第3章 第二代移动通信网络安全技术

第一代蜂窝移动通信系统出现于20世纪70年代后期，基于模拟通信技术，采用FDMA(Frequency Division Multiple Access，频分多址接入)模式，以模拟电路单元为基本模块实现话音通信，主要缺点是频谱利用率低，信令干扰话音业务。主要制式有美国的AMPS(Advanced Mobile Phone System，高级移动电话系统)、北欧的NMT(Nordic Mobile Telephone，北欧移动电话)、英国的TACS(Total Access Communication System，全接入通信系统)和日本的HCMTS(High Capacity Mobile Telecommunication System，高容量移动电信系统)等。第一代模拟蜂窝移动通信网络没有采用密码技术来保护无线网络访问的安全性，使得移动用户的通话信息很容易被窃听，移动用户的身份很容易被假冒。

第二代数字移动通信系统(2G)出现于20世纪80年代后期，以GSM和窄带CDMA(Code Division Multiple Access，码分多址接入)为代表，主要采用TDMA(Time Division Multiple Access，时分多址接入)的数字调制方式，提高了系统容量；采用数字语音编码技术，在保证话音质量的前提下可以提升通信带宽的利用效率；采用独立信道传送信令与差错控制技术可以增强网络的抗干扰能力；采用加密技术可以保护数字化的语音、数据和网络信令；采用身份鉴别技术可以鉴别移动用户的身份，防止身份假冒。但TDMA的系统容量仍然有限，越区切换性能仍不完善。无论是GSM系统还是CDMA系统，均无法提供高速的数据业务，难以满足数据通信业务迅猛发展的需要。向3G过渡的2.5代技术GPRS利用原有的2G电路交换技术来提供分组数据通信业务，其安全性与2G类似，在分组数据通信方面有其特殊性，具有IP网络的特点。

3.1 GSM网络系统结构

GSM系统全称为全球移动通信系统(Global System for Mobile Communication，GSM)，它依照ETSI(European Telecommunications Standards Institute，欧洲电信标准化协会)制定的规范研制而成，属于第二代移动通信技术。其开发目的是让全球各地可以共同使用一个移动电话网络标准。

GSM系统由移动站(MS)、基站子系统(BSS)、网络子系统(NSS)、操作支持子系统(OSS)四个分系统组成。图3-1是一个典型的GSM系统结构示意图。四个分系统及其

包含的实体介绍如下。

(1) 移动站(Mobile Station,MS)。

移动站是GSM移动通信网中用户使用的设备,也是用户能够直接接触的GSM系统中的唯一设备。移动站中一个重要的组成部分是SIM(Subscriber Identity Module,用户身份模块),它是一张符合ISO标准的"智慧"卡,它包含所有与用户有关的和某些无线接口的信息,包括身份鉴别和加密信息。

(2) 基站子系统(Base Station Sub-System,BSS)。

基站子系统是由BTS(Base Transceiver Station,基站收发信台)和BSC(Base Station Controller,基站控制器)这两部分的功能实体构成。实际上,一个基站控制器根据话务量需要可以控制数十个BTS,BTS可以直接与BSC相连接,也可以通过BIE(Base Station Interface Equipment,基站接口设备)采用远端控制的方式与BSC相连接。

基站子系统通过无线接口直接与移动站相接,负责无线发送接收和无线资源管理。同时,基站子系统也与网络子系统(NSS)中的移动业务交换中心(MSC)相连,实现移动用户之间或移动用户与固定网络用户之间的通信连接,传送系统信号和用户信息等。

(3) 网络子系统(Network Sub-System,NSS)。

NSS主要执行GSM系统的交换功能和用于用户数据与移动性管理、安全性管理所需的数据库功能,它对GSM移动用户之间通信和GSM移动用户与其他通信网用户之间通信起着管理作用。

NSS具体包括移动业务交换中心(MSC)、拜访位置寄存器(VLR)、归属位置寄存器(HLR)、身份鉴别中心(AuC)、设备识别寄存器(EIR)和操作维护中心(OMC)。

移动业务交换中心(Mobile Switching Center,MSC)可从三种数据库,即归属位置寄存器(HLR)、拜访位置寄存器(VLR)和身份鉴别中心(AuC)获取处理用户位置登记和呼叫请求所需的全部数据。反之,MSC也可根据其最新获取的信息请求更新数据库的部分数据。

拜访位置寄存器(Visitor Location Register,VLR)服务于其控制区域内的移动用户,存储着进入其控制区域内已登记的移动用户相关信息,VLR从该移动用户的归属位置寄存器(HLR)处获取并存储必要的数据。一旦移动用户离开该VLR的控制区域,则需重新在另一个VLR登记,原VLR将取消临时记录的该移动用户数据。因此,VLR可看作一个动态用户数据库,VLR功能通常可以在每个MSC中综合实现。

归属位置寄存器(Home Location Register,HLR)是GSM系统的中央数据库,存储着该HLR控制的所有存在的移动用户的相关数据。一个HLR能够控制若干移动交换区域以及整个移动通信网,所有移动用户重要的静态数据都存储在HLR中,这包括移动用户识别号码、访问能力、用户类别和补充业务等数据。HLR还可以为MSC提供移动用户漫游所在的MSC区域相关动态信息数据。

身份鉴别中心(Authentication Center,AuC)存储着身份鉴别信息和加密密钥,用来防止未授权用户接入系统,保证通过无线接口的移动用户的通信安全。AuC属于HLR的一个功能单元部分,专用于GSM系统的安全性管理。

移动设备识别寄存器(Equipment Identity Register,EIR)存储着移动设备的IMEI(International Mobile Equipment Identity,国际移动设备识别码),通过检查白色清单、黑

色清单或灰色清单这三种表格，就可以得到诸如准许使用的、出现故障需监视的、失窃不准使用的等移动设备的 IMEI，使得运营部门对于不管是失窃还是由于技术故障或误操作而危及网络正常运行的终端设备，都能采取及时的防范措施，以确保网络内所使用移动设备的唯一性和安全性。

(4) 操作支持子系统(Operation Sub-System，OSS)。

OSS 主要执行移动用户管理、移动设备管理以及网络操作和维护等功能任务。移动用户管理可包括用户数据管理和呼叫计费，用户数据管理一般由归属位置寄存器(HLR)来完成这方面的任务，SIM 卡的管理也可认为是用户数据管理的一部分。呼叫计费可以由移动用户所访问的各个移动业务交换中心 MSC 和 GMSC(Gateway Mobile Switching Center，移动业务交换中心网关)分别处理，也可以通过 HLR 或独立的计费设备来集中处理。

OSS 具体包括网络管理中心(NMC)、用于集中计费管理的数据库后台处理系统(DPPS)、用于管理用户识别卡的个人化中心(PCS)与安全性管理中心(SEMC)。

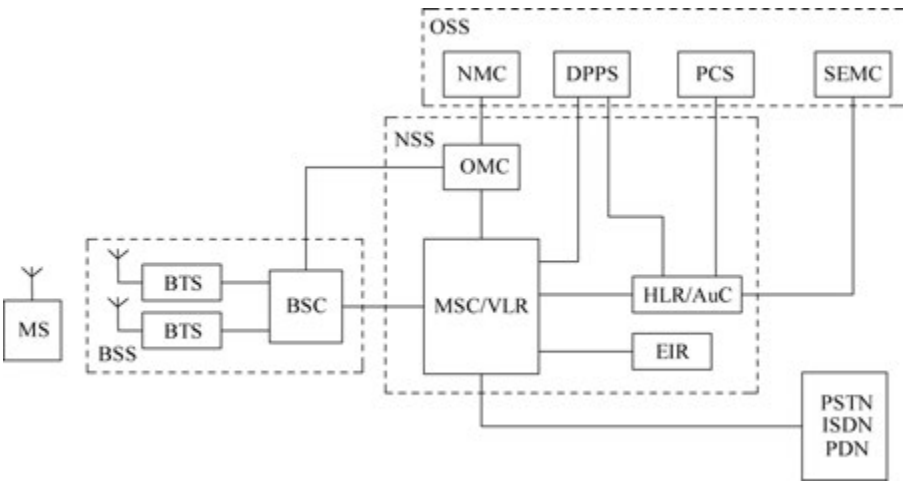

图 3-1　GSM 网络系统结构图

GSM 系统与各种公用通信网之间也都详细定义了标准接口规范，使 GSM 系统可以与各种公用通信网实现互连互通。GSM 系统除了可以开放基本的话音业务外，还可以开放各种承载业务、补充业务以及与 ISDN(Integrated Services Digital Network，综合业务数字网)相关的业务。GSM 系统采用 FDMA/TDMA 及跳频的复用方式，频率重复利用率较高，同时它具有灵活方便的组网结构，可满足用户的不同容量需求。

3.2　GSM 网络安全体系

3.2.1　GSM 网络中的安全保障机制

GSM 系统中的安全保障机制主要由用户身份鉴别、用户身份保密和信令及数据保密等模块组成，主要涉及移动站(MS)、基站子系统(BSS)和网络子系统(NSS)三部分。移

动站和基站间通过无线链路连接，系统其他部分间则通过有线链路连接。SIM 卡中存有用户在 GSM 系统中的注册信息，包括国际移动用户识别码（IMSI）、用户电话号码、身份鉴别算法（A3）、加密密钥生成算法（A8）、加密算法（A5）、个人识别码（PIN）和用户身份鉴别密钥（K_i）等。移动电话与基站通过无线信道进行通信，这是 GSM 系统中唯一使用无线信道的部分。所以，ITU-T（ITU-Telecommunication Standardization，国际电信联盟-电信标准部）建议只考虑移动电话和基站之间的信息需要加密。

在通话建立之前，系统通过一个呼叫响应过程进行用户身份鉴别，通过跟踪技术确定主叫位置，当然，被叫也可在接收通话前确认主叫身份。SIM 卡中的 IMSI（International Mobile Subscriber Identity，国际移动用户识别码）以及 K_i 组成了 GSM 系统中用户的识别凭证。GSM 系统中用户和基站之间的数据与信令由一个临时随机生成的加密密钥（K_c）来加密，K_c 由用户和运营商分别生成并保存。移动用户是通过 TMSI（Temporary Mobile Subscriber Identity，临时移动用户识别码），而不是 IMSI，来让网络识别自己，而 TMSI 由网络派送并周期性改变，所以第三方很难通过窃听对话来得到用户真正的 IMSI。

为了实现 GSM 移动用户数据的无线安全传输与跨国漫游，就需要有统一的加密算法。因此，采用 GSM 制式作为标准的欧洲各国成立了 MOU（Memorandum of Understanding，谅解备忘录）组织，凡是参加 MOU 的国家有权获得 A3、A5、A8 这些密码算法，但是也有不能向非 MOU 国家泄露密码算法的义务。不参加 MOU 的国家当然可以自定算法，然而将难以参与跨国漫游。GSM 运营商需与 GSM 的 MOU 签署相应的保密协定后方可获得具体加密算法，SIM 卡制造商也需签署相应协议才能将加密算法做到 SIM 卡中。GSM 规范规定了详细的空中接口加密协议，无线信道的加密由运营商决定，用户不能干涉身份鉴别和加密过程的应用与否。

GSM 建议书中说明 A3、A8 由各经营部门自行选定，其中包括了一种不加密方式，也就是允许经营部门在提供 GSM 数字移动通信业务时，可以不用加密，当然，这样也就降低了传输信息的安全性。

如前面所描述，网络子系统中的 HLR 和 VLR 为 MSC 提供协调呼叫所需的全部信息。在 HLR 中存有所有与本地用户相关的信息，如本地用户的 IMSI、电话号码、注册业务和 K_i 等永久数据和一些临时数据（如临时移动用户识别码 TMSI），为相应的 MSC 提供呼叫建立和身份鉴别阶段的支持。身份鉴别中心（AuC）是一个包含着 GSM 网络中最重要和最敏感信息的数据库，为 GSM 网络提供身份鉴别、加密数据所必需的全部信息。这些信息包括：每个 K_i，身份鉴别算法 A3，加密算法 A5，加密密钥生成算法 A8。AuC 生成一系列随机数 RAND、标识响应 SRES 和加密密钥 K_c，将它们传送并存储在 HLR 和 VLR 中，为身份鉴别和加密过程提供所需要的各种信息。

图 3-2 所示的是安全信息在 GSM 系统这三部分中的分布，存储在这三部分中的信息在安全机制中缺一不可。

GSM 系统采用多种方式对系统内部的用户进行识别。每个移动用户有 3 种识别号码，即 IMEI、IMSI 和 TMSI。每一台移动用户终端，不管是何种类型（车载、固定、便携或手持）、哪一家工厂生产，都要统一对设备编号。设备识别码 IMEI 是识别移动设备的永

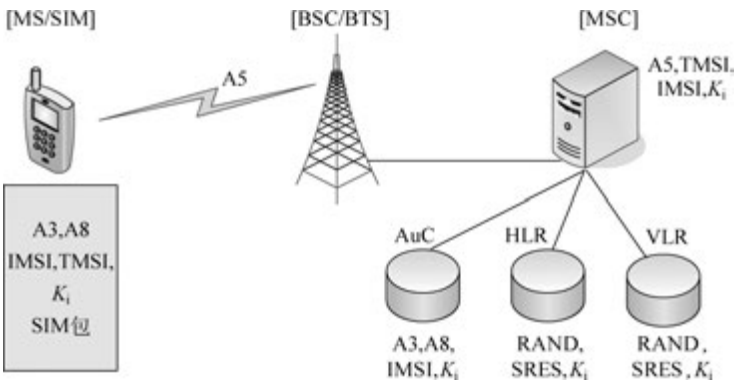

图 3-2　安全信息在 GSM 网络中的分布

久性号码，自设备检验合格出厂以后不再改变。当用户要使用移动设备时，必须首先向网络经营部门注册，根据该用户的归属地区，经营部门为移动用户分配一个 IMSI，同时将该设备的 IMEI 和 IMSI 分别存入移动通信网的 EIR 和 HLR 中。当移动用户首次启用或进入一个新的位置区域时，当地的交换机会给予一个随机号作为 TMSI，并通过地面网络从该用户归属地区的 HLR 中取得其 IMSI，把 IMSI 和 TMSI 一起保存在 VLR 中。TMSI 只在此位置区内有效，且必须与 LAI(Location Area Identity，位置区域识别码)一起使用，移动用户如离开该区域进入一个新的区域，会启动位置注册，从而可能得到一个新的 TMSI。分配 TMSI 时，使用加密信道进行传输，TMSI 与用户之间不存在永久性的对应关系，因此无法通过截取用户识别码来了解某个特定移动用户的行踪。

GSM 系统中除了上述专门考虑的各种信息保密措施以外，还有一些系统特性也增加了信息的安全性。为了改善移动环境下无线信号的传送质量，在 GSM 制式中使用了信道编码，包括卷积码和交织码。此外，系统还可选用跳频方式工作，在跳频方式下，每个 TDMA 帧不停变换载频，特别是对缓慢移动或静止的移动用户，可改善恶劣传输环境下的信号质量，对克服衰落和干扰有较好的效果。从安全方面来看，跳频使无线电传播不在一个固定的载频上，按 GSM 建议，有 64 种跳频序列可由网络端选用，从而增加了从射频传播中非法窃取信息的难度。

3.2.2　GSM 网络中的安全算法

GSM 网络中的敏感信息，如密钥和算法，绝不能在无线信道中以明文形式传送。下面，介绍 GSM 系统中的安全算法。

(1) 身份鉴别/密钥生成算法(A3/A8)。

GSM 中的身份鉴别算法 A3 和密钥生成算法 A8 都是基于带密钥的密码杂凑算法。A3 的输入是 GSM 网络发给移动电话的一个 128 比特的随机数和用户身份鉴别密钥(K_i)，输出为一个 32 比特的标示响应。这个标示响应发回到网络，与网络自己生成的结果进行比较，如果二者相符，用户便通过身份鉴别。A8 的输入也是一个随机数和 K_i，输出为一个 64 比特的加密密钥(K_c)。A3 算法和 A8 算法通常合在一起，统称为 COMP128 算法，目前，COMP128 算法几乎被世界上所有的 GSM 系统所采用。A3 及 A8 算法的应用如

图 3-3 所示。

图 3-3　A3/A8 算法的应用

图 3-4　COMP128-1 算法流程

COMP128 算法有 COMP128-1、COMP128-2 和 COMP128-3 三个版本，COMP128-2 和 COMP128-3 算法是对 COMP128-1 算法的改进。COMP128-1 算法采用的是三元组的 MAC 函数，由于算法主要是同一压缩函数迭代构成，所以又是迭代杂凑函数。输入为 256 比特的数据，输出为 96 比特的数据，输出中，最高 32 比特为 SRES，最低 64 比特为 K_c。COMP128-1 对数据流以字节为单位进行加密。下面就 COMP128-1 算法的原理进行介绍。

COMP128-1 进行 8 轮迭代运算，每一轮迭代开始的时候都首先进行蝶形运算过程，主要由 5 级查表构成。第 8 轮迭代后，将 128 比特输出进一步压缩为 96 比特，这 96 比特就是整个 COMP128-1 运算的最终输出。流程如图 3-4 所示。

在 COMP128-1 算法实现过程中，蝶形压缩实现了压缩值多对一的映射，满足了 MAC 函数的不可逆性要求；但同时，COMP128-1 算法也将输入数据的长度进行了压缩，因此，可能带来数据运算的冲突，即运算不同的输入可以输出相同的 MAC 值，这就使得 COMP128-1 算法不符合在计算上无碰撞的要求。

（2）加密算法（A5）。

GSM 系统中的移动站和基站之间的信令和数据通过加密算法 A5，并使用从 A8 中得到的 K_c 进行加密和解密。有三种 A5 算法，A5/1 被认为是这三种中性能最好的加密算法；A5/2 比 A5/1 在性能上差很多，被用在由于出口限制而禁用 A5/1 的地区；A5/0 虽然也是 A5 的一种，但实际并不对数据进行加密。在 A5/1 和 A5/2 算法中，GSM 网络向移动电话发送一个加密模式请求命令，使其开始加密数据，移动站从 SIM 卡中得到在身份鉴别过程中由 A8 生成的 K_c，用它对数据进行加密和解密。

3.2.3　GSM 网络中的身份鉴别与密钥协商流程

GSM 系统中的身份鉴别采用“挑战-响应”协议，具有较高的安全性，可以满足一般的

安全需求。身份鉴别是一个需要全网配合、共同支持的处理过程，几乎涉及 GSM 网络的所有实体，包括 MSC、VLR、HLR、AuC、BSS 和 MS。GSM 系统中每一用户的 SIM 卡中都保存着唯一的 IMSI-K_i 对，同时还将该 IMSI-K_i 对保存在 AuC 中。

当用户漫游到拜访网络时，GSM 系统中身份鉴别与密钥协商过程分为 3 个阶段，具体过程如图 3-5 所示。

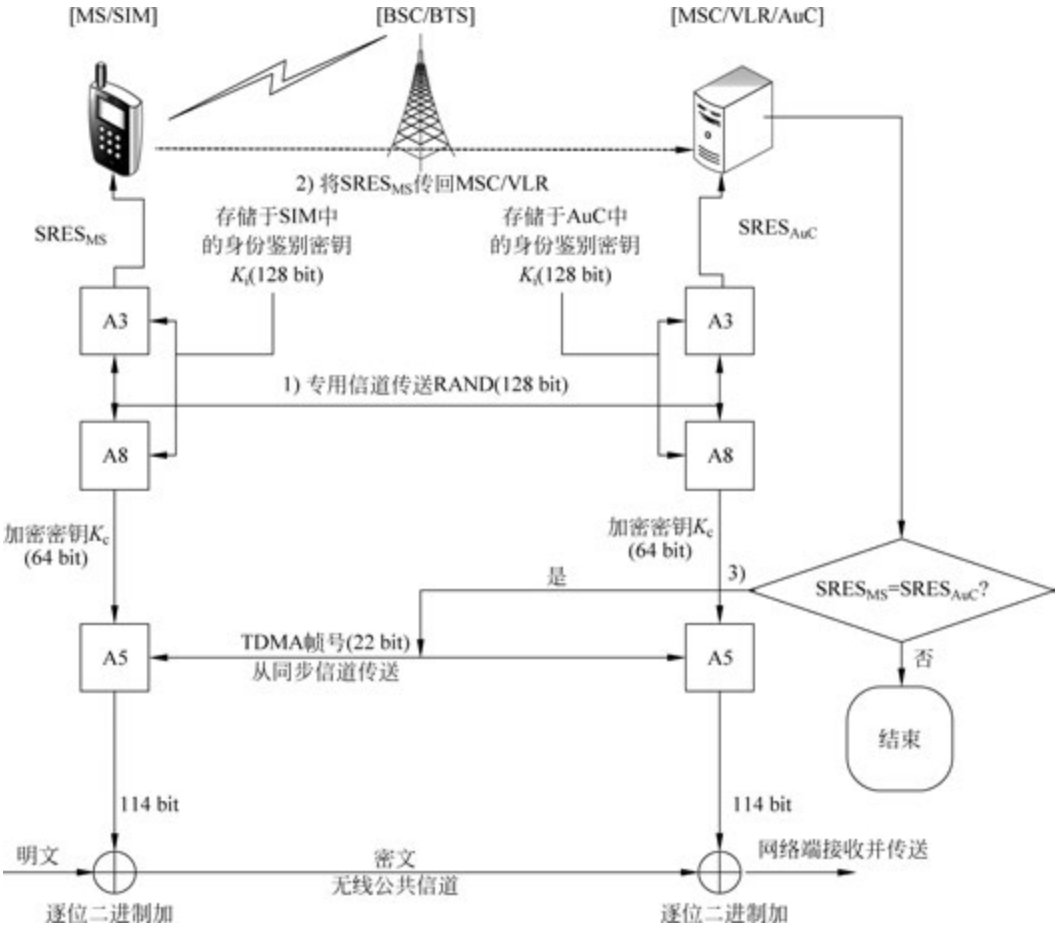

图 3-5　GSM 网络的身份鉴别、密钥协商和数据加解密流程

1. 移动用户注册

当移动用户到归属网络注册时，归属网络颁发给用户一个 SIM 卡。

2. 调用身份鉴别参数

(1) 用户传送 IMSI 给拜访网络。移动用户在拜访网络中注册，即传送 IMSI 给拜访网络。

(2) 拜访网络向归属网络请求身份鉴别参数。拜访网络将用户的 IMSI 传给归属网络，并请求归属网络传送该用户的相关身份鉴别信息，归属网络生成身份鉴别参数三元组 RAND、SRES、K_c。

(3) 归属网络将身份鉴别参数传给拜访网络。拜访网络利用身份鉴别参数三元组来鉴别移动用户身份的合法性。

3. 身份鉴别与密钥协商

在身份鉴别参数调用完成后,拜访网络已得到漫游用户的安全鉴别参数,然后执行如下过程:

(1) 网络向用户发送一个随机数。GSM 网络向移动站派送一个 128 比特的随机数(RAND)作为"呼叫"。

(2) 用户调用身份鉴别算法和密钥生成算法生成身份鉴别响应与加密密钥。移动用户的 SIM 卡以 K_i 和 RAND 为输入,通过身份鉴别算法 A3 和密钥生成算法 A8 生成 32 比特身份鉴别响应 $SRES_{MS}$ 和加密密钥 K_c,双方协商出来的密钥就是 K_c。然后,将标识响应 $SRES_{MS}$ 经基站传给拜访网络。

(3) 网络鉴别用户的身份。GSM 网络在收到 $SRES_{MS}$ 之后,用同样的身份鉴别密钥 K_i 进行 A3 运算,以验证用户的身份。如果 GSM 网络的运算结果 $SRES_{AuC}$ 与收到的 $SRES_{MS}$ 相同,移动站就成功地通过了身份鉴别。拜访网络分配一个临时用户识别码 TMSI,并用 K_c 加密后传给用户,来确认身份鉴别和密钥协商过程成功。否则连接就会中断。

至此,用户的身份鉴别与密钥协商过程全部结束。

在上述过程完成之后,GSM 网络和用户之间便可进行信令和数据的安全通信。在通信过程中,它们之间的信令和数据可以进行加密传输,以确保其机密性。

用户信息和重要的控制信号在无线信道上传送时都可加密,是否加密由网络端确定。加密过程如图 3-5 所示。通过 GSM 系统的身份鉴别与密钥协商过程,网络侧与用户侧可以得到 64 比特的加密密钥 K_c;通过 K_c,以 A5 算法与同步信道中获取的 TDMA 帧号可以算出 114 比特的密钥流。GSM 制式中每个 TDMA 帧有 8 个时隙,每一信道占用一个时隙,每一时隙带有 114 个信息比特。需要加密时,将上述由 A5 算出的 114 比特密钥流与 114 个信息比特逐位异或就得到密文信息。解密端用相同的步骤即可恢复出 114 个原来的明文信息比特。

在整个通信过程中,TMSI 是 GSM 系统中用户的临时标示符,用于隐藏用户的真实身份,它存储在 GSM 网络的 VLR 中,并分配给 GSM 网络的相应用户,它可以在一定时间内代替用户的真实身份,这样可以保证 IMSI 不经过无线网络传输。当一个用户第一次打开移动站时,使用的是存储在 SIM 卡中的 IMSI,在身份鉴别和加密过程之后,GSM 系统通过 A5 算法用密钥 K_c 把加密后的 TMSI 派送给移动站,移动站收到 TMSI 后,发送用同样的算法和密钥加密后的响应来确认接受。之后,当用户和网络通信时,便使用 TMSI 代替真正的身份标识 IMSI。

加密过程中各种密钥都不在无线信道中传送,唯一经无线信道传送的是随机数 RAND,而每次会话都使用不同的随机数。加密所用的密钥还与 TDMA 帧有关,每帧都改变密钥,更增加了解密的困难,从而提高了安全性。另外,K_c 由包含 A8 和 K_i 的 SIM 卡和 AuC 分别生成,在 AuC 中生成的 K_c 又被提供给 HLR 和 VLR。由于随机数

RAND 的不断改变，由其生成的 K_c 也会随之不断变化，这使得系统的安全系数得到进一步提升。K_c 是在 SIM 卡和 AuC 内部生成的，所有的敏感信息也没有经过无线信道传输，这样，敏感信息就得到了很好的保护。

总之，GSM 系统在身份鉴别过程中，传输的是鉴别参数，并未传输鉴别密钥，而且移动用户的身份鉴别密钥只有自己和归属网络知道，这就保护了身份鉴别密钥的安全。用户临时识别码 TMSI 的使用，又保护了移动用户的真实身份，可防止无线跟踪。

3.3 SIM 卡及其安全性

SIM 卡是一种带有微处理器的 IC 卡(Integrated Circuit Card，集成电路卡)，它符合 IC 卡国际标准 ISO 7816，该种 IC 卡内封装有中央处理器(CPU)、存储器及 I/O 电路。SIM 卡提供两方面的功能：业务的保密接入和数据的交换。在 GSM 系统中，通过对 SIM 卡的物理接口与逻辑接口的明确定义，来完成网络与移动终端的连接和信息交换，同时在 SIM 卡内部进行用户信息存储、执行身份鉴别算法和产生加密密钥等工作。只有插入 SIM 卡后，移动终端才能进入网络，用户以 PIN(Personal Identification Number，个人识别码)向 SIM 卡证实其使用权，一旦 SIM 卡从 GSM 等终端拨出，除了紧急呼叫外，终端就无法使用。

2G 时代的 SIM 卡已经是带有微处理器的芯片卡，内有 5 个模块，每个模块对应一个功能：CPU(8 位)、程序存储器 ROM(6～16 kbit)、工作存储器 RAM(128～256 kbit)、数据存储器 EEPROM(2～8 kbit)和串行通信单元，这 5 个模块集成在一块集成电路中。SIM 卡在与手机连接时，最少需要 5 个连接线：电源(Vcc)、时钟(CLK)、数据 I/O 口(Data)、复位(RST)和接地端(GND)。

SIM 卡内保存的数据可以归纳为以下四种类型：

(1) 由 SIM 卡生产厂商存入的系统原始数据。包括：ICCID(Integrate Circuit Card Identity，集成电路卡识别码)、IMEI、A3/A8 和 PUK(PIN Unblocking Key，PIN 码解锁码)等。

(2) 由 GSM 网络运营部门或者其他经营部门在将卡发放给用户时，注入的网络参数和用户数据，包括：K_i、IMSI、A3、A8、A5 等。

(3) 由用户自己存入的数据，比如短消息、固定拨号、缩位拨号、性能参数和话费记数等。

(4) 用户在用卡过程中自动存入和更新的网络接续和用户信息类数据，包括最近一次位置注册时的 LAI、设置的周期性位置更新间隔时间、TMSI、K_c 和随机数 RAND 等。

上面第(1)类数据通常属永久性的数据，由 SIM 卡生产厂商注入以后便无法更改，第(2)类数据只有网络运营的专门机构才允许查阅和更新，第(3)、(4)类中的大部分数据允许用户利用手机对其进行读/写操作。

SIM 卡中最敏感的数据采用 A3、A8 密码算法处理，如 K_i、PIN、PUK、K_c、A3、A8 等都是在生产 SIM 卡的同时写入的，一般人都无法读取 A3、A8 算法；PIN 码可由用户在手机上自己设定，K_c 在加密过程中由 K_i 派生出。K_i 和 IMSI 在 SIM 卡的个性化阶段产生并被写入 SIM 卡，同时，K_i 和 IMSI 这一对数据也会被送入交换机的 HLR。

SIM 卡本身是通过 PIN 码来保护的，PIN 码是一个 4～8 比特的个人识别码，只有当用户输入正确的 PIN 码时，SIM 卡才能被启用，移动终端才能对 SIM 卡进行存取，也只有使用 PIN 码方式的身份鉴别通过后，用户才能接入网络。当连续 3 次输入 PIN 码错误，PIN 码就会被锁住，只有输入更高一级的 PUK 码才能解锁。每张 SIM 卡有各自对应的 PUK 码，长 8 比特，可以交由用户自己管理，也可以由网络运营商自己控制。当连续十次输入 PUK 码错误，SIM 卡将永久损坏。

GSM 系统中对设备的识别在 EIR 中完成。EIR 中存有三种名单：

白名单：包括已分配给可参与运营的 GSM 各国的所有设备识别序列号码；

黑名单：包括所有应被禁用的设备识别码；

灰名单：包括有故障的及未经型号认证的移动站设备，由网络运营商决定。

移动站设备识别的程序是：MSC/VLR 向 MS 请求 IMEI，并将其发送给 EIR，EIR 将收到的 IMEI 与白、黑、灰三种名单进行比较，把结果发送给 MSC/VLR，以便 MSC/VLR 决定是否允许该移动站设备进入网络。

3.4 CDMA 网络身份鉴别机制

进入 21 世纪，CDMA(Code Division Multiple Access，码分多址)技术，经历了从窄带 CDMA(IS-95 CDMA)向宽带 CDMA 的演进，它以系统容量、业务质量、安全性和可靠性等方面的优势而备受瞩目。

窄带 CDMA 采用 CDMA IS-95 标准，其安全机制的关键是 CAVE(Cellular Authentication and Voice Encryption，蜂窝身份鉴别与语音加密)算法，主要包括统一查询、独特查询、SSD(Shared Secret Data，共享保密数据)更新等功能。CDMA 身份鉴别机制中，所有通过空中接口交换的信息只包括随机数和 CAVE 算法的结果，其他机密信息不通过空中接口交换，这样就保障了黑客不能从空中接口得到任何有用的信息。根据 ANSI41 协议，使用 CAVE 算法身份鉴别所涉及的相关参数主要有：MIN(Mobile Identification Number)、ESN(Electronic Serial Number)、A-KEY(Authentication Key，身份鉴别密钥)和 SSD(SSD_A 和 SSD_B)。其中，SSD 由 A-KEY、ESN、RAND_SSD 和 CAVE 算法生成，保存在手机和 AuC 中(在 SSD 共享时也保存在 VLR 中)。

CDMA 系统的身份鉴别机制由以下几部分组成，如图 3-6 所示。

CDMA 网络的身份鉴别机制使用二级安全密钥。第一级密钥称为 A-KEY，保存在身份鉴别中心和移动站中，并且网络中 A-KEY 不共享，A-KEY 的机密性对于身份鉴别机制的成功与否至关重要。第二级密钥称为 SSD(共享秘密数据)，SSD 定期由 A-KEY 产生，网络中 SSD 共享，但不在空中传送。

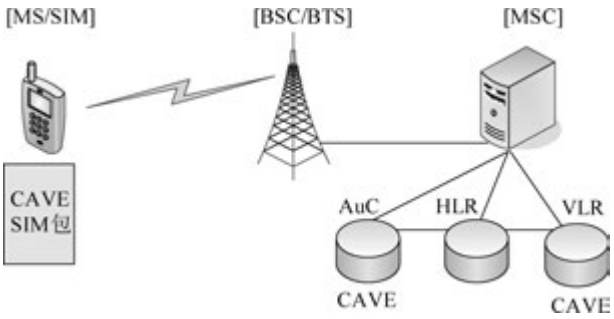

图 3-6　CDMA 网络身份鉴别机制的组成

当用户入网或开通身份鉴别功能时，通过固定的算法由 HLR 分配给该用户一个 A-KEY 值，该 A-KEY 值同时存入手机 SIM 卡中并保存在 AuC 中。A-KEY、ESN、RAND_SSD 利用 CAVE 算法得到 SSD；当手机开机注册、始呼链接时，手机使用 CAVE 算法，由 SSD、IMSI、ESN 和 RAND 计算得到 AUTHR；手机向交换机发送注册信令，其中包括的身份鉴别数据有 RAND 和 AUTHR。AuC 或者 VLR（当 SSD 共享时）收到身份鉴别信令后，也使用参数 SSD、IMSI、ESN、RAND 和 CAVE 算法得到 AUTHR，与手机的计算值比较，如果相同，则身份鉴别成功。基于管理或者其他原因，AuC 可能会更新 SSD，更新成功以后，手机、AuC 或者 VLR 中的 SSD 被同步刷新，在以后的身份鉴别运算中会使用这个新值。

身份鉴别密钥 A-KEY 是身份鉴别过程中的关键参数，A-KEY 由 64 比特二进制数组成，这 64 比特随机数和手机 ESN 等参数相互作用产生 18 比特校验值。A-KEY 不直接参与身份鉴别和保密过程，只用于产生子密钥，用子密钥来进行语音、信令及用户数据的加密，因此，保证 A-KEY 的安全至关重要。A-KEY 分配给移动站，并存储在移动站的永久性安全标识存储器中，仅对移动站和归属位置寄存器/身份鉴别中心（HLR/AuC）是可知的，并不在空中传输。A-KEY 可以重新设置，终端和网络身份鉴别中心 AuC 中的 A-KEY 必须同步更新。

身份鉴别算法中作为 CAVE 算法输入的随机数 RAND 应当合理定期更换，一般来说 RAND 改变得越频繁，攻击者越难分析出计算的过程。CAVE 算法与 GSM 网络中的身份鉴别算法的其中一个重要区别是，在不同的身份鉴别场合和不同的身份鉴别方式下，CAVE 算法输入参数的组成是不一样的，且不同场合输出的结果值在身份鉴别信令规程中的作用也是不一样的，移动站和网络必须按照要求提供或者使用这些参数和结果。

有关 CDMA 安全机制更为详细的描述，可参阅相关书籍和资料。

3.5　GPRS 网络安全机制

2001 年 GPRS（General Packet Radio Service，通用分组无线服务）投入商用。在无线上网方式中，GPRS 展现了其广阔的前景，这种被称为 2.5G 的无线通信技术有其特有

的优势。对用户来说，只要有一个 SIM 卡，就可以随时随地接入，真正实现 24 小时在线；对电信运营商来说，在 GSM 网络上增加与 GPRS 的相关投入，可以充分利用原有的投资，逐步实现向 3G 的过渡。

3.5.1 GPRS 网络系统结构

GPRS 是一种基于 GSM 系统的无线分组交换技术，提供端到端的、广域的无线 IP 连接。使用 GSM 的连接方式，在有数据需要传送时利用分组来传送数据包，通过对无线信道的统计复用能够有效地共享网络资源，提高现有设备以及无线信道资源的利用效率。另外，GPRS 核心网络采用了 IP 技术，既可以与迅速发展的 Internet/Intranet 互联，又顺应通信网的分组化发展趋势，逐步向第三代移动通信系统演进。

GPRS 是在现有的 GSM 网络上增加了 3 种新的网络逻辑实体并进行相应的软件升级而发展起来的，这 3 种逻辑实体是：SGSN(Servicing GPRS Support Node，服务 GPRS 支持节点)、GGSN(Gateway GPRS Support Node，网关 GPRS 支持节点)和 PCU(Package Control Unit，分组控制单元)。在数据传输应用中，用户在 GPRS 网络上可任意选择 UDP(通用数据报协议)与 TCP(传输控制协议)，而没有明确的标准，用户能够在端到端分组方式下发送和接收数据。其系统结构如图 3-7 所示。

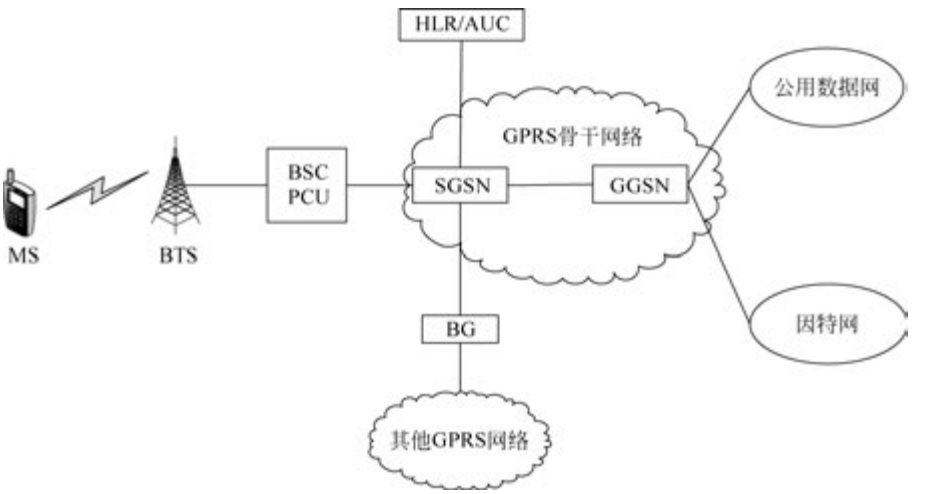

图 3-7　GPRS 系统结构

GPRS 系统包括下述功能单元。

MS(移动站)：支持 GPRS 的手机。

PCU(分组控制单元)：主要用于完成无线链路控制，并且实现与 SGSN 的通信接口。

HLR/AuC(归属位置寄存器/身份鉴别中心)：存放包括用户密钥在内的用户机密数据，产生身份鉴别消息及加密密钥。

SGSN(服务 GPRS 支持节点)：SGSN 是 GPRS 网络的主要组成部分，与 MSC(移动业务交换中心)处于网络体系的同一层，执行移动站注册、移动性管理、安全功能、接入控制及路由选择功能。

GGSN(网关 GPRS 支持节点)：GGSN 是连接 GPRS 网络和外部分组交换数据网的

网关。GGSN 与 SGSN 的通信是通过基于 IP 的 GPRS 骨干网进行的，GGSN 可以把 GPRS 网中的 GPRS 分组数据包进行协议转换，从而可以把这些分组数据包传送到远端的 TCP/IP 网络；另外 GGSN 还提供必要的网间安全机制（如防火墙）。

BG（Border Gateway，边界网关）：边界网关用于不同 GPRS 骨干网的互联，执行运营商之间的漫游协定，并具有基本的安全功能。

GPRS 业务传输的基本流程是：移动终端设备通过串行或无线方式连接到 GPRS 移动站上；GPRS 移动站与基站通信，但与 GSM 系统的数据呼叫不同，GPRS 分组是从基站经分组控制单元（PCU）处理后发送到 SGSN，而不是通过移动业务交换中心（MSC）连接到语音网络上；SGSN 与 GGSN 进行通信，GGSN 对分组数据进行相应的处理，再发送到目的网络，如因特网或 X.25 网络。来自因特网且标识有移动站地址的 IP 包，由 GGSN 接收，再转发到 SGSN，继而传送到移动站。

GPRS 充分利用共享无线信道，采用 IP Over PPP（Point to Point Protocol，点对点协议）实现数据终端的高速、远程接入。作为现有 GSM 网络向第三代移动通信演变的过渡技术（2.5G）。GPRS 的特点和技术优势有：

（1）为用户提供端到端的分组交换传输方式，能够高效地利用网络资源，降低通信成本；

（2）GPRS 网络连接速度快，提供了与现有数据网的无缝连接；

（3）GPRS 具有多种服务质量，可灵活支持多种数据应用；

（4）GPRS 的计费更加合理，用户使用更加方便。

GPRS 采用分组交换技术，每个用户可同时使用多个无线信道，同一无线信道又可以被多个用户共享，资源被有效利用。使用 GPRS，数据传输实现了分组发送和接收，用户在线按流量、时间计费，降低了服务成本。

3.5.2　GPRS 网络的身份鉴别机制

GPRS 提供的安全特征与 GSM 非常类似，由于 GPRS 的骨干网是 IP 网，因此 GPRS 的骨干网又可以利用 GSM 标准之外的安全机制。GPRS 提供了以下安全特性：

（1）身份鉴别。即确认用户身份，其目的是防止非授权使用网络资源，同时通过拒绝假冒授权用户的入侵来保护合法的 GPRS 用户。

（2）接入控制。即网络可采取措施，对 GPRS 用户的各种接入类型进行限制，如位置限制等。

（3）数据保密。用户数据信息对非授权的个体、实体或过程需要保密。

（4）身份保密。无线链路上的用户身份信息对非授权的个体、实体或过程需要保密。

GPRS 系统的用户身份鉴别过程与 GSM 中的身份鉴别过程类似，区别在于身份鉴别的执行过程由移动业务交换中心（MSC）转移到了服务 GPRS 支持节点。身份鉴别机制中使用了一个三元组，包括一个 128 比特的随机数 RAND，用于用户身份鉴别的 A3 算法结果 SRES（32 比特）以及由 A8 算法计算所得的 64 比特加密密钥 GPRS_Kc，这个密钥将用于身份鉴别结束后数据传输中使用的 GPRS 加密算法（GPRS Encryption Algorithm，GEA）。在网络侧，这个三元组从归属位置寄存器 HLR 处获取并存储于服务 GPRS 支持

节点内部。

GPRS 系统的身份鉴别由 MS、SGSN 和 HLR/AuC 共同完成。身份鉴别过程如图 3-8 所示。

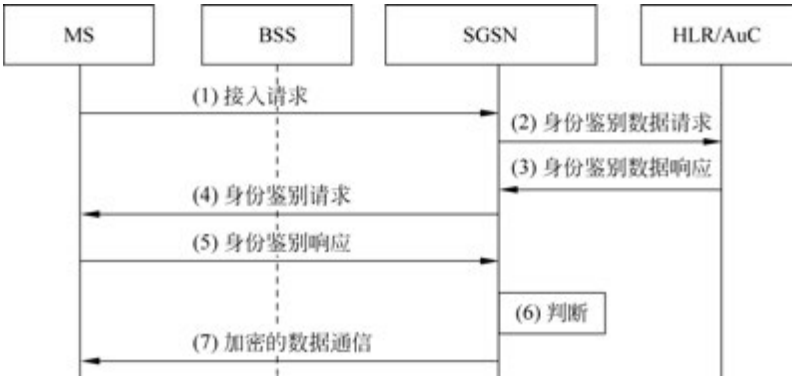

图 3-8　GPRS 的身份鉴别过程

(1) 移动站 MS 发出接入请求到 SGSN。

(2) SGSN 发送身份鉴别数据请求消息到 HLR/AuC，请求用户的身份鉴别数据。

(3) HLR 计算身份鉴别响应并发给 SGSN。HLR 接收到该信息后，用随机数发生器产生一个 128 比特的随机数 RAND，然后由用户身份鉴别密钥 K_i 和随机数 RAND 经 A3 算法产生签名响应 SRES，经 A8 算法产生加密密钥 GPRS_Kc，然后将身份鉴别向量(RAND、SRES、GPRS_Kc)作为一个三元组，发送到 SGSN。

(4) SGSN 向移动站发送身份鉴别请求消息。身份鉴别请求消息包含从 HLR/AuC 那里接收到的随机数 RAND。

(5) 移动站计算身份鉴别响应并发给 SGSN。移动站 MS 利用 SIM 卡存储的密钥 K_i 和接收到的随机数 RAND 经 A3 算法产生签名响应 SRES，再经 A8 算法产生加密密钥 GPRS_Kc，然后将 SRES 通过身份鉴别响应消息发送到 SGSN。

(6) SGSN 进行判断。SGSN 判断从移动站收到的 SRES 是否与从 HLR/AuC 收到的一致，如果一致，则通过对移动站 MS 的身份鉴别。

(7) 移动站与 SGSN 之间进行加密的数据通信。服务 GPRS 支持节点与移动站协商是否需要对数据传输进行加密，并保证服务 GPRS 支持节点与移动站之间加密解密的同步进行。

至此，GPRS 网络对用户的身份鉴别过程结束。

在接下来的通信中，MS 和 SGSN 将利用各自的加密密钥 GPRS_Kc 进行加密和解密。值得注意的是，GPRS 网络中的所有安全功能都建立在用户身份鉴别密钥 K_i 之上，因此，K_i 的保护是至关重要的。密钥 K_i 和 A3 算法都是保密的，它们被存储在用户 SIM 卡和网络的 HLR 中；在身份鉴别过程中，用户使用临时身份和加密参数对自己的身份鉴别信息进行保护。

3.5.3　GPRS 网络的数据与身份保密机制

如 3.5.2 节所描述，GPRS 系统提供了对数据和用户身份的保密机制，下面分别予以

介绍。

(1) 用户数据与信令的保密。

对照现有 GSM 系统中数据加密的范围(基站和移动用户之间),GPRS 加密的范围扩展到从服务 GPRS 支持节点到移动用户,见图 3-9。

图 3-9　GPRS 与 GSM 加密范围对比

GPRS 系统采用对称流加密方式,输入为加密密钥(GPRS_Kc)、输入数据流(INPUT)和传输方向标示(DIRECTION),输出为输出密钥流(OUTPUT)。加/解密过程如图 3-10 所示。

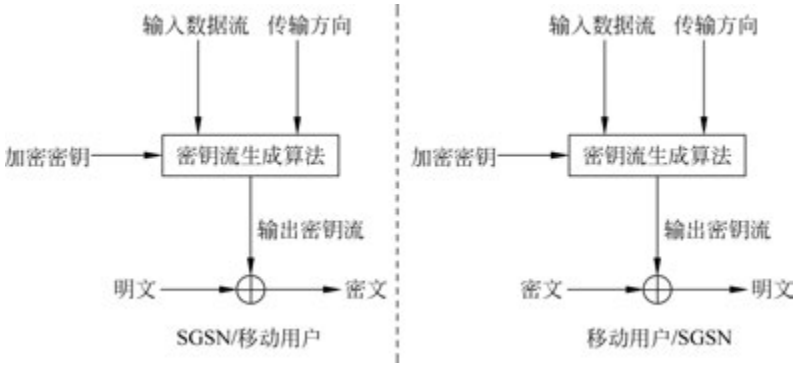

图 3-10　GPRS 加/解密过程

网络对移动终端的身份鉴别成功之后,就可以进行数据传输了。在 GPRS 网络数据传输过程中,数据和信令是受加密算法保护的,并且这种 GPRS 加密算法是保密的,处于逻辑链路控制(LLC)层。为了保证 GPRS_Kc 的安全性,GPRS 网络只向用户终端传送随机数 RAND,用户和网络都利用 RAND 和 K_i,使用 A8 算法来计算密钥 GPRS_Kc。密钥 GPRS_Kc 的最大长度为 64 比特,并且可以在数据传输过程中随时进行重新设置,网络和移动终端中始终保持最新的 GPRS_Kc。为了正确传递数据,服务 GPRS 支持节点和移动终端中对数据流的加密和解密过程必须保持同步,这可以通过 LLC 包的序列号以及数据传送方向来保证。

(2) 用户身份保密。

GPRS 系统的用户终端利用 SIM 卡保存用户信息,包括用户的密钥 K_i 及国际移动用户识别码 IMSI。SIM 卡中实现了 A3、A8 和 GEA 算法,与安全相关的运算都在 SIM 卡中进行。身份鉴别中心在用户注册时将用户的身份鉴别密钥 K_i 和 IMSI 分配给用户并装入 SIM 卡中,并同时存入 AuC 的数据库中,K_i 只在 SIM 卡和 AuC 中使用,不会在网络中传输,可以有效避免密钥的泄露。

GPRS 用户由临时逻辑链路标识(Temporary Logical Link Identity,TLLI)来识别。而唯一确定用户身份的 IMSI 一般不在无线接口上的使用,只有在网络无法识别其临时身份时才使用 IMSI。TLLI 和 IMSI 之间的对应关系分别保存在移动用户和服务 GPRS 支持节点中,TLLI 可以从服务 GPRS 支持节点分配的分组-临时移动用户识别码(P-TMSI)中得到。当移动用户处在准备状态时,服务 GPRS 支持节点可在任何时候重新分配 P-TMSI。

一般认为,GSM/GPRS 系统中主要有如下的安全缺陷。

(1) 身份鉴别的安全缺陷。身份鉴别过程是单向的,即只有网络对 MS 的身份鉴别,用户对 AuC/SGSN 不作身份鉴别,因而可能存在攻击者利用假的 AuC/SGSN 或基站对用户进行欺骗。

(2) 信令及数据加密的安全缺陷。GSM/GPRS 系统中的加密范围分别是从 MS 到基站与 MS 到 SGSN,网络内部的有线链路上信息却以明文方式传输,没有提供端到端的加密。

(3) 加密算法的安全缺陷。GSM/GPRS 的加密算法 A5/GEA 的密钥长度太短,只有 64 比特,无法抵抗穷举攻击。目前 A5 与 GEA 加密算法已经被攻破。

(4) SIM 卡的安全缺陷。GSM 及 GPRS 系统的安全性都是基于对称密钥,存储在 SIM 卡中的 IMSI-Ki 密钥对是系统安全的根本。如果 SIM 卡被复制,也就是说,如果能够得到用户 SIM 卡中的关键信息(如 K_i),就可以克隆一个 SIM 卡来盗用这部电话,则非授权用户可以使用授权用户的身份访问网络资源,这将使系统的安全性受到严重威胁。

本章小结

与第一代模拟蜂窝移动通信系统相比,第二代数字蜂窝移动通信系统为用户提供了更为安全的通信服务和技术。本章系统地介绍了 GSM 系统的安全保密体系,包括安全信息的分布、组成及其各部分的工作机理;描述了 GSM 系统的身份鉴别流程和安全算法,分析了系统存在的安全隐患,说明了 SIM 卡的基本概念、功能、现状及安全问题;对 CDMA 系统的安全机制进行了简要说明;介绍了 GPRS 系统的基本原理和技术特点;描述了 GPRS 系统的安全机制、身份鉴别流程与安全缺陷。

本章习题

3-1 GSM 移动通信系统主要包含哪些模块?分别具有什么功能?

3-2 GSM 移动通信系统中主要有哪些安全算法?

3-3 当用户漫游到拜访网络时,画图并文字描述 GSM 系统的身份鉴别与密钥协商过程。

3-4 SIM 卡由哪几部分组成?有何功能?

3-5 SIM 卡可以保存哪几种类型的数据?

3-6　简述 CDMA 网络系统的安全机制。

3-7　GPRS 网络系统主要包括哪些功能单元？

3-8　简述 GPRS 系统的身份鉴别过程。

3-9　简述 GPRS 系统中用户数据与信令保密的实现过程。

3-10　GSM/GPRS 系统的安全缺陷有哪些？