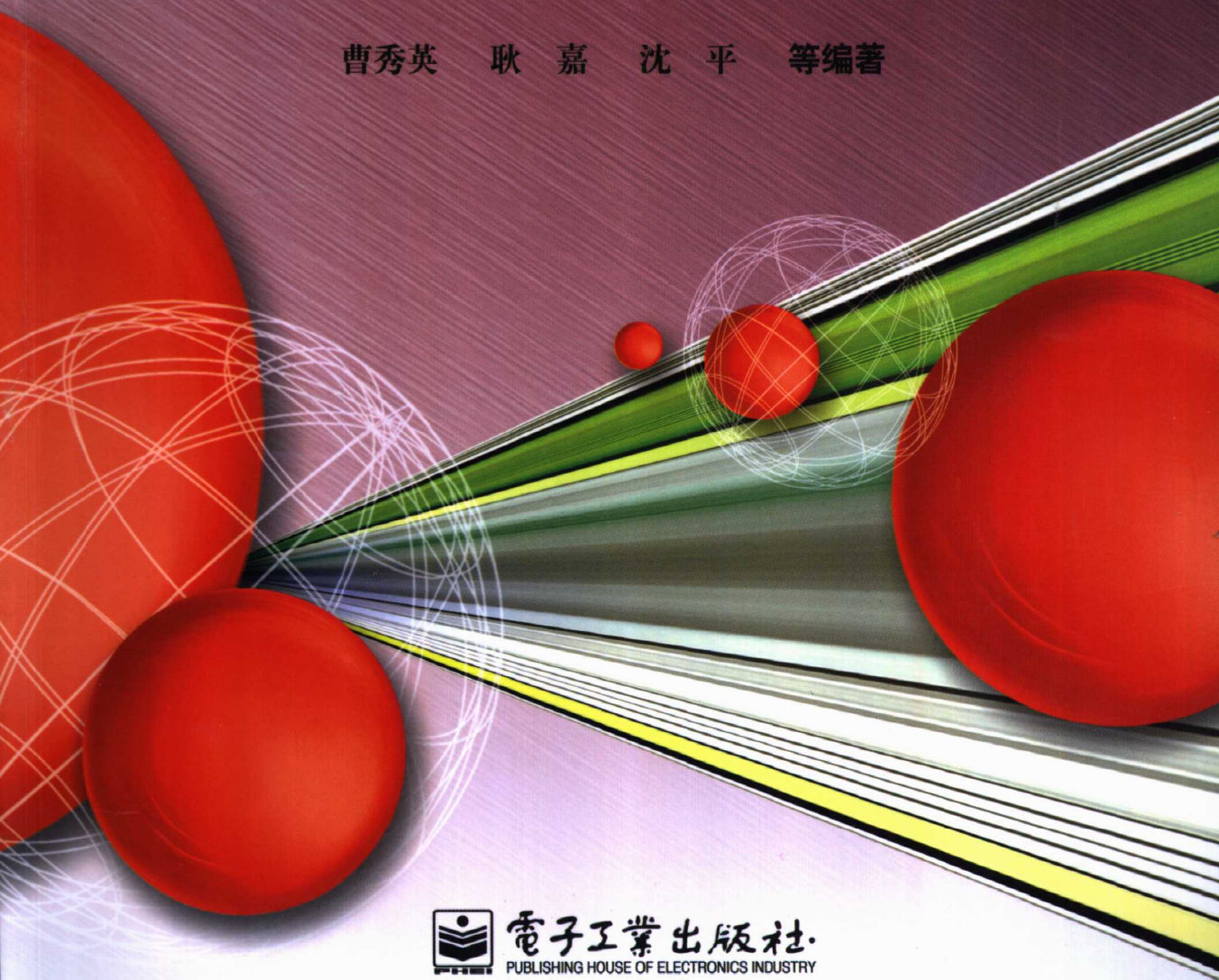
移动通信前沿技术丛书

无线局域网安全系统

曹秀英　耿　嘉　沈　平　等编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

移动通信前沿技术丛书

无线局域网安全系统

曹秀英　耿　嘉　沈　平　等编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书针对 IEEE 802.11 系列标准，对无线局域网安全系统进行研究。全书共分上、中、下三篇，主要讲述了无线局域网安全系统的基本理论和实际应用，其中包括无线局域网标准概述、IEEE 802.11 标准、无线局域网密钥管理协议、RADIUS 协议、RC4 算法、TKIP 密码协议、AES 算法分析、WRAP 与 CCMP 密码协议、ECC 体制、安全无线局域网的实现方案、无线局域网 AP 和网卡的嵌入式硬件设计、IEEE 802.11 MAC 层的软件实现、无线局域网安全认证和密钥管理系统的实现、RADIUS 服务器在 WLAN 中的实现等方面内容。

本书可作为网络通信领域的工程技术人员和科研人员的参考书，也可供高等院校通信与信息系统专业的本科生、研究生阅读。

图书在版编目（CIP）数据

无线局域网安全系统/曹秀英，耿嘉，沈平等编著. —北京：电子工业出版社，2004.3
（移动通信前沿技术丛书）
ISBN 7-5053-9657-9
Ⅰ.无… Ⅱ.① 曹… ② 耿… ③沈… Ⅲ.无线电通信—局部网络—安全技术 Ⅳ.TN925
中国版本图书馆 CIP 数据核字（2004）第 008500 号

责任编辑：沈艳波 特约编辑：杨 琳
印 刷：北京增富印刷有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编：100036
经 销：各地新华书店
开 本：787×1 092 1/16 印张：14 字数：360 千字
印 次：2004 年 3 月第 1 次印刷
印 数：5 000 册 定价：25.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 *dbqq@phei.com.cn*。

出 版 说 明

移动通信是当前发展最快、应用最广和最前沿的通信领域之一，有专家预测到 2003 年全球移动用户数将达到 10 亿。移动通信的最终目标是实现任何人可以在任何地点、任何时间与其他任何人进行任何方式的通信。移动通信技术现在已经发展到了以 WCDMA 为代表的第三代，而相互兼容各种移动通信技术的第四代标准目前已经悄然来临。为了促进和推动我国移动通信产业的发展，并不断满足社会各界和广大通信技术人员系统学习和掌握移动通信前沿技术的需求，电子工业出版社特约请国内从事移动通信科研、教学、工程、管理等工作并具有丰富的理论和实践经验的专家、教授亲自编著或翻译国外经典著作组成了这套《移动通信前沿技术丛书》，于新世纪之初相继地推出。

该丛书从我国移动通信技术应用现状与发展情况出发，以系统与技术为中心，全面系统地介绍了当今移动通信领域涉及的有关关键技术热点技术，如软件无线电原理与应用、智能天线原理与应用、蓝牙技术、移动 IP、通用无线分组业务（GPRS）、移动通信网络规划与优化、移动数据通信以及典型的第三代移动通信系统等内容。其特点是力求内容的先进性、实用性和系统性；突出理论性与工程实践性紧密结合；内容组织循序渐进、深入浅出，理论叙述概念清晰、层次清楚，经典实例源于实践。丛书旨在引导读者将移动通信的原理、技术与应用有机结合。

这套丛书的主要读者对象是广大从事通信技术工作的工程技术人员，也适合高等院校通信、计算机等学科各专业在校师生和刚走上工作岗位的毕业生阅读参考。

在编辑出版这套丛书过程中，参与编著、翻译和审定的各位专家都付出了大量心血，对此，我们表示衷心感谢。欢迎广大读者对这套丛书提出宝贵意见和建议，或推荐其他好的选题（E-mail：davidzhu@phei.com.cn），以便我们今后为广大读者奉献更多、更好的优秀通信技术图书。

电子工业出版社
通信与电子技术事业部

前　言

无线局域网（Wireless Local Area Network, WLAN）是迅猛发展的无线通信技术在计算机网络中的应用，采用了无线多址信道的方式支持计算机之间的通信，并为移动通信、个人通信、多媒体应用提供了实现方法。与此同时无线局域网的安全性也被提到议事日程上来。

我国无线局域网应用正处于起步阶段，如果沿用已有的国际标准，则势必导致一些安全问题，因而及时制定我国自主的兼容国际标准的安全无线局域网标准并推广应用势在必行。

本书是在“863”高科技项目基础上，致力于我国无线局域网安全技术的研究。在项目研究和写书的过程中，国际无线局域网新标准的不断完善为无线局域网安全技术提供了良好的借鉴，我们积极跟踪和借鉴国际标准中相关技术，对已确定的安全技术进行深入的研究和实现，在此基础上，力图为我国安全无线局域网标准的制订工作提供必要的理论和技术支持，逐步参与国际标准的讨论和制订，提出自主创新的见解。

“863”项目研究内容主要针对 IEEE 802.11 系列标准研究其相关技术，内容包括安全认证技术、加密技术和 WLAN 技术三方面，其中安全认证技术主要包括安全认证、密钥管理等；加密技术主要是指无线局域网中采用的数据保护技术，包括数据加密算法、加密模式、消息完整性检验算法等内容；WLAN 技术的研究主要涉及无线局域网媒体访问控制，网络协议的功能性仿真是研究安全技术的基础。通过对这些内容的深入研究，在无线局域网安全技术领域提出具有我国自主知识产权的理论和技术成果，为未来我国无线局域网产业化提供理论指导和技术支持。《无线局域网安全系统》一书是“863”高科技项目理论和技术的结晶，希望会给人们很多新的启迪。

《无线局域网安全系统》一书经过老师和同学们的共同努力，终于要跟大家见面了，这是课题组全体同志（曹秀英、沈平、耿嘉、沈基明、李枫、刘向宇、郑晓蕾、王璐和王兴猛）辛勤劳动的成果，在此向大家表示深深的感谢。同时，向电子工业出版社的领导和编辑对我们工作的支持和帮助表示最诚挚的谢意。

编著者

2003.10.29

目　录

上篇　概　述

中篇　基本理论与分析

下篇 实际应用

上篇　概　　述

第1章 绪 论

无线局域网（Wireless Local Area Network，WLAN）是高速发展的现代无线通信技术在计算机网络中的应用，它采用无线多址信道的有效方式支持计算机之间的通信，并为通信的移动化、个人化和多媒体应用提供了实现的手段。随着个人数据通信的发展，功能强大的便携式数据终端以及多媒体终端得到了广泛应用。为了实现任何人在任何时间、任何地点均能进行数据通信的目标，要求传统的计算机网络由有线向无线、由固定向移动、由单一业务向多媒体发展，顺应这一需求的无线局域网技术因此得到了普遍的关注。无线局域网以其方便、快捷、廉价等诸多优势，在企事业内部和公共热点地区等领域的应用中很快取得了长足的发展和巨大的成功，而与此同时用户对无线局域网的各种性能，尤其是安全性能的要求变得格外苛刻。

1.1 无线局域网标准概述

无线局域网协议标准目前主要有 IEEE 802.11 标准、蓝牙（Bluetooth）标准、HomeRF 标准和 HiperLAN2 标准。

- IEEE 802.11 标准：IEEE 802.11 无线局域网标准的制定是无线网络技术发展的一个里程碑。IEEE 802.11 标准除了使得各种不同厂商的无线产品得以互连之外，还促进了核心设备执行单芯片解决方案的实施，降低了无线局域网的成本。该标准的颁布，使得无线局域网在各种有移动要求的环境中被广泛接受，它也是目前最常用的无线局域网传输协议。不过该标准速率最高只能达到 2 Mbps，不能满足人们的需要，因此，IEEE 小组又相继推出了 IEEE 802.11b 和 IEEE 802.11a 两个新标准。IEEE 802.11b 标准速率最大可达到 11 Mbps，而 IEEE 802.11a 标准传输速率可达 54 Mbps，完全能满足语音、数据、图像等业务的需要。
- 蓝牙（Bluetooth）标准：蓝牙（IEEE 802.15）是一项新标准，对于 IEEE 802.11 来说，蓝牙的出现是与之相互补充。“蓝牙”是一种大容量近距离无线数字通信的技术标准，其目标是实现最高数据传输速率 1 Mbps，最大传输距离为 0.1～10 m，通过增加发射功率可达到 100 m，蓝牙比 IEEE 802.11 更具移动性。蓝牙成本低、体积小，可用于更多的设备。“蓝牙”最大的优势还在于：在更新网络骨干时，如果搭配“蓝牙”架构进行，使用整体网络的成本肯定比布设有线网络低。
- 家庭网络的 HomeRF：HomeRF 主要为家庭网络设计，是 IEEE 802.11 与 DECT（数字无绳电话标准）的结合，目的在于降低语音数据成本。HomeRF 采用了扩频技术，工作在 2.4 GHz 频带，能同步支持 4 条高质量语音信道。但目前 HomeRF 的最高传输速率只有 10 Mbps。
- HiperLAN2 标准：目前，欧洲电信标准制定机构——ETSI 批准了 HiperLAN2 标准的核心技术规范，这意味着，最终用户将能以 54 Mbps 的高速通过无线方式接入互联网（原始物理层吞吐率高达 54 Mbps，实际应用吞吐率最低也能保持在 20 Mbps 左右），

并使用今后推出的多媒体和即时视频服务。HiperLAN2 是一种新的高性能无线电技术，工作频率为 5 GHz。它是一种多用途的技术，将可以在企业办公、公共和家庭环境中为下一代移动通信提供高速的本地连接。该系统能够迅速且简单地安装，并可以与 IP、以太网、PPP、ATM 和 IEEE1394 等多种核心网络技术互连互通。它还包括一个面向 UMTS 的界面，可以作为其他面向第三代移动通信系统 IMT-2000 系列的界面基础。

1.2 IEEE 802.11 标准简介

1997 年 6 月 26 日，IEEE 802.11 标准制定完成，1997 年 11 月 26 日正式发布。IEEE 802.11 无线局域网标准承袭 IEEE 802 系列，规范了无线局域网的媒体访问控制层（Medium Access Control，MAC）及物理层 PHY （Physical）技术。目前，IEEE 802.11 标准系列主要有以下一系列协议。

- IEEE 802.11a：它扩充了 IEEE 802.11 标准的物理层，规定该层使用 5.8 GHz 的 ISM 频带。该标准采用正交频分（OFDM）调制数据，传输速率范围为 6～54 Mbps。这样的速率既能满足室内的应用，也能满足室外的应用。
- IEEE 802.11b：它是 IEEE 802.11 标准的另一个扩充，也被 WECA（The Wireless Ethernet Compatibility Alliance）称为 Wi-Fi，使用开放的 2.4 GHz 频率，一般采用直接序列扩频（DSSS）和补偿编码键控（CCK）调制技术，最大数据传输速率为 11 Mbps。表 1-1 是 IEEE 802.11, IEEE 802.11 b, IEEE 802.11 a 的特点比较。
- IEEE 802.11d：是 IEEE 802.11b 使用其他频率的版本，以适应一些不能使用 2.4 GHz 频段的国家。
- IEEE 802.11e：在 IEEE 802.11 系列协议中增加 QoS 能力。它用 TDMA 方式取代类似 Ethernet 的 MAC 层，为重要的数据增加额外的纠错功能。
- IEEE 802.11f：目的是改善 IEEE 802.11 协议的切换机制，使用户能够在不同的交换分区间（无线信道）或者在接入设备间漫游。这就使无线局域网能够提供与移动通信同样的移动性。
- IEEE 802.11g：也被称为 Wi-Fi，该标准也使用 2.4 GHz 频段，并将传输速率从现有 IEEE 802.11b 的 11 Mbps 提高到 54 Mbps，与 IEEE 802.11a 相当。调制方式遵循 Intersil 公司的 CCK-OFDM 与 TI 公司的 PBCC-22（分组二进制卷积码），而 PBCC-22 技术使得 22 Mbps 的速率与现有支持 11 Mbps 的 IEEE 802.11b 产品间相互兼容。
- IEEE 802.11h：比 IEEE 802.11a 能更好地控制发送功率和选择无线信道，与 IEEE 802.11e 一起可以适应欧洲的更严格的标准。
- IEEE 802.11i：改善 IEEE 802.11 标准最明显的缺陷——安全问题。
- IEEE 802.11j：目的是使 IEEE 802.11a 和 HiperLAN2 网络能够互通。

表 1-1 IEEE 802.11, IEEE 802.11b, IEEE 802.11a 的特点比较

	IEEE 802.11	IEEE 802.11b	IEEE 802.11a
频率	2.4 GHz	2.4 GHz	5 GHz
带宽	1～2 Mbps	可达 11 Mbps	可达 54 Mbps

续表

	IEEE 802.11	IEEE 802.11b	IEEE 802.11a
距离	100 m	功率增加可扩展 100 m	5～10 km
业务	数据	数据、图像	语音、数据、图像

人类需求推动技术的发展和应用，新的无线局域网协议将在今后不断出现。它们拥有高的数据速率、QoS 保证和安全性，将是对有线宽带数据网络的挑战。IEEE 还在不断改善现有的这些协议，已经推出或即将推出一些新的协议。

1.3 无线局域网安全系统

无线局域网安全系统由认证、加密、WLAN 三部分组成，如图 1-1 所示。

- 认证技术：通过 IEEE 802.1x, EAP, RADIUS 协议验证信息的发送者是合法的而不是冒充的，验证信息的完整性，是防止主动攻击的重要技术，对开放环境中的各种信息系统的安全性有重要作用。
- 加密技术：应用对称密钥、公钥密码、密钥管理来隐蔽和保护需要保密的信息。
- WLAN 技术：是计算机网络与无线通信技术相结合的产物，由 MAC 层和物理层组成。

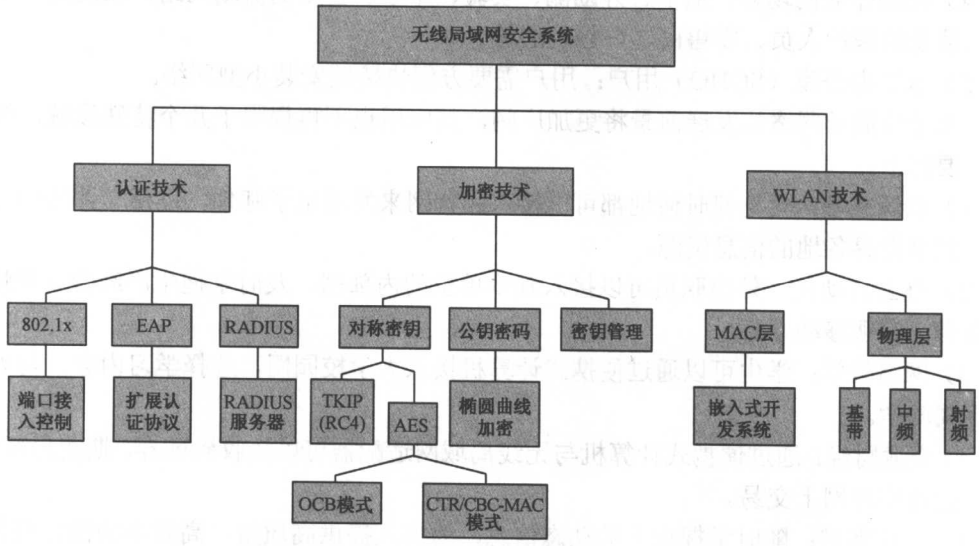


图 1-1 无线局域网安全系统结构示意图

1.4 无线局域网的优点及应用

无线局域网具有多方面的优点，其发展十分迅速。在最近几年里，无线局域网已经在医院、商店、工厂和学校等不适合网络布线的场合得到了广泛的应用。无线局域网主要有以下一些优点。

（1）灵活移动性：无线网络可为用户提供实时的、移动性的网络资源共享，这是普通局域网无法达到的。

（2）安装简单、快速。

（3）运行成本低廉：尽管初期投资比普通局域网要高，但从整体安装、运行成本以及使用寿命而言，都得到了巨大的改善。尤其是在用户经常移动的工作环境下，运行费用很低。

（4）可扩展性强：无线局域网可以配制成各种网络拓扑结构来满足多种应用和安装需要。从点对点的小型网络，到拥有数千台结点的网络系统，以及某一范围内实现漫游功能的大型网络，均不需要更改任何硬件设施。

（5）便于维护和管理：对于传统布线，局域网络管理的主要工作之一是检查电缆是否畅通，这种工作耗时耗力，而且整个网络的布线星罗棋布，不容易在短时间内找出问题。但无线局域网不存在这样的问题。

由于无线局域网与传统的有线局域网相比，具有可移动性、用户接入灵活、保密性强、抗干扰性好、维护方便以及良好的性能价格比等特点，在变动频繁、成长快速、突发性以及不方便铺设网络的情况下，已成为用户的一种最佳选择方案，目前主要应用在以下几个领域。

（1）布线困难的场所：受地理环境影响的城市建筑群、学校校园网、老建筑或布线昂贵的江河湖泊、山区草原、港口码头等露天区域。

（2）变化频繁的环境：经常更换工作地点和变更位置的销售商、生产商、银行储蓄所、各类售票代理点等。

（3）临时组建的网络：大型会议、商业展览、建设工地等场所需要临时组建的局域网。

（4）流动作业的场合：适于野外勘测、实验、军事、公安的流动网络，以及需要在流动时得到信息的医护人员、零售商、白领阶层等。

（5）家庭办公室（SOHO）用户：用户需要方便快捷地安装小型网络。

未来无线局域网络的发展前景将更加广阔，其应用也不再局限于几个特殊领域，今后的应用主要如下。

（1）资源共享：无论何时何地都可以接入因特网来发送电子邮件，进行文件传输与终端仿真，共享世界各地的信息资源。

（2）办公自动化：外出职员可以接入到本单位的内部网，及时掌握生产经营管理情况，收发指令，实现移动办公。

（3）网络教学：学生可以通过便携式计算机接入大学校园网，选择学习内容，与老师进行交互式教学。

（4）金融财经：通过便携式计算机与无线局域网适配器可以接收到证券、期货最新信息，方便快捷地实现网上交易。

（5）医疗保健：随时掌握病人的动态信息，为病人提供高质量、高效率的保健服务。

（6）商业零售：顾客随时随地选购各类商品，服务商可以直接送达现场。

（7）生产制造：连接布线困难的生产车间，可收集现场生产数据传到公司网络。

（8）码头仓储：通过无线局域网建立动态数据库系统，随时了解货运信息，减少仓储库存，节约生产资金。

可以预见，随着开放办公的流行和手持设备的普及，人们对移动性访问和存储信息的需求愈来愈多，因而无线局域网将会在办公、生产和家庭等领域不断获得更广泛地应用。

1.5 未来的无线局域网

在 IEEE 802.11g 被发布之前，现有的无线局域网市场存在的两个标准并不相互兼容：