

物联网 ZigBee 网关的设计与实现^①

张艺粟^{1,2}, 李鸿彬², 贾军营², 于波²

¹(中国科学院大学, 北京 100049)

²(中国科学院 沈阳计算技术研究所, 沈阳 110168)

摘要: 物联网中应用广泛的 ZigBee 协议与传统的 TCP/IP 协议并不兼容, 如何实现两种异构网络的融合是物联网的关键技术所在. 对物联网网关的需求进行了分析, 并基于 CC2530 开发套件、龙芯 1B 开发板、Zstack 协议栈和嵌入式 linux 系统, 设计并实现了一个物联网 ZigBee 网关的原型系统, 完成了 ZigBee 网络的管理、协议转换、数据收发等功能, 并通过实验对各部分功能进行了验证.

关键词: 网关; ZigBee; 物联网; TCP/IP; 嵌入式 Linux

Design and Implementation of ZigBee Gateway in the Internet of Things

ZHANG Yi-Su^{1,2}, LI Hong-Bin², JIA Jun-Ying², YU Bo²

¹(University of Chinese Academy of Sciences, Beijing 100049, China)

²(Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang 110171, China)

Abstract: The most used ZigBee protocol in Internet of Things (IOT) is not compatible with the TCP/IP protocols, so the convergence of these two kinds of networks is the essential technology in IOT. The thesis analyzes the requirement of the IOT gateway at the beginning, then designs and realizes a ZigBee gateway prototype, based on the CC2530 develop kit, Longson 1B develop board, Zstack and embedded Linux system, achieves functions such as management of the ZigBee network, protocol conversion and data transmission, and then verifies these functions through experiments.

Key words: gateway; ZigBee; Internet of Things; TCP/IP; embedded Linux

1 引言

2005 年, 国际电信联盟(ITU)在其年报(ITU2005: The Internet of Things^[1])中提出了物联网的概念. 报告对网络发展的前景进行了大胆的预测: 在未来, 网络将不仅仅是人与人之间信息交互的通道, 人与物甚至物与物之间也能够通过网络互相联络, 人们的生活将变得更加便利和智能化.

物联网的概念是随着近些年来无线传感器网络的发展而提出的. 无线传感器网络中各种传感设备可以极大地延伸和拓展人们的感知领域和范围. 传感器节点一般要求结构简单, 成本低廉, 能够长时间工作而无需频繁更换电池等. 与传统的 WiFi、蓝牙等较为复杂、功耗较高的无线传输技术相比, ZigBee 协议因其简单、低功耗的特点在物联网领域得到广泛的应用. 其 PHY 层和 MAC 层直接来源于 IEEE802.15.4 标准,

网络层、应用层和相应的安全机制则由 ZigBee 联盟制定, 主要面向短距离、低功耗、低数据传输率的应用.

互联网的发展极大地改变了人们的生活方式, 而 ZigBee 协议与互联网中 TCP/IP 协议族并不兼容. 如何将 ZigBee 网络接入 TCP/IP 网络使得人们能通过互联网对环境进行监控, 对接入节点进行远程管理和控制, 是目前物联网研究领域的热点问题. 而网关作为连接异构网络的设备, 吸引着众多的研究者.

目前网关的实现技术主要有以下几种. 一是通过通道机制, 当接收到无线传感器数据时, 不经过解封装而直接将其作为以太网的载荷, 加上 TCP/IP 的包头, 传至 IP 网络主机, 然后由该主机完成对数据的解析. 因为无线数据中某些内容, 如跳数, 封包序号等并不是必须的, 所以该方式会造成带宽的浪费. 二是通过远程过程调用 RPC(Remote Procedure Call)的方式, 使用表示状态转移

① 收稿时间:2012-11-30;收到修改稿时间:2013-01-06

REST(Representational State Transfer)或者简单对象访问协议 SOAP(Simple Object Access Protocol), 将待发送数据或请求转变成 XML 格式后进行发送. 该方式同样会造成带宽的浪费. 此外, 还有的使用了协议转换机制等方式. 本文自定义了一种数据封包格式, 首先对接收到的无线数据进行解析, 然后按自定义的数据格式封装, 加上 TCP/IP 包头, 再通过以太网传送至 IP 网络主机. 该方式可以有效的节省带宽, 并能达到数据传送的目的.

2 网关需求分析

典型的物联网应用体系架构由下到上依次为感知层、传输层和应用层^[2]. 感知层的作用有数据采集和无线传输, 一般采用 RFID、传感器、摄像头等对家庭、农业、交通、水利等环境数据进行采集, 然后通过无线传输技术传递数据. 传输层运用现有的 WiFi, 2G/3G, 宽带等通信技术, 拓展感知层数据传输的距离, 实现感知网络与通信网络的结合. 应用层主要负责对数据进行加工处理, 为用户提供丰富多彩的服务, 是物联网应用的最终目的所在. 物联网网关就位于中间的传输层, 连接传感网和传统通信网络, 其功能应包括协议转换, 数据收发, 传感网络管理等^[3].

2.1 协议转换功能

网关最基本的功能是实现不同协议之间的转换. 当收到 ZigBee 节点发来的数据后, 网关根据 ZigBee 协议规范去除 PHY 层、MAC 层、网络层的包头, 对应用层数据做相应处理, 然后按照 TCP/IP 协议标准重新对数据进行封装, 再通过以太网发送出去; 相反方向的数据传输也需要类似的过程^[4]. 因此, 网关应同时具有 ZigBee 和 TCP/IP 两种协议栈. 协议转换过程如图 1 所示.

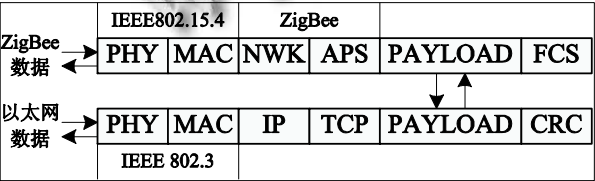


图 1 协议转换过程

2.2 数据收发功能

网关作为沟通传感网和通信网络的桥梁, 能够起到数据中转的作用. ZigBee 网络上传的数据通过网关

的处理之后可以到达 IP 网络的主机, 同样的 IP 网络的数据或者控制命令也可以通过网关到达相应的 ZigBee 节点.

2.3 传感器网络管理功能

ZigBee 网关还应实现 ZigBee 网络的管理, 如网络的建立, 处理节点的入网申请, 分配网络地址, 维持网络的拓扑结构, 节点离开时对地址的回收等.

3 网关总体设计

3.1 硬件设计

网关的硬件设计如图 2 所示. 其总体上采用双 CPU 结构, 包括 ZigBee 模块的 CC2530 芯片和主控模块的龙芯 1 号芯片. 设计中两个模块分别采用了 ZigBee 开发套件和龙芯 1B 开发板, 取套件中的一个节点作为 ZigBee 网络协调器, 协调器与龙芯 1B 开发板连接后, 共同完成网关的功能.

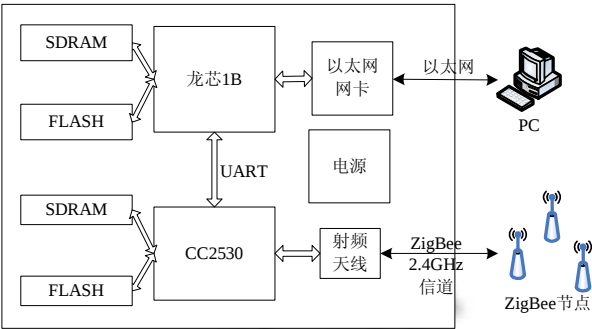


图 2 硬件总体设计

TI 公司的 CC2530 采用单片集成 SOC 方案, 将射频收发器、工业加强型 51 单片机核、Zstack 协议栈集成在同一芯片上. Zstack 协议栈与一些开源协议栈如 Freakz 相比, 更具完善性和稳定性. 且 TI 公司现已免费开放 Zstack 供开发者下载和使用, 可节省不少成本.

基于 MIPS 精简指令集的龙芯 1 号芯片, 主频为 200-233 MHz, 可配置到 266MHz, 能够满足网关对处理性能的需求, 与主流的 ARM 系列芯片相比, 具有更高的性价比. 1B 开发板的外设比较丰富, 方便调试和开发.

本设计中采用 UART 串口来连接 CC2530 和龙芯 1B 两个部分. 物联网中节点采集的多是一些温度、电压等传感器数据, 对传输率要求并不高, 用串口完全能够满足要求.

3.1 软件设计

软件的设计基于嵌入式 Linux 操作系统和 Zstack 协议栈, 根据需求分析可确定网关的各个功能模块. 网关软件结构、网关与 IP 网络主机及 ZigBee 网络节点之间的交互如图 3 所示.

Linux 操作系统开放源码, 模块化设计, 能够支持多种硬件, 其内核可以按需进行裁剪, 非常适合处理器性能、存储空间有限的嵌入式设备. Linux 内核本身对 TCP/IP 协议栈提供支持, 且提供了多线程、进程间通信等机制, 可实现相对较复杂的功能^[5].

嵌入式 Linux 系统和 Zstack 都提供了串口驱动, 调用相应的串口 API 即可实现对串口的读写等操作, 方便开发.



图 3 网关软件结构

4 软件各模块的设计与实现

4.1 ZigBee 内部通信模块

ZigBee 网络内部有终端节点、路由器、协调器三种节点. 与网关主控模块相连的 ZigBee 模块作为整个 ZigBee 网络的协调器, 其作用主要有: (1) ZigBee 网络管理. 包括网络建立, 处理入网申请等功能. (2) 数据收发. 包括接收 ZigBee 网络上传的数据、解封装并传送到网关主控模块; 对网关主控模块传来的数据, 按照 ZigBee 协议标准进行封装, 并发送至 ZigBee 网络. 协调器的程序流程如图 4 所示.

协调器与主控模块通信时, 要用到 Zstack 提供的串口 API: HalUARTInit() 初始化串口, 并设置波特率等参数, HalUARTOpen() 打开串口, HalUARTRead() 和 HalUARTWrite() 分别对串口进行读写操作. 在对串口进行读写操作时, 一般采用中断方式调用 HalUARTReadISR(), HalUARTWriteISR() 来完成. 同时 Zstack 也提供了 DMA 方式 API 来实现串口数据的高效读写, 相应的函数为 HalUARTReadDMA(), HalUARTWriteDMA().

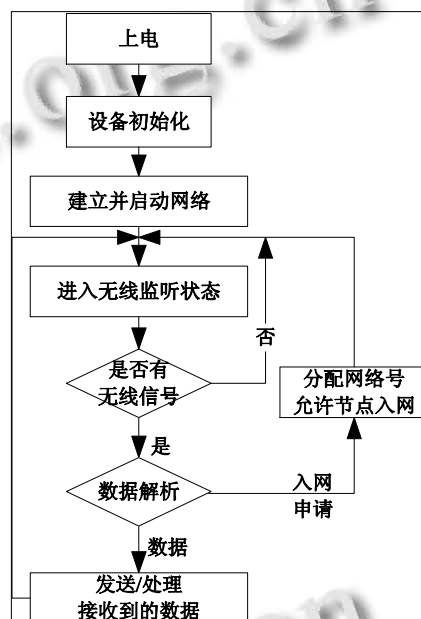


图 4 协调器的程序流程

4.2 网关主控模块

网关主控模块的工作包括: 与 ZigBee 模块通信, 获取 ZigBee 数据或将命令发送至 ZigBee 模块; 与 IP 网络的通信, 包括获取命令和上传数据.

4.2.1 与 ZigBee 模块的交互

主控模块和 ZigBee 模块通过串口连接, 在对嵌入式 Linux 系统内核进行裁剪时, 将串口驱动模块加入了内核中. Linux 下对串口的操作可以通过操作对应的设备文件进行, 通过 open()、read()、write() 等函数对串口设备文件进行操作, 进而完成串口的设置和数据通信. 串口数据格式的设计如图 5 所示.

其中开始标志为 0xFE, 帧长度为包括源地址/目的地址、命令 ID、数据长度、节点数据在内的 frame 的长度, 节点数据包括节点温度、节点电压、父节点地址. 命令类型和命令 ID 是根据应用的需要来进行定

义,如接收到节点上传的数据时的命令类型为 ZB_RECEIVE_DATA_INDICATION,节点上传数据时的命令 ID 定义为 SENSOR_REPORT_CMD_ID.节点数据的内容能够根据需要进行改变,长度由数据长度字段决定.

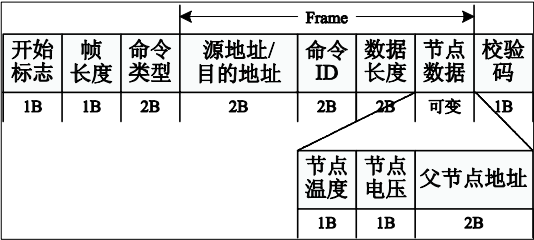


图 5 串口数据格式及节点数据

4.2.2 与 IP 网络的交互

TCP/IP 的 socket 可分为流式、数据报式和原始 socket 三种.为保证数据传输的质量和可靠性,本设计中采用了基于 TCP 协议的流式 socket^[6].通过 C/S 模型实现网关与 IP 网络客户端的命令和数据交互.

网关主控模块各以一个线程来完成上述两个方面的工作,来提高系统的并发性,包括串口通信线程和以太网通信线程.多线程程序实现的过程中,必须注意对线程同步和互斥问题的处理,本设计中采用互斥锁机制完成不同线程对公共缓冲区的互斥访问.两个线程的基本流程如图 6、图 7 所示:

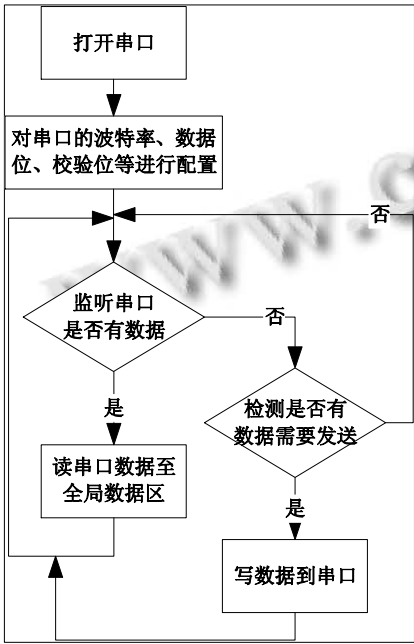


图 6 串口通信线程流程

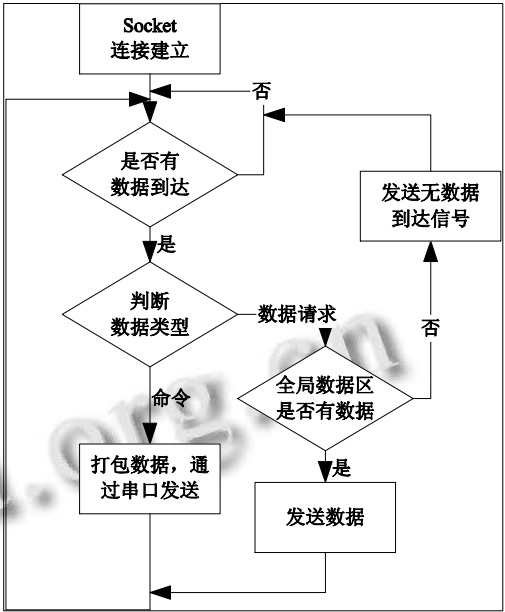


图 7 以太网通信线程流程

5 实验验证

实验通过 ZigBee 节点每隔 1 秒向网关发送温度、电压、父节点地址等信息,IP 网络客户端对这些数据进行监测.

5.1 ZigBee 模块与网关主控模块通信测试

网关和 ZigBee 节点上电后,ZigBee 网络建立,ZigBee 节点加入该网络并开始发送数据.设计中用到的 ZigBee 节点和 CC Debugger 连接后可作为协议分析仪使用,配合 TI 公司的 Package Sniffer 软件对无线数据进行抓包.抓包结果如图 8 所示.其中 APS Payload 部分就是节点所采集的温度、电压和父节点地址等数据.

APS Id	APS Profile Id	APS Src Endpoint	APS Counter	APS Payload	L
0x0F20	0x02	15	16 24	00 00	2.

图 8 Package Sniffer 抓包结果

网关的 ZigBee 模块部分接收到 ZigBee 节点发送的数据后,对其进行处理,并按照前面定义的串口数据格式将数据写到串口中.通过串口调试工具得到的结果如图 9 所示.其中方框中的数据就是 ZigBee 节点采集的数据,其它数据和前面定义的串口数据格式的各个领域是对应的.

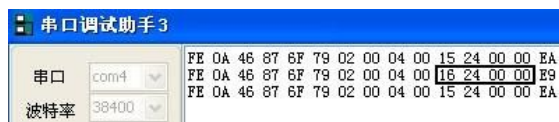


图 9 串口调试工具结果

以上结果表明, 网关 ZigBee 模块能够成功地接收到节点数据并通过串口发送出去。

5.2 网关主控模块测试

网关主控模块负责接收 ZigBee 模块通过串口传送的数据, 解析并发送到 IP 网络客户端。

网关 IP 地址配置为 192.168.139.76, 客户端 IP 地址为 192.168.139.75, IP 网络客户端解析接收到的数据后得到的结果如图 10 所示。从图中可以看到, 节点的网络地址为 796f, 父节点地址为 0, 即网关 ZigBee 模块的网络地址, 节点电压为 36, 温度为 22 或者 21。

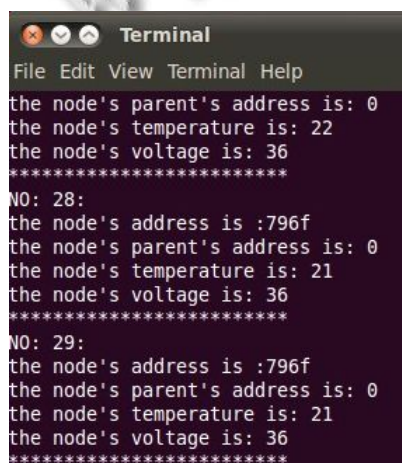


图 10 客户端显示结果

以上实验表明, 本设计方案的网关能够将 ZigBee 节点采集的数据正确上传至 IP 网络 PC 客户端, 实现 ZigBee 网络与 IP 网络的互联互通。

6 结语

ZigBee 网络与 IP 网络的融合关系到物联网今后的发展, 本文提出了一种基于嵌入式 Linux 系统和 Zstack 协议栈的 ZigBee 网关设计, 对网关的基本功能进行了实现, 最后通过实验验证了功能的有效性。ZigBee 节点采集的数据能够通过网关上传至 IP 网络 PC 客户端, 实现了 ZigBee 网络的管理, 协议转换, 数据收发等功能, 达到了两种异构网络互通互联的目的。下一步将对安全机制, IP 网络客户端对节点的访问控制等进行实现, 进一步完善网关的设计和功

参考文献

- 1 ITU Strategy and Policy Unit. Internet Reports 2005: The Internet of Things-Executive Summary. Tunis, ITU: 2005, 11. 16-18.
- 2 黄海昆, 邓佳佳. 物联网网关技术与应用. 电信科学, 2010 (4): 20-24.
- 3 陈琦, 韩冰, 秦伟俊, 皇甫伟. 基于 ZigBee/GPRS 物联网网关系统的设计与实现. 计算机研究与发展, 2011, 48(增刊): 367-372.
- 4 胡国珍, 王泉, 魏旻. 基于 ZigBee 的工业无线网关研究. 单片机与嵌入式系统应用, 2009(5): 25-28.
- 5 乔晓丹, 张鹏. 一个基于 Linux 操作系统的嵌入式网关的实现. 微计算机信息, 2005, 21(7-2): 26-28.
- 6 段玉顺. 用于无线网络协议转换的嵌入式网关的设计与实现[硕士学位论文]. 济南: 山东大学, 2009.