第3章 移动通信安全

随着半导体技术、微电子技术和计算机技术的发展，移动通信在最近的几十年里得到了迅猛发展和应用。1978年，美国芝加哥开通第一台模拟移动电话，标志着第一代移动通信的诞生；1987年，我国首个全网通信系统技术（total access communications system，TACS）制式模拟移动电话系统建成并投入使用；1993年，我国首个全球移动通信系统（global system for mobile communications，GSM）建成开通，标志着我国进入了第二代移动通信时代；2001年前后，数个国家相继开通了3G商用网络，标志着第三代移动通信时代的到来；2014年前后，我国各地相继开通4G网络服务，标志着第四代移动通信时代的到来。如今，随着世界各地5G网络的开通，我们的生活正在步入第五代移动通信时代。

3.1 移动通信系统概述

从移动通信的发展历史来看，移动通信的发展不是孤立的，而是建立在与其相关的技术发展和人们需求的基础上的：第一代移动通信是在超大规模模拟集成电路的发展基础和人们对移动通话的需求上发展起来的，第二代移动通信建立在超大规模数字集成电路技术和微计算机技术以及人们对通话质量的需求基础上，第三代移动通信建立在互联网技术和数据信息处理技术以及人们对移动数据业务的需求基础上，第四代移动通信建立在下一代互联网技术和多媒体技术以及人们对多媒体需求的基础上。

随着移动通信的普及，移动通信中的安全问题也受到越来越多的关注，人们对移动通信中的信息安全也提出了更高的要求。

安全威胁产生的原因来自网络协议和系统的弱点。攻击者可以利用网络协议和系统的弱点非授权访问和处理敏感数据，或是干扰、滥用网络服务，对用户和网络资源造成损失，主要威胁方式有窃听、伪装、流量分析、破坏数据的完整性、拒绝服务、否认、非授权访问服务和资源耗尽等。

第二代数字蜂窝移动通信系统（2G）只能提供语音和低速数据业务的服务。但是在信息时代，图像、语音和数据相结合的多媒体业务和高速率数据业务将会大大增加。

随着第三代移动通信（3G）网络技术的发展、移动终端功能的增强和移动业务应用内容的丰富，各种无线应用极大地丰富了人们的日常工作和生活，也为国家信息化战略提供了强

大的技术支撑,网络安全问题就显得更加重要了,第三代数字蜂窝移动通信业务包括第二代蜂窝移动通信可提供的所有业务类型和移动多媒体业务。

虽然 3G 系统解决了 1G、2G 系统的弊端,但其实际速度远未达到预期值。第四代移动通信技术(4G)可称为宽带接入和分布网络,具有非对称的超过 2Mb/s 的数据传输能力,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。第四代移动通信技术可以为不同的固定、无线平台和跨越不同频带的网络提供无线服务,可以在任何地方用宽带接入互联网(包括卫星通信和平流层通信),能够提供定位定时、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。

第五代移动通信技术(5G)是具有高速率、低时延和大连接等特点的新一代宽带移动通信技术,是实现人机物互联的网络基础设施。5G 为移动互联网用户提供更加极致的应用体验,海量机器类通信主要面向智慧城市、智能家居、环境监测等以传感和数据采集为目标的应用需求。

3.2 GSM 系统安全

GSM 原意为移动通信特别小组(group special mobile),是欧洲邮电管理委员会(Conference of European Posts and Telecommunications,CEPT)为开发第二代数字蜂窝移动系统而在 1982 年成立的机构,主要职责是制定适用于泛欧各国的一种数字移动通信系统的技术规范。1987 年,欧洲 15 个国家的电信业务经营者在哥本哈根签署了一项关于在 1991 年实现泛欧 900MHz 数字蜂窝移动通信标准的谅解备忘录(memorandum of understanding,MOU)。随着设备的开发和数字蜂窝移动通信网的建立,GSM 逐步成为欧洲数字蜂窝移动通信系统的代名词。后来,欧洲的专家们将 GSM 重新命名为 global system for mobile communications,即全球移动通信系统。

目前,宣布采用 GSM 系统并参加 MOU 的国家早就不限于欧洲了。在 1995 年年初,全世界就已有 69 个国家约 118 个经营者签字参加了 MOU。

3.2.1 GSM 系统简介

1. 系统组成

GSM 系统由交换分系统(mobile switching subsystem,MSS)、基站分系统(mobile station subsystem,BSS)、移动台(mobile station,MS)和操作与维护分系统(operation and maintenance subsystem,OMS)组成。它包括了从固定用户到移动用户(或相反)所经过的全部设备,如图 3.1 所示。

1) 交换分系统

交换分系统包括以下几个组成部分:移动交换中心(mobile service switching center,MSC)、归属位置寄存器(home location register,HLR)、拜访位置寄存器(visitor location register,VLR)、认证(鉴权)中心(authentication center,AuC)、设备标志寄存器(equipment identification register,EIR)。

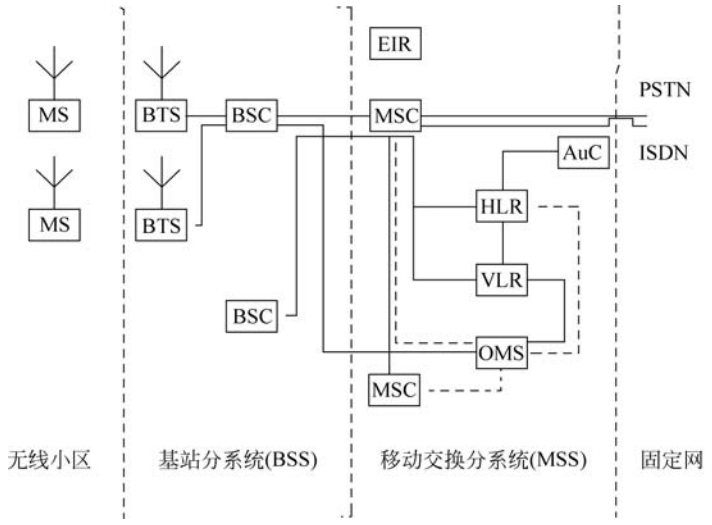

图 3.1　数字移动蜂窝网组成

(1) 移动交换中心。

MSC 主要处理与协调 GSM 系统内部用户的通信接续。MSC 对位于其服务区内的移动台进行交换与控制,同时提供移动网与固定公众电信网的接口。作为交换设备,MSC 具有完成呼叫接续与控制的功能,同时还具有无线资源管理和移动性管理等功能,例如移动台位置的登记与更新、MS 的越区转接控制等。移动用户没有固定位置,要为网内用户建立通信时,路由都先接到一个关口交换局(gateway MSC,GMSC),即由固定网接到 GMSC。GMSC 的作用是查询用户的位置信息,并把路由转到移动用户当时所拜访的移动交换局(visited MSC,VMSC)。GMSC 首先根据移动用户的电话号码找到该用户所属的归属位置寄存器 HLR,然后从 HLR 中查询到该用户目前的 VMSC。GMSC 一般都与某个 MSC 合在一起,只要使 MSC 具有关口功能就可实现。MSC 通常是一个大的程控数字交换机,能控制若干个基站控制器(basic station controller,BSC)。GMSC 与固定网相接,固定网有公众电话网(public switched telephone network,PSTN)、综合业务数字网(integrated services digital network,ISDN)、分组交换公众数据网(packet switched public data network,PSPDN)和电路交换公众数据网(circuit switched public network,CSPDN)。MSC 与固定网互联需要通过一定的适配才能符合对方网络对传输的要求,称为适配功能(inter-working function,IWF)。

(2) 归属位置寄存器。

HLR 是管理移动用户的数据库,作为物理设备,它是一台独立的计算机。每个移动用户必须在某个 HLR 中登记注册。在数字蜂窝网中,应包括一个或多个 HLR。HLR 所存储的信息分为两类:一类是有关用户参数的信息,例如用户类别、所提供的服务、用户的各种号码、识别码以及用户的保密参数等;另一类是用户当前的位置信息,例如移动台漫游号码、VLR 地址等,用于建立至移动台的呼叫路由。HLR 不受 MSC 的直接控制。

(3) 拜访位置寄存器。

VLR 是存储用户位置信息的动态链接库。当漫游用户进入某个 MSC 区域时,必须在

MSC 相关的 VLR 中进行登记；VLR 分配给移动用户一个漫游号(mobile station roaming number,MSRN),并在 VLR 中建立用户的有关信息,其中包括移动用户识别码(mobile subscriber identity,MSI)、移动台漫游号、移动用户所在位置区的标志及向用户提供的服务等参数,而这些信息是从相关的 HLR 中传过来的。MSC 在处理入网和出网呼叫时需要查访 VLR 中的有关信息。一个 VLR 可以负责一个或多个 MSC 区域。由于 MSC 与 VLR 之间交换信息很多,所以两者的设备通常合在一起。

(4) 认证(鉴权)中心。

AuC 直接与 HLR 相连,是认证移动用户身份及产生相应认证参数的功能实体。认证参数包括随机号码 RAND、信号响应 SREC 和密钥 KC。认证中心对移动用户的身份进行认证,将用户的信息与认证中心的随机号码进行核对,合法用户才能接入网络,并得到网络的服务。

(5) 设备标志寄存器。

EIR 是存储有关移动台设备参数的数据库,用来实现对移动设备的识别、监视、闭锁等功能。EIR 只允许合法的设备使用,它与 MSC 相连接。

2) 基站分系统

BSS 包含 GSM 数字移动通信系统中无线通信部分的所有地面基础设施,通过无线接口直接与移动台实现通信连接。BSS 具有控制功能与无线传输功能,可完成无线信道的发送、接收和管理。它由基站控制器和基站收发信台两部分组成。

(1) 基站控制器。

基站控制器(base station controller,BSC)的一侧与移动交换分系统相连接,另一侧与基站收发信台(base transceiver station,BTS)相连接。一个基站分系统只有一个 BSC,而有多套 BTS。BSC 通过对 BTS 和 MS 的指令来管理无线接口,主要负责无线信道的分配、释放以及越区信道的切换管理。

(2) 基站收发信台。

BTS 负责无线传输。每个 BTS 有多部收发信机,占用多个频率点。每部收发信机占用一个频率点,每个频率点又分成 8 个时隙,这些时隙就构成了信道。BTS 是覆盖一个小区的无线电收发信设备。

BTS 还有一个重要的部件称为码型转换器(transcoder)和速率适配器(rate adaptor),简称 TRAU,其作用是将 GSM 系统中的语音编辑信号与标准 64kb/s 的 PCM 相配合。例如移动台发话时,它首先进行语音编码,变为 13kb/s 的数字流；信号经 BTS 收信机接收后,其输出仍为 13kb/s 的信号；需经 TRAU 后变为 64kb/s 的 PCM 信号,才能在有线信道上传输。同时,要传送较低速率数据信号时,也需经过 TRAU 变成标准信号。

3) 移动台

移动台靠无线接入进行通信,线路不固定,因此它必须具备用户的识别号码。GSM 系统采用用户识别模块(subscriber identity module,SIM),将模块做成信用卡的形式。SIM 卡中存有用户身份认证所需的信息,并能执行一些与安全保密有关的信息。移动设备只有插入 SIM 卡后才能进网使用。

4) 操作维护分系统

操作与维护管理的目的是使网络运营者能监视和控制整个系统,把需要监视的内容从

被监视的设备传到网络管理中心，显示给管理人员；同时，管理人员在网络管理中心还应该能修改设备的配置和功能。

2. 主要特点

1) 移动台具有漫游功能

GSM 给移动台定义了三种识别码：一个是移动用户号码簿号码(directory number，DN)，是在公用电话号码簿上可以查到的统一电话号码；第二个是移动台漫游号码(mobile subscriber roaming number，MSRN)，是在呼叫漫游用户时使用的号码，由 VLR 临时指定，并根据此号码将呼叫接至漫游移动台；第三个是国际移动台识别码(international mobile subscriber identity，IMSI)，是在无线信道上使用的号码，用于用户寻呼和识别移动台。根据上述三个识别码，可以准确无误地识别某个移动台。

漫游用户必须进行位置登记。当 A 区的移动台进入 B 区后，它会自动搜索该区基站的广播信道，从中获得位置信息；当其发现接收到的区域识别码与自己的号码不同时，漫游移动台会向当地基站发出位置更新请求；B 区的被访局收到此信号后，会通知本局的 VLR；VLR 即为漫游用户指定一个临时号码 MSRN，并将此号码通过 CCS7 号信令通知移动台所在业务区备案。这样，当固定用户呼叫漫游移动用户时，拨移动台的 DN 码；DN 码首先经公用交换网络接至最近的本地 GSM 移动业务交换中心(GSM center，GSMC)；GSMC 利用 DN 码访问母局位置登记器即归属位置寄存器，从中获取漫游台的 MSRN 码；GSMC 根据此码将呼叫接至被访问的移动业务交换中心(VMS center，VMSC)；VMSC 接到 MSRN 号码后，证实漫游台是否仍在本区工作；经确认后，VMSC 将 MSRN 码转换成 IMSI，通过基站在无线信道上向漫游台发出呼叫，从而建立通话。

2) 可提供多种业务

除语音通话外，GSM 系统还能提供多种数据业务、三类传真、可视图文等，并能支持综合业务数字网(integrated services digital network，ISDN)终端。

3) 具有较好的保密功能

保密措施通过“认证中心”实现，认证方式是一个“询问—响应”过程。在通信过程开始时，首先由网络向移动台发出一个信号并同时启动自己的“用户认证”单元；移动台收到这个信号后，连同内部的“电子密钥”一起来启动“用户认证”单元，并将结果返回网络；网络将这两个“用户认证”单元结果相比较，只有相同才为合法。

4) 越区切换功能

在微蜂窝移动通信网络中，高频率的越区切换是不可避免的。在 GSM 中，移动台应主动参与越区切换。移动台在通话期间，不断向所在工作区基站报告本区及相邻区无线环境的详细数据。当需要越区切换时，移动台主动向本区基站发出越区切换请求。固定方(MSC 或 BSC)根据来自移动台的数据，查找是否有替补信道。如果不存在，则选择第二替补信道，直至选中一个空闲信道，使移动台切换到该信道上继续通信。

3. 业务功能

GSM 系统主要提供以下四大类业务。

1) 电话业务

紧急呼叫是由电话业务引申出来的一种特殊业务。移动台用户能通过一种简便而统一的手续接到就近的紧急业务中心(例如公安局或消防中心)。使用紧急业务不收费,也不需要认证使用者身份的合法性。

语音信箱能将话音存储起来,事后由被叫移动用户提取。

2) 数字业务

GSM 技术规范中列举了 35 种数字业务,主要是以下几类。

(1) 与公众电话通信网(PSTN)用户相连的数字业务。

PSTN 中最常用的数字业务有三类传真和可视图文(VIDEOTEX)。GSM 要与 PSTN 相连接,必须使用 MODEM。GSM 能处理 9600b/s 速率以下的全双工方式数据。

(2) 与综合业务数字网(ISDN)用户相连的数字业务。

GSM 系统中的数据速率最高为 9600b/s,而 ISDN 使用的速率是 64kb/s,因此必须采用速率转换技术。采用标准化的 ISDN 数据格式,在 64kb/s 链路上传送低速数据,这种方式可实现高于 2400b/s 的异步数据传输。

(3) GSM 用户之间的数字业务。

在大多数情况下,GSM 网内用户之间的通信会有外面的通信网参与,因为 GSM 网内交换机之间的传输都是通过公众固定网的缘故。目前,GSM 网所能提供的业务必须是 PSTN 传输网能支持的业务,GSM 用户之间的通信与 GSM 用户和 PSTN 用户间的连接是相同的。

(4) 与分组交换数据通信网(PSPDN)用户相连的数字业务。

PSPDN 是一种采用分组传输技术的通用性数据网,主要用于计算机之间的通信,同时也支持远端数据库的访问和信息处理系统。PSTN 采用的是电路传输技术,GSM 接入 PSPDN 的方式有数种。

3) 短消息业务

通过 GSM 网并设有短消息业务中心(short message service,SMS),便可实现短消息业务。短消息业务有以下两种:

(1) 点对点短消息业务。

点对点短消息业务有两种:一种是移动台接收点对点短消息(SMS-MT/PP),另一种是移动台发送点对点短消息(SMS-MO/PP)。GSM 数字移动通信网用户可以发出或接收有限长度的数字或文字消息,这就是短消息业务功能。

(2) 短消息小区广播业务。

短消息小区广播业务是向特定地区的移动台周期性地广播数据信息,移动台能连续地监测广播信息并显示给用户。

4) 补充业务

补充业务只限于电话业务,它允许用户能按自己的需要改变网络对其呼入呼出的处理,或者通过网络向用户提供某种信息,使用户能智能化地利用一些常规业务。

3.2.2 GSM 安全分析

在第一代模拟移动通信系统中,由于技术因素的限制,网络中没有采取有效的安全机

制，对运营商和用户都造成了巨大的损失。有数据显示，仅 1993 年一年内由于网络安全原因导致的经济损失就超过 3 亿美元。由此，移动通信系统的安全性问题开始引起人们的关注。

为了保障 GSM 系统的安全保密性能，在设计中采用了很多安全、保密措施，主要有临时识别符、加密、鉴权、设备识别、PIN 码保护等。

1. 临时识别符

为了保护用户的隐私，防止用户位置被跟踪，GSM 中使用临时识别符（temporary mobile subscriber identity，TMSI）对用户身份进行保密。只有在网络根据 TMSI 无法识别出它所在的 HLR/AuC，或是无法到达用户所在的 HLR/AuC 时，才会使用用户的 IMSI 来识别用户，从它所在的 HLR/AuC 获取鉴权参数来对用户进行认证。在 GSM 中，TMSI 总是与一定的位置区识别符（location area identity，LAI）相关联的。当用户所在的位置区（location area，LA）发生改变时，通过位置区更新过程实现 TMSI 的重新分配。重新分配给用户的 TMSI 是在用户的认证完成并启动加密模式后，由 VLR 加密后传送用户的，从而实现了 TMSI 的保密。同时在 VLR 中保存新分配给用户的 TMSI，将旧的 TMSI 从 VLR 中删除。

2. 鉴权（用户入网认证）

GSM 系统使用鉴权三参数组（随机数 RAND、符号响应 XRES、加密密钥 K_c）实现用户鉴权。

在用户入网时，用户鉴权键 K_i 同 IMSI 一起分配给用户。在网络端，K_i 存储在用户鉴权中心 AuC（authentication center）；在用户端，K_i 存储在 SIM 卡中。AuC 为每个用户准备了“鉴权三元组”，存储在 HLR 中。当 MSC/VLR 需要鉴权三元组的时候，就向 HLR 提出请求并发送消息“MAP—SEND—AUTHENTICATION—INFO”给 HLR（该消息包括用户的 IMSI），HLR 的回答一般包括五个鉴权三元组。任何一个鉴权三元组使用之后将被破坏，不再重复使用。

当移动台第一次到达一个新的移动业务交换中心（mobile-service switching center，MSC）时，MSC 会向移动台发出一个随机号码 RAND 并发起一个鉴权认证过程。整个过程如图 3.2 所示。

3. 加密

网络对用户的数据进行加密，以防止窃听。加密是受鉴权过程中产生的加密密钥 K_c 控制的，加密密钥的产生过程是通过相同的输入参数 RAND 和 K_i，将两个算法合为一个来计算符号响应和加密密钥。加密密钥 K_c 不在无线接口上传送，而是在 SIM 卡和 AuC 中，由这两部分来完成相应的算法，如图 3.3 所示。

加密的过程是：将 A8 算法生成的加密密钥 K_c 和承载用户数据流的 TDMA 数据帧的帧号作为 A3 算法的输入参数，生成伪随机数据流；再将伪随机数据流和未加密的数据流作模二加运算，得到加密数据流。在网络侧实现加密是在基站收发器（BTS）中完成的，BTS 中存有 A3 加密算法，加密密钥 K_c 是在鉴权过程中由 MSC/VLR 传送给 BTS 的。具体流程如图 3.4 所示。

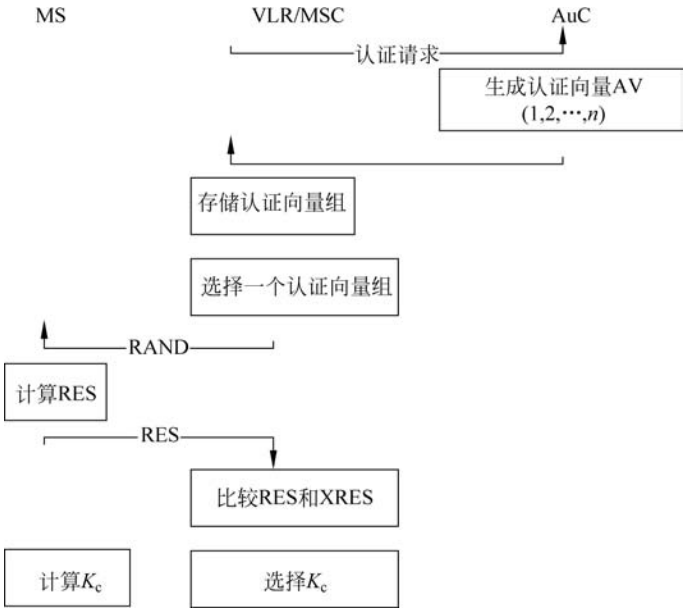

图 3.2 GSM 系统鉴权和认证过程

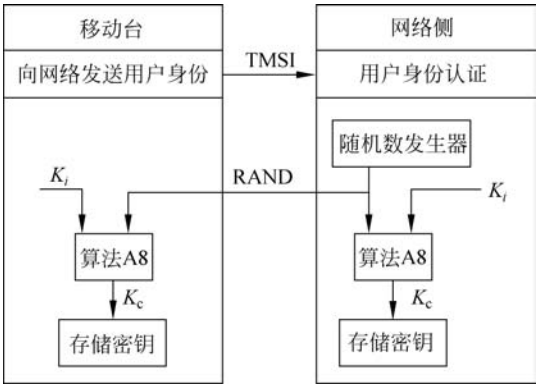

图 3.3 GSM 系统中加密密钥的产生

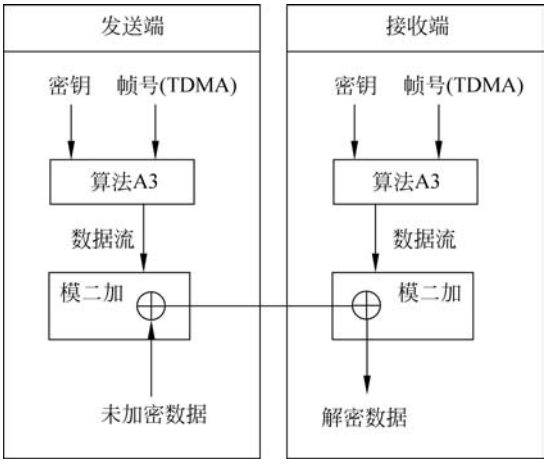

图 3.4 加解密过程

4. 设备识别

设备识别是为防止盗用或非法设备入网使用的。

(1) MSC/VLR 向 MS 请求 IMEI(international mobile equipment identity,国际移动设备识别码),并将其发送给 EIR(equipment identity register,设备识别寄存器)。

(2) 收到 IMEI 后,EIR 使用它所定义的三个清单。

① 白名单:包括已经分配给参加运营 GSM 各国的所有设备识别序列号。

② 黑名单:包括所有被禁止使用的设备的识别号。

③ 灰名单:由运营商决定,包括有故障的及未经型号入网认证的移动设备。

(3) 将设备鉴定结果发送给 MSC/VLR,以决定是否允许入网。

3.3 GPRS 安全

通用分组无线业务(general packet radio service,GPRS)移动通信系统是在 GSM 网络基础上构建的满足分组业务服务需求的无线通信网络。由于 GPRS 网络用户无线通信和终端 IP 移动性的制约,其安全性的构建必须综合权衡 GSM 和 IP 数据网络结合的特点,以保证移动用户终端之间安全有效的信息传输。

GPRS 移动通信系统的安全策略涉及两方面的内容:一是用户信息传送的准确性;二是用户信息的保密性。这些信息包括为移动用户传送的话音、数据业务以及用户位置、识别方式等个人资料信息。通常情况下,如何正确无误地传送用户信息,由移动通信系统的信道控制技术确定,我们这里主要介绍 GPRS 信息保密方面的安全性问题。

GPRS 是一种支持 GSM 网络分组业务扩展的数据传输体制标准,它充分利用 GSM 基础设备,以 115～170kb/s 的传输速率支持端到端的分组数据交换,可以提供基于移动无线应用协议(wireless application protocol,WAP)等高层应用的互联,灵活部署电信增值服务。GPRS 网络分为无线侧和网络侧,无线侧提供空中接口的终端接入能力,GPRS 安全控制主要是网络侧的功能。网络侧的安全控制是在 GSM 的基础上通过增加服务 GPRS 支持节点(serving GPRS support node,SGSN)和网关 GPRS 支持节点(gateway GPRS support node,GGSN)核心网络实体以及重新界定实体间接口实现的。SGSN 为移动台提供移动性管理、路由选择、加密及身份认证等服务,GGSN 则用于接入外部数据网络。边界网关(border gateway,BG)主要用于陆地移动网内不同本地互联网(local internet network,LIN)构成的 GPRS 核心网的互联,并可以根据运营商之间的漫游协议进行功能扩展与定制。

GPRS 的本质是扩展的 IP 分组数据通信网络,所面临的安全隐患多于基于 NO.7 信令进行电路交换的 GSM 系统。由于 TCP/IP 协议的广泛使用和 IP 安全的脆弱性,这将不可避免地增加 GPRS 安全威胁的可能性。

GPRS 的安全性表现为网络实体的安全威胁,涉及从外部 IP 网络侵入 GPRS 系统恶意攻击 GPRS 网络实体或浏览信息,以及用户、运营商内部、ISP 对系统非经授权访问等方面内容。GPRS 安全性主要从以下 6 方面加以阐述。

1. GPRS 安全策略

GPRS 的安全策略基于以下三方面的规则,在实现上可以综合采用不同的安全措施。

(1) 防止未经授权使用 GPRS 业务,即鉴权和服务请求确认。

(2) 保持用户身份的机密性,使用临时身份和加密。

(3) 保持用户数据的机密性,进行通信数据加密发送。

2. 用户鉴权与身份认证

GPRS 的用户鉴权与身份认证适用于网络内部的 MS 通信,与 GSM 原有的过程类似,区别在于鉴权与身份认证流程由 SGSN 发起,如图 3.5 所示。鉴权三元组存储在 SGSN,在开始加密时对所采取的加密算法进行选择。在鉴权与通信过程中,通过使用临时逻辑链路标志(temporary logical link identifier,TLLI)和临时移动台身份标识(temporary mobile station identifier,TMSI)实现用户真实身份的信息隐藏。其中,SGSN 收发用户的分组数据包,其功能包括分组路由和传输、移动管理、逻辑链路管理、认证和计费。GGSN(gateway GPRS support node)是 GPRS 网络中的关键部分,用于 GPRS 网络和外部分组交换网络(Internet,X.25,WiMAX)之间的交互。Firewall 为防火墙,实现对进、出内部网络的服务和访问的审计和控制。

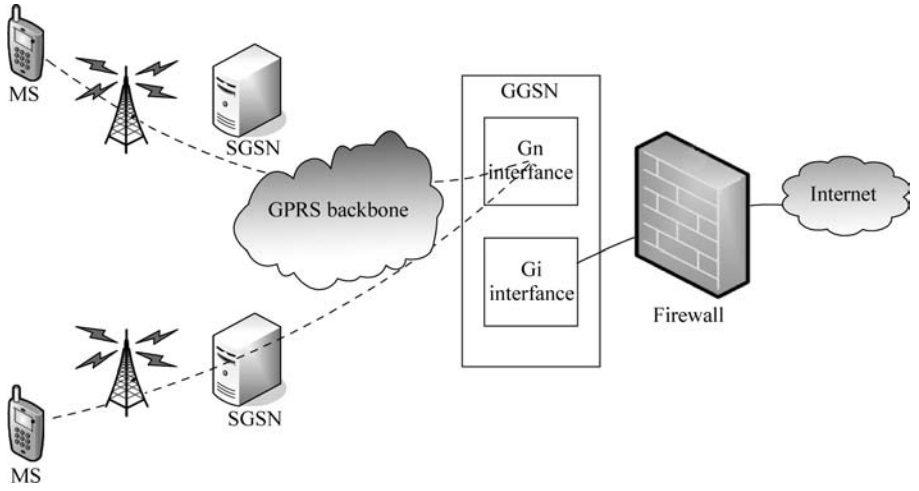

图 3.5 GPRS 网络 MS 之间的通信流程

3. 用户数据与信令机密性

GPRS 网络数据传输的数据和信令受保密加密算法(GPRS encryption algorithm,GEA)保护,加密范围在 MS 与 SGSN 之间,由逻辑链路层(logical link control,LLC)完成。为正确传送数据,GPRS 服务节点和移动终端对数据的加密和解密过程必须保持同步。

4. 安全协议

GPRS 网络之间通过分组交换数据网(packet switched data network,PSDN)或者数字

数据网(digital data network,DDN)的通信链路连接,其中专用网络链路的使用可以满足用户对服务质量和安全性能的要求。由于 GPRS 网络间的数据与信令通过 BG 进行传递,可以使用 Internet 协议安全性(Internet protocol security,IPSec)协议构建 VPN,以实现身份认证和以隧道保护为基础的数据安全性。

5. 信息容灾处理

信息容灾处理主要采用冗余可靠性工程的方法,对 GPRS 网络系统的重要节点进行设备或数据级别的周期备份,以利于系统的故障切换与数据恢复。

6. 安全防火墙技术

结合 GPRS 网络实体安全需求,GGSN 综合采用防火墙技术是保障网络安全的重要途径。从系统管理的角度而言,应加强 GPRS 设备和移动用户终端 MS 两方面的安全性,以确保 GPRS 网络本身以及存储在网络或 MS 内的信息不受外来非法攻击。图 3.5 展示了采用防火墙技术的 GPRS 与外部 IP 网络互连的结构。

(1) 防火墙由 GPRS 运营商设置,支持 IP 协议应用程序运行,应限制外部 IP 网络对 GPRS 网络的访问。

(2) 域名服务器可在 GPRS 侧,也可以由外部 IP 网络负责维护。

(3) GPRS 的动态 IP 地址由 GGSN 分配,也可以使用外部动态主机配置协议(dynamic host configuration protocol,DHCP)进行管理。

(4) GPRS 网络通过信息过滤检查,确保只有 MS 发起的请求能通过防火墙,来自网络外部的访问被拦截。

GGSN 防火墙可以有效地保护 MS 不受 GPRS 外部网络攻击。对于来自 GPRS 内部合法用户的安全威胁,要实现 GPRS 移动台的安全数据传输,则依赖于 SGSN 实体用户之间以双向用户鉴权与身份认证为核心的访问控制策略。

GPRS 是叠加在 GSM 网络之上的移动通信增值服务网络,其网络通信的数据安全性首先依赖于移动网络自身的安全机制。GPRS 通过综合用户鉴权、数据加密、信息容灾以及合理设置防火墙等可靠性与安全技术手段,确保移动用户安全有效的数据业务传输。在保证 GPRS 网络性能的前提下,实施基于通信协议不同层次的全方位访问控制、数据保密与信息备份策略,是提高 GPRS 网络安全性的一条可行途径。

3.4 第三代移动通信系统安全

GSM 和窄带码分多址(code division multiple access,CDMA)技术是第二代数字移动通信技术的主体技术。与前两代系统相比,第三代的主要特征是可提供移动多媒体业务,其中高速移动环境支持 144kb/s、步行慢速移动环境支持 384kb/s、室内支持 2Mb/s 的数据传输。第三代移动通信的设计目标是为了提供比第二代系统更大的系统容量、更好的通信质量,而且要能在全球范围内更好地实现无缝漫游及为用户提供包括话音、数据及多媒体等在内的多种业务,同时也要考虑与已有第二代系统的良好兼容性。与第一代模拟蜂窝移动通信相比,第二代移动通信系统具有保密性强、频谱利用率高、提供业务丰富、标准化程度高等

特点。以欧洲的 GSM 系统与北美的窄带 CDMA 系统为代表的 GSM 系统具有标准化程度高、接口开放的特点,真正实现了个人移动性和终端移动性。窄带 CDMA 也称 IS-95 等,具有容量大、覆盖好、话音质量好、辐射小等优点。

3.4.1 第三代移动通信系统简介

第三代移动通信 IMT-2000(国际移动通信-2000)工作在 2000MHz 频段,最高业务速率可达 2000kb/s。它具有支持多媒体业务的能力,特别是支持 Internet 业务的能力。现有的移动通信系统主要以提供话音业务为主,随着发展一般也仅能提供 100～200kb/s 的数据业务,如 GSM 演进到最高阶段的速率能力为 384kb/s,而第三代移动通信的业务能力比第二代有明显的改进,它能支持话音分组数据及多媒体业务,能根据需要提供所需带宽。在 ITU 规定的第三代移动通信无线传输技术的最低要求中,必须满足以下三种环境的要求,即快速移动环境,最高速率达 144kb/s; 室外到室内或步行环境,最高速率达 384kb/s; 室内环境,最高速率达 2Mb/s。

1. 第三代移动通信的主要技术

第三代移动通信(IMT-2000)分为 CDMA 和 TDMA 两大类共五种技术,这里主要简述以下两种 CDMA 技术,即 IMT-2000 CDMA-DS(IMT-2000 直接扩频 CDMA)和 IMT-2000 CDMA-MC(IMT-2000 多载波 CDMA)。

1) IMT-2000 CDMA-DS

IMT-2000 直接扩频 CDMA 即 WCDMA,它在一个宽达 5MHz 的频带内直接对信号进行扩频。WCDMA 分为 FDD(frequency division duplexing,频分双工)和 TDD(time division duplexing,时分双工)方式两种。在 FDD 方式下,WCDMA 的码片速率为 4.096Mchip/s,能与 GSM 同时使用一个时钟,实现 WCDMA 和 GSM 双模手机。另外,使用这个速率容易实现 2Mb/s 的数据速率。WCDMA 的每个载波能放入 5MHz 的频谱带宽。如果有 15MHz 的频带,则可支持 3 个载波。为保证与其他载波间有 200kHz 以上的间隔,15MHz 内的 3 个载波间隔可在 4.2～5.0MHz 间变动。下行信道是双数据信道结构,双信道二相相移键控(B/SK)调制是 WCDMA 的重要特征之一。一路为余弦信号调制,相当于四相相移键控(quadrature phase shift keying,QPSK)调制的 I 路,是专用的物理数据信道(dedicated physical data channel,DPDCH),用于传送信息业务数据; 另一路为正弦信号调制,相当于 QPSK 调制的 Q 路,是专用的物理控制信道(dedicated physical control channel,DPCCH),用于传送公共控制命令。

WCDMA 的越区切换方法也很具特色,它采用移动台发起的非同步软切换方法,基站之间不需要同步,也不需要特别的同步参考源。为实现软切换,基站要确定在什么时间、什么位置启动软切换算法。一个 WCDMA 的移动台在同一频率检测其他基站(包括本基站)的信号,确认它们之间的时间差。检测到的时间信息经由本基站到达新的候选基站,候选基站调整它的新的专用信道的发射时间,也就是在发送信息的时间上进行调整,使不同基站在这个信息比特期间的下行码道上同步。TDD 方式下扩频增益是不变的,可使用多码传输实现高速数据通信。它的最大特点是在上行链路的多用户联合检测技术,这项技术使得在同一时隙同时工作的扩频码被联合检测方法分离开,即使彼此功率有几分贝之差。这正好弥

补了在 TDD 方式中信号功率不宜高精密控制的不足；同时还使用了智能动态信道分配法，该方法把信道动态分配与快速小区内切换结合起来了。

2) IMT-2000 CDMA-MC

IMT-2000 多载波 CDMA 即 CDMA 2000。这是美国提出的技术，是由多个 1.25MHz 的窄带直接扩频系统组成的一个宽带系统。

CDMA 2000 是在原 IS-95 标准的基础上进一步改进上行链路，增设导频信号实现基站的相干接收的。上行链路在极低速率(低于 8kb/s)传输时，不再使用突发方法而采用连续信号发射。下行链路也使用与上行链路相同的功率控制。高速数据传输时，使用 Turbo 纠错编码，下行发射也采用分集方式，支持先进的天线技术和波束成形技术等。CDMA 2000 采用不同射频信道带宽，可实现从 1.2kb/s 到 2Mb/s 甚至更高速率的信息数据传输，建议的射频带宽是基本信道带宽 1.25MHz 加上保护频间间隔 1.7MHz，3 个基本信道合用为 3.75MHz，加上保护频间间隔后为 5MHz。当然，还可以增加为使用 6 个、9 个、12 个基本信道。

CDMA 2000 为支持传送不同速率的信息业务，在系统协议的第 2 层增添了媒体控制层(MAC)。WCDMA 与此相似，为支持 MAC 的运行，在物理层增加了专用控制信道(dedicated control channel，DCCH)和公共控制信道，并使用可变的信包数据帧方法，帧长为 5ms 和 20ms。这种链路设计的最大优点是与 CDMA One 的 IS-95 标准兼容，带宽与 IS-95 相同，多载波信道信号与 IS-95 的信号正交，因此，CDMA 2000 可与 IS-95 共存。同时，CDMA 2000 保留了与 IS-95 相同的导频信道、同频信道和寻呼信道，使它的基站能向下兼容，提供 IS-95 的通信服务。CDMA 2000 的上行链路设有连续的导频信号，提供反相信号的相干检测，能在低信噪比下工作，降低功率控制环路的时延，并使功率控制、定时和相位跟踪与传输速率无关。语音和低速率数据使用卷积码，而高速数据准备使用 Turbo 码。

2. 第三代移动通信的关键技术

1) 高效信道编译码技术

第三代移动通信的另外一项核心技术是信道编译码技术。在第三代移动通信系统的主要提案中(包括 WCDMA 和 CDMA 2000 等)，除采用与 IS-95 CDMA 系统相类似的卷积编码技术和交织技术之外，还建议采用 Turbo 编码技术及 RS-卷积级联码技术。

2) 智能天线技术

随着社会信息交流需求的急剧增加、个人移动通信的迅速普及，频谱已成为越来越宝贵的资源。智能天线采用空分复用(space division multiple access，SDMA)，利用在信号传播方向上的差别，将同频率、同时隙的信号区分开来。它可以成倍地扩展通信容量，并和其他复用技术相结合，最大限度地利用有限的频谱资源。另外在移动通信中，复杂的地形、建筑物结构对电波传播的影响以及大量用户间的相互影响会产生时延扩散、瑞利衰落、多径、共信道干扰等，使通信质量受到严重影响。采用智能天线可以有效解决这个问题。

智能天线也叫自适应阵列天线，由天线阵、波束形成网络、波束形成算法三部分组成。它通过满足某种准则的算法去调节各阵元信号的加权幅度和相位，从而调节天线阵列的方向图形状，达到增强所需信号、抑制干扰信号的目的。智能天线技术适宜于 TDD 方式的 CDMA 系统，能够在较大程度上抑制多用户干扰，提高系统容量。但是由于存在多径效应，

每个天线均需一个 Rake 接收机,使基带处理单元复杂度明显提高。

3) 初始同步与 Rake 多径分集接收技术

CDMA 通信系统接收机的初始同步包括 PN 码同步、符号同步、帧同步和扰码同步等。CDMA 2000 系统采用与 IS-95 系统相类似的初始同步技术,即通过对导频信道的捕获建立 PN 码同步和符号同步,通过同步(Sync)信道的接收建立帧同步和扰码同步。WCDMA 系统的初始同步则需要通过"三步捕获法"进行,即通过对基本同步信道的捕获建立 PN 码同步和符号同步;通过对辅助同步信道不同扩频码的非相干接收确定扰码组号等,再通过对可能的扰码进行穷举搜索建立扰码同步。

Rake 多径分集接收技术克服了电波传播所造成的多径衰落现象。在 CDMA 移动通信系统中,由于信号带宽较宽,因而在时间上可以分辨出较细微的多径信号。对分辨出的多径信号分别进行加权调整,可使合成之后的信号得以增强。

4) 多用户检测技术

在传统的 CDMA 接收机中,各个用户的接收是相互独立进行的。在多径衰落环境下,由于各个用户之间所用的扩频码通常难以保持正交,因而造成多个用户之间的相互干扰,并限制系统容量的提高。解决此问题的一个有效方法是使用多用户检测技术,通过测量各个用户扩频码之间的非正交性,用矩阵求逆方法或迭代方法消除多用户之间的相互干扰。

从理论上讲,使用多用户检测技术能够在很大程度上改善系统容量,但算法的复杂度较高,把复杂度降低到可接受的程度是多用户检测技术能否应用的关键。

5) 功率控制技术

常见的 CDMA 功率控制技术可分为开环功率控制、闭环功率控制和外环功率控制三种类型。在 CDMA 系统中,由于用户共用相同的频带,且各用户的扩频码之间存在着非理想的相关特性,用户发射功率的大小将直接影响系统的总容量,从而使得功率控制技术成为 CDMA 系统中最为重要的核心技术之一。

3.4.2 第三代移动通信系统安全分析

3G 系统建立在第二代移动通信系统基础之上,2G 系统中必不可少的和行之有效的安全方法在 3G 系统中继续被采纳,2G 系统中存在的安全缺陷在 3G 系统中则被抛弃或改进。3G 移动通信系统的安全网络图如图 3.6 所示。

3G 系统为我们提供了一个全新的业务环境,除了对传统的话音与数据业务的支持外,还支持分布式业务与交互式业务。在这种环境下,3G 系统的业务呈现出新的特征,同时也要求系统提供与之相应的安全特性。

上述新业务特征和安全特性主要包括:由于需同时对不同的 SP(service provider,服务提供商)提供不同业务的并发支持以及多种新业务,3G 系统的安全特征需要综合考虑多业务条件下被攻击的可能性;3G 系统可以为固定接入提供更优越的服务,使用对方付费方式和预付款方式的用户可能会大大增加;终端的应用能力和用户的服务控制得到显著提升;对于可能出现的主动攻击,3G 系统中用户须具备相应的抗击能力;对非话音业务的需求可能超过话音业务,系统需具备更高的安全性;终端可能成为其他应用或移动商务的平台,可以支持多种智能卡的应用等。

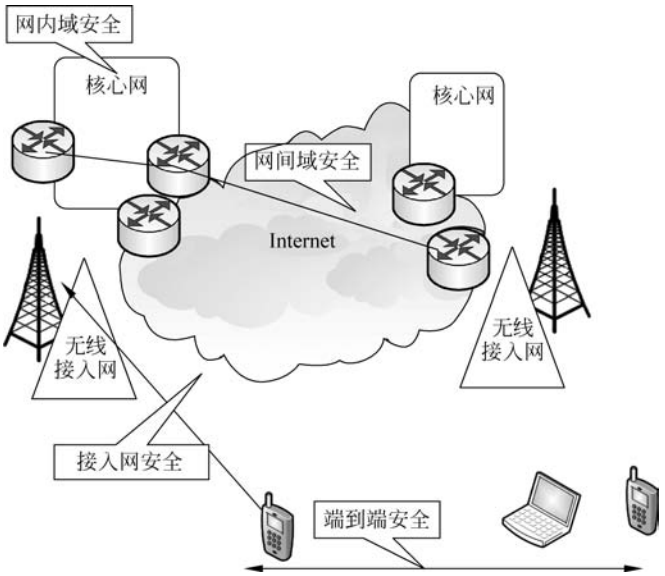

图 3.6　3G 移动通信系统的安全网络图

1. 3G 系统安全体系结构

3G 系统安全体系结构如图 3.7 所示，该结构中共定义了 3 个不同层面上的 5 组安全特性。每一组安全特性都针对特定的威胁，并可以完成特定的安全目标。

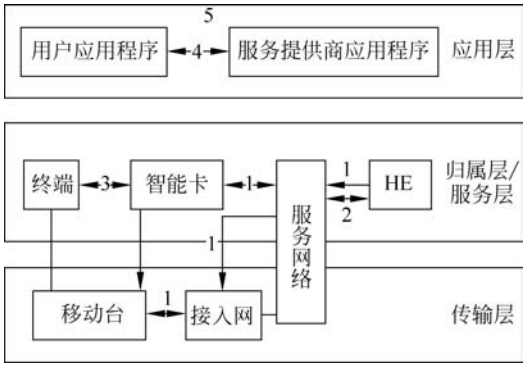

图 3.7　3G 系统安全体系结构图

三个层面由高到低分别是应用层、归属层/服务层和传输层，五组安全特性所包含的具体内容如下。

1）网络接入安全

网络接入安全主要是指提供接入 3G 服务网的安全机制，抵御对无线链路的攻击。空中接口的安全性是最重要的，因为无线链路最容易遭到攻击。这部分的功能主要有实体认证、用户识别机密性、机密性、移动设备识别和数据完整性。

（1）实体认证。

实体认证相关的安全特征有用户认证和网络认证。用户认证：服务网验证用户的身

份；网络认证：用户验证自己被连接到了一个由自己的 HE 授权并为其提供服务的服务网，并保证此次授权是新的。

为了实现这些目标，假设实体认证应该在用户和网络之间的每一个连接建立时出现。实体认证包含两种机制：一种是使用由用户移动终端传递给服务网 SN 的认证向量进行认证的机制；另一种是使用用户和 SN 之间在早先执行的认证和密钥建立过程期间已经建立的完整性密钥的本地认证机制。

(2) 用户识别机密性。

用户识别机密性相关的安全特征有：用户身份机密性，即业务传递到用户的永久用户识别不能在无线接入链路上被窃听；用户位置机密性，即用户在某个特定区域内出现或到达的位置不能在无线接入链路上被窃听被获取；用户的不可追溯性，即入侵者不能在无线接入链路上通过窃听判断出不同的业务是否被传递到相同的用户。

一般可通过使用临时识别符识别用户来实现上述目标，被拜访的服务网络通过这个临时识别符来识别用户。为了实现用户的不可追溯性，用户不能长时间使用同样的临时识别符，这就要求在无线接入链路上对任何可能暴露用户识别符的信令和用户数据都进行加密。

(3) 机密性。

与网络接入链路上的数据机密性相关的安全特征如下。

- 加密算法协商：MS 和 SN 能够安全地协商它们之间将要使用的算法。
- 加密密钥协商：MS 和 SN 能就它们随后使用的加密密钥达成一致。
- 用户数据的机密性：在无线接入接口上，用户数据不能被窃听。
- 信令数据的机密性：在无线接入接口上，信令数据不能被窃听。

加密密钥协商在执行认证和密钥协商机制的过程中实现，加密算法协商通过用户和网络之间的安全模式协商机制实现。

(4) 移动设备识别。

在某些情况下，SN 会请求 MS 发送终端的移动设备识别。除紧急呼叫外，移动设备识别应在 SN 的认证后发送。在网络上的传输是不受保护的，这个识别是不安全的，所以 IMEI 应当被安全地保存在终端中。

(5) 数据完整性。

与接入链路的网络上的数据完整性相关的安全特征如下。

- 完整性算法协商：MS 和 SN 可以就它们之后将要使用的完整性算法进行安全地协商。
- 完整性密钥协商：MS 和 SN 可以就它们之后将要使用的完整性密钥进行安全地协商并达成一致。

数据完整性和信令数据的信源认证是指接收实体(MS/SN)能够查证信令数据从发送实体发出之后没有被某种未授权方式修改，且与所接收的信令数据的数据源一致。

完整性密钥协商在认证和密钥协商机制的执行过程中实现，完整性算法协商使用用户和网络之间的安全模式下的协商机制实现，其中认证和密钥分配是建立在 HE/AuC 和 USIM 共享秘密信息基础上的相互认证。

2) 网络域安全

网络域安全定义了在运营商节点间数据传输的安全特性，保证网内信令的安全传送并

抵御对核心网部分的攻击。网络域安全包括以下三个层次。

第一层(密钥建立):非对称密钥对由密钥管理中心生成并进行存储;保存其他网络所生成的公开密钥;对用于加密信息的对称会话密钥进行产生、存储与分配;接收并分配来自其他网络的对称会话密钥,用于加密信息。

第二层(密钥分配):将会话密钥分配给网络中的节点。

第三层(通信安全):使用对称密钥来实现数据加密、数据源认证和数据完整性保护。

网络域的安全在GSM中没有提及,信令和数据在GSM网络实体之间是通过明文方式传输的。网络实体之间的交换信息是不受保护的,它们之间主要通过有线网络互联。依据3G系统的安全特性和安全要求,应该对现有有线网络的安全性进行增强,所以在3G系统中对网络实体之间的通信进行安全性保护。

在3G系统中,不同运营商之间通常是互联的。为了实现安全性保护,通常需要对安全域进行一定的划分。一般来说同一个运营商的网络实体统属一个安全域,不同的运营商之间的网络实体应设置安全网关(security gateway,SEG)。

SEG是用于保护本地基于IP的协议以及处理Za和Zb接口上的通信的、位于IP安全域边界上的实体,进入或离开安全域之前,所有的NDS/IP业务都要穿过边界实体SEG。每个安全域可能会涵盖一个或多个SEG,每个SEG负责处理所有进/出安全域的、朝向明确的、可到达的IP安全域的一组业务。一个安全域内的SEG的数量由外部可到达目的地、平衡业务负载和避免单点失败的需要来决定。SEG应该对网络之间的互操作具有加强的安全方法,这些安全包括过滤策略和防火墙等功能。由于SEG负责的是安全敏感的操作,在物理上我们应当对其给予保护。

在3G系统中,网络域之间的通信绝大部分都是基于IP方式的。因此网络域的安全中,IP网络层的安全是非常重要的一方面。IPSec方式是网络层安全的主要实现方式,3G系统中所使用的IPSec是修订后的IETF(Internet engineering task force,Internet工作任务组)所定义的标准IPSec,对移动通信网络的特点具有针对性。IPSec的使用可以用来实现网络实体间的认证,保护所传送数据的完整性、机密性以及对抗重放攻击。

3) 用户域安全

用户域安全是指安全接入移动站的安全特性,主要保证对移动台的安全接入,包括用户与USIM智能卡间的认证、USIM智能卡与终端间的认证以及链路的保护。

用户到USIM的认证是指用户接入USIM前必须经USIM认证,确保接入到USIM的用户为合法用户。该特征的性质是接入USIM是受限制的,直到USIM认证了用户为止,因此可确保接入USIM限制于一个授权用户或一些授权用户。为了实现该特征,用户和USIM必须共享安全存储在USIM中的秘密数据(例如PIN)。只有用户证明知道该秘密数据,它才能接入USIM。

USIM到终端的连接是指确保只有授权的USIM才能接入到终端或其他用户环境。最终,USIM和终端必须共享安全存储在USIM和终端中的秘密密钥。如果USIM未能证明它知道该秘密密钥,它将被拒绝接入终端。

4) 应用域安全

应用域安全是指用户应用程序与运营商应用程序安全交换数据的安全特性。USIM应用程序为操作员或第三方营运商提供了创建驻留应用程序的能力,这就需要确保通过网络

向 USIM 应用程序传输信息的安全性,其安全级别可由网络操作员或应用程序提供商根据需要选择。

在 USIM 和网络间的安全通信是指 USIM 应用工具包将为运营商或第三方提供者提供创建应用的能力,这些应用驻留在 USIM 上,类似于 GSM 中的 SIM 应用工具包。该功能需要用网络运营商或应用提供者选择的安全等级在网络上安全地将消息传递给 USIM 上的应用。

应用的安全性总是涉及用户终端的 USIM 卡,需要其支持来提供应用层的安全性。随着应用工具的发展,各种各样的应用业务将会出现。

5) 安全特性的可视性及可配置能力

安全特性的可视性及可配置能力是指用户能够得知操作中是否安全,以及对安全程度自行配置的安全特性,即用户能获知安全特性是否在使用以及服务提供商提供的服务是否需要以安全服务为基础。

虽然安全特征一般对用户是透明的,但对某些事件以及用户所关心的问题,应该提供更多安全特征的用户可视性,用以通知用户与安全相关的事件。

2. 3G 系统的安全功能结构

3G 系统的安全功能结构如图 3.8 所示。

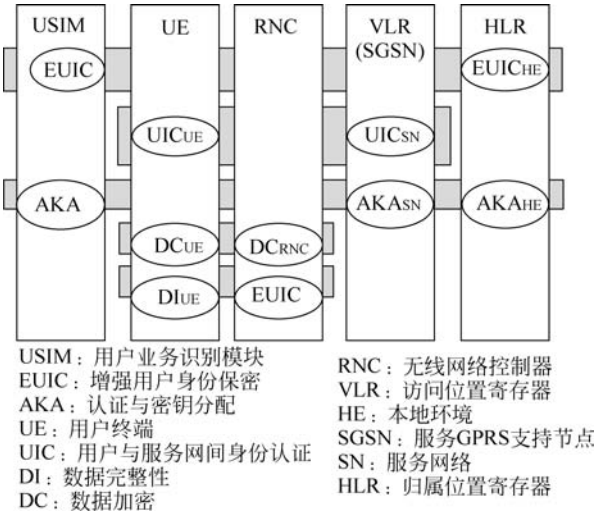

图 3.8 3G 系统的安全功能结构图

图 3.8 中竖条表示 3G 系统安全结构中包括的网络单元。

(1) 用户域:包括 USIM(用户服务识别模块)和 UE(用户设备)。

(2) 服务域(SN):包括 RNC(无线网络控制器)和 VLR(访问位置寄存器)。

(3) 归属环境(HE):包括 HLR/AuC(归属位置寄存器/认证中心)。

水平线表示安全机制,安全措施分为如下 5 类。

(1) 增强用户身份保密(EUIC):通过 HE/AuC(本地环境/认证中心)对 USIM(用户业务识别模块)身份信息进行认证。

(2) 用户与服务网间的身份认证(UIC)。

(3) 认证与密钥分配(AKA)：用于 USIM、VLR/SGSN(访问位置寄存器/服务 GPRS 支持节点)HLR(归属位置寄存器)间的双向认证及密钥分配。

(4) 数据加密：UE(用户终端)与 RNC(无线网络控制器)间信息的加密。

(5) 数据完整性：用于对交互消息的完整性、时效性及源与目的地进行认证。

3. 3G 系统的安全问题

1) 3G 系统面临的威胁

3G 系统的安全所面临的威胁大致可以分为如下几种。

(1) 非法获取敏感数据，攻击系统的保密信息，主要方式如下。

① 伪装：攻击者伪装成合法身份，使用户或网络相信其身份是合法的，以此窃取系统的信息。

② 窃听：攻击者未经允许非法窃听通信链路用以获取信息。

③ 业务分析：攻击者通过分析链路上信息的内容和特点，来判断用户所处位置或获取正在进行的重要交易的信息。

④ 泄露：攻击者以合法身份接入进程用以获取敏感信息。

⑤ 浏览：攻击者搜索敏感信息所处的存储位置。

⑥ 试探：攻击者发送信号给系统以观察系统会做出何种反应。

(2) 非法访问服务，主要方式有：攻击者伪造成用户实体或网络实体，非法访问系统服务；通过滥用访问权利网络或用户非法得到未授权的服务。

(3) 非法操作敏感数据，攻击信息的完整性，主要方式有攻击者有意篡改、插入、重放或删除信息。

(4) 滥用或干扰网络服务而导致的系统服务质量的降低或拒绝服务，包括如下内容。

① 资源耗尽：服务网络或用户利用特权非法获取未授权信息。

② 服务滥用：攻击者通过滥用某些特定的系统服务获取好处，或导致系统崩溃。

③ 干扰：攻击者通过阻塞用户控制数据、信令或业务使合法用户无法正常使用网络资源。

④ 误用权限：服务网络或用户通过越权使用权限以获取信息或业务。

⑤ 拒绝：网络或用户拒绝做出响应。

(5) 否认，包括网络或用户对曾经发生的动作表示否认。

2) 针对 3G 系统的攻击

针对 3G 的攻击方法主要包含针对系统核心网络的攻击、针对系统无线接口的攻击和针对终端的攻击三种方式。

针对系统核心网络的攻击包括如下内容。

(1) 非法获取数据：指入侵者进入服务网内窃听用户数据、信令数据和控制数据，未经授权访问存储在系统网络单元内的数据，甚至进行主动或被动流量分析。

(2) 数据完整性攻击：指入侵者修改、插入、删除或重放用户控制数据、信令或业务数据，或假冒通信的某一方修改通信数据，或修改网络单元内存储的数据。

(3) 拒绝服务攻击：指入侵者通过干扰在物理上或协议上的控制数据、信令数据或用户数据在网络中的正确传输，来实现网络中的拒绝服务攻击；或通过假冒某一网络单元来

阻止合法用户的业务数据、信令数据或控制数据,使得合法用户无法接受正常的网络服务。

(4) 否定:指入侵者冒充用户否认业务费用、数据来源或接收到的其他用户的数据;或冒充网络单元否认发出信令或控制数据,否认收到其他网络单元发出的信令或控制数据。

(5) 非法访问未授权业务:指入侵者模仿合法用户使用网络服务,或假冒服务网以利用合法用户的接入尝试获得网络服务,抑或假冒归属网以获取使他能够假冒某一方用户所需的信息。

针对 3G 系统无线接口的攻击方法主要包括如下内容。

(1) 非法获取非授权数据:指入侵者窃听无线链路上的用户数据、信令数据和控制数据,甚至被动或主动进行流量分析。

(2) 对数据完整性的攻击:指入侵者修改、插入、重放或者删除无线链路上合法用户的数据和信令数据。

(3) 拒绝服务攻击:指入侵者通过在物理上或协议上干扰用户数据、信令数据或控制数据在无线链路上的正确传输,来实现无线链路上的拒绝服务攻击。

(4) 非法访问业务的攻击:指攻击者伪装成其他合法用户身份非法访问网络,或切入用户与网络之间进行中间攻击。

(5) 捕获用户身份攻击:指攻击者伪装成服务网络,对目标用户发出身份请求,从而捕获用户明文形式的永久身份信息。

(6) 压制目标用户与攻击者之间的加密流程,使之失效。

针对终端的攻击主要是攻击 USIM 和终端,包括:使用借来的或偷窃的 USIM 或终端;篡改 USIM 或终端中的数据;窃听 USIM 或终端间的通信;伪装身份以截取 USIM 或终端间交互的信息;非法获取 USIM 或终端中存储的数据。与终端安全相关的威胁包括如下内容。

(1) 攻击者利用窃取的终端设备访问系统资源。

(2) 对系统内部工作有足够了解的攻击者可能获取更多的访问权限。

(3) 攻击者利用借来的终端超出允许的范围访问系统。

(4) 通过修改、插入或删除终端中的数据来破坏终端数据的完整性。

(5) 通过修改、插入或删除 USIM 卡中的数据来破坏 USIM 卡数据。

3.5 第四代移动通信系统安全

第四代移动通信技术(the fourth generation of mobile phone mobile communication technology standards,4G)是第三代移动通信系统的延伸,是一种用来替代 3G 蜂窝的无线蜂窝系统,在业务、功能、频带上都不同于第三代系统。

4G 通信技术具备向下相容、全球漫游、网络互联、多元终端应用等,并能从 3G 通信技术平稳过渡至 4G。4G 网络应用包括移动视频直播、移动/便携游戏、基于云计算的应用、导航等领域。

3.5.1 第四代移动通信系统简介

4G 可称为宽带接入和分布网络,具有非对称的超过 2Mb/s 的数据传输能力,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。它可以在不同的固定、无线平台和跨越不同频带的网络中提供无线服务，可以在任何地方用宽带接入互联网(包括卫星通信和平流层通信)，能够提供定位定时、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。

1. 4G 的技术特点

(1) 高速率。对于大范围高速移动用户(250km/h)，传输数据为 2Mb/s；对于中速移动用户(60km/h)，数据速率为 20Mb/s；对于低速移动用户(室内或步行者)，数据传输速率为 100Mb/s。

(2) 技术发展以数字宽带技术为主。在 4G 移动通信系统中，信号以毫米波为主要传输波段，蜂窝小区也会相应小很多，很大程度上提高了用户容量。

(3) 良好的兼容性，其中包括了对用户类型的兼容和对业务类型的兼容。针对不同类型的用户，4G 移动通信系统能根据动态的网络和变化的信道条件进行自适应处理，使低速的用户与高速的用户以及各种各样的用户设备能够共存与互通，从而满足系统多类型用户的需求。除此之外，4G 移动通信系统还支持丰富的移动业务，其中包括高清晰度图像业务、会议电视、虚拟现实等，使用户在任何地方都可以获得任何所需的信息服务，将个人通信、信息系统、广播和娱乐等行业结合成一个整体，更加安全方便地向用户提供更广泛的服务与应用。

(4) 先进技术的应用。4G 移动通信系统以几项突破性技术为基础，如 OFDM 多址接入方式、智能天线和空时编码技术、无线链路增强技术、软件无线电技术、高效的调制解调技术、高性能的收发信机和多用户检测技术等，这些大幅提高了无线频率的使用效率和系统可实现性。

(5) 高度自组织、自适应的网络。4G 移动通信系统是一个完全自治、自适应的网络，具有较强的灵活性、智能性和适应性，能够自适应地进行资源分配，对通信过程中不断变化的业务流的大小进行相应处理，拥有对结构的自我管理能力，以满足用户在业务和容量方面不断变化的需求。

(6) 开放的平台。4G 移动通信系统在移动终端、业务节点及移动网络机制上具有“开放性”，用户能够自由地选择协议、应用和网络；利用无线接入技术提供语音、高速信息业务、广播以及娱乐等多媒体业务接入方式，让用户可在任何时间、任何地点接入到系统中。

2. 4G 网络的关键技术

1) OFDMA 技术

正交频分多址(orthogonal frequency division multiple access，OFDMA)，是 OFDM 技术的演进，是将 OFDM 和 FDMA 技术结合，利用 OFDM 对信道进行子载波化后，在部分子载波上加载传输数据的传输技术。OFDMA 多址接入系统将传输带宽划分成正交的互不重叠的一系列子载波集，将不同的子载波集分配给不同的用户实现多址，可动态地把可用宽带资源分配给需要的用户，很容易实现系统资源的优化利用。OFDMA 又分为子信道 OFDMA 和跳频 OFDMA。

(1) 子信道 OFDMA。

将整个 OFDM 系统的带宽分成若干子信道,每个子信道包括若干子载波,分配给每一个用户(也可一个用户占用多个子信道),如图 3.9 所示。这种分配方式相对固定,即某个用户在相当长的时长内将使用指定的子载波组。OFDM 子载波可以按照两种方式组合子信道:集中式和分布式。集中式可以降低信道估计的难度,但这种方式获得的频率分集增益较小,用户平均性能略差;分布式获得的频率分集增益较大,但是信道估计复杂,无法采用频域调度,抗频偏能力也较差。

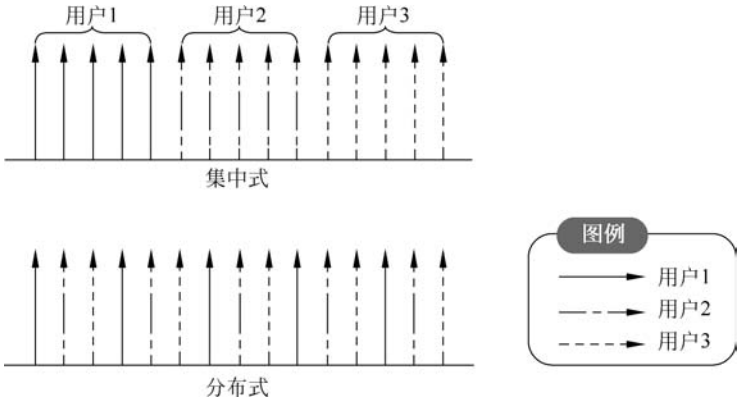

图 3.9 子信道 OFDMA 的组合模式

(2) 跳频 OFDMA。

在跳频 OFDMA 系统中,分配给一个用户的子载波资源快速变化。每个时隙,此用户在所有子载波中抽取若干子载波使用;同一时隙中,各用户选用不同的子载波组,如图 3.10 所示。不同的是,这种子载波的选择通常不依赖信道条件而定,而是随机抽取的。在下一个时隙,无论信道是否发生变化,各用户都跳到另一组子载波发送,但用户使用的子载波仍不冲突。这种方式的周期比子信道 OFDMA 的调度周期短得多,并且可以利用频域分集增益。使用的子载波可能冲突,但快速跳频机制可以将这些干扰在时域和频域分散开来,即可将干扰白化为噪声,大大降低干扰的危害,适用于负载不是很多的系统。

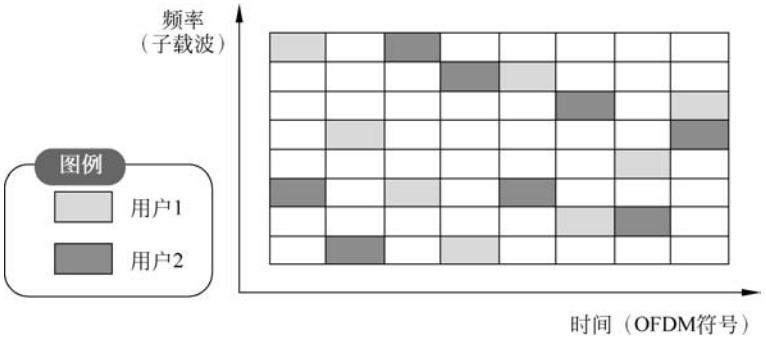

图 3.10 跳频 OFDMA 的组合模式

2) 软件无线电技术

软件定义无线电(software defined radio,SDR)是一种无线电广播通信技术,它基于软

件定义的无线通信协议而非通过硬连线实现。频带、空中接口协议和功能可通过软件下载和更新来升级，而不用完全更换硬件。其核心技术包括：多频段、多波束无线与宽带 RF 信号处理、宽带 A/D 变换、高速数字信号处理。软件无线电还采用了硬件平台与软件平台结合的全新体系结构，通过硬件平台来对软件进行编程和管理来实现通信功能。软件无线电的主要特点是具有很强的灵活性和开放性。

3）智能天线技术

智能天线（smart antenna，SA）也叫自适应阵列天线，它由天线阵、波束形成网络、波束形成算法三部分组成。它通过满足某种准则的算法去调节各阵元信号的加权幅度和相位，从而调节天线阵列的方向图形状，以达到增强所需信号、抑制干扰信号的目的。

4）MIMO 技术

多入多出系统（multiple-input multiple-output，MIMO）是指同时在发射端和接收端使用多个天线的通信系统。MIMO 可在不增加带宽的情况下成倍地提高通信系统的容量和频谱利用率，同时其空间分集可显著改善无线信道的性能，提高无线系统的容量及覆盖范围。

3.5.2 第四代移动通信系统安全分析

在 LTE 时代，国际标准化组织为 4G 网络打造了比现有 3G、2G 网络和固定互联网更可靠、鲁棒性更高的安全机制。TD-LTE 网络安全沿用 3G 网络的用户身份保护机制、双向身份认证和鉴权密钥协商机制，并根据 TD-LTE 扁平化网络架构定义了新的安全特性：4G 网络安全包括接入层（access stratum，AS）安全和非接入层（non-access stratum，NAS）安全，使得无线空口和核心网络安全相互独立，从而提高了整个系统的安全性。

随着网络运营环境的不断复杂化、4G 网络的日益普及扩大化、无线网络本身的开放性特点以及网络攻击技术的不断高级和多样化，网络线路的安全性受到越来越严重的威胁。

1. 4G 网络系统的缺陷及存在的安全问题

（1）4G 无线系统的网络层移动性管理和核心网的移动 IP 技术问题以及 4G 标准问题是 4G 网络系统投入使用的根本问题。网络层移动性往往关系到不同网络频段的漫游移动客户，这是 4G 移动性管理的关键问题。核心网的移动 IP 问题代表的是一种可升级的全球移动性的方案。

（2）4G 通信系统缺乏定位和快速无缝切换的技术支持。因此，采用先进的网络结构系统和管理方案，使用高速有效地发送和切换协议，切实有效地解决数据对视和延迟问题是解决这个问题的根本。

（3）无线网络容易受到干扰和攻击。除了局域网外，一般网络都处于开放的模式，因此给不法黑客提供了使用各种病毒软件威胁用户财产和人身安全的机会。

（4）无线网络终端存在安全隐患。无线网络在实际的应用中是无法移动的，一旦被黑客窃取，便可传播各种低俗非法的言论和视频。

（5）没有统一的标准约束。目前无线网络在全国范围内都可以进行移动通信，但是各

个通信系统之间却经常出现不兼容的现象,这是因为没有统一的标准来约束,导致无法实现无缝衔接,从而给用户带来诸多麻烦。

(6) 4G 技术尚不成熟。4G 网络架构非常复杂,在实际应用中并没有那么容易实现在理论上数据传输比 3G 网络高出一个数量级。

(7) 容量有限。随着用户的增多,网络的容量有限性将限制网速,其中一个解决的办法是减少基站的覆盖半径,但是很难达到理论的速度。

2. 4G 网络安全防范措施和对策

(1) 建立透明公开的 4G 安全体系:建立一套独立于系统设备,能够独立完成数据加密的安全系统。

(2) 用户普及网络安全防范意识:移动通信网络应该面向广大用户普及网络安全意识,用户应该根据需要设置保密级别和安全参数。

(3) 移动网络与互联网网络兼容:设计并使用移动网络与互联网网络相兼容的安全防护措施,对网络入侵进行实时预防和监测,隔离和避免恶意攻击;同时,定期升级安全防护系统,以应对新的网络入侵。

(4) 应用新的密码技术:随着科学技术的不断进步,生物识别技术、量子密码技术以及椭圆曲线密码技术等高端的加密技术可以融入 4G 网络通信加密技术中来,加强了 4G 网络自身的抗攻击能力,从而保证了网络系统的安全性和可控性。

(5) 建立健全网络系统结构模式:建立适合未来网络通信系统的安全体系结构模式,保护用户的个人隐私和人身财产安全。

(6) 安装更强级别的防火墙:用户在使用无线网络以及下载文件的过程中,无可避免地会受到来自互联网的病毒的入侵,这时候就需要一道安全可靠的防火墙阻止恶意入侵,因此需要在 4G 网络中设置比 3G 网络更为强大、高级、可靠的防火墙来保证整个网络的安全。

3.6 第五代移动通信系统安全

5G 作为新一代无线移动通信网络,主要用于满足 2020 年以后的移动通信需求。在高速发展的移动互联网和不断增长的物联网业务需求的共同推动下,要求 5G 具备低成本、低能耗、安全可靠的特点,同时传输速率比 4G 提升 10～100 倍,峰值传输速率达到 10Gb/s,端到端时延达到 ms 级,连接设备密度增加 10～100 倍,流量密度提升 1000 倍,频谱效率比 4G 提升 5～10 倍,能够在 500km/h 的速度下保证用户体验。5G 使信息通信突破了时空限制,给用户带来了极佳的交互体验:极大地缩短了人与物之间的距离,并快速实现了人与万物的互通互联。

5G 网络支持虚拟现实、超清视频以及移动游戏等应用。随着物联网技术的广泛普及,智能电网、智慧城市、移动医疗、车载娱乐、运动健身等服务将广泛运用 5G 网络技术;在公共安全方面,如紧急语音通话、无人机远程监测、入侵监测、急救人员跟踪等场景,5G 通信系统需要具有零延迟、高可靠性的特点。

3.6.1 第五代移动通信系统简介

目前,5G 技术已处于商用部署阶段,全世界 70 个国家已经有 169 个运营商发布了 5G,算上正在投资 5G 的运营商,整体运营商数量已经超过 400 个。5G 已经充分融入了人们的生活。

第五代移动通信网络基于如下关键技术实现了巨大突破。

1) 边缘计算技术

边缘计算是 5G 重要的应用技术之一。边缘计算是指在靠近物或数据源头的一侧,采用网络、计算、存储、应用核心能力为一体的开放平台,就近提供最近端服务。边缘计算可以为 5G 通信网络应用提供一个网络、计算、存储等多功能的平台,从而可以加快 5G 通信数据的处理速度。传统的无线网络在运行和计算时,需要将数据从基站传输到服务器进行加工处理和路由转发,数据处理时延较高。而边缘计算实现了无线数据存储的本地化,从而降低了数据处理时延,因此可以为车联网、工业控制提供技术支持。

2) 大规模 MIMO 技术

MIMO(multiple input multiple output,多进多出)技术在发射端和接收端分别使用多个发射天线和接收天线,使信号通过发射端与接收端的多个天线传送和接收,从而改善通信质量,在 4G 时代被广泛应用。而大规模 MIMO 技术在传统的 MIMO 技术基础上将 8 天线通道提升到了 16 通道、32 通道和 64 通道,显著提升了 5G 网络的信息收发能力,降低了数据传输时延,从而满足车联网、工业控制网络的实时性和高可靠性。

此外,大规模 MIMO 技术拥有如下优点:拥有更精确的 3D 波束赋形,使用户始终处于小区区域内的最佳信号区域;此外其波束非常窄,可以大大减小用户间的干扰,因此可以同时传输不同用户的数据,从而提高数据吞吐量和网络容量。

3) 超密集组网技术

如今,随着 5G 商业部署的完善,对于流量通信的需求变得极高,为了满足这一点,超密集组网是关键技术。超密集组网是多层异构网络,物理上由不同频段、不同功率的宏基站和大量微基站组成;逻辑上由虚拟宏小区和大量微小区组成。而由于其多层异构的特点,在网络部署中的灵活度、信息速率、系统容量等方面相对于传统的单层蜂窝网络具有极大的优势,这些优势符合 5G 的万物互联的重要思想,满足包括智慧医疗、智能电网等典型物联网业务关于场景多样、业务量巨大的新需求。

4) 网络切片技术

随着差异化服务的需求越来越多,传统的硬交换路由器因其提前配置难以更改的缺点已不能满足需求,因此网络切片技术成为 5G 中至关重要的一项技术。网络切片就是把运营商的物理网络分成多个虚拟的逻辑网络,每个网络针对不同的应用场景适应不同的服务需求,通过合理的切片规划、切片部署、切片维护、切片优化来确保网络的移动性、安全性、低时延和可靠性。例如,对于移动宽带来说,其主要需求是更高的数据容量;而对于任务关键性物联网,超低时延和高可靠性是其所需。

第五代移动通信系统开启了物联网时代,截至目前已经完成了大规模的商业部署,在社

会各个行业得到广泛应用,包括如下 6 个领域。

1) 政务与公共应用方面

随着第五代移动通信技术(5G)的广泛普及,5G 与云计算、物联网、大数据、人工智能等技术结合,大力发展智慧政务、智慧安防、智慧城市、智慧楼宇、智慧环保等领域,大大提升了远程政务服务能力,以及城市的安防反应速度和城市各方面管理水平。例如,广州南沙区 5G 电子政务中心目前提供材料高速上传、人脸识别、在线排队等业务,大大提高了人民群众的办事效率;雄安新区的 5G 智慧安防,采用基于 5G 网络的无人机、无人船、无人车等设备协调合作,实现海陆空全面一体化安防;千岛湖的 5G 智慧治水,借由 5G 网络并协同物联网、人工智能、大数据等技术,实现了水域科学治理的目标。

2) 工业方面

在传统模式下,制造商依靠有线技术连接应用,近年来也曾采用 WiFi、蓝牙和 WirelessHART 等无线技术,但是以上无线技术在带宽、可靠性和安全性方面存在局限。如今,随着 5G 网络的大规模部署,基于 5G 网络特性实现的远程设备操控能力使得制造业向着无线机器人云端控制这一方向迈出了历史性的一步,制造过程中的状态监控、环境监控等也变得越来越智能化,为制造业提供了一个高实时、高可移动性、高 QoS 保障的智能化产业链。例如,杭州汽轮动力集团有限公司的 5G 三维扫描建模检测系统,在传统的激光三维扫描建模系统基础上,使用 5G 技术将实时测量所得海量数据上传到云端,由云端服务器进行产品检测。对部件的检测时间从 2～3 天降低到 3～5 分钟,实现了生产力的巨大进步。

3) 农业方面

随着近年来人类社会的科技发展,农业的机械化一直处在演变之中,而随着 5G 技术的出现以及大规模普及,农业的发展渐渐转变为机械化、信息化、智慧化的跨越式融合发展。通过 5G 与相关尖端技术结合,使得农业生产过程中的流程监测、安全监控、病虫害监测等自动化、智能化。例如,淄博临淄区禾丰的 5G 智慧农场,通过 5G 网络以及人工智能等相关技术,实现农业生产自动化作业,包括无人驾驶的玉米播种机、旋耕机等,大大节省了人力物力,提高了生产力,创造了安全可靠、环保节能的农场作业。

4) 文体娱乐方面

目前,我国物质越趋丰富,精神需求渐渐加大,这也是保障人民身心健康的重要一环。5G 的一个重要商业用例就是固定无线接入(WTTx),即区别于固定线路,采用移动网络技术提供家庭互联网接入。基于这项技术提供的大带宽、8K 视频逐步上线。

5) 医疗方面

5G 网络为医院带来了远程诊断、远程手术、应急救援等智慧医疗应用,很好地解决了小城市和边远地区医疗资源不足、医疗水平较低的问题,并在应对紧急救援和突发事故以及病患难以挪动等特殊情况时提供了更多更好的选择,显著提升了医疗效率,极大地保护了人民的生命安全。早在 2019 年 7 月,北京协和医院就开展了 5G 远程眼科医疗会诊,并完成全球首例 5G 远程眼底靶向导航激光手术治疗。此次手术首次向全世界展示了 5G 网络低延时、大带宽的特点,为今后的远程诊断、远程手术等远程医疗做出了良好的示范。而基于 5G 的远程医疗技术,目前正在逐步覆盖全国各地。

6) 交通运输方面

5G 网络的实现以及商用部署,极大地推进了我们迈向 2035 年基本建成交通强国的目

标。2019年，广州地铁的5G＋智慧地铁示范项目正式启动，经过两年时间的运作，取得了非常不错的效果。通过分析地铁的运作模式以及其处于地下这一特殊的地理位置的情况，量身定制了5G专享网络，实现了智慧安检、高精度室内定位、高清视频监控、AI智能预警、AR辅助检修等功能，极佳地提升了客户的乘车体验，有效保障了客户的乘车安全，并显著节省了地铁运营的人力物力。

3.6.2　第五代移动通信系统安全分析

5G网络采用了新型组网方式，包括移动Ad Hoc网络、无定形小区、密集网络、异构网络融合及网络虚拟化等；多种无线和移动通信方式并存，D2D、M2M、WiFi、可见光、近场无线通信等新技术；移动业务层出不穷，移动数据流呈爆炸式增长，未来的移动终端也呈现多样化的趋势；用户周边的无线网络和终端设备显著增加，并且融合业务对网络资源的需求越来越大，因此异构无线网络及其终端之间协同为用户服务的业务提供方式势在必行。

随着5G核心技术研究的深入，未来5G网络构架主要走向两个趋势，一个是METIS（mobile and wireless communications enablers for the twenty-twenty information society），是一个由欧盟主导的5G关键技术研究项目，其目的在于保持欧洲在无线通信研究领域的领先地位；另一个是IMT-2020(5G)推进组，是由我国主导的5G技术研究和推进机构，目前已经集合了包括华为、中兴通信、大唐电信等众多国内信息和通信领域的顶级公司和研究机构。以下将选择IMT-2020(5G)推进组进行介绍，并对其安全性进行分析。

1. IMT-2020(5G)推进组的5G概念

IMT-2020(5G)推进组的5G概念由一个“标志性能力指标”和“一组关键技术”共同定义。“标志性能力指标”是指超高的用户体验速率(Gb/s级)，而“一组关键技术”则包括大规模天线阵列、超密集组网、新型多址、全频谱接入和新型网络架构。IMT-2020(5G)推进组的5G概念强调用户之于网络速度的感受。

1) IMT-2020(5G)推进组的5G架构

IMT-2020(5G)推进组认为未来的5G是基于SDN、NFV和云计算技术的更加灵活、智能、高效和开放的网络系统，并通过使用三朵云（接入云、控制云和转发云）的架构来描述未来5G的结构，如图3.11所示。

接入云支持多种无线制式的接入，并分为融合集中式和分布式这两种无线接入网络架构，适应各种类型的回传链路，实现更灵活的组网部署和更高效的无线资源管理。控制云实现局部和全局的会话控制、移动性管理和服务质量保证功能，并构建面向业务的网络能力开放接口，从而满足业务的差异化需求并提升业务的部署效率。转发云则基于通用的硬件平台，在控制云高效的网络控制和资源调度下，实现海量业务数据流的高可靠、低时延、均负载的高效传输。

2. IMT-2020(5G)推进组的安全性分析

IMT-2020(5G)推进组的5G架构强调云计算、云存储等技术的运用，因此传统的云计算安全问题也应当被5G安全考虑。在5G控制云中，涉及安全访问规则的云端存储、迁移、访问等云存储安全问题；接入云涉及边缘计算、大数据分布式计算及处理等安全融合问题；

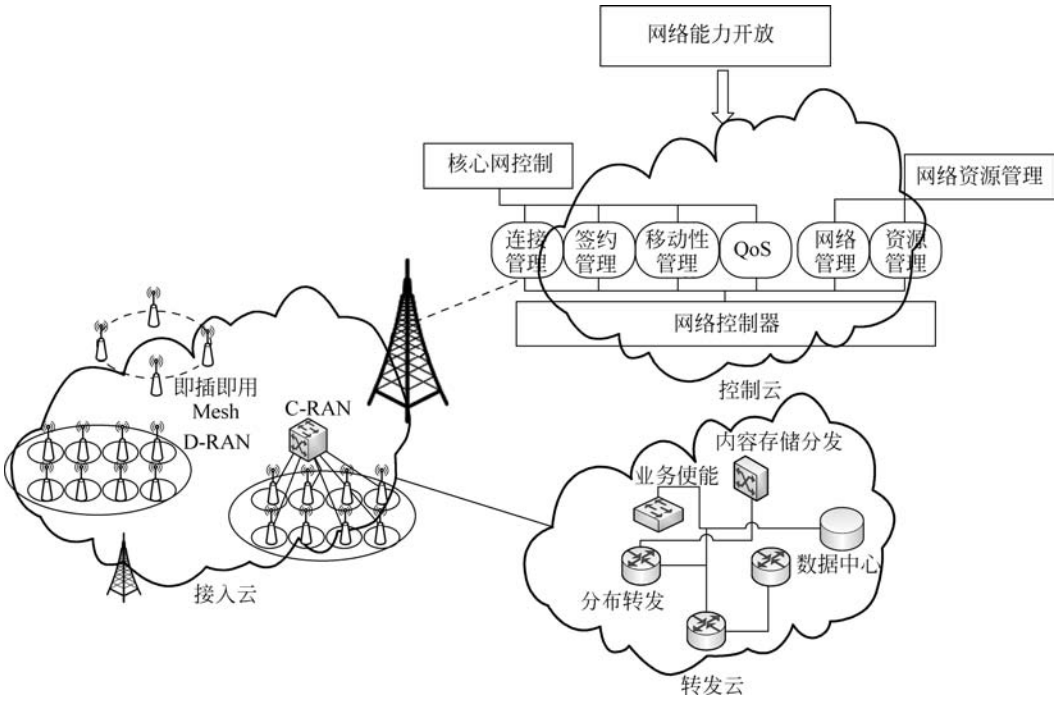

图 3.11 IMT-2020(5G)推进组的 5G 架构

转发云涉及分布式数据的私密性、完整性保密机制等安全问题都应当在 5G 环境中被进一步地讨论。

3.7 第六代移动通信安全

第六代移动通信技术(6G)是一个概念性无线网络移动通信技术,目前仍处于研发阶段,其主要促进的是物联网的发展,传输能力可能会相比 5G 提升 100 倍,同时网络延迟也可能从毫秒级降到微秒级。在峰值速率、时延、流量密度、连接数密度、移动性、频谱效率、定位能力等方面远优于 5G。

6G 网络将把卫星通信与地面无线相结合。在将来,借助 6G 的独特优势,网络信号将可以抵达世界上任意一个角落,实现全球全覆盖。一方面,这将有效解决某些偏远山区的孩子无学可上、病人无医可看的局面,让每个人都能平等地享受网络为人们生活带来的便利;另一方面,可以使与人们生活息息相关的"天气预报"进一步进化,帮助人们更加轻松地应对自然灾害,做到"不打无准备之仗"。

6G 相对于现在的 5G 网络来说,带来的将不仅是技术上的突破,在网络容量和传输速率上的进步将带来更为深远的影响,即距离智联万物这个"终极目标"的实现更进一步。

目前,实现第六代移动通信技术,要实现如下关键技术的突破。

(1) 太赫兹频段的频率相比 5G 的频率来说要高出许多倍,大概在 100GHz～10THz。从 1G 的 0.9GHz 到 6G 的太赫兹频段,人们所使用的无线电磁波的频率不断提高。当无线电磁波的频率提高时,允许分配带宽的范围也会相应增加,因此传递数据的效率就会随之增加。

（2）在空间通信方面，太赫兹波可以作为高速宽带的通信载体。太赫兹波具有强大的穿透能力以及极强的方向性，因此适用于高宽带需求的卫星通信领域。但目前6G在太赫兹频段的应用上存在如何改善覆盖和减少干扰的难题。

（3）当无线电磁波的频率大于10GHz时，其主要的信号传播方式为反射和散射。此外，随着无线电磁波的频率升高，其传播时的损耗随之增加，覆盖范围随之减小，绕射能力随之降低，这些现象带来了网络信号覆盖上的问题。

目前，在第五代移动通信技术使用的大规模MIMO技术是解决以上技术难题的主要研究方向。

3.8　本章小结

本章从第二代移动通信系统开始，分别介绍了GSM系统、通用分组无线业务（GPRS）、UMTS、3G、4G、5G的安全，最后简单介绍了6G概念和主要面临的挑战。

思考题

1. 如何保障GSM系统的安全保密性能？
2. 请简要介绍GPRS的安全防火墙技术。
3. 5G应用包括哪些方面？
4. 简要介绍第三代移动通信的主要技术。

参 考 文 献

[1] 张方舟，叶润国，冯彦君，等. 3G接入技术中认证鉴权的安全性研究[J]. 微电子学与计算机，2004，21(9)：33-37.

[2] 冯登国，徐静，兰晓. 5G移动通信网络安全研究[J]. 软件学报，2018，29(6)：1813-1825.

[3] 陈航宇，毛久嶂. 第三代移动通信系统安全技术解析[J]. 移动信息，2016，8(6)：229-230.

[4] 高倩. GSM移动通信系统概述[J]. 数字传媒研究，2015，32(7)：42-46.

[5] 余海燕. 第三代移动通信系统全网安全的研究与策略[D]. 青岛：中国海洋大学，2009.

[6] 赵国锋，陈婧，韩远兵，等. 5G移动通信网络关键技术综述[J]. 重庆邮电大学学报（自然科学版），2015，27(4)：441-452.