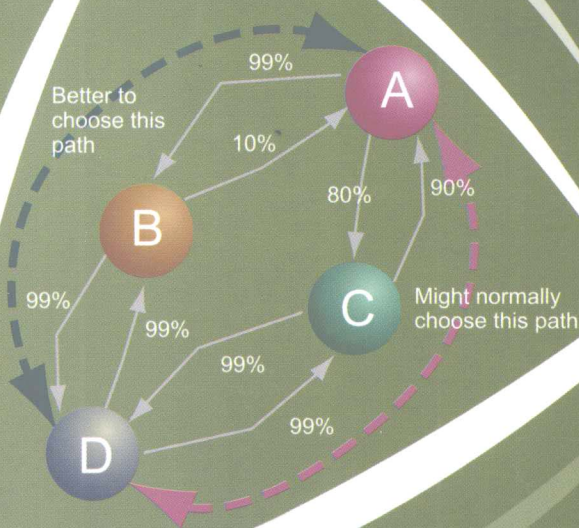


无线单片机技术丛书



ZigBee2007/PRO协议栈 实验与实践

李文仲 段朝玉 等编著



北京航空航天大学出版社

TN92
73

TN92
73
无线单片机技术丛书

ZigBee2007/PRO 协议栈 实验与实践

李文仲 段朝玉 等编著

北京航空航天大学出版社

内 容 简 介

介绍掌握 ZigBee 技术的关键——ZigBee 协议栈。从 ZigBee1.0 到 ZigBee1.1,再到目前的 ZigBee PRO,协议栈的结构、功能调用、参数设置、软件代码等都有了重大的变化,掌握的难度也在不断增加。如何在这复杂的协议栈技术手册和浩瀚的代码中抓住其中的精髓?如何驾驭协议栈和实现自己的应用设计?只有靠具体动手实践,靠大量的实验去体验和观察。同时介绍了本书涉及的 ZigBee 芯片 CC2520 及相关低功耗微控制器 MSP430。

本书没有太多的理论描述,主要从实践入手,让读者更多地体会 ZigBee 协议如何用程序实现,如何利用 ZigBee 协议达到需要的目的,如何在 ZigBee 协议栈之上建立自己的应用,从而更快速地完成项目。

本书可作为从事单片机、无线应用、自动化控制、无线传感等技术的工程技术人员的学习、参考用书,也可作为高等院校的计算机、电子、自动化专业无线通信课程的教材。

图书在版编目(CIP)数据

ZigBee2007/PRO 协议栈实验与实践/李文仲,段朝玉等编著.
北京:北京航空航天大学出版社,2009.3
ISBN 978-7-81124-493-9

I. Z… II. ①李…②段… III. 无线电通信—通信网 IV. TN92

中国版本图书馆 CIP 数据核字(2009)第 021433 号

ZigBee2007/PRO 协议栈实验与实践

李文仲 段朝玉 等编著

责任编辑 孔祥燮 范仲祥 范曼华

*

北京航空航天大学出版社出版发行

北京市海淀区学院路 37 号(100083) 发行部电话:010-82317024 传真:010-82328026

http://www.buaapress.com.cn E-mail:bhpress@263.net

涿州市新华印刷有限公司印装 各地书店经销

*

开本:787×960 1/16 印张:20.5 字数:459 千字

2009 年 3 月第 1 版 2009 年 3 月第 1 次印刷 印数:5 000 册

ISBN 978-7-81124-493-9 定价:35.00 元

序 言

当今世界通信技术迅猛发展。ZigBee 作为一种新兴的短距离无线通信技术,正有力地推动着低速率无线个人区域网络 LR - WPAN(Low - Rate Wireless Personal Area Network)的发展。ZigBee 是基于 IEEE 802.15.4 标准的应用于无线监测与控制应用的全球性无线通信标准,强调简单易用、近距离、低速率、低功耗(长电池寿命)且极廉价的市场定位,可以广泛应用于工业控制、家庭自动化、医疗护理、智能农业、消费类电子和远程控制等领域,拥有广阔的应用前景。

ZigBee 技术核心是运行于微控制器内部的一套软件,也称之为软件 ZigBee 协议栈,负责该协议规范制定的是 ZigBee 联盟。ZigBee 联盟于 2004 年 12 月通过了 ZigBee1.0(也称 ZigBee2004)标准,之后于 2005 年 9 月公布并提供下载。

2006 年 12 月,ZigBee 联盟又推出 ZigBee1.1(也称 ZigBee2006)版。ZigBee1.1 较原有 ZigBee1.0 作了比较大的改进,例如新增 ZCL(ZigBee Cluster Library)、集团装置(Group Device)、多播(Multicast)功效及更丰富的网络拓扑,并且可以直接通过无线方式(Over The Air, OTA)进行组态配置和软件更新,此外还移除了 KVP(Key Value Pair)的信息格式。

2007 年 10 月,ZigBee 联盟推出 ZigBee2007,制订出 ZigBee Pro Feature Set(简称 ZigBee PRO)的新标准,对 ZigBee 协议栈进行了重大升级,加强了对家庭自动化(Home Automation, HA)、建筑/商业大楼自动化(Building Automation, BA)和高级抄表结构(Advanced Meter Infrastructure, AMI) 3 种应用类型的支持;同时在自动跳频以及支持更大的网络、更高级的路由算法等方面的改进和提高,将 ZigBee 协议栈的可用性和可靠性提高到一个全新的阶段。

成都无线龙通讯科技有限公司(以下简称无线龙)自 ZigBee 协议公开以来,一直专注于 ZigBee 技术的研究开发,在 ZigBee 开发系统和相关教材书籍方面,努力跟踪该技术的发展。ZigBee1.0 的协议配套教材为《ZigBee 无线网络技术入门与实战》,配套开发系统为 C51RF - JKS; ZigBee1.1 的协议配套教材为《ZigBee2006 无线网络与无线定位实战》,配套开发系统为 C51RF - 3 - PK。本教材就是专门为 ZigBee PRO 协议而作,配套系统为 C51RF - CC2520 - PK。

掌握 ZigBee 技术的关键是掌握 ZigBee 协议栈,从 ZigBee1.0 到 ZigBee1.1,再到目前的 ZigBee PRO,协议栈的结构、功能调用、参数设置、软件代码等都有了重大的变化,掌握的难度也在不断增加。如何在这复杂的协议栈技术手册和浩瀚的代码中抓住其中的精髓?如何驾驭协议栈和实现自己的应用设计?只有靠具体动手实践,靠大量的实验,去体验和观察。因此本书没有太多的理论描述。如果读者需要了解相关 ZigBee 理论,可查阅北京航空航天大学出版社出版的《ZigBee 无线网络技术入门与实战》和《ZigBee2006 无线网络与无线定位实战》两本书。如果读者具有一些 ZigBee 的理论基础知识,那么此书必定会让读者尽快地去验证并应用

这些理论。如果读者还对 ZigBee 技术一无所知,那么此书前面的小部分理论性章节会让读者对 ZigBee 技术不再陌生。如果读者已经有 ZigBee 的开发经验,那么通过本书将使读者更进一步地领会最新 ZigBee PRO 协议应用。

此书也非常适合高校 ZigBee 技术的教学,因为大量的实例让学生学习不再空洞,让学生把高深的理论知识通过本书的实验直观地演示 ZigBee 组网、ZigBee 数据传输、ZigBee 网络拓扑等功能,使学生学习起来更加得心应手。

本书第 1、2 章主要介绍 ZigBee 必要的理论知识。其中:第 1 章主要介绍了从 ZigBee 的起源到 ZigBee PRO 技术的发展历程,ZigBee 技术的基本概念和基础知识,以及 ZigBee 技术的应用和将来的发展概述;第 2 章主要介绍目前市面上普遍采用的 ZigBee 芯片,重点介绍本书涉及的 ZigBee 芯片 CC2520 及相关处理器 MSP430。

第 3 章主要对无线龙推出的经典 ZigBee 专业开发系统 PK 进行全面讲解,为后续的实践打下硬件基础。为了承接 ZigBee2006 协议开发系统,介绍了 C51RF-3-PK 系统,并对 ZigBee2007/PRO 协议推出的 C51RF-CC2520-PK 进行了更为详细的介绍。

第 4、5 章针对 ZigBee2006 协议栈两个非常具有代表性的例程进行分析。其中:第 4 章介绍了 ZigBee 网络的建立、加入、退出,以及数据传输等 ZigBee 网络的基本功能;第 5 章介绍了 ZigBee 协议中非常具有实用性的“绑定”功能。通过这两章的介绍,读者应该能在 ZigBee2006 协议栈基础上建立自己的应用,并完成基于 ZigBee2006 协议栈的项目。

第 6~8 章主要对 ZigBee2007/PRO 协议栈进行剖析。其中:第 6 章是 ZigBee2007 基础实验,主要是让读者感觉 ZigBee2007 与 ZigBee2006 的区别;第 7 章是 ZigBee PRO 基础实验,让读者第一次认识这个 ZigBee 联盟推出的新概念,并通过程序去亲身体会它的存在和优势;第 8 章是 ZigBee PRO 进阶实验,通过 ZigBee 联盟规定的家庭自动化模式实现家庭智能化演示。

第 9 章介绍无线龙在前面所有实验基础上开发的一套无线传感器网络应用。从硬件的设计,到软件的实现,最后通过上位机 PC 软件监控界面来全面监控整个基于最新 ZigBee PRO 协议的传感器网络。本章对之前所学进行了全面总结,也为学习 ZigBee 协议画上了一个圆满的句号。

无线龙的工程师们为本书的实验开发了全部代码,而且这些实验均在无线龙系列开发系统上进行了实际验证。第 4、5 章实验是在 C51RF-3-PK 系统上验证通过的;第 6~8 章实验是在 C51RF-CC2520-PK 系统上验证通过的;而第 9 章的无线网络传感器方案是在 C51RF-CC2520-WSN 系统上验证通过的。

希望每位读者在学习完本书后都能自己动手开发 ZigBee 相关项目,也希望本书能为读者带去一份精彩的技术人生。我们的初衷是真诚地为读者服务!

最后,要特别感谢北京航空航天大学出版社的全力支持,如果没有他们的努力和辛勤劳动,这本书是不会这么快出版的。

作 者

2008 年 10 月

于锦江河畔

目 录

第 1 章 ZigBee 技术概述

1.1 ZigBee 技术的演变与进展	1
1.1.1 ZigBee 技术的由来	2
1.1.2 ZigBee 技术的发展历程	2
1.2 ZigBee 技术特点	5
1.3 ZigBee2007/PRO 特性	6
1.3.1 ZigBee 与 ZigBee PRO 比较	6
1.3.2 不同 ZigBee 版本的兼容分析	8
1.4 ZigBee 无线网络使用频谱和 ISM 开放频带	16
1.5 ZigBee 技术的广阔应用前景	17

第 2 章 低功耗微控制器 MSP430 与 ZigBee 芯片 CC2520

2.1 低功耗微控制器 MSP430	22
2.1.1 关键特性	22
2.1.2 MSP430 模块化架构	23
2.1.3 16 位 RISC 先进 CPU	24
2.1.4 超低功耗性能	25
2.1.5 灵活的时钟系统	26
2.1.6 智能外设	27
2.1.7 MSP430 应用	29
2.2 MSP430F2618 简介	29
2.2.1 MSP430F2xxx 介绍	30
2.2.2 MSP430F2618 特性	30
2.3 ZigBee 芯片 CC2520	31
2.3.1 CC2520 的特性	32
2.3.2 CC2520 引脚描述	34
2.3.3 CC2520 与 CC2420 的区别	35
2.3.4 CC2520 典型设计	36

第 3 章 ZigBee 无线网络多功能开发系统

3.1 无线网络 ZigBee 开发系统平台选择	39
--------------------------------	----

3.1.1	如何选择嵌入式无线开发工具和平台	40
3.1.2	需要的设备和必要条件	42
	总 结	43
3.2	多功能可视化 ZigBee 无线网络开发系统 C51RF-3-PK	44
3.2.1	C51RF-3-PK 仿真器	44
3.2.2	网络液晶扩展板	45
3.2.3	C51RF-3-PK 电池板	51
3.2.4	ZigBee 模块	53
3.3	图形化 ZigBee2007 开发系统	56
3.3.1	ZigBee 模块 CC2520	57
3.3.2	网络液晶扩展板	58
3.4	ZigBee 软件集成开发平台	63
3.4.1	IAR 集成开发环境的安装	65
3.4.2	添加文件或新建程序文件	72
3.4.3	设置工程选项参数	74
3.4.4	编译、链接、下载	78
3.4.5	仿真调试	79

第 4 章 ZigBee 开发入门

4.1	认识 ZigBee 协议栈	88
4.2	ZigBee 网络数据传输	90
4.2.1	实验目的	90
4.2.2	ZigBee 数据传输原理解析	90
4.2.3	实验设备准备	110
4.3	ZigBee 协议栈编译/下载	111
4.3.1	设备选择及设置	111
4.3.2	编译/下载程序	112
4.4	ZigBee 源代码剖析	113
4.4.1	发送一个信息包	113
4.4.2	收发数据过程	113
4.4.3	接收一个信息包	116
4.5	实验流程	117
4.5.1	流程图	117
4.5.2	路由器代码	118
4.5.3	协调器代码	120
4.6	ZigBee 分析仪分析 ZigBee 数据包	121
4.6.1	协议分析仪	121

4.6.2 ZigBee 数据格式	122
4.6.3 加入网络数据分析	125
4.6.4 收发数据分析	126
4.7 实验效果	128

第 5 章 ZigBee 无线网络开发进阶

5.1 ZigBee 协议栈结构	129
5.2 ZigBee 协议栈实时操作系统	132
5.2.1 OS 术语介绍	132
5.2.2 OSAL API 介绍	133
5.2.3 OSAL 任务	142
5.3 ZigBee2006 应用接口	144
5.3.1 实验目的	144
5.3.2 原理介绍	144
5.3.3 软件准备 SAPI 介绍	145
5.4 网络形成	145
5.4.1 协调器格式化网络	146
5.4.2 路由器和终端设备加入网络	146
5.4.3 ZDO_StartDevice	147
5.5 绑 定	148
5.5.1 绑定表格	149
5.5.2 绑定建立	151
5.5.3 绑定解除	156
5.6 命 令	156
5.6.1 命令定义及使用	156
5.6.2 串	159
5.6.3 ZCL 介绍	159
5.6.4 Profile 介绍	160
5.7 灯光控制实验	165
5.7.1 APP 函数分析	165
5.7.2 灯光控制实验过程	176
5.7.3 实验总结	178
5.8 无线温度传感器实验	179
5.8.1 设 备	179
5.8.2 命 令	180
5.8.3 发现和绑定	180
5.8.4 数据包发送和接收	181

第 6 章 ZigBee2007/PRO 入门

6.1	ZigBee2007/PRO 入门实验	185
6.2	实验设备	185
6.2.1	硬件介绍	185
6.2.2	硬件组成	186
6.3	实验基础知识	186
6.3.1	ZigBee2007 简介	186
6.3.2	ZigBee2007/PRO 协议栈简介	187
6.3.3	ZigBee 设备在 Zstack 中的体现	189
6.4	实验内容	191
6.4.1	建立任务	192
6.4.2	按键处理函数	197
6.4.3	发送函数	198
6.4.4	接收处理函数	200
6.5	实验步骤和结果	200
6.5.1	建立网络	200
6.5.2	路由设备加入网络	202
6.5.3	发送数据	203
6.5.4	退出小组	203
6.5.5	加入小组	203
6.6	实验拓展	204
6.6.1	项目分析	204
6.6.2	协调器函数的设计	204
6.6.3	路由器设备函数设计	205
6.7	实验总结	206

第 7 章 ZigBee2007/PRO 进阶

7.1	实验目的	207
7.2	实验设备	207
7.2.1	硬件介绍	207
7.2.2	硬件组成	208
7.2.3	ZigBee2007 协议栈	208
7.3	实验基础知识	209
7.3.1	ZigBee PRO 简介	209
7.3.2	ZigBee PRO 中的路由	210
7.3.3	ZigBee PRO 新功能	211

7.3.4 信息包格式	211
7.4 实验内容	212
7.4.1 初始化任务	213
7.4.2 任务处理	215
7.4.3 UART_RX_CB_EVT 事件	219
7.4.4 串口发送函数	222
7.4.5 串口接收中断函数	223
7.4.6 串口读取函数	224
7.4.7 ZigBee 发送函数	225
7.4.8 ZigBee 接收处理函数	226
7.5 实验步骤和现象	228
7.5.1 建立网络	228
7.5.2 路由设备加入网络	229
7.5.3 查看网络中节点	230
7.5.4 配置地址	231
7.5.5 收发数据	231
7.6 实验总结	233

第 8 章 ZigBee2007/PRO 高级应用——家庭自动化

8.1 家庭自动化概念	234
8.2 ZigBee2007/PRO 的家庭自动化	236
8.3 家庭自动化实验目的	236
8.4 家庭自动化体系	236
8.5 实验设备	237
8.6 家庭自动化实验工程	238
8.7 家庭自动化工程剖析	239
8.7.1 实验操作流程	240
8.7.2 灯和控制器主函数程序流程图	240
8.7.3 其他初始化关键函数	242
8.7.4 网络状态变化函数	243
8.7.5 绑定相关函数	246
8.8 操作系统	250
8.8.1 操作系统关键参数	251
8.8.2 操作系统关键函数	252
8.9 灯设备关键任务	256
8.10 控制器关键任务	260
8.11 实验操作步骤	265

8.12 家庭自动化例程总结	268
第 9 章 ZigBee2007 无线传感器网络	
9.1 无线传感器网络概述	269
9.1.1 什么是无线传感器网络	269
9.1.2 无线传感器网络现状	270
9.1.3 ZigBee 在无线传感器网络上的应用	272
9.1.4 ZigBee 无线传感器网络系统特点	272
9.2 ZigBee2007 无线传感器网络实验概述	273
9.3 ZigBee2007 无线传感器网络硬件设计	274
9.3.1 网关底板设计	275
9.3.2 传感器底板设计	276
9.4 网关与 PC 机的数据连接	281
9.5 ZigBee2007 无线传感器网络建立与网络管理	287
9.5.1 网络通信过程介绍	287
9.5.2 网关网络节点的地址管理	288
9.6 网关与节点间的无线采集过程	293
9.7 程序编译、下载	303
9.8 实验效果	304
附录 A 网络层所定义的特性常量	311
附录 B 网络层信息库属性	312
参考文献	315

第 1 章

ZigBee 技术概述

ZigBee 是一种新兴的短距离、低速率无线网络技术。它是一种介于无线标记技术与蓝牙之间的技术提案,此前被称作 HomeRF Lite 或 FireFly 无线技术,主要用于近距离无线连接。它有自己的无线电标准,是通过数千个微小的传感器之间相互协调来实现通信的。这些传感器只需要很少的能量,以接力的方式通过无线电波将数据从一个传感器传到另一个传感器,所以通信效率非常高。而这些数据就可以进入计算机用于分析,或者被另外一种无线技术如 WiMax 收集。

1.1 ZigBee 技术的演变与进展

ZigBee 的基础是 IEEE 802.15.4。它是 IEEE 无线个人区域网(Personal Area Network, PAN)工作组的一项标准,被称作 IEEE 802.15.4(ZigBee)技术标准。

ZigBee 不只是 802.15.4 的名字。因为 IEEE 仅规范了低级媒体控制层(MAC)层和物理层协议,所以 ZigBee 联盟对其网络层协议和 API 进行了标准化。IEEE 802.15.4 完全协议用于一次可直接连接到一个设备的基本节点的 4 KB,或者作为 Hub 或路由器的协调器的 32 KB。每个协调器可连接多达 255 个节点,几个协调器则可形成一个网络,而对路由传输的数目则没有限制。ZigBee 联盟还开发了安全层,以保证这种便携设备不会意外泄漏其标识,而且这种利用网络的远距离传输不会被其他节点获得。

ZigBee 联盟成立于 2001 年 8 月。2002 年下半年,英国 Invensys 公司、日本 Mitsubishi 公司、美国 Motorola 公司及荷兰 Philips 半导体公司四大巨头共同宣布,它们将加盟“ZigBee 联盟”,以研发名为“ZigBee”的下一代无线通信标准。这一事件成为该项技术发展过程中的里程碑。

到目前为止,除了 Invensys、Ember、Mitsubishi、Motorola、TI(德州仪器)、Freescale(飞思卡尔)和 Philips 等国际知名的大公司外,该联盟已有 200 多家成员企业,并在迅速发展壮大。

其中涵盖了半导体生产商、IP 服务提供商、消费类电子厂商及 OEM 商等,例如 Honeywell、Eaton 和 Invensys Metering Systems 等工业控制和家用自动化公司,甚至还有像 Mattel 之类的玩具公司。所有这些公司都参加了负责开发 ZigBee 物理和媒体控制层技术标准的 IEEE 802.15.4 工作组。

有关 ZigBee 的详细介绍,可查阅北京航空航天大学出版社出版的《ZigBee2006 无线网络与无线定位实战》。

1.1.1 ZigBee 技术的由来

在蓝牙技术的使用过程中,人们发现蓝牙技术尽管有许多优点,但仍存在着许多缺陷。对工业、家庭自动化控制和遥测遥控领域而言,蓝牙技术显得太复杂,且功耗大、距离近、组网规模太小等,因此这些领域对无线通信的需求越来越强烈。正因为如此,经过人们的长期努力,ZigBee 协议于 2004 年正式制定。

ZigBee 是一个由可多达 65 000 个无线数传模块组成的无线数传网络平台,十分类似现有移动通信的 CDMA 网或 GSM 网。其中每一个 ZigBee 网络数传模块类似移动网络的一个基站,在整个网络范围内,它们之间可以进行相互通信;每个网络节点间的距离可以从标准的 75 m,到扩展后的几百米,甚至几公里。另外,整个 ZigBee 网络还可以与现有的其他各种网络连接。例如,可以通过互联网在北京监控云南某地的一个 ZigBee 控制网络。

不同的是,ZigBee 网络主要为自动化控制数据传输而建立,而移动通信网主要为语音通信而建立。每个移动基站价值一般都在百万元人民币以上,而每个 ZigBee“基站”却不到 1 000 元人民币。每个 ZigBee 网络节点不仅本身可以与监控对象连接,例如与传感器连接直接进行数据采集和监控,还可以自动中转别的网络节点传过来的数据资料。除此之外,每一个 ZigBee 网络节点(FFD)还可在自己信号覆盖的范围内,与多个不承担网络信息中转任务的孤立子节点(RFD)无线连接。

每个 ZigBee 网络节点(FFD 和 RFD)可支持多达 31 个的传感器和受控设备,并且每一个传感器和受控设备还可以有 8 种不同的接口方式。另外,ZigBee 可以采集和传输数字量和模拟量。

1.1.2 ZigBee 技术的发展历程

ZigBee 是以 IEEE 802.15.4 标准为基础发展起来的无线通信技术。2000 年 12 月,工作小组成立,负责起草 IEEE 802.15.4 标准。2002 年 10 月,ZigBee 联盟当时的成员有 Philips Semiconductor、Honeywell、Mitsubishi、Invensys 和 Motorola 等。其中 Philips Semiconductor 于 2004 年 4 月退出,改由 Philips Lighting(飞利浦照明)接替其在 ZigBee Alliance 中的原

有会员位置。

2004 年 12 月, ZigBee1.0 标准(又称为 ZigBee2004)出台, 之后于 2005 年 9 月公布并提供下载。2006 年 12 月, 又对 ZigBee1.0 进行了修订, 推出了 ZigBee1.1 版(又称为 ZigBee2006)。ZigBee1.1 对原有 ZigBee1.0 作了若干修改, 例如新增 ZCL(ZigBee Cluster Library)、群化式装置(Group Device)、多播(Multicast)功效, 以及直接通过无线方式(Over The Air, OTA)进行组态配置。此外, 还移除了 KVP(Key Value Pair)的信息格式。

然而 ZigBee1.1 依然无法达到最初的理想, 此标准又于 2007 年 10 月完成再次修订(称为 ZigBee2007/PRO, 或者 ZigBee PRO 或 ZigBee2007), 推出了 ZigBee Pro Feature Set(简称 ZigBee PRO)的新标准。此新标准 ZigBee 联盟更专注 3 种应用类型的拓展, 包括家庭自动化(Home Automation, HA)、建筑/商业大楼自动化(Building Automation, BA)和先进抄表基础设施建设(Advanced Meter Infrastructure, AMI)。

ZigBee PRO 与之前的 ZigBee1.1 有诸多的不同, 且推翻了许多在 ZigBee1.0、1.1 版本中的设计, 例如移除了 Cskip 的地址排定(Address Assignment)法。这就表示 ZigBee PRO 不支持 1.1 版本中的树状路由(Tree Routing)法。然而却同时增加了新的机制, 例如或然性的地址安排(Stochastic Address Assignment)、多对一性的路由(Many to One Routing)和来源节点性的路由(Source Routing)。

另外, 还增加了快速频率切换(Frequency Agility)、封包拆解(Fragmentation)与重组(Re-assembly)及群组性寻址(Group Addressing)等功能, 并且将安全性机制区分成标准安全与高度安全两种模式。

由于许多标准有直接以制定年份为名的习惯, 因此 ZigBee1.0 有时也称为 ZigBee2004。ZigBee1.1 有时也称为 ZigBee2006。ZigBee PRO 有时也称为 ZigBee2007。又如 IEEE 802.16d 于 2004 年完成, 有时也称为 IEEE 802.16 2004。另外, 从修订角度而言, ZigBee1.0 为 Rev 7, 1.1 版本为 Rev 13, PRO 版本则为 Rev 16。

自从 2003 年 12 月 CHIPCON 公司推出业界第一款 ZigBee 收发器 CC2420 以来, 各大半导体厂家可谓百家争鸣, 先后推出了许多款 ZigBee 收发芯片, 其中仍然以 CHIPCON 公司最受关注。先后有多家公司推出与 ZigBee 收发芯片匹配的专业处理器, 除了 CHIPCON 公司外, 就以微芯公司的 PIC18F4620 和 ATMEL 公司的 A222222 最为成功。2004 年 12 月, CHIPCON 公司推出了全球第一个 IEEE 802.15.4/ZigBee 片上系统(SoC)解决方案——CC2430 无线单片机。该款芯片内部集成了一颗增强型的 8051 内核以及业内性能卓越的 ZigBee 收发器 CC2420。2005 年 12 月, CHIPCON 公司再接再厉, 推出了内嵌定位引擎的 ZigBee/IEEE 802.15.4 解决方案 CC2431。

2006 年 2 月, TI 公司收购了 CHIPCON 公司, 以巩固其在 RF 行业的龙头地位。之后, TI 公司在发布的 ZigBee 收发器以及无线单片机上进行不断修订, 也陆续开发出了许多具有针对性的开发系统, 并于 2006 年 10 月把其自身的 MSP430 处理器用于对 ZigBee 收发器的控制,

而且在 2007 年 5 月又推出了整套 CC2420 + MSP430 ZigBee/IEEE 802.15.4 Development Kit 开发包。另外, TI 公司于 2008 年 2 月, 推出了第二代 ZigBee/IEEE 802.15.4 收发芯片 CC2520; 2008 年 4 月, 推出了 ZigBee 协处理器 CC2480; 2008 年 6 月, 推出了 2.4 GHz 放大芯片 CC2591。

在国内, 嵌入式无线开发工具供应商成都无线龙通讯科技有限公司(以下称无线龙)从 2005 年就开始进行 ZigBee 无线网络技术研发, 并相继跟随芯片发展步伐推出相关 ZigBee 开发工具。例如 ZigBee2004 开发系统 C51RF-3-JKS, 配套北京航空航天大学出版社出版的《ZigBee 无线网络技术入门与实战》; ZigBee2006 开发系统 C51RF-3-PK, 配套北京航空航天大学出版社出版的《ZigBee2006 无线网络与无线定位实战》; ZigBee2007 开发系统 C51RF-CC2520-PK, 配套北京航空航天大学出版社出版的《ZigBee2007/PRO 协议栈实验与实践》; ZigBee 协处理器 CC2480 开发工具 ARMRF2-STR911。

不仅是硬件, 软件方面 TI 公司也跟进得相当快, 而且是唯一一家免费公开协议栈的公司。

2007 年 1 月, TI 公司宣布推出 ZigBee 协议栈(Z-Stack), 并于 2007 年 4 月提供免费下载版本 V1.4.1。Z-Stack 达到 ZigBee 测试机构德国莱茵集团(TUV Rheinland)评定的 ZigBee 联盟参考平台(golden unit)水平, 目前已为全球众多 ZigBee 开发商所广泛采用。Z-Stack 符合 ZigBee2006 规范, 支持多种平台, 其中包括面向 IEEE 802.15.4/ZigBee 的 CC2430 片上系统解决方案、基于 CC2420 收发器的新平台以及 TI 公司的 MSP430 超低功耗微控制器(MCU)。

除了全面符合 ZigBee2006 规范以外, Z-Stack 还支持丰富的新特性, 如无线下载, 可通过 ZigBee 网状网络(Mesh Network)无线下载节点更新。Z-Stack 还支持具备定位感知(Location Awareness)特性的 CC2431。上述特性使用户能够设计出可根据节点当前位置改变行为的新型 ZigBee 应用。

Z-Stack 与低功耗 RF 开发商网络, 是 TI 公司为工程师提供的广泛性基础支持的一部分, 其他支持还包括培训和研讨会、设计工具与实用程序、技术文档、评估板、在线知识库、产品信息热线以及全面周到的样片供应服务。

2007 年 7 月, Z-Stack 升级为 V1.4.2, 之后对其进行了多次更新, 并于 2008 年 1 月升级为 V1.4.3。2008 年 4 月, 针对 MSP430F4618 + CC2420 组合把 Z-Stack 升级为 V2.0.0; 2008 年 8 月, 升级为 Z-Stack V2.0.0, 支持 CC2520 + MSP430; 2008 年 7 月, Z-Stack 升级为 V2.1.0, 支持 ZigBee PRO and Smart Energy。

Z-Stack 2.1.0 软件全面支持 ZigBee 与 ZigBee PRO 特性集并符合最新智能能源规范, 非常适用于高级电表架构(AMI)。Z-Stack 2.1.0 软件可与无线龙的 C51RF-CC2520-PK 平台协同工作。该平台包括 MSP430 超低功耗微控制器、CC2520 RF 收发器以及 CC2591 距离扩展器, 通信距离可达数公里。该软件提供了其所支持的应用范例库, 其中包括智能能源、

家庭自动化以及无线下载 (OAD) 等功能。

目前, TI 公司一共推出了 3 种 ZigBee 方案: 方案 1 为单芯片 (SOC) CC2430/ CC2431; 方案 2 为协处理器 (CC2480) 方案, 提供 AT 命令接口; 方案 3 为微控制器加射频收发器 (CC2520/CC2420)。

方案 1 和 3 功耗理想, 其中方案 1 是单芯片方案, 集成度高; 方案 3 是采用 TI MSP430 加上外置的射频收发器。方案 2 的 ZigBee 协处理器可以与任何微控制器接口, 下一步还将与 DSP 对接, 因此方案 2 更加灵活, 易于尽快上市。

对于方案 1, 无线龙提供的开发平台是 C51RF - 3 - PK; 对于方案 2, 提供的开发平台是 RF2 - STR911; 对于方案 3, 提供的开发平台是 C51RF - CC2520 - PK。相关开发平台介绍, 详见第 3 章。

1.2 ZigBee 技术特点

ZigBee 技术特点包括以下几方面。

- 可靠: 采用了碰撞避免机制, 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; 节点模块之间具有自动动态组网的功能, 信息在整个 ZigBee 网络中通过自动路由的方式进行传输, 从而保证了信息传输的可靠性。
- 时延短: 针对时延敏感的应用做了优化, 通信时延和从休眠状态激活的时延都非常短。通常时延都在 15~30 ms 之间。
- 网络容量大: 可支持高达 65 000 个节点。
- 安全: ZigBee 提供了数据完整性检查和鉴权功能, 加密算法采用通用的 AES - 128。
- 高保密性: 采用 64 位出厂编号, 并支持 AES - 128 加密。
- 数据传输速率低: 只有 10~250 KB/s, 专注于低传输应用。
- 功耗低: 在低功耗待机模式下, 两节普通 5 号干电池可使用 6 个月到 2 年, 免去了充电或者频繁更换电池的麻烦。这也是 ZigBee 的支持者一直引以为自豪的独特优势。
- 成本低: 因为 ZigBee 数据传输速率低, 协议简单, 且 ZigBee 协议免收专利费, 所以大大降低了成本。
- 优良的网络拓扑能力: ZigBee 设备具有无线网络自愈能力, ZigBee 具有星、树和网状网络结构的能力, 因此通过 ZigBee 无线网络拓扑能简单地覆盖广阔范围。
- 有效范围大: 有效覆盖范围为 10~75 m (通过功放可在低功耗条件实现 1 000 m 以上的通信距离), 具体依据实际发射功率的大小和各种不同的应用模式而定, 基本上能够覆盖普通家庭或办公室环境。
- 工作频段灵活: 使用的频段分别为 2.4 GHz (全球)、868 MHz (欧洲) 及 915 MHz (美

国),均为免执照频段。

ZigBee 技术和 RFID 技术在 2004 年就被列为当今世界发展最快,市场前景最广阔的 10 大最新技术中的两个。关于这方面的报道,只需在百度或 GOOGLE 搜索栏中键入“ZigBee”,就会看到大量的有关报道。总之,今后若干年,都将是 ZigBee 技术飞速发展的时期。

尽管,国内不少人已经开始关注 ZigBee 这门新技术,而且也有不少单位开始涉足 ZigBee 技术的开发工作,然而,由于 ZigBee 本身是一种新的系统集成技术,应用软件的开发必须与网络传输、射频技术和底层软硬件控制技术结合在一起,因而深入理解这个来自国外的新技术,再组织一个在这几个方面都有丰富经验的配套队伍,本身就不是一件容易的事情。因此到目前为止,国内除了成都无线龙等几家公司外,有关 ZigBee 开发的公司还是很少。但可喜的是,随着无线龙 ZigBee 各个系列的实用开发系统推向市场(可通过 <http://www.c51rf.com> 查看最新的消息),目前各大高校以及公司相继加入了 ZigBee 的开发行列中。

1.3 ZigBee2007/PRO 特性

ZigBee2007 规范定义了 ZigBee 和 ZigBee PRO 的两个特性集。全新 ZigBee2007 规范构建于 ZigBee2006 之上,不但提供了增强型功能,而且在某些网络条件下还具有向后兼容性。

1.3.1 ZigBee 与 ZigBee PRO 比较

ZigBee 特性集提供了树寻址、AODV 网状路由、单播、广播和群组通信,以及安全等特性。相比之下,ZigBee PRO 用随机寻址取代了树寻址;其虽然包括了 ZigBee2006 和 ZigBee2007 规范中所使用的相同的 AODV 路由,但却提供了多对一源路由备选方案。ZigBee PRO 还增加了有限的广播寻址功能,并增加了对“高级”安全性的支持功能。ZigBee 和 ZigBee PRO 特性集均对可选频率捷变和拆分提供了更多的支持。

ZigBee 的树寻址按照等级分配地址。ZigBee PRO 采用的随机寻址法随机地为设备分配地址,并通过不断监控和达到“管理”流量将冲突挑选出来。ZigBee 不仅受益于可靠、独特的寻址方法,而且不存在经常性的监控通信与处理地址冲突的开销。但 ZigBee PRO 却得益于调整功能,如当通信限制会导致一个由多个(5 个以上)跳频(Hop)组成的网络时,或当一个网络由多个移动终端设备组成时,该优势是以不断增加的启动延迟为代价的。这是因为 ZigBee PRO 必须允许一定的时间用来解决地址冲突问题,而对于树寻址而言则并非必须。

ZigBee 和 ZigBee PRO 路由均使用 Ad Hoc 方式的按需距离矢量(AODV)路由协议,但是只有 ZigBee PRO 可支持多对一源路由选项。在牺牲一个较大协议栈的前提下,多对一源路由实现了快速路由建立,此时多个设备(如传感器)均向一个接收器(Sink)报告(如网关设