ZigBee 在智能家居系统中的应用研究

Research on Application of ZigBee in Smart Home System

张 周 周剑扬 闫 沫 (厦门大学,福建 厦门 361005)

摘 要

ZigBee 是一种新兴的短距离无线通信技术,非常适合低速率、低功耗、网络覆盖范围大、节点多的无线互连应用。分析了家庭网络通信的特点,并着重剖析了 ZigBee 技术极其协议和特点,介绍了一种基于 ZigBee 技术的智能家居无线网络系统,并阐述了实现该系统的关键问题。

关键词:ZigBee,智能家居,协议栈,嵌入式系统

Abstract

ZigBee,which is a kind of new short-distance wireless communication technology,is quietly suitable for the wireless communication applications which need low rate、low power、large-scale cover and lots of nodes.Analyze home network communication and ZigBee technology,laying stress on its protocol and features.This paper introduces a kind of wireless network system based on ZigBee technology and discuss some key issues while designing it.

Keywords:ZigBee,smart home,stack,embedded system

1 ZigBee 技术

1.1 ZigBee 技术概述

ZigBee 是一种新兴的近距离、低复杂度、低功耗、低数据速率、低成本的无线网络技术。它主要工作在无须注册的 2.4G ISM 频段,传输范围在 10~75m,典型距离为 30m。ZigBee 主要通过降低收发信机的忙闲以及数据传输的频率,降低帧开销以及实行严格的功率管理机制,例如关机及睡眠模式等方式来降低设备的综合功耗。

ZigBee 是一组基于 IEEE802.15.4 无线标准研制开发的有关组网、安全和应用软件方面的技术标准,ZigBee 协议栈由高层应用规范、应用汇聚层、网络层、数据链路层和物理层组成,网络层以上的协议由 ZigBee 联盟负责制定,IEEE 则制定物理层(PHY)和链路层(MAC)标准,如图 1 所示。

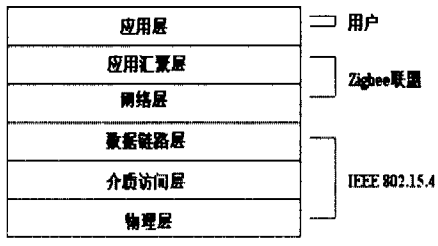

图 1 ZigBee 协议结构

1.2 ZigBee 技术的优势

ZigBee 技术的主要技术优势在于:

1)功耗低:由于 ZigBee 的传输速率低,只有 10KB/s 到 250KB/s,发射功率仅为 1mW,而且采用了休眠模式,功耗低。根据 ZigBee 联盟的估算,两节普通 5 号干电池可使用六个月到两年。

2)成本低:ZigBee 模块的成本在 6 美元左右,而且估计很快就能降到 1.5 到 2.5 美元,而且 ZigBee 协议免专利费。

3)网络容量大,组网灵活:一个 ZigBee 网络可以容纳最多 254 个从设备和一个主设备,一个区域内可以同时存在 100 个 ZigBee 网络。

4)时延短:通信时延和从休眠状态激活的时延都非常短。设备搜索时延典型值为 30ms,休眠激活时延典型值为 15ms,活动设备信道接入时延为 15ms。

5)安全:ZigBee 提供了数据完整性检查和鉴权功能,采用 AES-128 加密算法。

6)可靠:采取了碰撞避免机制,同时为需要固定带宽的通信业务预留了专用时隙,避免了发送数据时的竞争和冲突。MAC 层采用了完全确认的数据传输机制,每个发送的数据包都必须等待对方的确认信息。

1.3 ZigBee 技术相关概念

(1)ZigBee 设备

ZigBee 网络中的设备通常可以划分为两种类型,一种是全功能器件(FFD),它承担了网络协调者的功能,可以同网络中的任何设备通信,支持任何拓扑结构;另一种是简化功能器件(RFD),它不能作为网络协调者,只能与 FFD 通信,两个 RFD 之间不能通信,RFD 通常只用于星型拓扑结构中。

ZigBee 网络支持三种功能设备:网络协调器(coordinator),网络路由器(router),网络终端设备(end device)。前两种都是 FFD,后一种是 RFD。网络协调者的主要功能是协调建立网络,其他功能还包括:传输网络信标,管理网络节点及存储网络节点信息,并提供关联节点之间的路由信息;此外,网络协调器还要存储网络内所有节点的设备信息,数据包转发表,设备关联表以及与安全有关的密钥等。网络路由器,顾名思义,主要是起路由的作用,搜索可用的网络,传输数据以及向网络协调器请求数据。网络终端设备,在网络中扮演从属角色,在具体的应用中,他们是作为真正的功能设备。

(2)ZigBee 网络模型

ZigBee 主要采用三种组网方式:星型网、树型网和网状网。每一个 ZigBee 网络至少需要一个 FFD(coordinator)实现网络协调功能。在星型网中,网络协调器负责建立和维持网络,而其他的设备(end device)直接和网络协调器通信。树型网中,增加了 router,每一个终端设备要和其他的终端设备通信,都必须通过一层层向根节点(coordinator)回溯,再从根节点向下路由。网状网则提供了更加灵活的机制,网络中任意两个节点都可以建立链路,网络节点间的路径多,碰撞和阻塞可以减少,局部的故障不会影响整个网络的正常工作,可靠性高。

ZigBee 的组网采用的是 ad-hoc 方式,这是一种无基础设施的移动网络,网络中的每个终端可以自由移动,地位相等。这种网络对网络内部的设备数量不加限制,并随时可以建立无线通信链路。在 ZigBee 网络中,协调器(coordinator)一直处于监

听状态，当一个RFD设备被协调器发现，这时，FFD会把RFD的信息传送给协调器，由协调器进行编址，并计算其路由信息，更新数据转发表和设备关联表。如果发现的设备是FFD，则直接把自身信息上报协调器，并对周围的RFD设备进行轮询，记录它们的地址信息，通知协调器更新路由，此时新加入的FFD起到了一个桥梁作用，RFD通过FFD和协调器进行通信。

在ZigBee网络中，所有设备均有两个地址，一个是64位的唯一的IEEE地址，另一个是16位的每次加入网络后动态分配的网络地址。可用任何一种地址找到设备进行数据的传送。

1.4 ZigBee联盟和ZigBee解决方案

ZigBee联盟成立于2002年8月，由英国Invensys公司，日本三菱电气公司，美国摩托罗拉公司及荷兰飞利浦公司组成，迄今已吸引了上百家芯片公司，无线设备公司及产品开发商。由于ZigBee技术拥有低数据速率和通信范围较小的特点，这也决定了ZigBee技术适合于承载数据流量较小的业务。ZigBee技术的目标就是针对工业、家庭自动化、遥测遥控、汽车自动化、农业自动化和医疗护理等，例如灯光自动化控制，传感器的无线数据采集和监控，油田、电力、矿山和物流管理等应用领域。

由于ZigBee巨大的市场潜力，越来越多的厂商提供ZigBee解决方案。在几大IC厂商的大力支持和推动下，现在市场上已经有了一些供开发人员应用的器件或者套件。现在市面上比较有影响的解决方案主要是由Freescale、Ember、Chipcon、Atmel、Microchip等大公司提供的ZigBee芯片和协议栈。如Freescale的解决方案主要是通过一个8位MCU和一个ZigBee射频收发模块来实现。笔者所采用的就是Freescale的MC13192+GT60开发套件。该套件支持网状网，同时提供Z-stack开发工具。MC13192为该公司研发的射频收发芯片。

家庭网络通讯具有这些方面的特点：①传输数据量小，无需太大的传输速度；②网络的容量要大，家庭中的各种设备多；③信息的实时性要好，时延要短。ZigBee的技术特点决定了其能很好的满足家庭网络的上述需求。

2 基于ZigBee技术的家庭网络平台的构成

家庭网络ZigBee实现方案可以简单的概括为：在各种家庭电子设备中嵌入基于ZigBee芯片的无线网络收发模块，通过这些无线网络收发模块在各个网络子节点之间进行数据的传送，从而实现家庭内电子设备的无线互连和家庭自动化。

基于ZigBee技术的家庭网络平台主要由一个家庭网关和若干个无线通讯ZigBee功能模块组成。系统模型如图2所示。

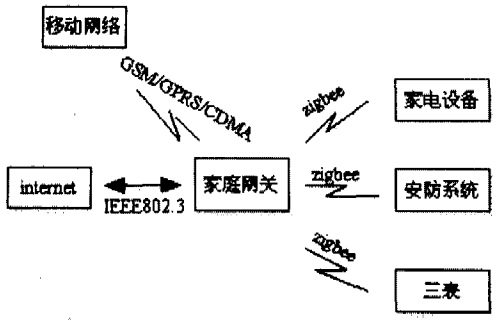

图2 基于ZigBee技术的家庭网络平台模型

根据ZigBee协议，该系统由一个ZigBee coordinator负责建立家庭网络，由若干个ZigBee router负责路由中继，剩下的就是作为功能部件的ZigBee end device。考虑到可靠性和灵活性，采用网状网的拓扑结构。当网络的覆盖范围不够的时候，可以适当添加router，保证通信，如图3所示。

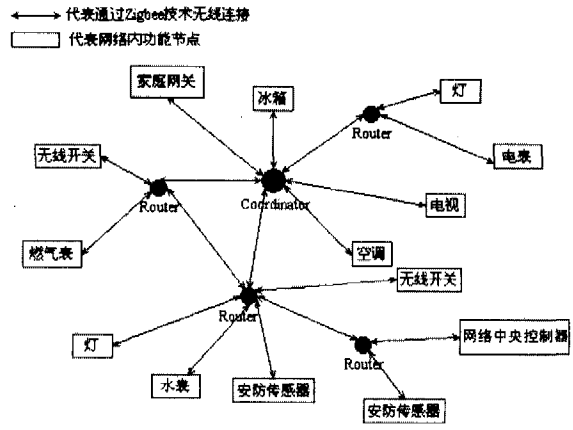

图3 基于ZigBee技术的家庭网络

(1)家电设备

将ZigBee无线收发模块嵌入在各种家电设备中，可以实现家电设备的无线控制，在家电设备供应商未提供ZigBee支持的时候，简单的做法是设计基于ZigBee的控制电源插座，以实现家电设备的简单控制，如开、关等。随着ZigBee技术的不断发展和家电设备供应商的加入，我们可以实现复杂的控制。

(2)安防系统

安装各种传感器，通过ZigBee模块与家庭网关通信，从而实现自动报警和撤警。

(3)家庭网关

家庭网关具备连入internet的功能。通过一个用户友好的web界面，用户可以轻松了解家里的情况，防止财产受到入侵者的破坏，并且只需要点击鼠标就可以从全球如何地方控制日常家电设备的运行。同时，通过市场上提供的GSM/GPRS/CDMA模块接入成熟的GSM/GPRS/CDMA移动网络，从而利用网络运营商提供的服务通过手机终端控制家庭网络。

(4)无线抄表系统

定期采集水表、电表和天然气表的数据，通过ZigBee模块发送给家庭网关，在(3)的支持下进而发给物业管理中心，实现自动抄表，节省人力和物力。

3 基于ZigBee技术的家庭网络实现的关键

通过对基于ZigBee技术的家庭无线网络平台的分析，在实际实现时应注意以下几个方面：

(1)ZigBee设备

ZigBee协调器(Coordinator)是整个ZigBee网络的核心。可以说，网络协调器是家庭网络存在的根本，网络协调器的故障将直接导致整个网络的瘫痪。所以，在网络协调器的设计实现上尤其要考虑其的可靠性。ZigBee协调器在我们的家庭网络中，并不是一个作为一个功能部件的，它的作用就是建立家庭网络，而其他的功能节点都是在它的协调下相互通信的。因此从软件方面来看，一般来说，ZigBee协调器不存在应用层面上的编程，所以这里所说的保证其可靠性主要是指在硬件方面的保证。

通常，FFD和RFD由微控制器(MCU)控制，该MCU通过队列串行外设接口(SPI)与ZigBee收发器相连。MCU的选择取决于该设备是否作为一个其下仍辖有ZigBee网络节点的FFD。一般的RFD通常由一个8位MCU控制，但对FFD来说，根据其复杂程度及所连接的网络，其控制单元可以是8位、16位或考虑选择功能强大的32位MCU。当我们要实现节点多、功能复杂的家庭网络时，就应当考虑选择16位或32位的MCU来作为ZigBee协调器的控制单元，以尽量避免由于计算能力不够

而引起的死机现象。

(2)家庭网关

利用 ZigBee 技术能够轻松实现家庭内部节点的无线连接。设计家庭网关则可以实现家庭网络与外部网络的连接以实现远程控制。根据不同的应用可以定义不同的家庭网关。由于我们定义的家庭网络内部只采用 ZigBee 技术进行无线连接,所以我们不需要考虑家庭网络内部不同协议的转换,而主要考虑实现 internet 接入和移动网络接入。家庭网关实际上就是一个功能齐全的嵌入式系统,硬件设计上采用功能强大的 ARM 芯片加上其他功能模块,如图 4 所示,而主要的工作在软件开发上,移植 μCLinux 操作系统,并在其上开发驱动程序、应用程序。为了使用户可以在 internet 上通过浏览器控制家庭网络,需要在网关上架设 web 服务器与用户进行通信,并通过 CGI 接口调用后台 CGI 程序。CGI 程序在 Web 服务器和控制程序间建立联系,调用具体的控制程序,实现对家庭网络内部节点的指定操作。

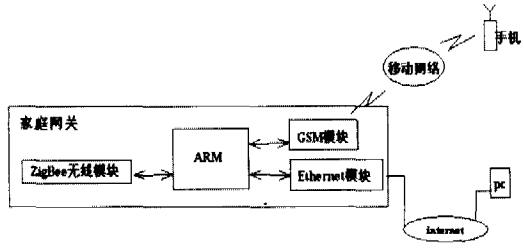

图 4 家庭网关结构图

(3)网络中心控制器

提起无线,离不开各种各样的遥控器。网络中心控制器就是协调整个网络管理的一个遥控器。它实际上是一个 (end device)。可以将它设计成一个带液晶显示的手池设备,从而通过它监控网络,随时随地都能知道网络内设备的状态并控制网络内的各种设备。网络监控在家庭网络中也是非常重要的,我们可以随时了解网络的状况,如设备的加入退出,设备故障等等。

(4)ZigBee 网络节点的低功耗

对于某些特殊的应用,低功耗问题是必须考虑的。例如,采取电池供电的传感器节点。就采用了基于需求时唤醒的工作模式。笔者使用的传感器节点由传感器加 ZigBee 模块(MC13192 和 MC9S08 两部分所组成)构成,在大部分时间里传感器节点处于睡眠模式,当满足传感器的触发条件时,触发 ZigBee 模块的 I/O 中断将信息传送给 ZigBee 模块,模块从睡眠状态唤醒,模块利用自身的控制芯片对信息进行处理后,再以无线的方式传送给网关。这种模式可以大大节省传感器节点的功耗,减少信息上报的时的碰撞概率,延长网络的寿命。

4 结束语

ZigBee 技术弥补了低成本、低功耗和低速率无线通信市场的空缺,随着正式版本协议的公布,更多的注意力和研发力量已经将转到应用的设计和实现上。可以预测,随着越来越多的内置 ZigBee 功能的设备投入市场,基于 ZigBee 的家庭网络将真正走入我们的生活。

参考文献

[1]张维勇,冯琳.ZigBee 实现家庭组网技术的研究[J].合肥工业大学学报(自然科学版),2005,28(7):755-759

[2]王磊.基于 ARM7 的嵌入式系统在智能家庭网络网关中的应用以及嵌入式 μcLinux 的研究[D].杭州:浙江大学,2005

[3]汤碧玉,曾楠,郑灵翔,等.嵌入式系统中基于 Web 的远程监控与实现[J].厦门大学学报(自然科学版),2004,43(5):632-635

[4]ZigBee Alliance,ZigBee Specification,version 1.0,2005

[收稿日期:2006.5.22]

(上接第 6 页)

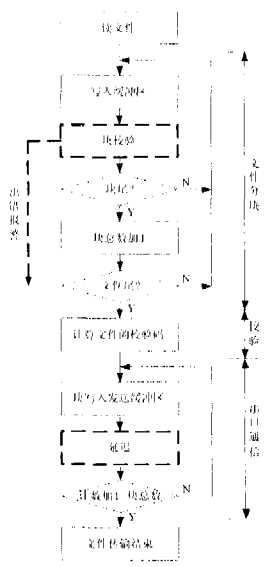

图 1 上位机程序流程图

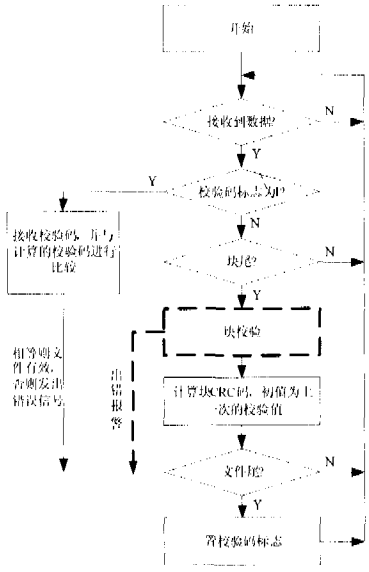

图 2 下位机程序流程图

实际应用中,根据数据流的特点,可以在分块的数据中添加块校验(如图 1、2 所示),这样可以及时的发现错误,并反馈错误信息。此外,MCU 接收到分块的数据并计算校验后,并非弃而不用,通常还要对数据块做其他的处理,根据工作量的大小很可能使得数据没有处理完(校验已完成),又接收到另一块数据,从而使得系统紊乱,所以数据处理的时间(不包括校验时间)在串行通信中是必须的考虑的。解决方法是上位机在每块数据发送后加一定延迟(如图 2 所示),待下位机有充足的时间处理好数据,再发送下一块数据,直至整个数据流发送完成。

表 2 文件传输测试记录

	文件I	文件II	文件III	备注
有效数据长度	120byte	2010byte	85024byte	
块总数(m)	8	105	3869	文件行数
块长度	(5~21) byte			每块均有和校验
理论传输时间	31.52ms	523.44ms	22141.67ms	串行波特率38400bps
理论校验时间	1.53ms	25.68ms	1086.22ms	按字节计算CRC码
实际传输时间	31ms	500ms	21156ms	在上位机由clock()函数获得

3 结束语

本文讨论了串行通信数据流的循环冗余校验方法,CRC 确保了通信的可靠性;同时对串行通信和校验计算时间进行分析,采用边传输边校验的方法,确保了通信的实时性;根据系统设计特性将数据流分块,采用逐块按位的方法计算 CRC 校验码,并对其可行性进行了论证。

参考文献

[1]常晓明,潘卫华.CRC 校验及其软件实现[J].电子技术应用,1995(6)

[2]徐爱钧,彭秀华.Keil Cx51 V7.0 单片机高级语言编程与 μVision2应用实践[M].北京:电子工业出版社,2005

[收稿日期:2006.9.25]