第3章 chapter 3

无线局域网

无线局域网(WLAN)目前已很常见,其原理、结构、应用和传统有线局域网较为接近,因而本书将WLAN作为第一种无线网络予以介绍。首先概述其原理和特点,阐述其组成与服务、协议体系结构,重点是IEEE 802.11标准、性能和信道分配。其次介绍发展趋势和主要应用。最后,提供相关的NS2仿真实例。

3.1 无线局域网概述

WLAN类似传统的有线局域网,可以是客户机/服务器类型,也可是无服务器的对等网。网络链路从线缆改为无线,用户能方便地通过无线方式连接网络和收发数据。

3.1.1 无线局域网的定义

WLAN是计算机网络与无线通信技术相结合的产物,通常指采用无线传输介质的计算机局域网。其利用无线电和红外线等无线方式,提供对等或点对点连通性的数据通信。从技术角度分析,WLAN利用无线多址信道和宽带调制技术来提供统一的物理层平台,以此来支持节点间的数据通信,为通信的移动化、个性化和多媒体应用提供可能。

WLAN的覆盖范围较为有限,距离差异使数据传输的性能不同,导致网络具体设计和实现上有所区别。WLAN能在几十到几千米范围内支持较高数据率,可采用微蜂窝(microcell)、微微蜂窝(picocell)或非蜂窝(Ad Hoc)结构。图3.1是WLAN与有线网络的集成部署示意图。图3.2为常见的WLAN设备。

目前WLAN领域主要有两个典型标准:IEEE 802.11和HiperLAN。

IEEE 802.11系列标准由IEEE 802.11工作组提出,包括多个子标准,如目前较常见的IEEE 802.11g/n等。IEEE 802.11g工作于2.4GHz频率,采用补码键控(CCK)、OFDM和分组二进制卷积码(PBCC)等技术,可提供54Mbps的速率。IEEE 802.11n进一步使用MIMO和OFDM等技术,将速率提升至300Mbps甚至600Mbps。WiFi是IEEE 802.11的商业名称,由WiFi联盟持有。很多场合下WiFi和IEEE 802.11概念相同。

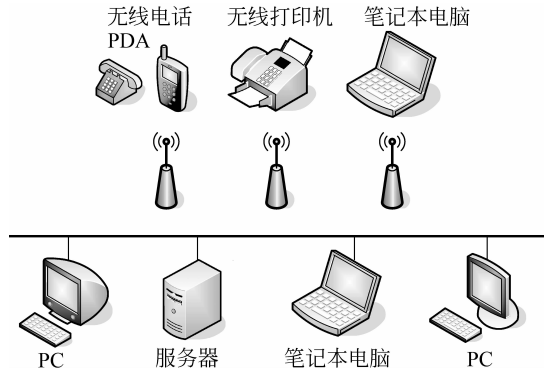

图 3.1 典型 WLAN 和 LAN 集成部署示意图

(a) PCMCIA无线局域网卡 (b) USB无线局域网卡 (c) 室内AP (d) 室外AP

图 3.2 WLAN 的常用设备

HiperLAN 由欧洲 ETSI 开发，包括 HiperLAN1、HiperLAN2、室内无线骨干网 HiperLink 和室外接入有线基础设施 HiperAccess 4 种标准。HiperLAN 致力实现高速无线连接，减少无线技术复杂性，采用了移动通信中广泛使用的高斯最小频移键控调制技术。

3.1.2 无线局域网的特点

1. 无线局域网的优点

WLAN 是在有线局域网的基础上发展而来的，主要特点如下：

(1) 移动性。网络和主机迁移方便。通信范围不再受线路环境的限制，扩大了覆盖范围，为便携式设备提供有效的网络接入功能，用户可随时随地获取信息。

(2) 灵活性。安装简单，组网灵活，可将网络延伸到线缆无法连接的地方。

(3) 可伸缩性。放置或添加接入点(Access Point，AP)或扩展点(Extend Point，EP)，可扩展组网。

(4) 经济性。可用于难以物理布线的环境，节省了线缆、附件和人工费用。同时省去布线工序，快速组网，快速投入使用，成本效益显著。可低成本快速组建临时性网络。而对需频繁布线或更换地点的场合，费用节约更明显。

2. 无线局域网的局限性

WLAN 尽管有很多优点，也面临一些不足，具体如下：

(1) 可靠性。传统 LAN 的信道误码率小于 10^{-9}，可靠性和稳定性极高。而 WLAN

的无线信道并不十分可靠,各种干扰和噪音会引起信号衰落和误码,进而导致吞吐性能下降和不稳定。此外,无线传输的特殊性还会产生“隐藏节点”、“暴露节点”等现象。

(2) 兼容性与共存性。兼容性包括:WLAN 要兼容有线局域网;兼容现有网络操作系统和网络软件;多种 WLAN 标准互相兼容;不同厂家的无线设备兼容。共存性包括:同一频段的不同制式或标准共存,如 2.4GHz 的 IEEE 802.11 和蓝牙系统共存;不同频段、制式或标准共存,如 2.4GHz 和 5GHz 的 WLAN 共存。

(3) 带宽与系统容量。由于频率资源匮乏,WLAN 的信道带宽远小于有线网络带宽。即使进行复用,其系统容量通常也小于有线网。

(4) 覆盖范围。WLAN 的低功率和高频率限制了其覆盖范围。为扩大覆盖范围,可引入蜂窝或微蜂窝网络结构,或中继与桥接等措施。

(5) 干扰。外界干扰可影响无线信道和设备,WLAN 内部会形成自干扰,也会干扰其他无线系统。因此规划和使用 WLAN 时,要综合考虑电磁兼容和抗干扰性。

(6) 安全性。包括两方面:一是信息安全,即信息传输的可靠性、保密性、合法性和不可篡改性等;二是人员安全,即电磁波辐射对人体的影响。不同于有线封闭信道,WLAN 中无线电波可能遭受窃听和恶意干扰。WLAN 系统也会存在一些安全漏洞。

(7) 能耗。WLAN 的终端多为便携设备,如笔记本电脑、智能手机等,为延长使用时间和提高电池寿命,网络应有节能管理功能。当设备不进行数据收发时,应使收发功能处于休眠状态;而要收发数据时,再激活收发功能。

(8) 多业务与多媒体。已有 WLAN 标准和产品主要面向数据业务,而由于语音、图像等多媒体业务的需求,要进一步开发保证多媒体服务质量的相关标准和产品。

(9) 移动性。WLAN 虽支持站的移动,但对大范围移动和高速移动的支持机制尚不完善。而小范围低速移动也会对性能造成一定影响。

(10) 小型化和低成本。这取决于大规模集成电路,尤其是高性能、高集成度技术的进步。目前相关技术已较成熟,具备了生产小型、低价 WLAN 射频器件的能力。

3.1.3 无线局域网的分类

WLAN 可根据不同层次、不同业务、不同技术、不同标准及不同应用等进行分类。

(1) 按频段分,可分为专用频段和自由频段两类,如图 3.3 所示。

(2) 根据业务类型,可分为无连接和面向连接两类,如图 3.4 所示。前者常用于高速数据传输,如 IP 分组。后者常用于语音等实时性较强的业务以及基于 TDMA 等技术。

(3) 根据网络拓扑和应用要求,可分为对等、基础架构、接入和中继等。

WLAN 应用可分室内和室外两类。室内如家庭或小型办公室、大型建筑物、企事业单位、工商业等,室外包括园区和较远距离的无线网络连接以及更远距离的网络中继。公共 WLAN 接入近年来发展较快,主要部署在热点(hot spots)场所。

WLAN 主要有 3 种应用:WLAN 接入、无线网络互联和定位。前两类较普遍,而定位应用近年来才发展起来,第 11 章将介绍无线室内定位技术。

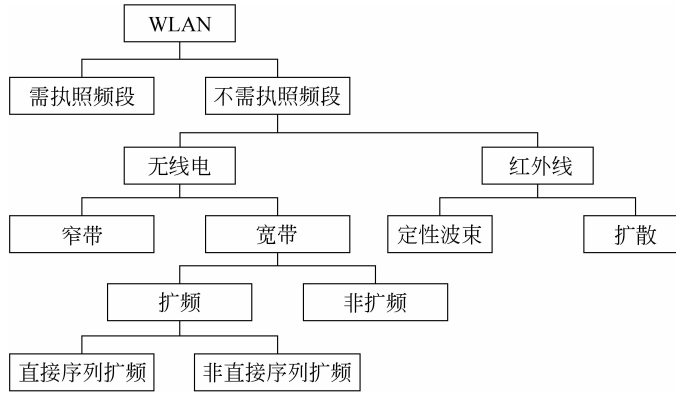

图 3.3 无线局域网分类一

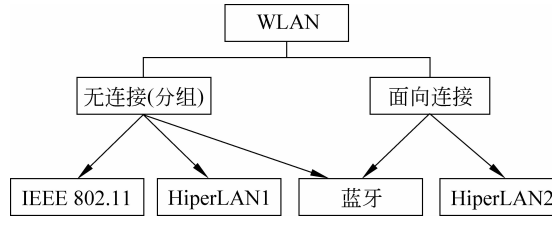

图 3.4 无线局域网分类二

3.2 无线局域网的组成与服务

3.2.1 无线局域网的组成

WLAN 由站、无线介质、无线接入点或基站、分布式系统等组成。

1. 站(STA)

站也称主机或终端,是 WLAN 的基本组成单元。站一般作为客户端,是具备无线网络接口的计算机设备,通常包括终端用户设备、无线网络接口和网络软件 3 部分。

站如果移动,称为移动主机或移动终端。按移动性可分为固定站、半移动站和移动站。固定站指位置固定不动;半移动站指经常改变地理位置,但移动时并不要求保持网络连接;而移动站则要求在移动状态保持连接,典型移动速率为 2~10m/s。

站之间的通信距离由于天线辐射能力有限和应用环境不同而受限制。WLAN 能覆盖的区域范围称为服务区(Service Area,SA),由移动站的无线收发信机及地理环境确定的通信覆盖区域称基本服务区(BSA)或小区(cell),是网络的最小单元。一个 BSA 内相互联系、相互通信的一组主机组成了基本服务集(BSS)。

2. 无线介质(WM)

无线介质是 WLAN 中站或 AP 间通信的传输介质,空气是无线电波和红外线传播

的良好载体。WLAN 中的无线介质由物理层标准定义。

3. 无线接入点(AP)

AP 类似于移动通信网络的基站(BS),常处于 BSA 中心,固定不动。其功能如下:

(1) 完成其他非 AP 站的接入访问和同一 BSS 中的不同功能。

(2) 作为桥接点,完成 WLAN 与分布式系统间的桥接功能。

(3) 作为 BSS 的控制中心,控制和管理其他非 AP 站。

无线 AP 是具有无线网络接口的网络设备,一般包括:与分布式系统的接口;无线网络接口和相关软件;桥接、接入控制、管理等 AP 软件和网络软件。

4. 分布式系统(DS)

单个 BSA 受环境和主机收发信机特性的限制。为覆盖更大区域,可将多个 BSA 通过 DS 连接,形成一个扩展服务区(ESA),而通过 DS 互连的属同一 ESA 的所有主机组成一个扩展服务集(ESS)。

用来连接不同 BSA 的通信信道称为分布式系统介质(DSM)。DSM 可分为有线或无线信道。无线分布式系统(WDS)可通过无线连接不同的 BSS。DS 通过入口(portal)连接骨干网。WLAN 和有线网的数据传输都需经过入口。入口能识别有线网和 WLAN 的帧,它是一个逻辑接入点,可以是单一设备,也可集成于 AP 中。

3.2.2 无线局域网的拓扑结构

WLAN 的拓扑结构可从几方面分类。根据物理拓扑可分为单区网和多区网;根据逻辑拓扑可分为对等式、基础架构式和总线型、星型、环型等;根据控制方式可分为无中心分布式和有中心集中控制式两种;根据与外网的连接性可分为独立和非独立两种。

BSS 是 WLAN 的基本构造模块,有两种基本拓扑结构或组网方式:分布对等式拓扑和基础架构集中式拓扑。单个 BSS 称单区网,多个 BSS 通过 DS 互连构成多区网。

1. 分布对等式拓扑

分布对等式网络是独立 BSS(IBSS)。它是典型的自治方式单区网,任意站之间可直接通信而无须依赖 AP 转接,如图 3.5 所示。由于无 AP,站之间是对等、分布式或无中心的。由于 IBSS 网络不必预先计划,可按需随时构建,因此也称为自组织网络。该结构中各站竞争公用信道,如站点数过多,竞争会影响网络性能,因此,较适合小规模、小范围的 WLAN,多用于临时组网和军事通信。注意,IBSS 是一种单区网,但单区网并不一定就是 IBSS。另外 IBSS 不能接入 DS。

2. 基础架构集中式拓扑

一个基础架构除 DS 外,至少要有一个 AP。只包含一个 AP 的单区基础架构网络如图 3.6 所示。AP 是 BSS 的中心控制站,其他站在该中心站的控制下互相通信。

与 IBSS 相比,基础架构 BSS 的可靠性较差,如 AP 发生故障或遭破坏,整个 BSS 就

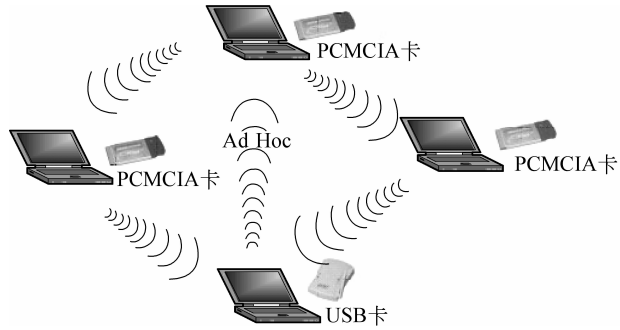

图 3.5 分布对等式工作模式

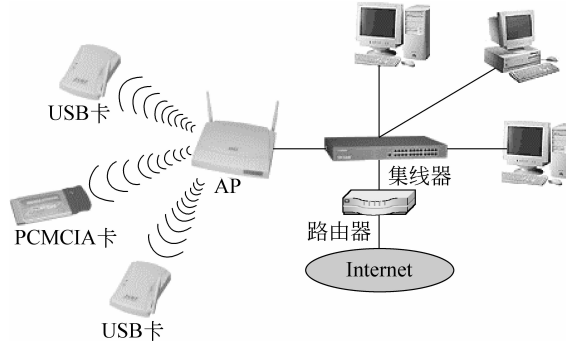

图 3.6 基础架构 BSS 工作模式

会瘫痪。此外,中心站 AP 的复杂度较大,成本也较高。

基础架构 BSS 中的某个站在与另一站通信时,须经源站→AP→目标站的两跳过程,由 AP 转接。其占用了链路,增加了传输时延,但比两站间直接通信仍有以下优势:

(1) BSS 内的所有站都需在 AP 通信范围之内,而对各站间的距离无限制,即网络中的站点布局受环境限制较小。

(2) 由于各站不需保持邻居关系,其路由复杂性和物理层实现复杂度较低。

(3) AP 作为中心站,控制所有站点对网络的访问,当网络业务量增大时,网络吞吐和时延性能的恶化并不剧烈。

(4) AP 可对 BSS 内站点进行同步、移动和节能管理等,可控性好。

(5) 为接入 DS 或骨干网提供了逻辑接入点,可伸缩性较强。可通过增加 AP 数量、选择 AP 位置等扩展容量和覆盖区域。即将单区 BSS 扩展成为多区 ESS。

3. ESS 网络拓扑

ESA 是多个 BSA 通过 DS 连接形成的扩展区域,范围可达数千米。同一 ESA 的所有站组成 ESS。ESA 中,AP 除完成基本功能外,还可确定一个 BSA 的地理位置。ESS 是一种由多个 BSS 组成的多区网,每个 BSS 都有一个 BSS 标识(BSSID)。如果网络由多个 ESS 组成,每个 ESS 也有一个 ESSID,所有 ESSID 组成一个网络标识(NID)以区分不

同网络。

4. 中继或桥接型网络拓扑

两个或多个网络(LAN 或 WLAN)或网段可通过无线中继器、网桥或路由器等连接和扩展。如中间只经过一个设备,称单跳网络;如经过多个设备,则称多跳网络。

3.2.3 无线局域网的服务

WLAN 的不同层次都有相应服务。与 WLAN 体系结构密切相关的服务有 STA 服务和 DS 服务。这两种服务均在 MAC 层。IEEE 802.11 标准中定义了 9 种服务,3 种用于传输数据,6 种为管理操作。下面介绍 STA 服务和 DS 服务。

1. STA 服务

1) 认证(authentication)

WLAN 无法像有线局域网那样用物理接口来实现授权接入,因为其传输介质没有精确边界。所以考虑认证服务控制接入,所有站均可用认证获取其他站的身份。如果两站间未建立交互式认证,则无法建立连接。站间认证可为链路级认证,也可为端对端或用户到用户的认证。认证过程和方案可自由选择。IEEE 802.11 支持开放系统认证和共享密钥认证,后者可使用有线等价保密(Wired Equivalent Privacy,WEP)算法。

2) 解除认证(deauthentication)

如欲终止已存在的认证,需唤醒解除认证服务。由于认证是连接的先决条件,因此解除认证将使站解除连接。解除认证服务可由任一连接实体唤醒,是通知型而非请求型服务,解除认证不能被另一方拒绝。AP 发给已连接的站解除认证通知时,连接将终止。

3) 保密(privacy)

有线局域网中只有物理连接的站可侦听局域网通信。而无线共享介质则不同,任何一台符合标准的站均可侦听到其覆盖范围内的所有物理层通信。因此,某个 WLAN 的无保密通信会严重影响该 WLAN 的安全性能,应考虑安全机制。

2. DS 服务

DS 提供的服务称为 DSS。WLAN 中,DSS 通常由 AP 提供,包括以下几种。

1) 关联(association)

为在 DS 内传输信息,对于给定站,DSS 需知道接入哪个 AP。这种信息由关联提供给 DS,支持 BSS 的切换移动,关联是必要非充分条件,仅支持无切换移动。

站通过 AP 发送数据前,首先关联至 AP。欲建立关联,先唤醒关联服务,该服务提供了站到 DS 的 AP 映射。DS 使用该信息完成其消息分布业务。任一瞬间,一个站仅能和一个 AP 关联。一旦关联完成,站就能充分利用 DS(通过 AP)进行通信。关联通常由移动站激活,一个 AP 可在同一时间关联多个站。

2) 重新关联(reassociation)

BSS 切换移动需重新关联服务,即当前关联从一个 AP 移动到另一 AP。当站在 ESS

内从一个 BSS 移动到另一 BSS 时，它保持了 AP 与站之间的当前映射。当站保持与同一 AP 的关联时，重新关联还能改变已建关联的属性。重新关联总是由移动站激活。

3）解除关联(disassociation)

终止一个已有关联时会唤醒解除关联。ESS 中，它告诉 DS 取消已存在的关联消息。关联任一节点均可唤醒解除关联服务，解除关联是通知型而非请求型服务，不能被关联的任一方拒绝。AP 可解除站关联，使 AP 从网络中移走。站也可试图在需要它们离开网络时解除关联，而 MAC 协议并不依靠站来唤醒解除关联服务。

4）分布(distribution)

作为站使用的基本服务，由来自或发送到工作在 ESS(此时帧通过 DS 发送)中的 WLAN 站的每个数据消息唤醒，分布借助于 DSS 完成。

5）集成(integration)

如果分布式服务确定消息的接收端为集成 LAN 成员，则 DS 的输出点是端口而非 AP。分发到端口的消息使得 DS 唤醒集成功能，集成功能负责完成消息从 DSM 到集成 LAN 介质和地址空间的变换。

3.3 IEEE 802.11 协议体系结构

3.3.1 IEEE 802.11 协议标准

1. IEEE 802.11 标准的发展

1990 年 IEEE 802.11 工作组成立，1993 年形成基础协议，此后协议标准一直不断发展和更新，迄今形成了许多子集，如表 3.1 所示。

表 3.1 IEEE 802.11 系列标准

协 议 名 称	发布时间/年	简 要 说 明
IEEE 802.11	1997	2.4GHz 微波和红外线标准，速率为 1Mbps 和 2Mbps
IEEE 802.11a	1999	5GHz 微波标准，速率为 54Mbps
IEEE 802.11b	1999	2.4GHz 微波标准，速率为 5.5Mbps 和 11Mbps
IEEE 802.11c	2000	IEEE 802.11 网络和普通以太网之间的互通
IEEE 802.11d	2000	国际间漫游的规范
IEEE 802.11e	2005	服务质量控制，包括数据包脉冲
IEEE 802.11f	2003	服务访问点间通信协议
IEEE 802.11g	2003	2.4GHz 微波标准，速率达 54Mbps
IEEE 802.11h	2003	5GHz 微波频谱管理(欧洲)
IEEE 802.11i	2004	增强安全机制
IEEE 802.11j	2004	微波频谱扩展(日本)
IEEE 802.11k	2008	微波测量规范
IEEE 802.11n	2009	使用 MIMO 技术，速率为 100Mbps
IEEE 802.11p	2010	车载环境的无线接入(见本书第 10 章)

续表

协议名称	发布时间/年	简要说明
IEEE 802.11r	2008	快速的 BSS 切换
IEEE 802.11s	2010	网状网络的扩展服务集
IEEE 802.11u	2010	和非 802 类型的网络协同
IEEE 802.11v	2010	无线网络管理
IEEE 802.11w	2009	被保护的网络管理帧
IEEE 802.11y	2008	3650～3700MHz 微波(美国)
IEEE 802.11z	2011	扩展到直接链路建立
IEEE 802.11aa	2011	音视频流的鲁棒性
IEEE 802.11ac	2012	使用 MIMO 技术对 IEEE 802.11n 的改进
IEEE 802.11ad	2012	60GHz 微波标准,最高理论速率达 7Gbps
IEEE 802.11ae	2012	帧管理的优先级
IEEE 802.11af	2014	利用电视空白频段
IEEE 802.11ah	2014	1GHz 无线传感子网,智能表计量
IEEE 802.11ai	2015	快速初始链路设置
IEEE 802.11aj	2016	针对中国毫米波频段的下一代 WLAN
IEEE 802.11ak	2015	一般链路
IEEE 802.11aq	2015	预关联发现
IEEE 802.11mc	2015	标准维护

2. IEEE 802.11 若干子标准简介

先简单介绍 IEEE 802.11g,其载波频率为 2.4GHz,原始传输速率为 54Mbps,净传输速率约为 24.7Mbps。采用 OFDM 等技术,兼容性和高数据速率弥补了 IEEE 802.11a/b 等早期标准的缺陷,已得到广泛使用。

而 IEEE 802.11n 是目前较为主流的应用,它将传输速率增至 100Mbps 以上,最高可达 600Mbps。为双频(2.4/5GHz)模式,兼容以往标准。结合 MIMO 与 OFDM 等技术,提高了无线资源的利用率,扩大了无线信号的传输范围,提高了系统容量。

表 3.2 对一些子标准进行了性能比较。

表 3.2 一些 IEEE 802.11 子标准性能比较

子标准	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
发布时间	1999	1999	2003	2009
物理层	OFDM	DSSS	OFDM	OFDM
频带	5GHz	2.4GHz	2.4GHz	2.4G/5GHz
传输速率	6～54Mbps	1,2,5.5,11Mbps	最高 54Mbps	最高 600Mbps
传输距离	室内 30m, 室外 45m	室内 30m, 室外 100m	室内 30m, 室外 100m	室内 70m, 室外 250m

IEEE 802.11e 协议加入了 QoS 功能，以改进和管理 WLAN 的服务质量，进行音视频多媒体传输，以及增强的安全应用、移动访问应用等。

IEEE 802.11i 则针对安全性，弥补了 WEP 的不足。包括数据加密与用户身份认证，定义了基于 AES 的加密协议 CCMP、向前兼容 RC4 的加密协议 TKIP 等。

IEEE 802.11k 提供测量信息以提高网络效率。能实现站点报告，列出移动客户。实现无破坏连接转移漫游时，有效选择接入点，从而帮助用户实现无间断的网络连接。

IEEE 802.11s 包括网状网络中的拓扑学习、路由与转发、安全性、测量、发现与联系、介质访问协调、服务兼容性、互联、配置及管理等。

3. IEEE 802.11 层次结构

IEEE 802.11 层次结构如图 3.7 所示，物理层包括物理汇聚子层、物理介质相关子层和物理管理子层。物理汇聚子层主要侦听载波和对不同物理层形成不同格式分组，物理介质相关子层识别相关介质传输信号使用的调制与编码技术，物理管理子层为不同物理层选择信道。数据链路层分为介质访问控制(MAC)子层、逻辑链路控制(LLC)子层和 MAC 管理层。MAC 子层主要控制节点获取信道访问权，LLC 子层负责建立和释放逻辑连接，提供高层接口、差错控制、添加帧序号等。MAC 管理层负责越区切换、功率管理等，还有站点管理以协调物理层和链路层交互。

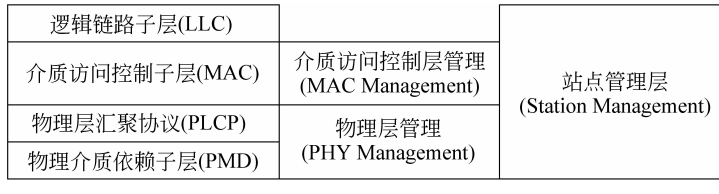

图 3.7 IEEE 802.11 层次结构

IEEE 802.11 较完整的协议体系如图 3.8 所示。

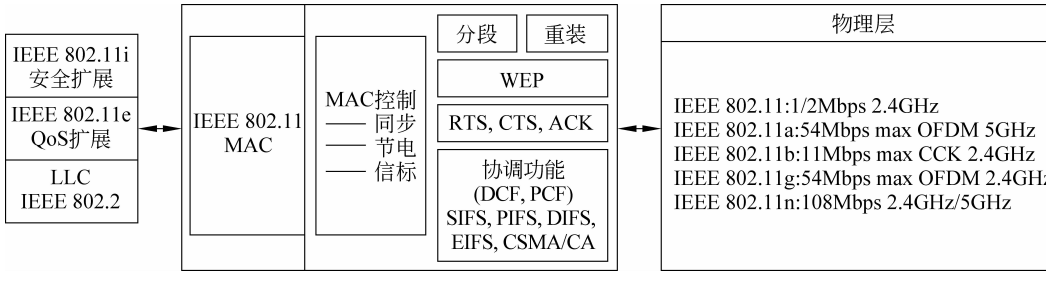

图 3.8 IEEE 802.11 较完整的协议体系

3.3.2 IEEE 802.11 物理层

表 3.3 给出了 IEEE 802.11 物理层规范的一些细节。

表 3.3 IEEE 802.11 部分物理层规范

(a) 直接序列扩频

数据速率/Mbps	芯片码长度	调 制	符号速率/Mbps	位/符号
1	11(巴克序列)	DBPSK	1	1
2	11(巴克序列)	DQPSK	1	2
5.5	8(CCK)	DQPSK	1.375	4
11	8(CCK)	DQPSK	1.375	8

(b) 跳频扩频

数据速率/Mbps	调 制	符号速率/Mbps	位/符号
1	2 级 GFSK	1	1
2	4 级 GFSK	1	2

(c) 红外线

数据速率/Mbps	调 制	符号速率/Mbps	位/符号
1	16PPM	4	0.25
2	4PPM	4	0.5

(d) OFDM

数据速率/Mbps	调制	编码率	每个子载波的编码位数	每个 OFDM 符号的码位数	每个 OFDM 符号的数据位数
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
49	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

3.3.3 IEEE 802.11 MAC 层

MAC 子层协议对网络吞吐率、时延等性能有重要影响,还影响小区结构、频谱利用率、系统容量、设备成本和复杂度等。需要合理选择 MAC 子层规范,并根据网络业务特征有效配置信道资源,以提高无线信道效率、系统吞吐量和传输质量。

1. MAC 体系结构

MAC 子层的功能首先是提供可靠的数据传输。通过 MAC 帧交换协议来保障无线介质上的数据传输可靠性。MAC 子层还能实现共享介质访问的公平控制,通过两种访问机制来实现:基本访问机制,即分布式协调功能(DCF);集中控制访问机制,即点协调功能(PCF)。MAC 子层的安全服务具体使用 WEP 等保护数据传输。

2. IEEE 802.11 的 MAC 接入协议

即基于分布式的无线介质访问控制协议(DFWMAC),支持自组织和基础架构,具体有 DCF 和 PCF 两种。DCF 是基础协议,核心是载波监听多路访问/冲突避免(Carrier Sense Multiple Access/Collision Avoidance,CSMA/CA),包括载波检测、帧间间隔和随机退避。在自组织网和基础架构网中超帧的竞争期使用,支持异步服务。每个节点使用 CSMA 分布接入算法,各站竞争信道使用。PCF 用于超帧无竞争期,支持时限服务,是可选协议。

为避免冲突,MAC 子层规定所有站在完成发送后必须等待一个短时间(继续监听)才能发送下一帧,该时间称为帧间间隔(InterFrame Space,IFS)。IFS 的长短取决于该站将发送的帧类型。高优先级的等待时间较短,可优先获得发送权,而低优先级则需等待较长时间。若低优先级帧尚未发送而其他站的高优先级帧已发送,则介质被占用,低优先级帧推迟发送以避免冲突。IEEE 802.11 规定了 4 种 IFS,以实现不同的访问优先级别,其时间长度关系为 SIFS<PIFS<DIFS <EIFS。

(1) SIFS (Short IFS)。它是最小的 IFS,采用 SIFS 的节点具有访问最高优先级。一些特殊帧要求使用 SIFS 访问介质,如应答帧(ACK)、清除发送帧(CTS)、MAC 服务数据单元(MSDU)的非头分段、被轮询到的站回应帧等。

(2) PIFS (PCF IFS)。PIFS 为 SIFS 和时隙时间之和,AP 在无竞争期开始时获得介质访问权的时间间隔,即 AP 总比普通节点具有更高的访问信道的优先级。

(3) DIFS (DCF IFS)。DIFS 为 SIFS 和两倍时隙时间之和,工作在 DCF 模式的终端通过载波监听到介质空闲超过 DIFS,且本终端随机退避结束,可立即发送。

(4) EIFS (Extended IFS)。EIFS 为 ACK 帧传输时间和 SIFS、DIFS 的时间之和,在前一帧出错的情况下,发送节点不得不延迟 EIFS 时间后再发送下一帧。EIFS 期内收到正确帧将使得该站重新同步并结束 EIFS,进入正常介质访问状态。

3.3.4 IEEE 802.11n 标准

目前 IEEE 802.11n 已成为主流应用标准,它结合物理层和 MAC 层的优化技术提高吞吐率。其传输速率提高到 300Mbps 甚至 600Mbps。IEEE 802.11n 采用智能天线,通过多组独立天线组成的天线阵列,动态调整波束,减少其他信号干扰,使覆盖范围扩大,而移动性极大提高。在兼容性方面,IEEE 802.11n 采用软件无线电,不同系统的基站和终端都可通过软件实现互通和兼容。IEEE 802.11n 向前后兼容,还可结合无线广域网如 3G 网络。

IEEE 802.11n 的部分关键技术简介如下:

(1) 物理层 MIMO 技术。数据经过多天线进行同步传输,为避免信号传输互扰,通过不同反射或穿透路径,因此到达接收端的时间会不一致。为避免数据不一致而无法重新组合,接收端同时具备多天线接收,然后利用 DSP 重新计算,根据时间差因素,重新组合数据,实现准确传输。MIMO 非常适用于室内环境,在室内 WLAN 环境下的频谱效率可达 20～40bps/Hz,传统无线移动蜂窝通信的频谱效率仅 1～5bps/Hz,而点对点的固

定微波系统也只有 10～12bps/Hz。

(2) 物理层 OFDM 技术。给定信道分成许多正交子信道,每个子信道上使用子载波调制,并行传输,其频谱可相互重叠,减小了子载波间相互干扰,提高了频谱利用率。

(3) 物理层 40MHz 技术。由于 2.4GHz 频段资源并不丰富,最多只能承载一个 40MHz 的频带,所以目前在 2.4GHz 频段,通常使用 20MHz 的频谱带宽,以保证 3 个不相干扰的信道。

(4) MAC 层技术。传统 IEEE 802.11 标准中,拟发送的 MAC 数据单元 MSDU,加上 MAC 首部和帧校验等,构成物理层业务数据单元 PSDU,再加上 PLCP 前缀等,构成物理层协议数据单元 PPDU,然后发送。接收方收到后,回复 ACK 帧。而 IEEE 802.11n 采用帧聚合机制,多个 MSDU 聚合成一个 MAC 协议数据单元 MPDU,而多个 MPDU 又聚合成一个 PSDU。对接收地址相同的 MAC 帧而言,可封装成一个聚合帧,只使用一个帧头,减少 ACK 帧数量,降低负荷,提高吞吐量。

(5) 兼容 IEEE 802.11a/b/g 标准。IEEE 802.11n 信号可能无法被 IEEE 802.11a/b/g 的设备检测到,设备如果直接发送信号,会导致信道冲突。为此,IEEE 802.11n 运行在混合模式,即网络中同时有 IEEE 802.11a/b/g 设备时,会在发送的报文首部添加能被 IEEE 802.11a/b/g 设备正确解析的前缀码,以实现兼容和避免冲突。

3.3.5 IEEE 802.11 优化技术

WLAN 的应用日趋普遍,提高和优化网络性能显得十分重要。简介如下。

1. 物理层优化

IEEE 802.11 不同标准工作在不同频段,采用不同调制方式。当一个 IEEE 802.11b 终端进入 IEEE 802.11a 小区中,将无法联系 AP。这种不同物理层标准导致的网络兼容性问题可引入双频多模技术解决。如一个双频多模 AP 可同时支持 IEEE 802.11a/b/g/n 设备。

双频指可自适应工作于 2.4GHz/5GHz 的产品。双频产品具有很大的灵活性,自动辨认信号并支持漫游连接,用户在不同网络下都能保持连接。随着 IEEE 802.11g/n 标准的应用和普及,双频多模也融合起来,同时支持 IEEE 802.11a/b/g/n 等标准。

2. MAC 层优化

1) IEEE 802.11 分布式协调功能(DCF)

DCF 有两种工作模式:CSMA/CA 和 RTS/CTS。

(1) CSMA/CA

IEEE 802.11 与 IEEE 802.3 的 MAC 层采用不同策略。IEEE 802.3 中采取载波侦听多路访问/冲突检测(Carrier Sense Multiple Access/Collision Detection,CSMA/CD)机制,而无线网络中的冲突检测较难,原因在于:信号强度衰减,无法准确检测出冲突;节点隐藏,如两个相反方向的工作站共同使用一个中心接入点进行连接时,可能因障碍或距离原因无法感知对方存在,而会导致冲突。所以 IEEE 802.11 采用 CSMA/CA。

CSMA/CA 方式中，检测到信道空闲期间大于某一 IFS 后立即开始发送帧，否则延迟发送直到检测到所需 IFS，然后选择退避时间进入退避，结束后重新开始上述过程。

CSMA/CA 的基础是载波侦听，存在两种不同的侦听机制：虚拟载波侦听（Virtual Carrier Sense，VCS）和物理载波侦听（Physical Carrier Sense，PCS）。

VCS 依靠网络分配向量（Network Allocation Vector，NAV），而 NAV 由根据时间设置的位于数据帧的 Duration/ID 域值所决定。NAV 提供给其他站关于信道需被某个站占用的时间信息。而 PCS 是一个由物理层向 MAC 层发送警报信号的机制，以表明目前是否有信号被侦听到。结合 VCS 和 PCS，MAC 层协议使用了冲突避免机制。发送数据前先进行 VCS，然后进行 PCS 一个 DIFS 的时间长度。

发送方和接收方使用确认机制来判断传输是否正确，称为 CSMA/CA＋ACK。发送方先检测信道，通过物理层直接载波侦听，利用收到的相对信号强度是否超过一定阈值判定有否其他站使用本信道。源站发送首帧时，若检测到信道空闲，则等待 DIFS 后就可发送。目标站若正确收到该帧，则经过 SIFS 后就可向源站回复 ACK 帧。若源站规定时间内未收到 ACK，该帧重传，直至正确接收为止，或若干次失败后放弃。

源站检测到正在信道中传输的 MAC 帧首部的持续时间字段，就调整自身 NAV。因此，当信道从忙变为空闲，任何站要发送帧时，不仅须等待一个 DIFS 间隔，还要进入竞争窗口，并计算随机退避时间，退避间隔（BI）是从竞争窗口 CW_{min} 和 CW_{max} 随机选择的。CW 为 CW_{max} 与 CW_{min} 的差值。两个以上站选择相同 BI 会发生冲突，很多站一起竞争信道时尤甚。为减少冲突，每次冲突后 CW 加倍，直至 CW_{max}。

进入退避后，站继续侦听信道，只要信道空闲，退避计时器就开始递减至零。当侦听到信道正忙，则冻结退避计时器，一直等到信道空闲再重新激活。为防止传输中断，接收站或 AP 等到一个 SIFS 并回应一个 ACK 以确认每一次成功传输。

图 3.9 所示为一个数据帧成功传输的过程。

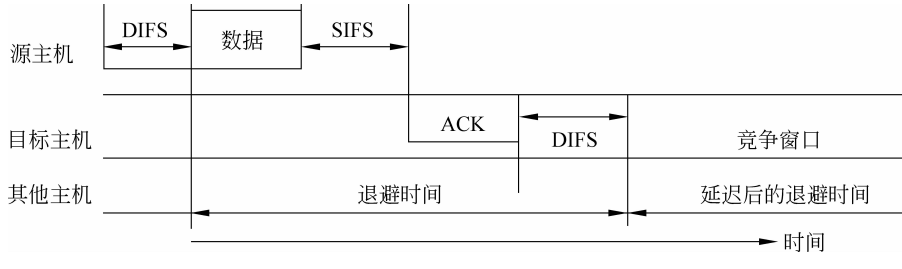

图 3.9 数据帧成功传输的时间图

（2）RTS/CTS

如前所述，当一个站只能侦听到部分其他站时，就存在隐藏节点问题。为解决该问题，IEEE 802.11 提供了另一个机制，即 RTS/CTS。

4 次握手的 RTS/CTS 方式工作过程如下：假设站 A 要向站 B 发送数据，A 先向 B 发送 RTS 信号，表明自己准备向 B 发送数据。B 收到 RTS 后，会向周围广播 CTS 信号，表明准备接收就绪。接下来 A 可发送数据，其余站暂处于静止态。B 接收完数据后，即向周围广播 ACK 帧。所有站又开始监听信道，开始新一轮信道竞争。

传输数据前发送 RTS/CTS 帧,意味着额外开销,尤其对短数据报文影响明显,所以 RTS/CTS 帧都很短。RTS 帧包含帧控制(2B)、持续时间(2B)、接收方地址(6B)、发送方地址(6B)、FCS(4B),共 20B。而 CTS 帧包含帧控制(2B)、持续时间(2B)、接收方即 RTS 发送方地址(6B)、FCS(4B),共 14B。

站可灵活选择发送方式,设置了 RTS 阈值,决定传输某个数据帧是否要启动 RTS/CTS。如果分组大于 RTS 阈值,为提高传输效率则启动 RTS/CTS 会话,否则使用基本方式。图 3.10 为 BSS 中 RTS/CTS 机制的示意图,W-CTS 是指等待目标主机的 CTS 帧,W-ACK 指等待目标主机的确认,W-DATA 指等待和接收源主机的数据。

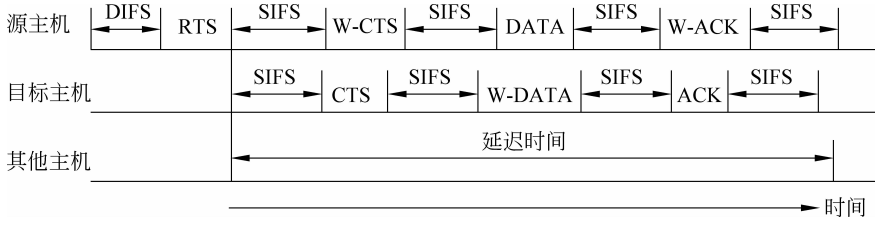

图 3.10 BSS 中 RTS/CTS 示意图

2) IEEE 802.11e 增强分布式通道存取(EDCA)

实时多媒体等业务对 WLAN 提出了更高要求。MAC 层需提供可靠传输,同时时延低、抖动小。IEEE 802.11e 对 MAC 协议做了改进,使其可支持 QoS 要求的应用。对 DCF 和 PCF 在 QoS 支持方面进行了加强,通过设置优先级,既保证大带宽应用的通信质量,同时又能向下兼容 IEEE 802.11 设备。

对 DCF 的修订称为增强分布式通道存取(EDCA)。为提供更高的 QoS,EDCA 把数据流按设备不同分成 8 类,定义了 8 个队列访问类别(Access Category,AC),其优先级不同。优先级越高,等待时延越小。另一个参数为竞争窗口,实际也是一个时间段,长短为一个不断递减的随机数。竞争窗口先减至 0 的设备就可发送数据。

EDCA 的特点主要如下:

(1) 使用 AIFS 代替 DIFS。EDCA 中传输数据前的等待称为仲裁帧间间隔 AIFS(Arbitration IFS)。AIFS 值根据不同业务类型变化,低优先级的 AIFS 值要大于高优先级,即优先级越低等待越久。小 AIFS 值意味着实时多媒体比一般数据能更快地获得信道。

(2) 最大最小竞争窗口改变。等待一个 AIFS 后,每个退避过程将计时器设置成[1,CW+1]间的任意值,不同于 DCF 的[0,CW]。最小竞争窗口 CW_{min} 和最大竞争窗口 CW_{max} 与 AC 有关。越小的 CW_{min} 和 CW_{max} 意味着站以越大的概率接入信道,优先级越高。

不同的参数设置如表 3.4 所示,可让这些队列在竞争信道时的优先级有差异。各队列的传输优先级别为音频>视频>尽力而为>背景。

表 3.4 IEEE 802.11 各队列参数设置

访问类别	AIFS	CW_{min}	CW_{max}	访问类别	AIFS	CW_{min}	CW_{max}
0(背景)	7	31	1023	2(视频)	2	15	31
1(尽力而为)	3	31	1023	3(音频)	2	7	15

为访问信道，各站的 AC 都基于上面的参数独立竞争。一旦某个 AC 侦测到信道处于长为 AIFS 的空闲时间状态，便启动退避过程，退避时间减为 0 的站有权发送帧。如有多个 AC 的退避时间减至 0，则高优先级 AC 将获得发送机会。

EDCA 通过设置不同优先级，实现了统计意义上的节点区分服务。优势如下：

(1) 划分了不同优先级的业务流。

(2) 等待信道空闲的时间间隔为 AIFS。AIFS 与 AC 呈反相关。

(3) 不同 AC 的业务流等待信道空闲以后，退避时的初始窗口大小也不同。优先级越高，初始最小退避窗口也越小。

(4) 增加了时间受限的发送机会的概念。限制时间内，两个站之间可传输多帧交换序列，帧间隔仅为 SIFS。

3. 网络层优化和移动 IP(Mobile IP)

因特网使用域名对应 IP 地址，而 IP 地址常对应某个物理网络位置，这种传统方式不能适应位置的变化。移动 IP 解决了 WLAN 的 IP 漫游问题，是网络层的优化方案。用户凭一个 IP 地址进行不间断跨网漫游，即为移动 IP。移动 IP 技术扩展了 WLAN 接入方案的覆盖范围，提供大范围的移动能力，使用户在移动中保持因特网连接。

移动主机(Mobile Node，MN)在外地通过外地代理(Foreign Agent，FA)向位于家乡的家乡代理(Home Agent，HA)注册，使 HA 获知 MN 的当前位置，即实现了移动性。这样 MN 可跨越 IP 子网实现漫游。IP 子网的网关连接 FA，负责其内部用户的注册认证。FA 不断向本地发送代理通告，MN 进入时收到广播通告，获得当地 FA 信息，通过 FA 向 HA 注册，经认证后可被授权接入。MN 在本子网内部移动时，不断监测 AP 和 FA 的信号质量，获得当前所有 FA 的优先级，再根据策略适时切换。如果仅在同一网段 AP 间切换，因 IP 子网不变，无须重新注册。而 MN 在跨网段 AP 间切换时，IP 子网改变。此时须通过新 FA 向 HA 重新注册，以后的数据会被 HA 转发至新位置。

3.4 IEEE 802.11 信道分配

目前 IEEE 802.11 标准使用 2.4GHz 和 5GHz 两个频段，前者为通用的 ISM 频段。具体可用信道各国互不相同，取决于无线电频谱分配的规定。如图 3.11 所示，2.4GHz 频带包括 14 个载波频道，每个占用 22MHz。中国、欧洲和澳大利亚允许使用 1～13 频道，美洲国家允许使用 1～11 频道，日本允许使用所有 14 个频道。

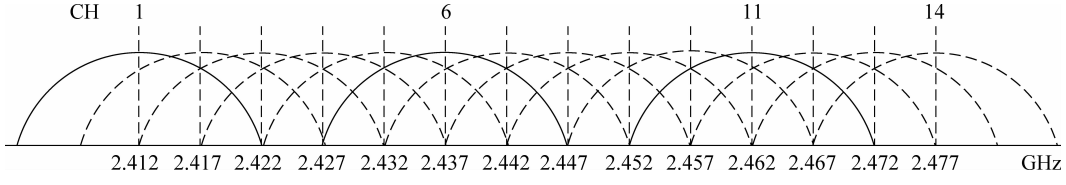

图 3.11 IEEE 802.11 使用的 2.4 GHz ISM 频段信道

由于 IEEE 802.11 技术已得到广泛应用,信道分配对 WLAN 的吞吐性能有重要影响。针对不同网络环境,信道分配主要涉及集中式管理环境和无协调环境。

3.4.1 集中式管理环境的信道分配

集中式管理环境中由中心节点决定和分配每个 AP 的信道。AP 部署需要中心控制以使得网络中无线覆盖范围最大化。具体分配可分为有 AP 放置和无 AP 放置两类。

1. 有 AP 放置的信道分配

(1) 传统方法。早期 WLAN 的信道通常作为网络规划的一部分。即为 AP 分配信道是在 AP 位置确定后执行。在指定 AP 试用地点后,需考虑网络参数和要求,如移动性、用户人群、周围基础设施、应用前景、代价和安全水平等。然后通过现场调查来细化设计,通常在不同通信位置测量信号强度来确定信号覆盖范围和 AP 最佳位置。换言之,信道分配问题可视作一个地图着色问题,每个 AP 代表一个顶点和非重叠信道的颜色。目标是要给一个 AP 分配一个非重叠通道,以使信道相邻单元格间的覆盖范围重叠最小化。

(2) 整数线性规划方法。不仅考虑无线电覆盖范围,还考虑 AP 负载平衡。因为 AP 相连的活跃无线终端数量影响了网络性能,AP 的传输拥塞会降低网络吞吐量。因此基本思想是将终端分到 AP,这样 AP 拥塞最小,相应的吞吐量最大。

(3) 优先级映射方法。优先级映射生成后,首先找到一系列可能的 AP 放置点以提供给每个像素充足的无线电覆盖。为此需用波传播预测模型(如射线追踪技术)来预测每个待定 AP 的覆盖范围。对每种 AP 放置,需要剔除与其形成不可接受的大重叠区域的相邻 AP,注意剔除后不会影响每个像素得到充足通信量和可用性。为确定重叠区域大小,需使用从相邻 AP 接收到的功率平均差。即如果重叠区域的每个像素接收到的功率平均差低于阈值,其中一个 AP 就可去掉。该步骤消除了相邻 AP 重叠覆盖可能造成的干扰。

(4) 修补方法。是一个特殊的高复杂度的全局启发式算法。初始给定基于平面图的一系列待定 AP 位置及一系列不重叠信道。使用修补方法计算得到 AP 在某个信道下生成的目标最大值。选出有适合信道的 AP,放置或修补到楼层中,并从候补列中删除。该过程在剩下的候补 AP 和相同的不重叠信道序列中重复进行,直至预定 AP 数目。每次迭代中,由于新放入 AP 会导致一些节点重新关联,这些节点的个体吞吐量受到重关联的影响而变化,需相应重新估计。

(5) 面向覆盖的方法。该方法中 AP 放置和信道分配连续和共同最优化。使用整数线性规划模型,目标是使满足特定数目的 AP 的所有服务区域的总吞吐量最大化。网络吞吐量函数由适合吞吐量测量的多项式方程的接收信号功率变化而来。该测量使用特定网络性能工具,测量当 TCP 流从 AP 到一个处于不同位置或所有区域像素的活动终端传输的平均下载数据吞吐量,记录与每个吞吐量测量相联系的接收信号功率。

2. 无 AP 放置的信道分配

(1) 基于顶点着色的饱和度方法。AP 作为图形顶点,每条边代表一对相邻 AP 可能的干扰。对一系列重叠信道有一系列颜色。频率分配问题就变为顶点着色问题,使用颜色要最少,相联节点不能同色,即求解最佳着色问题。基本思想是每个迭代中选择饱和度最高的顶点涂上不可用颜色最少的颜色。算法中建立一个精确的图是关键,需要交互 AP 协议来协同建立该图。一种建图方法是让服务区域所有 AP 侦听相邻 AP 信号。在交互中提取发送方 MAC 地址、信噪比和接收信号强度等信息。识别邻居后,每个 AP 通过分布式系统向网络中其他 AP 发送该信息。然后本算法就可用于整个网络。

(2) 自由碰撞设定涂色方法。力求实现终端可以达到冲突最小的形式分布(与 AP 相联),冲突表示两个属于不同 BSS 的基站(AP 或终端)在相同频率上互扰,由此也解决了负载均衡问题。该方法试图在零冲突的情况下将终端数量最大化,零冲突终端数量算法的效率与网络中所有基站实际反映的信道环境形成的范围和干扰有关。因此,所有终端需周期或动态提交精确的站点报告,包含每个终端在当前位置可侦听的信道。

(3) 局部坐标测量法。该方法的成本函数是加权干扰,可被 AP 和无线终端观察到。终端需物理测量现场干扰功率,包括所有频率信道,无论其关联 AP 是否空闲。终端然后将测得的干扰功率值予以平均,报告 AP。AP 自身也要测量现场干扰功率并予以平均,即可计算每个 BSS 或单元的加权干扰。权重因素包括单元内终端平均传输量和平均接收信号功率。更大的传输量导致更大的干扰,而更高的接收信号功率意味着对干扰有更大的容忍。

3.4.2 无协调环境的信道分配

由于 IEEE 802.11 的无协调部署发展迅速,多个热点和私有 WLAN 在不同地理位置以不同密度共存。在 AP 位置给定的条件下,有研究考虑只调整信道分配来改进网络性能,主要特征是分布执行,信道分配由每个 AP 而非集中控制器执行。

(1) 最少拥塞信道搜索方法。每个 AP 自动搜索负载最轻(如终端最少)的信道,并切换到该信道工作直至找到负载更小的信道。AP 首先搜索每个信道,找到相邻 AP 发布的可辨别信标,如对应每个 AP 的可区分信标。每个信标包含了各 AP 所关联的终端数目。搜索所有可用信道后,AP 了解各信道终端数,然后选择在终端最少的信道上工作。该方法也隐式解决了负载均衡问题,但前提是每个无线终端传输量相同,关联终端越多意味传输量越大。

(2) MinMax 方法。信道分配问题是从 AP 的观点看的,将特定信道分配重载 AP 会降低性能。假设相关区域已有一系列 AP,只考虑下载传输。目标函数是 AP 的有效信道利用率,定义为信道分配给 AP 的时间与 AP 使用其传输或因同信道邻居干扰造成侦听为忙时间之比。该方法的目标是给定各 AP 的不同固定传输负载,对最重载 AP 的最大有效信道利用率予以最小化。该问题等效 NP 完全问题,可用启发式算法求解。一开

始为所有 AP 随机分配信道,算法随机重新调整瓶颈 AP 干扰邻居的信道分配,降低瓶颈 AP 的有效信道利用率,从而减少网络拥塞。启发式算法并不保证最优解,尤其是有几十个 AP 的大型 WLAN。

(3) MinMax Ⅱ方法。该方法自适应地为 AP 分配信道,针对给定负载和一组 AP 干扰下,减少最重载 AP 的最大信道利用率。一组干扰 AP 被定义为与该 AP 共用信道的邻居,其传输可对该 AP 产生干扰而使其感知到信道繁忙。动态 MAC 模型规范了信道使用,考虑了活动用户数量。信道分配是动态的,每个信道调整或分配期活动客户数量测算是实时完成的,且作为新信道分配的结果。最后还检查网络性能和预定义 QoS 阈值。为确保快速收敛和避免死循环,基于马尔可夫状态转换图导出最优信道切换。每个 AP 同时且独立进行最优信道分配,并不依赖 AP 间通信。

此外,还有加权着色、信道跳、无坐标测量等方案,各有特点,这里不再赘述。

3.4.3 信道分配方案的挑战

当 BSS 和终端数目增加时,WLAN 的信道分配比蜂窝网络更为复杂,因为蜂窝网络的覆盖范围通常规范部署且有规则单元形状。而一般室内布局的 WLAN 则不然,建筑物布局和材料常使覆盖范围复杂化,对整体网络性能有显著影响。由于 WLAN 部署开始走向户外,如城市中的热点,其将面对和蜂窝网络一样的动态环境,但单元覆盖条件难以计划和控制。

尽管可以设计地理上不相交的单元覆盖,但由于 CSMA 协议的本质,同信道或相邻信道间干扰仍不可避免。随机信道访问机制和随机终端位置使得 WLAN 信道分配复杂化,而且有效的信道分配还要考虑终端的移动性。

另外,蜂窝通信系统的信道分配技术不能直接用于 WLAN。蜂窝通信网络中,数据和控制信号在不同信道上传输。而 WLAN 中数据和控制信号共享信道。

3.5 IEEE 802.11 测量及工具

3.5.1 IEEE 802.11 测量的参数和步骤

WLAN 的通信质量受很多因素影响,如节点隐藏、多径效应、衰退、分散和干扰等导致可能的高丢包率。通常仿真可在完全可控的动态环境下学习和分析新协议,但仿真不能精确反映传输协议的实际表现,需在真实环境下进行协议测试。

无线网络的测量实验需要复杂的配置,并且需监控和分析大量参数,可分为如下 4 个方面:

(1) 每个分组的参数:物理层的时间戳、接收信号强度指示(RSSI)、信道、噪声级别、数据率、前缀;MAC 层的类型、分片、重传、功率管理、保护、持续时间、地址、序号控制、帧校验序列等。

(2) 每个流的参数:吞吐量、数据丢失率、时延、失真、空中传输时间、重传概率等。

(3) 每个站的参数：活动标志、关联状态、关联持续期、关联 AP 的地址、当前 RSSI、当前的物理层数据率等。

(4) 每个基本服务集的参数：信道容量、整体数据吞吐量、整体信号吞吐量、丢包空间关联、负载级别、可用带宽等。

测量分析 WLAN 最重要的信息源是信道上的数据分组，基站可使用分组嗅探器被动侦听无线介质中的全部分组。下面介绍测量的步骤：

(1) 嗅探，即搜索和记录所有无线传输帧。硬件方面，依赖网卡的探测、解码、缓存和复制功能。软件方面，驱动程序将收到的全部分组发送到内核分组过滤器。无线网卡应处于监控(混杂)模式。嗅探器生成事件日志，包含所有嗅探到的分组。

(2) 归并，即生成精确的分组记录。无线的空间差异性使单嗅探器监控所有信道并不可行，因此，需在信道中重新构建多个空间分布探测器。如果嗅探器太少、放置不合适、使用不合适的硬件等，会造成丢包、乱序以及时间戳错误等。而使用多个嗅探器，需将各自独立的记录结合起来，以微秒级的间隔进行同步来建立所有帧传输的记录。

(3) 处理，即对完成的分组记录进行实际过滤处理。首先删除记录中与分析无关的一些分组。然后解析相关参数，需与其他统计数据相结合。接下来是各种计算，如均值计算，以向用户呈现结果。

3.5.2 IEEE 802.11 的典型测量工具

目前的许多 IEEE 802.11 评测工具可用于监控网络、探测拓扑、识别异常和安全漏洞等，其中一些可用于无线网络实验。本节结合几个代表性工具进行分析说明。

1. Wireshark

Wireshark(http://www.wireshark.org/)是流行的网络数据包分析软件，可捕获数据包，详细分析数据包各层内容。它是开源的网络协议分析器，综合了多用途的包嗅探器和分析工具，可用于几乎所有类型的网络，支持数百种不同协议，可针对捕获包的不同字段建立特定过滤器。但其缺少后期处理和分析工具，只提供基础统计数据和图形。

Wireshark 是应用层软件，在 Windows 上由底层的 winpcap 提供捕获包支持，而在 Linux 上则依赖 libpcap 捕获包。其捕获和分析包如图 3.12 所示。

2. Xirrus

Xirrus(http://www.xirrus.com/Products/Wi-Fi-Inspector.aspx)是一款 WiFi 网络扫描和信号测量软件，能提供无线网络信号搜索和各网络热点信息，包括 AP 的 SSID、MAC 地址、信号强度和访问加密方式等，还有网速测试、网络质量测试等功能，能全面测量无线网络的性能。该免费软件可在 Windows 环境下运行，如图 3.13 所示。其它工具软件还有 inSSIDer、Kismet 等工具，读者可自行了解。