



车载无线通信技术

Vehicle Wireless Communication Technology

金 纯 林金朝 陈前斌 柳 兴 徐洪刚 编著



國防工業出版社
National Defense Industry Press

内 容 简 介

本书介绍当前在无线局域网技术领域内的热点协议——无线存取(WAVE),主要内容包括5部分:第1部分车载环境下无线存取试用标准——资源管理器,其规定了多个远程应用和资源管理间的控制互换流程;第2部分车载环境下无线存取试用标准——应用和管理信息的安全服务,包括无线存取信息安全抵制窃听、电子欺诈和其他袭击方法;第3部分车载环境下无线存取试用标准——网络服务,定义支持该无线连接的网络和传输层中的服务;第4部分车载环境下无线存取试用标准——多信道运行,规定通信协议栈媒介接入控制接口和IEEE802.11p的多信道运行对单信道操作;第5部分车载环境下无线存取试用标准——车载无线接入协议的架构,对无线存取系统和它的组件及其运行进行整体介绍。

本书可用做相关专业研究生的教材,也可用做从事车载无线通信研究的技术人员的工作手册,同时还可作为车载无线通信技术爱好者的读物。

图书在版编目(CIP)数据

车载无线通信技术 / 金纯等编著. —北京:国防工业出版社,2012.4
ISBN 978-7-118-07409-3

I. ①车... II. ①金... III. ①汽车-无线电通信-通信技术 IV. ①U463.67

中国版本图书馆CIP数据核字(2012)第035297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100048)
涿中印刷厂印刷
新华书店经售

*

开本 787×1092 1/16 印张 19¼ 字数 433 千字
2012年4月第1版第1次印刷 印数 1—4000 册 定价 49.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777 发行邮购:(010)88540776
发行传真:(010)88540755 发行业务:(010)88540717

前 言

车载无线通信技术的应用最早可追溯到 20 世纪 80 年代,但时至今日,这一技术才顺应市场对于车载功能的多样化和集成化的需求而全面发展。科学技术日新月异,汽车不再是简单的代步工具,高标准、高质量的生活要求它成为集安全、环保、舒适、娱乐、办公及服务于一体的电子化汽车。

在现今汽车产业时代,车载无线通信技术作为一种将汽车技术、电子技术、计算机技术、无线通信技术紧密结合,整合各种不同的应用系统而产生的一种新型技术,引领了新一轮的行业时尚变革。

本书对车载无线通信技术,多角度、多层次、多结构地进行了剖析与介绍,为所有对该技术有兴趣研究与学习的读者提供了专业指导。

本书是在金纯教授的策划和主持下,由五位作者共同完成的,第 1 部分由金纯教授编写,第 2 部分由林金朝编写,第 3 部分由金纯教授和徐洪刚共同编写,第 4 部分由柳兴编写,第 5 部分由陈前斌编写。另外,重庆邮电大学的何山和罗伟为本书的编写做了许多工作,在此一并表示感谢。

目 录

第1部分 车载环境下无线存取试用标准 ——资源管理器

第1章 概述	1
1.1 范围	1
1.2 目的	2
第2章 结构和通信流摘要	3
2.1 概况	3
2.2 应用软件组件参考	4
2.3 WAVE 的 RMA 数据传送和管理服务	4
2.4 数据结构描述	5
2.4.1 协议数据单元(PDU)	5
2.4.2 服务数据单元(SDU)	5
2.5 操作概要	7
第3章 OBU 资源	10
3.1 概况	10
3.2 内存	10
3.2.1 存储页	11
3.2.2 内存映射页	11
3.2.3 转发页	11
3.3 用户接口(UI)	11
3.3.1 可视化的显式	11
3.3.2 蜂鸣器(声音警告)	12
3.3.3 发音器	12
3.3.4 字符读出器	12
3.3.5 键盘	12
3.3.6 未来的用户接口资源	12
3.4 内存资源的数据格式	12
第4章 RM 命令和响应	14
4.1 概述	14
4.2 命令格式	14
4.2.1 命令标识符域	15

4.2.2	未响应标识位	16
4.2.3	命令处理标识符域	16
4.2.4	命令参数长度域	16
4.2.5	命令参数域	17
4.3	响应格式	17
4.3.1	命令标识符域	17
4.3.2	命令处理标识符域	18
4.3.3	响应状态域	18
4.3.4	响应长度域	19
4.3.5	响应数据域	19
4.4	命令定义	20
4.4.1	读内存页命令	20
4.4.2	写内存页命令	20
4.4.3	插入信息命令	21
4.4.4	设置用户接口命令	22
4.4.5	睡眠处理命令	24
4.4.6	保留内存页命令	25
4.4.7	释放内存页命令	25
4.4.8	保留分区命令	26
4.4.9	释放分区命令	26
第5章	RM 向 RMA 提供的服务	28
5.1	概述	28
5.2	RM - RMA 接口服务元素	28
5.2.1	PDU - RMA APDU	28
5.2.2	SDU - RMA ASDU	29
5.2.3	PDU 和 SDU 命名规则	29
5.3	协议服务	29
5.4	协议管理服务	29
5.4.1	激活请求服务	29
5.4.2	激活响应服务	30
5.4.3	通知指示服务	31
5.4.4	通知确认服务	32
5.4.5	终止会话指示服务	32
5.4.6	终止会话确认服务	33
5.4.7	撤消服务请求	34
5.4.8	撤消响应服务	34
5.5	协议数据转发服务	34
5.5.1	交换请求服务	35
5.5.2	交换响应服务	35

5.5.3 交换确认服务	36
第6章 RM 所使用的服务接口	37
6.1 概述	37
6.2 使用标准命令集不能访问 OBU 的信息	37
6.3 RM 和 RCP 的登记	37
6.4 WME 对 RCP 的通知	37
6.5 RCP 回复给 PST 中的 OBU 信息	38
6.5.1 内存配置域	38
6.5.2 OBU 配置域	39
6.5.3 最大的应用软件数据块域	39
6.6 RM 接收 RPST	40
6.7 自动命令序列处理	40
6.8 进行应用软件会话	40
6.9 终止应用软件会话	41
附录 A ASN.1 编码	42
附录 B 已登记的页和分区	47
附录 C 协议执行一致性声明(PICS)查验表	48
C.1 概述	48
C.2 缩写词和特殊符号	48
C.3 完成 PICS 查验表的指令	48
C.3.1 PICS 查验表的一般结构	48
C.3.2 附加信息	49
C.3.3 例外信息	49
C.3.4 有限制的情形	49
C.4 PICS 查验表——IEEE Std 1609.1	50
C.4.1 执行确认	50
C.4.2 协议摘要	50
C.4.3 顶级结构	50
C.4.4 标准分区	51
附录 D 定义	55
D.1 命令	55
D.2 车载设备(OBE)	55
D.3 页	56
D.4 分区	56
D.5 协议数据单元	56
D.6 路侧设备(RSE)	57
D.7 服务数据单元(SDU)	57
D.8 会话	58
D.9 处理	58

D.10 用户	59
参考文献	60

第2部分 车载环境下无线存取试用标准 ——应用和管理信息的安全服务

第7章 概述	61
7.1 简介	61
7.2 范围	61
7.3 目的	61
7.4 文献组织	62
7.5 文献规范	62
第8章 语言介绍	63
8.1 概述	63
8.2 符号协定	63
8.3 基本字区大小	63
8.4 数字	63
8.5 固定长度向量	64
8.6 可变长度向量	64
8.7 opaque 和 opaqueExtLength 类型	65
8.8 枚举类型	65
8.9 构造类型	66
8.10 case 声明	66
8.11 外部语句	67
8.12 签名	68
8.12.1 签名字段的使用	68
8.12.2 签名字段的编码	68
第9章 安全的信息	70
9.1 概述	70
9.2 安全信息类型	70
9.3 SignedMessage、ToBeSignedMessage 和 MessageFlags 类型	70
9.4 SignedWSM 和 ToBeSignedWSM 类型	72
9.5 PublicKey、PKAlgorithm 和 SymmAlgorithm 类型	72
9.6 ECPublicKey 类型	73
9.7 CertID8 和 CertID10 类型	74
9.8 The ApplicationID 和 FullySpecifiedAppID 类型	74
9.9 Time64 和 Time32 类型	75
9.10 SignerInfo 类型	75

9.11	Signature 类型	76
9.12	ECDSASignature 类型	76
9.13	EncryptedMessage、EncryptedContentInfo 和 RecipientInfo 类型	76
9.14	ECIESNISTp256EncryptedKey 和 AESCCMCiphertext 类型	78
9.15	WAVE Certificate、ToBeSigned WAVECertificate 和 CertSpecificData 类型	78
9.16	WAVECRL、ToBeSignedCRL、CRLType 和 IDAndDate 类型	80
9.17	WAVECertificateRequest 和 WAVECertificateResponse 类型	82
9.18	GeographicRegion 和 RegionType 类型	83
9.18.1	GeographicRegion 类型	83
9.18.2	from_issuer Region 类型	83
9.18.3	CircularRegion 类型	84
9.18.4	RectangularRegion 类型	84
9.18.5	PolygonalRegion 类型	84
9.19	The 2DLocation 和 3DLocationAndConfidence 类型	84
9.20	认证范围	85
9.20.1	CAScope 类型	85
9.20.2	WSASignerScope 类型	86
9.20.3	IdentifiedScope 类型	87
9.20.4	CSRSignerScope 类型	87
9.20.5	OBUIdentifiedScope 类型	88
9.20.6	CRL 发信者认证	88
第 10 章	其他安全消息格式	89
第 11 章	安全消息处理	90
11.1	安全服务请求信息	90
11.2	缓存和存储	90
11.2.1	简介	90
11.2.2	根认证存储区	90
11.2.3	CA 认证缓存	90
11.2.4	消息签名认证缓存	91
11.2.5	近期接收信息的缓存	91
11.2.6	潜在的加密接收者认证存储	91
11.2.7	撤消认证存储区	92
11.2.8	传入片段的信息缓存	92
11.3	签名消息	92
11.3.1	概述	92
11.3.2	传输处理	92
11.3.3	接收处理	93
11.4	处理加密消息	98

11.4.1	概述	98
11.4.2	传输处理	98
11.4.3	接收处理	99
11.5	处理签名和加密消息	100
第 12 章	安全消息的具体应用	101
12.1	WSA 安全	101
12.1.1	概述	101
12.1.2	发送安全的 WSA	101
12.1.3	WSIE 的接收处理	103
12.2	安全 WSM	105
12.2.1	概述	105
12.2.2	已签名的 WSM	106
12.2.3	已加密的 WSM	108
12.3	安全管理	109
12.3.1	概述	109
12.3.2	应用类型鉴定	109
12.3.3	认证撤销列表	109
12.3.4	根认证更新	110
12.4	认证请求	111
12.4.1	概述	111
12.4.2	认证请求产生	111
12.4.3	认证请求接收处理	111
12.4.4	认证请求响应	112
12.5	片段消息	112
12.5.1	Overview 概述	112
12.5.2	片段消息语法	113
12.5.3	传输片段信息	113
12.5.4	接收片段信息	114
附录 E	消息格式	115
附录 F	消息结构	123
F.1	概要	123
F.2	CA 认证	123
F.3	OBU 签名认证	124
F.4	RSU 署名和加密证书	124
F.5	已签名消息	124
F.6	已签名 WSM	126
F.7	已加密消息	126
附录 G	总体叙述	128
G.1	介绍	128

G.2	WAVE 系统	128
G.2.1	系统中的实体	128
G.2.2	WAVE 无线栈	128
G.3	通信安全	129
G.3.1	简介	129
G.3.2	加密服务	130
G.3.3	匿名	132
附录 H	增加安全性考虑	133
H.1	OBU	133
H.1.1	密钥材料	133
H.2	根认证	133
H.3	公共安全车载	133
H.3.1	认证和确认	133
H.3.2	公共安全证书寿命	134
H.4	RSU	134
H.4.1	密钥材料	134
H.4.2	位置	134
H.5	其他考虑	134
H.5.1	随机	134
H.5.2	加密密钥尺寸	134
附录 I	威胁模式	135
I.1	攻击者的分类	135
I.2	基本的安全消息	135
I.3	收费	136
I.4	通用的互联网访问	136
I.5	路边电子商务	137
附录 J	带宽考虑和优化机会	138
J.1	概述	138
J.2	地理范围标识符	138
J.3	应用软件标识符	138
J.4	使用 certificate_Digest 签名者信息类型	138
参考文献		140

第 3 部分 车载环境下无线存取试用标准 ——网络服务

第 13 章	概述	142
13.1	范围	142

13.2	目标	142
13.3	文档组织	142
13.4	文档协定	143
13.5	系统总述	143
13.6	适用性	143
第 14 章	概述	144
14.1	WAVE 系统	144
14.1.1	WAVE 网络服务	145
14.1.2	数据服务	145
14.1.3	管理服务	145
14.1.4	下层	145
14.1.5	上层	146
14.1.6	WAVE 服务安全性	146
14.1.7	外部实体	146
14.2	WAVE 系统属性	146
14.2.1	信道类型	146
14.2.2	通信协议	146
14.2.3	通信服务类型	146
14.2.4	WBSS 设备的角色	147
14.2.5	优先权	147
14.2.6	设备类型	147
14.2.7	信道协调	147
14.3	WAVE 系统操作	147
14.3.1	没有 WBSS 的操作	148
14.3.2	有 WBSS 的操作	148
14.3.3	WAVE 中的地址和标识符	151
14.3.4	请求登记	152
14.4	路边单元上分布式系统的入口	152
14.5	IPv6 相邻缓存	155
14.6	安全考虑	155
第 15 章	数据平面服务	156
15.1	逻辑链路控制 (LLC)	156
15.2	IPv6	156
15.3	用户数据报协议 (UDP)	156
15.4	包含传输控制协议 (TCP) 的选择性协议	156
15.5	WAVE 短消息 (WSM) 协议	156
第 16 章	管理平面服务	158
16.1	请求登记	158
16.1.1	增加登记实体	158

16.1.2	删除登记实体	159
16.2	WBSS 管理	159
16.2.1	建立链接	159
16.2.2	动态 WBSS	164
16.2.3	WBSS 确认	167
16.2.4	WBSS 完成	167
16.2.5	保持 WBSS 请求状态	168
16.3	信道监听的方式	170
16.4	IPv6 结构	170
16.5	接收信道功率指示(RCPI)测试	170
16.6	维护 MIB	171
第 17 章	服务原语	172
17.1	WSMP SAP	173
17.1.1	WSM-WaveShortMessage.request	173
17.1.2	WSM-Wave 短消息显示	174
17.2	WME SAP	175
17.2.1	WME-Application 请求	175
17.2.2	WME-Application 确认	176
17.2.3	WME-Application 指示	176
17.2.4	WME-Application.response	177
17.2.5	WME-Notification.indication	177
17.2.6	WME-ApplicationRegistration.request	178
17.2.7	WME-ApplicationRegistration.confirm	180
17.2.8	WME-Get.request	180
17.2.9	WME-Get.confirm	181
17.2.10	WME-Set.request	181
17.2.11	WME-Set.confirm	182
17.2.12	WME-RCPIREQUEST.request	182
17.2.13	WME-RCPIREQUEST.indication	183
17.3	LSAP	183
17.4	MLME SAP	183
17.5	SAP 参数定义和帧结构	184
17.5.1	SAP 参数定义	184
第 18 章	Over-the-air 帧格式	189
18.1	WAVE 服务广播(WSA)格式	190
18.1.1	WAVE 版本	190
18.1.2	服务器服务表	190
18.1.3	WRA 长度	192
18.1.4	WAVE 路由广播(可选)	193

18.2 WSM 格式	194
18.2.1 WSM 版本	194
18.2.2 安全类型	194
18.2.3 信道数	194
18.2.4 数据速率	194
18.2.5 TxPwr_Level	194
18.2.6 服务器服务标识符	194
18.2.7 WSM 长度	194
18.2.8 WSM 数据	195
18.3 WSM 编码	195
附录 K WME MIB 的 ASN.1 编码	196
附录 L 1609.3 协议执行一致性声明 (PICS) 查验表	209
L 1 执行确认	209
L 2 协议摘要	209
L 3 标准部分	209
参考文献	214

第 4 部分 车载环境下无线存取试用标准 ——多信道操作

第 19 章 概述	215
19.1 范围	215
19.2 目的	215
第 20 章 标准参考	216
第 21 章 总体描述	217
21.1 参考模型	217
21.2 服务概述	217
21.2.1 信道路由	218
21.2.2 用户优先级	218
21.2.3 信道协调	218
21.2.4 MSDU 数据转换	218
第 22 章 帧格式	220
22.1 EtherType 的使用	220
22.2 可靠的 WSA 和 WSIE	220
第 23 章 功能描述	222
23.1 概述	222
23.2 信道路由分配	223
23.2.1 WSMP 数据路由分配	223

23.2.2	IP 数据报的路由	223
23.3	用户优先级	224
23.3.1	控制信道优先级	225
23.3.2	服务信道优先级	225
23.4	信道协调	225
23.5	传输操作	226
23.6	接收操作	227
第 24 章	层管理	228
24.1	管理模型概述	228
24.2	普通初步管理原语	229
24.3	MLME 服务原语	229
24.3.1	WAVE 服务广播	229
24.3.2	WAVE 连接	232
24.3.3	发送配制文件登记	233
24.3.4	发送配制文件删除	235
24.3.5	WSA 更新	236
24.3.6	取消每个信道的传输	237
24.3.7	获得 UTC 时间	238
24.3.8	服务信道休眠状态	239
24.3.9	结束 WAVE	239
第 25 章	信道协调管理	241
25.1	同步	241
25.1.1	公共时基定义	241
25.1.2	公共时基估计	241
25.1.3	定时信息	242
25.1.4	同步偏差	243
25.2	MAC 管理扩展	243
25.2.1	WSA 和 WAVE 通知	243
25.2.2	WSAUPDATE 和 WAVEANNOUNCEMENT	246
25.2.3	WAVEJOIN 和 WAJOIN	246
25.3	持续性服务管理流	247
25.4	非持续性服务管理流	248
25.5	WSA 更新	249
25.6	多重服务器通信	250
25.7	服务信道休眠状态	251
附录 M	信道间隔运行时的竞争窗口	252
附录 N	避免预保护间隔的传输	253
附录 O	IEEE 1609.4 MIB(管理信息库)的 ASN.1ASN 编码	254
附录 P	精确的计时源和计时质量评估	263

附录 Q 1609.4 协议执行一致性声明(PICS)查验表	265
Q.1 PICS 查验表——IEEE Std 1609.4	265
Q.1.1 执行确认	265
Q.1.2 协议摘要	265
Q.1.3 标准部分	265
参考文献	267

第 5 部分 车载环境下无线存取试用标准

——车载无线接入协议的架构

第 26 章 系统概述	268
26.1 WAVE 的概念	268
26.2 系统的组成和连接	268
26.3 协议体系结构	269
26.4 接口	270
26.4.1 内部接口	270
26.4.2 外部接口	270
26.5 信道类型	271
26.6 通信服务	271
26.7 设备角色	271
26.8 优先类型	271
26.9 信道协调	272
26.10 服务启动	272
第 27 章 相关标准	274
27.1 智能交通系统概述	274
27.2 WAVE 标准	274
第 28 章 WAVE 系统的运转	276
28.1 无服务的通信	276
28.2 有服务的通信	276
28.2.1 WAVE 广播	277
28.2.2 发起服务	278
28.2.3 SCH 通信	278
28.2.4 服务终止	278
28.2.5 应用软件加入和退出广播	278
28.3 时间同步和信道调节	279
28.4 WAVE 中的地址和标识符	279
28.4.1 MAC 地址	279
28.4.2 IPv6 地址	279

28.4.3	协议/端口.....	280
28.4.4	使用 PSID 和 PSC 的应用软件认证	280
28.5	路边单元上分布式系统(DS)的入口	280
28.6	IPv6 相邻缓存.....	283
28.7	安全考虑.....	283
附录 R	系统结构举例	284
附录 S	定义和缩略语	285
S.1	定义	285
S.2	缩略语	290

第 1 部分 车载环境下无线存取试用标准 ——资源管理器

第 1 章 概 述

在车载环境中存在 2 种类型的无线存取 (WAVE) 设备: 第一种类型设备称为路边单元 (RSU), 在操作过程中, 它是静止不动的, 并且, 在通常情况下, 它都被安置在路边; 第二种类型设备称为车载单元 (OBU), 它通常在移动环境下工作, 并且总是被放置在车辆上。一般情况下, 静止设备有与之相应的应用软件, 该应用软件可以提供相应的服务; 移动设备也有一种对应的应用软件, 该应用软件就是去使用下述的服务。在远离 RSU 的设备上可能还会有更多应用软件, 这些应用软件的目的就是向 OBU 提供服务。这个标准描述了一种 WAVE 应用软件, 这种应用软件存在于 RSU 内, 但是该应用软件能把来自于远程应用软件的请求进行复用, 使得它们能够访问 OBU。

本部分具体说明了 WAVE 应用软件, 这个应用软件称为资源管理器 (RM), 它存在于 RSU 内。与它对等的软件称为资源命令处理器 (RCP), 它存在于 OBU 内。其他远离 RSU 的应用软件称为资源管理器应用软件 (RMA), 它是通过 RM 与 RCP 来实现通信的。这个标准描述了 RM 是如何复用来自于多个 RMA 的请求, 每一个请求都和多个拥有 RCP 的 OBU 进行通信。通信的目的就是使得 RMA 能够去访问资源, 例如, 内存、用户接口以及其他被 RCP 所控制的车载设备的接口, 以一种一致的、可互操作的、及时的方式去满足 RMA 的需求。

RM 使用了所有通信的概念, 这些通信被一个称为服务器的实体所初始化, 服务器向一个被称为用户的实体发布请求, 用户只对它接收到的请求进行响应。在这个标准内, RM 是一个服务的服务器 (作为 RMA 的一个代表), RCP 是这个服务的用户 (可视为将要被管理的资源)。RSU 或 OBU 都可以以服务器的身份运行, 换言之, 每一种设备类型都能够拥有 RM。拥有 RM 的设备 (RSU 或 OBU) 称为服务器设备。

1.1 范围

这个标准具体描述了 WAVE RM 的接口和服务, 包括安全性与私密性的保护机制, 它对在 5.9 GHz 带宽内的 DSRC 模式操作和 WAVE 模式操作的所有使用者都适用。其中, 5.9 GHz 带宽是由联邦通信委员会授权的。