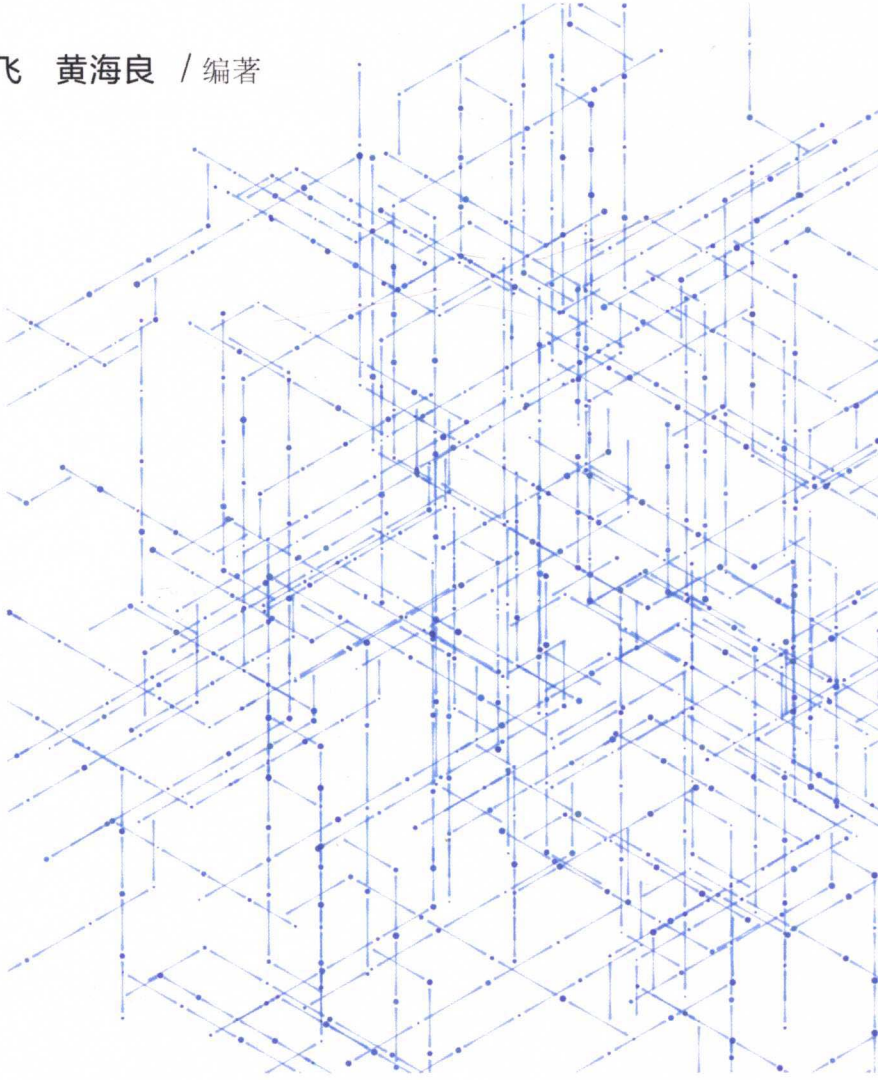
普通高等学校新工科应用型“十三五”规划教材

无线网络技术

原理、实验与网络设计

杨敬民　刘王飞　黄海良　/ 编著



厦门大学出版社 XIAMEN UNIVERSITY PRESS
国家一级出版社
全国百佳图书出版单位

普通高等学校新工科应用型“十三五”规划教材

无线网络技术

原理、实验与网络设计

WUXIANWANGLUO JISHU
YUANLI SHIYAN YU WANGLUOSHEJI

杨敬民　刘王飞　黄海良　/ 编著

厦门大学出版社 XIAMEN UNIVERSITY PRESS
国家一级出版社
全国百佳图书出版单位

图书在版编目(CIP)数据

无线网络技术:原理、实验与网络设计/杨敬民,刘王飞,黄海良编著. —厦门:厦门大学出版社,2018.12
ISBN 978-7-5615-7163-7

Ⅰ.①无… Ⅱ.①杨…②刘…③黄… Ⅲ.①无线网—研究 Ⅳ.①TN92

中国版本图书馆 CIP 数据核字(2018)第 268501 号

出 版 人 郑文礼
责任编辑 李峰伟

出版发行 厦门大学出版社
社　　址 厦门市软件园二期望海路 39 号
邮政编码 361008
总 编 办 0592-2182177　0592-2181406(传真)
营销中心 0592-2184458　0592-2181365
网　　址 http://www.xmupress.com
邮　　箱 xmup@xmupress.com
印　　刷 虎彩印艺股份有限公司

开本 720 mm×1 000 mm　1/16
印张 23.75
字数 428 千字
版次 2018 年 12 月第 1 版
印次 2018 年 12 月第 1 次印刷
定价 68.00 元

厦门大学出版社
微信二维码

厦门大学出版社
微博二维码

前　言

无线通信技术在推动信息化社会发展中的作用日益重要，在智慧校园、智慧城市等诸多领域的应用层出不穷，无线网络工程师供不应求。同时，网络工程是一门实践性很强的工科学科，以社会需求为导向，培养应用型人才，培养学生解决复杂工程问题的能力，是网络工程专业本科教育的一个发展方向。基于此，我们将长期在网络工程专业本科教学中的实践总结成本教材。

本书分为4大篇，共19章。“原理篇”主要包括无线局域网基础知识，无线通信基础，IEEE 802.11无线局域网标准，HiperLAN无线局域网标准，标准化机构，WLAN转发原理，无线射频管理，无线基本安全功能和无线地勘9章。“工具篇”介绍了完成本课程实验所需的工具软件的使用，主要包括无线射频信号分析工具WirelessMon和inSSIDer，网络流量发生器IxChariot和网络流量分析器Wireshark 4章。“实验篇”主要包括15个无线网络实验。“设计篇”主要包括无线网络设计，高可用性，移动组、AP组、RF组，漫游和设计考虑事项5章。

本书由杨敬民主持编写，其中“原理篇”由杨敬民负责编写，“工具篇”和“实验篇”的第1～8个实验由刘王飞负责编写，“实验篇”的第9～15个实验和“设计篇”由杨敬民和黄海良编写。全书由杨敬民和黄海良共同统稿和校对，研究生林敏敏、陈镇威、黄伟德、张楷雄参与了实验验证工作。

在本书的编写过程中，厦门卓网信息科技股份有限公司（Nbest Co.，Ltd.）提供了部分实验器材和实验验证场地，公司研发工程师提

供了相关技术支持,在此表示感谢。

本书的最大特点是理论结合实践,以实践为主,重点培养学生实际动手解决工程问题的能力。为了帮助学生更好地掌握实验内容,实验案例都给出了实验目的、应用场景、实验拓扑、实验设备、实验原理、实验步骤等。

本书可以作为高等院校师生无线网络教学的参考教材,也可以作为无线网络工程师的参考书。

编者:杨敬民　刘王飞　黄海良

2018 年 10 月 10 日

目　录

原理篇

工具篇

实验篇

设计篇

原理篇

第一章　无线局域网基础知识

第一节　无线局域网介绍

无线局域网(wireless local area network,WLAN)是计算机网络和无线通信技术相结合的产物。广义上的WLAN,主要采用无线电波、激光、红外线等传输媒介代替传统的电缆,如双绞线、光纤等有线传输介质,实现随时、随地的网络接入;既可以单独组网,也可以作为有线网络的补充和延伸。狭义的WLAN定义是:基于电气电子工程师学会(Institute of Electrical and Electronics Engineers,IEEE)发布的IEEE 802.11系列标准,利用高频无线射频(2.4 GHz或5 GHz频段的无线电磁波)作为传输介质的WLAN。

无线网络的初步应用可以追溯到第二次世界大战期间,当时美国陆军采用无线电信号进行资料的传输。他们研发出了一套无线电传输技术,并且采用相当高强度的加密技术,得到美军和盟军的广泛使用。

1971年,夏威夷大学(University of Hawaii)的研究员创造出第一个基于封包式技术的无线电通信网络——ALOHANET网络。ALOHANET包括7台计算机,采用双向星形拓扑(bi-directional star topology),横跨4座夏威夷的岛屿,中心计算机放置在瓦胡岛上,是最早的WLAN。

目前,国际上WLAN主要有两大标准体系:IEEE的802.11和欧洲电信标准组织(European Telecommunications Standards Institute,ETSI)的高性能无线电局域网(high performance radio local area network,HiperLAN)。

1990年,IEEE正式启用了802.11项目。自IEEE 802.11标准诞生以来,先后有802.11a、802.11b、802.11g、802.11e、802.11f、802.11h、802.11i、802.11j、802.11ac、802.11ax等标准制定或者酝酿。目前,802.11n应用已经非常普遍,在智慧校园、智慧园区、智慧城市等诸多领域得到了广泛的应用。HiperLAN则是在欧洲广泛应用的WLAN技术。

WLAN广泛应用于公司内部设备的连接,如会议室,常常用于举行会议、

培训等。通过 WLAN,会议室无须部署大量的网线、交换机和固定的网络有线接口,不仅可省下大量的布线和硬件维护费用,而且可提高会议效率。

仓库也是 WLAN 的一个主要应用场景,如可以使用 WLAN 进行货物的盘点,通过 WLAN 连接存货控制软件来跟踪货物的变化,能节省大量的人力。

医院也是 WLAN 的重要应用场所。通过 WLAN,医护人员的手持医疗终端、无线医疗器械可以更方便地接入医院的信息系统,医护人员在病房即可开展检查、开具处方,从而提高医疗效率。

与有线网络相比,WLAN 具有使用灵活、扩展方便、成本经济、安装简单等特点。

一、使用灵活

在有线网络建设中,网络布线施工工程存在施工周期长、受物理环境影响大的问题,且在施工过程中,往往需要破墙掘地、穿线架管。而 WLAN 最大的优势就是免去或减少了网络布线的工作量,一般只要安装一个或多个无线访问接入点(access point,AP)设备,就可建立覆盖整个建筑或地区的局域网络。

二、扩展方便

WLAN 可以在有线网络的基础上,通过增加无线控制器(access controller,AC)和 AP 释放无线信号。一个普通 AP 的覆盖范围在 30～100 m 之间,室外高功率 AP 有的可达 600 m。用户终端接入无线网络后,就可以在无线信号覆盖的范围内自由移动。

三、成本经济

WLAN 一般有点对点(ad-hoc)和基础架构(infrastructure)两种组网模式。ad-hoc 模式无中心拓扑结构,是由移动终端组成的临时性自治系统,这些移动终端以相同的工作组名、服务区别号(extended service set identifier,ESSID)、密码等对等的方式相互直接连接,在 WLAN 的覆盖范围之内,进行点对点与点对多点间的通信,如图 1-1 所示。infrastructure 网络以 AP 为中心,移动终端与 AP 连接后,通过 AP 接入有线网络,如图 1-2 所示。在这两种组网模式中,WLAN 对有线布线的依赖很少,或者可以依托于现有的有线网络,减少相关的成本和时间。另外,无线网络拓扑变化灵活,改造费用较低。

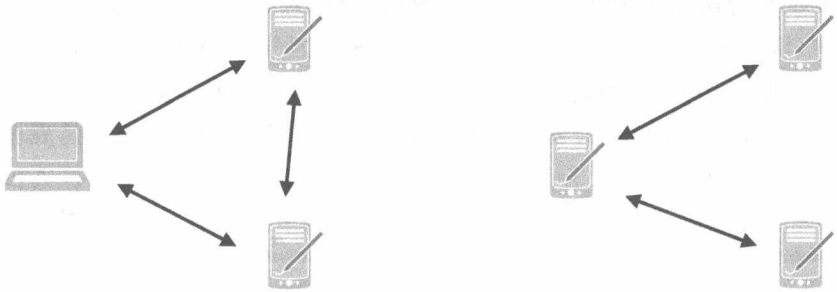


图 1-1　ad-hoc 网络架构

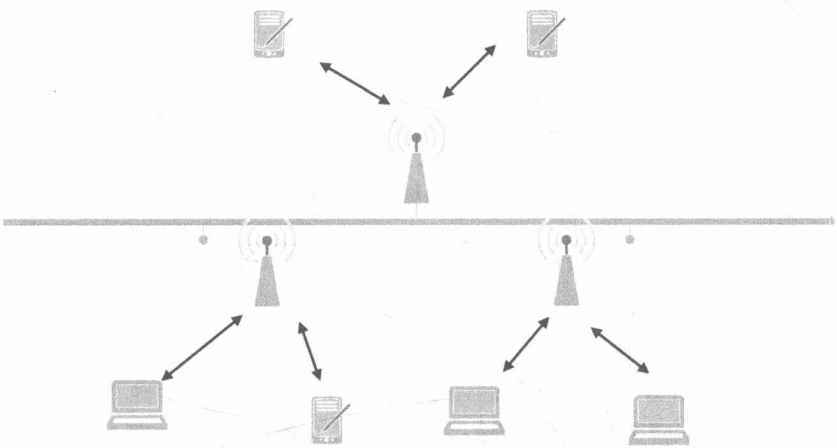


图 1-2　infrastructure 网络架构

第二节　无线网络架构

一、基本服务集

基本服务集(basic service set,BSS)是用于描述通过共享链路层特性(如射频、调制模式等)进行通信的移动设备的集合。一个 BSS 主要由分配点(redistribution point,RP)和终端(station,STA)组成,但是 RP 不是必需的。BSS 有两种类型:基础设施模式(infrastructure mode)和独立模式(independent mode)。基础设施模式的基本服务集包含一个单一的 RP 和与 RP 互连的多个 STA,如 AP 就是一类典型的 RP。RP 作为中心节点,管理整个基础设施模式的基本服务集的运行参数,STA 只能和 RP 通信,该基础设施模式的基本服务

集内的流量都由 RP 进行路由转发。基础设施模式的基本服务集通过基本服务集标识(basic service set identifier,BSSID)进行区分,BSSID 一般用 48 b 的媒体访问控制(media access control,MAC)地址充当,由前 24 b 的组织唯一标识符(organizationally unique identifier,OUI)和后 24 b 的组织自定义扩展标识符组成,如图 1-3 所示。

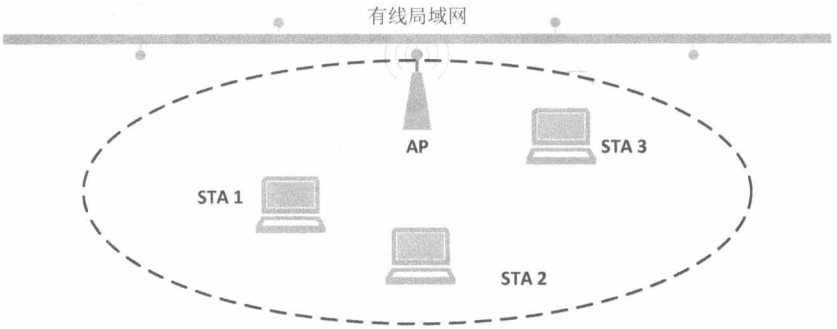


图 1-3 基础设施模式的基本服务集

独立模式的基本服务集更像是一个 ad-hoc 网络,STA 互相通信,没有 RP 作为集中点转发网络流量。独立模式的基本服务集也用 MAC 地址来作为 BSSID 的标识,但是与基础设施模式的基本服务集不同,独立模式下的 BSSID 的设置由如下规则生成:48 b MAC 中"individual/group"字段通常设置为"individual","universal/local"字段通常设置为"local",其余 46 b 随机生成,如图 1-4 所示。

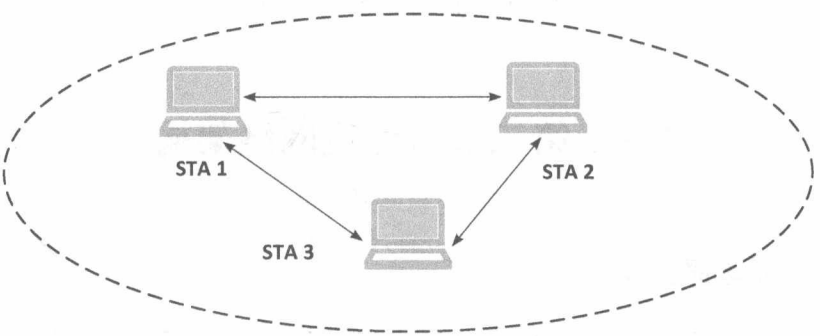


图 1-4 独立模式的基本服务集

二、扩展服务集

扩展服务集(extended service set,ESS)是在共同逻辑网段[如同样的互联网协议(internet protocol,IP)子网和虚拟局域网(virtual local area network,VLAN)]上的多个基础服务器的集合。ESS 通过扩展服务集标识(extended

service set identifier，ESSID)进行区分，有时也可以用 SSID。与 BSSID 的设定规则不同，ESSID 可以用自然语言命名，如使用英文字符，用于标识“网络名称”。SSID 是一个 32 B 的序列，IEEE 802.3 标准并不强制要求一定要有 SSID，或者 SSID 都需要唯一，或者特定编码定义。在 ESS 中，BSS 可以有多个，STA 可以在多个 BSS 中自由移动，ESS 中的 AP 相互通信，可以把数据从一个 BSS 转发到另外一个 BSS，如图 1-5 所示。

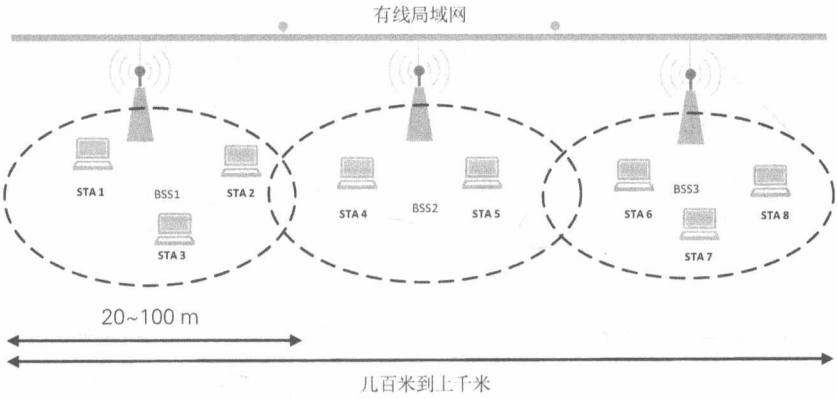


图 1-5　扩展服务集(ESS)

第三节　无线频谱资源

无线电波是频率介于 3 Hz 和约 300 GHz 之间的电磁波，也称为射频电波，或简称射频、射电。无线电技术将声音信号或其他信号经过转换，利用无线电波传播。无线电技术被广泛使用，特别是在电信领域。为防止不同用户之间的干扰，无线电波的产生和传输受国际法律的严格管制，由国际电信联盟(International Telecommunications Union，ITU)协调。ITU 规定的无线电频谱分布参见表 1-1。

ITU 为不同的无线电传输技术和应用分配了无线电频谱的不同部分，并在“无线电规则”中定义了约 40 项无线电通信业务。在某些情况下，部分无线电频谱被出售或授权给私人无线电传输业务的运营商(如蜂窝电话运营商或广播电视台)，分配频率的范围通常根据运营商提供的服务用途来确定，如分配蜂窝频谱或电视频谱。由于用户数量不断增加，导致固定资源需求增加，近几十年来无线频谱已经越来越拥挤，因此需要更加有效地利用它，以推动现代电信的创新，如扩频(超宽带)传输、频率复用、动态频谱管理、频率汇集和认知无线电。

除了ITU规定的无线电频谱分布标准,其他地区和国家也有不同的标准,如欧洲标准和中国微波标准,分别参见表1-2和表1-3。

表1-1 无线电频谱分布

ITU波段号码	频段名称	缩写	频率范围/Hz	波段	波长范围/km	用法
			≤3		≥10^5	
1	极低频	ELF	3～30	极长波	10^5～10^4	潜艇通信或直接转换成声音
2	超低频	SLF	30～300	超长波	10^4～10^3	直接转换成声音或交流输电系统(50～60 Hz)
3	特低频	ULF	300～3 000	特长波	10^3～10^2	矿场通信或直接转换成声音
4	甚低频	VLF	3 k～30 k	甚长波	10^2～10^1	直接转换成声音、超声,地球物理学研究
5	低频	LF	30 k～300 k	长波	10^1～10^0	国际广播、全向信标
6	中频	MF	300 k～3 M	中波	10^0～10^{-1}	调幅(AM)广播、全向信标、海事及航空通信
7	高频	HF	3 M～30 M	短波	10^{-1}～10^{-2}	短波、民用电台
8	甚高频	VHF	30 M～300 M	米波	10^{-2}～10^{-3}	调频(FM)广播、电视广播、航空通信
9	特高频	UHF	300 M～3 G	分米波	10^{-3}～10^{-4}	电视广播、无线电话通信、无线网络、微波炉
10	超高频	SHF	3 G～30 G	厘米波	10^{-4}～10^{-5}	无线网络、雷达、人造卫星接收
11	极高频	EHF	30 G～300 G	毫米波	10^{-5}～10^{-6}	射电天文学、遥感、人体扫描安检仪
			>300 G		<10^{-6}	

表1-2 欧洲标准

波段	类型	波长/cm	频率/GHz
A	米波		<0.25
B	米波		0.25～0.50
C	分米波	30～60	0.5～1.0
D	分米波	15～30	1～2