无线局域网及其对抗技术

鲁智勇　熊志昂　李志勇　等编著
陈永光　主审

国防工业出版社
National Defense Industry Press

无线局域网及其对抗技术

鲁智勇　熊志昂　李志勇　等编著
陈永光　主审

国防工业出版社
·北京·

图书在版编目(CIP)数据

无线局域网及其对抗技术/鲁智勇等编著. —北京：国防工业出版社，2006.1

ISBN 7-118-04278-1

Ⅰ. 无… Ⅱ. 鲁… Ⅲ. ①无线电通信—局部网络—基本知识②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 150617 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 100044)

京南印刷厂印刷

新华书店经售

*

开本 850×1168 1/32 **印张** 13 **字数** 341 千字

2006 年 1 月第 1 版第 1 次印刷 **印数** 1—4000 册 **定价** 25.00 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

网络及其对抗技术的迅速发展使战争加速进入信息化时代，计算机网络对抗已经成为一种重要的战争样式。可以肯定，随着新军事革命的纵深发展、武器装备信息化程度的提高，以及数字化部队的闪亮登场，网络空间上的斗争将更加激烈，这一切极大地刺激了网络攻防对抗装备的迅速发展，对这种特殊装备的研制必将成为武器装备发展的重要内容。

网络战（Network-Warfare）是指在国际互联网及其他网络上，利用计算机技术侦察、获取、干扰、破坏敌方指挥系统、武器系统及人事、组织、后勤等系统中的重要信息，进行思想、文化渗透，从而影响、加速甚至决定战争进程的高技术行为。它以信息技术为支撑、以网络为载体，可使作战双方在互不见面的条件下遂行作战。而作战样式从“以平台为中心”逐渐转向以“网络为中心”。计算机及其网络将传感器、指挥控制系统和火力系统紧密连接起来，使得以往主要依靠平台自身探测器、武器和平台之间难以共享信息的所谓“以平台为中心”的作战模式，转向借助“网络平台”（利用网络将分散的传感器、指挥控制中心及主战武器等连接在一起）、实施联合作战的所谓以“网络为中心”的作战模式。这种转变必将大大拓宽战场空间，加速战争进程。

现阶段，我军指挥控制系统内部及系统与系统之间的互联互通多采用有线和无线两种方式，因此，进行无线局域网的原理、协

议、网络防御和攻击技术的研究对于提高我军武器装备的战场网络生存能力，夺取未来高技术战争的“制信息”、“制网络”权，将起到一定的推动作用。

本书作者近些年一直致力于C^3I系统对抗和网络对抗技术的研究与应用，取得了一些研究成果。在撰写此书的过程中，查阅了大量的文献和资料，并将近几年来我们在理论和工程应用的成果融入到有关章节中。编写本书的目的是促进无线局域网新技术的应用，同时也为无线局域网安全防护技术的研究和开发提供应用思想和可操作性技术。

本书由鲁智勇、熊志昂、李志勇、李学蔷、张部生、朱峰共同策划编著，该书的完成体现了团队精神。宝国辉、周磊等在本书的编写工作中查阅、翻译、提供了大量的资料，同时也为文稿的最终完成和校对工作付出了辛勤的劳动。国防工业出版社汪淳编辑对本书的编著和出版给予了极大的支持，63880部队的陈永光研究员、总参54所的吕跃广研究员审阅了本书，提出了宝贵的意见，在此表示诚挚的感谢。

由于无线局域网对抗是一个崭新的领域，涉及的内容范围又比较广，书中难免有不妥之处，敬请广大读者提出宝贵意见，并给予批评指正。

作　者

2005年10月

目　录

第1章　无线局域网概述

20世纪90年代以来，移动通信和Internet是信息产业发展最快的两个领域，它们直接影响了亿万人的生活，大大地改变了人类的生活方式。移动通信使人们可以任何时间、任何地点和任何人进行通信，Internet使人们可以获得丰富多彩的信息。那么，如何把移动通信和Internet结合起来，达到可以任何人、任何地方都能联网呢？无线网络的出现解决了这个问题。

无线局域网是计算机网络与无线通信技术相结合的产物。通俗点说，无线局域网（Wireless Local-Area Network，WLAN）就是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，网络所需的基础设施不需要再埋在地下或隐藏在墙里，网络却能够随着实际需要移动或变化。无线网络的出现解脱了线路的束缚，和传统的有线网络相比，无线网络有着高移动性、低成本、方便快捷等传统有线网络无可比拟的优点。无线网络和个人通信网（PCN）代表了21世纪通信网络技术的发展方向。PCN主要用于支持速率小于56kb/s的语音/数据通信，而无线网络主要用于传输速率大于1Mb/s的局域和室内数据通信，同时为未来多媒体应用（语音、数据和图像）提供了一种潜在的手段。

无线局域网技术具有传统局域网无法比拟的灵活性。无线局域网的通信范围不受环境条件的限制，网络的传输范围大大拓宽，最大传输范围可达到几十千米。在有线局域网中，两个站点的距离在使用铜缆时被限制在500m，即使采用单模光纤也只能达到3000m，而无线局域网中两个站点间的距离目前可达到50km，距离数千米的建筑物中的网络可以集成为同一个局域

网。

此外，无线局域网的抗干扰性强、网络保密性好。对于有线局域网中的诸多安全问题，在无线局域网中基本上可以避免。而且相对于有线网络，无线局域网的组建、配置和维护较为容易，一般计算机工作人员都可以胜任网络的管理工作。

无线网络到现在已经有了 40 年的历史，其产品标准刚刚制订完成。当前，无线网络正在迅速膨胀，人们已开始领略到无线联网技术的无穷魅力。可以预见，在不久的将来，无线网络将会取得长足的进步，得到广泛的应用和发展。

1.1 无线局域网基础知识

1.1.1 无线局域网起源和发展

无线网络通信系统的发展历程，大体上可以分为 3 个阶段。第一代(1G)系统是面向语音的模拟蜂窝和无绳电话。第二代(2G)无线网络是面向语音的数字蜂窝、PCS 系统和面向数据的无线 WAN 和 LAN。第三代(3G)无线网络把蜂窝电话和 PCS 语音业务用各种分组交换数据业务综合在一个统一的网络中。目前正在广泛使用的是第二代(2G)无线网络。

第一代模拟蜂窝系统。从 20 世纪 80 年代起，利用模拟传输方式实现语音业务的移动系统开始在欧美盛行，有几种标准得以发展，如：美国的 AMPS(先进的移动电话业务)、英国的 TACS(全接入通信系统)等。

第二代数字移动通信系统。1991 年，利用数字传输方式的移动通信系统投入使用。它们能提供更高的频谱利用率、更好的数据业务以及比第一代系统更先进的漫游。GSM(全球移动通信系统)、PDC(个人数字蜂窝)、CDPD(移动数字分组数据)都属于第二代系统。GSM 采用电路交换数据业务，由于网络通话质量较差，频繁掉线和数据传输的低速率，使得它无法满足移动通信用户的需求，研发具有高通话质量、高传输速率的新一代移动通信网络

成为解决这一问题的惟一途径。

在第二代向第三代演变的过程中出现了2.5代通信系统，如GPRS(General Packet Radio Service)通用分组无线业务，它是在现有GSM网络上开通的一种新型分组数据传输业务。早期的电路交换数据业务，传输速率为9.6kb/s，而GPRS可以达到115kb/s。它不仅具有速度上的优势，而且还能做到“永远在线”，即用户可随时与网络保持联系，使得用户有专线上网的感觉。另外，GPRS是按流量计费的，有“发呆免费”之称，浏览网页的时候就是“打瞌睡”，也不用花钱。利用GPRS可以聊天、浏览网页、收发电子邮件、结合卫星定位系统实现汽车定位和非语音移动服务等。中国移动的GPRS业务已于2001年7月开始在全国16个省25个城市投入试用，容量达到40万户。

第三代多媒体移动通信系统，又称为3G，最早于1985年由国际电信联盟(ITU)提出。当时称为未来公众陆地移动通信系统(FPLMTS)，1996年更名为ITM-2000(国际移动通信-2000)。它利用卫星移动通信网与地面移动通信网的结合，形成一个对全球无缝覆盖的立体通信网络，满足城市和偏远地区不同密度用户的通信需求，支持语音、数据和多媒体业务，提供高达2Mb/s的宽带数据业务。经过几年的技术评估、研究分析及大量的协调和融合工作之后，1999年底，国际电信联盟(ITU)认可了3种3G标准，它们是欧洲提出的W-CDMA、北美提出了CDMA2000和中国提出的TD-SCDMA，第三代移动通信系统主要采用这3种CDMA技术，它们的出现标志着第三代无线移动通信技术的格局被最终确定。

与统一的3G标准并列存在的宽带局域网与Ad Hoc网络也吸引了更大的注意力，并且为之开发了自己的标准。当前这两种网络在频段上的主要区别是3G系统使用需要许可证的频段，而宽带局域网与Ad Hoc网络使用免许可证的频段。使用免许可证频段接入宽带局域方式和需要许可证的3G标准可以结合起来共

同形成下一代无线网络的核心。

1.1.2 面向数据无线网络的发展

表1-1给出了面向数据的无线网络发展的主要年代表。面向数据的无线网络分为广域无线数据网络和宽带无线局域网与Ad Hoc网络。无线局域网支持较高的数据速率，而Ad Hoc工作在用户数量较少的场合。宽带无线局域网通常是指WLAN，而Ad Hoc局域网是指WPAN。WLAN的概念是在1980年左右被首次推出的，而第一个WLAN产品却是在10年以后才完成。现在的宽带无线局域网和Ad Hoc网的一个主要特点是工作在免许可证的频段。第一个免许可证的频段是ISM频段，它是由美国在1985年发布的。随后在1994和1997年，美国又发布了免许可证的PCS频段和U-NⅡ(免许可证的国家信息基础结构)频段。WLAN的主要标准是IEEE 802.11，该标准从20世纪80年代末期开始研究，到1997年完成。IEEE 802.11和802.11b标准运行在ISM频段，而IEEE 802.11a标准运行在U-NⅡ频段。欧洲在WLAN上参与竞争的标准是高性能无线局域网(HIPERLAN)。HIPERLAN-1于1997年完成，HIPERLAN-2现在还在研究中。1996年，异步传输模式(ATM)论坛的无线ATM工作组成立，它立足于把ATM技术与宽带局域接入技术相结合。近几年，随着蓝牙技术在1998年公布之后，WPAN获得了巨大的关注。WPAN的覆盖范围比传统的WLAN要小，WPAN的目的是用于ad hoc场合，把个人设备(如膝上电脑、手机和耳机)连接起来。在写本书的时候，IEEE 802.11产品每年可获得10亿美元的收入。在过去的几年中，全世界在WLAN和WPAN芯片组的研究上进行了大量的投资。这些投资期望从有可能并入蜂窝移动行业的WLAN中和WPAN所拥有的巨大用户产品与家庭网络市场中获得巨大收入。

首次移动数据服务是由摩托罗拉和IBM在1983年推出的

表 1-1　面向数据的无线网络的发展

年	事　件
1979	普及红外线(IBM Rueschlikon 实验室,瑞士)
1980	使用 SAW 设备扩展频谱(HP 实验室,加利福尼亚)
20 世纪 80 年代初期	无线调制解调器(数据无线通信)
1983	ARDIS(摩托罗拉/IBM)
1985	SM 频段用于商业扩频应用
1986	Mobitex(瑞典电信和爱立信)
1990	无线局域网标准 IEEE 802.11
1990	RAM 移动产品发布
1991	RAM 移动(Mobitex)
1992	组成 WIN Form
1992	欧洲的 ETSI 和 HIPERLAN
1993	欧洲发布 2.4GHz、5.2GHz 和 17.1GHz～17.3GHz 频段
1993	CDPD(IBM 和 9 家运营公司)
1994	PCS 的需要许可证频段和免许可证频段
1996	无线 ATM 论坛创立
1997	发布 U-NⅡ频段、IEEE 802.11 完成、GPRS 出现
1998	推出 IEEE 802.11b 和蓝牙技术
1999	IEEE 802.11a/HIPERLAN-2 出现

ARDIS(现在称为 DATATAC)项目。ARDIS 的目的是使 IBM 的全体人员无论在何地都可以使用便携式计算机来传输业务。1986 年爱立信推出 Mobitex 技术,它是一种 ARDIS 的开放式体系结构实现。1993 年,IBM 和美国的 9 家运营公司开始推出 CDPD(蜂窝数字分组数据)项目,希望能在 2000 年获得巨大的市场。在 20 世纪 90 年代后期,把 GPRS(通用分组无线业务)数据业务结合在已经取得成功的 GSM 系统中,可以获得比原来的技术高得多的速率等级,这吸引了很多人的注意力。较高的数据速率对于最流行的无线数据应用即无线 Internet 接入而言,是必不可少

的。第三代(3G)蜂窝移动通信系统计划提供 2Mb/s 的移动数据服务,这显然高于 GPRS 的数据速率。然而,这种数据速率并没有 GPRS 那样广泛的覆盖范围。早期的移动数据网 ARDIS 和 Mobitex 是独立的网络,有自己的基础结构。随后的 CDPD 是在 AMPS 系统之上扩展它的基础结构,而 GPRS 实际上是与 GSM 的基础结构相结合。这种蜂窝电话行业逐渐吸收移动数据行业的过程会在下一代蜂窝系统中完成。

随着 PCS 和移动数据行业在下一代蜂窝系统中的结合,我们将会看见两个产业的出现:工作在需要许可证频段的下一代传统蜂窝系统和工作在免许可证频段的宽带局域与 Ad Hoc 网络。

1.1.3 无线局域网的主要协议标准

无线接入技术区别于有线接入的特点之一是标准不统一,不同的标准有不同的应用。无线局域网采用的标准有很多,目前比较流行的有 802.11 标准(包括 802.11a、802.11b 及 802.11g 等标准)、蓝牙(Bluetooth)标准以及 HomeRF(家庭网络)标准、HIPER LAN2 标准等。

1. 802.11 家族

IEEE802.11 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。它也是目前最常用的无线局域网传输协议。802.11 标准除了使得各种不同厂商的无线产品得以互联之外,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。它是无线局域网目前最常用的传输协议,各个公司都有基于该标准的无线网卡产品。802.11 在该标准中 RF 传输标准是跳频扩频(FHSS)和直接序列扩频(DSSS),工作在 2.4000GHz ~2.4835GHz 频段。在 MAC 层则使用载波侦听多路访问/冲突避免(CSMA/CA)协议。802.11 标准主要用于解决办公室局域网和校园网中,用户与用户终端的无线接入,业务主要限于数据存

取，速率最高只能达到 2Mb/s。1999 年 8 月，已经修订了 802.11 标准成为 IEEE/ANSI 和 ISO/IEC 的一个联合标准，ISO/IEC 将该标准定为 ISO8802－11。由于 802.11 在速率和传输距离上都不能满足人们的需要，因此，IEEE 小组相继推出了 802.11b、802.11a 和 802.11g 标准。

1) IEEE 802.11b

IEEE802.11b 于 1999 年底制定，以直接序列扩频(DSSS:Direct Sequence Spread Spectrum)作为调制技术，即采用与信息无关的随机序列表示原来的信号，使得原来高功率、窄带的信号的功率降低，宽带展宽。802.11b 标准采用一种新的调制技术，使得传输速率能根据环境变化，它采用 2.4GHz 直接序列扩频，最大数据传输速率为 11Mb/s，无须直线传播。当射频情况变差时，动态速率转换可将数据传输速率降低为 5.5Mb/s、2Mb/s 和 1Mb/s；支持的范围是在室外为 300m，在办公环境中最长为 100m。802.11b 使用与以太网类似的连接协议和数据包确认，来提供可靠的数据传送和网络带宽的有效使用。

802.11b＋是一个非正式的标准，称为增强型 802.11b。802.11b＋与 802.11b 完全兼容，只是采用了 Packet Binary Convolutional Coding(PBCC)数据调制技术，所以能够实现高达 22Mb/s 的通信速率，完全适用于数字图像、视频、MP3 等多媒体文件的传输。

2) IEEE 802.11a

802.11a 标准是已在办公室、家庭、宾馆、机场等众多场合得到广泛应用的 802.11b 无线局域网标准的后续标准。802.11a 标准的传输更惊人，传输速度可达 54Mb/s，完全能满足语音、数据、图像等业务的需要。可在更多的应用中使用，曾一度被视为下一代高速无线局域网络规格，IEEE802.11a 选择具有能有效降低多重路径衰减与有效使用频率的 OFDM 为调制技术，同时选择工作于干扰较少的 5GHz 频段。

与以前相比，现在对安全性和互操作性有了更大的需求，这也