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，移动通信在短短的二十多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1代移动通信的诞生。1987年，我国首个TACS制式模拟移动电话系统建成并投入使用。1993年，我国首个全数字移动通信系统(GSM)建成开通，这使我国进入了第2代移动通信时代。2001年前后，多个国家相继开通了3G商用网络，标志着第3代移动通信时代的到来。

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增长的基础上的。第1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2代移动通信是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3代移动通信是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4代移动通信是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于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2代数字蜂窝移动通信系统(2G)的安全机制都是基于私钥密码体制，采用共享秘密数据(私钥)的安全协议，实现对接用户的认证和数据信息的保密，在身份认证及加密算法等方面存在着许多安全隐患。例如网络间的密钥是明传的；加密未达核心网络，导致部分网段有明文传输；对信道的保护依赖于加密技术；未提供数据完整性认证；升级改善安全功能无灵活性等。

随着第3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，各种无线应用将极大地丰富人们的日常工作和生活，也将为国家信息化战略提供强大的技术支撑，因而网络安全问题就显得更加重要。

3.2 GSM 系统安全

GSM 原意为“移动通信特别小组”(Group Special Mobile),是欧洲邮电主管部门会议(CEPT)为开发第二代数字蜂窝移动系统而在 1982 年成立的机构,开始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。在 1995 年年初,全世界就已有 69 个国家 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 系统由以下分系统构成:交换分系统(MSS),基站分系统(BSS),移动台(MS)和操作与维护分系统(OMS)。它包括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。

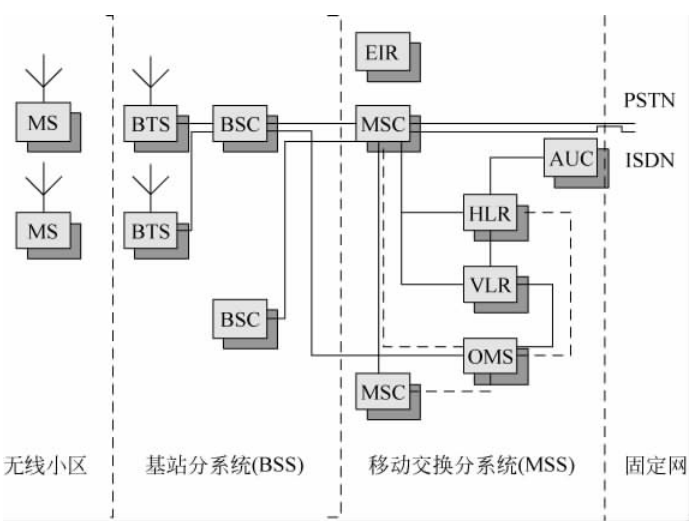

图 3.1 数字移动蜂窝网组成

1) 交换分系统

MSS 包括以下几个组成部分:移动交换中心(MSC),归属位置寄存器(HLR),拜访位置寄存器(VLR),认证(鉴权)中心(AUC),设备标志寄存器(EIR)。

(1) 移动交换中心。

移动交换中心(Mobile Service Switching Center,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(MS)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(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(BSC)。GMSC与固定网相接,固定网有公众电话网PSTN、综合业务数字网ISDN、分组交换公众数据网PSPDN和电路交换公众数据网CSPDN。MSC与固定网互连需要通过一定的适配才能符合对方网络对传输的要求,称其为适配功能(Inter Working Function,IWF)。

(2) 归属位置寄存器。

归属位置寄存器(Home Locate Register,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。

拜访位置寄存器(Visitor Location Register,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(MSRN)。在VLR中建立用户的有关信息,其中包括移动用户识别码(MSI)、移动台漫游号(MSRN)、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。

认证(鉴权)中心(Authentication Center,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。

设备标志寄存器(Equipment Identification Register,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,进而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

BTS 相连接。一个基站分系统只有一个 BSC，而有多套 BTS。它的功能是负责控制和管理，BSC 通过对 BTS 和 MS 的指令来管理无线接口，主要进行无线信道分配、释放以及越区信道的切换管理。

(2) 基站收发信台。

基站收发信台(Base Transceiver Station，BTS)负责无线传输，每个 BTS 有多部收发信机(TRX)，即占用多个频率点，每部 TRX 占用一个频率点，而每个频率点又分成 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。它的作用是将 GSM 系统中话音编辑信号与标准 64kb/s PCM 相配合，例如移动台(MS)发话，它首先进行语音编码，变为 13kb/s 的数字流，信号经 BTS 收信机的接收，其输出仍为 13kb/s 信号，需经 TRAU 后变为 64kb/s 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)将模块制成信用卡的形式。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) 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，应该使管理人员在网络管理中心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 DN 码，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(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(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，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靠近的本地 GSM 移动业务交换中心(GSMC)，GSMC 利用 DN 码访问母局位置登记器即归属位置寄存器(HLR)，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(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 码转换成国际移动台识别码(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

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的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4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(例如警察局或消防中心)。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

在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),数字网(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下的数据。

(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可以有几种方式接入PSPDN。

3) 短消息业务

通过GSM网并设有短消息业务中心(SMS),便可实现短消息业务。

(1) 点对点短消息业务

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的短消息业务(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

这种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 1 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三亿美元。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:接入网采用用户鉴权、无线链路上采用通信信息加密、用户身份(IMSI)采用临时识别码(TKSI)保护、移动设备采用设备识别、SIM 卡用 PIN 码保护等。

1. 临时识别符 TMSI(用户身份保密)

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 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 LAI(位置区识别符)相关联的,当用户所在的 LA(位置区)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时,启动加密模式后,由 VLR 加密后传送用户,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(Authentication Center,AuC),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 5 个鉴权三元组。任何一个鉴权三元组在使用之后,将被破坏,不再重复使用。

当移动台第一次到达一个新的 MSC(Mobile-Service Switching Center,移动业务交换中心)时,MSC 会向移动台发出一个随机号码 RAND,发起一个鉴权认证过程。整个过程如

图 3.2 所示。

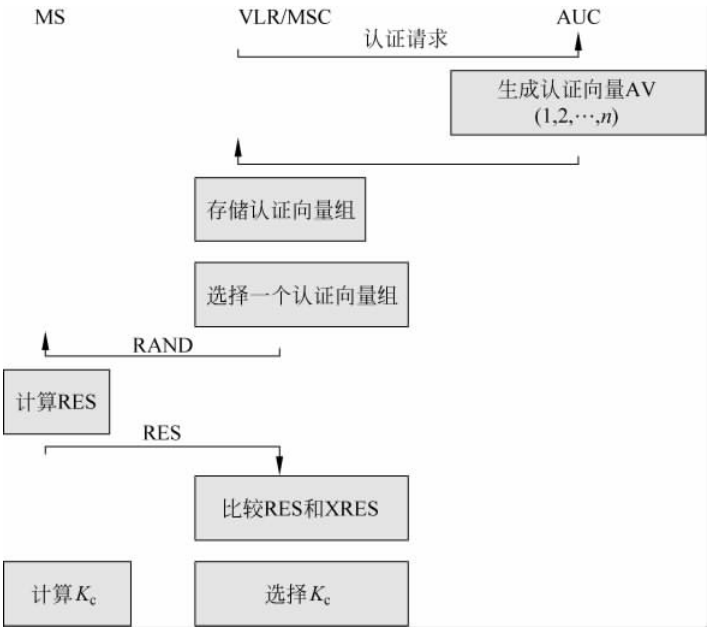

图 3.2 GSM 系统鉴权和认证过程

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。

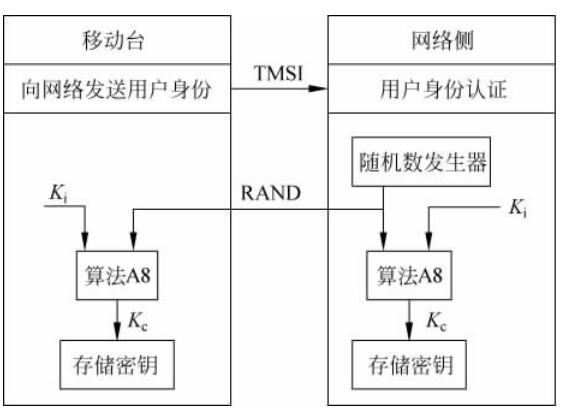

图 3.3 GSM 系统中加密密钥的产生

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 2 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。

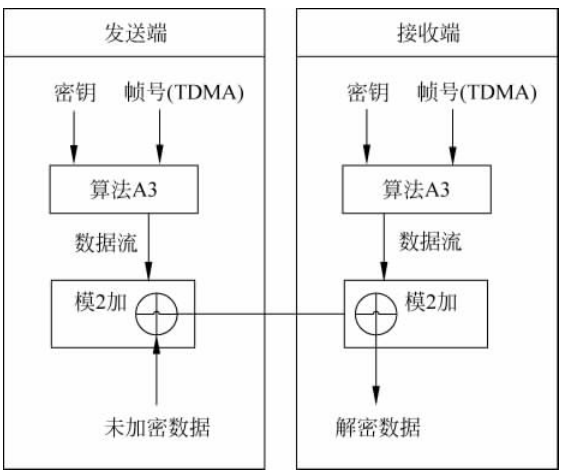

图 3.4　加解密过程

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(国际移动设备识别码),并将其发送给 EIR(设备识别寄存器)。

(2) 收到 IMEI 后,EIR 使用它所定义的如下三个清单。

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。

3.2.3　GSM 系统的安全问题

通过上面的介绍,可以了解到 GSM 尽管采取了一些安全机制,但 GSM 系统中仍然存在一些安全问题,主要包括以下几个方面。

在用户开机注册,或者网络无法从 TMSI 恢复出 IMSI 的时候,比如 VLR/SGSN 的数据丢失,用户将被要求以明文方式发送 IMSI。

GSM 系统中的用户鉴权是单向的,只有网络对用户的认证,而没有用户对网络的认证。非法的设备(如基站)就可能会伪装成合法的网络成员,骗取到用户的重要信息。

GSM 系统只是在接入网中进行了加密,在核心网中没有采取加密等安全措施,因此在核心网络的网元间,信令消息和数据都采用明文传输,容易被窃听;K_c长度只有 64b,比较短,容易被破解;加密算法是不公开的,这些算法的安全性不能得到客观的评价,许多潜在的漏洞不易被及时发现、改进;加密算法固定不变,缺乏算法协商和 K_c协商的过程。

在 GSM 网络中没有考虑对信令、数据进行完整性保护,如果数据在传输的过程中被篡改,将难以发现。

3.3 GPRS安全

通用分组无线业务(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个方面的内容: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,如何正确无误传送用户信息,由移动通信系统的信道控制技术确定,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。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(WAP)等高层应用的互连,灵活部署电信增值服务。GPRS的安全性由如图3.5所示的网络体系结构所确定。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。GPRS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(GGSN)和网关GPRS支持节点(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(Ms)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(BG)主要用于PLMN内不同本地互联网(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。

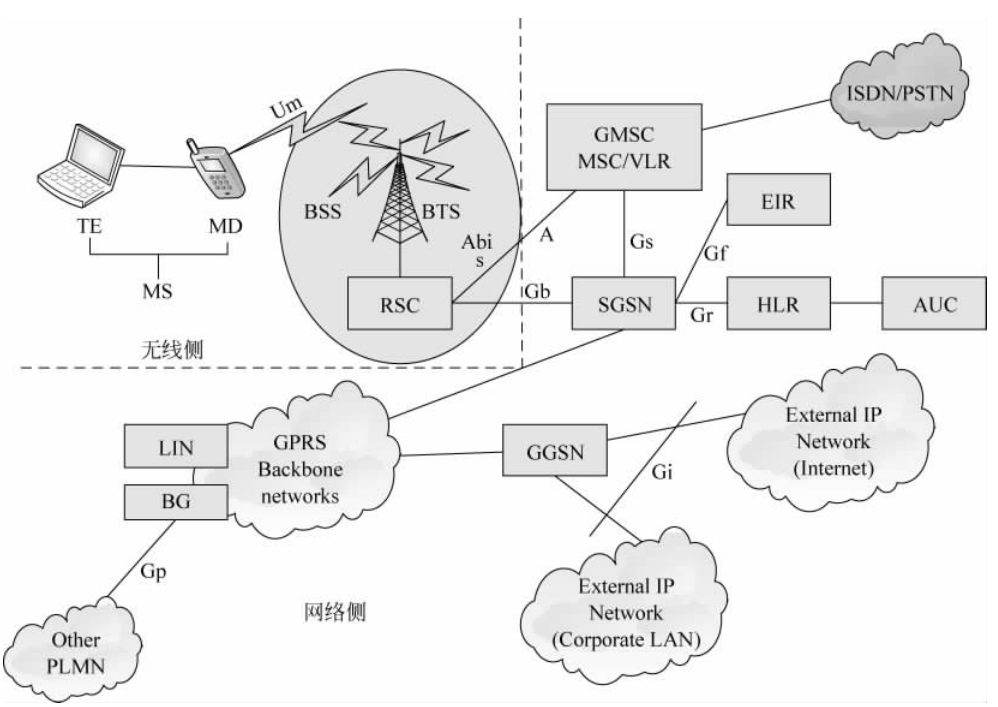

图3.5 GPRS网络体系结构

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 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 网络侵入到 GPRS 系统，进行恶意攻击 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 网络实体根据是否执行 GPRS 传输协议(GTP)可以分成两大类：GTP 节点和 IP 节点。

• GTP 节点

(1) 移动台(MS)在 GPRS 开放网络运营环境下，不可避免地存在使用上的安全隐患。

(2) GGSN 连接到 GPRS 网络的路由器发起的 GGSN 节点攻击。

(3) LIN/计费网关(CG)来自于骨干网内部的拒绝服务攻击或恶意修改计费数据。

• IP 节点

(1) 网络管理站(NMS)从骨干网接入到 GPRS 网络或进行 IP 伪装成 NMS 节点攻击其他网络设备。

(2) 域名服务器(DNS)作为 GPRS 网络用来查询其用户的设备，易受拒绝服务攻击。

1. GPRS 安全策略

GPRS 的安全策略基于以下三个方面的规则，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 3.6 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。鉴权与通信过程中，通过使用临时逻辑链路标志(TLLI)和临时移动台身份标识(TMSI)实现用户真实身份的信息隐藏。

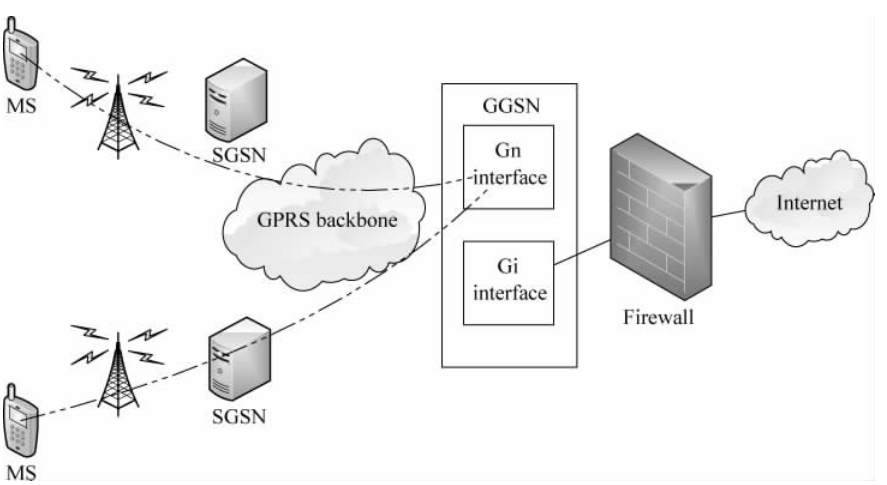

图 3.6　GPRS 网络 MS 之间通信流程

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(GEA)保护,加密范围在MS与SGSN之间,由逻辑链路层(LLC)完成。为正确地传送数据,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PSDN或者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IPSec协议构建VPN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,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3.7展示了采用防火墙技术的GPRS与外部IP网络互连的结构。

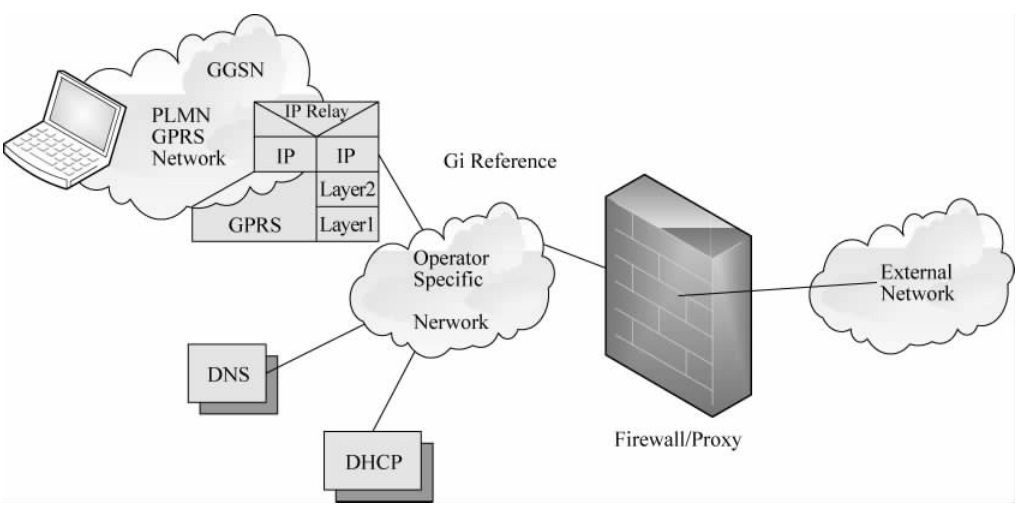

图3.7 GPRS与外部IP通过防火墙相连

(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。预防来自GPRS内部合法用户的安全威胁,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 UMTS 系统的安全

前面讲到，在 GSM 制式中除了话音通过模/数变换、压缩编码后经无线信道以数字信号方式传送以获得一定安全性外，还考虑了多种有效措施，主要有用户鉴权、无线接口通信加密和使用临时标识符(TMSI)等，这增强了用户信息在无线信道上传送的安全性。然而随着技术的进步，攻击者有了更加先进的工具和手段，GSM 在得到广泛使用的同时在安全上的缺陷也渐渐凸现出来。这些缺陷主要有以下几方面。

(1) 单向身份认证。只有网络认证用户，用户不认证网络，无法防止伪造基站和 HLR 的攻击。

(2) 敏感的控制信息没有受到保护。例如，用于无线接口加密的密钥是在没有加密的情况下在不同网络间进行传输的。

(3) 缺乏数据完整性认证等。

针对 2G 系统的种种缺陷，3G 提出了相应的解决对策，在继承 2G 系统基本安全特性的基础上，针对 3G 系统的新特性定义了更加完善的安全特征与安全服务。

UMTS(Universal Mobile Telecommunications System，通用移动通信系统)采用 3G 主流技术，3GPP 所规范的 WCDMA/UMTS 系统包括无线接入网络和核心网络两大部分，在系统安全结构中重点描述了网络接入的安全技术规范。下面将具体介绍 UMTS 以及它的安全机制。

3.4.1 UMTS 系统简介

如图 3.8 所示，图中展示了 UMTS 系统的体系结构模型。按模块划分的概念，整个 UMTS 系统可以分成三个功能实体：用户设备(UE)、无线接入网(UTRAN)以及核心网(CN)。UE 和 UTRAN 之间通过 Uu 接口相连接，UTRAN 和 CN 之间通过 Iu 接口相连接。

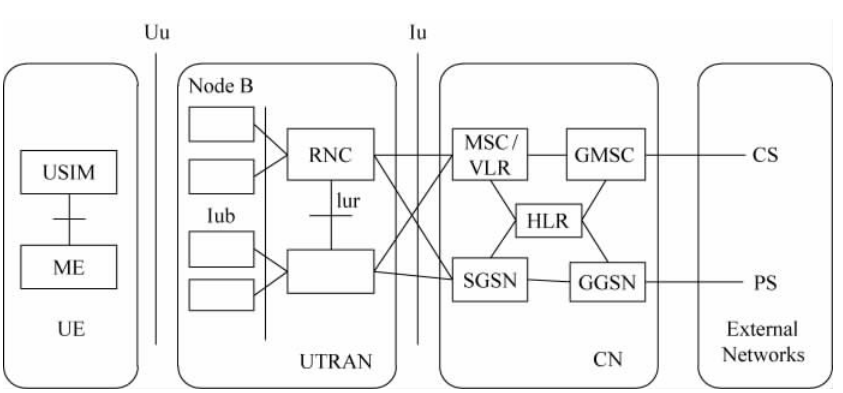

图 3.8 UMTS 系统体系结构

从图中可以看出,UE包括两部分:用户设备(ME)和UMTS用户识别模块(USIM)。ME是进行无线通信的设备,它通过Uu接口与Node B进行通信。USIM是存储用户身份的智能卡,具有用户鉴权功能,并能存储鉴权信息和用户信息。

在第3代移动通信系统中,Uu接口采用WCDMA技术。与FDMA(Frequency Division Multiple Access,频分多址)和TDMA(Time Division Multiple Access,时分多址)相比,WCDMA具有更大的技术优势,这主要体现在以下几个方面。

(1) WCDMA采用直接序列扩频。不同的用户靠不同的扩频码字来区分,这大大提高了系统的容量。当多个用户同时传送扩频信号时,接收端必须能够区分这多个不同的用户。由于每个用户都有一个独一无二的扩频码,而且不同用户的扩频码字间的相关性非常小,当用特定用户的扩频码对接收到的信号进行相关运算时,该用户的频谱得以恢复,而其他用户的频谱进一步被扩展,因此在信号带宽范围内,该用户的信号功率比其他用户的干扰信号功率大得多,从而可以方便地提取出该用户的信号。

(2) WCDMA系统能够克服多径干扰。在无线信道中,由于存在反射和折射现象,发送端和接收端之间存在多条信号传输路径。从不同的路径接收到的信号实质上是同一传输信号的变形,它们只是在幅度、相位、时延以及到达角度上存在着差异。这些信号合并后的波形与频谱不同于原来信号的波形与频谱,因此接收端不易正确接收。但扩频技术能够消除这种多径干扰的影响。

(3) WCDMA系统具有良好的保密功能。只有接收端截获了用户的扩频码之后才能对信号进行解扩处理以获得用户信息。并且由于扩展频谱信号具有较低的功率谱密度,这使得敌方很难截获,截取概率低。

此外,当扩频码字和一个窄带干扰信号进行相关运算后,窄带干扰信号功率谱被扩展,从而降低了干扰信号的功率,这使得WCDMA系统具有较强的抗干扰能力。

UTRAN也由两部分构成:Node B和无线网络控制器(RNC)。Node B和RNC之间通过Iub接口相连,RNC和RNC之间通过Iur接口相连。Node B主要用于在Iub接口和Uu接口之间传送数据流,同时也对无线资源进行管理。RNC主要负责管理、控制无线资源,同时它也是UTRAN向CN提交业务的接入点。第3代移动通信系统的一个基本概念就是将移动通信系统中的无线接入网络的功能同核心网络的功能分开。无线接入网向移动终端提供了一个接入平台,该平台使得移动终端能够接入核心网络并且能够利用移动核心网络所提供的业务。

第3代移动通信系统中大部分业务是话音业务和接入互联网的业务。虽然第2代移动通信系统也提供这些业务。但第3代移动通信系统能在更复杂的环境里提供这些业务,且业务的服务质量(QoS)更好。此外,为了在UMTS和IMT-2000这样的基于W-CDMA的移动通信网络中提供移动性和软越区切换功能,网络需要能快速建立和拆除连接。这就要求建立一个面向连接的有严格QoS控制能力的接入网。目前,最适合这一要求的技术是AAL2。AAL2既能满足所承载业务的服务质量要求,又能获得高效的资源利用率。

CN主要包括以下模块:归属位置寄存器(HLR)、移动交换中心/访问位置寄存器(MSC/VLR)、网关MSC(GMSC)、服务通用分组无线业务支持节点(SGSN)、网关GPRS支持节点(GGSN)。

HLR是存储移动用户信息的数据库,每个移动用户必须在某个HLR中登记注册。

HLR 存储的用户信息有两类，一类是有关用户参数的信息，一类是有关用户当前位置的信息。MSC/VLR 是在电路交换系统中为 UE 提供服务的交换设备和数据库。MSC 对位于其服务区内的移动台进行交换和控制，同时提供移动网与固定公共电信网互联的接口。VLR 是存储用户位置信息的动态数据库。当漫游用户进入某个 MSC 区域时，必须在与该 MSC 相关的 VLR 上建立相应的用户信息。UMTS PLMN 通过 GMSC 与外部的电路交换网相连。SGSN 的功能和 MSC/VLR 基本相同，但它适用于分组交换(PS)业务。GGSN 的功能和 GMSC 基本相同，同样它也适用于分组交换(PS)业务。

核心网分为两类。一类核心网基于 GSM 系统，它可以和 ISDN、PSDN 等网络互通；另一类核心网基于通用分组无线系统(GPRS)，它可以提供分组交换业务，能接入到 Internet 或其他的 IP 网络。

和第 2 代移动通信系统相比，UMTS 系统不但在结构和性能上有了很大的改进，更重要的是它能够提供更多的业务类型，给人们的日常生活带来更大的便利。

UMTS 系统能够提供不同服务质量(QoS)等级的业务。根据业务对时延敏感程度的不同，UMTS 系统将所支持的业务分为 4 个等级：会话型业务、流业务、交互型业务、后台型业务。在这 4 种业务等级中，会话型业务对时延最敏感，而后台型业务对时延的要求最低。

1. 会话型业务

会话型业务属于实时应用业务，它对业务时延很敏感，要求端到端时延小。在会话型业务中，会话的双方是对称的实体。会话型业务最典型的应用是电路交换的话音业务。此外，一些接入 Internet 的业务和多媒体业务，如用 IP 承载的话音业务以及可视电话业务也属于会话型业务。

在 UMTS 系统中，话音业务通常采用自适应多速率(AMR)技术进行压缩编码。AMR 编码器能够提供 12.2kb/s、10.2kb/s、7.95kb/s、7.40kb/s、6.70kb/s、5.90kb/s、5.15kb/s 和 4.75kb/s 8 种源编码速率。但究竟采用哪种源速率进行编码则由无线接入网决定。AMR 编码器提供的某些编码速率和现有的一些蜂窝系统相同，如 GSM EFR 编码器采用的 12.2kb/s 的速率、US-TDMA 编码器采用的 7.4kb/s 的速率和日本的 PDC 编码器采用的 6.7kb/s 的速率。AMR 编码器还可以进行速率转换。无线接入网能根据空中接口的负荷情况和话音连接的质量来控制 AMR 编码的速率。在负荷较重时，采用较低的编码速率能够扩大系统容量，但这将造成话音质量下降。当移动台处于小区边缘时，它的发射功率最大，此时采用较低的编码速率可以扩大小区的覆盖范围。总之，采用 AMR 编码方式能在一定程度上调节网络容量、小区覆盖范围和话音质量，以获得令人满意的效果。UMTS 系统提供的可视电话业务同话音业务一样对时延非常敏感，由于采用了图像压缩技术，此种业务要求具有很低的比特错误概率和比特丢弃概率。

2. 流业务

多媒体数据流作为一种传输数据的技术，可以将数据以稳定、连续的数据流形式进行传输。这种技术被越来越广泛地应用在 Internet 上。当用户下载大容量的多媒体文件时，由于数据传输速率的限制，将整个文件下载完再浏览需要等较长时间。采用流业务技术无须将整个文件下载完，而是在下载文件数据的同时即可通过用户的浏览器或插件显示数据。接收数据的用户端必须能够及时处理下载下来的数据，将其转换成声音或图像。流业务是不对称的，它对时延的敏感程度比会话型业务低得多。

3. 交互型业务

当终端用户(一个人或一台机器)要求从远端设备上获取数据时,就需要按照交互型业务方式进行通信。例如,人作为终端用户时,可以上网浏览网页,检索远端数据库中的信息;机器作为终端用户时,可以轮询测量报告,自动查询数据库。

交互型业务是一种典型的数据通信业务,它的一个特征是终端用户采用"要求-应答"的模式进行通信。消息传输往返时延是交互型业务的一个重要的参数。交互型业务的另一个特征是分组数据必须以透明的方式进行传输。基于位置的服务是一种典型的交互型业务。例如,在基于位置的服务中,可以通过终端查询相关位置信息。在终端上输入一定的信息,就可以找到最近的加油站、医院或学校;外出旅游时,可以事先查询该地的名胜古迹。提供基于位置的服务的终端可以根据需要显示一幅地图,地图上有文字标识。单击地图上的标识,终端就会显示出相关的信息。在不远的将来,基于位置的服务将成为 UMTS 系统的一项主要业务。联网游戏也属于交互型业务,但当网络游戏时延要求较高时,它属于会话型业务。

4. 后台型业务

后台型业务对时延的要求最低,接收消息的实体并不要求消息在很短的时间内到达,它的时延可能是几秒、几十秒甚至几分钟。典型应用包括:电子邮件(E-mail)、短消息业务(SMS)、下载数据、接收测量报告。目前,一种新兴的后台型业务——电子贺卡正悄然兴起,随着终端采用内置式照相机及大型彩显的小型化,电子贺卡业务的应用将日益广泛。

3.4.2 UMTS 安全分析

从某种意义上来讲,通用移动通信系统(UMTS)是全球移动通信系统(GSM)的改进方案。GSM 中的基本接入安全机制正是 UMTS 接入安全的基础。当然,安全体系结构的设计目标并不局限于 GSM 中已有的安全解决方案。

UMTS 的安全机制主要原则如下。

(1) UMTS 的安全体系将基于第 2 代系统(2G)的安全体系,即仍将保留现有的 GSM 系统的安全特性。

(2) UMTS 的安全体系将针对 2G 系统中已发现的安全漏洞做出改进,其中包含交互式认证机制和基于 128b 密钥的强加密机制。

(3) UMTS 安全体系将提供新的安全性能。UMTS 必须保障 3G 环境下的新业务,包括多运营商、多服务提供商交互工作环境下提供的新业务。

此外,研究人员通过对 3G 系统面临的威胁进行分析,定义了对 3G 系统的安全要求。这将用作定义安全体系中所需的安全特性的基础,并基于这些安全特性定义了一套安全机制。

研究人员在 3G 的技术规范 TS 33.102 中定义了 UMTS 接入安全的安全体系结构。其主要目标可概括为:①对用户模块(UE)进行认证,特别是用户服务标识模块(USIM),其中包括确认 UE 是否已接入一个有效的网络;②向 UE 和服务网络 SN 提供会话密钥;③在会话密钥的保护下在 UE 和 SN 之间建立连接。

当然,安全结构体系还包括其他方面,但是认证、密钥生成以及接入链路的加密和完整性保护是其主要部分。以下将对该体系结构进行更加详细的介绍,我们以认证的基础,即实

体认证作为开始。

1. 认证的实体

进行实体认证的前提条件是该实体已预先定义好一个独一无二的身份标识。在移动网络中，主要的用户身份标识是国际移动用户身份标识号(IMSI)，如图 3.9 所示。但 IMSI 并不是用户的电话号码(即所谓的 MSISDN 号)。MSISDN 号是包含完整国家代码的电话号码，并同运营商数据库中的 IMSI 号相对应。MSISDN 号基本上是公共信息，但 IMSI 号是用作系统内部标识和路由之用的，通常是非公开的。

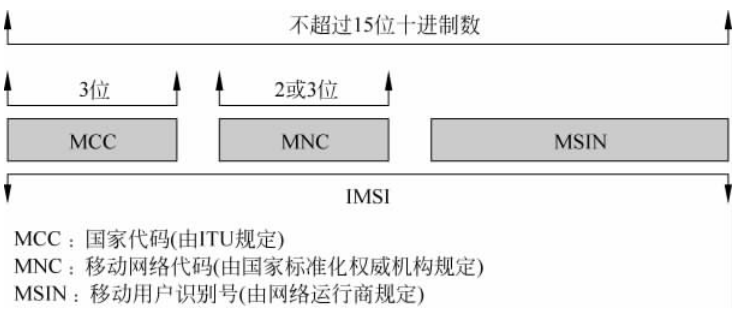

图 3.9　IMSI 的结构

认证程序将产生加密中使用的会话密钥。在某些情况下，永久标识 IMSI 可在网络的空中接口处被截取，这使得攻击者可对用户位置进行跟踪。为解决这个问题，SN 可以发布一个本地暂时身份标识符 TMSI(4B，十六进制编码)，用来进行身份认证。因此，正规的程序是当 UE 首次进入一个新服务区时(如服务 GPRS 支持节点(SGSN)或访问位置寄存器(VLR))，将向基站发送自己的 IMSI 号。随着加密技术的出现，SN 将给 UE 发布一个 TMSI 号。TMSI 号是以加密的形式公布，因此难以对一个特定的用户进行跟踪，因为在 IMSI 和 TMSI 之间没有明显的联系。通过使用 TMSI，提供了一种对用户身份和位置进行保密的方法。

除了用 IMSI 对 UISM 进行标识以外，对移动台(MS)也有一个标识号，称之为国际移动台设备标识号(IMEI)，这也是一个独一无二的标识号。IMEI 将由设备标识寄存器(EIR)的数据库进行周期性的核查。用户可以通过采取合法的措施，将被盗用的手机登记入 EIR 的“黑名单”中，运营商将随后停止对该手机提供服务。

2. 实体认证和会话密钥的产生

在连接建立阶段，UE 将通过 IMSI 或 TMSI 来标识自己的身份，而该公布的标识号将通过网络执行的认证程序对其进行认证。UMTS 的安全体系结构是基于一个交互式程序，该程序是在用户端(USIM)和网络端的 SGSN 和 VLR 之间执行。该程序称为 UMTS 认证和密钥协商(AKA)协议，因为除了提供认证服务以外，该程序还包含会议密钥的生成和在用户端提供机密性和数据的完整性保护。

AKA 程序的执行包含两个步骤，如图 3.10 所示。第一步包含安全证书(认证矢量，AV)的传递，即从归属网络(HE)到服务网络(SN)。HE 主要由本地用户数据库 HLR 和认证中心 AuC 组成；SN 则由核心网络中直接参与连接建立的部分组成。就运营商而言一般都包含 HE 和 SN 节点。

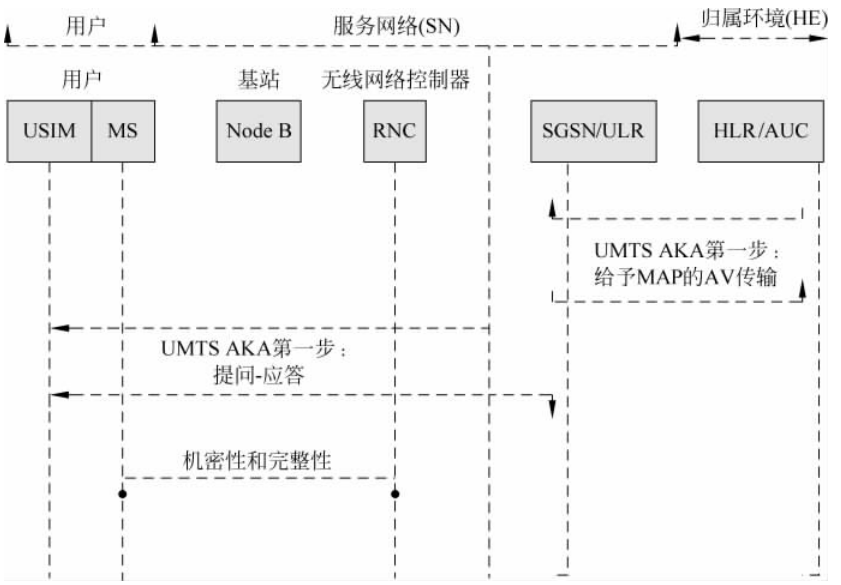

图 3.10　简化的 UMTS 结构体系和基本的接入安全体系

认证矢量中包含类似提问-应答认证数据和加密密钥等敏感数据。因此,在 HLR/AuC 和 SGSN/VLR 之间传送认证矢量需要采取安全措施以防止窃听和篡改(例如,传输的机密性和完整性都必须加以保护)。

AKA 协议的第二个步骤是 SGSN/VLR 执行单向提问-应答程序,用以实现在 UMTS 和网络(SN,HE)之间完成交互式实体认证。须注意的一点是在两步的 AKA 协议中,HE 具有为 SN 提供安全性保护的责任。因此,在 HE 和 SN 之间必须建立一种相互信任的关系。在 GSM 中,这种信任关系通过漫游协议得以建立,在 UMTS 中也应该采用同样的模式。

在 AKA 程序中应用的加密函数,只在 USIM 和 AuC 中专用。3GPP 采用了 MILENAGE 算法以实现 AKA 功能。虽然标准 MILENAGE 算法只是作为算法集中的一个例子,但实际上它是为实现 AKA 功能而建议采用的算法集。算法是基于对称分组密码体制 Rijndael 之上的。表 3.1 中描述了 UMTS 中采用的加密函数及其应用。

表 3.1　UMTS 安全算法

算法	用　途	O：运营商规定的 S：完全标准化的	位　置
f_0	随机数生产函数	O-(MILENAGE)	AuC
f_1	网络认证函数	O-(MILENAGE)	USIM 和 AuC
f_{1*}	消息重同步函数	O-(MILENAGE)	—
f_2	用户随机数认证函数	O-(MILENAGE)	—
f_3	密钥生产函数	O-(MILENAGE)	—
f_4	完整性密钥生产函数	O-(MILENAGE)	—
f_5	用于普通操作的匿名密钥生成函数	O-(MILENAGE)	—
f_{5*}	用于重同步的匿名密钥生成函数	O-(MILENAGE)	—

续表

算法	用　途	O：运营商规定的 S：完全标准化的	位　置
f_6	MAP 加密算法	S	MAP 节点
f_7	MAP 完整性算法	S	—
f_8	UMTS 加密算法	S-(KASUMI)	MS 和 RNC
f_9	UMTS 完整性算法	S-(KASUMI)	—

交互式认证使得 USIM 成为一个活跃的实体。在 GSM 中用户不能对网络进行认证；因此，UE 不能拒绝网络。在 UMTS 中，UMTS 将会尝试对网络进行认证。因此，USIM 可能拒绝进入网络。

3. 接入链路的保护

安全保护是通过加密实现的，这些加密密钥是由 AKA 程序产生的。密钥 CK 通常具有 128b，但可通过配置密钥生成函数 f_3 来控制密钥中重要比特的长度。由 MILENAGE f_3 算法所生成的默认值是长度为 128b 的机密密钥。

在 GSM 系统中，机密性保护通常是在基站实现的。这符合最初的设计目标，即在无线接口上防止窃听。然而现已发现在基站和控制器之间的大量连接是基于无安全保障的无线链路的，因此，对 UMTS 而言，有必要扩大对链路进行安全加密的范围。

数据完整性的安全保护服务是通过消息认证码(MAC)机制来实现的，该机制为防止恶意篡改提供了消息认证和数据完整性保护功能。完整性密钥通常具有 128b，但同 CK 类似，在需要的情况下 IK 也可以通过配置而具有较少的重要字节。默认的函数 MILENAGE f_4 生成一个具有 128b 的 IK。UMTS 中的完整性保护和机密性保护一样，具有相同的物理覆盖范围(例如，完整性保护是应用在 MS 和 RNC 之间)。但 UMTS 中的机密性保护包含用户相关的系统信令和用户数据，而完整性保护则只包含系统信令。

4. 交互式实体认证和密钥协商协议

在 SGSN/VLR 和 USIM 之间执行的认证过程是一种交互的认证策略。该策略使用一个长期共享的 128b 的密钥(K)，而这个密钥只储存在 UICC/USIM 和 HE 的 AuC 中。UICC 是能够防止篡改的具有身份验证功能模块的智能卡，而 USIM 是运行在 UICC 上的一个模块。为了保证认证的安全性，一个基本要求即是在给定的 UICC/USIM 的使用期内 K 绝不能泄漏或者损坏。

AKA 序列通常是当网络需要对用户身份进行验证时由 VLR/SGSN 初始生成的。如果当网络中出现某用户而 VLR/SGSN 并没有为其生成有效的认证矢量 AV 时，该用户必须从 HLR/AuC 处申请至少一个 AV。AV 是通过运营商规定的认证函数($f_0 \sim f_{5^*}$)生成并存储在 HE 中的 AuC 节点处的。

这里需提及函数 f_0，该函数用以产生随机数，而且这个函数是唯一在 AuC 处使用的函数。下面的定义说明 f_0 的输出只依赖于内部状态。

$$f_0: f(\text{internal} - \text{state}) \rightarrow \text{RAND}$$

在 UICC/UISM 的使用期内函数 f_0 的输出值是不能重复的，因为攻击者可通过对函数的输出值进行在线监听，对随机数中出现的某个特殊值所对应的内容进行猜测。

SGSN/VLR 通过发送包含随机数 RAND 和认证令牌 AUTH 的轮询消息对本地 AKA

程序进行初始化。网络端的认证是基于随机数的认证(函数 f_1),由此可见,只有知道密钥 K 的实体才能生成可接受的随机数。整个认证过程有两个显著的特点:首先,轮询过程采用令牌环方式,每次轮询只有一个节点通过认证;其次,认证过程扩展了轮询响应的机制,用 MAC 提供交互式的认证过程。

选择单向 AKA 方案经证明对 AKA 的性能有重要的影响,因为在连接建立阶段对时间是严格限定的。以下简单讨论基于 MAC 的 AKA 机制。基于 MAC 解决方案有十分优越的计算性能,这种性能对于在 UICC/USIM 上运行的函数 f_1 和 f_2 是必须具备的。假定认证算法必须在实时约束的条件下执行,故 3GPP 安全工作组(SA3)决定采用基于 MAC 函数的常规方法。而 MAC 函数已经在 GSM/GPRS 系统中得以应用,这无疑也对此决定造成了较大的影响。

在接收到随机数后,USIM 将对网络中的实体进行认证。这是通过利用接收到的 RAND,AUTH 执行函数 f_1 来完成的。USIM 将把计算得到的 XMAC-A 同接收到的 MAC-A 进行比较。如果 XMAC-A 同包含在 AUTH 中的 MAC-A 参数相等,则通过认证。

$$f_1: f(\mathrm{RAND}, \mathrm{SQN}, \mathrm{AMF}) \rightarrow \mathrm{MAC-A}(\text{or } \mathrm{XMAC-A})$$

随后 USIM 必须验证序列号 SQN 是否在有效的范围内,这将通过一种窗口机制来完成。在通过验证后,窗口的大小将根据可接收的随机数的范围进行调整,而 USIM 必须产生一个应答数(RES)用以回发给网络。

$$f_2: f(\mathrm{RAND}) \rightarrow \mathrm{RES}(\text{or } \mathrm{XRES})$$

随后,SGSN/VLR 将对接收到的 RES 值进行验证,以确认其是否和 AV 中的 XRES 值完全相同。

$$f_3: f(\mathrm{RAND}) \rightarrow \mathrm{CK}$$

$$f_4: f(\mathrm{RAND}) \rightarrow \mathrm{CK}$$

AKA 程序也通过函数 f_5 生成的一个匿名密钥 AK 来隐藏存储在 SQN 值中的序列的值。隐藏的使用使得位置跟踪更加困难,而隐藏的具体实现是通过将 AK 和 SQN 做异或运算完成的。需要注意的是,函数 f_5 必须在函数 f_1 之前运行用以生成 SQN 参数。

$$f_5: f(\mathrm{RAND}) \rightarrow \mathrm{CK}$$

5. MILENAGE 算法集

加密函数 $f_0 \sim f_5^*$ 在原则上是由运营商定义的,而且这些函数没有必要在漫游的用户之间存在任何的协同工作的能力。这些函数都只专用于由 HE 控制的 USIM 和 AuC 中。虽然如此,研究人员还是决定设计一个对销售商和运营商都同样适用的标准函数集。这样做的目的在于保证 UMTS 系统有一个有效而固定的函数集,使得不会因此而延缓对 UMTS 的使用或由于认证函数中存在的漏洞而降低其安全性。

这个标准算法集是欧洲电信标准化组织安全算法专家组(ETSI SAGE)在 SA3 工作组的委任下设计的。该算法集建立在一个普通分组密码的核心之上,而其构架的设计应该具有一定的兼容性,以便运营商可根据其需要更换加密算法的核心部分。该设计的成果即是 MILENAGE 结构框架,它同其他任何以 128 位密钥控制且以 128b 为分组单位的分组密码都可协同工作。

这种 MILENAGE 结构框架并不包含伪随机数生成函数 f_0,并且该加密算法的核心是建立在 Rijndael 分组密码算法基础上的。选择 Rijndael 作为 MILENAGE 的算法基础是在

Rijndael 成为高级加密标准 AES 算法之前。ETSI SAGE 选择 Rijndael 的主要目的在于：该算法在具有有限计算能力的平台上表现出良好的性能特性；在 AES 的评选阶段对 Rijndael 做了综合的评估；该算法没有知识产权。其中性能特性十分重要，因为认证函数必须在智能卡上运行而智能卡的资源是有限的。

从上述可以看出，UMTS 中的接入安全结构体系明显优于 2G 的 GSM 系统。在 UMTS 中，通过采用交互式认证机制完全解决了 GSM 中存在的伪基站问题。并且 MILENAGE 中的认证算法集大大优于现在使用于 GSM 中的算法集。

另外，UMTS 中的完整性函数对于 GSM 而言是全新的内容。完整性保障机制是独立于机密性保护的，所以可以不允许加密或在加密无效的环境中提供保护机制。完整性机制对于防止主动攻击也同样非常重要，但在完整性保护机制中一个被忽略的因素是没有对用户数据进行保护，这也是主要需要改进完善的部分。

3.5 第 3 代移动通信系统安全

GSM 和窄带 CDMA 技术是目前第 2 代数字移动通信技术的主体技术，与前两代系统相比，第 3 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 3 代移动通信的设计目标是为了提供比第 2 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 2 代系统的良好的兼容性。与第 1 代模拟蜂窝移动通信相比，第 2 代移动通信系统具有保密性强、频谱利用率高、能提供丰富的业务、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，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。

3.5.1 第 3 代移动通信系统简介

第 3 代移动通信 IMT-2000(国际移动通信-2000)，即该系统工作在 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语音业务为主，随着发展一般也仅能提供 100～200kb/s 的数据业务，GSM 演进到最高阶段的速率能力为 384kb/s，而第 3 代移动通信的业务能力将比第 2 代有明显的改进。它应能支持话音分组数据及多媒体业务；应能根据需要，提供所需带宽。ITU 规定的第 3 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。

第 3 代移动通信(IMT-2000)分为 CDMA 和 TDMA 两大类共 5 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 W-CDMA，它是在一个宽达 5MHz 的频带内直接对信

号进行扩频。W-CDMA分为FDD和TDD方式两种,在FDD方式下,W-CDMA的码片速率为4.096Mchip/s,能与GSM同时使用一个时钟,实现W-CDMA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。W-CDMA的每个载波能放入5MHz的频谱带宽。如果有15MHz的频带,则可支持三个载波。为保证与其他载波间有至少200kHz以上的间隔,15MHz内的三个载波间隔可在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(BPSK)调制,是W-CDMA的重要特征之一。一路做余弦信号调制,相当于四相相移键控(QPSK)调制的I路,是专用的物理数据信道(DPDCH),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(DPCCH)传送公共控制命令。W-CDMA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。W-CDMA的基站之间不需要同步,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、在什么位置启动软切换算法。一个W-CDMA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,即使彼此功率有好几分贝之差也行。这正好弥补了在TDD方式中信号功率不易高精密控制的不足。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,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加上保护频间间隔为1.7MHz,三个基本信道合用,为3.75MHz,加上保护频间间隔,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,在系统协议的第二层增添了媒体控制层(MAC),W-CDMA与此相似,为支持MAC的运行,在物理层增加了专用控制信道(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。CDMA 2000的重要技术特征之一是下行链路使用多载波方式,实现5MHz带宽通信。下行链路采用多载波,被1.2288Mchip/s的扩频码调制,每个载波彼此间隔1.25MHz,三个载波加上保护频隙,构成5MHz。上行采用直接扩频方式,使用3.75Mchip/s的扩频码调制到载波上,正好为三个1.25MHz频宽。加上保护频隙构成5MHz带宽。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，这样能在低信噪比下工作，降低了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。

第 3 代移动通信关键技术如下。

1. 高效信道编译码技术

第 3 代移动通信的另外一项核心技术是信道编译码技术。在第 3 代移动通信系统主要提案中(包括 WCDMA 和 CDMA 2000 等)，除采用与 IS-95CDMA 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(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，由于复杂的地形、建筑物结构对电波传播的影响，大量用户间的相互影响，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地解决这个问题。

智能天线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，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，从而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的不同扩频码的非相干接收，确定扰码组号等，最后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，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系统中的最为重要的核心技术之一。

3.5.2 第3代移动通信系统安全分析

3G系统建立在第2代移动通信(2G)系统基础之上,对于2G系统中必不可少的和行之有效的安全方法在3G系统中将继续被采纳,而对于2G系统中存在的安全缺陷,在3G系统中将会被抛弃或改进。3G系统呈现出的新特性,要求我们提供更加完善的安全服务和安全特征,此外,3G系统的安全体系也呈现出了新的特点。

3G移动通信系统的安全网络图如图3.11所示。

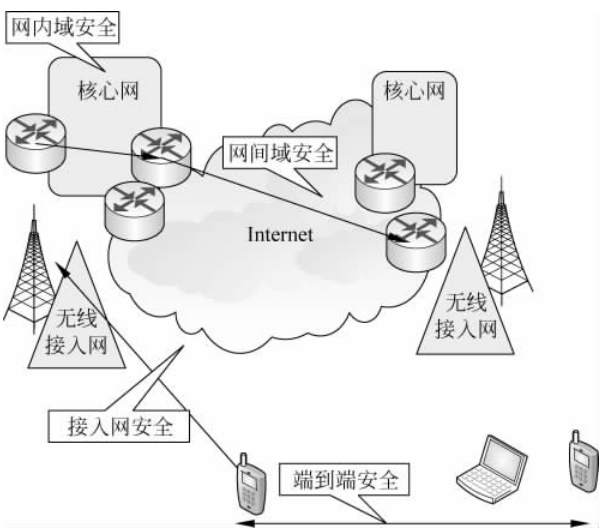

图3.11 3G移动通信安全网络

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(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;对于可能会出现的主动攻击,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会超过话音业务,系统需具备更高的安全性;终端可能会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。

1. 3G系统安全体系结构

3G系统安全体系结构如图3.12所示。该结构中共定义了三个不同层面上的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。

三个层面由高到低分别是:应用层、归属层/服务层和传输层。5组安全特性所包含的

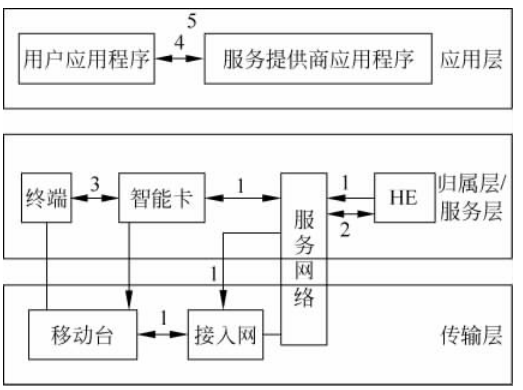

图 3.12　3G 安全体制结构图

具体内容如下。

1）网络接入安全

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、用户身份机密性、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：①用户认证，服务网验证用户的身份；②网络认证，用户验证自己被连接到了一个由自己的 HE 授权并为他提供服务的服务网，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：一种是使用由用户的 HE 传递给 SN 的认证向量进行认证的机制；另一种是使用在用户和 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

用户识别机密性有关的安全特征有：用户身份机密性，业务传递到用户的永久用户识别(INSI)不能在无线接入链路上被窃听；用户位置机密性，用户在某个特定区域内出现或到达不能在无线接入链路上被窃听被获取；用户的不可追溯性，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被识别，这就要求在无线接入链路上对任何可能暴露用户的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得到实现。

(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。IMEI 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。

在认证和密钥协商机制的执行过程中完整性密钥协商得以实现。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得以实现。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)：生成的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)：分配会话密钥给网络中的节点。

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，网络实体之间的交换信息是不受保护的，网络实体之间主要是通过有线网络互联。依据 3G 系统的安全特性和安全要求，应该对现有的有线网络的安全进行增强，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现同属一个安全域，不同的运营商之间的网络设置安全网关(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 处理所有进/出安全域朝向明确的一组可到达的 IP 安全域的业务。一个安全域内的 SEG 的数目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，在此网络域的安全中，IP网络层的安全是最非常重要的一个方面。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和机密性以及对抗重放攻击。

3）用户域安全

用户域安全定义了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：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能够限制于一个授权的用户或一些授权的用户。为了实现该特征，用户和USIM必须共享一安全地存储在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：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和终端必须共享一安全地存储在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

应用域安全定义了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：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，那些应用驻留在USIM上（类似于GSM中的SIM应用工具包）。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定义了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，但对某些事件以及根据用户所关心的问题，应该提供更多安全特征的用户可视性。这产生了一些特征，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系统安全功能结构如图3.13所示。

图中竖条表示3GPP安全结构中包括的网络单元。

（1）在用户域中：USIM（用户服务识别模块），HE（向用户发放的接入模块），UE（用户设备）。

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

（3）在归属环境（HE）中：HLR/AuC（归属位置寄存器/认证中心）。

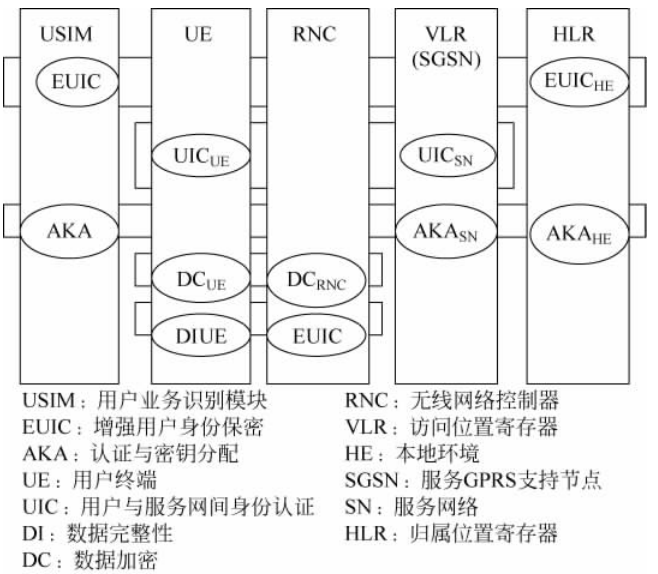

图 3.13　3G 系统的安全功能结构图

水平线表示安全机制,安全措施分为以下 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 的安全问题

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。主要方式有以下几种。

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。

窃听：攻击者未经允许非法窃听通信链路用以获取信息。

业务分析：攻击者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。

泄漏：攻击者以合法身份接入进程用以获取敏感信息。

浏览：攻击者搜索敏感信息所处的存储位置。

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,包括以下几个。

资源耗尽:服务网络或用户利用特权非法获取未授权信息。

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。

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。

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。

拒绝:网络或用户拒绝做出响应。

(5) 否认,网络或用户对曾经发生的动作表示否认。

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以下几种。

(1) 非法获取数据。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。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。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。用户否认业务费用、数据来源或接收到的其他用户的数据。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。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以下几种。

(1) 非法获取非授权数据。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。入侵者可以修改、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。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。攻击者伪装其他合法用户身份,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。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有以下几种。

(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以破坏终端数据的完整性。

(5) 通过修改、插入或删除 USIM 卡中的数据以破坏 USIM 卡数据的完整性。

3.6 第4代移动通信系统安全

第4代移动通信技术(简称4G),是第3代移动通信系统的延伸,是一种设想用来替代3G蜂窝的无线蜂窝系统,其在业务、功能、频带上都不同于第3代系统。

2008年11月宏达国际电子与俄罗斯 WiMax 移动通信电运营商 Scartel 共同发表了全国第一支 GSM/WiMAX 集成式双模手机 HTC Max 4G。截至2010年2月,共有24个国家的51家移动通信公司表示会提供4G服务。2013年12月18日,中国移动在广州宣布,将建成全球最大4G网络。截至2015年12月月底,全国电话用户总数达到15.37亿户,其中移动电话用户总数13.06亿户,4G用户总数达到近四亿户。

4G通信技术具备向下相容、全球漫游、网络互联、多元终端应用等特性,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。

3.6.1 第4代移动通信系统简介

4G可称为宽带接入和分布网络,具有非对称且超过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4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、高质量。对于大范围高速移动用户(250km/h),数据传输速率为2Mb/s;对于中速移动用户(60km/h),数据传输速率为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,这些技术能大幅度提高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，将 OFDM 和 FDMA 技术结合，在利用 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来实现多址。它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。其又分为子信道 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 3.14 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。

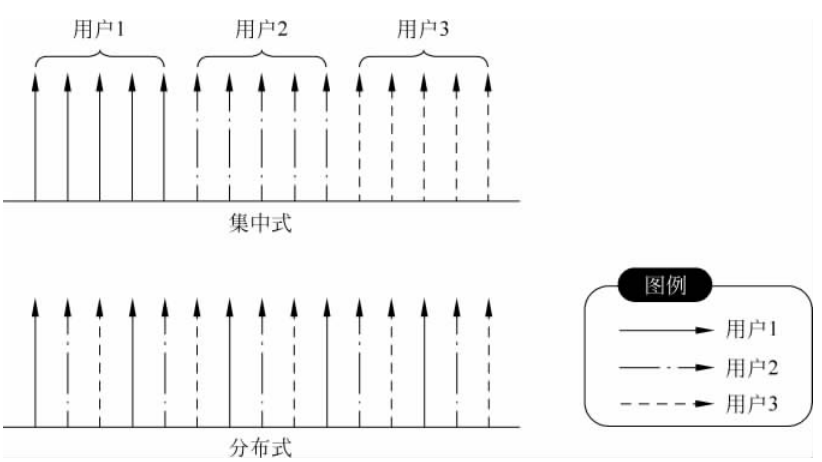

图 3.14　子信道 OFDMA 的组合模式

(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3.15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,适用于负载不是很重的系统中。

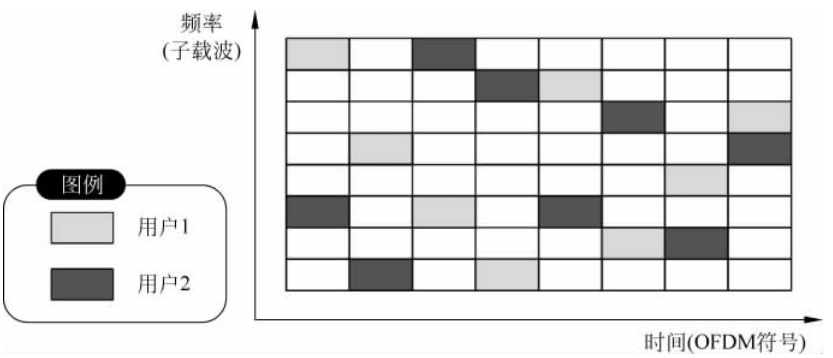

图3.15 跳频OFDMA的组合模式

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。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以实现通信功能。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)指同时在发射端和接收端使用多个天线的通信系统,在不增加带宽的情况下可以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。

3.6.2 第4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(AS)安全和非接入层(NAS)安全,使得无线空口和核心网络安全相互独立,从而提高整个系统的安全性。

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。除了局域网之外，一般网络都是处于开放的模式，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）容量限制。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，防护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，高端的加密技术如生物识别技术、量子密码技术以及椭圆曲线密码技术等可以融入到 4G 网络通信加密技术中来，加强 4G 网络自身的抗攻击能力，从而保证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，不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。

3.7 第5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,频谱效率提升5～10倍,能够在500km/h的速度下保证用户体验。5G将使信息通信突破时空限制,给用户带来极佳的交互体验:极大缩短人与物之间的距离,并快速地实现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。预计到2020年,各种物联网应用将得到广泛应用,智能电网、智慧城市、移动医疗、车载娱乐、运动健身等这类服务将广泛运用到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。

3.7.1 第5代移动通信系统简介

目前,5G技术仍处于研究阶段,主要发展趋势包含8个方面。

1. 超密集异构网络

在未来5G网络中,减小小区半径,增加低功率节点数量,是保证未来5G网络支持1000倍流量增长的核心技术。未来无线网络将部署超过现有站点10倍以上的各种无线节点,在基站覆盖区内,站点间距离将保持在10m以内,并且支持在每平方千米范围内为25 000个用户提供服务。同时也可能出现活跃用户数和站点数的比例达到1∶1的现象,即用户与服务节点一一对应。密集部署的网络拉近了终端与节点间的距离,使得网络的功率和频谱效率大幅度提高,同时也扩大了网络覆盖范围,扩展了系统容量,并且增强了业务在不同接入技术和各覆盖层次间的灵活性。

虽然超密集异构网络架构在5G中有很大的发展前景,在开发的过程中仍然存在以下三个问题。

(1) 节点间距离的减小,越发密集的网络部署使得网络拓扑更加复杂,从而容易出现与现有移动通信系统不兼容的问题。

(2) 三种主要干扰:同频干扰,共享频谱资源干扰,不同覆盖层次间的干扰。现有通信系统的干扰协调算法只能解决单个干扰源问题,而在5G网络中,相邻节点的传输损耗一般差别不大,这将导致多个干扰强度相近,进一步恶化网络性能,使得现有协调算法难以应对。

(3) 业务和用户对QoS(Quality of Service)需求的差异性很大,5G网络需要采用一系列措施来保障系统性能,主要有:不同业务在网络中的实现,各种节点间的协调方案,网络的选择,以及节能配置方法等。

2. 自组织网络

在未来5G网络中将面临网络的部署、运营及维护的挑战,这主要是由于网络存在各种无线接入技术,并且网络节点覆盖能力各不相同,它们之间的关系错综复杂,因此自组织网络(Self-Organizing Network, SON)的智能化将成为5G网络必不可少的一项关键技术。其优势体现在网络效率和维护方面,同时减少了运营商的资本性支出和运营成本投入。

自组织网络技术解决的关键问题主要有以下两点。

(1) 网络部署阶段的自规划和自配置。自规划的目的是动态进行网络规划并执行,同时满足系统的容量扩展、业务监测或优化结果等方面的需求。自配置即新增网络节点的配置可实现即插即用,具有低成本、安装简易等优点。

(2) 网络维护的自优化和自愈合。自优化的目的是减少业务工作量,达到提升网络质量及性能的效果,其方法是通过 UE 和 eNB 测量,在本地 eNB 或网络管理方面进行参数自优化。自愈合指系统能自动检测问题、定位问题和排除故障,大大减少维护成本并避免对网络质量和用户体验的影响。

自组织网络架构目前有集中式、分布式和混合式三种。

(1) 集中式:具有控制范围广、冲突小等优点,不足在于运行速度慢、算法复杂度高等。

(2) 分布式:主要通过 SON 分布在 eNB 上来实现,效率和影响速度高,网络扩展性较好,对系统的依赖性小。缺点是协调困难。

(3) 混合式:结合以上两种架构的优点,缺点是设计复杂。

3. 内容分发网络

在未来 5G 中,面向大规模用户的音频、视频、图像等业务急剧增长,网络流量的爆炸式增长会极大地影响用户访问互联网的服务质量。仅依靠增加带宽并不能解决问题,它还受到传输中路由阻塞和延迟、网站服务器的处理能力等因素的影响,内容分发网络(Content Distribution Network, CDN)对 5G 网络的容量与用户访问具有重要的支撑作用。它是在传统网络中添加新的层次,即智能虚拟网络。

CDN 系统综合考虑各节点连接状态、负载情况以及用户距离等信息,通过将相关内容分发至靠近用户的 CDN 代理服务器上,实现用户就近获取所需的信息,使得网络拥塞状况得以缓解,降低响应时间,提高响应速度。

4. 设备到设备通信

在未来 5G 中,网络容量、频谱效率需要进一步提升,更丰富的通信模式以及更好的终端用户体验也是 5G 的演进方向。设备到设备通信(Device-to-Device Communication, D2D)具有潜在的提升系统性能、增强用户体验、减轻基站压力、提高频谱利用率的前景。它是一种基于蜂窝系统的近距离数据直接传输技术。

D2D 会话的数据直接在终端之间进行传输,不需要通过基站转发,而相关的控制信令,如会话的建立、维持、无线资源分配以及计费、鉴权、识别、移动性管理等仍由蜂窝网络负责。

另外,当无线通信基础设施损坏,或者在无线网络的覆盖盲区,终端可借助 D2D 实现端到端通信甚至接入蜂窝网络。

5. M2M 通信

M2M(Machine to Machine Communication)的定义主要有广义和狭义两种。广义的 M2M 主要是机器对机器、人与机器间以及移动网络和机器之间的通信,它涵盖了所有实现人、机器、系统之间通信的技术;从狭义上说,M2M 仅指机器与机器之间的通信。智能化、交互式是 M2M 有别于其他应用的典型特征,这一特征下的机器也被赋予了更多的“智慧”。

6. 信息中心网络

信息中心网络(Information-Centric Network, ICN)即以信息为中心的发展趋势,用以满足海量数据流量分发的要求。ICN 所指的信息包括实时媒体流、网页服务、多媒体通信

等,它的主要概念是信息的分发、查找和传递,不再是维护目标主机的可连通性。有别于传统的以主机地址为中心的TCP/IP网络系统体系结构,ICN忽略IP地址的作用,甚至只是将其作为一种传输标识。全新的网络协议栈能够实现网络层解析信息名称、路由缓存信息数据、多播传递信息等功能,从而较好地解决计算机网络中存在的扩展性、实时性以及动态性等问题。尽管ICN可以解决IP网络的固有问题,但在扩展性、数据移动性及大范围部署等方面存在不足,其中最为突出的是部署性问题。

7. 移动云计算

移动云计算是一种全新的IT资源或信息服务的交付与使用模式,它是在移动互联网中引入云计算的产物。

移动云计算中,移动设备需要处理的复杂计算和数据存储从移动设备迁移到云中,降低了移动设备的能源消耗并弥补了本地资源不足的缺点。此外,由于云中的数据和应用程序存储和备份在一组分布式计算机上,降低了数据和应用发生丢失的概率,移动云计算还可以为移动用户提供远程的安全服务,支持移动用户无缝地利用云服务而不会产生延迟、抖动。移动云是一个云服务平台,还可以支持多种移动应用场景,例如移动学习、移动医疗、智能交通等。

但是由于移动智能终端与云计算中心的端到端网络传输时延与带宽具有不稳定性,移动云计算的信道传输时延无法保证。满足异构网络间服务的无缝交互是移动云计算面临的一个重要的挑战。

8. 软件定义网络/网络功能虚拟化

软件定义网络(Software Defined Network, SDN)作为一种新型的网络架构与构建技术,其提倡的控制与数据分离、软件化、虚拟化思想,为突破现有网络的困境带来了希望。

SDN架构的核心特点是开放性、灵活性和可编程性。可以消除大量手动配置的过程,简化管理员对全网的管理,提高业务部署的效率。SDN不会让网络变得更快,但它会让整个基础设施简化,降低运营成本,提升效率。

网络功能虚拟化(Network Function Virtualization, NFV)的核心思想是将网络逻辑功能与物理硬件解耦,利用软件编程实现虚拟化的网络功能,并将多种网元硬件归成标准化的通用三大类IT设备,即高容量服务器、存储器和数据交换机,实现软件的灵活加载,大幅降低基础设备硬件成本。网络资源的虚拟化有望构成统一的、云化的虚拟资源池以供统一调度使用。

从网络部署模式来看,NFV技术实现各网元设备的虚拟化,SDN则实现虚拟设备之间的数据交换与转发,业务编排,这样可以实现快速便捷的新业务部署,并简化网络层次,降低网络的部署与运维成本。

3.7.2 第5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、Wi-Fi、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,因此异构无线网络以及终端之间协同为用户提供服务的业务方式势在必行。

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，一种是METIS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；另一种是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。

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”来共同定义。“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3.16所示)。

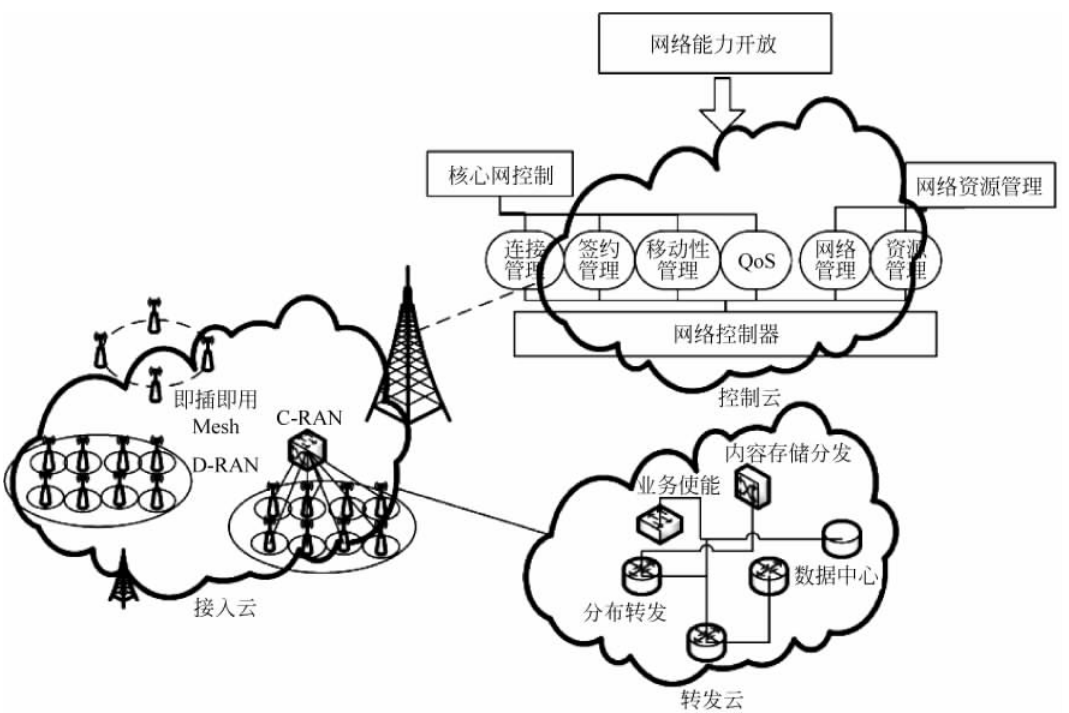

图3.16　IMT-2020(5G)推进组的5G架构

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安全所考虑。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;接入云内涉及边缘计算、大数据分布式计算及处理等安全融合问题;转发云内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环境中被进一步的讨论。

3.8 未来移动通信系统展望

5G时代来临将会对人们的生活产生深远的影响,它将为我们提供一个开放、灵活、可扩展且十分安全的网络环境,满足人们对高质量生活的需求。

目前,世界各国针对未来5G移动通信网络在技术上的可行性研究、标准化以及产品发展方面进行了大量的投入,5G的发展需要在统一的框架下进行全国范围内的协调。同时,在5G通信系统中,采用6GHz频点以上无线频谱的可行性问题成为移动通信业界讨论的热门话题,对高频段的大宽带无线频谱资源的使用,不仅能够有效改善无线频谱效率,而且加快了无线数据传输速率和海量数据的处理能力。为了应对未来信息社会高速进步的趋势,网络应具备智能化的自感知和自调节能力,并且高度的灵活性也将成为未来5G网络必不可少的特性之一。同时,绿色节能也将成为5G发展的重要方向,网络的功能不再以能源的消耗为代价,实现无线移动通信的可持续发展。

小　　结

本章从第2代移动通信系统开始,先详细介绍了GSM系统,包括GSM系统的构成,主要特点以及它的安全特性,并且对GSM系统的安全机制进行了详细的分析,介绍了GSM系统中可能出现的安全问题,主要包括:在GSM系统中的用户鉴权是单向的,只有网络对用户的认证,而没有用户对网络的认证以及SM系统只是在接入网中进行了加密,在核心网中没有采取加密等安全措施,因此在核心网络的网元间,信令消息和数据都采用明文传输,容易被窃听等;详细讲解了通用分组无线业务(GPRS),它是移动通信系统在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。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。

随后介绍了UMTS,它是由GSM扩展改进而来,正因为如此,GSM中的基本接入安全机制正是UMTS接入安全的基础。当然,UMTS的安全体系结构的设计目标并不局限于GSM中已有的安全解决方案,对GSM的安全机制做了多项改进。之后介绍了第3代移动通信系统以及它的安全特点,第3代移动通信系统在原有的基础上添加了很多安全机制以确保网络的安全,但是依旧面临多种威胁。最后介绍了包括4G在内的之后的移动通信系统的概况以及之后的可能的发展方向,我们相信,在不久的将来,4G在业务、功能、频宽上均

有别于3G，应该会将所有无线服务综合在一起，能在任何地方接入因特网，包括定位定时、数据收集、远程控制等功能。移动无线因特网的覆盖范将会是无边无际的。所以，4G将会是多功能集成的宽带移动通信系统，是宽带接入IP的系统，是新一代的移动通信系统。

思 考 题

1. GSM系统的主要特点有哪些？
2. 如何保障GSM系统的安全保密性能？
3. 请简要介绍GPRS的安全防火墙技术。
4. UMTS的安全机制主要原则是什么？
5. 简要介绍第三代移动通信的主要技术。

参 考 文 献

[1] 宁涛. UMTS系统接入安全机制的研究[D]. 武汉：中国地质大学，2008.
[2] 邓智华. 移动通信网络的安全与策略[D]. 北京：北京邮电大学，2007.
[3] 牛静媛. 移动通信安全性分析[D]. 北京：北京邮电大学，2008.
[4] 毛光灿. 移动通信安全研究[D]. 成都：西南交通大学，2003.
[5] 林德敬，林柏钢，林德清. 3G系统全网安全体制的探讨与分析[J]. 中兴通讯技术，2003，9(2)：32-36.
[6] 朱红儒，肖国镇. 基于整个网络的3G安全体制的设计与分析[J]. 通信学报，2002，23(4)：117-122.
[7] 赵丽萍. GPRS移动通信网络安全策略研究[J]. 微计算机信息，2004，20(8)：109-110.
[8] 韩斌杰. GPRS原理及其网络优化[M]. 北京：机械工业出版社，2003.
[9] Xavier Lagrange. GSM网络与GPRS. 顾肇基，译. 北京：电子工业出版社，2002.
[10] 吴文，李旭. GSM和UMTS网络安全性的比较研究[J]. 现代电信科技，2005，10：014.
[11] 张梁，卢军. UMTS接入的安全性研究[J]. 信息安全与通信保密，2005，2：058.
[12] 谢军伟，李小文. UMTS系统接入安全技术的研究[J]. 重庆邮电学院学报(自然科学版)，2006，2：005.
[13] 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
[14] 鲜鹏. 第三代移动通信系统信息安全机制研究[J]. 重庆邮电大学学报(自然科学版) ISTIC，2008，20(6).
[15] 卢军. 移动通信发展的现状及未来趋势. 技术论坛，2005.
[16] 彭艺，查光明. 第四代移动通信系统及展望[J]. 电信科学，2002，6：8-12.
[17] 苏锐. 第四代移动通信系统(4G)关键技术综述[J]. 科技资讯，2005 (25).
[18] 尤肖虎. 未来移动通信技术发展趋势与展望[J]. 电信技术，2003，6：14-17.
[19] 李维科，李方伟. UMTS的接入安全研究[J]. 江西通信科技，2004，4：002.
[20] 彭艺，查光明. 第四代移动通信系统及展望[J]. 电信科学，2002，6：8-12.
[21] 刘颖，杨家玮. UMTS系统体系结构及应用[J]. 电子科技，2002，3：011.
[22] 钟杏梅，蔡国权，牛忠霞. 第三代移动通信的系统组成与主要技术[J]. 无线通信技术，2000，9(4)：18-21.
[23] 张堑. 移动通信网络安全策略研究[D]. 武汉：华中科技大学，2006.
[24] 张媛. 第三代移动通信系统安全技术研究[D]. 大庆：大庆石油学院，2005.
[25] 刘建华. 4G移动通信特点和技术发展综述[J]. 电脑知识与技术，2004，29：44-46.

[26] 钱芳.移动通信系统的安全性研究[J].计算机安全，2012，4：007.
[27] 夏坚.通信安全性试验的现状,问题和对策[J].硅谷，2011(20)：179-179.
[28] 李建权. 4G网络安全问题防范与对策研究[J].电子技术与软件工程，2015.
[29] 黄开枝,金梁,赵华. 5G安全威胁及防护技术研究.中国人民解放军信息工程大学，2015.
[30] 李晖,付玉龙. 5G网络安全问题分析与展望.西安电子科技大学，2015，4.
[31] 赵国峰,陈婧,韩远兵,徐川.5G移动通信网络关键技术综述.重庆邮电大学未来网络研究中心，2015，4.