

现代 *移动* 通信技术丛书

蓝牙协议 及其实现

张禄林 雷春娟 郎晓虹 编著

人民邮电出版社
www.pptph.com.cn

现代移动通信技术丛书

蓝牙协议及其实现

张禄林 雷春娟 郎晓虹 编著

人民邮电出版社

图书在版编目(CIP)数据

蓝牙协议及其实现/张禄林, 雷春娟, 郎晓虹编著. 北京: 人民邮电出版社, 2001.10

(现代移动通信技术丛书)

ISBN 7-115-09518-3

I. 蓝... II. ①张... ②雷... ③郎... I III. 短距离—无线电通信: 数字通信—通信协议
IV. TN915.04

中国版本图书馆 CIP 数据核字(2001)第 052158 号

内 容 提 要

本书围绕最新的蓝牙 1.1 版规范, 集中讨论了蓝牙协议及其开发和实现要点。全书共分三篇, 主要内容包括蓝牙协议、4 种通用剖面 and 9 种蓝牙用户剖面, 并介绍了蓝牙的开发和实现, 包括开发环境的创建、软硬件模块的功能结构、产品的测试和认证过程。

本书适合蓝牙产品的开发人员使用, 也适合希望从总体上了解蓝牙协议和实现的读者阅读使用。

现代移动通信技术丛书

蓝牙协议及其实现

◆ 编 著 张禄林 雷春娟 郎晓虹

责任编辑 孙宇昊

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号

邮编 100061 电子函件 315@pptph.com.cn

网址 <http://www.pptph.com.cn>

北京汉魂图文设计有限公司制作

北京鸿佳印刷厂印刷

新华书店总店北京发行所经销

◆ 开本: 787 × 1092 1/16

印张: 27.25

字数: 658 千字

2001 年 10 月第 1 版

印数: 1 - 5 000 册

2001 年 10 月北京第 1 次印刷

ISBN 7-115-09518-3/TN·1750

定价: 46.00 元

本书如有印装质量问题, 请与本社联系 电话: (010) 67129223

F22.07

前 言

蓝牙的出现是用户需求和通信技术发展的必然。像 PDA 和移动电话一样, 蓝牙产品也用来满足人们对移动性的需求, 但是, 与它们相比, 蓝牙产品更具有划时代的意义。首先在技术上, 它不仅使用成熟、实用和先进的无线技术替代了电缆, 而且以网络的形式把所有的固定和移动设备连接在一起; 其次在应用范围上, 它把无线通信、计算机网络和家电等有机地结合在一起, 实现了前所未有的大融合; 最后在开发策略上, 蓝牙技术的推动者提出了“竞争前合作”的思想, 开放协议, 实现全球统一。自从 1998 年特别兴趣小组 (SIG, Special Interest Group) 成立以来, 在短短 3 年内, 已经有将近 2500 多家公司加入, 其中包括了信息行业和电子行业所有世界知名的厂家, 覆盖了与电子相关的各个行业, 从而蓝牙也成为投资公司的主要目标之一。由于蓝牙在技术和市场上的优势, IEEE 802 标准委员会已经决定把蓝牙发展成为国际标准。

蓝牙的市场是巨大的。能不能掌握蓝牙技术并将其产业化将在很大程度上影响我国信息产业的发展。目前其他国家也都刚刚进入大规模开发阶段, 在这些方面我们与国外先进国家的差距还不是很大。从目前来看, 我们的研发队伍在规模上还不够大, 研发的经验也比较缺乏, 因此加紧培养一批具有相当实力的研发人员是当务之急。写作本书的主要目的就是希望能帮助从事蓝牙开发和研究的人员尽快熟悉蓝牙开发环境, 尽快掌握蓝牙技术。

蓝牙技术是一项非常繁杂的技术, 覆盖面很广, 无线通信技术、计算机网络技术及各种应用环境都与蓝牙有关。随着蓝牙技术的成熟, 今后通信产品、网络产品、计算机及其操作系统中都会运用蓝牙技术。目前从事这些行业的人员也想有一本介绍蓝牙技术应用的图书, 来帮助他们尽快了解蓝牙, 应用蓝牙。本书的蓝牙剖面部分很好地解释了蓝牙产品是如何嵌入到现有的产品中提供服务的。因此, 本书对于那些想了解蓝牙应用, 希望掌握蓝牙技术的人员是非常有用的。

本书在内容上参考最新的蓝牙 1.1 版规范, 遵循了蓝牙规范的层次结构划分。为了增加可读性, 我们没有介绍规范中不必要的重复内容和一些细枝末节, 并对相关的内容进行一些融合和总结。通过本书, 读者会很快地建立起一个有关蓝牙技术的合理的知识结构。

本书分为三篇, 第一篇介绍蓝牙协议, 包括基带协议、链路管理、逻辑链路控制与适配协议和服务发现协议, 以及一些支持传统应用的适配协议, 例如串行仿真协议和电话控制协议; 第二篇介绍蓝牙通用剖面和用户剖面, 包括通用访问剖面、服务发现应用剖面、无绳电话剖面、互联剖面、串行接口剖面、耳机剖面、拨号网络剖面、传真剖面、LAN 接入剖面、通用对象交换剖面、对象推剖面、文件传输剖面和同步剖面。第三篇介绍蓝牙的开发与实现, 包括开发环境的创建、软件和硬件模块的功能结构以及产品的测试和认证过程等。其中, 第一篇由张禄林博士执笔, 第二篇由雷春娟博士执笔, 第三篇由郎晓虹高级工程师执笔。张禄林对全文进行了统稿。

在本书的写作过程中，得到了李承恕教授的帮助和指导，是他把我们带进蓝牙的大门。另外还得到了周彬博士与曹晏波博士的大力协作。在此我们表示衷心的感谢。

由于时间和水平有限，书中错误及不当之处在所难免，还望广大读者不吝指正。

作者

2001年7月于北京

目 录

第一篇 蓝 牙 规 范

第一章 蓝牙概述	2
1.1 蓝牙组织结构	2
1.1.1 蓝牙产生的背景	2
1.1.2 蓝牙 SIG	3
1.2 蓝牙技术特点	3
1.2.1 蓝牙结构	3
1.2.2 蓝牙低层模块	4
1.2.3 软件模块	6
1.2.4 蓝牙应用模型	7
1.3 蓝牙市场前景	7
1.4 蓝牙 SIG 与其他国际组织的关系	8
1.4.1 IEEE 802.15	8
1.4.2 IETF	8
第二章 蓝牙无线部分规范	10
2.1 频段和信道安排	10
2.2 发射器特性	10
2.2.1 调制特点	11
2.2.2 杂散辐射	11
2.3 接收器特性	12
2.3.1 真实灵敏度	13
2.3.2 干扰性能	13
2.3.3 带外截止	13
2.3.4 交调特性	13
2.3.5 最大可用电平	14
2.3.6 杂散辐射	14
2.3.7 接收信号强度指示	14
2.3.8 参考信号定义	14
第三章 蓝牙基带规范	16
3.1 物理信道、链路和分组	17
3.1.1 物理信道	17

3.1.2	物理链路	17
3.1.3	分组	18
3.1.4	纠错	28
3.1.5	逻辑信道	29
3.1.6	数据白化	30
3.1.7	发送和接收例程	30
3.1.8	发送接收定时	34
3.2	信道控制和网络控制	38
3.2.1	概述	38
3.2.2	主从定义	38
3.2.3	蓝牙时钟	38
3.2.4	状态概述	39
3.2.5	STANDBY 状态	39
3.2.6	接入过程	39
3.2.7	查询过程	42
3.2.8	连接状态	45
3.2.9	散射网	47
3.2.10	功率管理	49
3.2.11	链路监控	49
3.3	蓝牙语音规范	50
3.3.1	对数 PCM 编解码	50
3.3.2	CVSD 编解码	50
3.3.3	错误处理	50
3.4	跳频选择和蓝牙地址	50
3.4.1	跳频选择	50
3.4.2	蓝牙地址	52
3.5	蓝牙安全	54
3.5.1	随机数生成	55
3.5.2	密钥管理	55
3.5.3	加密过程	57
3.5.4	鉴权	59
第四章	链路管理器协议	61
4.1	LMP 概述	61
4.1.1	LMP 在协议中的位置	61
4.1.2	LMP 的格式	61
4.2	过程规则和 PDU	62
4.2.1	通用响应消息	62
4.2.2	鉴权	62

4.2.3	PAIRING	63
4.2.4	改变链路密钥	64
4.2.5	改变当前链路密钥	65
4.2.6	加密	66
4.2.7	时钟偏移请求	67
4.2.8	时隙偏移信息	67
4.2.9	定时准确度信息请求	68
4.2.10	LMP 版本	68
4.2.11	所支持的特征	68
4.2.12	主从角色切换	69
4.2.13	设备名称请求	70
4.2.14	断开连接	70
4.2.15	Hold 模式	71
4.2.16	Sniff 模式	72
4.2.17	Park 模式	72
4.2.18	功率控制	74
4.2.19	质量激励下信道在 DH 和 DM 间的转换	74
4.2.20	服务质量 (QoS)	75
4.2.21	SCO 链路	76
4.2.22	多时隙分组的控制	77
4.2.23	寻呼方案	77
4.2.24	链路监视	78
4.3	建立连接	78
4.4	LMP PDU 总结和参数列表	79
4.4.1	LMP PDU 总表	79
4.4.2	LMP PDU 参数	83
4.5	测试模式和错误处理	85
4.5.1	测试模式的激活和关闭	86
4.5.2	测试模式的控制	86
4.5.3	用于测试模式的 PDU 总结	86
4.5.4	错误处理	86
第五章	逻辑链路控制和适配协议规范	88
5.1	L2CAP 概述	88
5.2	常规操作	89
5.2.1	信道标识符	89
5.2.2	设备之间的操作	90
5.2.3	层间操作	90
5.2.4	分割与重组	91

5.3	状态机	92
5.3.1	事件	92
5.3.2	动作	95
5.3.3	信道操作状态	96
5.3.4	事件到动作的映射	97
5.4	数据分组格式	99
5.4.1	面向连接的信道	99
5.4.2	无连接数据信道	99
5.5	信令	100
5.5.1	命令拒绝	102
5.5.2	连接请求	102
5.5.3	连接响应	103
5.5.4	配置请求	104
5.5.5	配置响应	105
5.5.6	断开连接请求	107
5.5.7	断开连接响应	107
5.5.8	回送请求	107
5.5.9	回送响应	108
5.5.10	信息请求	108
5.5.11	信息响应	108
5.6	配置参数选项	109
5.6.1	最大传输单元	109
5.6.2	刷新超时选项	110
5.6.3	服务质量选项	110
5.6.4	配置过程	112
5.7	服务原语	113
5.7.1	事件指示	113
5.7.2	CONNECT	114
5.7.3	连接响应	115
5.7.4	配置	116
5.7.5	配置响应	117
5.7.6	断开连接	118
5.7.7	写	119
5.7.8	读	119
5.7.9	生成组	120
5.7.10	关闭组	120
5.7.11	增加组成员	121
5.7.12	移去一个组成员	121
5.7.13	得到组成员信息	122

5.7.14	PING	122
5.7.15	索取信息	123
5.7.16	关闭无连接业务	123
5.7.17	使能无连接业务	124
第六章	服务发现协议	126
6.1	SDP 概述	126
6.1.1	SDP 客户/服务器交互	126
6.1.2	服务记录	127
6.1.3	服务属性	128
6.1.4	属性 ID	128
6.1.5	属性值	128
6.1.6	服务类	128
6.1.7	搜索业务	129
6.1.8	浏览服务	129
6.2	数据表示	131
6.2.1	数据元素	131
6.2.2	数据元素的类型描述符	131
6.2.3	数据元素大小描述符	132
6.3	协议描述	132
6.3.1	协议数据单元格式	132
6.3.2	部分响应和继续状态	133
6.3.3	错误处理	133
6.3.4	服务搜索交易	133
6.3.5	服务属性交易	134
6.3.6	服务搜索属性交易	134
6.4	服务属性定义	135
6.4.1	通用属性定义	135
6.4.2	服务发现服务器的服务类属性定义	135
6.4.3	浏览组描述符服务类属性定义	136
第七章	适配协议	138
7.1	RFCOMM 协议	138
7.1.1	RFCOMM 协议概述	138
7.1.2	服务接口描述	141
7.1.3	RFCOMM 对 TS.07.10 的支持与修改	142
7.1.4	流控制	147
7.2	电话控制协议	148
7.2.1	电话控制协议概述	148

7.2.2	呼叫控制 (CC)	150
7.2.3	组管理 (GM)	152
7.2.4	无连接 TCS (CL)	154
7.2.5	补充服务 (SS)	154
7.2.6	消息格式	155
7.2.7	消息编码	155
7.2.8	协议参数	166
7.3	IrDA 互操作	166
7.3.1	OBEX 简介	166
7.3.2	OBEX 对象及协议	167
7.3.3	OBEX OVER RFCOMM	169
7.3.4	OBEX OVER TCP/IP	170
第八章	主机控制器接口功能规范	171
8.1	HCI 概述	171
8.1.1	蓝牙软件栈的低层	171
8.1.2	可能的物理总线结构	172
8.1.3	HCI 流控制	173
8.2	HCI 命令和事件	174
8.2.1	HCI 命令概述	174
8.2.2	HCI 专用信息的交换	174
8.2.3	链路控制命令	177
8.2.4	链路策略命令	179
8.2.5	主机控制器和基带命令	180
8.2.6	信息参数	183
8.2.7	状态参数	183
8.2.8	测试命令	183
8.2.9	事件	184
8.2.10	错误代码列表	186
8.3	HCI USB 传输层	187
8.3.1	概述	187
8.3.2	USB 端点要求	187
8.3.3	分类码	190
8.4	HCI RS-232 传输层	190
8.4.1	概述	190
8.4.2	协商协议	191
8.4.3	分组传输协议	193
8.4.4	同步方式	193
8.5	HCI UART	196

8.5.1	概述	196
8.5.2	协议	196
8.5.3	RS-232 设置	197
8.5.4	错误恢复	197

第二篇 蓝牙剖面结构

第九章	蓝牙设备互操作性及剖面概述	200
9.1	蓝牙设备互操作性及剖面涵义	200
9.1.1	设备互操作性	200
9.1.2	蓝牙剖面涵义	200
9.2	蓝牙剖面构成	202
9.2.1	蓝牙剖面及其相互关系	202
9.2.2	蓝牙通用剖面	202
9.2.3	蓝牙应用剖面	203
第十章	蓝牙通用剖面	204
10.1	普通接入剖面	204
10.1.1	简介	204
10.1.2	剖面概述	205
10.1.3	用户接口剖面	206
10.1.4	模式	207
10.1.5	安全性方面	209
10.1.6	空闲模式程序	212
10.1.7	创建程序	217
10.2	服务发现应用剖面	222
10.2.1	简介	222
10.2.2	剖面概述	222
10.2.3	用户接口方面	224
10.2.4	应用层	225
10.2.5	服务发现	226
10.2.6	L2CAP	227
10.2.7	链路管理	230
10.2.8	链路控制	231
10.2.9	定义	233
10.3	串行端口剖面	234
10.3.1	简介	234
10.3.2	剖面概述	234
10.3.3	应用层	235
10.3.4	RFCOMM 互操作性要求	237

10.3.5	L2CAP 互操作性要求	238
10.3.6	SDP 互操作性要求	239
10.3.7	链路管理互操作性要求	239
10.3.8	链路控制互操作性要求	239
10.4	普通对象交换剖面	241
10.4.1	简介	241
10.4.2	剖面概述	242
10.4.3	应用层	243
10.4.4	OBEX 互操作性要求	243
10.4.5	串行端口剖面互操作性要求	249
10.4.6	普通接入剖面互操作性要求	250

第十一章 蓝牙应用剖面

11.1	无绳电话剖面	252
11.1.1	简介	252
11.1.2	剖面概述	252
11.1.3	应用层	255
11.1.4	TCS-BIN 程序	256
11.1.5	业务发现程序	261
11.1.6	L2CAP 程序	263
11.1.7	LMP 程序概述	263
11.1.8	链路控制特征	263
11.1.9	普通接入剖面互操作性要求	266
11.2	内部通信剖面	267
11.2.1	剖面概述	267
11.2.2	应用层	268
11.2.3	TCS 二进制	269
11.2.4	SDP 互操作性要求	271
11.2.5	L2CAP 互操作性要求	272
11.2.6	链路管理的互操作性要求	272
11.2.7	链路控制的互操作性要求	272
11.2.8	普通接入剖面	274
11.3	拨号网络剖面	275
11.3.1	简介	275
11.3.2	剖面概述	276
11.3.3	应用层	277
11.3.4	拨号和控制互操作性要求	278
11.3.5	串行端口剖面互操作性要求	280
11.3.6	普通接入剖面	280

11.4	传真剖面	282
11.4.1	简介	283
11.4.2	剖面概述	283
11.4.3	应用层	284
11.4.4	拨号和控制互操作性要求	285
11.4.5	串行端口剖面	286
11.4.6	普通接入剖面互操作性要求	287
11.5	耳机剖面	288
11.5.1	简介	288
11.5.2	剖面概述	289
11.5.3	应用层	290
11.5.4	耳机控制互操作性要求	290
11.5.5	串行端口剖面互操作性要求	294
11.5.6	普通接入剖面互操作性要求	296
11.6	对象 Push 剖面	297
11.6.1	简介	297
11.6.2	剖面概述	298
11.6.3	用户接口方面	299
11.6.4	应用层	300
11.6.5	OBEX	302
11.6.6	业务发现	304
11.7	文件传输剖面	305
11.7.1	简介	305
11.7.2	剖面概述	306
11.7.3	用户接口方面	307
11.7.4	应用层	309
11.7.5	OBEX	311
11.7.6	业务发现	315
11.8	同步剖面	316
11.8.1	简介	316
11.8.2	剖面概述	317
11.8.3	用户接口方面	318
11.8.4	应用层	320
11.8.5	IrMC 同步要求	321
11.8.6	OBEX	321
11.8.7	业务发现	322
11.9	局域网接入剖面	324
11.9.1	简介	324
11.9.2	剖面概述	325

11.9.3	用户接口方面	327
11.9.4	应用层	328
11.9.5	PPP	329
11.9.6	RFCOMM	330
11.9.7	业务发现	330
11.9.8	L2CAP	331
11.9.9	链路管理	331
11.9.10	链路控制	332
11.9.11	管理实体程序	332

第三篇 蓝 牙 实 现

第十二章	蓝牙开发	336
12.1	蓝牙开发概述	336
12.1.1	蓝牙开发的意义	336
12.1.2	开发前的准备工作	336
12.1.3	蓝牙软件与硬件的独立实现	337
12.2	蓝牙硬件模块开发	338
12.2.1	硬件模块设计的目标和挑战	338
12.2.2	硬件模块的构成	338
12.3	高层协议栈开发	341
12.3.1	高层协议栈的设计要求	341
12.3.2	主要的模块	342
12.3.3	模块及其应用程序接口	344
12.4	蓝牙剖面开发	352
12.4.1	普通接入剖面	352
12.4.2	串行口剖面	353
12.4.3	服务发现应用剖面	353
12.4.4	OBEX 及其接口	354
第十三章	蓝牙认证与测试	356
13.1	蓝牙的认证过程	356
13.2	蓝牙收发器和基带规范测试	357
13.2.1	一般描述	357
13.2.2	测试环境	358
13.2.3	LMP 消息概览	363
13.3	蓝牙的测试控制接口	365
13.3.1	概述	365
13.3.2	一般描述	365
13.3.3	测试配置	368

13.3.4	TCI-L2CAP 规范	368
13.4	测试系统的确认	370
13.4.1	确认的基本过程	371
13.4.2	RF 测试系统的确认	373
第十四章	蓝牙产品介绍	376
14.1	单芯片蓝牙控制器	376
14.1.1	AT76C551	376
14.1.2	Transilica 的 TR0700 单芯片系统	382
14.2	蓝牙协议栈产品	387
14.2.1	东芝蓝牙协议栈	387
14.2.2	BlueStack	389
14.2.3	BTSWS 蓝牙协议栈	390
14.2.4	T-BTS 协议栈	393
14.3	开发系统产品	395
14.3.1	BTW-DK	395
14.3.2	XTNDCCConnect Blue SDK 简介	396
14.3.3	BByK	398
14.3.4	WDS	399
14.4	协议分析仪产品	401
14.4.1	BPA100	401
14.4.2	Merlin 蓝牙协议分析仪	405
14.4.3	WaveCatcher 蓝牙协议分析仪	407
14.4.4	蓝牙协议分析仪性能比较	411
	蓝牙规范缩略语	415
	参考文献	420

第一篇

蓝牙规范