ZigBee

技术基础及案例分析

金纯 罗祖秋 罗凤 陈前斌 编著

国防工业出版社
National Defense Industry Press

ZigBee 技术基础及案例分析

金 纯 罗祖秋 罗 凤 陈前斌 编著

国防工业出版社

内 容 简 介

本书介绍了ZigBee技术，对其网络体系结构、规范等做了深入浅出的介绍，并对其应用案例做了具体的分析。

本书共分为八章。第一章为ZigBee概述，介绍了ZigBee联盟及网络体系结构中各层的总体概况。第二章介绍了ZigBee物理层规范。第三章介绍了MAC层规范。第四章介绍了网络层规范。第五章介绍了应用层规范。第六章介绍了安全服务规范。第七章分析了短距离无线通信技术，并把它们与ZigBee技术的性能作了比较。第八章对ZigBee应用案例进行分析。全书整体内容由金纯博士进行策划和统编，罗祖秋执笔本书第二、三章的内容，罗凤执笔第一、四、五、六、七、八章的内容，陈前斌博士对本书进行了修改及校对。同时本书还得到了李银国教授、林金朝教授的帮助和指导，以及得到研究生蒋小宇、齐岩松、万正兵、陈许、邝杨、杨帆、汤芳剑的大力协作。在此表示衷心的感谢。

本书适合通信相关专业的学生学习和阅读，也可作为希望了解或从事ZigBee和其他无线短距离通信技术的工程技术人员参考。

图书在版编目(CIP)数据

ZigBee技术基础及案例分析/金纯等编著. —北京：国防工业出版社，2008.1
ISBN 978-7-118-05334-0

Ⅰ.Z... Ⅱ.金... Ⅲ.无线电通信-通信网 Ⅳ.TN92

中国版本图书馆CIP数据核字（2007）第128827号

※

国防工业出版社出版发行
（北京市海淀区紫竹院南路23号 邮政编码100044）
国防工业出版社印刷厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 22.25 字数 608千字
2008年1月第1版第1次印刷 印数 1—4000册 定价 42.00元

（本书如有印装错误，我社负责调换）

国防书店：(010)68428422 发行邮购：(010)68414474
发行传真：(010)68411535 发行业务：(010)68472764

前　言

随着21世纪社会经济的迅速发展，人们对能够随时随地提供信息服务的移动计算和宽带无线通信的需求越来越迫切。无处不在的网络终端，以人为本、个性化、智能化的移动计算，以及方便快捷的无线接入和无线互连等新概念和新产品，已逐渐融入人们的工作领域和日常生活。随之而来的便携式终端和与无线通信相关的新技术层出不穷。一方面是受无线频率资源日益稀罕的影响，另一方面是摆脱各种线缆对个人终端束缚的要求，造成短距离无线通信技术的发展突飞猛进，其应用日新月异。ZigBee是其中一种具有代表性的短距离无线通信技术标准。

ZigBee一词来源于蜜蜂群使用的赖以生存和发展的通信方式。蜜蜂通过跳ZigZag形状的舞蹈来传递新发现的食物源的位置、距离与方向等信息。ZigBee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。Zigbee的基础是IEEE 802.15.4，这是IEEE无线个人局域网(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联盟在制定ZigBee标准时，采用了IEEE802.15.4作为其物理层和媒体接入层规范。在其基础之上，ZigBee联盟制定了数据链路层(DLL)、网络层(NWK)和应用编程接口(API)规范，并负责高层应用、测试和市场推广等方面的工作。

ZigBee技术将主要嵌入在消费性电子设备、家庭和建筑物自动化设备、工业控制装置、电脑外设、医用传感器、玩具和游戏机等设备中，支持小范围的基于无线通信的控制和自动化等领域中的应用，同时还支持地理定位功能。ZigBee具有很广阔的应用前景。

本书根据ZigBee 1.0版规范，遵循IEEE 802.15.4和ZigBee规范的层次结构划分，主要内容包括ZigBee的接口描述、对象描述、协议和与ZigBee协议标准相关的算法，包括应用支持子层(APS)、ZigBee设备对象(ZDO)、ZigBee设备剖面(ZDP)、应用框架、网络层(NWK)和ZigBee安全服务规范等。

本书的目的是提供ZigBee协议标准的一个定义性的描述和基础性的阐述。可以供想了解ZigBee标准、ZigBee应用平台和设备的设计者和操作者参考。

由于时间仓促，加之水平有限，书中的不足之处在所难免，敬请读者批评指正。

目　录

第一章　ZigBee 概述

1.1　引　言

随着科学技术的不断发展，通信技术深入到人类生活的各个方面，人们提出了在人自身附近几米范围内通信的需求，这样就出现了个人区域网络（personal area network，简称 PAN）和无线个人区域网络（wireless personal area network，简称 WPAN）的概念。WPAN 网络为近距离范围内的设备建立无线连接，把几米范围内的多个设备通过无线方式连接在一起，使它们可以相互通信甚至接入局域网或互联网。IEEE 802.15 工作组致力于 WPAN 网络的物理层（PHY）和媒体访问层（MAC）的标准化工作，目标是为在个人操作空间（personal operating space，简称 POS）内相互通信的无线通信设备提供统一的通信标准。POS 通常是指用户附近 10m 左右的空间范围，这个范围内用户可以是固定的，也可以是移动的。

在 IEEE 802.15 工作组内有四个任务组（task group，TG），分别制定适合不同应用的标准。这些标准在传输速率、功耗和支持的服务等方面存在差异。

下面是四个任务组各自的主要任务。

（1）任务组 TG1：制定 IEEE 802.15.1 标准，又称蓝牙无线个人区域网络标准。这是一个中等速率、近距离的 WPAN 网络标准，通常用于手机、掌上电脑等手持移动设备的短距离通信。

（2）任务组 TG2：制定 IEEE 802.15.2 标准，主要研究 IEEE 802.15.1 与 IEEE802.11（无线局域网标准，WLAN）的共存问题。

（3）任务组 TG3：制定 IEEE 802.15.3 标准，研究高传输速率无线个人区域网络标准。该标准主要考虑无线个人区域网络在多媒体方面的应用，追求更高的传输速率与服务品质。

（4）任务组 TG4：制定 IEEE 802.15.4 标准，针对低速无线个人区域网络（low - rate wireless personal area network，简称 LR - WPAN）制定标准。该标准以低能量消耗、低速率传输、低成本作为重点目标，为家庭范围内不同设备之间的低速无线互连提供统一标准。

1.2　ZigBee 联盟的由来

2000 年 12 月 IEEE 成立了 IEEE802.15.4 工作组。这个工作组将致力于定义一种提供廉价的固定、便携或移动设备使用的极低复杂度、低成本、低功耗、低速率的无线连接技术。ZigBee 正是这种技术的商业化命名。这个名字来源于蜂群使用的赖以生存和发展的通信方式，蜜蜂通过跳 ZigZag 形状的舞蹈来分享新发现的食物源的位置、距离和方向等信息。

在标准化方面，IEEE802.15.4 工作组主要负责制定物理层和 MAC 层的协议，其余协议主要参照和采用现有的标准，高层应用、测试和市场推广等方面的工作将由 ZigBee 联盟负责。ZigBee 联盟成立于 2002 年 8 月，由英国 Invensys 公司、日本三菱电气公司、美国摩托罗拉公司以及荷兰飞利浦半导体公司组成，如今已吸引了上百家芯片公司、无线设备公司和开发商的加入。ZigBee 联盟负责制定网络层及以上层协议。同时，IEEE802.15.4 标准也引起了其他标准化组织的注意力，比如 IEEE1451 工作组正在考虑在 IEEE802.15.4 标准基础上实现无线传感器网络（sensor networks）。

1.3 ZigBee 技术概述

ZigBee 栈体系结构由一组称为层的块儿组成。每个层为上层执行指定一套服务：数据实体提供数据传输服务，管理实体提供所有其他服务。每个服务实体通过一个服务接入点(SAP)为上层提供一个接口，每个 SAP 支持一些服务原语来完成必须的功能。

ZigBee 栈体系结构，是基于标准开放网络互联(OSI)七层协议模型，但是仅仅定义这些层在市场空间里完成相应的功能。IEEE802.15.4－2003 标准定义了较低的两层：物理(PHY)层和媒体接入控制(MAC)子层。ZigBee 联盟通过提供网络(NWK)层和应用层结构，构造这个基础。它包括应用支持子层(APS)，ZigBee 设备对象(ZDO)和制造商定义的应用对象。

IEEE802.15.4－2003 有两个 PHY 层，它操作于两个分离的频率范围：868/915MHz 和 2.4GHz。低频率 PHY 层包括 868MHz 欧洲频段和在美国和澳大利亚等国家使用的 915MHz 频段。高频率 PHY 层实际上是供全世界使用。

IEEE802.15.4－2003 MAC 子层控制使用 CSMA－CA 机制接入到无线信道。它的职责可能也包括传输信标帧，同步和提供可靠传输机制。

ZigBee NWK 层的责任应该包括加入和离开一个网络所用到的机制、应用帧安全机制和它们的目的地路由帧机制。另外，在两个设备中路由的发现和维护被移交到 NWK 层。一跳邻居的发现和储存相关的信息也在 NWK 层里完成。ZigBee 协调器(见“网络拓扑”)的 NWK 层负责建立一个新的网络，在适当时，分配地址到新的相关设备。

ZigBee 应用层包括 APS 应用框架(AF)、ZDO 和制造商定义的应用对象。APS 子层的责任包括维护绑定表，绑定表主要根据设备之间的服务和它们的需求使它们相互匹配，同时在它们之间转发消息。ZDO 负责定义设备在网络中的角色(例如是 ZigBee 协调器或是终端设备)，发现设备和决定它们提供哪种应用服务，发起和/或响应绑定请求，在网络设备之间建立安全关联。ZDO 也负责发现网络上的设备并且决定它们提供哪些应用服务。

ZigBee 网络层(NWK)支持星形、树形和网状网拓扑结构。在星形拓扑结构里，网络由一个单独设备——ZigBee 协调器控制。ZigBee 协调器负责发起和维护网络上的设备和所有的其他设备，如众所周知的直接和 ZigBee 协调器通信的终端设备。在网状网和树形拓扑里，ZigBee 协调器发起网络并负责选择确定的关键网络参数，但是可能通过使用 ZigBee 路由器扩展网络。在树形网络里，路由器使用一个等级寻路策略移动数据和控制通过网络的消息。树形网络可能使用信标定向通信，网状网应允许全对等的通信。网状网中的 ZigBee 路由器不应发出规则的 IEEE 802.15.4－2003 信标。

1.4 LR－WPAN 技术概述

低速率无线个人区域网(LR－WPAN)是一个简单的、低成本的通信网络，它应用于一些功率有限和对网络吞吐量无严格要求的设备之间的无线连接。LR－WPAN 的目标是建立一个易于安装、有可靠的数据传输、通信距离短、成本低、极好的电池寿命这样的一个网络，并且它能保持简单的和灵活的网络协议。

LR－WPAN 具有如下的一些特征：

(1) 传输速率有 250kb/s，40kb/s 和 20kb/s 三种；

(2) 星形或对等网络拓扑结构；

(3) 设备有 16bit 的短地址和 64bit 的扩展地址；

(4) 保证时隙(GTS)的分配;

(5) CSMA - CA 的信道接入;

(6) 为保证可靠性传输的完全应答机制;

(7) 低功率;

(8) 能量检测;

(9) 链路质量标识。

LR - WPAN 中含有两种不同类型的设备:全功能设备(FFD)和简单功能设备(RFD)。FFD 在三种网络模式中可作为整个 PAN 的网络协调器、路由器或网络中的应用设备。FFD 可以和 RFD 或者 FFD 通信,而简单功能设备(RFD)只能和 FFD 通信。RFD 设备在网络中主要是一个应用设备,它们相当简单,比如它们可以作为灯的开关或者红外线传感器,但不能传输大规模的数据,且在某一时刻只能和一个 FFD 相联系。因而,RFD 的存储容量是有限的。

1.5 802.15.4(WPAN)的组成

一个 802.15.4 系统由几个部分组成。最基本部分是设备,设备既可以是 FFD,也可以是 RFD。如果两个和更多的设备在一个个人通信空间(POS)范围内,且在同一信道通信,那么这些设备就组成一个 WPAN。但网络中必须含一个 FFD 设备作为 PAN 协调器。

对于无线多媒体来说,由于传播的动态性和不确定性,一个精确的覆盖区域是不存在的。位置和方向的微小变化,都可能引起信号强度和通信链路质量的急剧改变。不管静态设备或移动设备都可能出现这种结果。

1.6 网络拓扑结构

LR - WPAN 有两种拓扑结构:星形拓扑结构和对等拓扑结构(图 1 - 1)。在星形拓扑结构中,通信是在设备和一个中心协调器(也称为 PAN 协调器)之间进行的。设备可以作为发起设备,也可以是终端设备。PAN 协调器是一个特殊的应用设备,但是它可以作为发起设备、终端设备或作为路由器。PAN 协调器是 PAN 中的控制设备。运行在任何一种拓扑结构中的设备都应当有其独一无二的 64bit 扩展地址,这个地址在 PAN 中用于直接通信,或者当设备同协调器连接以后,用它与 PAN 协调器分配给它的短地址进行交换。PAN 协调器可由交流电供电,而设备由电池供电。星形拓扑网络结构主要用于家庭自动化、PC 外围、玩具、游戏设备和个人卫生保健设备。

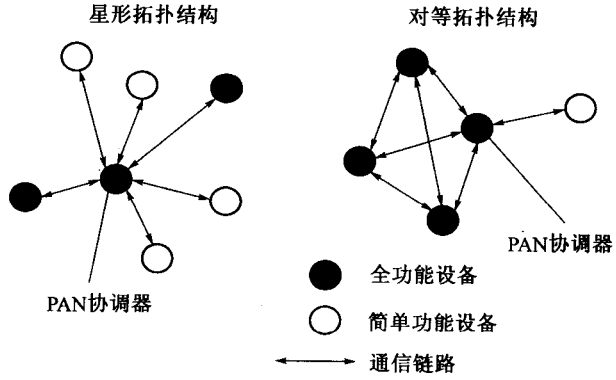

图 1 - 1 星形网络的基本结构

端到端的对等拓扑结构同样需要一个 PAN 协调器，然而，它同星形拓扑网络结构的不同地方是：网络中的任何设备只要在其他设备的通信范围内，它们之间就可以直接进行通信，而不必通过协调器中转。对等网络拓扑结构可以用很复杂的组网形式实现，例如，网状网（mesh network）拓扑。对等网络拓扑结构主要应用于：工业控制与监测、无线传感器网络、智能农业等。一个对等网络是一个自组织、自愈合的网络。在网络中任何设备发送的消息经过多跳路由以后可以到达任何其他设备。

网络的形成

1. 星形网络的形成

星形网络的基本结构如图 1－1 所示。当 FFD 被激活后，它就建立一个自己的网络，并作为 PAN 协调器。所有的星形网络和其他的星形网络各自独立运行。通过选择一个 PAN 标识符可实现其唯一性，即在某个网络的覆盖范围内，这个标识符不能被其他网络所使用。当选定 PAN 标识符以后，PAN 协调器就可以允许其他设备加入该网络当中，这些设备包括 FFD 和 RFD。

2. 对等网络的形成

在对等网络中，一个设备在其射频覆盖范围内可与其他任何设备通信。簇形树状网络（Cluster－tree）是对等网络的一个典型拓扑结构。在 Cluster－tree 网络中大部分设备是 FFD，由于 RFD 在某个时间只能和一个 FFD 连接，因而它只能作为边缘设备连接到 Cluster－tree 网络的树枝上。任何 FFD 都可作为协调器，以便为其他设备和协调器提供同步信息。但在这些协调器中只有一个能成为 PAN 协调器。在网络中相对于其他设备，PAN 协调器具有更强的计算能力。通过把自己作为簇头（簇的标识符为 0），选择一个没有使用的 PAN 标识符，广播信标帧给邻近的其他设备，PAN 协调器就组成一个簇。一个设备接受到信标帧后，可请求在簇头处加入网络。如果 PAN 协调器允许此设备加入，它就把该设备作为子设备添加到它的邻居表中。而这个新加入的设备把簇头作为父设备添加到它自己的邻居表中，并开始发送周期性信标，其他的设备可以通过这个新加入的设备加入到网络当中。如果设备最初不能在簇头处加入到网络中，它就会搜寻其他的父设备以便加入网络。最简单的 cluster－tree 网络是单簇网络，许多相邻的簇可以结合在一起形成一个更大的网络。

一旦需要实现组网，PAN 协调器就会指定一个设备作为其相邻簇的簇头，与其他设备逐渐连接形成一个多簇的网络结构（图 1－2）。图中的线代表父设备和子设备之间的关系，而并不代表通信链路。多簇结构增大了网络的覆盖区域，但同时也增加了通信的时延。

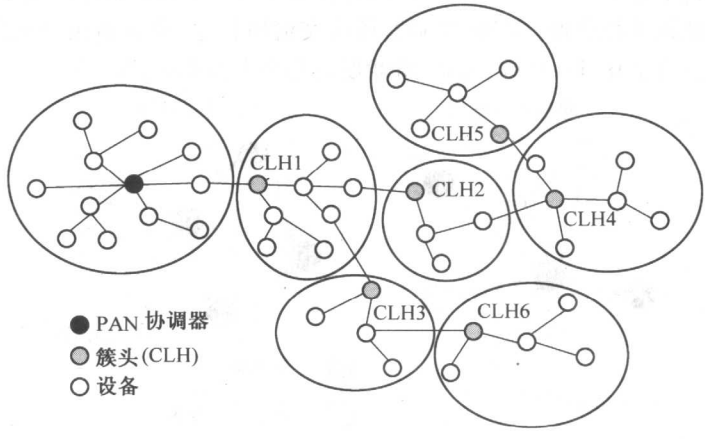

图 1－2　多簇网络结构

1.7 体系结构

一个 LR－WPAN 设备包含一个物理层和一个 MAC 子层(图 1－3),物理层包含 RF 收发器和它的低电平控制机制;MAC 层解决了物理信道的接入方式。图中的高层由网络层和应用层组成。网络层提供网络配置、操作和消息路由。应用层提供设备想要完成的功能。IEEE802.2 类型逻辑链路控制(LLC)能通过服务协议汇聚层(SSCS)接入 MAC 子层。LR_WPAN 体系结构可以作为嵌入设备或者作为支持外围设备的请求设备实现,如作为一个 PC。

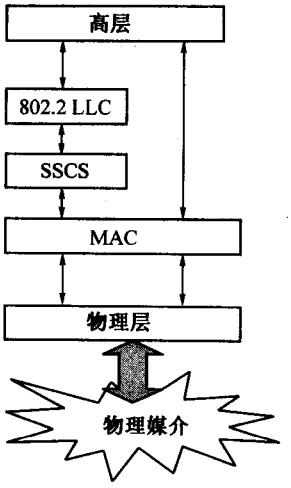

图 1－3 LR－WPAN 的体系结构

1.7.1 物理层

物理层(PHY)提供了两种服务:物理层数据服务和物理层管理服务。物理层数据服务能通过无线信道发送和接收物理层协议数据单元(PPDU)。物理层的特性是激活和关闭无线收发器、能量检测、链路质量指示、空闲信道评估、通过物理媒介接收和发送分组数据。物理层运行在三个不同的频段:868MHz～868.6MHz(欧洲),902MHz～928MHz(北美),2400MHz～2483.5MHz(全球)。

1.7.2 MAC 层

MAC 层提供了两种服务:MAC 层数据服务和 MAC 层管理服务。MAC 层数据服务通过物理层数据服务发送和接收 MAC 层协议数据单元(MPDU)。MAC 的功能是进行信标管理、信道接入、保证时隙(GTS)管理、帧确认、应答帧传送、连接和断开连接。此外,MAC 层为实现适当的安全机制应用提供一些方法。

1.8 功能概述

LR－WPAN 的一般功能包括超帧结构、数据传输模式、帧结构、鲁棒性、功耗和安全性。

1.8.1 超帧结构

LR－WPAN 标准允许选用超帧结构。超帧格式由协调器定义。超帧由协调器发送并受网络信标的限制(图 1－4),而且它还被分为 16 个大小相同的时隙。超帧的第一个时隙用来传输信标帧。

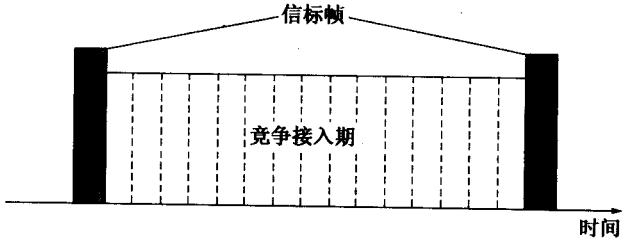

图 1－4 没有 GTS 的超帧结构

如果协调器不希望使用超帧结构，它就不发送信标。信标在网络中用于设备之间的同步、区分 PAN 和描述超帧结构。任何设备想要在两个信标之间的竞争接入期（CAP）内进行通信，就必须同其他设备采用时隙免冲突载波检测多路接入 CSMA－CA 机制进行竞争，所有的处理必须在下一个网络信标的到达之前完成。超帧有活动和不活动部分。在不活动部分，协调器与 PAN 之间不能发生联系，并进入低功耗模式。

对于应用于低延迟或需要在特定数据带宽的情况下，PAN 协调器可以用活动超帧的一部分来实现，这些部分称为保证时隙（GTS），保证时隙形成了非竞争期（CFP），它始终出现在 CAP 之后和活动超帧之前（图 1－5）。PAN 协调器可分配七个 GTS，而每个 GTS 时间不少于一个时隙。然而 CAP 的有效部分应当保留，使基于竞争的其他网络设备和新设备能接入网络。所有基于竞争的传输应当在 CFP 开始之前完成，同时每个工作在 GTS 时期的设备应当确保它的传输在下一个 GTS 开始和 CFP 的结束之前完成。

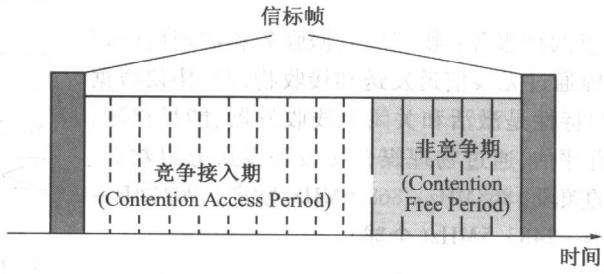

图 1－5　带 GTS 的超帧结构

1.8.2　数据传输模式

在 Zigbee 技术中存在三种数据传输模式：第一种是数据从设备传输到协调器；第二种是数据从协调器传输到设备；第三种是数据传输在两个对等设备之间。在星形网络中，只有第一种和第二种这两种数据传输模式，因为数据交换只能在协调器和设备之间进行；而在对等网络中，由于设备之间可以交换数据，所以它有三种数据传输模式。

网络是否支持信标传输决定了其传输类型，使用信标的网络用于低延迟设备的传输，比如 PC 外围等。如果网络不支持那样的设备，它就选择不用信标来进行正常的传输，然而，在网络之间的连接中信标是必不可少的。

1. 向协调器传输数据

在使用信标的网络中，当设备希望传输数据到协调器时，它首先监听网络信标。在监听到信标以后，设备将与超帧结构保持同步。在适当的时候，设备使用时隙 CSMA－CA 机制向协调器发送数据帧。协调器成功接收后，可发送一个可选应答帧予以应答，最后完成整个过程，如图 1－6 所示。

当设备在非信标的网络中传输数据时，它采用非时隙 CSMA－CA 接入机制向协调器传输数据。协调器成功接收后，可发送一个可选应答帧予以应答，整个过程完成如图 1－7 所示。

2. 协调器传输数据

在使用信标的网络中，当协调器需要向其他设备传输数据时，网络信标就表明有待发送的数据。设备周期性监听网络信标，当有消息发送时，设备就使用时隙 CSMA－CA 传输 MAC 子层请求命令。协调器通过发送可选应答帧予以应答，表示已接受 MAC 子层请求命令。接着，协调器使用时隙 CSMA－CA 接入机制发送数据帧。设备成功接收后，通过发送应答帧予以确认，整个过程完成如图 1－8 所示。