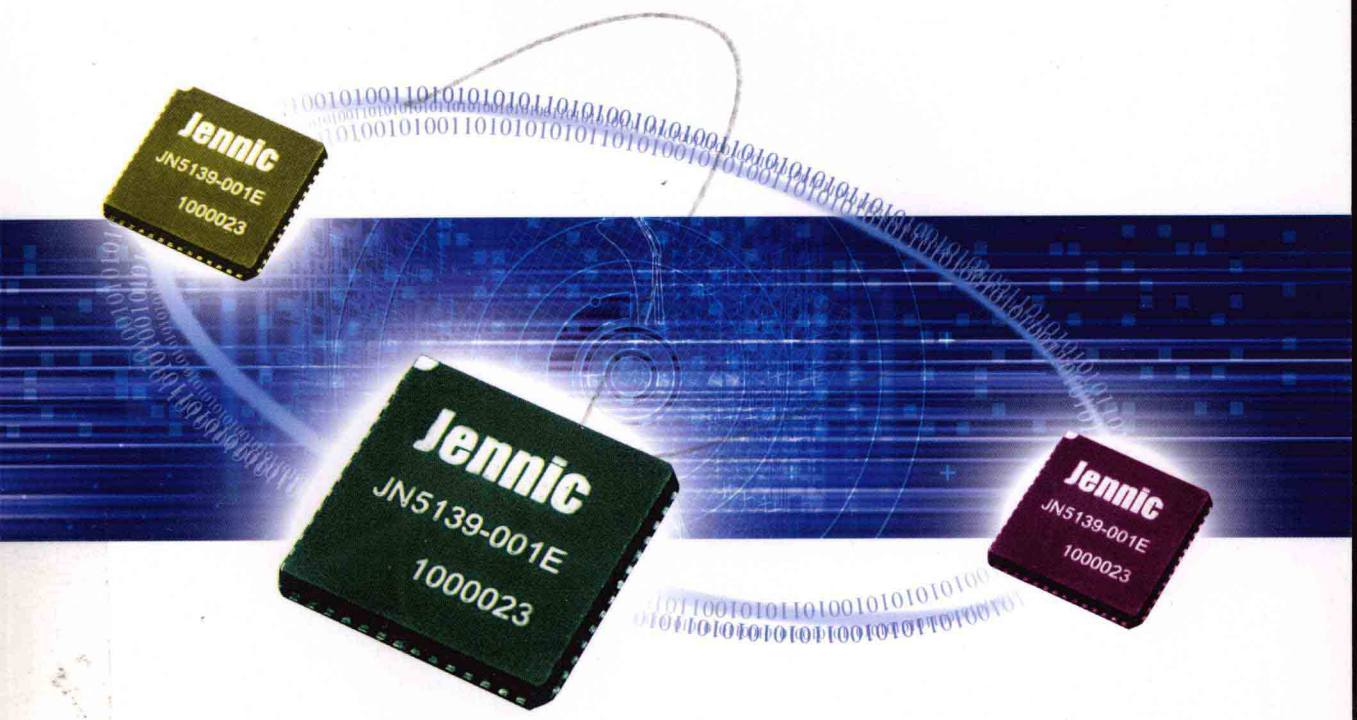
低速无线个域网实验教程

Practice Guide to Low－Rate Wireless Personal Area Network

徐勇军　刘　峰　王春芳　姜　鹏　编著



北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

低速无线个域网实验教程

徐勇军　刘峰　王春芳　姜鹏　编著

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

图书在版编目（CIP）数据

低速无线个域网实验教程/徐勇军等编著. —北京：北京理工大学出版社，2008.6

ISBN 978-7-5640-1451-3

Ⅰ.低…　Ⅱ.徐…　Ⅲ.无线电通信-局部网络-实验-教材

Ⅳ.TN925-33

中国版本图书馆 CIP 数据核字（2008）第 030422 号

出版发行 / 北京理工大学出版社
社　　址 / 北京市海淀区中关村南大街 5 号
邮　　编 / 100081
电　　话 / (010)68914775(办公室)　68944990(批销中心)　68911084（读者服务部）
网　　址 / http：//www.bitpress.com.cn
经　　销 / 全国各地新华书店
印　　刷 / 北京国马印刷厂
开　　本 / 787 毫米×1092 毫米　1/16
印　　张 / 23
字　　数 / 540 千字
版　　次 / 2008 年 6 月第 1 版　2008 年 6 月第 1 次印刷
印　　数 / 1～3000 册　　责任校对 / 陈玉梅
定　　价 / 46.00 元　　责任印制 / 吴皓云

前言

低速无线个域网实验教程

无线个域网（Wireless Personal Area Network，WPAN）是指提供个人及消费类电子设备之间进行互联的无线短距离专用网络，它实现了设备与设备以及人与设备之间的连接与控制。围绕无线个域网这一应用场景，先后出现了红外技术、家用射频技术、蓝牙技术、超宽带技术和ZigBee技术等。近几年，ZigBee技术脱颖而出，成为争相研究的焦点。本书以Jennic公司的JN51xx芯片为基础，以实验的形式介绍ZigBee无线个域网技术。

作为无线个域网的热点技术之一的ZigBee技术随着研究界及产业界的广泛努力，已经取得了长足的进步。特别是随着无线传感器网络技术的发展，越来越多的人开始参与到相关的关键核心技术的研究中，中科院计算所无线传感器网络实验室就是其中之一。中科院计算所在短距离无线通信技术，特别是传感器网络方面的研究已有多年，研究内容涉及传感器网络节点、协议、芯片、测试及开发平台，及其他相关核心技术，目前已发表相关学术论文60余篇，申请国家发明专利20余项，软件著作权登记20余项。关于传感器网络的相关知识，可以参考前期出版的《无线传感器网络技术》和《无线传感器网络实验教程》两本书。

中科院计算所宁波分部（宁波中科集成电路设计中心）无线通信事业部专注于短距离无线通信技术，从事无线个域网及射频识别相关产品的研发工作。设计完成了一款面向无线个域网的低功耗处理器、GAINS、GAINZ、GAINSJ、ForeID及GMesh等多个系列的无线个域网相关产品，开发出多种主动式或被动式RFID应用方案，相关产品还在智能闸口、车辆管理、医疗监护、精准农业、电力线远程监控、远程抄表及智能家居等领域进行了广泛应用。另外宁波中科还是Jennic公司目前在中国内地地区唯一的第三方，在无线个域网领域具有良好的技术积累和发展态势。为了帮助大家及时地了解无线个域网ZigBee的技术原理及开发方法，在Jennic公司的建议及帮助下，特编写了本实验教程。

本实验教程在大量收集客户需求及意见的基础上，考察目前ZigBee技术及无线个域网的众多应用场景，以宁波中科集成电路设计中心自主开发的基于Jennic51xx的ZigBee解决方案GAINSJ开发套件、后台可视化软件iSnamp-J和ZigBee网络分析软件为背景，深入浅出地介绍了ZigBee技术的实验方案，其主要内容包括如下三个部分。

第一部分为基础模块实验，包括中断测试实验、定时器实验、串口测试实验、低功耗休眠实验、数/模转换实验、传感数据采集实验，这些基础实验可以较全面地帮助初学者掌握Jennic无线个域网方案的中断函数的调用、定时器及基本外设的使用和传感数据采集等功能，为后面的通信实验进行必要的准备；第二部分为基础通信实验，包括IEEE 802.15.4协议开发模板实验、Tx Power测试实验、Packet Error Rate测试实验、IEEE 802.15.4无

线 UART、IEEE 802.15.4 无线灯控实验等，这部分实现了 ZigBee 无线个域网的双向通信功能，并且可以完成简单的组网实验；第三部分为高级应用实验，包括办公室个域网组建、智能灯光控制、环境监测、厂房无线门控制、室内无线定位等实验，这部分选用了典型的应用场景，并结合 ZigBee 技术特点精心设计而成，可以给更进一步的应用开发者提供直接的参考。本书全部实验由浅入深、内容详尽、步骤清晰、代码完备，是有志于在 Jennic 的无线个域网 ZigBee 技术方案进行学习者的较好入门材料。

本实验教程的编写是在中科院计算所徐勇军博士的组织下展开的。其主要实验内容是由团队骨干成员刘峰和王春芳在 GAINSJ 硬件平台上开发和编写的，iSnamp-J 可视化后台和 ZigBee 网络分析软件是由博士生安竹林负责组织开发的，张兴国与朱冠男提供了升级与维护。夏鹏为本书全部实验的校验和验证做了大量的工作，产品经理姜鹏收集了大量客户反馈信息，并提出许多建设性的修改意见。感谢 Jennic 公司的首席执行官 Jim Lindop 和市场主管 Tony Lucido 邀请我们成为其第三方，并给予在经济和技术上的大力支持，特别是 William Chen、Phil Lin 和 Belie Song 等，没有他们的鼓励和不知疲倦的交互，本书可能仍然只是公司内部的技术文档，在此对他们一并表示感谢。本书所涉及的代码、软件工具、实验硬件产品介绍等可以网站上免费下载（http：//www. wsn. org. cn/ebook. htm），另外还提供了实验内容相关的答疑与互动论坛（http：//bbs. wpanclub. com），欢迎随时访问。

另外，本书相当多的内容都参考了网友在论坛上发表的观点或网络上的其他公开资源，在此不能逐一列举，对他们的工作致以深切的谢意，当然本书中的任何错误或者不妥之处都与他们无关。需要指出的是，面向无线个域网应用的 ZigBee 技术的研究虽然已经被科研及产业界关注多年，但其中许多技术还不够成熟，特别是应用方面还有待进一步的推广，因此要编写一个全面完善的实验教程非常困难。由于水平有限，书中一定存在疏漏或者错误，希望广大读者不吝赐教。任何建议、意见或者疑问，请及时反馈（wsnbooks@nbicc. com），我们将进行及时的修改和完善。

编者

目 录

低速无线个域网实验教程

第1章　基础知识介绍

在正式进入无线个域网 ZigBee 技术实验之前，本章首先对无线个域网、IEEE 802.15.4，及 ZigBee 相关的背景知识做一个简单的介绍，以便帮助读者更好地理解并完成后面的实验。如果需要了解更详细的知识，可以参考团队前期已经正式出版的另外两本相关书籍：《无线传感器网络技术》和《无线传感器网络实验教程》，它们均是本书的有益补充。

1.1　无线个域网简介

无线个域网（Wireless Personal Area Network，WPAN）[①] 是指提供个人及消费类电子设备之间进行互联的无线短距离专用网络。无线个域网专注于便携式移动设备（如个人计算机、外围设备、PDA、手机、数码产品等消费类电子设备）之间，以及这些设备与人之间的双向通信技术问题，其典型覆盖范围一般在 10 m 以内。IEEE 802.15 工作组就是为完成这一使命而专门设置的，已经完成了一系列相关标准的制定工作。目前与无线个域网相关的技术方案主要包括：红外（IrDA）技术、家用射频（HomeRF）技术、蓝牙（Bluetooth）技术、超宽带（UWB）技术和 ZigBee 技术（通信距离可达到 100 m）等，其共同的特点是短距离、低功耗、低成本、个人专用等。这些无线个域网技术所处的发展阶段及应用水平具有较大的差异，本教程的实验内容主要集中了目前研究及产业界普遍看好，也是目前正在飞速发展的 ZigBee 技术。为了让读者对无线个域网技术有个全面的了解，下面逐一进行简单地介绍。

1. 红外（IrDA）技术是棵常青树

红外技术是一种利用红外线进行点对点通信的技术，是由成立于 1993 年的非盈利性组织红外线数据标准协会 IrDA（Infrared Data Association）负责推进的，该协会致力于建立无线传播连接的国际标准，目前拥有 130 个以上的正式企业会员。红外技术的传输速率已经从最初 FIR 的 4Mb/s 上升为现在 VFIR 的 16Mb/s，接收角度也由最初的 30°扩展到了 120°。由于采用点到点的连接，其数据传输所受的干扰较少。由于产品体积小、成本低、功耗低、免频率申请等优势，红外技术从诞生到现在一直得到较好的应用，可谓无线个域网领域的一

① A Wireless Personal Area Network (WPAN) is a personal, short distance area wireless network for interconnecting devices centered around an individual person's workspace.

棵常青树。经过多年的发展，其硬件与配套的软件技术都已相当成熟，目前全世界有至少5 000万台设备采用IrDA技术，并且仍然以年递增50%的速度在增长。当今有95%的手提电脑都安装了IrDA接口，而遥控设备（电视机、空调、数字产品等）更是普遍采用红外技术。

但是IrDA是一种视距传输技术，核心部件红外线LED也不是十分耐用，更无法完成长时间稳定的网络，这促使红外技术终究不能成为无线个域网的标准。

2. 家用射频（HomeRF）技术昙花一现

家用射频工作组（Home Radio Frequency Working Group，HomeRF WG）成立于1998年3月，是由美国家用射频委员会领导的，首批成员包括Intel、IBM、Compaq、3Com、Philips、Microsoft、Motorola等公司，其主旨是在消费者能够承受的前提下，建设家庭中的互操作性语音和数据网络。家用射频工作组于1998年即制定了共享无线访问协议（Shared Wireless Access Protocol，SWAP），该协议主要针对家庭无线局域网，其数据通信采用简化的IEEE 802.11协议标准，沿用了以太网载波侦听多路访问/冲突检测（CSMA/CD）技术，在进行语音通信时，采用DECT（Digital Enhanced Cordless Telephony）标准，使用时分多址（TDMA）技术。家用射频工作频段是2.4GHz，最初支持数据和音频最大数据的传输速率为2Mb/s，在新的家用射频2.x标准中采用了WBFH（Wide Band Frequency Hopping，宽带调频）技术来增加跳频带宽数据峰值达到10Mb/s，已经能够满足大部分应用。

2000年左右家用射频技术的普及率一度达到45%，但由于技术标准被控制在数十家公司手中，并没有像红外技术一样开放，特别是802.11b标准的出现，从2001年开始，家用射频的普及率骤然降至30%，2003年家用射频工作组更是宣布停止研发和推广，曾经风光无限的家用射频终于退出无线个域网的历史舞台，犹如昙花一现。

3. 蓝牙（Bluetooth）技术昨日之星

1998年5月，就在IEEE 802.15无线个域网工作组成立不久，5家世界著名的IT公司：Ericsson、IBM、Intel、Nokia和Toshiba联合宣布了一项叫做“蓝牙”（Bluetooth）的计划，旨在设计通用的无线空中接口（Radio Air Interface）及其软件的国际标准，使通信和计算机进一步结合，让不同厂家生产的便携式设备具有在没有电线或电缆相互连接的情况下，就能在近距离范围内互通。计划一经公布，就得到了包括Motorola、Lucent、Compaq、Siemens、3Com、TDK，以及Microsoft等大公司在内的近2000家厂商的广泛支持和采纳。1999年7月，蓝牙工作组推出了蓝牙协议1.0版，后来又经历了多次升级与完善。

蓝牙技术也是工作在2.4GHz的ISM（Industrial Scientific and Medical）频段，采用快速跳频和短包技术减少同频干扰，保证物理层传输的可靠性和安全性，具有一定的组网能力，支持64Kb/s的实时语音。蓝牙技术日益普及，市场上的相关产品也在不断增多，但随着超宽带技术、无线局域网及ZigBee技术的出现，特别是其安全性、价格、功耗等方面的问题日益显现，其竞争优势开始下降，技术及市场都开始失去往日风采，已悄然成为昨日之星。

4. 超宽带（UWB）技术初露锋芒

超宽带（Ultra Wide-Band，UWB）技术起源于20世纪50年代末，是一项使用从几赫兹到几兆赫兹的宽带收发电波信号的技术，通过发射极短暂的脉冲信号，并接收和分析反射

回来的脉冲位置，就可以得到检测对象的信息。其特点是发送输出功率非常小，甚至低于普通设备放射的噪声。超宽带技术最初主要在军事技术、雷达探测和定位等应用领域中使用，美国 FCC（联邦通信委员会）于 2002 年 2 月准许该技术进入民用领域。除了低功耗外，超宽带技术的传输速率轻易可达 100Mb/s 以上，其第二代产品可望达到 500Mb/s 以上，仅这一项指标就让其他众多技术望尘莫及。围绕 UWB 的标准之争从一开始就非常激烈，Freescale 的 DS-UWB 和由 TI 倡导的 MBOA 逐步脱颖而出，近几年国内在这方面的研究也非常热门。

由于其功耗低、带宽高、抗干扰能力强，超宽带技术无疑具有梦幻般的发展前景，但超宽带芯片产品却迟迟未曾面市，这无疑留给人们一个大大的遗憾。近年来开始有出现相关产品的报道，不过这项底蕴极深的技术还需要整个产业界的共同推动。目前超宽带技术可谓初露锋芒，相信它是大器晚成、老而弥坚的，必会大有作为。

5. ZigBee 技术众望所归

ZigBee/IEEE 802.15.4 是一种新兴的短距离、低速率、低成本、低功耗的无线网络技术，它采用直接序列扩频（DSSS）技术，工作频率为 868MHz、915MHz 或 2.4GHz 的 ISM 频段。该技术的突出特点是应用简单、电池寿命长、有组网能力、可靠性高以及成本低，主要应用领域包括工业控制、消费性电子设备、汽车自动化、农业自动化和医用设备控制等。ZigBee 联盟（ZigBee Alliance）成立于 2001 年 8 月，最初成员包括 Honeywell、Invensys、MITSUBISHI、Motorola 和 Philips 等，目前拥有超过 200 多个会员。ZigBee 1.0（Revision 7）规格正式于 2004 年 12 月推出，2006 年 12 月，推出了 ZigBee 2006（Revision 13），即 1.1 版，2007 年又推出了 ZigBee 2007 Pro。IEEE 802.15.4 标准是 ZigBee 技术的基础，后面将有专门的章节对它们分别进行介绍。

ZigBee 技术具有功耗低、成本低、网络容量大、时延短、安全可靠、工作频段灵活等诸多优点，是目前被普遍看好的无线个域网解决方案，本教程主要关注 ZigBee 技术实验。

1.2　IEEE 802.15.4 简介

IEEE 802.15.4 标准针对低速无线个域网（Low-Rate Wireless Personal Area Network，LR-WPAN）制定标准。该标准把低能量消耗、低速率传输、低成本作为重点目标，旨在为个人或者家庭范围内不同设备之间低速互联提供统一标准。由于 IEEE 802.15.4 定义的 LR-WPAN 网络的特性和无线传感器网络有很多相似之处，很多研究机构把其作为传感器网络的通信标准。

IEEE 802.15.4 标准定义了物理层和 MAC 子层，符合开放式系统互联模型（OSI），物理层包括射频收发器和底层控制模块，MAC 子层为高层提供了访问物理信道的服务接口。图 1-1 表明了层与层之间的关系。

IEEE 802.15.4 在媒体访问控制（MAC）层方面，主要是沿用无线局域网（WLAN）中 IEEE 802.11 系列标准的带冲突避免的载波侦听多路访问技术（Carrier Sense Multiple Access with Collision Avoidance，CSMA/CA）方式，以提高系统兼容性。所谓的 CSMA/CA 是在传输之前，会先检查信道是否有数据传输，若信道无数据传输，则开始进行数据传输动作；若产生碰撞，则稍后重新再传。这种 MAC 层的设计，不但使多种拓扑结构网络的应用变得简单，还可实现非常有效的功耗管理。

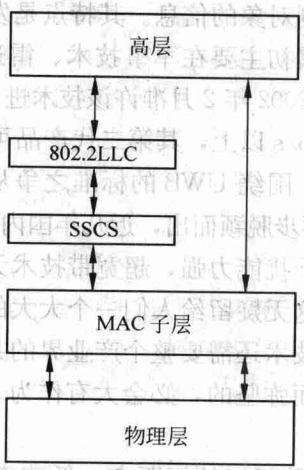


图 1-1 IEEE 802.15.4 协议栈架构

IEEE 802.15.4 在物理（PHY）层设计中面向低成本和更高层次的集成需求，采用的工作频率分为 868MHz、915MHz 和 2.4GHz 三种，各频段可使用的信道分别有 1、10、16 个，各自提供 20Kb/s、40Kb/s 和 250Kb/s 的传输速率，其传输范围介于 10M～100M 之间。由于 ZigBee 使用的 868MHz、915MHz 和 2.4GHz 频段是免费开放的，故已有多种无线通信技术使用，为避免被干扰，故在各个频段皆采用直接序列展频（DSSS）技术，以化整为零的方式将一个信号分为多个信号，再经由编码方式传送信号以避免干扰，这对大部分较低端的实现来说，直接序列展频技术的应用可使模拟电路变得简单，具有更高的容错性能。

在 IEEE 802.15.4 中定义了两种器件：全功能器件（Full-Function Device，FFD）和简化功能器件（Reduced-Function Device，RFD）。对于 FFD，要求它支持所有的 49 个基本参数，而对于 RFD，在最小配置时只要求它支持 38 个基本参数。一个 FFD 可以与 RFD 和其他 FFD 通话，而 RFD 只能与 FFD 通话，仅用于非常简单的应用。但无论如何，一个 IEEE 802.15.4 网络中必定存在一个网络协调器（PAN Coordinator），它是网络的主控制器，负责建立网络、网络成员管理、分组转发等任务。

IEEE 802.15.4 标准支持星型和点对点两种网络拓扑结构，有 16 位和 64 位两种地址格式，其中 64 位地址是全球唯一的扩展地址，支持 CSMA/CA，支持确认（ACK）机制，保证传输的可靠性。

1.3 ZigBee 规范简介

ZigBee 技术是一种近距离、低复杂度、低功耗、低数据速率、低成本的双向无线通信技术或无线网络技术，是一组基于 IEEE 批准的 802.15.4 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，主要适合于承载数据流量较小的业务，可嵌入各种设备中，同时支持地理定位功能。其目标市场是工业、家庭以及医学等需要低功耗、低成本无线通信的应用。与现有的各种无线通信技术相比，ZigBee 技术是最低功耗和最低成本的技术。

目前，市场上的近距离无线通信技术主要有无线局域网 Wi-Fi、蓝牙和一些专用标准。与这些标准相比，如表 1-1 所示，ZigBee 具有数据传输速率低、功耗低、网络容量大、安

全、自动动态组图、自由路由等特点。

表 1-1　ZigBee 技术与现有的各种无线通信技术相比

市场名/标准	GPRS/GSM 1xRTT/CDMA	Wi-Fi/802.11b	Bluetooth/ 802.15.1	ZigBee/802.15.4
应用重点	范围广阔，声音、数据	Web、E-mail、图像	电缆替代品	监测控制
系统资源	16MB+	1MB+	250KB+	4KB～32KB
电池寿命/天	1～7	0.5～5	1～7	100～1 000+
网络容量	1	32	7	255/65 000
带宽/KB·s^{-1}	64～128+	11 000+	720	20～250
传输距离/m	1 000+	1～100	1～10+	1～100+
特点	覆盖面大、质量好	速度快、灵活性大	价格便宜、方便	可靠、低功耗、价格便宜

ZigBee 联盟对网络层协议和 API 进行了标准化。ZigBee 协议栈架构基于 OSI 的 7 层模型，但只定义了与其应用息息相关的几个层，如图 1-2 所示。

图 1-2　ZigBee 协议栈模型

IEEE 802.15.4 标准定义了物理层和 MAC 子层，ZigBee 标准在这个基础之上扩展了网络层（Network layer，NWK）和应用层框架，其中包括应用支持子层（Aplication Support Sub-layer，APS）、ZigBee 设备对象（ZigBee Device Object，ZDO），以及设备商自定义的应用组件。ZigBee 所制定的网络层主要负责网络拓扑的搭建和维护，以及设备寻址、路由等，属于通用的网络层功能范畴，应用层负责业务数据流的汇聚、设备发现、服务发现、安全与鉴权等。

ZigBee 规范确定了三种设备：ZigBee 协调器、ZigBee 路由器和 ZigBee 终端设备。每个网络都必须包括一台 ZigBee 协调器。网络协调器负责为网络的建立和启动网络这一过程设置参数，其中包括选择一个射频信道、唯一的网络标识符，以及一系列操作参数；路由器作为远程设备之间的中继器来进行通信，能够用来拓展网络的范围；终端装置只能选择加入他人已经形成的网络，可以收发信息，但不能转发信息，不具备路由功能。

在组网方式上，ZigBee 主要采用了如图 1-3 所示的三种组网方式。一种为星状网，网络为主从结构，一个网络有一个网络协调者和最多可达 65 535 个从属装置，而网络协调者必须是 FFD，由它来负责管理和维护网络；另一种为树状形网，可以是扩展的单个星状网或

互联的两个星形网络；再有一种为网状网，网络中的每一个 FFD 同时可作为路由器，根据 AD hoc 网络路由协议来优化最短和最可靠的路径。

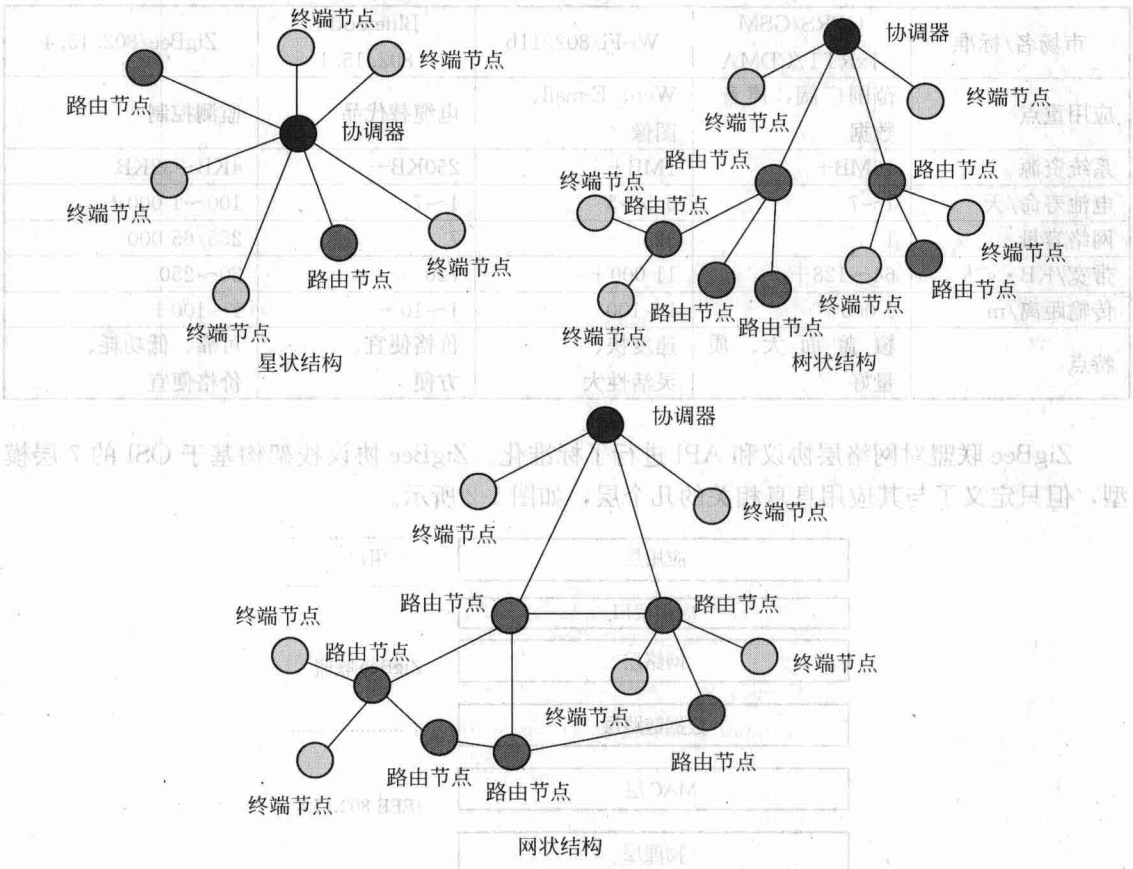


图 1-3 ZigBee 三种不同的组网方式

对于应用层，主要有三个部分，与网络层连接的 APS、ZDO，以及装置应用 Profile。ZigBee 的应用层架构，最重要的是已涵盖了服务（Service）的观念，所谓的服务，简单来看就是功能。对于 ZigBee 装置而言，当加入到一个 WPAN 后，应用层的 ZDO 会发动一系列初始化的动作，先通过 APS 做装置搜寻（Device Discovery）以及服务搜寻（Service Discovery），然后根据事先定义好的描述信息（Description），将与自己相关的装置或是服务记录在 APS 里的绑定表（Binding Table）中，之后，所有服务的使用，都要通过这个绑定表来查询装置的资料或行规。而装置应用 Profile 则是根据不同的产品而设计出不同的描述信息（Description），以及 ZigBee 各层协议的参数设定。在应用层，开发商必须决定是采用公共的应用类，还是开发自己专有的类。ZigBee V1.0 已经为照明应用定义了基本的公共类，并正在制定针对 HVAC、工业传感器和其他传感器的应用类，任何公司都可以设计与支持公共类的产品相兼容的产品。例如，一个采用公共 ZigBee 照明类的荧光灯镇流器供应商可与采用相同类的第三方灯开关调光器实现互操作。开发人员可对该公共类加入他们自己的看法和感觉。ZigBee 设备采用应用对象进行建模，这些应用对象通过交换类对象和它们的属性实现与其他设备的通信。

安全性一直是个人无线网络中极其重要的话题。ZigBee 为其提供了一套基于 128 位高

级加密标准（Advanced Encryption Standard，AES）的安全类和软件，并集成了 IEEE 802.15.4 的安全元素。为了提供灵活性和支持简单器件，IEEE 802.15.4 在数据传输中提供了三级安全性：第一级实际是无安全性方式，对于某种应用，如果安全性并不重要或者上层已经提供了足够的安全保护，器件就可选择这种方式来转移数据；对于第二级安全性，器件可使用接入控制清单（ACL）来防止非法器件获取数据，在这一级不采取加密措施；第三级安全性在数据转移中采用属于 AES 的对称密码，如 ZigBee 的 MAC 层使用了 AES 算法进行加密，并且它基于 AES 算法生成一系列的安全机制，用来保证 MAC 层帧的机密性、一致性和真实性。选择 AES 的原因主要是考虑到在计算能力不强的平台上实现起来较容易，目前大多数的 RF 芯片，都会加入 AES 的硬件加速电路，以加快安全机制的处理。

另外，ZigBee 联盟也负责 ZigBee 产品的互通性测试与认证规格的制定。ZigBee 联盟会定期举办 ZigFest 活动，让发展 ZigBee 产品的厂商有一个公开场合，能够互相测试互通性。而在认证部分，ZigBee 联盟共定义了三种层级的认证：第一级（Level 1）是认证 PHY 与 MAC，与芯片厂有最直接的关系；第二级（Level 2）是认证 ZigBee Stack，所以又称为 ZigBee-compliant Platform Certification；第三级（Level 3）是认证 ZigBee 产品，通过第三级认证的产品才允许贴上 ZigBee 的标志，所以也称为 ZigBee-Logo Certification。

根据 ZigBee 之技术本质，ZigBee 具有下列特性：

①功耗低、时延短、实现简单。装置可以在使用电池的供电情况下，运行数月甚至数年，低功耗意味着较高的可靠性和可维护性，更适合体积小的众多应用；非电池供电的装置同样需要考虑能量的问题，因为功耗还关系着成本等一系列问题。ZigBee 传输速率低，使其传输信息量亦少，所以信号的收发时间短，其次在非工作模式时，ZigBee 处于睡眠模式，这对省电极为有利。另外，在工作与睡眠模式之间的转换时间短，一般睡眠激活时间只有 15 ms，而装置搜索时间为 30 ms。

②可靠度高。ZigBee 的 MAC 层采用 CSMA/CA 机制，此机制无疑能大幅提高系统信息传输的可靠度。

③高度扩充性。每个 ZigBee 网络最多可支持 255 个装置，其中一个是主装置，其余则是从装置。若通过网络协调器，则整体网络最多可达到 65 000 多个 ZigBee 网络节点。ZigBee 通过使用 IEEE 802.15.4 标准的 PHY 和 MAC 层支持几乎任意数目的装置数目，这一点对于大规模传感器阵列和控制尤其重要。

④装置、安装、维护的低成本。对用户来说，低成本意味着较低的装置费用、安装费用和维护费用。ZigBee 装置可以在标准电池供电的条件下（低成本），而不需要任何重换电池或充电操作（低成本、易安装）。ZigBee 在其内部自动可配置和网络装置的冗余等方面的简化更是提供了较低的维护费用。另外电池供电可使装置的体积和面积都得到有效地降低，从而降低一系列与之相关的成本。

⑤协议简单，国际通用。ZigBee 协议栈只有 Bluetooth 或其他 IEEE 802.11 的 1/4 或更小，这种简化对低成本、可交互性和可维护性非常重要。IEEE 802.15.4 的 PHY 层的使用可以支持欧洲的 868MHz 的频段、全球美洲和澳洲的 915MHz 的频段和现在已经被广泛使用的 2.4GHz 的频段，这使得该协议具有强大的生命力。

⑥自配置。802.15.4 在媒体接入控制层中加入了关联和分离功能，以达到支持自配置的目的。自配置不仅能自动建立起一个星状网，而且还允许创建自配置的对等网。在关联过

程中可以实现各种配置，例如，为个域网选择信道和识别符（ID），为器件指配16位短地址，设定电池寿命延长选项等。

从802.15.4到ZigBee不难发现，这些标准的目的就是希望以低价切入产业自动化控制、能源监控、机电控制、照明系统管控、家庭安全和RF遥控等领域。

在ZigBee网络中传输的数据通常分为三类：周期性数据，如传感器中传递的数据，数据速率是根据不同的应用定义的；间断性数据，如控制电灯开关时传输的数据，数据速率是由应用或外部激励定义的；还有反复性的低反应时间的数据，如无线鼠标传输的数据，数据速率是根据分配的时隙定义的。因此，凡是只需传递少量信息，例如，控制（Control）或是事件（Event）的信息传递，都是ZigBee容易发挥作用的战场。

1.4 ZigBee WAPN平台

目前市场上出现了较多的ZigBee解决方案，有代表性的包括Jennic的JN5121/JN5139、Chipcon的CC2430/CC2431及Freescale MC13192、Ember的EM250 ZigBee等系列的开发工具及芯片，表1-2对这些SoC芯片进行比较。

表1-2 几个主流ZigBee解决方案芯片的比较

特征	JN5121	MC131xx	EM250	CC2430
微处理器	16MHz晶振 32位RISC	40MHz晶振 8位MCU	16位MCU	32MHz晶振 8051MCU
存储器	96k RAM, 64k ROM	4k RAM, 60k FLASH	5k RAM, 128k FLASH	8k RAM, 128k FLASH
休眠电流消耗/μA	5	40	1.5	1
接收/发送电流消耗/mA	50/40	43/39	29/33	27/25
外设资源	ADC，DAC， UART，SPI， 12C，Timer， Comparator	ADC，UART， SPI，12C，Timer， Comparator	ADC，UART， SPI，12C， Timer	ADC，UART， Timer

1. Freescale：MC13191、MC13192和MC13193平台

其中MC13191对应低成本应用，通过Freescale提供的软件，用户可以组建简单的星状网络；MC13192可以满足用户组织自己非标准网络的需求，Freescale提供符合IEEE 802.15.4的MAC软件，用户基于此在上面建立自己的复杂网络；而MC13193是ZigBee产品，提供IEEE 802.15.4 MAC软件，再加上ZigBee MAC软件Zstack，用户可以基于此建立起ZigBee网络。

2. Chipcon：CC2430、CC2431平台

Chipcon的CC2430包含一个高性能2.4GHz DSSS（直接序列扩频）射频收发器核心和一颗工业级小巧高效的8051控制器。其中MCU包括存储器及外围，其他模块提供电源管理、时钟分配和测试等重要功能。CC2430的设计结合了8KB的RAM及强大的外围模块，并且有三种不同的版本，它们是根据不同的闪存空间32KB、64KB和128KB来优化复杂度与成本的组合。CC2430的尺寸只有7mm×7mm的48-pin封装，使用具有内嵌闪存的0.18 μm CMOS标准技术。

3. Ember：EM250、EM260 平台

Ember 提供了 EM250 ZigBee 系统晶片及 EM260 网络处理器。两款晶片均嵌入了 Ember 的 EmberZNet——第二代 ZigBee 通信协议，专为使用包括网状、星状及群树形等多种网络形态而设的自动组网及自动重构无线网络，并提供符合 ZigBee 标准的可靠安全、通用性好、低成本、电池寿命长的网络管理。就开发工具而言，Ember 提供 Ember InSight Development Environment。这是 Eclipse-based 的综合开发环境，让开发人员就整个网络为应用做开发及调试。

4. Jennic：JN5121、JN5139 平台

Jennic 是一家将无线连接革新技术带入新应用中的半导体设计公司。提供了 802.15.4 及 ZigBee 标准的高度整合的低成本硅片解决方案，该公司的产品包括一流的低功耗无线微控制器、收发器及低成本开发平台，其总部位于英国 Sheffield，过去几年来，该公司拥有面向无线应用的成功硅片开发的骄人记录。

Jennic 的 JN5121 是业界第一款兼容于 IEEE 802.15.4 的低功耗，低成本 SoC 芯片。最新推出的高功率版本的模块传输距离更可以达到空前的 1 km 以上，而功耗只有 100mW。Jennic 新推出的 JN5139 更是整合了 192KB 的只读存储器和高达 96KB 的随机存储器。在本教材中以 JN5121/JN5139 作为硬件基础。

GAINSJ 是宁波中科集成电路设计中心有限公司设计开发的基于 JN5121/JN5139 的无线传感网络实验平台，工作在 2.4GHz 频段上。GAINSJ 开发板在保证原产性能的基础上，采用串行接口直接调试和烧写程序，给开发者带来了很大的便捷。另外 40 针的外括 I/O 接口，将主芯片上的主要接口全部引出，用户可以在节点上扩展各种传感器子板。板载的温湿度传感器，用于监测节点所处环境状况，节点上提供的按键和 LED 灯可以用于程序调试和节点状态指示。

GAINSJ 套件提供了资源丰富的软硬件开发平台，以及针对 GAINSJ 节点的无线个域网可视化软件。套件还提供了基于 C 语言的开发环境、调试器和 FLASH 编程器、网络分析工具。完善的硬件、软件及技术支持使得用户可以将该套件广泛地应用于工业、科研和教学等领域。实验平台的详细介绍请参见本书第 2 章。

第 2 章　实验开发平台

本教程实验都是基于 GAINSJ 硬件平台的，GAINSJ 节点采用了 Jennic 公司的 ZigBee 解决方案。Jennic 是一家领导无线通信进入新纪元的 IC 设计公司，提供了无线个域网单芯片解决方案。Jennic 的专业在于世界级 RF、数字化芯片及结合系统和软件设计领域，并将焦点集中在 IEEE 802.15.4 和 ZigBee 标准上，以专门技术提供了无线通信市场一项低成本、高集成度的无线射频 SoC 解决方案。公司产品包括最新型的低功率射频 SoC 芯片、模块、开发平台、通信协议及应用软件，为客服提供了一站式 ZigBee 解决方案，如图 2-1 所示。

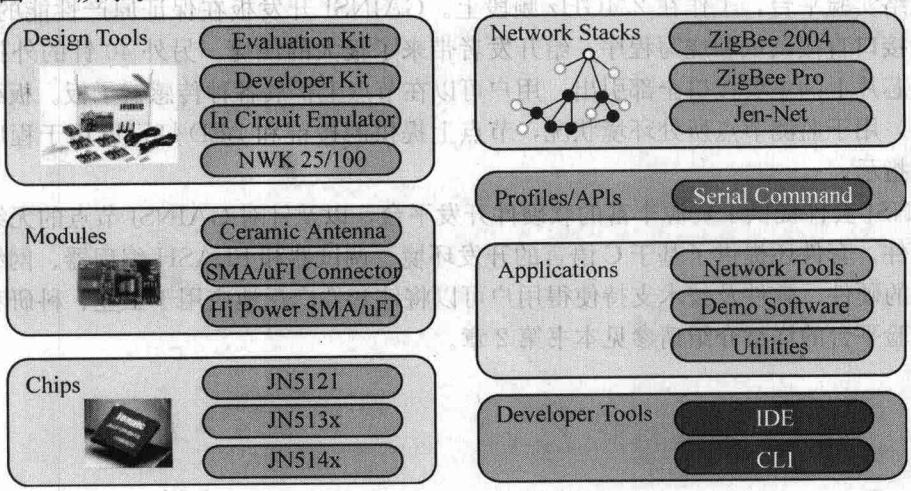


图 2-1　Jennic 公司一站式 ZigBee 解决方案

Jennic 公司 JN5121 微控制器是市场上最早大量销售的全集成、单芯片 ZigBee 解决方案。JN513x 是继 JN5121 后又一颗高性能的全集成单芯片 ZigBee 解决方案，除了达到新的价格门槛外，此系列产品不论在微控制器性能的表现、成本及功率消耗等都优于现有的 JN5121 系列。除了芯片的推出外，一系列基于 JN513x 的模块、开发工具、软件及通信协议软件也同时供应上市。Jennic 公司的产品发展远景如图 2-2 所示。