移动互联网安全丛书

移动网络安全
体系架构与防护技术

Mobile Network Security
Architecture and Defense Technology

张 滨/冯运波/王庆丰/袁 捷
王红艳/李祥军/于 乐/李 斌 编著

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

移动互联网安全丛书

移动网络安全
体系架构与防护技术

Mobile Network Security
Architecture and Defense Technology

张　滨/冯运波/王庆丰/袁　捷
王红艳/李祥军/于　乐/李　斌　编著

人民邮电出版社
北京

图书在版编目（CIP）数据

移动网络安全体系架构与防护技术 / 张滨等编著
. -- 北京 : 人民邮电出版社, 2016.11
（移动互联网安全丛书）
ISBN 978-7-115-43872-0

Ⅰ. ①移… Ⅱ. ①张… Ⅲ. ①移动网－安全技术
Ⅳ. ①TN929.5

中国版本图书馆CIP数据核字(2016)第255160号

内 容 提 要

本书全面介绍了网络安全体系架构和防护技术，内容新颖、理论知识与实际案例并重。本书由浅入深、由概括到具体地讲解了移动网络的安全体系架构、安全防护技术与安全管理方案，以移动网络发展为主线，涵盖了移动网络基础知识、安全威胁分析、安全体系架构、网络安全防护技术等。

本书适合移动互联网从业人员、IT 技术人员、咨询分析师、科研人员及其他对移动网络安全感兴趣的人士阅读。

◆ 编　　著　张　滨　冯运波　王庆丰　袁　捷
　　王红艳　李祥军　于　乐　李　斌
责任编辑　代晓丽
执行编辑　刘　琳
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京隆昌伟业印刷有限公司印刷

◆ 开本：700×1000　1/16
印张：10.5　　2016 年 11 月第 1 版
字数：206 千字　　2016 年 11 月北京第 1 次印刷

定价：58.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广字第 8052 号

前　言

随着移动互联网的高速发展，网络速度越来越快，移动用户也越来越多地使用移动通信网络来进行社会经济生活。高速的网络发展一方面带来了巨大的社会价值和经济价值，另一方面也带来了潜在的信息安全风险。通信网络一旦出现安全问题，就会造成用户的信息沟通障碍、信息泄漏及经济损失，带来无法预料的损失。

随着移动互联网环境中移动终端和业务平台的逐步开放，受 TCP/IP 协议族的脆弱性、终端操作系统的安全漏洞、攻击技术的普及等因素影响，移动互联网下的安全管理形势将会更加复杂。移动互联网上的安全问题逐渐呈现出来，网络上出现了大量如 GTP over Billing 攻击、DDoS 攻击、DHCP 地址耗尽攻击、伪冒地址恶意阻断上下文攻击、“沉默诅咒”拒绝服务攻击、垃圾信息群发、隐私信息窃取、手机病毒等在内的威胁移动互联网安全事件。2014 年 12 月 18 日据《华盛顿邮报》报道，德国科学家发现全球移动通信网络 SS7 信令系统存在重大漏洞，可导致对全球任何手机用户进行定位及监听通话和短信；2015 年 8 月，澳大利亚电视节目《60 分钟时事》展示了黑客利用 SS7 信令系统缺陷实现对国会议员的远程监听和定位。

移动通信网络安全关系到用户财产安全、个人信息安全、社会稳定及国家安全。移动通信网络的安全管控需要国家、行业、通信厂商及用户各个方面的共同努力。本书以当前广泛应用的通信系统和代表发展趋势的通信网络安全新技术为背景，在介绍移动通信网络基本原理的基础上，充分反映出最新的通信网络安全技术的发展。

本书作者均有多年从事通信网络安全工作的经验，不仅参与了电信行业通信网络安全相关标准的制定、电信运营商对通信网络安全环境的治理，还在长期实践中形成了较全面的移动通信网络安全视角。本书在系统深入阐述通信网络安全理论知识的基础上，结合实际案例，详细分析了移动通信网络各层面的安全风险。

特别鸣谢中国移动通信研究院张峰博士、设计院董江波博士对书稿内容提出的宝贵意见。

移动通信网安全技术发展日新月异，作者愿与广大读者深入交流、共同进步。

由于作者水平有限，书中不当之处恐难避免，敬请广大作者批评指正。

作　者

2016 年 10 月

目　录

第 1 章　绪论 …… 1

1.1　移动互联网体系架构 …… 1
1.1.1　通信技术的演进 …… 4
1.1.2　移动互联网的关键技术 …… 5
1.2　移动互联网的组成 …… 11
1.3　移动互联网的发展 …… 11
1.3.1　移动互联网的发展趋势 …… 12
1.3.2　移动互联网对网络的影响 …… 13
参考文献 …… 14

第 2 章　移动通信网络安全 …… 15

2.1　移动通信网络的安全现状 …… 15
2.2　移动通信网络的安全风险 …… 18
2.2.1　身份假冒攻击风险 …… 18
2.2.2　单向鉴权安全风险 …… 19
2.2.3　加密算法的弱点 …… 19
2.2.4　信令系统安全风险 …… 20
2.2.5　拒绝服务攻击 …… 21
2.3　移动通信网络的安全保障 …… 21
2.3.1　核心网安全防护 …… 22
2.3.2　支撑网安全防护 …… 22
2.3.3　网络传输安全防护 …… 23
参考文献 …… 24

第 3 章　2G 网络安全体系架构 …… 25

3.1　GSM 通信系统 …… 25
3.1.1　GSM 网络结构 …… 25

3.1.2 GSM 安全机制 …… 28
3.2 CDMA 通信系统 …… 35
3.2.1 CDMA 网络结构 …… 35
3.2.2 CDMA 安全机制 …… 40
3.3 GPRS 通信系统 …… 43
3.3.1 GPRS 网络结构 …… 43
3.3.2 GPRS 安全机制 …… 47
参考文献 …… 48

第 4 章 3G 网络安全体系架构 …… 49

4.1 WCDMA 通信系统 …… 49
4.2 TD-SCDMA 通信系统 …… 50
4.3 CDMA2000 通信系统 …… 50
4.4 3G 网络安全 …… 51
4.4.1 网络接入安全 …… 52
4.4.2 网络域安全 …… 53
4.4.3 用户域安全 …… 53
4.4.4 应用域安全 …… 53
4.4.5 安全可见度和可配置性 …… 53
4.5 WiMAX 安全框架 …… 54
4.5.1 IEEE 802.16 标准及 WiMAX 概述 …… 54
4.5.2 IEEE 802.16d 固定无线接入安全机制 …… 57
4.5.3 IEEE 802.16e 移动无线接入安全机制 …… 63
4.5.4 IEEE 802.16e 安全原理 …… 63
参考文献 …… 64

第 5 章 4G 网络安全体系架构 …… 65

5.1 LTE/SAE 系统结构 …… 65
5.1.1 LTE 系统（E-UTRAN） …… 66
5.1.2 EPC 系统（SAE） …… 67
5.2 LTE/SAE 安全体系框架 …… 68
5.2.1 接入层的安全机制 …… 69
5.2.2 非接入层的安全机制 …… 70
5.2.3 网络域的安全机制 …… 70
5.3 LTE 系统中的无线接口安全 …… 71
5.4 LTE 系统中的用户安全 …… 73
5.4.1 密钥架构 …… 73

5.4.2 安全鉴权机制 ····· 74
5.5 LTE 系统中的传输安全 ····· 75
5.5.1 下行多址接入技术 ····· 76
5.5.2 上行多址接入技术 ····· 78
参考文献 ····· 79

第 6 章 下一代网络的安全愿景 ····· 80

6.1 5G 网络介绍 ····· 81
6.2 5G 网络架构 ····· 82
6.3 5G 网络安全风险 ····· 83
6.3.1 终端形式及其安全考虑 ····· 85
6.3.2 5G 接入网安全 ····· 86
6.3.3 5G 核心网安全 ····· 87
6.3.4 NFV 网络安全 ····· 89
6.4 5G 网络安全架构愿景 ····· 99
参考文献 ····· 102

第 7 章 WLAN 网络安全体系架构 ····· 103

7.1 WLAN 网络架构 ····· 103
7.2 WLAN 的认证及安全问题 ····· 105
7.2.1 Cookie 安全问题 ····· 105
7.2.2 伪 AP 接入钓鱼攻击 ····· 107
7.2.3 接入非授权假冒 AP ····· 107
7.2.4 IP 地址冒用攻击 ····· 108
7.2.5 接入认证方式 ····· 108
7.2.6 WLAN 服务的数据安全 ····· 109
7.2.7 手机用户接入认证问题 ····· 110
7.2.8 WLAN 安全策略 ····· 110
7.3 WLAN 的网络安全问题 ····· 111
7.3.1 Web Portal 安全防护 ····· 111
7.3.2 ARP 泛滥攻击 ····· 112
7.3.3 利用 DNS 端口绕开计费问题 ····· 112
7.3.4 对 AP 的 DoS 攻击 ····· 113
7.3.5 伪 DHCP 服务器攻击 ····· 113
7.3.6 IP 地址滥用问题 ····· 114
7.4 WLAN 的安全管理与监控问题 ····· 114
7.5 WLAN 的协议安全问题 ····· 118

7.5.1 WAPI 协议安全性 ····· 118
7.5.2 IEEE 802.1x 协议安全性 ····· 119
7.5.3 IEEE 802.11i 协议安全性 ····· 121
7.5.4 IEEE 802.11r 协议安全性 ····· 125
7.5.5 IEEE 802.11s 协议安全性 ····· 126
7.6 WEP 安全性 ····· 129
7.6.1 WEP 漏洞 ····· 129
7.6.2 WEP 数据帧 ····· 130
7.6.3 WEP 的加解密机制 ····· 130
7.6.4 WEP 的身份认证 ····· 131
参考文献 ····· 131

第 8 章 移动通信网络的安全防护 ····· 133

8.1 流量清洗 ····· 133
8.2 恶意软件监控 ····· 136
8.3 DPI 技术应用 ····· 138
8.3.1 DPI 技术的分类 ····· 138
8.3.2 DPI 技术的特征 ····· 139
8.3.3 DPI 技术的功能 ····· 140
8.4 OTT 业务安全 ····· 141
8.5 不良信息治理 ····· 143
参考文献 ····· 145

第 9 章 移动通信网络的业务安全服务 ····· 146

9.1 GBA 安全认证 ····· 146
9.1.1 GBA 体系结构 ····· 146
9.1.2 GBA 认证流程 ····· 148
9.2 业务流精细化运营 ····· 151
9.3 OTT 业务安全管控 ····· 152
参考文献 ····· 154

缩略语列表 ····· 155

第1章 绪 论

移动互联网（Mobile Internet，MI）是一种通过智能移动终端，采用移动无线通信方式获取业务和服务的新兴业务，包含终端、软件和应用3个层面。终端层包括智能手机、平板电脑、电子书、移动互联网设备（Mobile Internet Devices，MID）等；软件层包括操作系统、中间件、数据库和安全软件等；应用层包括休闲娱乐类、工具媒体类、商务财经类等不同应用与服务。移动互联网将移动通信技术、终端技术与互联网技术相融合，而不是将固定互联网在移动网上的简单复制，是一种新能力、新思想和新模式的体现，并将不断催生出新的产业形态和业务形态。它主要由公众互联网上的内容、移动通信接入、便携式终端和不断创新的商业模式所构成，运营模式大致包括3种类型：以移动运营为主导的封闭式移动互联网、以终端厂商为主导的相对封闭式移动互联网和以网络运营为主导的开放式移动互联网。

移动互联网基于电信网络，是具有管理系统的层次管理网，具有完整的计费和管理系统；而且，移动互联网的移动终端具有不同于互联网终端的移动特性、个性化特征，用户体验也不尽相同[1]。

1.1 移动互联网体系架构

移动互联网是移动通信与互联网融合的产物，移动互联网继承了移动通信随时随地的特点及互联网分享、开放、互动的优势。4G时代的开启以及移动终端设备的凸显必将为移动互联网的发展注入巨大的能量，移动互联网的演进分为以下4个阶段。

① 移动增值网：是为移动通信系统提供增值业务的网络，能够提供移动的各种增值业务，属于业务网络。

② 独立WAP（Wireless Application Protocol，无线应用协议）网站：是独立

于移动网络体系的移动互联网站点，网站独立于运营商，直接面向消费者。

③ 移动互联网：是以互联网技术（如 HTTP/HTML 等）为基础，以移动网络为承载，以获取信息、进行娱乐和商务等服务的公共互联网。

④ 宽带无线互联网：是移动互联网的高级阶段，可以采用多种无线接入方式，如 3G、4G、WiMAX（World Interoperability for Microwave Access，全球微波互联接入）等。

开放系统互连（Open System Interconnect，OSI）[2]参考模型是 ISO 组织在 1985 年研究的网络互联模型，该模型定义了网络互连的 7 层框架：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。OSI 模型如图 1-1 所示，其中，第 1～3 层属于 OSI 参考模型的低 3 层，负责创建网络通信连接的链路；第 4～7 层为 OSI 参考模型的高 4 层，具体负责端到端的数据通信。

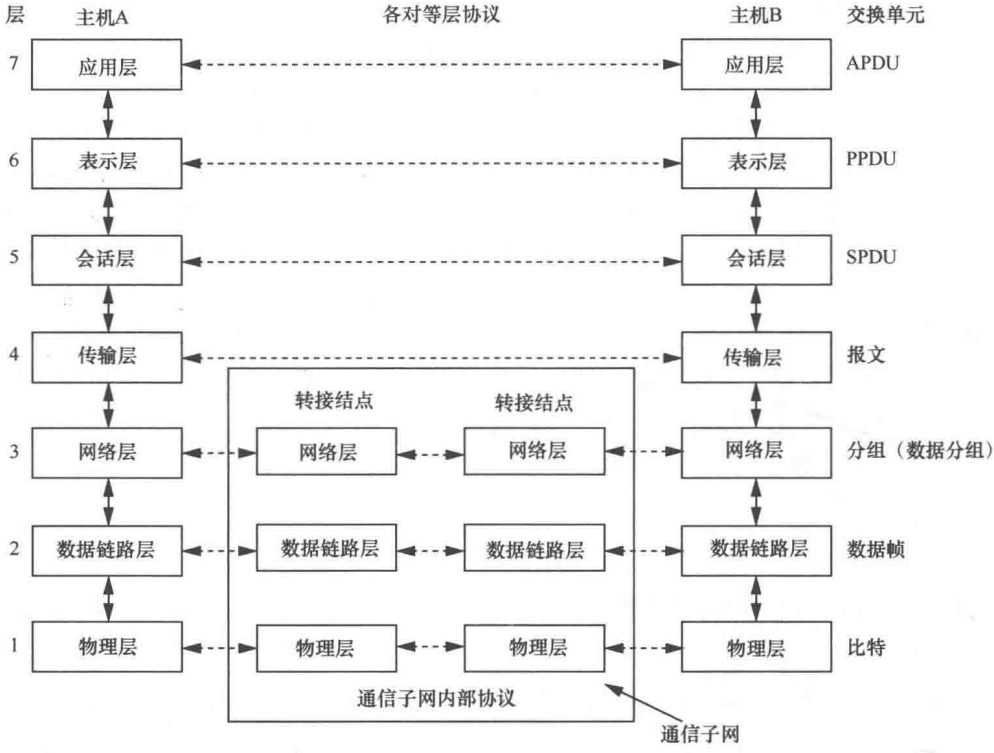

图 1-1 OSI 模型

移动互联网因为是互联网和移动通信的结合，分层与互联网稍有不同，移动互联网可分为 3 个层次，即移动终端和移动子网、接入网、核心网，如图 1-2 所示[3]。

移动互联网的总体架构如图 1-3 所示[3]，移动终端通过 3 种方式（Wi-Fi、通信网及卫星）接入到相应的通信网络中，并通过互联网来访问移动互联网业务。

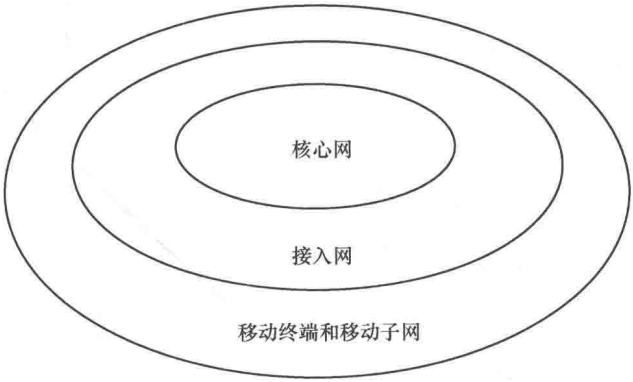

图 1-2 移动互联网体系架构

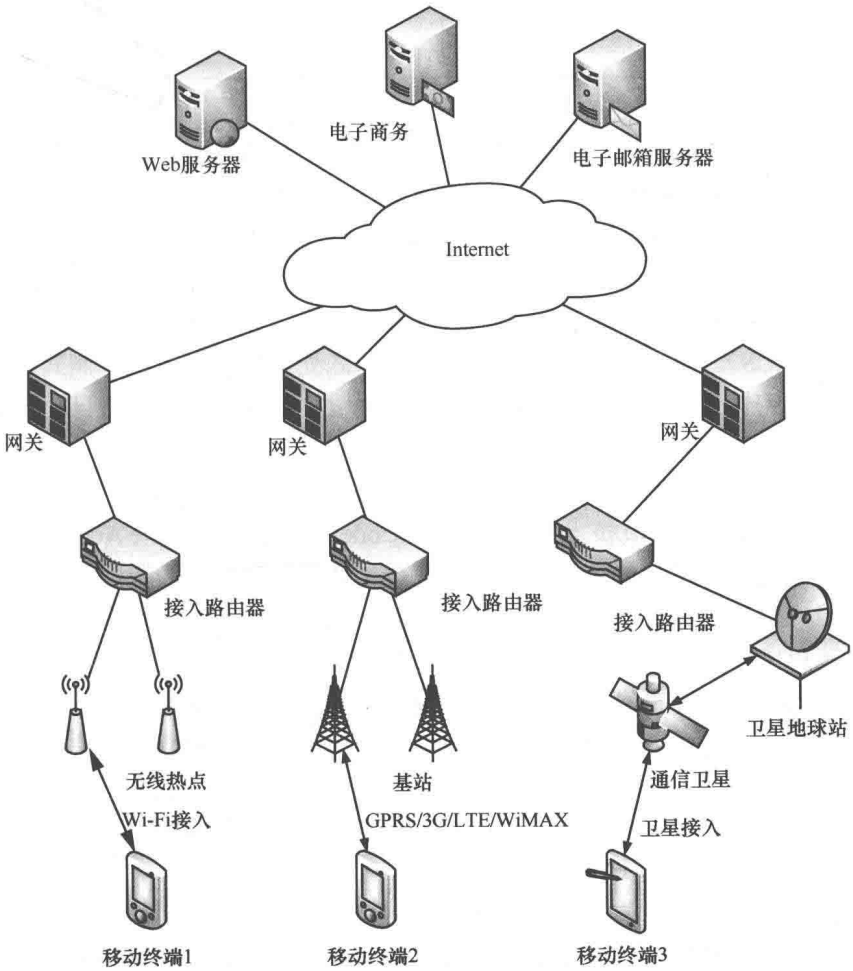

图 1-3 移动互联网总体架构

1.1.1 通信技术的演进

移动互联网从概念的提出到实现经历了很短的时间，目前正以一种前所未有的速度向全球推进。从第一代的 WAP 手机到第二代 GPRS（General Packet Radio Service，通用分组无线业务），再到现在的 3G、4G 技术，以及正在研发的 5G 技术，人类通信在互联网技术的推动下创造了一个又一个的应用新境界[4]。具体见表 1-1。

表 1-1 移动互联网代际分期

代际	信号	制式	主要功能	典型应用
1G	模拟	—	话音	通话
2G	数字	GSM TDMA	数据	短信、彩信
2.5G	数字	GPRS	窄带	WAP 网络
3G	数字	CDMA2000、WCDMA、TD-SCDMA、WiMAX	宽带	多媒体
4G	数字	TD-LTE	广带	高清

（1）第一代移动通信技术

第一代移动通信技术（1G）是指最初的模拟、仅限话音的蜂窝电话标准，制定于 20 世纪 80 年代，第一代移动通信主要采用的是模拟技术和频分多址（Frequency Division Multiple Access，FDMA）技术。由于受到传输带宽的限制，不能进行移动通信的长途漫游，只是一种区域性的移动通信系统。第一代移动通信有多种制式，我国主要采用的是全入网通信系统（Total Access Communications System，TACS）。第一代移动通信有很多不足之处，如容量有限、制式太多、互不兼容、保密性差、通话质量不高、不能提供数据业务和不能提供自动漫游等。

（2）第二代移动通信技术

第二代移动通信技术（2G）主要采用的是数字时分多址技术（Time Division Multiple Access，TDMA）技术和码分多址（Code Division Multiple Access，CDMA）技术，主要提供数字化的话音业务及低速数据业务。第二代为数字蜂窝移动通信系统，以 GSM（Global System for Mobile communication，全球移动通信系统）、CDMA、PDC 等系统为代表的。它克服了模拟移动通信系统的弱点，话音质量、保密性能得到很大的提高。第二代移动通信替代第一代移动通信系统完成了模拟技术向数字技术的转变，但由于采用的是不同的制式，导致移动通信的标准不统一，用户只能在同一制式覆盖的范围内进行漫游，因为无法进行全球漫游。而且，第二代数字移动通信系统带宽有限，从而限制了数据业务的应用，也无法实现高速率的业务。

（3）第三代移动通信技术

第三代移动通信技术（3G）是指支持高速数据传输的蜂窝移动通信技术[5]。3G 服务能够同时传送话音及数据信息，速率一般在几百 kbit/s 以上。目前 3G 存

在4种标准：CDMA2000、WCDMA（Wideband CDMA，宽频码分多址复用）、TD-SCDMA（Time Division Synchronous CDMA，时分同步码分多址接入）、WiMAX。其中TD-SCDMA属于时分双工（Time Division Duplexing，TDD）模式，是由中国提出的3G技术标准；而WCDMA和CDMA2000属于频分双工（Frequency Division Duplexing，FDD）模式，WCDMA技术标准由欧洲和日本提出，CDMA2000技术标准由美国提出。中国国内支持国际电联确定3个无线接口标准，分别是中国电信的CDMA2000、中国联通的WCDMA、中国移动的TD-SCDMA。与前两代移动通信技术相比，第三代移动通信能够实现高速数据传输和带宽多媒体服务。第三代移动通信网络能将高速移动接入和基于互联网协议的服务结合起来，提高无线频率利用率，提供包括卫星在内的全球覆盖，并实现有线和无线以及不同无线网络之间业务的无缝连接；满足多媒体业务的要求，从而为用户提供更经济、内容更丰富的无线通信服务。

（4）第四代移动通信技术

第四代移动通信技术（4G）的概念可称为宽带接入和分布网络，具有非对称的超过2 Mbit/s的数据传输能力。它包括宽带无线固定接入、宽带无线局域网、移动宽带系统和交互式广播网络。第四代移动通信标准比第三代标准具有更多的功能，第四代移动通信可以在不同的固定、无线平台和跨越不同的频带的网络中提供无线服务，可以在任何地方以高带宽接入互联网，能够提供全球定位、数据采集、远程控制等综合功能。此外，第四代移动通信系统是集成多功能的宽带移动通信系统，是宽带接入IP系统。第四代移动通信技术将数据速率从2 Mbit/s提高到100 Mbit/s，并且满足高速数据和高分辨率多媒体服务的需要。

1.1.2 移动互联网的关键技术

1. 蜂窝移动通信网络发展

基站[6]是指在一定的无线电覆盖区中，通过移动通信交换中心，与移动电话终端之间进行信息传递的无线电收发信电台。基站的建设是我国移动通信运营商投资的重要部分，随着移动通信网络业务向数据化、分组化方向发展，基站的发展趋势也必然是宽带化、大覆盖面建设及IP化。

在不同的网络系统中，基站结构也不尽相同，但相互没有本质差异。以GSM网络[6]为例，包括基站收发台（Base Transceiver Station，BTS）和基站控制器（Base Station Controller，BSC）。一个基站控制器可以控制十几以至数十个基站收发信机。而在WCDMA等系统中，类似的概念有NodeB和RNC（Radio Network Controller，无线网络控制器）。

一般情况下在某个区域内，多个基站相互组成一个蜂窝状的网络，通过控制收发台与收发台之间的信号相互传送和接收来达到移动通信信号的传送，这个范

围内的地区也就是我们常说的网络覆盖区。如果没有了收发台，那就不可能完成手机信号的发送和接收。基站收发台不能覆盖的地区也就是手机信号的盲区。所以基站收发台发射和接收信号的范围直接关系到网络信号的好坏以及手机是否能在这个区域内正常使用。

GSM 系统越区时采用切换方式，即当用户到达小区边界时，手机会先与原来的基站切断联系，然后再与新的服务小区的基站建立联系。当新的服务小区繁忙时，不能提供通话信道，这时就会发生掉线现象。

3G 网络相对于 2G 网络有一个不同，就是 3G 网络使用了频率复用技术，虽然增加了频谱利用率，但也给它本身的网络带来了同频复用的自干扰[7]。

在整个蜂窝移动通信系统中，基站子系统是移动台与移动中心连接的桥梁，其地位极其重要。整个覆盖区中基站的数量、基站在蜂窝小区中的位置、基站子系统中相关组件的工作性能等因素决定了整个蜂窝系统的通信质量。基站的选型与建设，已成为组建现代移动通信网络的重要一环。

2. 移动网络接入技术

移动互联网的网络接入技术主要包括：移动通信网络、无线局域网（Wireless Local Area Network，WLAN）、无线 Mesh 网络（Wireless Mesh Network，WMN）、其他接入网络技术、异构无线网络融合技术等[4]。

一是移动通信网络。移动通信网络经历了 1G、2G、3G 时代，目前正在大力部署 4G 网络，并在加快研发 5G 技术。4G 能够以 100 Mbit/s 的速率下载数据，20 Mbit/s 的速率上传数据。5G 的目标是，到 2020 年，相对于当前而言，实现数据流量增长 1 000 倍，用户数据速率提升 100 倍，速率提升至 10 Gbit/s 以上，入网设备数量增加 100 倍，电池续航时间增加 10 倍，端到端时延缩短 5 倍。

二是无线局域网。目前正在发展 AC-AP 架构的 WLAN 解决技术，即无线控制器负责管理无线网络的接入和无线接入点的配置与监测、漫游管理及安全控制等，无线接入点只负责 802.11 报文的加解密。另外，802.11ad 标准提出了利用 60 GHz 频段进行无线通信的技术，传输速率达到 6.76 Gbit/s，并降低了天线的尺寸，提高了抗干扰能力。电气与电子工程师协会（IEEE）制定的无线局域网标准见表 1-2。

表 1-2　　IEEE 制定的无线局域网标准

协议	发布时间	频率（GHz）	宽带（MHz）	最大传输速率（Mbit/s）
802.11	1997	2.4	20	2
802.11a	1999	5/3.7	20	54
802.11b	1999	2.4	20	11
802.11g	2003	2.4	20	54
802.11n	2009	2.4/5	20	82/150

三是无线 Mesh 网络。WMN 是一种自组织、自配置的多跳无线网络技术，Mesh 路由器通过无线方式构成无线骨干网，少数作为网关的 Mesh 路由器以有线方式连接到互联网。

四是其他接入网络。小范围的无线个域网有 NFC、蓝牙、UWB、ZigBee、IrDA 等技术。

五是异构无线网络融合技术。针对多种无线接入技术，正在发展异构无线网络融合技术。异构无线网络架构分为紧耦合技术和松耦合技术两类。紧耦合技术的网络架构是指无线接入系统之间存在主从关系，松耦合技术网络架构是指无线接入系统之间不存在主从关系。

（1）Wi-Fi 技术

Wi-Fi 技术应用灵活，能灵活胜任只有几个用户的小型网络，也能胜任使用者达到数千人的大型网络。组网成本也相对低廉，但是数据传输速率有限和无线电波之间的相互影响是制约其发展的两个原因。

（2）3G 之 WCDMA

WCDMA 是 CDMA 演变而来，由欧洲提出，技术成熟。这个标准在全球应用是最广泛的。

（3）3G 之 CDMA2000

CDMA2000 是窄带 CDMA 发展而来，由美国提出。这个标准在亚太地区应用比较广泛，主要集中在中国、日本和韩国。

（4）3G 之 TD-SCDMA

这个标准由我国提出，主要优点是频谱利用率高。从理论上来说，这是中国第一次在全球通信领域内的有力尝试，也是自主知识产权的代表成就之一。

3. *移动 IP 技术*

IP 协议（Internet Protocol）[8]要求所有参加互联网的网络节点要有一个统一规定格式的地址，简称 IP 地址。在互联网上，每个网络和每一台移动终端都被分配有一个 IP 地址，这个 IP 地址在整个互联网网络中是唯一的。IP 地址是供全球识别的通信地址。在互联网上通信必须采用这种 32 位的通用地址格式，才能保证互联网成为向全球的开放互联数据通信统。它是全球认可的计算机网络标识方法。IP 地址可采用二进制格式或十进制格式。

互联网工程任务组（Internet Engineering Task Force，IETF）[2]将 IP 地址分为成 3 个普通类（加上 2 个特殊类）。IP 地址由 4 个 8 位组的二进制组成，也可以使用 4 个带点的十进制数字表示。不同类之间的区别在于当寻址网络与主机对立时，分配给寻址网络的 8 位组的方式不同。这种分配方式称作第一个 8 位组规则。世界上的任何一个路由器都能够阅读 IP 地址的第一个 8 位组，并且知道哪些位能翻译成网络地址的一部分，哪些能翻译成主机地址的一部分。如果路由器不能进

行这样的区分，那么互联网将不能正常工作。大部分网络使用 B 类或 C 类地址，每一个类的第一个 8 位组的范围如图 1-4 所示。

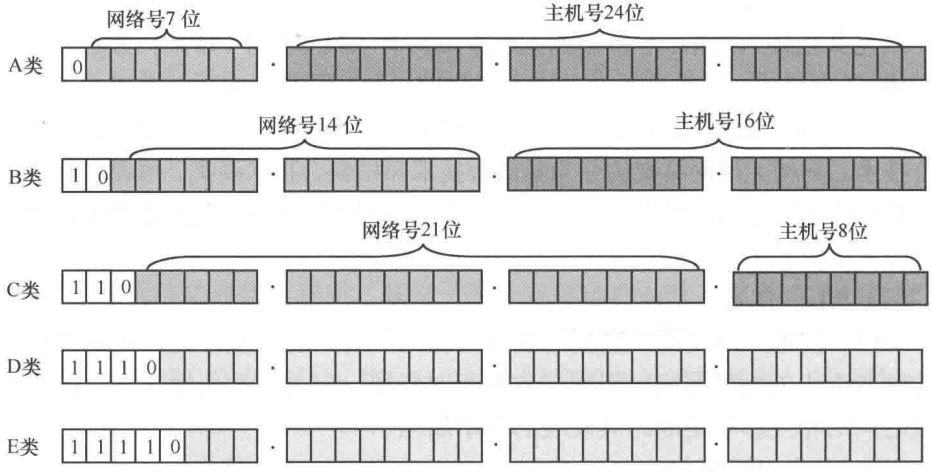

图 1-4　IP 地址分类

移动 IP[9]是移动通信和 IP 的深层融合，也是对现有移动通信方式的深刻变革，它将真正实现话音和数据的业务融合，它的目标是将无线话音和无线数据综合到一个技术平台上传输，这一平台就是 IP 协议。

我们在连接互联网时，需要使用固定的 IP 地址和 TCP 端口号进行相互通信，在通信期间它们的 IP 地址和 TCP 端口号必须保持不变，否则 IP 主机之间的通信将无法继续。而移动 IP 的基本问题是 IP 主机在通信期间可能需要移动，它的 IP 地址也许经常会发生变化，最终导致通信中断[9]。

如何解决因节点移动，即 IP 地址的变化而导致通信中断的问题[9]？蜂窝移动电话提供了一个非常好的解决问题先例。因此，解决移动 IP 问题的基本思路与处理蜂窝移动电话呼叫相似，它将使用漫游、位置登记、隧道技术、鉴权等技术，从而使移动节点使用固定不变的 IP 地址，一次登录即可实现在任意位置上保持与 IP 主机的单一链路层连接，使通信持续进行。

（1）归属代理（Home Agent，HA）

一个在移动节点（Mobile Node，MN）归属网上的路由器，它至少有一个接口在归属网上，当移动节点离开归属网时，它通过 IP 通道把数据分组传给移动节点，并且负责维护移动节点的当前位置信息。

（2）外区代理（Foreign Agent，FA）

移动节点当前所在网络上的路由器，它向已登记的移动节点提供选路服务。当使用外区代理转交地址时，外区代理负责解除原始数据分组的隧道封装，取出原始数据分组，并将其转发到该移动节点。对于那些由移动节点发出的数据分组