

21世纪高等学校规划教材 | 计算机应用

无线网络安全技术

姚琳 王雷 编著



清华大学出版社

TP393.08/504

21世纪高等学校规划教材 | 计算机应用

无线网络安全技术

姚琳 王雷 编著

清华大学出版社
北京

内 容 简 介

本书针对无线局域网、无线城域网、移动通信网、无线传感网和 Ad Hoc 网等无线网络中的安全问题进行了详细归纳和总结,内容丰富,概念和原理讲解细致,深入浅出。书中的每一章都相对独立,兼顾了通用性和系统性,对典型的案例进行了分析,并介绍了当下最新的研究进展和今后的发展趋势。

本书内容的编排充分考虑了高校的教学需求和无线网络安全课程的教学特点,可以作为网络相关专业的高年级本科生和硕士研究生的教材,也可作为其他工程技术人员和教师系统学习无线安全技术的参考书。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

无线网络安全技术/姚琳等编著. —北京:清华大学出版社,2013

21 世纪高等学校规划教材·计算机应用

ISBN 978-7-302-32466-9

I. ①无… II. ①姚… III. ①无线网—信息安全—高等学校—教材 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2013)第 106323 号

责任编辑:高买花 王冰飞

封面设计:傅瑞学

责任校对:梁 毅

责任印制:宋 林

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社总机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

课 件 下 载: <http://www.tup.com.cn>, 010-62795954

印 装 者:北京国马印刷厂

经 销:全国新华书店

开 本:185mm×260mm 印 张:15 字 数:372 千字

版 次:2013 年 10 月第 1 版 印 次:2013 年 10 月第 1 次印刷

印 数:1~2000

定 价:29.00 元

产品编号:047364-01

出版说明

随着我国改革开放的进一步深化,高等教育也得到了快速发展,各地高校紧密结合地方经济建设发展需要,科学运用市场调节机制,加大了使用信息科学等现代科学技术提升、改造传统学科专业的投入力度,通过教育改革合理调整和配置了教育资源,优化了传统学科专业,积极为地方经济建设输送人才,为我国经济社会的快速、健康和可持续发展以及高等教育自身的改革发展做出了巨大贡献。但是,高等教育质量还需要进一步提高以适应经济社会发展的需要,不少高校的专业设置和结构不尽合理,教师队伍整体素质亟待提高,人才培养模式、教学内容和教学方法需要进一步转变,学生的实践能力和创新精神亟待加强。

教育部一直十分重视高等教育质量工作。2007年1月,教育部下发了《关于实施高等学校本科教学质量与教学改革工程的意见》,计划实施“高等学校本科教学质量与教学改革工程”(简称“质量工程”),通过专业结构调整、课程教材建设、实践教学改革、教学团队建设等多项内容,进一步深化高等学校教学改革,提高人才培养的能力和水平,更好地满足经济社会发展对高素质人才的需要。在贯彻和落实教育部“质量工程”的过程中,各地高校发挥师资力量强、办学经验丰富、教学资源充裕等优势,对其特色专业及特色课程(群)加以规划、整理和总结,更新教学内容、改革课程体系,建设了一大批内容新、体系新、方法新、手段新的特色课程。在此基础上,经教育部相关教学指导委员会专家的指导和建议,清华大学出版社在多个领域精选各高校的特色课程,分别规划出版系列教材,以配合“质量工程”的实施,满足各高校教学质量和教学改革的需要。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作,提高教学质量的若干意见》精神,紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”,在有关专家、教授的倡议和有关部门的大力支持下,我们组织并成立了“清华大学出版社教材编审委员会”(以下简称“编委会”),旨在配合教育部制定精品课程教材的出版规划,讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师,其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求,“编委会”一致认为,精品课程的建设工作从开始就要坚持高标准、严要求,处于一个比较高的起点上。精品课程教材应该能够反映各高校教学改革与课程建设的需要,要有特色风格、有创新性(新体系、新内容、新手段、新思路,教材的内容体系有较高的科学创新、技术创新和理念创新的含量)、先进性(对原有的学科体系有实质性的改革和发展,顺应并符合21世纪教学发展的规律,代表并引领课程发展的趋势和方向)、示范性(教材所体现的课程体系具有较广泛的辐射性和示范性)和一定的前瞻性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐),经“编委会”认真评审,最后由清华大学出版

社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。推出的特色精品教材包括:

(1) 21 世纪高等学校规划教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2) 21 世纪高等学校规划教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 21 世纪高等学校规划教材·电子信息——高等学校电子信息相关专业的教材。

(4) 21 世纪高等学校规划教材·软件工程——高等学校软件工程相关专业的教材。

(5) 21 世纪高等学校规划教材·信息管理与信息系统。

(6) 21 世纪高等学校规划教材·财经管理与应用。

(7) 21 世纪高等学校规划教材·电子商务。

(8) 21 世纪高等学校规划教材·物联网。

清华大学出版社经过三十多年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

联系人:魏江江

E-mail: weijj@tup.tsinghua.edu.cn

前言

在网络信息技术高速发展的今天,信息安全已变得至关重要,信息安全已成为信息科学的热点课题。“无线网络安全”作为信息安全专业、软件工程专业及物联网工程专业的一门重要的专业课,主要讲解各种无线网络中的安全问题及其基本对策。通过学习这门课程,可以提高和培养学生无线安全协议方面的分析和设计能力以及学生综合知识运用能力和创新能力。

无线网络的开放性、移动性、动态的拓扑结构、无线信道的不可靠性以及无线设备资源的有限性,导致了无线通信环境下更容易发生主动攻击和被动攻击,原本在有线环境下的安全方案和安全技术不能直接应用于无线环境。所以,编者精心组织编写了本书,让读者对无线环境下的安全机制有更好的了解。

本书对当今主流的无线技术——无线局域网、无线城域网、移动通信网、无线传感网和Ad Hoc网的概念进行了概要阐述,对每种无线网络下的安全问题、安全目标、安全机制进行了系统性和先进性的阐述。以实际应用案例来阐述相关知识模块,做到了理论和实践联系,对安全协议设计中的普遍问题和解决方法进行了介绍,并融合了对相关科研领域最新发展和成果的介绍。

本书的思路是作者从多年的计算机网络、无线通信技术、信息安全技术等课程的教学基础上探索出来的,并结合作者的科研工作。本书体系也经过了两年以上的本科教学的检验,效果较好。

尽管本书由笔者本人独立撰写,但思路的形成和工作的积累得到了业内许多专家和老师的影响和帮助,首先要感谢这些老师和朋友!他们是来自大连理工大学的徐遣、宋奇、张天宇、张家宁等。本书参考和引用了许多学者的著作和文章,在此表示感谢!尤其需要说明的是,本书有些内容来源于我的教学讲义,讲义的形成过程长、文献引用渠道多,其中可能包含某个专家的发言、网页、笔记、文献摘要等,多数内容已经沉淀在我的记忆中,尽管我们也做了文献核对和查找工作,但还是难以一一标出某些文献出处,因此要特别对这些有价值的工作表示感谢!

限于时间和作者本身水平的局限性,书中难免有错漏之处,恳请读者给予批评指正。

姚琳 王雷

2013年5月于大连

目 录

第 1 章 无线网络导论	1
1.1 无线网络概述	1
1.1.1 无线网络的历史背景	1
1.1.2 无线网络的分类	2
1.1.3 无线网络未来的发展和挑战	6
1.2 无线网络安全概述	10
1.2.1 无线网络的安全要求	10
1.2.2 无线网络与有线网络的区别	11
1.2.3 无线网络安全威胁	12
1.2.4 无线网络安全研究现状	15
1.3 本书结构	17
思考题	18
参考文献	18
第 2 章 无线局域网安全	19
2.1 无线局域网基本概念	19
2.2 WEP 协议分析	22
2.2.1 WEP 协议原理	22
2.2.2 WEP 协议安全分析	24
2.3 IEEE 802.1x 协议分析	26
2.3.1 IEEE 802.1x 协议原理	26
2.3.2 IEEE 802.1x 安全分析	30
2.4 WAPI 协议分析	32
2.4.1 WAPI 协议原理	33
2.4.2 WAPI 安全分析	34
2.5 IEEE 802.11i 协议分析	35
2.5.1 IEEE 802.11i 协议原理	35
2.5.2 IEEE 802.11i 安全分析	39
2.6 IEEE 802.11r 协议分析	40
2.6.1 基于 IEEE 802.11r 的快速切换方案	41
2.6.2 IEEE 802.11r 安全分析	43
2.7 IEEE 802.11s 协议分析	44

2.7.1 IEEE 802.11s 协议原理	44
2.7.2 IEEE 802.11s 安全分析	48
2.8 本章小结	50
思考题	50
参考文献	51
第3章 无线城域网安全	52
3.1 无线城域网简介	52
3.1.1 无线城域网概述	52
3.1.2 IEEE 802.16 分析	52
3.2 IEEE 802.16 标准的安全机制分析	54
3.2.1 安全风险及保护协议	54
3.2.2 密钥的分配更新方法	57
3.2.3 加密方法分析	58
3.3 WiMAX 两种典型标准的安全机制分析	59
3.3.1 IEEE 802.16d 标准	59
3.3.2 IEEE 802.16e 标准	63
3.4 WLAN Mesh 快速切换与漫游接入认证协议	66
3.4.1 WLAN Mesh 切换	67
3.4.2 WLAN Mesh 漫游接入	71
3.5 本章小结	75
思考题	75
参考文献	75
第4章 移动通信安全	77
4.1 移动通信系统概述	77
4.2 GSM 系统安全	78
4.2.1 GSM 系统简介	78
4.2.2 GSM 安全分析	82
4.3 GPRS 安全	85
4.4 UMTS 系统安全	88
4.4.1 UMTS 系统简介	89
4.4.2 UMTS 安全分析	92
4.5 第三代移动通信系统安全	97
4.5.1 第三代移动通信系统简介	97
4.5.2 第三代移动通信系统安全分析	99
4.6 第四代移动通信系统安全展望	106
4.7 本章小结	110
思考题	111

参考文献	111
第 5 章 移动用户的安全和隐私	112
5.1 移动用户面临安全问题概述	112
5.2 实体认证机制	113
5.2.1 域内认证机制	113
5.2.2 域间认证机制	118
5.2.3 组播认证机制	122
5.3 信任管理机制	131
5.3.1 信任和信任管理	131
5.3.2 基于身份策略的信任管理	135
5.3.3 基于行为信誉的信任管理	138
5.4 位置隐私	140
5.4.1 基于位置服务的位置隐私	142
5.4.2 位置隐私保护举例	147
5.5 本章小结	150
参考文献	151
第 6 章 无线传感器网络安全	153
6.1 无线传感器网络概述	153
6.1.1 无线传感器网络的特点	154
6.1.2 无线传感器网络的安全威胁	155
6.1.3 无线传感器网络的安全目标	157
6.2 无线传感器网络安全路由协议	158
6.2.1 安全路由概述	158
6.2.2 典型安全路由协议及安全性分析	159
6.3 无线传感器网络密钥管理及认证机制	162
6.3.1 密钥管理的评估指标	162
6.3.2 密钥管理分类	163
6.3.3 密钥管理典型案例	165
6.4 无线传感器网络认证机制	166
6.4.1 实体认证机制	167
6.4.2 信息认证机制	170
6.5 无线传感器网络位置隐私保护	172
6.5.1 位置隐私保护机制	172
6.5.2 典型的无线传感器网络位置隐私保护方案	173
6.6 入侵检测机制	175
6.6.1 入侵检测概述	175
6.6.2 入侵检测体系结构	176

6.7 本章小结	177
思考题	178
参考文献	178
第7章 移动 Ad Hoc 网络安全	181
7.1 移动 Ad Hoc 网络概述	181
7.1.1 移动 Ad Hoc 网络特点	181
7.1.2 移动 Ad Hoc 网络安全综述	182
7.1.3 移动 Ad Hoc 网络安全目标	183
7.2 移动 Ad Hoc 网络路由安全	184
7.2.1 路由攻击分类	184
7.2.2 安全路由解决方案	187
7.3 移动 Ad Hoc 网络密钥管理	188
7.3.1 完善的密钥管理的特征	189
7.3.2 密钥管理方案	189
7.4 入侵检测	191
7.4.1 入侵检测概述	191
7.4.2 传统 IDS 问题	192
7.4.3 新的体系结构	193
7.5 无线 Mesh 网络安全	194
7.5.1 无线 Mesh 网络概述	194
7.5.2 Mesh 安全性挑战	196
7.5.3 Mesh 其他应用	200
7.6 本章小结	202
思考题	202
参考文献	202
附录 A 密码学基础	205
A.1 密码学基本知识	205
A.2 对称密码机制	206
A.2.1 对称加密原理	206
A.2.2 古典密码	206
A.2.3 序列密码	208
A.2.4 分组密码	210
A.2.5 分组加密工作模式	215
A.3 公钥密码算法	219
A.3.1 公钥密码算法简介	219

A. 3. 2	RSA	220
A. 3. 3	Diffie-Hellman	221
A. 4	密码学数据完整性算法	222
A. 4. 1	密码学 Hash 函数	222
A. 4. 2	消息认证码	225
A. 5	小结	226

第1章

无线网络导论

1.1 无线网络概述

在过去的十年中,整个世界逐渐走向移动化,连接世界的传统方式已经无法应付日益加快的生活节奏和全球化的步伐所带来的挑战。因此,一个新的概念“无线网络”便应运而生。

无线网络代表了任何一种使用无线连接(但不包括无线电波)的计算机网络。目前,家庭、企业(商业机构)和电信网络都大量地采用无线网络连接,目的是避免在楼房内安装光纤电缆,或者是在不同地区的设备之间建立连接而产生巨大的开销。无线通信网络通常是通过无线电通信来实现和管理,这是在 OSI 网络模型结构的物理层实现的。如果必须通过实体电缆才能够连接到网络,用户的活动范围势必大幅缩小。无线网络便无此限制,用户可以享有较宽广的活动空间。因此,无线技术正逐渐侵占传统的“固定式”或“有线式”网络所占有的领域。

1.1.1 无线网络的历史背景

无线网络的历史背景可以追溯到无线电波的发明。1888年,海因里希·赫兹发现并率先提出了无线电波的概念。1896年,古列尔默·马可尼实现了通过电报光纤传送信息。他在1901年把长波无线电信号从康沃尔(位于英国的西南部)跨过大西洋传送到3200km之外的圣约翰(位于加拿大)的纽芬兰岛。他的发明使双方可以通过彼此发送用模拟信号编码的字母数字符号来进行通信。

“二战”期间,美国军队率先在数据传输中使用无线电信号。这给之后的科学研究提供了灵感:1971年,夏威夷大学的研究小组基于无线电通信网络——ALOHNET设计了第一个报文。ALOHNET是第一个无线局域网(WLAN)。第一个WLAN包含了7台计算机,它们构成了一个双流向的星形拓扑以实现相互通信。

第一代的WLAN技术采用了未经许可的频带(902~928 MHz ISM),这一频带随后被小型的应用和工业机械的通信干扰所阻塞。一种扩频技术随后被用来减小这种干扰,它每秒可以传输50万比特。第二代的WLAN技术的传输速率达到了2Mbps,是第一代的四倍。第三代的WLAN技术和第二代WLAN运行在同样的频带上,这也是我们今天仍然用到的WLAN技术。

1990年,IEEE 802.11执行委员会建立了802.11工作小组来设计无线局域网

(WLAN)标准。这一标准规定了在 2.45GHz ISM 频带下的工作频率。在 1997 年,工作小组批准 IEEE 802.11 成为世界上第一个 WLAN 标准,规定的数据传输速率是 1Mbps 和 2Mbps。

除 WLAN 之外,无线网络还衍生出多种应用:无线网络技术使商业企业能够发展广域网(WAN)、城域网(MAN)和个域网(PAN)而无需电缆设备;IEEE 开发了作为无线局域网标准的 802.11;蓝牙(Bluetooth)工业联盟也在致力于能提供一个无缝的无线网络技术。

蜂窝或移动电话是马可尼无线电报的现代对等技术,它提供了双方的、双向的通信。第一代无线电话使用的是模拟技术,这种设备笨重且覆盖范围是不规则的,然而它们成功地向人们展示了移动通信的固有便捷性。现在的无线设备已经采用了数字技术。与模拟网络相比,数字网络可以承载更高的信息量并提供更好的接收和安全性。此外,数字技术还将带来可能的附加值的服务,诸如呼叫者标识。更新的无线设备使用能支持将更高信息速率的频率范围连接到 Internet 上。

无线技术为人类社会带来了深刻的影响,而且这种影响还会继续。没有几个发明能够用这样的方式使整个世界“变小”。定义无线通信设备如何相互作用的标准很快就会有一致的结果,人们不久就可以构建全球无线网络,并使之提供广泛的多种服务。

1.1.2 无线网络的分类

无线网络可根据数据传输的距离分为下面几种不同类型。

1. 无线个域网

无线个域网(WPAN)是计算设备之间通信所使用的网络,这些计算设备包括电话、个人数据助手(PDA)等。PAN 可以使用在私人设备之间的通信,或者与更高级别的网络或者因特网(向上连接)取得连接。无线个域网是采用了多种无线网络技术的个域网,这些网络技术包括:IrDA,无线 USB,蓝牙,Z-Wave,ZigBee,甚至是人体域网。WPAN 的覆盖范围从几厘米到几米不等。IEEE 802.15 工作组为 HomeRF 和 Bluetooth 等 WPAN 制定了相关的物理层和 MAC 层标准,同时也处理了一些包括与 IEEE 802.11 局域网共同存在的问题。

HomeRF 是关于 PC 与各类电器之间语音和数据数字通信的技术标准。它可以连接 PC、打印机、电话、互联网等,如图 1-1 所示。Bluetooth 是在小范围语音和数据通信的技术标准。Bluetooth 的应用包括 PC 使用无线连接键盘、鼠标器等设备,在小范围的无线局域网、蜂窝网络、有线网络和卫星网络的 AP 等。Bluetooth 制定了协议栈以支持各种传输介质和各种各样的应用。Bluetooth 物理层采用 FHSS 和 GFSK,工作频率在 2.402GHz 到 2.480GHz,数据传送速率是 1Mbps。Bluetooth 的 MAC 层采用 FH-CDMA/TDD 机制。

2. 无线局域网

无线局域网(WLAN)采用一些分布式无线措施(通常是扩频或 OFDM 无线电技术)来连接两个或更多的设备,并且在一个接入点向更大的互联网范围提供连接。像广域网一样,局域网也是一种由各种设备相互连接,并在这些设备间提供信息交换手段的通信网络。这

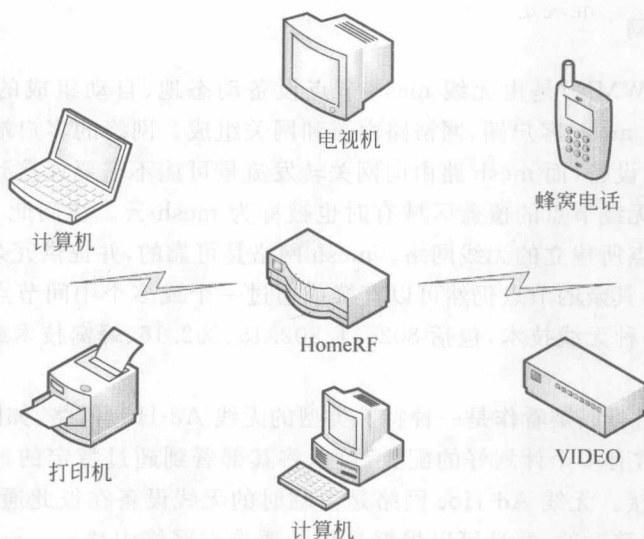


图 1-1 无线个域网

给用户提供了更多的移动性,使得他们可以在局域性的覆盖区域内移动的同时接入网络。而相对于广域网,局域网的范围较小,通常是一栋楼或一片楼群,但是局域网内的数据传输速率通常要比广域网的高得多,大多数的现代 WLAN 技术都是基于 IEEE 802.11 标准,以 Wi-Fi 提供商的品牌名字命名并运营。WLAN 曾经被美国国防部称为 LAWN(在本地区提供无线网络)。

无线局域网因其易于安装的优势,在家用网络中得到了非常广泛的应用,并且在很多商业场所都向客户提供免费的接入服务。

IEEE 802.11 是关于无线局域网的标准,它主要涉及物理层和介质访问子层(MAC 层)。在 IEEE 802.11 标准无线用户通过接入点(AP)连接到网络,每个用户终端使用无线网卡与 AP 连接。无线网卡和 AP 支持 IEEE 802.11 物理层和 MAC 层标准,同样 AP 也负责将这些用户连接到像 IEEE 802.3 那样的网络。图 1-2 显示了 WLAN 和 LAN 的连接。

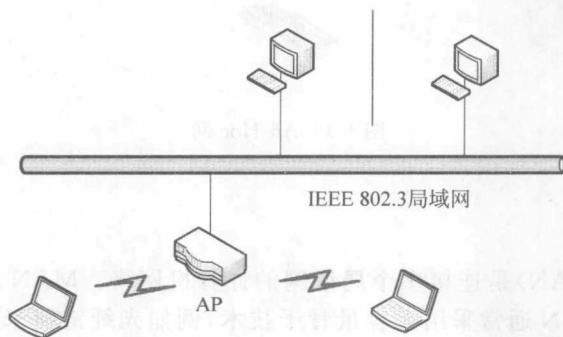


图 1-2 WLAN 和 LAN 的连接

3. 无线 mesh 网

无线 mesh 网(WMN)是由无线 mesh 节点设备动态地、自动组成的通信网络。无线 mesh 网络通常是由 mesh 客户端、网格路由器和网关组成。网络的客户端往往是笔记本电脑、手机和其他无线设备,而 mesh 路由向网关转发流量可能不需要连接到互联网。为一个单一的网络工作的无线节点的覆盖区域有时也被称为 mesh 云。访问此 mesh 云是依赖于彼此和谐工作的节点所建立的无线网络。mesh 网络是可靠的,并提供冗余检错。当一个节点不能工作的时候,其余的节点仍然可以直接或通过一个或多个中间节点互相通信。无线 mesh 网络可以与各种无线技术,包括 802.11、802.15、802.16、蜂窝技术或多种类型的组合来实现。

无线 mesh 网络可以被看作是一种特殊类型的无线 Ad-Hoc 网络,如图 1-3 所示。一个无线 mesh 网络通常有多个计划好的配置,可以将其部署到超过特定的地理区域中来提供动态的和高效的连接。无线 Ad-Hoc 网络是由临时的无线设备在彼此通信范围内形成的。mesh 路由器是可以移动的,并且可以根据具体的要求在网络中移动。mesh 路由器通常不受节点的资源限制,因此可以用来执行更多资源密集型的功能。由于 Ad-Hoc 网络中的节点通常受资源约束,所以无线 mesh 网络与 Ad-Hoc 网络有所不同。

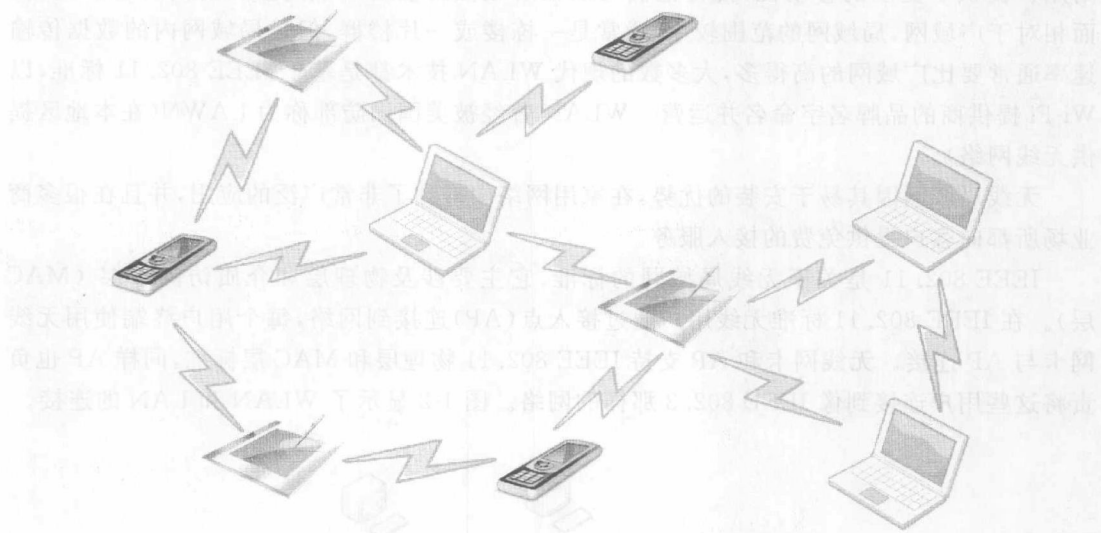


图 1-3 Ad-Hoc 网

4. 无线城域网

无线城域网(WMAN)是连接多个局域网的计算机网络。MAN 经常覆盖一个城市或者是大型的校园。MAN 通常采用大容量骨干技术,例如光纤链路来连接多个局域网。此外 MAN 还能向更大的网络(如 WAN)提供向上连接服务。

人们之所以对城域网感兴趣,是因为用于广域网中的传统的点到点连接和交换网络技术不足以满足一些组织机构不断增长的通信需求。局域网标准中的高度共享媒体技术具有很多的优点,这些都可以在构建城市范围的网络中实现。

无线城域网的主要市场是那些在城市范围内对高容量通信有需求的用户。相比于从本地电话公司那里获得的同样服务,一个无线城域网就是要以更低的成本和更高的效率为用户提供所需容量的通信服务。

5. 无线广域网

无线广域网(WWAN)是无线网络的一种。相比于局域网,广域网覆盖了更大的地理范围。它可能需要通过公共信道,或者至少有一部分依靠的是公共载波电路进行传输。一个典型的无线广域网包括了多个相互连接的交换节点。所有的传输过程都是从一个设备出发,途经这些网络节点,最后到达所规定的目的设备。所有规模的无线网路为电话通信、网页浏览和串流视频影像等应用提供数据传输服务。

无线广域网采用了无线通信蜂窝网络技术来传输数据。例如 LTE, WiMAX(通常也称为无线城域网, WMAN), UMTS, CDMA 2000, GSM 等。GSM 数字蜂窝系统是由欧洲电信公司提出的标准, CDMA 接入技术采用 TDMA 和 FDMA, 调制采用 GMSK 技术。WLAN 也可以采用局域多点分布式接入服务(LMDS)或者 Wi-Fi 来提供网络连接。这些技术是区域性、全国性甚至是全球性的,并且是由无线服务提供商负责提供。WWAN 的连通性使得持有便携式计算机和 WWAN 上网卡的用户可以浏览网页、收发邮件,或者接入虚拟私人网络(VPN)。只要用户处在蜂窝网络服务的区域范围之内,就都能够享受到 WWAN 带来的服务。不同的计算机有着统一的 WWAN 性能。

目前中国当前可供选择的无线广域通信服务,有联通 CDMA1X 服务、移动公司的 GPRS 服务、中国卫星通信公司的专线服务等。

6. 蜂窝网络

蜂窝网络(或移动网络)是一个分布在陆地区域的无线网络,称为“细胞”,每一个“细胞”都由一个固定的无线电收发机提供服务,这也被称为移动通信基地台或者基站。在蜂窝网络中,每一个“细胞”通常都采用与其他邻居“细胞”相同的无线电频率来避免干扰。

当共同加入网络后,这些“细胞”在广阔的地理区域内提供无线电覆盖。这使得大多数便携的无线电收发机(例如:移动电话,寻呼机等)可以相互之间或者是与网络中任意固定的电话和收发机通过基站进行通信。即使一些收发机在多个细胞之间移动,通信也不会受到影响。

尽管蜂窝网络最初是为移动电话设计的,但随着智能手机的发展,蜂窝电话网络在电话对讲之外还照常携带数据进行传输:

(1) 全球移动通信系统(GSM): 全球移动通信系统网络可以分为三个主要系统: 交换系统, 基站系统和运营支持系统。连接到基站的移动电话可以接入运营支持系统站点; 再接入交换系统站点, 在这里, 通话可以被转发到它需要去的地方。GSM 是目前最常用的标准, 并且它在绝大多数的移动电话中得到了使用。

(2) 个人通信服务(PCS): PCS 是一种无线电波段, 它在北美和南亚地区的移动电话中得到使用。Sprint 成为第一个创立 PCS 的服务提供商。

(3) D-AMPS: 数字高级移动电话服务(D-AMPS)是 AMPS 的一种升级版本, 由于技术的更新, AMPS 正逐渐被淘汰。新的 GSM 网络也正在代替旧的系统。

1.1.3 无线网络未来的发展和挑战

1. 无线局域网的应用前景

作为无线网络中应用最广的技术,无线局域网技术经过不断的发展,目前正逐渐趋于成熟,但仍在产生着意义重大的革新,目的是在与有线网络和蜂窝网络的竞争中处于优势。此外,WLAN 也在不断产生分化,尽管其核心特征正逐渐商品化并且服务提供商正逐渐趋于统一。例如,WLAN 的传输速度,正呈指数增长,并计划最早在 2013 年达到多倍十亿比特每秒的速率。所有的无线网络服务提供商正逐渐走在一起,致力于提升所部署服务的可信性和安全性,这在之前几乎是纸上谈兵的事,现在却即将变成现实。

商业领域产生的对于 WLAN 性能的新要求正逐渐提高,特别是在移动设备变得更流行和多样化的今天。这种发展趋势的关键驱动在于商业用户对所用设备的可用性和功能性提出了严格的要求。这意味着对于智能手机、便携式计算机和多媒体应用设备在商务环境下的要求更高,并且对于企业级的 WLAN 也有着不同的严格要求。

技术的发展同样也在支持着 WLAN 的进步:便携式计算机和平板电脑都依赖于 Wi-Fi 的发展。此外,随着无线热点、酒店接入点和其他形式的公共无线接入点有着更广泛的应用,商务人士和其他职场雇员会越来越多地利用 Wi-Fi,并在他们的办公场所对 Wi-Fi 的服务质量有同样高的期待。这将会使得相关 WLAN 服务提供组织的建立,它们具备更快适应新的无线网络技术的能力,以更好地服务于移动用户。这与商务人士开始严格要求无线网络下的无打扰的连接、高速传播的多媒体应用和所有形式的基于云的功能等需求密切相关。

与此同时,不断进步的工业化标准以及服务提供商的技术革新使得 WLAN 速率显著提高,并且更加可信且更加安全。现行的 802.11n 标准相比于之前的 802.11g 版本在数据吞吐量方面有着 10 倍的提升,从 54Mbps 到将近 GBE。这有助于弥补有线和无线环境的性能差距。事实上,企业应该考虑的是 802.11n 而不是工作站的电缆分支,如果该标准能够有效部署,这将创建一个真正的无线办公室,而伴随着这些优点的同时也满足了带宽的要求。

2. 无线传感网的发展

无线传感网(WSN)在过去几年已经成为最受关注的研究领域之一。WSN 是由若干无线传感器节点形成的一个传感器区域和一个接收器。这些有能力感知周围环境的大量节点,执行有限的计算和无线通信进而形成了 WSN。最近无线和电子技术的进步已经使无线传感网在军事、交通监视、目标跟踪、环境监测和医疗保健监控等方面有了很广阔的应用。随之而来有许多新的挑战已经浮出水面,无线传感网要满足各种应用的要求,如检测到的传感器数量、节点大小、节点的自主性等。因此需要改进当前的技术,更好地迎接这些挑战。未来传感器的发展必须功能强大并节约成本,让应用程序使用它们,如水下声学传感器系统、基于传感器的信息物理系统、对时间有严格要求的应用、认知传感和频谱管理、安全和隐私管理等。无线传感器在如下几个典型领域得到了广泛应用。

1) 认知感应

认知传感器网络通过部署大量智能的和自治的传感器来获取本地的和周围环境的信息。管理大量的无线传感器是一项复杂的任务。认知感应两个众所周知的例子是群智能和