



蓝牙4.0BLE开发

完全
手册

物联网开发技术实战

欧阳骏 陈子龙 黄宁淋 编著
栗思科 审校

写作特点

- 理论和实践相结合，夯实理论基础，强化实践环节
- 结构新颖、条理清晰、突出重点、简洁明了
- 立足蓝牙4.0 BLE技术，并提供了部分系统的设计思想与方案

内容特点

- 内容全面。详细阐述了蓝牙4.0 BLE技术的基本概念与理论
- 实用性强。在介绍基础理论的同时，附有详细的实例分析
- 概念清晰，内容翔实，体系合理

适用对象

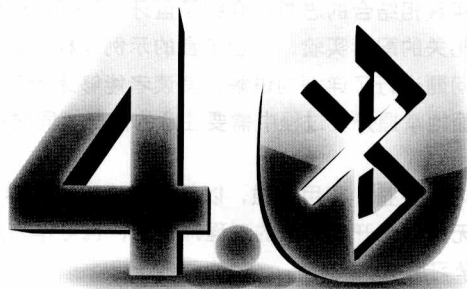
- 从事蓝牙应用开发的技术人员
- 向无线网络开发转型的工程师
- 高等院校电子、通信、自动控制等专业学生



化学工业出版社

013032954

TN929.5-62
05



蓝牙4.0BLE开发

完全
手册

物联网开发技术实战

欧阳骏 陈子龙 黄宁淋 编著
栗思科 审校



北航

C1640724



化学工业出版社

·北京·

TN929.5-62

05

本书采用理论与实践相结合的思想,介绍了蓝牙4.0 BLE技术的基础知识、开发环境以及硬件资源;通过相关的配套实验,结合丰富的示例工程,针对蓝牙4.0 BLE技术开发过程中的重点、难点问题进行了详细的讲解,使读者能够逐步了解蓝牙4.0 BLE无线网络的开发流程并快速全面地掌握开发过程中需要注意的问题,同时给出了部分开发经验和技巧供读者参考。

本书循序渐进、内容完整、实用性强,以教材方式组织内容,可供蓝牙4.0 BLE技术开发的初学者以及向无线网络开发转型的工程师使用,也可作为高等院校电子、通信、自动控制等相关专业的学习用书。

图书在版编目(CIP)数据

蓝牙4.0 BLE开发完全手册——物联网开发技术实战 /
欧阳骏,陈子龙,黄宁淋编著. —北京:化学工业出版社,
2013.4

ISBN 978-7-122-16527-5

I. ①蓝… II. ①欧…②陈…③黄… III. ①无线电
通信-移动通信-通信技术-手册 IV. ①TN929.5-62

中国版本图书馆CIP数据核字(2013)第027682号

责任编辑:李军亮 婁利娜
责任校对:宋 夏

装帧设计:尹琳琳

出版发行:化学工业出版社(北京市东城区青年湖南街13号邮政编码100011)
印 装:大厂聚鑫印刷有限责任公司
710mm×1000mm 1/16 印张17 $\frac{1}{2}$ 字数356千字 2013年5月北京第1版第1次印刷

购书咨询:010-64518888(传真:010-64519686) 售后服务:010-64518899

网 址: <http://www.cip.com.cn>

凡购买本书,如有缺损质量问题,本社销售中心负责调换。

定 价:68.00元

版权所有 违者必究



前言

Foreword

蓝牙无线技术是使用范围最广泛的全球短距离无线标准之一，全新的蓝牙 4.0 版本将三种蓝牙技术（即传统蓝牙、高速蓝牙和低功耗蓝牙技术）合而为一。它继承了蓝牙技术在无线连接上的固有优势，同时增加了高速蓝牙和低功耗蓝牙的特点。这三个规格可以组合使用也可以单独使用。蓝牙 4.0 规范的核心是低功耗技术（Low Energy），即蓝牙 4.0 BLE。该技术最大特点是拥有超低的运行功耗和待机功耗，蓝牙低功耗设备使用一粒纽扣电池可以连续工作数年之久，可应用于对成本和功耗都有严格要求的无线方案，广泛用于医疗保健、体育健身、家庭娱乐、传感器物联网等众多领域。

大多数读者，在学习新知识的时候很难静下心来去阅读大篇幅的概念性的内容，至少笔者当初在学习的时候就是这种心理，总以为那些话是写给明白人看的，因此为了让读者更轻松、更容易地理解蓝牙技术，本书按照如下主线编写：以蓝牙 4.0 BLE 协议栈为基础，结合智造者科技股份有限公司的 CC2540 蓝牙 4.0 BLE 多功能开发系统，通过大量实例分析向读者展示了构建一个符合蓝牙 4.0 BLE 协议的无线网络的总体过程，带领读者从实践的角度去掌握蓝牙 4.0 BLE 无线网络构建和开发的基础知识以及编程技巧。

本书的特点

▲ 理论与实践相结合。本书以实例为基础，详细阐述了进行蓝牙 4.0 BLE 应用开发所需要的基础知识和编程技巧，同时恰当地摒弃了一些对于初学者而言暂时不用或者很少用到的知识点，目的在于突出学习重点。

▲ 讲解简明，步骤详细。每个实例都是以通俗易懂的语言，并穿插图片和表格进行阐述。

▲ 模块化设计与系统设计相结合。

本书的编写原则

▲ 尽量向读者展示技术细节

书中有些地方可能看似很简单，显得有点啰嗦，但是为了给初学者展现出蓝牙 4.0 BLE 无线网络构建的全貌，笔者选择了这种通俗易懂的编写风格，因为笔者在以

往的学习过程中遇到很多问题，到技术论坛发帖求助，查阅资料，经过很长时间才解决问题，因此为了向读者展现一个完整的开发过程，宁可啰嗦一点，也不漏掉细节问题。

▲ 代码注重的是可读性，没有拘泥于效率和编程规范

本书代码力求通俗易懂，并没有过多的考虑程序执行的效率和编程风格。如果读者对基本的编程都没有大概了解的话，又谈何编程规范呢。因此，尽快掌握编程才是硬道理，其他问题可以后续解决。

▲ 尽量用朴实的语言去描述看似深奥的理论

笔者努力使本书作为一本蓝牙 4.0 BLE 无线网络构建和应用开发的实战手册，想展现出开发过程中的问题及其解决方法，尽量给读者提供一个参考，使读者少走弯路，因此，笔者选择用尽量通俗的语言来叙述，并不想用晦涩难懂的语言来迷惑读者。

虽然蓝牙 4.0 BLE 技术涉及电子、通信、射频等多学科的知识，但是，本书将给读者提供了一个崭新的学习思路，即从应用的角度去学习、理解进而掌握蓝牙无线网络构建的基本原理。

本书内容概述

▲ 第 1 章——简要介绍蓝牙 4.0 BLE 技术的基础知识和应用前景，同时给出智造者科技股份有限公司的 CC2540 开发板的硬件组成，这也是本书中采用的硬件平台。

▲ 第 2 章——对 IAR 集成开发环境进行讲解，摒弃部分初学者暂时用不到的功能，突出重点。

▲ 第 3 章——对 CC2540 开发板硬件资源的设计进行讲解，并介绍如何使用仿真调试下载器进行程序的仿真调试和下载。

▲ 第 4 章——给出一系列基础实验，帮助读者快速掌握 CC2540 射频单片机硬件资源的使用。

▲ 第 5 章——深入讲解蓝牙 4.0 BLE 协议栈中各层的机制，同时给出一个在协议栈中使用串口进行通信的实验。

▲ 第 6 章——对蓝牙 4.0 BLE 节点设备和集中器设备编程进行详细阐述。

▲ 第 7 章——结合实例详细阐述 PC 端调试开发工具 BToll 的使用方法。

▲ 第 8 章——讲述如何搭建蓝牙 4.0 BLE 协议分析仪，并结合协议分析仪捕获的数据对蓝牙无线数据传输流程进行分析。

▲ 第 9 章——结合实例，对蓝牙 4.0 BLE 无线网络中常用的项目开发经验进行阐述。

本书是蓝牙 4.0 BLE 应用开发入门级的读物，阅读完本书后，读者需要结合自己的项目需求，对相应的源代码进行修改来完成应用开发，只有通过不断的练习，才能真正

正掌握蓝牙 4.0 BLE 无线网络应用开发的技术。

适用对象

- ☐ 高等院校电子、通信、自动控制等专业学生
- ☐ 从事蓝牙 4.0 BLE 应用开发的技术人员
- ☐ 向无线网络开发转型的工程师

编者与致谢

本书由欧阳骏、陈子龙、黄宁淋编著，栗思科审校，参与本书编写工作的人员还有王小强、张凯之、李岩、王治国、钟晓林、王娟、胡静、杨龙、张成林、方明、王波、雷晓、李军华、陈晓云、方鹏、龙帆、刘亚航、凌云鹏、陈龙、曹淑明、徐伟、杨阳、张宇、刘挺、单琳、吴川、李鹏、朱榕、陈思涛和孙浩，另外还要感谢唐鑫、张剑、陈小军、王博、谢德华、童凯、田野、王丹、严林祥为本书编写所提供的帮助。

配套服务

我们为蓝牙读者和用户尽心服务，围绕蓝牙 4.0 BLE 技术、产品和项目市场，探讨应用与发展，发掘热点与重点；开辟了本书的讨论专区并提供技术支持，俱乐部 QQ: 183090495，电子邮箱: hwhpc@163.com。欢迎读者讨论交流。

由于编者水平有限，加之时间仓促，书中难免有不恰当的地方，恳请广大读者及同行专家批评指正。

编者著



第1章 蓝牙 4.0 BLE 简介

1.1 无线网络数据传输协议对比	2
1.2 短距离无线网络的分类	4
1.2.1 什么是蓝牙 4.0 BLE	4
1.2.2 蓝牙 4.0 BLE 的特点	4
1.3 蓝牙 4.0 BLE 协议简介	6
1.4 蓝牙 4.0 BLE 无线网络通信信道分析	6
1.5 蓝牙 4.0 BLE 无线网络拓扑结构	8
1.6 蓝牙 4.0 BLE 技术在物联网的应用	9
1.7 CC2540 开发板硬件资源概述	11
1.8 本章小结	13
[扩展阅读] 蓝牙技术发展历程	13

第2章 IAR 集成开发环境

2.1 IAR 集成开发环境简介	15
2.2 工程的编辑与修改	16
2.2.1 建立一个新工程	16

2.2.2 建立一个源文件	19
2.2.3 添加源文件到工程	20
2.2.4 工程设置	24
2.2.5 源文件的编译	28
2.3 本章小结	29
[扩展阅读] 模块化编程技巧	29

第3章 CC2540 开发板硬件资源

3.1 CC2540 核心板硬件资源	32
3.1.1 CC2540 简介	32
3.1.2 天线及巴伦匹配电路设计	33
3.1.3 晶振电路设计	33
3.1.4 电源电路设计	34
3.1.5 LED 电路设计	34
3.1.6 AD 转换电路设计	35
3.1.7 串口电路设计	36
3.2 仿真调试与下载	36
3.2.1 仿真调试下载器驱动的安装	36
3.2.2 程序仿真调试	38
3.2.3 结合 SmartRF Flash Programmer 软件 实现程序下载	39
3.2.4 读取 CC2540 蓝牙设备的 IEEE 地址	41
3.3 本章小结	42
[扩展阅读] 天线基础理论	42

❷ 第4章 CC2540 基础实验

4.1 流水灯基础实验	46
4.2 定时器 / 计数器基础实验	49
4.3 定时器 / 计数器高级实验——定时器中断	53
4.4 UART 串口基础实验	57
4.5 UART 串口高级实验	61
4.6 UART 串口编程高级技巧	68
4.7 AD 转换实验之测量 VDD 实验	71
4.8 AD 转换实验之温度采集实验	75
4.9 本章小结	78
[扩展阅读] 可变参数函数的使用技巧	78

❷ 第5章 蓝牙 4.0 BLE 技术入门

5.1 蓝牙 4.0 BLE 协议栈	81
5.1.1 什么是蓝牙 4.0 BLE 协议栈	81
5.1.2 如何使用蓝牙 4.0 BLE 协议栈	82
5.1.3 蓝牙 4.0 BLE 协议栈的安装、编译与下载	82
5.2 深入理解蓝牙 4.0 BLE 协议栈的构成	84
5.2.1 BLE 协议栈基础	84
5.2.2 BLE 协议栈开发平台配置	85
5.2.3 BLE 协议栈执行流程浅析	87
5.3 操作系统抽象层	88
5.3.1 OSAL 常用术语	88
5.3.2 OSAL 运行机理	90

5.3.3	OSAL 消息队列	97
5.3.4	OSAL 添加新任务	98
5.3.5	OSAL 应用编程接口	99
5.4	硬件抽象层	102
5.4.1	硬件抽象层文件目录	102
5.4.2	硬件抽象层驱动编译	104
5.4.3	用户自定义驱动	105
5.5	配置文件层	105
5.5.1	通用访问配置文件 (GAP)	106
5.5.2	通用属性配置文件 (GATT)	108
5.5.3	使用 GAP 和 GATT 的堆栈 API	110
5.6	蓝牙 4.0 BLE 协议栈中串口应用详解	110
5.6.1	串口收发实验	111
5.6.2	实例测试	113
5.6.3	串口工作原理剖析	118
5.7	本章小结	124
[扩展阅读]	OSI 七层模型及协议栈分层思想	124

第 6 章 蓝牙 4.0 BLE 无线网络技术

6.1	蓝牙无线网络节点设备示例工程	128
6.1.1	工程概述	128
6.1.2	初始化	129
6.1.3	周期事件	132
6.1.4	外设状态通知回调	134
6.1.5	按键服务	136
6.1.6	LCD 显示	138

6.2 蓝牙无线网络集中器示例工程	140
6.2.1 工程概述	140
6.2.2 初始化	141
6.2.3 事件处理	143
6.2.4 回调函数	153
6.2.5 服务发现	157
6.3 网络处理器工程简介	167
6.3.1 工程概述	167
6.3.2 BLE 协议栈的外部设备控制	168
6.4 本章小结	168
[扩展阅读] 探究接收数据的存放位置	169

第 7 章 PC 端调试开发工具

7.1 启动 BToll 工具	173
7.2 创建 BToll 与蓝牙节点设备的连接	175
7.2.1 设置节点设备的可发现状态	175
7.2.2 扫描节点设备	177
7.2.3 连接参数设置	178
7.2.4 建立连接	178
7.3 GATT 数据服务	180
7.3.1 通过 UUID 读取特性	180
7.3.2 通过句柄写入特性值	183
7.3.3 通过句柄读取特性值	184
7.3.4 通过 UUID 发现特性	185
7.3.5 通过句柄读取多个特性值	186

7.3.6 特性值通知功能	188
7.4 自定义 GATT 数据服务	191
7.4.1 节点设备编程	191
7.4.2 实例测试	202
7.5 本章小结	207
[扩展阅读] GATT 数据服务的通知与指示	207

第8章 蓝牙 4.0 BLE 无线数据传输分析

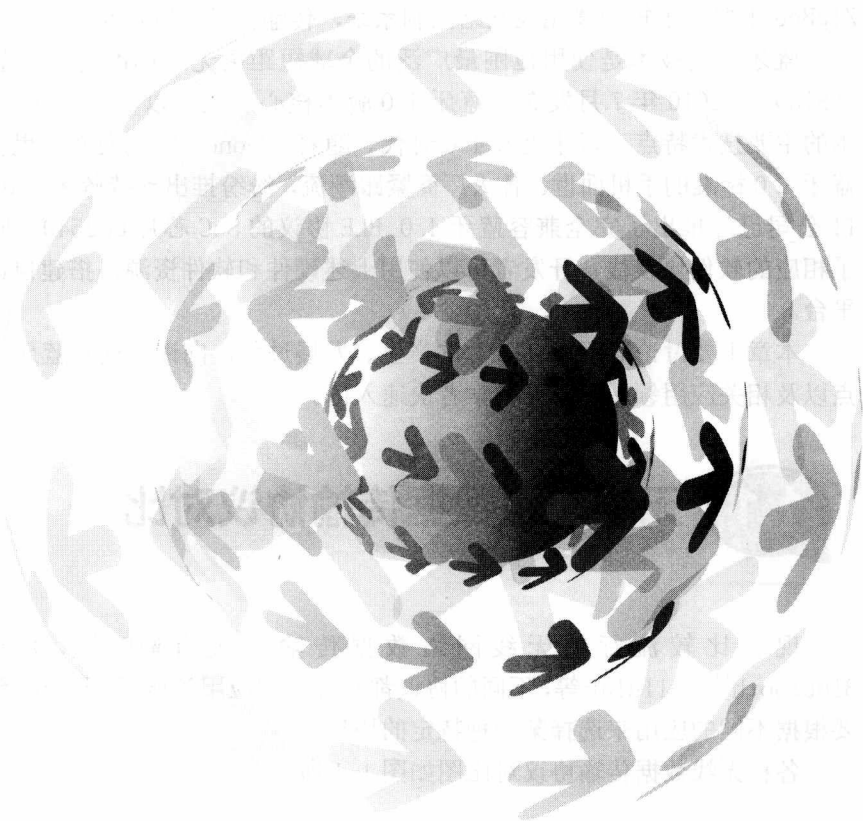
8.1 蓝牙 4.0 BLE 数据包的捕获	210
8.1.1 构建蓝牙 4.0 BLE 协议分析仪	210
8.1.2 蓝牙 4.0 BLE 数据包的结构	212
8.2 蓝牙 4.0 BLE 数据传输实验剖析	213
8.2.1 实验原理及流程图	213
8.2.2 节点设备发送的广告数据	214
8.2.3 节点设备扫描回应的数据	215
8.2.4 蓝牙 4.0 BLE 应用数据传输流程分析	217
8.2.5 数据收发实验回顾	225
8.3 本章小结	226
[扩展阅读] 蓝牙 4.0 BLE 协议栈数据包格式	226

第9章 蓝牙 4.0 BLE 无线网络技术拓展

9.1 BLE 协议栈的中断处理机制	230
9.1.1 中断处理编程	230
9.1.2 实例测试	237
9.2 获取广告设备地址	238

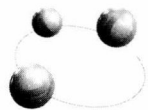
9.2.1	广告设备编程	239
9.2.2	集中器设备编程	244
9.2.3	实例测试	249
9.3	无线温度采集系统设计	250
9.3.1	实验原理及流程图	250
9.3.2	节点设备编程	250
9.3.3	集中器设备编程	254
9.4	蓝牙 4.0 BLE 无线传感器网络组建	256
9.4.1	集中器与多个节点设备建立连接	257
9.4.2	实例测试	263
9.5	本章小结	264
[扩展阅读]	倒 F 天线设计	264

参考文献



第1章

..... 蓝牙 4.0 BLE 简介



近年来,无线网络得到了快速的发展,在此过程中也出现了各种无线网络数据传输标准,诸如WiFi™、Wireless USB、ZigBee,不同的协议标准对应不同的应用领域,例如,WiFi™主要用于大量数据的传输;Wireless USB主要用于视频数据的传输;ZigBee主要用于短距离无线网络控制系统,传输少量控制信息等。

蓝牙无线技术是使用范围最广泛的全球短距离无线标准之一,蓝牙技术联盟(SIG)于2010年7月发布了蓝牙4.0版本核心规范,以低功耗(BLE)作为新版本的主要技术特点,蓝牙迈入4.0时代。随着iPhone 4S的发布,世界上首款支持蓝牙4.0标准的手机面世。各大厂商紧跟潮流,纷纷推出支持蓝牙4.0的智能设备。TI公司已经推出了完全兼容蓝牙4.0 BLE协议的SoC芯片CC2540,同时也开发出了相应的软件协议栈,开发者可以使用上述硬件和软件资源,搭建自己的应用开发平台。

本章主要讨论蓝牙4.0 BLE的产生、发展过程,向读者展示蓝牙4.0 BLE的特点以及相关应用领域,帮助初学者快速入门。

1.1 无线网络数据传输协议对比

现在比较流行的无线网络数据传输协议有WiFi™、Wireless USB、Bluetooth™、Cellular等,不同的协议都有各自的应用领域,因此,选择网络协议时,要根据不同的应用来选择某一种特定的协议。

各种无线数据传输协议对比图如图1-1所示。

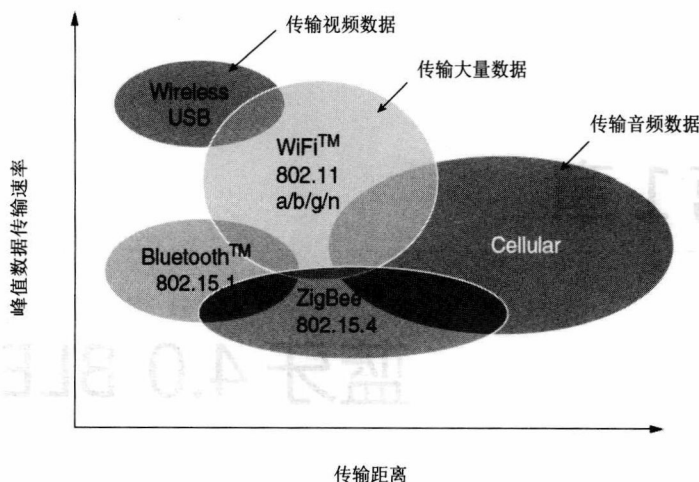


图 1-1 各种无线数据传输协议对比图

从图 1-1 中可以看到不同的无线数据传输协议在数据传输速率和传输距离有各自的使用范围。

传统蓝牙、ZigBee 以及 IEEE 802.11b 标准都是工作在 2.4GHz 频段的无线通信标准，下面将传统蓝牙与 ZigBee、IEEE 802.11b 标准进行简要的比较，帮助读者快速地了解几种无线传输标准的应用领域。

▲ 传统蓝牙数据传输速率小于 3Mbps，典型数据传输距离为 2 ~ 10 m，典型应用是在两台蓝牙设备之间进行小量数据的传输。

▲ IEEE 802.11b 最高数据传输速率可达 11Mbps，典型数据传输距离在 30 ~ 100 m，IEEE 802.11b 技术提供了一种 Internet 的无线接入技术，如很多笔记本电脑可以使用自带的 WiFi 功能实现上网。

▲ ZigBee 协议可以理解为一种短距离无线传感器网络与控制协议，传输速率低，主要用于传输控制信息，数据量相对来说比较小，适用于电池供电的系统。此外，相对于上述两种标准，ZigBee 协议实现成本较低。

传统蓝牙、ZigBee 以及 IEEE 802.11b 标准对比情况如表 1-1、图 1-2 所示。

表 1-1 传统蓝牙、ZigBee 以及 IEEE 802.11b 标准对比

数据传输协议	数据速率	数据传输距离 /m	典型应用领域
传统蓝牙	1-3Mbps	2 ~ 10	无线手持设备、无线鼠标
ZigBee	20-250Kbps	10 ~ 100	无线传感器网络
IEEE 802.11b	1-11Mbps	30 ~ 100	无线 Internet 接入

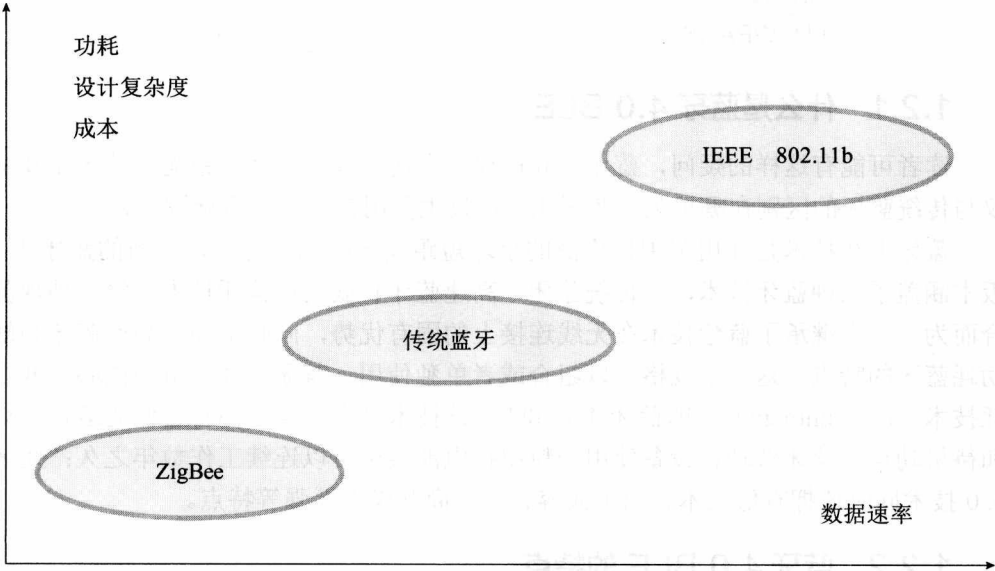
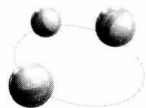


图 1-2 传统蓝牙、ZigBee 以及 IEEE 802.11b 标准对比



1.2 短距离无线网络的分类

短距离无线网络主要分为两类：

- ▲ 无线局域网（WLANs, Wireless Local Area Networks）；
- ▲ 无线个域网（WPANs, Wireless Personal Area Networks）。

无线局域网是有线局域网（LANs, Wired Local Area Networks）的扩展，一个无线局域网设备可以很容易地接入到有线局域网。

无线个域网是为了在 POS（Personal Operating Space）范围内提供一种高效、节能的无线通信方法，其中 POS 是指以无线设备为中心半径 10m（33ft）内的球形区域。

按照数据传输速率的不同，无线个域网又分为三种：

- ▲ HR-WPLANS——High-Rate WPLANS；
- ▲ MR-WPLANS——Medium-Rate WPLANS；
- ▲ LR-WPLANS——Low-Rate WPLANS。

上述三类个域网所对应的协议如表 1-2 所示。

表 1-2 个域网所对应的通信协议

无线个域网	通信协议
HR-WPANS	802.15.3
MR-WPANS	BlueTooth
LR-WPANS	802.15.4

1.2.1 什么是蓝牙 4.0 BLE

读者可能有这样的疑问，蓝牙 4.0 协议与上述协议有什么关系呢，蓝牙 4.0 协议与传统蓝牙的区别在哪里呢，蓝牙 4.0 协议主要用在哪些应用领域呢？

蓝牙无线技术是使用范围最广泛的全球短距离无线标准之一，全新的蓝牙 4.0 版本涵盖了三种蓝牙技术，即传统蓝牙、高速蓝牙和低功耗蓝牙技术，将三种规范合而为一。它继承了蓝牙技术在无线连接上的固有优势，同时增加了高速蓝牙和低功耗蓝牙的特点。这三个规格可以组合或者单独使用。蓝牙 4.0 规范的核心是低功耗技术（Low Energy），即蓝牙 4.0 BLE。该技术最大特点是拥有超低的运行功耗和待机功耗，蓝牙低功耗设备使用一粒纽扣电池甚至可以连续工作数年之久；蓝牙 4.0 技术同时还拥有低成本、向下兼容、跨厂商互操作性强等特点。

1.2.2 蓝牙 4.0 BLE 的特点

总体而言，蓝牙 4.0 BLE 技术具有如下特点。