IEEE 802无线通信新技术丛书

ZigBee WIRELESS SENSOR NETWORKS

ZigBee无线传感器网络

钟永锋　刘永俊　编著

北京邮电大学出版社
www.buptpress.com

IEEE 802 无线通信新技术丛

ZigBee 无线传感器网络

钟永锋　刘永俊　编著

北京邮电大学出版社
·北京·

内 容 简 介

本书是基于ZigBee技术的无线传感器网络的一本入门级参考书，ZigBee技术是非赢利性组织ZigBee联盟开发的一套无线传感器网络协议和应用规范，本书在行文中力争与ZigBee联盟的官方规范保持一致，并以架构设计者的角度全面系统介绍了无线传感器网络的物理层/MAC层规范(IEEE 802.15.4)、ZigBee网络层协议、应用层协议，以及与技术实现密切相关网关、安全和应用子集等规范。

图书在版编目(CIP)数据

ZigBee无线传感器网络/钟永锋，刘永俊编著．--北京：北京邮电大学出版社，2011.3
ISBN 978-7-5635-1935-4

Ⅰ.①Z… Ⅱ.①钟…②刘… Ⅲ.①无线电通信－通信网 Ⅳ.①TN92

中国版本图书馆CIP数据核字(2010)第228780号

书　　名：ZigBee无线传感器网络
编 著 者：钟永锋　刘永俊
责任编辑：孔　玥
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路10号(邮编：100876)
发 行 部：电话：62282185　传真：62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京源海印刷有限责任公司
开　　本：787 mm×960 mm　1/16
印　　张：16.25
字　　数：356千字
印　　数：1—3 000册
版　　次：2011年3月第1版　2011年3月第1次印刷

ISBN 978-7-5635-1935-4　　定　价：32.00元

总　　序

纵观当今无线移动通信技术迅猛发展的趋势，人们会注意到，近年来无线移动通信技术的发展实际上是沿着两条主线进行的。一条是以话音业务为主开始的，从 2G、3G 及 B3G 向宽带移动数据通信发展的电信业务技术主线；另一条是以计算机数据通信网络为主开始的，从无线个域网、无线局域网及城域网向下一代网络 NGN 发展的 IT 业务技术主线（可以说是以 IEEE 802 的无线网络技术标准为主要代表的路线）。前者主要面向高速移动的用户，所采用的技术比较复杂，成本较高；而后者原来主要是面对以计算机或笔记本电脑为主，并不需要高速移动的用户，所采用的技术多为免申请牌照的、低成本的无线通信技术，在性价比方面具有一定优势，因而受到人们的普遍关注。

IEEE 802 无线网络标准工作组自 IEEE 802.11 无线局域网标准发布以来，后来又有 Bluetooth（IEEE 802.15.1）、ZigBee（IEEE 802.15.4）、超宽带（UWB）（IEEE 802.15.3a）、WiMax（IEEE 802.16）等新技术的出现，近年来有了很大的发展。从原来的计算机网络的无线延伸与扩展，已经发展成为集无线局域网（WLAN）、无线个域网（WPAN）、无线城域网（WMAN）甚至包括高速宽带移动无线接入（MBWA）在内的，门类齐全的，几乎涵盖无线移动通信各个领域的，世界范围内业界十分关注的一个无线通信网络技术标准化组织。其中仅涉及移动无线接入标准的就有 802.11p、802.16e、802.20 等，而且新的技术好像雨后春笋一样不断涌现。目前，有关无线通信网络技术标准已经成立的并且开展工作的小组有 9 个，即 IEEE 802.11/15/16/17/18/19/20/21/22，其各个工作组的名称及主席如下：

802.11 Wireless Local Area Network (WLAN) Working Group 无线局域网

Chair-Stuart Kerry E-mail: stuart.kerry@philips.com

802.15 Wireless Personal Area Network (WPAN) Working Group 无线个域网
Chair-Bob Heile E-mail: bheile@ieee.org

802.16 Broadband Wireless Access (BBWA) Working Group 宽带无线接入
Chair-Roger Marks E-mail: r.b.marks@ieee.org

802.17 Resilient Packet Ring (RPR) Working Group 弹性分组环
Chair-Mike Takefman E-mail: tak@cisco.com

802.18 Radio Regulatory Technical Advisory Group 无线频率规划技术咨询
Chair-Carl Stevenson E-mail: carl.stevenson@ieee.org

802.19 Coexistence Technical Advisory Group 共存技术咨询
Chair-Steve Shellhammer Email: stephen.j.shellhammer@intel.com

802.20 Mobile Wireless Access Working Group 移动无线接入
Chair-Jerry Upton E-mail: Jerrylupton@aol.com

802.21 Media Independent Handover Working Group 跨媒质越区切换
Chair-Ajay Rajkumar E-mail: ajayrajkumar@lucent.com

802.22 Wireless Regional Area Networks (WRAN) Working Group 无线区域网
Chair-Carl R. Stevenson E-mail: carl.stevenson@ieee.org

以蓝牙及 IEEE 802.11 无线局域网、UWB 等为代表的无牌照移动接入技术的发展突飞猛进，其他相应无线新技术的发展也是不断涌现，令人耳目一新。我们仅以无线个域网的发展为例，即从 IEEE 802.15 WPAN 系列的短距离无线通信新技术的发展就可以明显看出这种发展的新趋势：

IEEE 802.15.1 兼容蓝牙(Bluetooth)技术标准；
IEEE 802.15.2 WLAN 与 WPAN 共存的技术；
IEEE 802.15.3 高速无线个域网技术；
IEEE 802.15.3a 物理层为超宽带的高速无线个域网技术；
IEEE 802.15.3c 物理层为毫米波的高速无线个域网技术；
IEEE 802.15.4 低速无线个域网兼容 ZigBee 的技术；
IEEE 802.15.4a 物理层为超宽带的低速无线个域网技术；
IEEE 802.15.4b 低速家用无线网络技术；

IEEE 802.15.5 网状网 WPAN 无线通信技术等。

由于新技术层出不穷，市场需求发展空间巨大，所以 IEEE 802 标准工作组会议的规模越来越大。参加会议的成员除了来自计算机网络行业以外，近年来一些知名的电信企业及研究机构和运营商，也都非常积极地投入人力、物力开展研究，提出各种提案参与各种标准的制定与投票竞争。我国的一些企业和研究机构也已经参与其中的标准制定工作，但是，无论是参加会议的人数、涉及的领域，还是投入的力量都非常有限。如此情况对未来我国无线通信事业的发展、科研水平的提高、增强企业的竞争力以及参与国际标准制定将会产生负面影响。

另一方面，随着信息社会经济的快速发展，人们对移动通信及宽带无线接入业务的需求不断增长，无线频谱资源也就显得愈加珍贵。因此，如何提高频谱的利用率，一直以来就是无线通信领域研究的主要任务。近年来随着通信技术的发展及市场竞争日益激烈，固定与移动通信业务相互融合、电信与 IT 业务相互融合的发展趋势更加明显。主要出发点就是：有线网络的带宽是无限的；而无线网络的带宽却是有限的，因为可用的无线频谱资源非常有限，随着社会经济的发展，无线频谱资源将更加紧张。移动与固定通信业务相互融合的意义在于充分发挥两种资源的优势，即有线网络带宽宽、资源充足的优势以及无线接入移动性好、使用便利的优势，因此，固定与移动通信业务相互融合已经引起业界的普遍关注。而且，随着 IEEE 802 无线通信网络新技术的迅猛发展，也为移动与固定通信业务的相互融合及无牌照移动接入技术的发展创造了良好的有利条件。UMA (Unlicensed Mobile Access)无牌照移动接入技术也已经成为 3GPP2 相应的接入标准之一。

例如，美国 FCC 为超宽带无线通信技术的民用开放了相应的频段，而且 FCC 在 2005 年 3 月 10 日发布的 No. 05-57 规定中，又确认了一条新的技术手段，即所谓频谱多重应用(Spectrum M ultipurposing)，就是允许采用认知无线电或软件无线电的方式动态分配无线频谱的使用，同时还应保证当需要时，该技术手段必须及时将相应的频率使用权交还给授权频率的所有人。这种频谱的使用方式，有些像计算机的中断程序；而 FCC 也并没有为这种可中断的频谱使用方式专门规定一种特殊的应用模式。FCC 这种做法的目的，就是要最大限度

地提高频谱的利用率。IEEE 802.22 无线区域网技术(又称认知无线电加软件无线电及动态频率规划和管理)就是针对这种需求新成立的工作组。

因此,为了让我国的企事业单位及科研机构的广大工程技术人员,对日新月异发展的无线通信新技术及其国际无线通信标准竞争有更多的了解,并且能够更积极主动地参与到这个无线通信新技术相互竞争而又相互融合的主战场当中来,我们组织国内外的一些通信领域的专家学者,编写了这套无线通信新技术丛书。这套丛书旨在将 IEEE 802 系列的无线通信新技术的基本原理、主要特点、关键技术及其应用介绍给广大读者,并企盼读者从中得到一些启发,以便在工程应用及技术创新中获益。

这套丛书将主要包括以下一些内容:

无线局域网(WLAN)的新技术及其应用;

无线个域网(WPAN)的新技术(例如蓝牙、ZigBee、超宽带等)及其应用;

宽带无线接入,即无线城域网的新技术及其应用;

移动无线接入的新技术及其应用;

无线区域网认知无线电的新技术及其应用;

有关跨媒质越区切换等其他的无线通信新技术及其应用。

人们常以超宽带为例,超宽带无线电以极低频谱功率密度和极宽频谱范围的形式进行通信,开创了以一种衬垫式或地毯式利用无线频谱资源的先河;或者说是开辟了基于次热噪声的形式进行无线通信的新的研究方向。面对超宽带这种新型无线通信技术的出现,人们曾经怀疑、困惑;因为对现有的一些传统观念而言,这的确是一种新的挑战。业内专家曾给出这样一种很形象的比喻:现在就好像是潘多拉魔盒被打开了,放出来的第一个"妖怪"就是超宽带。那么,今后还会放出哪些"妖怪"来,我们将拭目以待。

北京邮电大学教授

周　正

2006 年 5 月

序

我很高兴能为这本优秀的 ZigBee 无线传感器网络的入门新书做个序言。ZigBee 无线技术是新兴的低成本低速率短距离的无线网络技术，并以大大延长的电池寿命为特点作为支撑物联网的领导技术之一。这些标准规范是通过 ZigBee 联盟，一个由全球众多公司在一起工作的组织，所开发出来的；通过联盟每个公司都能基于一个开放的全球标准而提供可靠的、高性价比的无线监控产品。目前这个标准在广泛的应用领域得到了实践，包括消费电子、健康医疗、电信服务和智能电网。本书的目的就是能给读者一个准确的 ZigBee 技术领域的指导。

这本书的特别之处在于它是第一本由亲自参与 ZigBee 标准制定的来自中国的技术专家所撰写的，而且是完全从系统架构者的角度而不仅是产品开发。本书提供了一个 ZigBee 技术的完整视图，从 IEEE 802.15.4 的媒体访问层协议、物理层协议到应用层开发和网关，同时它的内容和章节组织也非常适合学习。另外，所有的名词，表格和图示都是来自原汁原味的 ZigBee 标准规范。

本书给中国读者介绍了 IEEE 802.15.4、ZigBee 技术标准和应用，以及这些不断发展的技术在未来如何满足多样的需求。重要的是，本书的内容非常丰富，完全可以为构建各种规模的 ZigBee 网络提供可实践的架构指导。

简而言之，我向每位有志于了解 ZigBee 技术的中国读者推荐此书，希望它可以帮助您理解 ZigBee 所独有的低功耗、低速率无线组网的特点，并能在物联网中应用这些技术。

Dr. Bob Heile

ZigBee 联盟主席 & IEEE 802.15 标准工作组主席

FOREWORD

I am very pleased to provide a Foreword and recommendation for this excellent new introductory book on ZigBee based wireless sensor networks. ZigBee Wireless Technology is emerging as the leading method for implementing low-cost, low-data rate, short-range wireless networks with extended battery life for use in creating the "Internet of Things". These standards are produced by the ZigBee Alliance which is a global association of companies working together to enable reliable, cost effective, low-power, wirelessly networked, monitoring and control products based on open global standards. These standards are finding applications in a wide variety of things from Consumer Electronics, Healthcare, and Telecom Services to the Smart Grid. This book addresses this need with a concise introduction and tutorial on ZigBee technology.

What makes this book special is the fact that it is the first book written by Chinese authors who were directly involved in the development of the standards. It is written from the point of view of the system architect rather than a product developer. It provides a complete picture of ZigBee wireless networking, from the IEEE 802.15.4 Medium Access Control (MAC) and Radio Frequency (RF) Physical layer (PHY) up to the application layer development and gateways. The book is very well organized and the materials are easy to follow. All the terms, charts and figures in the book are drawn from original ZigBee material.

This book serves as a great introduction for the Chinese audience to IEEE 802.15.4, the ZigBee standards and their applications and how they are evolving to meet the needs of tomorrow. Just as importantly, the content is sufficiently thorough to provide deep understanding of the practical architectural considerations of implementing any size ZigBee wireless network.

In short, I recommend this book to anyone in China who is interested in having a basic understanding of the principals and applications of ZigBee for low-power, low data rate wireless networking and how it may be used in the "Internet of Things"

Dr. Bob Heile
Chairman of the ZigBee Alliance

前　言

2005年初夏当我在奥斯陆第一次参加ZigBee联盟会议的时候，国内的通信技术圈子还在为3G牌照的尽快发放而等待着，不过当时世界上很多国家的3G网络都已经开始商用了，其中就包括华为公司在2004年底为阿联酋建设的中东地区第一个3G网络，这也是华为的第一个3G合同。但很多3G网络运营商都很快发现，尽管3G网络提供了比2G高数十倍的带宽，但实际上的业务发展却乏善可陈，人们最喜欢使用的还是打电话和发短信，手机上网也仅仅是少数人的消费习惯，寻找真正适合3G的新业务是后来摆在技术公司面前的首要问题。

同年国际电信联盟(ITU)发布了一份物联网(Internet of Things)的研究报告，正式开始了物联网领域的深入研究。ZigBee联盟成立于2002年，从最初的几家发起公司到发展至近300家成员单位，该组织为了推广基于IEEE 802.15.4的短距离无线通信技术应用而成立，而到了2004年第一款ZigBee/IEEE 802.15.4芯片的诞生揭开了无线传感器网络快速发展的大幕。学术界讨论了近10年的技术愿景——低功耗短距无线技术、MESH自组织网络等变成了现实。

2010年被称为中国的物联网产业元年，政府和企业对其投入了很大的资源，并希望培育成为继互联网之后的另一大新兴信息产业。一个好消息是中国的3G网络已经商用近2年了，具有良好覆盖的无线回程(backhaul)带宽可以灵活满足很多低速率需求的传感器网络应用部署，把3G和物联网应用结合起来的纽带就是以ZigBee为代表的无线传感器网络，而发展了多年的ZigBee技术也会迎来芯片年出货量过亿的重大发展阶段。本书的初衷正是藉此国内物联网产业发展初期给广大技术研究人员提供一个深入浅出的技术参考，降低基于ZigBee无线传感器网络技术应用开发难度。同时本书的所有引

用的专业定义、原语和协议规范都得到了 ZigBee 联盟的官方授权，为了使读者理解方便，也尽量与英文协议中的定义保持一致。

在本书的撰写过程中得到了我的合作伙伴刘永俊先生的大力协助，他长期参加 ZigBee 联盟成员会议并参与了多个协议的起草和修订工作。同时也感谢北京邮电大学的蒋挺教授、ZigBee 联盟主席 Bob Heile 博士的无私帮助，蒋挺教授为本书主要章节进行了细心审阅，并提供了非常有价值的编辑建议。Bob Heile 博士做为国际传感网技术权威专家为 ZigBee 技术的第一本官方中文辅导书提供了极大的支持。希望该书的出版能帮助国内技术人员深入理解 ZigBee 无线传感器网络技术并加之应用，以后可以反过来向 ZigBee 联盟提供后续演进的技术建议。

本书的出版得到了北京邮电大学出版社的大力支持，在此一并表示感谢。

限于时间和作者水平，书中的不妥之处，在所难免，敬请专家和广大读者批评指正。

编著者

目　录

第1章　无线传感器网络概述

无线通信技术发展到今天，已经成为人们日常生活中不可缺少的沟通和交流手段，从当年简单易用的寻呼机，到如今功能日益强大的手机，都是无线通信技术的代表产品。一方面，随着人们沟通的逐渐扩展和深入，人与人之间的通信已满足不了人们对信息的巨大需求，人们对物理世界的感知需求越来越多，也希望现代通信技术能够架起人类感官与物理世界沟通的桥梁，从而实现机器与机器（Machine-to-Machine）之间和人与机器（Human-to-Machine）之间更为丰富的业务体验。另一方面，随着个人移动通信在以个人为目标市场的渗透率逐渐提高，越来越多的机器设备之间需要自动地进行通信，这种通信通常无须人类的参与，在预先设定好的机制下自动完成，这就是机器到机器通信的来源。为了满足海量的人到机器以及机器到机器的通信需求，传统的移动通信网络已很难独立满足这些新兴应用在成本、功耗、灵活性等方面的要求，做为现代无线通信网络的重要的补充，无线传感器网络也就应运而生了。

无线传感器网络本身是一种特殊的无线通信网络，它采用的无线技术与其他无线通信网络可以说没有本质的区别，也是通过调制编码技术把有用的数字信息通过无线电波（载波）发送出去，接收端通过解调和解码把信息恢复出来。这些物理层技术可以是时分多址（TDMA），也可以是码分多址（CDMA），甚至是正交频分复用（OFDM）。与移动通信系统的最大差别在于传输的信息内容通常是物理世界的一些特征，如温度、压强、速度等，而不是日常手机使用中传输的语音、消息、邮件等。从网络的角度来看无线传感器网络也是一个完备的网络体系，由多个节点组成在一起，不同的节点扮演不同的功能实体。

接下来本章通过对无线传感器网络的体系结构、网络特点、应用等几方面的介绍使读者有一个简单初步的理解。

1.1　无线传感器网络体系结构

无线传感器网络是从通信网络中产生并演化而来的一种特殊形态，其体系结构从逻辑上与现代通信网络的结构一脉相承，而且大部分网络节点也重用了骨干通信网络的设备，或者说它本身也是扩展后的现代通信网络的重要组成部分，如图 1-1 所示。

从自然的分层来看无线传感器网络分为 3 个部分：终端局域网络部分、骨干传输网络部分和业务管理网络部分。

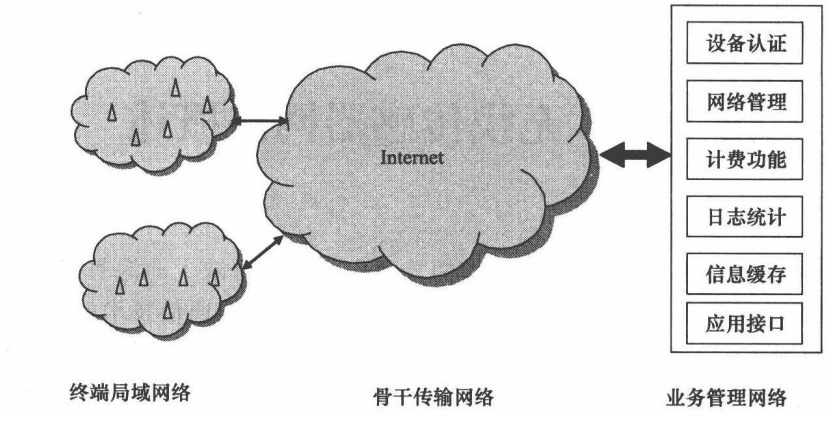

图 1-1　无线传感器网络的基本体系结构

(1)终端局域网络

终端局域网络是无线传感器网络最为重要的组成部分,也是区别于其他通信系统的核心功能。现代通信网络的终端(terminal)是指对等通信协议的终结点,例如人们常见的固定电话、移动通信系统中的手机、计算机网络中的客户端,这些终端背后的使用者就是我们常说的用户。这些传统的终端都是一个完整的设备实体,那么终端局域网络(terminal-side local network)的概念是无线传感器网络对终端概念一个拓展,它的基本定义是多个无线设备通过自组织的形式连接在一起并通过一个或多个网关(gateway)与骨干通信网络相连接。通俗的理解就是从骨干通信网络的角度把一群设备看做一个终端。举个类似的例子就是蓝牙耳机等设备和蓝牙手机之间形成的一个终端局域网络,对于网络而言它只看得见手机终端(做为网关),其他蓝牙设备通过蓝牙连接关联到手机上。

无线传感器网络的终端局域网络主要是由各类传感节点、路由中继节点和网关这几种设备组成,它们之间通过无线通信接口与某种高层通信协议连接在一起共同完成对各种物理信息的采集汇聚的功能,最常见的无线通信接口包括 IEEE 802.11(WiFi)、蓝牙和 IEEE 802.15.4 等,其中 IEEE 802.11 和蓝牙都是比较成熟的技术,但相比而言 IEEE 802.15.4 具有更好的技术优势,本书将在第 2 章介绍该技术标准的一些基本知识。高层通信协议这里指的是网络层及以上的协议,目前以 IEEE 802.15.4 为底层技术的无线传感器网络协议非常多,最为著名的是 ZigBee 联盟开发的 ZigBee 系列协议,本书的第 3 章、第 4 章、第 5 章和第 6 章将详细介绍该协议的工作原理及各子层标准规范。

值得注意的是,许多文献中提及无线传感器网络的狭义解释就是指这个终端局域网络部分。本书中如无特别说明,无线传感器网络是指广义范围的定义,同时包含了骨干传输网络以及业务管理网络。在有的文献和报道中,终端局域网络也被称做无线传感器网络的"感知层",在此不作特别解释说明。

(2)骨干传输网络