“十一五”重点规划教材
高等学校计算机及其应用系列

无线局域网安全分析与防护

主　编　李贤玉　吴小华
副主编　贺　晖　郑建群　李晓坤
王　山　刘培涛

重点规划教材

哈尔滨工程大学出版社
Harbin Engineering University Press

无线局域网安全分析与防护

李贤玉　吴小华　主编

哈尔滨工程大学出版社
Harbin Engineering University Press

内容提要

近几年来，随着无线技术的迅猛发展，无线局域网（WLAN）得到了广泛的应用。无线局域网由于其自由组网快捷、使用方便和成本低等优势而备受青睐。但是其通信内容因具有公开性而极易被攻击者获得，因此无线局域网的安全问题变得十分突出。

本书从无线局域网的组成和应用环境出发，结合 Internet 系统的体系结构，按照密码学的基本原则对无线局域网 IEEE 802.11 标准的安全机制，结合相应的安全技术原理的论述，进行了深度分析，指出了现有的无线局域网 IEEE 802.11 标准自身的安全防护机制和常用无线局域网的安全策略所存在的安全缺陷或漏洞，为便于说明问题，本书介绍了一些常见的、针对这些安全缺陷和漏洞的攻击方法和技术，旨在通过这些缺陷分析来说明无线局域网络目前存在的潜在安全隐患，并且提出较好的无线局域网络安全解决方案，以促进网络安全管理员给出更好的网络防护方案，加强无线局域网络的安全防护意识和能力。

图书在版编目（CIP）数据

无线局域网安全分析与防护/李贤玉，吴小华主编.
哈尔滨：哈尔滨工程大学出版社，2009.1
ISBN 978-7-81133-387-9
Ⅰ.无… Ⅱ.①李…②吴… 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（2009）第 005152 号

出版发行：哈尔滨工程大学出版社
社　　址：哈尔滨市南岗区东大直街 124 号
邮　　编：150001
发行电话：0451－82519328
传　　真：0451－82519699
经　　销：新华书店
印　　刷：北京市通州京华印刷制版厂
开　　本：787mm×1092mm　1/16
印　　张：13
字　　数：248 千字
版　　次：2009 年 1 月第 1 版
印　　次：2009 年 1 月第 1 次印刷
定　　价：28.00 元
http：//press.hrbeu.edu.cn
E-mail：heupress@hrbeu.edu.cn

无线局域网安全分析与防护

编 委 会

主　编： 李贤玉　吴小华

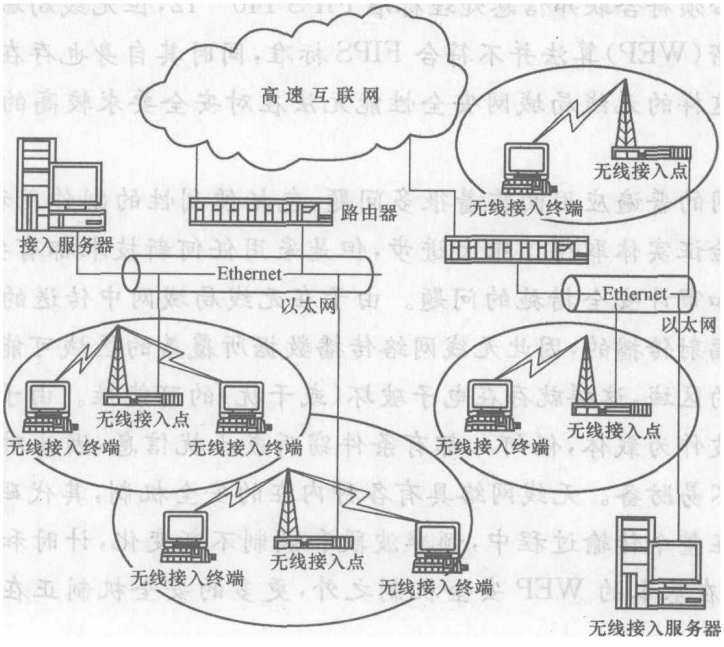
副主编： 贺　晖　郑建群　李晓坤

王　山　刘培涛

前言

个人通信的目标，就是使人们能够在任何时候和其他任何人进行任意的通信联系，自由地享用网络提供的多种业务。宽带无线 IP 技术将目前最热门的两大技术——IP 技术和无线通信技术有机地融合起来，并顺应宽带化的发展趋势，为移动主机或移动终端提供方便、快捷、高速的 Internet 接入服务，以适应人们对高速网络和多媒体通信业务不断增长的需求。

无线局域网（Wireless Local Area Network，WLAN）不仅支持移动计算，而且具有灵活性、快捷性及可扩展性等优点。以无线局域网为基础，基于 Internet 的宽带无线接入网络结构如下图所示。它主要由移动终端（Mobile Terminal，MT）、无线接入点（Access Point，AP）及无线接入服务器（Wireless Access Server，WAS）等设备组成，其中移动终端 MT 可在网中任意移动，无线接入点 AP 可实现包括越区切换在内的小区管理、对移动终端 MT 的管理及桥接功能，无线接入服务器 WAS 可实现无线接入终端的网间漫游管理。从固定接入 Internet 到移动无线接入 Internet，宽带无线 IP 技术为世界网络环境带来了全新的观念和巨大的冲击。



基于 Internet 的宽带无线接入网络结构示意图

近年来，随着无线通信技术的发展，无线局域网因其便利的安装、使用，高速的接入速度，可移动的接入方式等优点，已经有了非常广泛的应用。无线局域网解决方案提供了在有限覆盖区域内的无线连接，可以支持典型办公台式电脑或家用台式电脑与其他网络资源的通信。随着网络时代的发展，无线局域网络的规模和应用领域不断发展，已经渗透到经济、军事、科技与教育，以及人们的日常生活等各个领域，其基础性、全局性的地位和作用日益增强。

由于无线电通信特殊的辐射性质，无线空间传播通道的开放性导致其存在多种不安全因素，非法用户在接收到无线信号的任何地方都可以发起对无线局域网的攻击，无须授权即可使用网络服务，这不仅会占用宝贵的无线通道资源，增加带宽费用，降低合法用户的服务质量，而且别有用心的人还可以利用这一漏洞进入到局域网内部窃取机密。这对于正在高速发展的中国计算机网络来说是一个巨大的安全隐患。

事实上，中国无线局域网市场经过多年的发展，目前已经进入一个比较务实、讲求满足商用需求与回报、可运营可盈利的市场阶段。但是，无论是对于运营商还是企业、行业市场，安全问题都是导致无线局域网市场无法发展企业、行业高端客户的第一道屏障。2004 年以来，中国乃至全球无线局域网市场结构和利润空间的低迷，除却新技术标准发展对投资者信心的影响外，国际标准安全方案较差的易用性和安全性，以及各厂商补救方案的兼容性问题都是无线局域网本身迟迟不能打入高端用户市场，进而导致产业结构升级困难的根本原因。例如，美国政府要求所有部门采用的无线设备必须符合联邦信息处理标准 FIPS 140—12，但无线局域网国际标准中的有线等价保密(WEP)算法并不符合 FIPS 标准，同时其自身也存在“根本性的、系统性的缺陷”，这样的无线局域网安全性能无法在对安全要求较高的政府和行业市场得到认可。

无线局域网的普遍应用面临着很多问题，包括便利性的副作用和安全问题，虽然安全标准和验证实体取得了很大进步，但是采用任何新技术都有安全风险，而且存在如何应用和审计安全措施的问题。由于在无线局域网中传送的数据是利用无线电波在空中辐射传播的，因此无线网络传播数据所覆盖的区域可能会超出一个组织物理上控制的区域，这样就存在电子破坏(或干扰)的可能性。由于无线局域网采用公共的电磁波作为载体，任何人都有条件窃听或干扰信息，因此对越权存取和窃听的行为也更不易防备。无线网络具有各种内在的安全机制，其代码清理和模式跳跃是随机的。在整个传输过程中，频率波段和调制不断变化，计时和解码采用不规则技术。目前，在基本的 WEP 安全机制之外，更多的安全机制正在出现和发展之中。

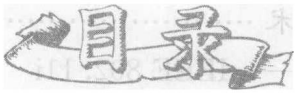
作为重要基础技术与设施的无线局域网络的安全问题已经成为影响社会经济

发展的重要因素，是当前世界各国共同关注的焦点。维护网络安全的原则是维护数据与计算机资源的机密性、完整性和可用性。无线局域网的普遍应用要求防止用户之间的通信受到有意或无意的未经授权的访问，保证用户信息在处理过程中的准确性和完备性，并确保用户可以实时访问的资源或数据是可靠的和可用的。然而面对无线局域网络日趋多样化的结构和多样化的应用，特别是随着无线网络攻击和破坏行为的日益频繁和攻击工具的逐渐多样化，传统的无线局域网络安全防护及其研究已经不能满足无线网络发展的实际需求。

无线局域网络安全的研究工作很早就受到了人们的关注，其发展主要经历了三个阶段。在第一阶段，人们试图构建绝对安全的系统，主要研究如何保护无线局域网络系统不被恶意入侵，并且普遍认为无线局域网络安全事件发生是由于系统设计上存在漏洞，可以通过系统细节的改进和复杂协议的设计来阻止攻击和避免安全破坏事件的发生。在第二阶段，人们逐渐认识到有一部分恶意入侵很难阻止其发生，因此将注意力转移到如何及时检测入侵的发生，并提醒管理员采取补救措施，如打补丁等。事实证明，要保证网络的绝对安全是非常困难的，特别是在网络攻击日益普遍和加剧的情况下，网络攻击和入侵不可避免且对其很难及时检测和发出报警。在第三阶段，人们更多地考虑无线网络的容侵容错，即研究如何使无线网络在受到攻击和破坏后仍能恢复且继续实现预定功能。

鉴于当前无线网络安全领域存在的严峻问题，为用户提供系统级的安全服务已经逐渐成为无线网络安全领域发展的新趋势，而对无线网络的安全缺陷以及安全解决方案的研究也已经成为国内外研究的热点。

本书针对当前无线局域网络安全领域存在的诸多问题，在无线网络安全解决方案方面作了一些积极而有意义的探索研究，详细介绍了无线局域网络安全的基本知识和防护机制，并在此基础上对 WEP 协议安全机制、IEEE802.11b 协议安全机制以及无线局域网络存在的缺陷和漏洞进行了分析，列举出了一些针对这些安全机制常见的攻击方法，并就这些攻击方法给出了有针对性的无线局域网络安全解决方案，旨在帮助广大无线局域网络的使用者构建起有效的网络安全体系，以有力地抵御各种恶意网络攻击，提高无线局域网络领域的安全性。



前 言

第1章 无线局域网络概述

第2章 信息安全入门

第3章 无线局域网安全防护机制

第6章 针对WEP协议安全机制的攻击

第7章 针对IEEE 802.11b协议安全机制的攻击

第8章 针对无线局域网络的攻击

第9章 无线局域网络综合安全解决方案

第10章 结束语

第1章 无线局域网络概述

1.1 无线局域网简介

人们生活在“移动”的世界中，越来越多的移动产品的出现，标志着人们对快捷数据访问的需求在不断增加。近年来计算机局域网得到了很大的发展与普及，局域网已成为提高工作效率及生产率不可缺少的工具。通过无线局域网可以实现许多新的应用，这表明无线局域网的时代已经来临。

无线局域网提供了在有限覆盖区域内的无线连接。覆盖范围通常是指以基站或者 AP（Access Point）为中心，半径在 10～100m 的区域。无线局域网提供了支持典型办公台式电脑或者家用台式电脑与其他网络资源通信的必要功能。这种情况下的数据流通常由远程应用程序访问和文件传输构成。无线局域网为无线通信网络节点提供了与有线局域网络资源对接的方案。这样就出现了有线通信网络节点与无线通信网络节点可以交互的混杂型网络。

由于无线局域网潜在的市场规模巨大，许多制造商都在致力于无线局域网的研究与开发。为使无线局域网产业健康发展，欧美日等发达国家及有关国际标准化组织都已经或正在制定有关无线局域网的法规与标准。在 20 世纪 80 年代，伴随着以太局域网的迅猛发展，无线局域网以不用架线、灵活性强等优点，赢得了特定市场的认可，但也正是因为当时的无线局域网是作为有线以太网的一种补充，遵循了 IEEE 802.3 标准，使直接架构于 802.3 上的无线局域网络产品存在着易受其他微波噪声干扰、性能不稳定、传输速率低且不易升级等缺点，不同厂商的产品相互也不兼容，这一切都限制了无线局域网的进一步应用。

1997 年 6 月，IEEE 通过了 802.11 标准。IEEE 802.11 标准是 IEEE 制定的无线局域网标准，主要是对网络的物理层（PH）和媒质访问控制层（MAC）进行了规定，其中对 MAC 层的规定是重点。各厂商的产品在同一物理层上可以相互操作，逻辑链路控制层（LLC）是一致的，即 MAC 层以下对网络应用是透明的。这样就使得无线局域网的两种主要用途——（同网段内）多点接入与多网段互联，易于质优价廉地实现。对应用来说，某种程度上的“兼容”就意味着竞争开始出现，而在 IT 这个行业，“兼容”，就意味着“十倍速时代”来临了。

1999 年底，朗讯（Lucent）推出了速率为 11M、与 10M 以太网等同的 WaveLAN

新产品——从而实现了“无线网达到有线网速率”这一近期目标，相对于以前无线网络最大速率2Mbps来说，这无疑是一个飞跃，而这其中，IEEE 802.11无疑也是原动力之一。

在MAC层以下，IEEE 802.11规定了三种发送及接收技术：扩频（Spread Spectrum）技术；红外（Infared）技术；窄带（Narrow Band）技术。而扩频又分为直接序列（Direct Sequence，DS）扩频技术（简称直扩）和跳频（Frequency Hopping，FH）扩频技术。直扩技术，通常又会结合码分多址CDMA技术。IEEE 802.11标准的逻辑结构如图1.1所示，每个站点所应用的802.11标准的逻辑结构包括一个单一MAC层和多个PHY中的一个。MAC层在LLC层的支持下为共享介质PHY提供访问控制功能（如寻址方式、访问协调、帧校验序列生成的检查，以及LLC PDU定界等）。MAC层在LLC层的支持下执行寻址方式和帧识别功能。IEEE 802.11标准MAC层采用CSMA/CA（载波监听多路访问/冲突检测）协议控制每一个站点的接入。

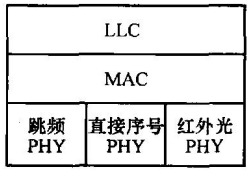


图1.1 IEEE 802.11MAC层支持三个分离的PHY

1992年7月，IEEE 802.11工作组决定将无线局域网的工作频率定为2.4GHz的ISM频段，用直接序列扩频和跳频方式传输。因为2.4GHz的ISM频段在世界大部分国家已经放开，无须无线电管理部门的许可。在美国，FCC规定ISM频段的天线增益最大为6dBi，发射功率不超过100mW。1993年3月，IEEE 802.11标准委员会接受建议，制定一个直接序列扩频物理层标准。经过多方讨论，直接序列扩频物理层规定两个数据速率：

- 利用差分四进制相移键控（DQPSK）调制的2Mbit/s；
- 利用差分二进制相移键控（DBPSK）调制的1Mbit/s。

在DSSS中，将2.4GHz的频宽划分成14个22MHz的信道（Channel），临近的信道互相重叠，在14个信道内，只有3个信道是互相不覆盖的，数据就是从这14个信道中的一个进行传送而不需要进行信道之间的跳跃。在不同的国家信道的划分是不相同的。与直接序列扩频相比，基于IEEE 802.11的跳频PHY利用无线电从一个频率跳到另一个频率发送数据信号。跳频系统按照跳频序列跳跃，一个跳频序列一般被称为跳频信道（Frequency Hopping Channel）。如果数据在某一个跳跃序列频率上被破坏，系统必须要求重传。IEEE 802.11委员会规定跳频PHY层利用GFSK调制，传输的数据速率为1Mbit/s。该规定描述了已在美国被确定的79信道中心频率。

目前IEEE 802.11b实际上已成为无线局域网（WLAN）的主流标准，被多数

厂商所采用，但是不可否认，许多 WLAN 的新标准正在崭露头角，其中 IEEE 802.11a 和IEEE 802.11g更是备受业界关注。

扩展频谱技术在 20 世纪 50 年代第一次被美国军方公开介绍，它用来进行保密传输。从一开始扩展频谱技术就具有抗噪音、抗干扰、抗阻塞和抗未授权检测等功能。扩展频谱发送器用一个非常弱的功率信号在一个很宽的频率范围内发射出去，与窄带射频相反，它将所有的能量集中到一个单一的频点。扩展频谱的实现方式有多种，最常用的两种是直接序列和跳频序列。在 IEEE 802.11b 标准中，大多数的用户都使用“直接序列扩展频谱技术”（Direct Sequence Spread Spectrum，DSSS）作为实体层的选择。DSSS 将每一帧数据传送之后再附加另外一个数据位，称为“chip”，提供容错的功能，以及保证数据传输的一致性。同时，“chip”也让数据传输更加安全。尽管如此，我们还是可以使用展频分析仪去截取无线电波，也可以用特定的无线网卡去搜寻各频道内的数据，进而加以解析与破解。

因此，IEEE 802.11b 制定了一个共享密钥加密机制 WEP（Wired Equivalent Privacy），其运作在媒质访问控制层（OSI MAC Layer），提供访问控制（Access Control）以及数据加密的机制，其目的就是要提供跟有线网络一样的保密功能给无线局域网络使用。

1.2 扩展频谱通信技术

扩频通信，即扩展频谱通信技术（Spread Spectrum Communication），它的基本特点是其传输信息所用信号的带宽远大于信息本身的带宽。除此以外，扩频通信还具有如下特征：

- 是一种数字传输方式；
- 带宽的展宽是利用与被传信息无关的函数（扩频函数）对被传信息进行调制实现的；
- 在接收端使用相同的扩频函数对扩频信号进行相关解调，还原出被传信息。

扩频通信系统由于在发送端扩展了信号频谱，在接收端解扩还原了信息，其优点是大大提高了抗干扰容限。理论分析表明，各种扩频系统的抗干扰性能与信息频谱扩展后的扩频信号带宽比例有关。

频谱的扩展是用数字化方式实现的。在一个二进制码位的时段内用一组新的多位长的码型予以置换，新码型的码速率远远高出原码的码速率，由傅立叶分析可知新码型的带宽远远高出原码的带宽，从而将信号的带宽进行了扩展。这些新的码型也叫伪随机（PN）码，码位越长系统性能越高。通常，商用扩频系统 PN 码码长应不低于 12 位，一般取 32 位，军用系统可达千位。

目前常见的码型有以下三种：

- M 序列，即最长线性伪随机系列；
- GOLD 序列；
- WALSH 函数正交码。

当选取上述任意一个序列后，如 M 序列，将其中可用的编码即正交码两两组合并划分为若干组，各组分别代表不同用户，组内两个码型分别表示原始信息“1”和“0”。系统对原始信息进行编码、传送，接收端利用相关处理器对接收信号与本地码型相关进行运算，解出基带信号（即原始信息）实现解扩，从而区分出不同用户的不同信息。微波无线扩频通信的原理如图 1.2 所示。

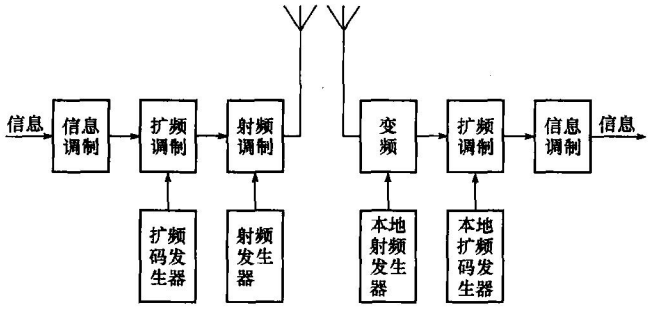


图 1.2　微波无线扩频通信原理

由图 1.2 可见，一般的无线扩频通信系统都要进行三次调制。第一次调制为信息调制，第二次调制为扩频调制，第三次调制为射频调制。接收端有相应的射频解调、扩频解调和信息解调。根据扩展频谱方式的不同，扩频通信系统可分为直接序列扩频（DS）、跳频（FH）、跳时（TH）、线性调频及以上几种方法的组合。这是重点介绍直接序列扩频技术。

所谓直接序列扩频（Direct Sequency，DS），就是用高码率的扩频码序列在发送端直接去扩展信号的频谱，在接收端直接使用相同的扩频码序列对扩展的信号频谱进行解调，还原出原始的信息。直接序列扩频的频谱扩展和解扩过程如图 1.3 和图 1.4 所示。

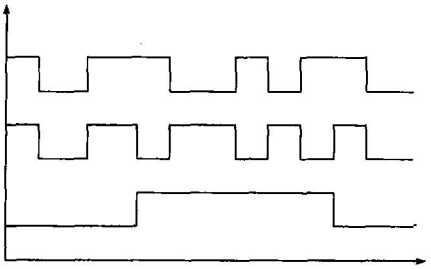


图 1.3　信息的频谱扩展过程

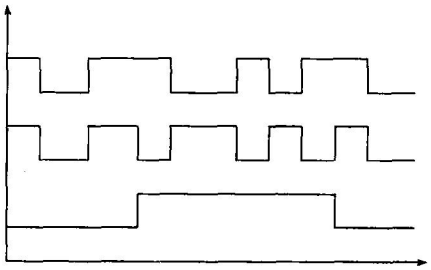


图 1.4　扩频信号的解扩过程

由图1.3和图1.4可以看出：

(1) 在发送端，信息码经码率较高的PN码调制以后，频谱被扩展了。在接收端，扩频信号经同样的PN码解调以后，信息码被恢复。

(2) 信息码经调制、扩频传输、解调然后恢复的过程，类似于PN码进行二次“模二相加”的过程。

扩频通信具有许多窄带通信难以替代的优良性能，使得它能迅速推广到各种公用和专用通信网络之中。简单来说主要有以下几项优点。

1. 抗干扰性强，误码率低

扩频通信系统由于在发送端扩展信号频谱，在接收端解扩还原信息，产生了扩频增益，从而大大地提高了抗干扰容限。根据扩频增益不同，甚至在负的信噪比条件下，也可以将信号从噪声中提取出来。在目前商用的通信系统中，扩频通信是唯一能够工作于负信噪比条件下的通信方式。

各种人为形式的干扰（如电子对抗中）或其他窄带或宽带（扩频）系统的干扰，只要波形、时间和码元稍有差异，解扩后仍能保持其宽带性，而有用信号将被压缩。从图1.4可以看出，对于脉冲干扰，在信号的接收过程中，它是一个被一次“模二相加”的过程，可以看成是一个被扩频过程，其带宽将被扩展，而有用信号却经过了一个被二次“模二相加”的过程，是一个解扩过程，其信号被恢复（压缩）后，保证高于干扰。由于扩频系统这一优良性能，其误码率很低，远高于普通的微波通信（如通常所说的一点多址）的效果，完全能满足目前国内SCADA系统对通信传输质量的要求。应该说，抗干扰性能强是扩频通信的最突出的优点。

2. 易于同频使用，提高了无线频谱利用率

无线频谱十分宝贵，虽然从长波到微波都已得到开发利用，仍然满足不了社会的需求。为此，世界各地都设计了频谱管理机构，用户只能使用申请获得的频率，依靠频道划分来防止信道之间发生干扰。

由于扩频通信采用了相关接收这一技术，信号发送功率极低（<1W，一般为1～100mW），且可工作在信道噪声和热噪声背景中，易于在同一地区重复使用同一频率，也可以与现今各种窄带通信共享同一频率资源。

3. 抗多径干扰

在无线通信中，抗多径干扰问题一直是难以解决的问题。利用扩频编码之间的相关特性，在接收端可以用相关技术从多径信号中提取分离出最强的有用信号，也可把多个路径来的同一码序列的波形相加使之得到加强，从而达到有效的抗多径干扰。

4. 适用数据业务

扩频通信是数字通信，特别适合数字话音和数据同时传输，扩频通信自身具有加密功能，保密性强，便于开展各种通信业务。扩频通信容易采用码分多址、语音压缩等多项新技术，更适用于计算机网络以及数字化的话音、图像信息传输。

5. 使用简便

扩频通信绝大部分是数字电路，设备高度集成，安装简便，易于维护，也十分小巧可靠，便于安装，便于扩展，平均无故障率时间也很长；另外，扩频设备一般采用积木式结构，组网方式灵活，方便统一规划，分期实施，利于扩容，有效地节省前期投资。

1.3 IEEE 802.11 协议简述

作为全球公认的局域网权威，IEEE 802 工作组建立的标准在过去 20 年内在局域网领域内独领风骚。这些协议包括了 IEEE 802.3 Ethernet 协议、IEEE 802.5 Token Ring 协议、IEEE 802.3z 100BASE－T 快速以太网协议。在 1997 年，经过了 7 年的工作以后，IEEE 发布了 802.11 协议，这也是在无线局域网领域内的第一个国际上被认可的协议。在 1999 年 9 月，他们又提出了 IEEE 802.11b High Rate 协议，用来对 802.11 协议进行补充。IEEE 802.11b 在 802.11 的 1Mbps 和 2Mbps 速率下又增加了 5.5Mbps 和 11Mbps 两个新的网络吞吐速率。利用 IEEE 802.11b，移动用户能够获得同 Ethernet 一样的性能、网络吞吐率、可用性。这个基于标准的技术使得管理员可以根据环境选择合适的局域网技术来构造自己的网络，满足他们的商业用户和其他用户的需求。IEEE 802.11 协议主要工作在 ISO 协议的最低两层上，并在物理层上进行了一些改动，加入了高速数字传输的特性和连接的稳定性。

1. IEEE 802.11 无线局域网标准

1997 年 IEEE 802.11 标准的制定是无线局域网发展的里程碑，它是由大量的局域网以及计算机专家审定通过的标准。IEEE 802.11 标准定义了单一的 MAC 层和多样的物理层，其物理层标准主要有 IEEE 802.11b，IEEE 802.11a 和 IEEE 802.11g。

(1) IEEE 802.11b。1999 年 9 月正式通过的 IEEE 802.11b 标准是 IEEE 802.11 协议标准的扩展。它可以支持最高 11Mbps 的数据速率，运行在 2.4GHz 的 ISM 频段上，采用的调制技术是 CCK。但是随着用户的不断增长，对数据速率的要求也越来越高，CCK 调制方式就不再是一种合适的方法了。因为对于直接序