无线局域网安全：设计及实现

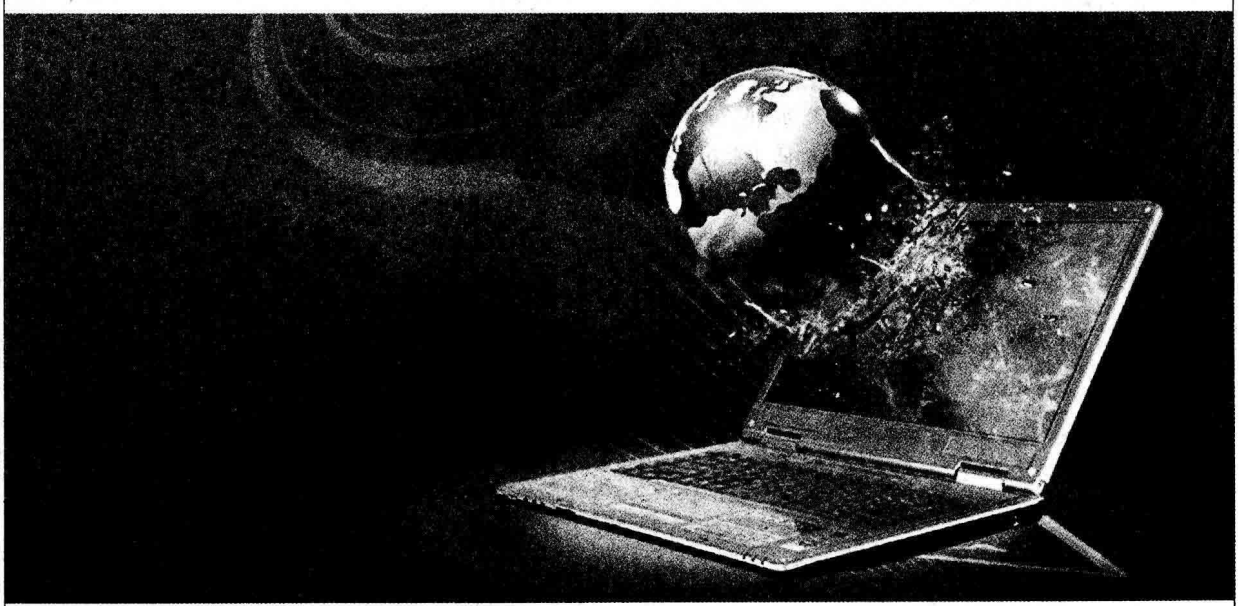
WUXIAN JUYUWANG ANQUAN: SHEJI JI SHIXIAN

郭渊博　杨奎武　张 畅　等著
马建峰　审

国防工业出版社
National Defense Industry Press

无线局域网安全：设计及实现

WUXIAN JUYUWANG ANQUAN: SHEJI JI SHIXIAN



郭渊博 杨奎武 张畅 刘威 马骏 著
马建峰 审

国防工业出版社
National Defense Industry Press

内 容 简 介

本书系统论述了无线局域网安全的基本需求、设计原理与实现方法。针对无线局域网络面临的安全攻击和所需的安全目标，从平台安全、通信安全和运行安全三个层面分析了无线局域网络存在的安全威胁和相应的安全需求，全面论述了各种安全措施的实现原理与关键技术，覆盖了无线局域网络安全体系结构设计、一体化的无线局域网安全接入、无线局域网络攻击渗透及检测、无线局域网安全管理、嵌入式无线终端安全防护、基于专用硬件的嵌入式安全无线接入点系统设计与实现、自适应无线局域网络安全结构、可信无线局域网安全终端体系结构与可信接入等内容。

本书针对有一定网络安全技术和无线通信技术基础的中、高级读者，适合军内外从事无线网络安全理论研究、设备研制、工程应用、项目管理人员，以及高校信息安全、计算机、通信等专业高年级本科生和研究生参考使用，对从事网络的安全防护系统研究与研制人员也有一定的借鉴与参考价值。

图书在版编目(CIP)数据

无线局域网安全:设计及实现 / 郭渊博等著. —
北京:国防工业出版社,2010.3
ISBN 978-7-118-06708-8

Ⅰ.①无… Ⅱ.①郭… Ⅲ.①无线电通信—局部网络—安全技术 Ⅳ.①TN925

中国版本图书馆 CIP 数据核字(2010)第 036387 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)
腾飞印务有限公司印刷
新华书店经售
*
开本 787×1092　1/16　印张 15¼　字数 348 千字
2010 年 3 月第 1 版第 1 次印刷　印数 1—4000 册　定价 29.00 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

无线局域网以其方便、快捷、廉价等诸多优势，近年在民用领域取得了长足的发展和巨大的成功，同时无线局域网的诸多特性也符合现代战争对军事通信提出的许多新要求。无线局域网络安全研究是近年来学术界和工业界的研究热点。然而现有研究大多数都仅关注了无线安全的接入和数据加解密的安全通信功能，对于无线平台安全和无线网络运行安全，以及无线局域网安全方案的设计开发，则关注甚少。

本书是作者近年来致力于无线局域网络安全保密的研究与开发所取得成果的提炼和总结，在对国际最新无线局域网安全标准 IEEE802.11i 和中国无线局域网安全标准 WAPI 的安全机制及其所存在的问题进行深入讨论的基础上，通过分析无线局域网络面临的安全攻击，根据实现安全无线局域网络所需的安全目标，从平台安全、通信安全和运行安全 3 个层面分析了无线局域网络存在的安全威胁和相应的安全需求，并据此提出了保障无线局域网络安全所需的各种安全措施，给出了无线局域网络安全保密体系结构，然后给出无线局域网安全体系结构中所需实施的各种安全措施的研究成果，重点内容如下：

(1)设计实现了一个一体化的无线局域网安全接入系统。首先讨论了无线局域网安全接入系统应用环境，分析了安全的接入系统的基本系统组成及工作原理，然后给出了无线接入客户端、基于主机的无线接入点以及认证授权服务器端这三大组成部件的设计与实现方法，最后简要介绍了系统的安装操作说明。所设计实现的无线局域网安全接入系统，可实现基于端口的访问控制，无线客户端到认证服务器之间基于证书的双向认证、无线客户端快速漫游切换、无线防火墙、对用户进行统一认证等，还可支持 EAP - MD5、EAP - TLS 等其他常用的接入认证方式。

(2)针对无线局域网的运行安全防护需求，研究了无线局域网络攻击渗透检测及安全管理技术，并给出了相应的开发方法。重点包括无线拓扑发现、无线密钥破解、无线拒绝服务攻击及检测、无线网络漏洞扫描、无线入侵检测、非法站点接入检测、MAC 地址欺骗检测、无线定位、无线蜜罐等方面。

(3)针对传统防病毒、入侵检测等软件的体积将随着病毒种类的增加和入侵手段的日新月异而不断增大，并不适合计算、存储能力以及电池容量有限的无线物理平台的问题，研究了嵌入式无线终端安全防护系统的设计与实现，基于 FPGA 内的多模式匹配引擎作为嵌入式无线网络安全防护系统的底层部件，基于 FPGA 的并行分类查找和多模式匹配实现高速深包检测。网络接收的数据经过网络接口部件之后直接进入 FPGA，实现数据信息流的高速多模式匹配，寻找组合特征信息以检测特殊攻击，为内容过滤、入侵防御、

防病毒以及反垃圾邮件等与处理有效载荷相关的操作提供高速硬件平台。

(4)给出了基于专用硬件的嵌入式安全无线接入点系统设计与实现。其中嵌入式微处理器采用 Atmel 公司 ARM 内核的 AT91RM9200,使用 Altera 公司的 CycloneII 系列芯片中的 EP2C50 大规模高性能的 FPGA 芯片实现数据加密/解密算法。除提供安全的无线接入方式外,系统还提供了 100Mb/s 速率的以太网接口和提供 RS-232 串口作为系统监控接口。给出了硬件部分以及无线网口和加密/解密模块等的驱动程序的软件部分的设计原理及其开发实现细节。最后,讨论了安全无线接入点在安全无线局域网络中的系统应用配置和部署方法,并给出了实际应用中的性能测试结果。

(5)提出了一种多重驱动的自适应无线局域网络安全结构,讨论了自适应结构中所涉及的关键性技术:给出了一种密码协议安全运行检测系统,可在无线局域网络环境执行过程中准确高效地自动检测协议的运行是否遭受攻击;设计了一种基于 D-S 证据推理方法的系统安全态势评估模型和一种基于层次分析方法的安全策略决策模型,能够根据不确定的、模糊的,甚至可能是矛盾的多源安全/入侵警报进行推理,以得到关于系统安全态势的定量结论,同时根据系统当前安全态势及系统资源状态和系统配置变化、用户使用偏好等因素,对系统的当前安全策略进行自适应调节;给出了无线局域网络环境中基于构件的自适应安全接入结构,针对无线局域网络安全接入方式多样、安全需求不同的问题,通过自适应配置的方式组装适当的协议功能,以产生适用于各种不同类型需求的安全协议,组合形成相应的安全接入系统。

(6)针对无线终端物理硬件平台缺乏完整性保护和验证机制,平台中各个模块的固件容易被攻击者篡改的问题,研究了可信无线局域网安全终端体系结构与可信接入。首先在对可信计算、可信计算框架、可信平台模块、可信移动平台介绍的基础上,研究了基于可信计算的无线终端安全体系结构,讨论了其软/硬件模块实现;然后在讨论实现可信无线局域网络需要解决的问题的基础上,基于 TCG 的可信网络连接 TNC 架构,结合可信移动平台体系结构,提出了一个可信移动 IP 平台框架,可以实现可信终端与可信网络的一致性,还给出了可信无线局域网络实现的逻辑结构。

书中的内容是作者所在课题组近年来致力于无线局域网络安全保密的研究与开发所取得成果的提炼和总结,在内容安排上,尽量避免与现有介绍和分析无线局域网安全标准和相关协议理论等的书籍相重复,而是着重论述作者的设计思路与关键技术方案及其实现等内容,系统地给出了无线局域网络安全保密的基本原理和实现方法。与同类出版的书相比,本书具有以下特点:

(1)内容和技术理念新:本书是首次以正式出版物的方式全面介绍无线局域网络安全防护设计开发细节的书籍,是作者课题组近年来最新的理论与工程实践结果,注重描述设计过程的思维方式和解决问题的方法。

(2)系统性强:从平台安全、通信安全和运行安全 3 个层面着手,分析无线局域网络存在的安全威胁和相应的安全需求,然后据此提出并实现保障无线局域网络安全所需的

各种安全措施。

(3)实用性强:每章都能够独立成文,都针对无线局域网络安全防护的一个方面,读者可以根据需要阅读感兴趣的章节。

全书着重论述作者的设计思路与关键技术方案及其实现,内容涵盖了作者研究开发的整个实践过程,可作为军内外从事无线网络安全理论研究、设备研制、工程应用、项目管理人员的参考,以及大专院校相关专业博士、硕士和高年级本科生的教材或学习参考书,对于从事类似网络的安全防护系统研究与研制人员也具有一定的借鉴与参考价值。

该书的完成体现了团队协作的精神,全书由郭渊博统稿和安排章节布局,第1、2、3章由郭渊博、张明雷完成,第4章由张畅、马骏完成,第5章由张畅完成,第6章由刘威完成,第7章由杨奎武、赵俭、马骏完成,第8章由郭渊博、郝耀辉完成,第9章由杨奎武完成。胡永进、李每虎等人在资料整理、实验测试等方面都做了许多辅助性的工作。解放军信息工程大学电子技术学院陈性元院长、4系寇红召主任和401教研室韦大伟主任在课题完成和资料撰写过程中给了很多的指导和帮助,西安电子科技大学计算机学院院长马建峰教授仔细审阅了全书并提出了很多宝贵意见,国防工业出版社电子信息图书事业部陈洁老师为本书的出版付出了很多辛苦的劳动,在此一并表示感谢。

本书参考了大量文献和资料,在此对原作者深表感谢,恕不一一列举。另外,互联网是本书的另一个重要参考资料的来源。由于网上许多资料无法找到其出处,所以书中如有内容涉及相关人士的知识产权,请给予谅解并请及时与我们联系。

由于无线局域网安全保密与防护是一个崭新的领域,涉及的内容范围又比较广,再加上作者水平所限,书中错误和不足之处在所难免,恳请专家、读者提出宝贵意见,并给予批评指正。

限于篇幅,书中重点给出了各种安全防护系统的设计原理,实现细节则一笔带过。读者如果对书中所给出的各类软、硬件系统感兴趣,可通过以下邮箱与我们联系:yuanbo_g@hotmail.com。

目　录

第 1 章　无线局域网技术概述 …… 1

1.1　基本概念 …… 1
1.2　无线局域网基本组成原理 …… 2
1.2.1　网络结构 …… 2
1.2.2　IEEE802.11 网络提供的服务 …… 3
1.3　IEEE802.11 协议分析 …… 4
1.3.1　物理层 …… 5
1.3.2　MAC 层 …… 5

第 2 章　无线局域网安全机制分析 …… 11

2.1　WLAN 安全机制发展过程 …… 11
2.2　WEP 协议分析 …… 12
2.2.1　RC4 算法 …… 12
2.2.2　WEP 数据加解密流程 …… 12
2.2.3　WEP 数据完整性校验 …… 14
2.2.4　WEP 身份认证原理 …… 15
2.2.5　WEP 协议中的安全隐患 …… 15
2.3　IEEE802.11i 协议分析 …… 17
2.3.1　IEEE802.11i 协议的加密机制 …… 18
2.3.2　IEEE802.11i 协议加密机制安全性分析 …… 25
2.3.3　IEEE802.11i 协议的认证机制 …… 26
2.3.4　IEEE802.11i 认证方法分析 …… 31
2.3.5　IEEE802.11i 密钥管理机制 …… 35
2.3.6　IEEE802.11i 密钥管理机制安全性分析 …… 38
2.4　WPA 安全框架 …… 39
2.4.1　WPA 的认证机制 …… 40
2.4.2　WPA 的加密机制 …… 40
2.4.3　WPA 的数据完整性机制 …… 40

2.4.4 WPA 存在的问题 …… 41
2.5 WAPI 安全框架 …… 41
2.5.1 WAI …… 41
2.5.2 WPI …… 44
2.5.3 WAPI 安全性分析 …… 45

第 3 章 无线局域网安全体系结构 …… 46

3.1 针对无线局域网的安全攻击 …… 46
3.1.1 逻辑攻击 …… 47
3.1.2 物理攻击 …… 49
3.1.3 DoS 攻击 …… 50
3.2 无线局域网安全保密体系结构 …… 58
3.2.1 安全目标 …… 58
3.2.2 安全威胁 …… 60
3.2.3 安全需求 …… 62
3.2.4 所需提供的安全措施 …… 63
3.3 安全无线局域网的基本结构和实现方案 …… 65
3.3.1 基本部署结构 …… 65
3.3.2 基本实现方案 …… 67

第 4 章 无线局域网安全接入系统 …… 70

4.1 系统概述 …… 70
4.2 无线局域网安全接入系统设计与实现 …… 73
4.2.1 无线接入客户端 …… 73
4.2.2 基于主机的 AP …… 75
4.2.3 无线防火墙 …… 90
4.2.4 认证服务器 …… 91

第 5 章 无线局域网安全管理系统 …… 102

5.1 系统概述 …… 102
5.2 无线局域网安全管理系统设计与实现 …… 104
5.2.1 无线拓扑发现 …… 104
5.2.2 WEP 密钥破解 …… 112
5.2.3 WPA – PSK 密钥破解 …… 113
5.2.4 无线拒绝服务攻击 …… 117

5.2.5 基于 Nessus 的网络漏洞扫描 …… 122
5.2.6 无线入侵检测 …… 125
5.2.7 无线局域网定位 …… 127
5.2.8 无线蜜罐 …… 129
5.2.9 威胁处理 …… 133

第 6 章 嵌入式无线局域网/高速安全防护引擎研究 …… 134

6.1 高速安全防护引擎设计 …… 134
6.1.1 整体结构 …… 134
6.1.2 实现方案 …… 135
6.2 多模式匹配算法研究 …… 137
6.2.1 单模式匹配算法 …… 138
6.2.2 多模式匹配算法 …… 138
6.2.3 基于硬件的模式匹配 …… 141
6.3 基于 Bloom Filter 的高速多模式匹配引擎研究与设计 …… 142
6.3.1 标准 Bloom Filter 查询算法基本操作 …… 142
6.3.2 标准 Bloom Filter 查询算法理论分析 …… 143
6.3.3 Bloom Filter 引擎设计 …… 145
6.3.4 位拆分状态机研究与设计 …… 146
6.3.5 连接结构 …… 148
6.3.6 性能分析 …… 150
6.4 过滤引擎的实现 …… 151
6.4.1 过滤引擎 …… 151
6.4.2 可扩展性问题 …… 153
6.5 精确匹配引擎的实现 …… 153
6.6 引擎性能 …… 156

第 7 章 嵌入式安全无线接入点系统 …… 158

7.1 嵌入式安全无线接入点设计方案 …… 158
7.1.1 安全无线局域网中的接入点 …… 158
7.1.2 嵌入式安全无线接入点设计方案 …… 159
7.2 硬件系统设计 …… 160
7.2.1 硬件系统总体设计 …… 160
7.2.2 硬件系统各模块说明 …… 160
7.2.3 硬件电路调试 …… 163

7.3 底层软件设计与移植 …… 166
7.3.1 板级支持包(BSP)的移植 …… 166
7.3.2 针对目标板的嵌入式操作系统的移植 …… 170
7.3.3 无线接入设备驱动程序的设计与移植 …… 172
7.3.4 具有一定安全功能的无线接入点设计 …… 175
7.3.5 RAMDisk 文件系统 …… 177

第8章 自适应的无线局域网安全结构 …… 178

8.1 基本概念 …… 178
8.2 自适应安全系统模型 …… 179
8.3 自适应无线局域网安全结构模型 …… 180
8.4 无线局域网中密码协议运行安全检测系统 …… 183
8.4.1 系统结构 …… 183
8.4.2 密码协议执行特征 …… 184
8.4.3 监视器的构造 …… 186
8.4.4 检测原理 …… 190
8.5 基于 D-S 证据理论的安全态势估计方法 …… 191
8.5.1 D-S 证据理论简介 …… 192
8.5.2 无线局域网络安全态势估计 …… 193
8.6 基于层次分析方法的自适应安全策略决策方法 …… 195
8.6.1 层次分析法理论简介 …… 195
8.6.2 安全无线局域网系统的自适应策略选择 …… 196
8.7 安全策略决策器设计 …… 197
8.7.1 内部结构 …… 197
8.7.2 各组成部件功能介绍 …… 198
8.8 无线终端自适应安全接入结构研究 …… 198
8.8.1 原理与接入方法 …… 199
8.8.2 系统设计 …… 202

第9章 可信无线局域网安全终端体系结构与可信接入 …… 206

9.1 可信计算平台 …… 206
9.1.1 TCG 可信计算平台体系结构及特征 …… 206
9.1.2 TPM 可信平台模块 …… 210
9.1.3 TCG 信任链传递技术 …… 212
9.1.4 可信平台的密钥与证书 …… 213

9.2 基于可信计算的终端安全体系结构 …… 214
9.2.1 基于安全内核的体系结构 …… 215
9.2.2 基于微内核的结构 …… 216
9.2.3 基于虚拟机的结构 …… 217
9.2.4 基于 LSM 机制的结构 …… 217
9.3 无线局域网可信接入体系结构 …… 218
9.3.1 可信网络连接需要解决的问题 …… 218
9.3.2 无线局域网可信体系结构 …… 222
9.3.3 可信无线终端接入可信无线局域网 …… 224

参考文献 …… 226

缩略词 …… 230

第1章　无线局域网技术概述

1.1　基本概念

无线局域网，顾名思义，就是在局部区域以无线媒体或介质进行通信的一种网络形态。它利用空中电磁波代替传统的缆线进行信息传输，在不采用传统电缆线的同时，提供传统有线局域网的所有功能，可以作为传统有线网络的延伸、补充或替代。与有线网络相比较，具有以下许多优点：

1. 移动性(Mobility)

“无线”就意味着可以移动，无线局域网的明显优点是提供了移动性。通信范围不再受环境条件的限制，这样就拓宽了网络传输的地理范围。在有线局域网中，两个站点的距离在使用铜缆(粗缆)时被限制在500m内，即使采用单模光纤也只能达到3km，而无线局域网中两个站点间的距离目前可达到50km。无线局域网系统能够为用户提供实时的无处不在(Ubiquitous)的网络接入功能，使用户可以很方便地获取信息。

移动性分为用户移动和用户设备移动两类。在无线局域网中，无线局域网设备的移动又可分为不移动或固定(Fixed)、半移动(Nomadic)、便携式(Portable)移动和全移动(Mobile或Moving)。半移动是指设备可在网内移动，但只能在静止状态下与网络进行通信。全移动是指设备可在移动状态下保持与网络的通信，即“动中通”，它还可以细分为慢速移动和快速移动。目前的无线局域网系统一般只支持固定、半移动和慢速移动。

此外，从网络层次上讲，移动又分为链路层移动和网络层移动。链路层移动又称为越区切换(Handoff)或散步(Walking)，网络层移动也称为漫游(Roaming)。

2. 灵活性(Flexibility)

安装容易，使用简便，组网灵活，无线局域网可以将网络延伸到线缆无法连接的地方，并可方便地增减、移动和修改设备。无线局域网的组网方式灵活多样，可以通过基础结构(Infrastructure)接入骨干网(Backbone)，也可以自组网(Ad hoc)；可以组成单区网和多区网，还可以在不同网间进行移动。

3. 可伸缩性(Scalability)

在适当的位置放置或添加接入点(Access Point，AP)或扩展点(Extend Point，EP)，就可以满足扩展组网的需要。

4. 经济性(Saving)

无线局域网可用于物理布线困难或不适合进行物理布线的地方，如危险区和古建筑等场合，节省了缆线及其附件的费用，省去布线工序，可快速组网，可以节省人员费用，并能将网络快速投入使用，提高了经济效益。对于临时需要网络的地方，无线局域网可以低

成本地快速实现，对于需要频繁重新布线或更换地方的场合，无线局域网可以节省长期费用。

1.2 无线局域网基本组成原理

1.2.1 网络结构

无线局域网的物理组成或物理结构如图 1－1 所示，由站（Station，STA）、无线介质（Wireless Medium，WM）、基站（Base Station，BS）或接入点（Access Point，AP）和分布式系统（Distribution System，DS）等几部分组成。

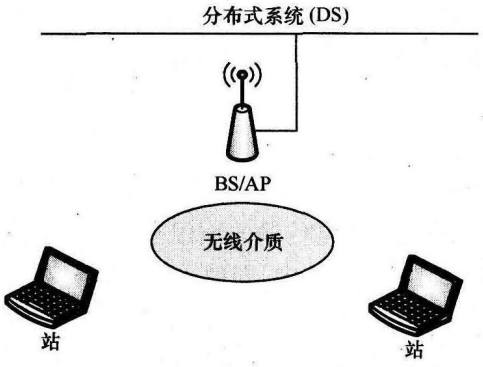


图 1－1 无线局域网的物理结构

1. 站（STA）

站（点）也称主机或终端，是无线局域网的最基本组成单元。网络就是进行站间数据传输的，我们把连接在无线局域网中的设备称为站。站在无线局域网中通常用做客户端，它是具有无线网络接口的计算设备。它包括以下几部分：

（1）终端用户设备。终端用户设备是站与用户的交互设备。这些终端用户设备可以是台式计算机、便携式计算机和掌上电脑等，也可以是其他智能终端设备，如 PDA 等。

（2）无线网络接口。无线网络接口是站的重要组成部分，它负责处理从终端用户设备到无线介质间的数字通信，一般采用调制技术和通信协议的无线网络适配器（无线网卡）或调制解调器（Modem）。无线网络接口与终端用户设备之间通过计算机总线（如 PCI）或接口（如 RS－232、USB）等相连，并由相应的软件驱动程序提供客户应用设备或网络操作系统与无线网络接口之间的联系。

（3）网络软件。网络操作系统（NOS）、网络通信协议等网络软件运行于无线网络的不同设备上。客户端的网络软件运行在终端用户设备上，它负责完成用户向本地设备软件发出命令，并将用户接入无线网络。当然，对无线局域网络的网络软件有其特殊的要求。无线局域网中的站之间可以直接相互通信，也可以通过基站或接入点进行通信。在无线局域网中，站之间的通信距离由于天线的辐射能力有限和应用环境的不同而受到限制。我们把无线局域网所能覆盖的区域范围称为服务区域（Service Area，SA），而把由无线局域网中移动站的无线收发信机及地理环境所确定的通信覆盖区域称为基本服务区（Basic Service Area，BSA）。考虑到无线资源的利用率和通信技术等因素，BSA 不可能太

大,通常在100m以内,也就是说同一BSA中的移动站之间的距离应小于100m。

2. 无线介质

无线介质是无线局域网中站与站之间、站与接入点之间通信的传输媒介。在这里指的是空气,它是无线电波和红外线传播的良好介质。无线局域网中的无线介质由无线局域网物理层标准定义。

3. 无线接入点(AP)

无线接入点类似于蜂窝结构中的基站,是无线局域网的重要组成单元。无线接入点是一种特殊的站,它通常处于BSA的中心,固定不动。其基本功能有:

(1)作为接入点,完成其他非AP的站对分布式系统的接入访问和同一(Basic Service Set,基本服务区)中的不同站间的通信连接。

(2)作为无线网络和分布式系统的桥接点完成无线局域网与分布式系统间的桥接功能。

(3)作为BSS的控制中心完成对其他非AP的站的控制和管理。

4. 分布式系统(DS)

一个BSA所能覆盖的区域受到环境和主机收发信机特性的限制。为了能覆盖更大的区域,就需要把多个BSA通过分布式系统连接起来,形成一个扩展业务区(Extended Service Area,ESA),而通过DS互相连接起来的属于同一个ESA的所有主机组成一个扩展业务组(Extended Service Set,ESS)。分布式系统就是用来连接不同BSA的通信通道,称为分布式系统信道(Distribution System Medium,DSM)。DSM可以是有线信道,也可以是频段多变的无线信道。这样在组织无线局域网时就有了足够的灵活性。

1.2.2 IEEE802.11网络提供的服务

在无线局域网中,所有无线设备的一切行为都应遵守IEEE802.11协议的规范,无线设备可以进行的活动其实就是协议提供的服务。IEEE802.11定义了9项服务,其中5项为分发服务,用于管理BSS内的成员以及不同BSS成员之间的交互工作,另外4项为站点安全可靠服务,用于单个BSS内的工作。

1. 分发服务(Distribution service)

(1)Association(关联)。关联即移动主机将自身与基站相连接;当一个移动主机进入某基站的信号范围时,应该把自己的标识、相关性能(包括数据传输速率,需要的PCF服务polling和能源管理等)通报给基站;基站可以接受也可以拒绝,如果接受,以后当基站轮询时,该主机必须能识别。

(2)Disassociation(解除关联)。解除关联即移动主机或基站之间断开连接;当移动主机关机或者离开某基站前,应先与该基站解除关联;基站在断电维护前也应先与连接的移动主机解除关联。

(3)Reassociation(重新关联)。重新关联即移动主机在不同的BSS之间移动时改变所连接的基站;在移动过程中不应丢失数据;IEEE802.11与Ethernet相似,也是采用尽力而为的服务策略。

(4)Distribution(分发)。决定如何将帧送往目的站点,如果目的站点与本基站同属一个BSS,则可直接传送,否则将由分发系统DS并通过有线网络转发给另一个基站,分发功

能由 AP 实现。

(5) Integration(整合)。整合即 IEEE802.11 网络与非 IEEE802.11 网络通信时的地址和报文格式的转换,即桥接功能。由于 BSS 之间的通信或无线网络与有线网络(通常是 IEEE802.3)之间的通信必须通过有线网络,所以整合功能也由 AP 实现。

2. 站点服务(Station service)

(1) Authentication(认证)。为提高通信的安全性,该项服务提供身份认证机制,当移动主机进入某个 BSS 并与基站关联后,基站便向移动主机发出一个特殊的查询帧,通过核对已分配给移动主机的密钥来确认该移动主机的合法性,并最终同意该主机在 BSS 注册。

(2) Deauthentication(撤消认证)。当已被认证的移动主机要离开网络时,必须撤消认证,不再允许使用原网络。

(3) Privacy(保密)。处理信息的加密与解密。

(4) Data delivery(数据的递交)。IEEE802.11 不提供 100% 的可靠性保证,当需经过以太网通信时,以太网也不提供 100% 的可靠性保证,所以必须由高层协议来负责检查和校正差错,以保证最终数据递交的正确性。

1.3 IEEE802.11 协议分析

完整的网络结构包括自上而下的各个层次,但无线网络仅仅工作在 OSI/RM 的下三层,即通信子网层,如图 1-2 所示。其中 WLAN 可以包括物理层和数据链路层的功能,只有 WWAN 才具有网络层的功能。

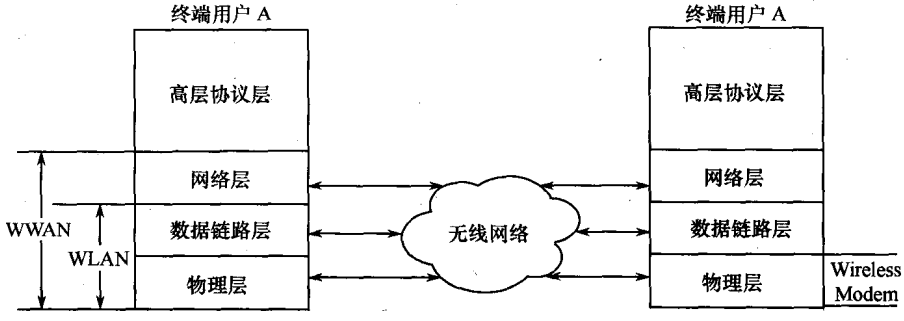


图 1-2 无线网络逻辑结构

IEEE802.11 标准是 IEEE 制定的无线局域网标准,主要是对网络的物理层(PHY)和媒质访问控制层(MAC)进行了规定,而其中对 MAC 层的规定是重点。各种局域网有不同的 MAC 层,而逻辑链路控制层(LLC)是一致的,即逻辑链路层以下对网络应用是透明的。这样就使得无线网的两种主要用途——"多点接入"和"多网段互连",易于质优价廉地实现。

IEEE802.11 系列标准的协议体系结构如图 1-3 所示。LLC 层与其他 IEEE802 局域网一样并共用,而 MAC 子层为多种物理层标准所共用。IEEE802.11MAC 子层支持的物理层有以下几种:

(1)IEEE802.11 跳频(Frequency Hopping Spread Spectrum,FSSS)物理层,在2.4GHz频段上提供1Mb/s~2Mb/s的传输速率。

(2)IEEE802.11 直接序列扩频(Direct Sequence Spread Spectrum,DSSS)物理层,在2.4GHz频段上提供1Mb/s~2Mb/s的传输速率。

(3)IEEE802.11b 物理层,在2.4GHz频段上提供1Mb/s~11Mb/s的传输速率。

(4)IEEE802.11a 物理层,在5GHz频段上提供6Mb/s~54Mb/s的传输速率。

(5)IEEE802.11g 物理层,在2.4GHz频段上提供高达54Mb/s的传输速率。

(6)IEEE802.11 红外线(IR)物理层,提供1Mb/s~2Mb/s的传输速率。

(7)IEEE802.11n 物理层将提供108Mb/s~340Mb/s的传输速率。

<table>
<tr><td rowspan="3">站管理</td><td></td><td colspan="6">LLC</td><td rowspan="2">DLL</td></tr>
<tr><td>MAC管理</td><td colspan="6">MAC</td></tr>
<tr><td>PHY管理</td><td>IEEE802.11 FHSS</td><td>IEEE802.11 DSSS</td><td>IEEE802.11 IR</td><td>IEEE802.11a</td><td>IEEE802.11b</td><td>IEEE802.11g</td><td>PLCP
PMD</td></tr>
</table>

图1-3 IEEE802.11协议体系

MAC层也分为MAC子层和MAC管理子层。MAC子层负责访问机制的实现和分组的拆分与重组。MAC管理子层负责ESS散步管理、电源(节能)管理,以及连接过程中的连接、解除连接和重新连接等过程的管理。

1.3.1 物理层

物理层定义了数据传输的信号特征和调制方式。无线局域网可以使用两种介质进行传输:射频(RF)和红外线(Infrared);而且有两种调制方式:直接序列扩频(DSSS)和跳频扩频(FHSS)。

DSSS采用扩展的冗余编码方式进行数据传输,其利用比发送信息速率高许多的伪随机代码对信息数据的基带频谱进行扩展,形成宽带低功率谱密度的信号;在接收端用相同的伪随机代码对接收到的信号进行相关的处理,恢复出原始信息。

FHSS技术是将2.4GHz~2.483GHz频道划分为75个1MHz的子频道,在一个频带上发送完一段较短的信息后,跳转到另一个频带上;接收方和发送方协商一个跳频模式,数据按照这个序列在各个子频道上进行传送。在一段时间内跳转完所有规定的频带后,再开始另一个跳转周期。物理层能够根据环境噪声情况自动地对传输速率进行调节。

1.3.2 MAC层

介质访问控制(MAC)属于数据链路层的一部分,该部分与逻辑链路控制子层(LLC)共同组成了数据链路层。MAC作为局域网的关键一层,对局域网的网络性能有非常重要的影响,无线局域网由于使用开放的媒体作为传输介质以及移动性等特点,与有线局域网中的MAC协议存在很大差异。IEEE802.11无线局域网MAC层主要采用了如下关键技术。

1. CSMA/CA

IEEE802.11MAC 提供了在不可靠的无线媒质上可靠传输用户数据的机制。它采用了与传统的有线局域网采用的 CSMA/CD(载波监听多路访问/冲突检测)协议类似的 CSMA/CA(载波监听多路访问/冲突避免)协议,这是 WLAN 的 MAC 层最基本的接入方式。操作方式是:欲发送数据的站点先监听介质,若介质空闲,则保持一段时间间隔 DIFS,就立即发送数据;如介质忙,则推迟发送并继续监听直到当前传输结束。当空闲时间超过 DIFS 时,站点进入退避状态,利用二进制指数退避算法,即随即选择等待 $1-2n$ 个时间片,再次发送。退避过程中,如检测到介质忙,则退避计时器暂停计时,直至介质空闲时间大于 DIFS 后恢复计时。当退避计时器为 0 时,站点开始发送数据。为增强 CSMA/CA 对异步数据传输的可靠性,还采用了 MAC 层确认机制,这样可以对丢失的帧予以检测。

2. 媒体接入控制

IEEE802.11 MAC 的基本接入方式包括分布控制方式(DCF)和中心控制方式(PCF)。其中 DCF 基于 CSMA/CA,利用载波检测机制,适用于分布式网络,传输具有突发性和随机性的普通分组数据,支持无竞争型实时业务及竞争型非实时业务。而 PCF 则是建立在 DCF 工作方式之上,并且仅支持竞争型非实时业务,适用于具备中央控制器的网络上,如 AP。

MAC 帧是构成 MAC 协议和保证有效数据通信的基础。在 MAC 协议中,共有 3 种类型的 MAC 帧,它们分别是数据帧、控制帧和管理帧。IEEE802.11bMAC 帧格式如图 1-4 所示。

2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

图 1-4 IEEE802.11bMAC 帧格式

MAC 帧类各个字段的具体含义如下:

1)帧控制域

帧控制域的长度为 16 个比特位,用于在工作站之间发送控制信息,具体内容如图 1-5所示。

2	2	4	1	1	1	1	1	1	1	1
Protocl Version	Type	Subtype	To DS	From DS	More Frag	Retry	Rwr Mgt	More Data	WEP	Order

图 1-5 帧控制域

帧控制域内各字段含义如下:

(1)协议版本字段。用来表示当前构成 IEEE802.11MAC 协议的版本号。

(2)帧类型字段。表明当前的帧是管理帧、控制帧还是数据帧。

(3)子类型字段。用来表明 3 种类型帧中的完成特定功能的帧。

(4)DS 目的地址字段和 DS 源地址字段。这两个字段不同取值的具体含义如表 1-1 所列。