ZigBee 技术在工业监控网络中的应用①

贺才军[1] 方厚辉[1] 管于球[2] 黄 丽[1] (1.湖南大学 电气与信息工程学院 湖南 长沙 410082;
2.长沙高新开发区天富电子科技有限公司 湖南 长沙 410003)

摘 要: 介绍了ZigBee技术及其特点,对ZigBee网络结构进行了分析,利用CC2430设计了一种基于ZigBee技术的工业监控网络系统。详细地介绍了系统各节点的硬件设计,基于MSSTATE_LRWPAN协议栈节点的应用程序设计,设计了PC机与协调器节点间的通信协议,最后给出了网络系统的测试结果。

关键词: ZigBee; CC2430; MSSTATE_LRWPAN 协议栈; 工业监控

Application of ZigBee Technology in Industrial Monitoring Network

HE Cai-Jun[1], FANG Hou-Hui[1], GUAN Yu-Qiu[2], HUANG Li[1]
(1.College of Electrical and Information Engineering, Hunan University, Changsha 410082, China;
2.Tianfu Electronic Technology Co., Ltd. Changsha High-tech Development Zone, Changsha 410003, China)

Abstract: This paper introduces the ZigBee technology and its characteristics. It analyzes the ZigBee network structure and designs an industrial monitoring network system by using the CC2430 based on ZigBee technology. It describes the hardware designing in each node of the system and protocol stack node application design based on the MSSTATE_LRWPAN. It designs a communication protocol between PC computer and the nodes of coordinator, and finally gives testing results of the network system.

Keywords: Zigbee; CC2430; MSSTATE_LRWPAN protocol stack; industrial monitoring

1 引言

在大型工业企业中,存在生产地域分散、业务分工复杂、设备数量多、价值高、生产环境恶劣等特点[1]。企业需要对各种设备的状态进行实时监控,以便出现问题时能够及时报警与处理。现有的工业监控网络一般采用工业以太网与现场总线,这两种方式都具有布线麻烦、接线复杂、维护困难、成本高等缺点。

随着通信技术、嵌入式计算技术和传感器技术的飞速发展和日益成熟,具有感知能力、计算能力和通信能力的微型传感器开始在世界范围内出现。由这些微型传感器构成的传感器网络综合了传感器技术、嵌入式计算技术、分布式信息处理技术和通信技术,能够协作地实时监测、感知和采集网络分布区域内的各种环境或监测对象的信息,并对这些信息进行处理,获得详尽而准确的信息,传送到需要这些信息的用户。将这种无线传感器网络应用于工业领域,能够解决现有工业监控网络中存在的一些问题,因而具有巨大的科学意义和应用前景[2]。

ZigBee是一种新型的低功率、低成本、近距离的无线通信技术,是实现无线传感器网络的理想解决方案。本文根据工业监控的要求,设计了一个ZigBee工业监控网络系统,测试结果表明此系统能够达到设计要求。

2 Zigbee技术及其特点

ZigBee 技术是一种具有统一技术标准的短距离无线通信技术,其 PHY 层和 MAC 层协议为 IEEE 802.15.4 协议栈标准,网络层与应用层由 ZigBee 技

① 基金项目:科技部创新基金(08C26214302173)
收稿时间:2009-09-14;收到修改稿时间:2009-10-19

术联盟制定，其协议栈结构如图 1[3]。

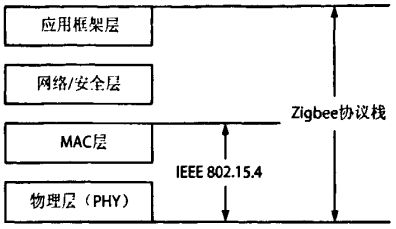

图 1　ZigBee 技术协议组成

物理层的特征是启动和关闭无线收发器，能量检测，链路质量，信道选择，清除信道评估(CCA)，以及通过物理媒体对数据包进行发送和接收[3]。MAC 层的具体特征是：信标管理、信道接入、时隙管理、发送确认帧、发送连接及断开连接请求，且为应用合适的安全机制提供一些方法[3,4]。网络层/安全层主要用于 ZigBee 的 LR-WPAN(低速率无线个人区域网)网的组网连接、数据管理以及网络安全等[5]。应用框架层主要为 ZigBee 技术的实际应用提供一些应用框架模型等[5]。

ZigBee 网络层支持星型网、树型网和网状。ZigBee 网络中的设备分为 FFD(全功能设备)和 RFD(简化功能设备)2 种。FFD 是具有路由与中继功能的网络节点，可作为协调器与路由器使用，RFD 只能作为终端节点使用。

ZigBee 无线网络具有如下特点：(1)低速率，其数据传输速率为 10~250kbps，专注于低传输应用；(2)短距离，两个节点之间的单跳距离在 10~75m 之间；(3)低功耗，在低功耗待机模式下，两节普通 5 号电池可使用 6~24 个月；(4)低成本，ZigBee 数据传输速率低，协议简单，所以大大降低了成本；(5)短时延，典型搜索设备时延为 30ms，休眠激活时延为 15ms，活动设备信道接入时延为 15ms；(6)网络容量大，网络可容纳 65,000 个设备；(7)网络的自组织、自愈能力强，通信可靠；(8)高安全性，ZigBee 提供了数据完整性检查和鉴权功能，采用 AES-128 加密算法,且各个应用可灵活确定其安全属性；(9)免执照频段，使用的频段分别为 2.4GHz(全球)、868MHz(欧洲)和 915MHz(美国)，均为免执照频段。ZigBee 的以上技术特点决定了它将是无线传感器网络的最好选择[3,4]。

3　基于Zigbee的无线传感器网络系统设计

3.1 系统概述

本文主要以某工厂的一个车间为对象，以监测各设备的温度信号为例进行说明。如果还需要监控其它参数，在网络中添加其它类型的传感器模块即可。本系统采用 ZigBee 树状网络拓扑结构，它主要由四部分组成：传感器节点、路由器、协调器以及 PC 机(管理系统)，系统框图见图 2。

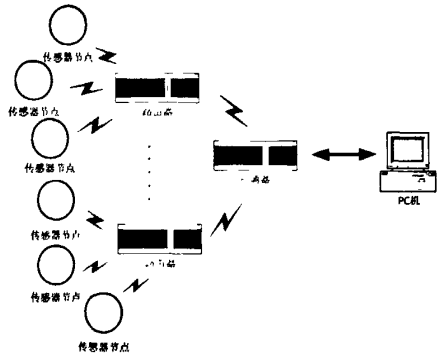

图 2　系统总体结构图

传感器节点位于被监控设备处，它把采集到的设备温度经过一定的处理后通过 ZigBee 网络发送到路由器。路由器放在一部分传感器节点的信号覆盖范围内，作传感器节点的父节点，把它的子节点数据转发给上一级(可以是路由器，也可以是协调器)。这样路由器增加了传感器节点的传输距离。协调器位于监控室外，它通过串口与监控室内的 PC 机连接，主要负责收集与处理路由器转发过来的数据，然后发送到 PC 机上显示与存储。协调器在 ZigBee 网络中负责整个网络的建立与维护。PC 机上的管理系统具有显示整个监控区域中设备的状态，它还具有报警与控制功能。若网络中的某个节点损坏，节点具有重新加入网络或者加入新节点之后，动态路由会自动调整网络，网络具有很强的自组织、自愈能力。

3.2 系统硬件设计

系统的实现采用 Chipcon 公司 (已被 TI 公司收购) 的 CC2430 射频芯片，它是全球首颗符合 ZigBee 联盟标准的 2.4GHz 射频芯片[6]。CC2430 符合 IEEE 802.15.4 标准，具有高性能 8051 内核的无线单片机，它在单个芯片上整合了 ZigBee RF 前端、内存和微控制器。CC2430 芯片采用 0.18um CMOS 工艺生

产，工作时的电流损耗为 27mA；在接收和发射模式下，电流损耗分别低于 27mA 或 25mA[6]。CC2430 的休眠模式和转换到主动模式的超短时间的特性，特别适合那些要求电池寿命非常长的应用[6]。网络中的三种节点的硬件框图如图 3 所示，其中图 3(a)为协调器，图 3(b)为路由器，图 3(c)为传感器节点。协调器、路由器、传感器节点都采用 CC2430 作为节点的微处理器与无线收发器，可以根据协议栈的大小选择 CC2430 芯片的闪存，它有 32/64/128KB 三种闪存可以选择[6]。选择合适大小的闪存可以减小系统成本。

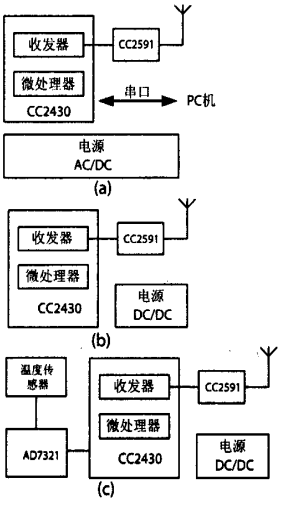

图 3　网络节点硬件框图

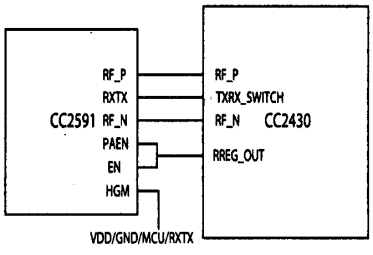

图 4　CC2591 与 CC2430 的接口

天线采用标准的 2.4GHz 杆状天线，可以根据实际情况选择 PCB 板天线、SMA 天线、陶瓷天线或弹簧天线，这里根据实际情况选择 SMA 天线[4]。CC2591 是TI公司专为低功耗与低电压无线应用而推出的集成度最高的 2.4GHz 射频前端。CC2591 集成的功率放大器输出功率高达+22dBm，并且集成了可以将接收机灵敏度提高+6dB 的低噪声放大器，从而能够显著增加无线系统的覆盖范围[7]。采用 CC2591 主要是考虑一般的生产厂房都比较大，节点的分布比较广，加大节点的发送距离可以适当减少路由器的个数。CC2591 与 CC2430 的接口电路[7]见图 4。

协调器的电源部分采用 AC/DC 转换，把 220V 的交流电转换为 3.3V 的直流电供 CC2430 与 CC2591。采用 CC2430 的 UART 与 PC 机连接，PC 机作为网络监控系统。路由器的电源由标准的+24V 工业用电经过 DC/DC 转化为 3.3V，供给 CC2591 与 CC2430。传感器节点的电源也采用+24V 工业用电经 DC/DC 转化为两种电压 3.3V 与±15V，3.3V 供 CC2430、CC2591 与 AD7321；±15V 供 AD7321。AD 芯片采用 ANALOG DEVICES 公司的 AD7321，通过 SPI 串行接口与 CC2430 连接。温度传感器采用显示变送一体化温度变送器，分度号为 Pt100，输出 4~20mA 标准电流信号，量程为-200~400℃，精度为 0.2% FS，供电为+24V 工业用电。

3.3 系统软件设计

系统软件设计主要包括上位机(管理系统)与下位机(ZigBee 无线传感器网络)设计两部分，本文重点讲述下位机软件。下位机软件基于 MSSTATE_LRWPAN 协议栈[8]，并选择 IAR Systems 公司的 IAR Embedded Workbench 嵌入式集成开发环境。下位机的软件包括三个部分：协调器软件、路由器软件、传感器节点软件。下位机系统的程序流程图如图 5 所示。

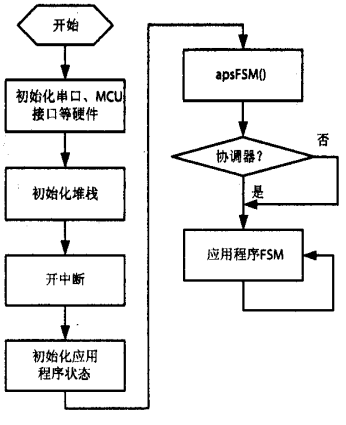

图 5　下位机系统程序流程图

系统大致分为硬件初始化、堆栈初始化、应用程序状态初始化、apsFSM()、应用程序 FSM。硬件初始

化包括串口初始化(协调器)、SPI 初始化(传感器节点)、MAC 定时器初始化、IO 口初始化、状态指示灯 LED 初始化；堆栈初始化主要设置协议栈各层初始状态；应用程序状态初始化应用程序的状态。若为协调器会先建立网络，其它类型的节点则在应用程序 FSM 中申请加入网络，这是为其它节点添加重入网功能。三种节点的其它区别在应用程序 FSM 中，所有的应用程序都在应用程序 FSM 中,这里就不详细说明了。

协调器与上位机的通信数据帧格式为：消息头+数据长度+消息类型+MAC 地址+短地址+RSSI+端点 EP+节点数据+预留位+校验信息。

传感器节点把采集到的传感器信息进行处理、打包后经路由器转发给协调器，同时还接受通过路由器转发来的协调器命令帧。路由器主要转发来自于协调器的命令帧与传感器节点的数据帧。协调器接收路由器转发的传感器节点数据帧，把收到的数据帧进行适当的处理、组合后发给上位机；还接受上位机的命令帧，对命令帧做适当的处理后发给传感器节点。Zigbee 网络中的数据发送方式采用直接发送，地址为网络地址。路由器也可以为多级路由，以便把远处的传感器节点与协调器连接起来。

3.4 系统测试与实现

根据文中所叙开发了一个工业监控网络，对系统进行了初步的测试。主要测试了节点的通信距离、组网延时、节点重入、采集间隔的设置等。通信距离：在空旷的室外，单个协调器与单个传感器节点在 300m 的距离通信误码率少于 1%。组网延时：单个协调器与单个节点,在室外 100m 组网时感觉不到延时，200m 延时 5s。节点重入：由协调器、路由器、传感器节点组成的三级网络，传感器节点掉电重新上电能够重新加入网络，当传感器节点的父节点离开网络时，传感器节点能够寻找其它父节点重新加入网络。采集间隔设置：可在 PC 机的网络管理系统上对传感器节点的温度传感器的采集间隔进行设置。

4 结语

本文提出了将 ZigBee 技术应用于工业监控网络中，能够解决工业监控网络传统布线的局限性。本文设计的 ZigBee 无线温度传感器网络经过试验证明具有通信距离远、节点加入方便、节点重入网络、组网灵活、可扩展性、设置采集间隔，能够满足工业应用的要求，具有很高的实用性。

参考文献

1 张克,李洋,陈炼,徐熙宗.基于Zigbee的传感器网络在石化工业中的应用探讨.计算机工程与设计, 2007,28(2):409－414.

2 陆霓凤,王培爱.基于 ZigBee 的无线传感器网络在工业监控中的应用.准备制造技术, 2009,(4):76－78.

3 蒋挺,赵成林.紫蜂技术及其应用.北京:北京邮电大学出版社, 2006. 2－9.

4 吴光荣,章剑雄,徐向华. ZigBee 网络系统节点硬件设计与实现.杭州电子科技大学学报, 2008,28(4):49－52.

5 Alliance Z. zigbee specification. Zigbee Document 053474r13,2006-12-1.

6 李文仲,段朝玉,等.ZigBee 无线网络技术入门与实战.北京:北京航空航天大学出版社, 2007. 41－44.

7 TI.CC2591 data sheet.SWRS070A, 2008-6.

8 Reese R. A ZigbeeTM-subset/IEEE 802.15.4TM multiplatform Protocol Stack. In: Electrical/Computer Engr MSU, editor, 2006.

(上接第 170 页)

IEEE Transactions on Neural Networks, 2005,16(3): 645－678.

5 Frey BJ, Dueck D. Clustering by passing messages between data points. Science, 2007,315(5814):972－976.

6 王开军.识别聚类间远近关系的双几何体模型.技术报告. 福建师范大学, 2009. http://www.mathworks.com/matlabcentral/fileexchange/authors/24811

7 王开军,张军英,李丹,张新娜,郭涛.自适应仿射传播聚类.自动化学报, 2007,33(12):1242－1246.

8 Dembélé D, Kastner P. Fuzzy C-means method for clustering microarray data. Bioinformatics, 2003,19(8):973－980.

9 Hartuv E, Schmitt A, Lange J, Meier-Ewert S, Lehrach H, Shamir R. An algorithm for clustering cDNAs for gene expression analysis. Genomics, 2000,66(3):249－256.