节水灌溉、楼宇自动化、智能电网等众多领域, 基于 ZigBee 技术的无线传感器网络都具有很好的应用价值和发展前景^[2-3]。ZigBee 无线网络的网关设计有多种方法, 设计方案各有优缺点, 难易程度和成本开支存在差异。本文所介绍的基于 ZigBee 技术的无线传感器网络网关通过 GPRS 将互联网中的计算机通过网络与无线传感器网络的协调器连接在一起, 通过互联网中的计算机对无线传感器网络进行监控。且该系统的网关实现了 ZigBee 无线传感网络和基于 TCP/IP 协议的互联网的有机融合, 网关 GPRS 从网络中分配到一个 IP 地址, 使整个无线传感器网络成为互联网中的一台“计

算机”^[4-5]。该网关设计方案实现较为容易, 且成本低廉, 对无线传感器网络在工业控制、智能电网、环境监测、智能家居等领域的应用开发具有很好的参考价值。

1 系统的拓扑结构

ZigBee 是由 ZigBee 联盟在 IEEE 802.15.4 的物理层 (PHY) 和媒体介质访问层 (MAC) 基础上增加网络层 (NWK) 和应用层 (APL) 等所形成的协议体系结构^[2, 6]。在 ZigBee 网络中存在两种设备, 即全功能设备 (FFD) 和精简功能设备 (RFD)。网络中的节点可分为网络协调器、路由器和终端节点。网络协调器和路由器必须是 FFD, 而终端节点则可以是 FFD 或者 RFD。FFD 既可以与 FFD 通信, 也可以与 RFD 通信, 而 RFD 与 RFD 之间不能直接通信。ZigBee 网络的拓扑结构可分为星形网络、网状网络和树状网络。

本系统主要是由 ZigBee 无线传感器网络、网关和远程服务器组成, 系统的整体结构如图 1 所示。系统的 ZigBee 无线传感器网络选用树状网络拓扑结构。网关是整个 ZigBee 无线网络的控制中心, 它由以 CC2430 为处

* 基金项目: 华侨大学校级自然科学基金资助项目 (06HZR26)

网络与通信

Network and Communication

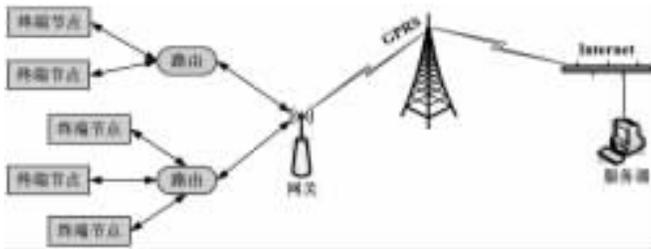


图1 系统整体结构

理器的 ZigBee 网络协调器、8 位单片机 C8051F120、GPRS 模块、电源模块及其他外围电路所构成。网络服务器是连接在互联网中具有公网 IP 地址的一台个人计算机,在该台计算机中安装有基于 Visual C++ 开发环境所设计开发的带有 Access 数据库的控制软件。

2 硬件设计

此系统无线网关的主要功能是将 ZigBee 无线网络和互联网中的计算机连接起来,使得通过互联网可以监控 ZigBee 网络中的所有节点,通过该网关也可以对 ZigBee 网络中的节点进行监控。该无线网关的硬件主要由 ZigBee 网络协调器、GPRS 模块和 C8051F120 微处理器组成。网络协调器的核心芯片选择 TI 公司生产的 CC2430 单片机,GPRS 模块选用的是 SIM300 模块,C8051F120 单片机是美国 Silicon Laboratories 公司的产品。

CC2430 是由一颗高性能、低功耗的 8051 单片机内核和符合 IEEE 802.15.4 标准的 2.4 GHz 的无线电收发机组成^[7]。CC2430 的闪存根据存储空间的大小可以分成 3 种,分别是 32 KB、64 KB 和 128 KB,本系统的网络协调器微处理器选择的是 128 KB 的 CC2430。

C8051F120 是一款完全继承的混合信号片上系统型的 8 位 MCU,具有 64 个数字 I/O 引脚,该款芯片共有 100 个引脚,具有丰富的片上资源;具有 128 KB 的 Flash 存储器 and 8 448 B 的片内 RAM;两个串行通信接口,分别是 UART0 和 UART1,在此系统网关设计中这两个串行端口对数据和控制指令的传输起到关键作用。

SIM300 是一款内嵌了 TCP/IP 网络通信协议、可以通过标准的 AT 指令进行操作的高性能 GPRS 模块。通过 AT 指令操作可以轻松使 GPRS 与互联网中的计算机建立基于 TCP/IP 的网络连接,该模块还具有短信息和语音通话功能,非常适合应用于工业监控和楼宇自动化等领域。

该系统网关的硬件设计结构如图 2 所示,C8051F120



图2 网关的硬件结构

与 SIM300 之间的通信基于 RS232 串口通信协议,使用的是 UART0 端口,TX0 和 RX0 分别是 I/O 端口的 P0.0 与 P0.1;与网络协调器之间的通信同样基于 RS232 串口通信协议,使用的是 UART1 端口,TX1 和 RX1 分别是 I/O 端口的 P0.2 与 P0.3。网络协调器端的串口通信选择的是 CC2430 的 UART0,TX 和 RX 分别是 I/O 端口的 P0.3 与 P0.2。在串口通信中,TX 应该与接收方的 RX 连接,RX 应该与发送方的 TX 连接,所以 C8051F120 与 GPRS 的串口连接要交叉连接,也就是 C8051F120 的 TX0 连接 GPRS 的 RX,RX0 连接 GPRS 的 TX。同理,C8051F120 与网络协调器的连接也要交叉连接。在该网关的设计中,还要考虑到一个电源参考电压的问题,为了使它们有一个共同的地,网关的这三部分的地要连接在一起。

通过中间的 C8051F120 对网络协调器和 GPRS 之间的双向数据进行处理,可以使协调器不会因为 GPRS 的握手协议的存在而提高串口通信的中断频率,把主要的工作放在 ZigBee 无线网络这一端,从而提高网络协调器的运行稳定性并且使 ZigBee 无线网络具有良好的可扩展性。

3 软件编程

网关的软件设计是在网关的硬件设计基础上展开的。根据前面的硬件设计,程序设计可以分为两个部分:网络协调器的程序设计和基于 C8051F120 的程序设计。GPRS 模块的操作属于 C8051F120 的程序处理范畴。

3.1 网络协调器的程序设计

网络协调器是整个 ZigBee 网络的控制中心,在 ZigBee 网络中处于核心地位。整个系统中,网络协调器的作用主要分为两个方面:(1)对 ZigBee 网络进行组网;(2)连接 ZigBee 网络与 C8051F120,使二者之间互相通信。具体而言,网络协调器对 ZigBee 网络进行组网,为网络中的各个节点分别分配一个 16 位的网络地址,对网络中的节点进行控制和采集相关节点信息。在 ZigBee 网络与 C8051F120 之间起到“桥梁”的作用,即接收并处理来自 C8051F120 的控制指令,采集来自 ZigBee 网络的数据并打包传输给 C8051F120,由 C8051F120 做进一步处理。

网络协调器与 C8051F120 之间的通信是基于 RS232 串口通信协议的串口通信。ZigBee 协议栈所定义的串口通信波特率有 38 400 bit/s 和 115 200 bit/s,此处选择 115 200 bit/s 作为协调器与 C8051F120 通信的波特率。系统开发过程中,选用 Z-Stack 的例程 SimpleApp 并以此为基础设计协调器和 ZigBee 节点的程序,此举可节省较多开发时间。协调器程序设计时,与串口通信相关的一些参数应在 sapi.h 文件中定义,而初始化部分应放在 sapi.c 中的初始化函数 SAPI_Init(byte task_id)中,当协调器开始工作时即可初始化 CC2430 的串口通信。ZigBee 网络协调器开始工作时是从协议栈的 ZMain.c 文件中的主函数 main (void) 开始运行的,在此过程中需调用 os-

网络与通信

Network and Communication

al_int_disable(INTS_ALL)关中断,再调用协议栈各层的初始化函数及CC2430片上资源的初始化函数进行初始化,初始化之后调用osal_int_enable(INTS_ALL)允许中断。最后程序通过osal_start_system()进入协议栈的任务操作系统。该函数是协议栈操作系统的主循环函数,进入该函数后将不再返回。在操作系统的运行过程中如果有事件产生将调用函数task_event_processor()对事件进行处理。

系统开发过程中,网络协调器和终端节点的程序是在同一个工程中进行开发的,即Z-Stack中的sapi.c文件和sapi.h文件是由网络协调器程序和终端节点程序共同调用的,故在这两个文件中单独涉及到网络协调器和单独涉及到终端节点的程序部分应分别存入各自的条件编译程序块中。网络协调器的程序运行流程图如图3所示。

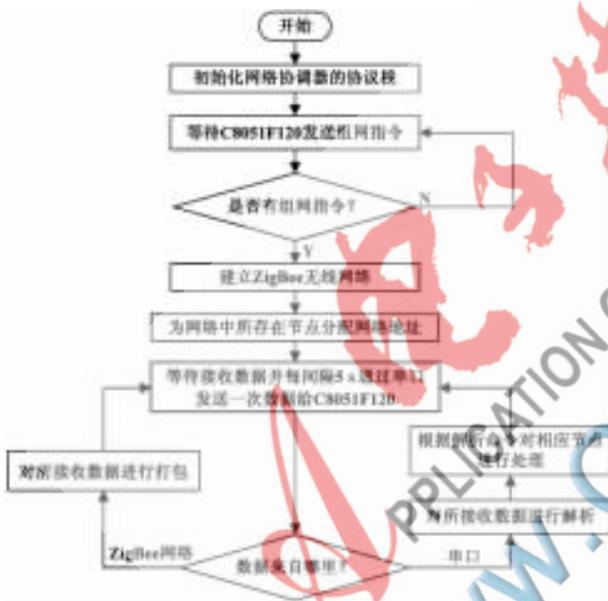


图3 网络协调器的程序运行流程图

3.2 基于C8051F120的程序设计

在系统设计中,C8051F120是一个很重要的中间件,它将ZigBee网络与互联网中的远程服务器连接起来,使得管理员可以通过服务器的控制软件或其他客户端控制软件对ZigBee网络进行实时监控。C8051F120通过UART0与SIM300连接在一起,在启动时首先要做的工作就是初始化SIM300模块并与互联网中的远程服务器建立连接,这样管理员才可以通过远程服务器上的控制软件对ZigBee无线网络进行监控。这一步非常重要,如果不与服务器建立连接,则管理员就无法通过服务器上的控制软件对ZigBee无线传感器网络进行监控。根据系统要求,C8051F120对GPRS模块的初始化可以分为表1所示的几个部分。

表1 GPRS 模块初始化列表

指令	操作
"AT+CSTT\r\n"	启动服务
"AT+CHCR\r\n"	移动场景
"AT+CLOPRT=\\"TCP\\", \\"PORT\\"\r\n"	设置本地TCP端口,PORT为本地端口号
"AT+CIFSR\r\n"	获取IP地址
"AT+CIPSTART=\\"TCP\\", \\"IP\\", \\"PORT\\"\r\n"	连接指定公网IP地址和端口号的服务器
"AT+CIPSPRT=0\r\n"	设置发送"AT+CIPSEND\r\n"之后不返回'>'字符

C8051F120的程序设计用到两个串口通信,串口通信的数据收发均通过中断服务程序实现^[8]。C8051F120总共有20个中断源。在中断系统中,UART0的中断优先级是4,UART1的中断优先级是20,即UART0的优先级比UART1高。系统选用外部22.1184MHz晶振经锁相环二倍频后,产生50MHz时钟源。Timer2通过16位自动重装模式设置115200bit/s的波特率作为UART0波特率。而Timer1通过8位自动重装模式设置115200bit/s的波特率作为UART1波特率,这个波特率与协调器的波特率相匹配。该部分的设置均采用Silicon Laboratories IDE集成开发环境来编程实现。C8051F120的程序运行流程图如图4所示。

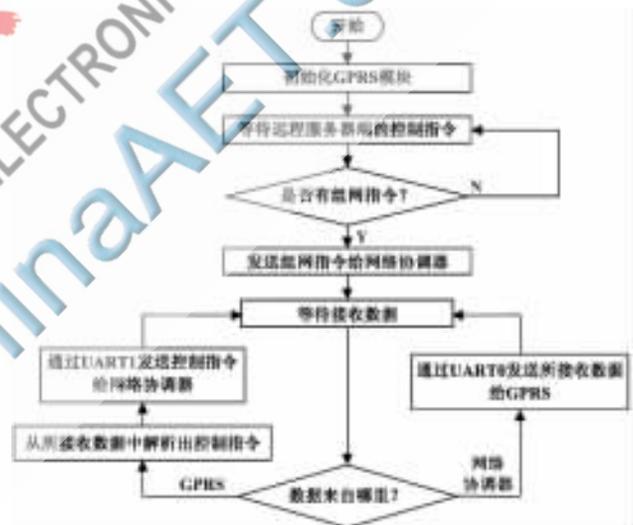


图4 单片机C8051F120的程序运行流程图

由于ZigBee网络与远程服务器之间的通信属于通过GPRS进行的基于TCP/IP的网络通信,受移动网络的影响,因此系统通信容易产生时滞,多次发送的数据集中在同一时间接收,易产生误控制及数据的误处理。为解决该问题,需按照以下基本格式定义无线通信的握手协议:从服务器端发送来的控制指令的格式为0xAA+节点序号+节点网络地址+指令+0xAA,总字节数是6B。如果C8051F120从GPRS接收到的数据不符合这种数据格式,则对这样的数据不做处理,直接从缓存中删除。C8051F120从网络协调器接收到的数据帧也是由固定的帧头和帧尾以及中间的相关数据组成,数据帧的格式是0xFF+(节点序号+节点网络地址+节点状态)+...+(节点序号+节点网络地址+节点

网络与通信 Network and Communication

状态)+0xFF。C8051F120 接收到网络协调器发送过来的数据时,则转到 UART1 串口通信的中断服务子程序进行处理,要处理的内容包括判断数据帧的帧头、帧尾、总字节数等。如果中间的数据判断有哪个与程序设计过程中定义的不一致,则退出中断并清空接收缓存,否则按流程图的顺序执行程序。在程序的运行过程中,C8051F120 每完成一个任务都会用一个相应的全局变量来标志,以便作为下一个环节程序处理依据。例如变量 InitOrRun,当 InitOrRun=0 时,表示此时程序处于 GPRS 的初始化阶段;InitOrRun=1 时,表示此时程序处于系统正常运行阶段。

ZigBee 技术在各种监测与控制领域的应用将会越来越广泛,根据系统的要求以及特定通信协议设计一个网关,把不同的通信协议组合或转换,是一项非常重要的工作,对系统的开发实现起到关键作用。本系统的网关不仅可以基于 TCP/IP 的网络通信的数据转换为监控 ZigBee 无线网络的控制指令,也可以将 ZigBee 无线网络的数据进行转换后通过互联网传输给远程服务器和客户端计算机。此网关设计方案中单片机 C8051F120 的程序稍作修改即可应用于类似的系统中,例如工业控制、智能家居、农业节水灌溉、环境监测、煤矿安全等。

参考文献

- [1] ZigBee Alliance.ZigBee Specification[S].2006.
- [2] 金纯,罗祖秋,罗凤,等.ZigBee 技术基础及案例分析[M].北京:国防工业出版社,2008.
- [3] 崔逊学,赵湛,王成.无线传感器网络的领域应用与设计技术[M].北京:国防工业出版社,2009.
- [4] 刘元安,叶靓,邵谦明,等.无线传感器网络与 TCP/IP 网络的融合[J].北京邮电大学学报,2006,29(6):1-4.
- [5] 庞训磊,殷保群,奚宏生.一种使用 TCP/IP 协议实现无线传感器网络互连的新型设计[J].传感技术学报,2007,20(6):1386-1390.
- [6] REESE R.A ZigBee TM-subset/IEEE 802.15.4TM multi-platform protocol stack[C].In Electrical/Computer Engr MSU. 2006.
- [7] Chipcon.CC2430 preliminary data sheet(Rev.1.03) SWRS036A[S].2005.
- [8] 陈连坤.单片机原理及接口技术(C语言版)[M].北京:清华大学出版社,北京交通大学出版社,2010.

(收稿日期:2012-12-31)

作者简介:

项雷军,男,1979 年生,讲师,工学硕士,主要研究方向:计算机控制技术、嵌入式网络控制系统的开发。