信息科学与技术丛书

信息安全系列

无线局域网络技术与安全

王顺满　陶　然　陈朔鹰　吴长奇　等编著

王　越　主　审

- 无线局域网结构与组成
- 无线局域网协议
- 无线局域网 PHY 层与 MAC 层
- 无线局域网设计与评估
- 无线局域网安全与措施
- 无线局域网技术走向

机械工业出版社
CHINA MACHINE PRESS

信息科学与技术丛书

信息安全系列

无线局域网络技术与安全

王顺满　陶 然　陈朔鹰　吴长奇　等编著

王 越　主审

机械工业出版社

全书分为基础篇、理论篇、实践篇、安全篇和展望篇，共 12 章。分别讲述与无线局域网络有关的基本概念、基本理论、技术标准、系统组成、设计方法、影响网络性能的各种因素、安全隐患与防范方法等内容，并在最后一篇对无线局域网的技术发展趋势进行了展望。

本书结构紧凑，内容简练，可作为通信工程、信息安全、电子对抗、电子工程、信息系统等专业本科生以及相关专业研究生的学习用书，也可以作为从事无线局域网及其安全问题分析及研究的工程技术人员的参考用书。

图书在版编目（CIP）数据

无线局域网络技术与安全/王顺满等编著. —北京：机械工业出版社，2005.9
（信息科学与技术丛书）
ISBN 7-111-17014-8

Ⅰ.无… Ⅱ.王… 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（2005）第 081580 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：胡毓坚
责任编辑：丁 诚
责任印制：杨 曦

北京蓝海印刷有限公司印刷

2005 年 9 月第 1 版·第 1 次印刷
787mm×1092mm 1/16·21.5 印张·521 千字
0001-5000 册
定价：33.00 元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话（010）68326294
封面无防伪标均为盗版

出 版 说 明

随着信息科学与技术的迅速发展，人类每时每刻都会面对层出不穷的新技术、新概念。毫无疑问，在节奏越来越快的工作和生活中，人们需要通过阅读和学习大量信息丰富、具备实践指导意义的图书，来获取新知识和新技能，从而不断提高自身素质，紧跟信息化时代发展的步伐。

众所周知，在计算机硬件方面，高性价比的解决方案和新型技术的应用一直备受青睐；在软件技术方面，随着计算机软件的规模和复杂性与日俱增，软件技术受到不断挑战，人们一直在为寻求更先进的软件技术而奋斗不止。目前，计算机在社会生活中日益普及，随着因特网延伸到人类世界的层层面面，掌握计算机网络技术和理论已成为大众的文化需求。由于信息科学与技术在电工、电子、通信、工业控制、智能建筑、工业产品设计与制造等专业领域中已经得到充分、广泛的应用，所以这些专业领域中的研究人员和工程技术人员越来越迫切需要汲取自身领域信息化所带来的新理念和新方法。

针对人们对了解和掌握新知识、新技能的热切期待，以及由此促成的人们对语言简洁、内容充实、融合实践经验的图书迫切需要的现状，机械工业出版社适时推出了“信息科学与技术丛书”。这套丛书涉及计算机软件、硬件、网络、工程应用等内容，注重理论与实践相结合，内容实用，层次分明，语言流畅，是信息科学与技术领域专业人员不可或缺的图书。

现今，信息科学与技术的发展可谓一日千里，机械工业出版社欢迎从事信息技术方面工作的科研人员、工程技术人员积极参与我们的工作，为推进我国的信息化建设作出贡献。

机械工业出版社

前　言

本书结合目前较为流行的无线局域网技术及信息安全问题在无线局域网系统中的重要性两个方面，对无线局域网的技术与安全问题进行了分析和阐述。本书对笔者近年来在无线局域网、信息安全、电子对抗、移动通信等学科领域的研究进行了归纳总结，同时也融合了许多无线局域网的先进技术与原理，力争使全书在论述过程中保持系统性和前瞻性的特点。

全书共分为 5 篇 12 章，第 1 篇为基础篇，由第 1 章和第 2 章组成，主要讲述了无线局域网的基本概念与基本组成。第 2 篇为理论篇，由第 3 章、第 4 章、第 5 章和第 6 章组成，分别讲述了无线局域网的技术标准、无线局域网物理层、扩频技术和介质访问层基本原理。第 3 篇为实践篇，由第 7 章、第 8 章和第 9 章组成，分别讲述了无线传输信道、无线局域网的干扰源与整体性能分析以及无线局域网的性能与测试等方面的内容。第 4 篇为安全篇，由第 10 章和第 11 章组成，主要讲述了与无线局域网安全有关的密码学理论和无线局域网安全问题及其解决方案。第 5 篇为展望篇，由第 12 章组成，主要从无线局域网的技术发展方向角度来对无线局域网的未来发展问题进行阐述。全书涉及的内容非常广泛，本科生、研究生和工程技术人员都能够从本书中获取希望学习的知识点。

本书非常注重基础理论的讲述，这是本书的一个特色。在讲述原理的过程中，注意将现象与物理内涵及数学逻辑推理进行有机结合，注意理论内容与实际工程的结合；注意严谨性与可读性的结合，使该书各章节的讲述细致而全面，相辅相成，浑然一体。

在本书的编写过程中，得到了许多同志和友人们的热情鼓励与帮助。王越院士为本书的撰写提出了许多宝贵意见，为本书的组织结构和整体写作思想提出了具体要求并对本书进行了审阅。陶然教授、陈朔鹰教授和吴长奇教授组织完成了相应章节的撰写工作并为本书提供了许多写作素材和建议。参加编写的还有王占禄、卢凤珍、许文权、姬桂霞、张颖、张文霞、马涛、罗国良、王磊、彭闻宇、郝彬、杨鼎才、王成儒、魏忠、杨帆等人。在此向所有对本书出版给以支持和帮助的友人们致以诚挚的谢意。

限于笔者的学识水平，本书缺陷和疏漏之处在所难免，恳请广大读者批评指正。

目　录

第1篇 基 础 篇

本篇主要针对无线局域网的基本知识进行概述性介绍。其内容主要包括：无线局域网发展史、无线局域网的组成、应用环境及其相关无线通信技术知识。本篇包括第1章和第2章。

第 1 章　网络知识概述

通过本章的学习，你将掌握如下内容：

- 网络发展史；
- 网络的基本概念；
- 无线网络的种类；
- 局域网的基本概念；
- 典型无线通信网络的基本原理。

通信网络技术是通信技术与计算机技术结合的产物。通信网络尤其是计算机网络技术，从产生到现在只有半个世纪，但是已经对人类产生了深刻的影响。计算机网络就是将功能彼此独立的多台计算机，以共享资源和传递信息为目的，利用通信线路（有线、无线）相互连接起来所构成的整体。

可以认为，计算机网络是通信网络大范畴中的一个子范畴。计算机网络按照通信范围的不同可以分为局域网（LAN）、城域网（MAN）和广域网（WAN）三类；按照网络的传输介质不同可以分为有线网和无线网，有线网所采用的传输介质主要为双绞线、同轴电缆和光纤，而无线网则主要以无线电波、卫星和红外线等作为其传输介质。我们要研究的无线局域网就是局域网中的一种，它所采用的传输介质是无线形式的。那么什么是局域网？什么是无线局域网？为什么要研究无线局域网？无线局域网的优缺点有哪些？采用什么样的技术？应用环境有哪些？我们将在随后论述中对上述这些问题逐一介绍。

1.1　局域网概述

1.1.1　局域网发展与特征

局域网是一种比较常用的计算机网络，我们常说的以太网就是局域网的一个典型代表网络。局域网具有如下特点：

- 覆盖范围小。一般来讲，局域网都是被限定在一个比较小的范围内，其覆盖范围可能是一间办公室、一个公司、一个部门或者一个学校，等等。局域网的通信范围一般被限定在 0.1～25km 之间。
- 传输速度高。相对于广域网而言，有线方式的局域网数据传输速度要远高于广域网，现在已经出现了千兆以太网，而广域网的数据传输速度就要慢得多。目前局域网的数据传输速率一般为 10Mbit/s，光纤分布式数据网络（FDDI）的数据传输速率为 100Mbit/s，而广域网（WAN）的主干线速率国内仅为 64Kbit/s 或 2.048Mbit/s。无线局域网的数据传输速率相比有线网络要低得多。
- 差错率低。相对于广域网而言，有线局域网的数据传输差错率非常小，一般来讲，

局域网的差错率为 10^{-8}～10^{-11}。

- 安全性高。有线局域网的通信范围一般被限定在一个固定的范围内，对其进行安全防护相对广域网和城域网要容易一些，可以利用防火墙、入侵检测、系统日志以及防病毒等措施对局域网进行安全防护。
- 扩展性强。局域网的终端用户可以根据需要进行适当调整，不需要特别多配置。相对而言，其扩展性比广域网要强。

上面是局域网相对于广域网的一些性能比较，关于有线局域网与无线局域网之间的详细比较，将在随后的内容中加以讲述。

1.1.2 局域网的基本组成

一般而言，局域网必须能够将各终端设备连接起来，所以各终端设备就是构建局域网的基本设备；其次，如果要构建局域网，那就必须要将各台彼此功能独立的计算机进行连接，因此，需要各种连接介质，这些连接介质包括同轴电缆、双绞线、光纤和无线电波等；另外，在局域网中还需要使用专用的网络连接设备，如网卡、集线器、RJ-45 插头和发射天线等；最后，还需要具有网络操作系统和局域网内部的网络管理软件等相关软件的支持。

1.1.3 局域网的网络拓扑结构

拓扑结构是从拓扑学（topology）中引申出来的一个专业术语。网络拓扑结构指的是各种终端设备与各种传输媒体之间的物理布局。将各种终端设备模拟成“点”，将各种传输介质模拟成“线”，则这些点和线所组成的网络结构称为网络的拓扑结构。在有线局域网中，主要采用总线型、星型和环型拓扑结构，另外还包括网型和树型拓扑结构等。

1. 总线型拓扑结构

在总线型拓扑结构中，物理介质是由所有终端设备所共享的，其结构如图 1-1 所示。使用这种结构的局域网必须要解决的一个问题就是要通过特定的机制来确保终端用户在使用传输介质发送数据的时候不会发生冲突。因为在局域网中，各终端设备的地位都是平等的，终端设备可以独立地获取网络资源，因此必须要在局域网中制定一种既能共享传输线路又能够避免冲突的信道管理机制。在局域网中的介质访问控制机制就是带有冲突检测的载波侦听多路访问机制，简称为 CSMA/CD。

总线型网络拓扑结构具有费用低、数据端用户接入灵活、安全性高、可靠性高、扩展性强等诸多优点，因此总线型网络是局域网中一种比较普遍的网络拓扑结构，也是应用最为广泛的一种网络拓扑结构。

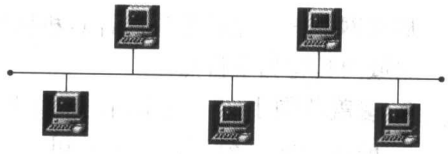

图 1-1 总线型拓扑结构

2. 星型拓扑结构

星型拓扑结构是最古老的一种局域网连接方式，如图 1-2 所示。在这种拓扑结构中，以中心节点为中心，将各终端设备连接在一起。由于各种中心节点的不同，局域网的物理拓扑结构和逻辑拓扑结构也随之不同。其中集线器的作用相当于一个多端口中继器，数据从一个端口进入之后，集线器会将这些数据通过其他所有端口广播出去，这种连接法方式的特性就相当于总线型连接方式，因此可以认为其物理拓扑结构为星型，而逻辑拓扑为总线型。当中

心节点的设备为交换机时，整个结构才能叫做星型拓扑结构。10BASE-T 就是星型拓扑结构的一种应用。

星型拓扑结构的特点是便于实现集中控制，因为终端用户之间的通信必须要经过一个中心节点来实现。因此这种结构的网络也具有易于维护和安全性高等优点。各台终端用户设备的故障或者死机都不会影响其他终端用户之间的通信；但是在这种结构中，有一点是需要我们注意的地方，就是要求中心节点设备的可靠性必须非常高，一旦中心节点设备发生了故障，就将导致整个系统的瘫痪。因此需要对此中心系统采用双机热备份的方式来提高系统的可靠性。

3. 环型拓扑结构

环型拓扑结构在局域网中也是使用比较多的一种连接方式，如图 1-3 所示。在这种结构中，传输介质将所有终端用户连接在一起，组成一个环型结构网络，同时各终端设备都必须要使用相同的网络适配器来与传输介质进行连接；在环型拓扑结构中，数据将按照一个固定方向进行传输，不论是顺时针还是逆时针，都只能按照一个方向进行。相对于星型结构的局域网来讲，其控制部分都被分散到各终端机器上，这样就消除了各终端用户对中心节点的依赖性。

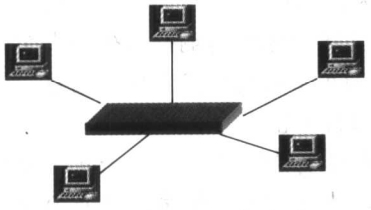

图 1-2　星型拓扑结构

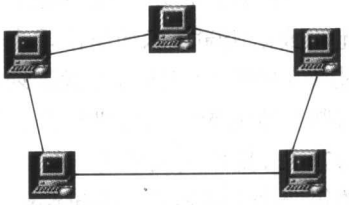

图 1-3　环型拓扑结构

4. 树型网络拓扑结构

树型拓扑结构也是局域网中的一种网络连接方式，如图 1-4 所示。这种网络拓扑结构的特点是：按层次进行连接以及信息交换仅在上下保持连接的两层实现。

5. 网状网络拓扑结构

网状拓扑结构在局域网中也有使用，如图 1-5 所示。这种网络拓扑结构的特点是：网络各节点可以任意连接；系统具有高可靠性；网络结构复杂，维护困难。

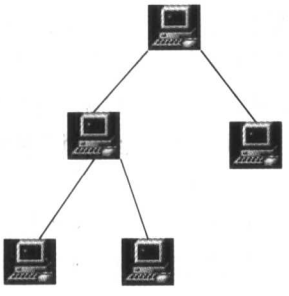

图 1-4　树型拓扑结构

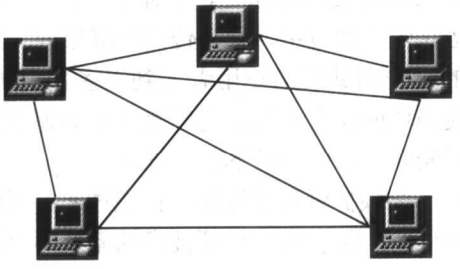

图 1-5　网状拓扑结构

1.2 无线局域网发展史

通过前面的讲述我们知道，在局域网领域中，按照传输介质的不同可以分为有线局域网和无线局域网，这两种网络也就是我们常说的 LAN 和 WLAN。以前我们常将局域网的概念限制在有线网络的范围内，但是随着无线方式和移动方式应用的不断增多，需要我们对无线局域网的概念与特性等有一个更为明晰的了解。因此我们首先要介绍一下与无线局域网有关的基本概念和无线局域网的发展史。

无线局域网（WLAN：Wireless Local Area Network）是指以无线信道来代替传统线传输介质所构成的局域网络。无线局域网是在有线网络的基础上发展而来的，WLAN 的出现能够使网络上的各种终端设备摆脱有线连接介质的束缚，使其具有更多的移动性，并能够实现与有线网络之间的互连和互通。

无线局域网也有广义与狭义之分。狭义无线局域网技术通常指的是我们常说的 WLAN，狭义无线局域网的内容包括 IEEE 802.11 系列标准和 HiperLAN1。而广义无线局域网的范围就要广泛得多，除了上述的 IEEE 802.11 系列标准和 HiperLAN1 标准之外，还包括无线个人局域网（WPAN）和以 IEEE 802.16 和 HiperLAN2 标准为代表的宽带无线接入技术等。

无线数据传输技术最早出现在第二次世界大战中，当时的无线传输技术被用于军队作战时越过敌人的防线来传送作战计划等军事行动信息。因为军事行动信息是保密信息，所以需要对这些传输的无线信号进行安全加密，以防止军事情报被泄密。

1971 年，夏威夷大学的一些研究人员创建了第一个无线电通信网络。由 Norman Abramson 开发的第一个无线网络 AlohaNet 于 1971 年投入运行，当时的数据传输速率为 9.6Kbit/s。AlohaNet 实际上是第一个无线网络，尽管它的发展经过了很长的一段时间。AlohaNet 是个无线广域网（WWAN），由双向星型拓扑结构连接的计算机组成，其卫星和陆地无线电传输协议也是以 Aloha 命名的。移动终端可以在任意时间传输信息，但是如果在同一时刻有多个终端要同时进行传输的话，那么这些终端之间就可能会发生冲突。减少冲突的一种方法是将信道划分为多个时隙并且要求所有终端设备只有在时隙开始的时候传输数据。

以太网的发展经历了跳跃式的飞速发展过程。以太网的效率比较高，数据传输速度也比较快，但是它必须使用物理传输线路作为其传播介质。无线网络则将以太网的可靠性、高速性与无线数据网络的优点恰如其分地结合在了一起。

无线局域网虽然具有很多灵活性和其他方面的优点，但是直到 1994 年，WLAN 才首次在商业运作中得到应用，且其传输速度很低（12Mbit/s），工作频段为 900MHz。这些因素导致早期的无线局域网的使用者受到很多数据传输速度方面的限制。除了数据传输速率低以外，无线局域网还存在彼此之间兼容能力差等方面的问题。不同厂家的无线局域网系统之间可能会不兼容，原因有以下三个方面。

第一，跳频扩频和直接序列扩频技术是无线局域网最常用的技术，但是这两种技术是不会同时工作的，基于跳频扩频技术的系统不可能与另外一个基于直接序列扩频技术的系统进行通信。

第二，即使两个系统都采用了相同的技术，但由于各自工作在不同的频带上，也是不能互通的。如果两个系统不是在同一个信道上工作，那么无线网络中的接入点和无线网卡也是