第 3 章

CHAPTER 3

数字移动通信系统(2G)

3.1 GSM 系统概述

GSM 的英文全名为：Global System for Mobile Communications，中文译为全球移动通信系统，俗称“全球通”，是一种起源于欧洲的数字移动通信系统标准。早在 1982 年，欧洲已有几大模拟蜂窝移动系统在运营，例如北欧多国的 NMT(北欧移动电话)和英国的 TACS(全接入通信系统)，西欧其他各国也提供移动业务。但由于各国之间的移动通信系统的体制和标准不统一，移动通信很难实现国家间的漫游，为了方便全欧洲统一使用移动电话，北欧国家向 CEPT(欧洲邮电行政大会)建议制定一种公共的数字移动通信系统标准，统一规范欧洲电信业务，因此成立了一个在 ETSI 技术委员会下的“移动特别小组(Group Special Mobile)”，简称“GSM”，来制定有关的标准和建议书。

3.1.1 GSM 系统的结构

GSM 系统结构如图 3-1 所示，主要由移动台、基站子系统(BSS)和网络子系统(NSS)组成。

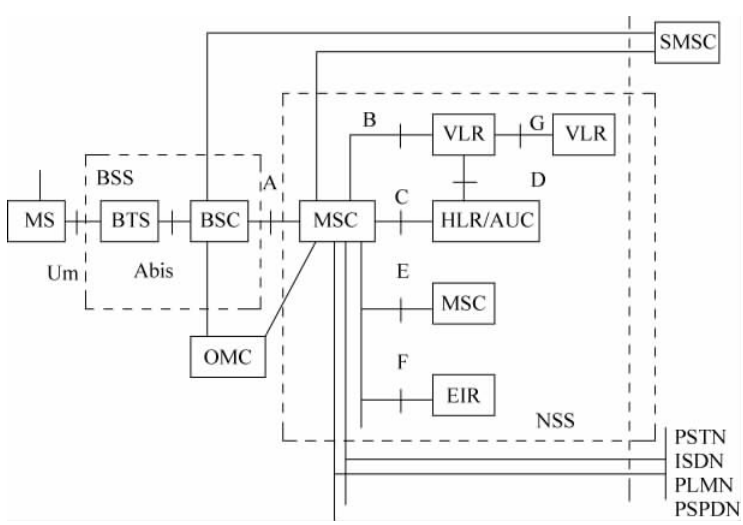

图 3-1 GSM 系统的网络结构

1. 网络各部分的主要功能

MS(移动台)包括 ME(移动设备)和 SIM(用户识别模块)卡,移动台可分为车载台、便携台和手机 3 类,其主要作用是通过无线接口接入网络系统,也提供人机接口。SIM 卡是识别卡,用来识别用户,它基本上是一张符合 ISO 标准的"智慧"磁卡,其中包含与用户有关的无线接口的信息,也包括鉴权和加密的信息。除紧急呼叫外,移动台都需要插入 SIM 卡才能得到通信服务。

BSS 主要的功能是负责无线发射和管理无线资源,BSS 由 BTS(基站收发台)和 BSC(基站控制器)组成。BSS 中的 BTS 是用户终端的接口设备,BSC 可以控制一个或多个 BTS,可以控制信道分配,通过 BTS 对信号强度的检测来控制移动台和 BTS 的发射功率,也可作出执行切换的决定。

NSS(网络子系统)由 MSC(移动交换中心)和 OMC(操作维护中心)以及 HLR(归属位置寄存器)、VLR(访问位置寄存器)、AUC(鉴权中心)和 EIR(设备标志寄存)等组成,NSS 主要负责完成 GSM 系统内移动台的交换功能和移动性管理、安全性管理等。

MSC 是 GSM 网络的核心部分,也是 GSM 系统与其他公用通信系统之间的接口,主要是对位于它所管辖区域中的移动台进行控制、交换。

OMC 主要对 GSM 网络系统进行管理和监控。

VLR 是一个动态的数据库,用于存储进入其控制区用户的数据信息,例如用户的号码、所处位置区的识别、向用户提供的服务等参数,一旦用户离开了该 VLR 的控制区,用户的有关数据将被删除。

HLR 是一个静态数据库,每个移动用户都应在其 HLR 登记注册; HLR 主要用来存储有关用户的参数和有关用户目前所处位置的信息。

EIR 用来存储有关移动台设备参数的数据库,对移动设备进行识别、监视和闭锁等。

AUC 专用于 GSM 系统的安全性管理,进行用户鉴权及对无线接口上的语音、数据、信令信号进行加密,以防止无权用户的接入和保证移动用户的通信安全。

SMSC(短消息业务中心)与 NSS 连接可实现点对点短消息业务,与 BSS 连接完成小区广播短消息业务。

在实际的 GSM 网络中,可根据不同的运营环境和网络需求进行网络配置。具体的网络单元可用多个物理实体来承担,也可以将几个网络单元合并为一个物理实体,比如将 MSC 和 VLR 合并在一起,也可以把 HLR、EIR 和 AUC 合并为一个物理实体。

2. GSM 网络接口

如图 3-1 所示,GSM 网络共有 10 类接口,其中的主要接口包括 A 接口、Abis 接口和 Um 接口,这 3 个接口直接连接了移动台、基站子系统和网络子系统。

GSM 网络各接口的主要功能描述如下。

A 接口。A 接口定义为网络子系统与基站子系统之间的通信接口,其物理连接是通过采用标准的 2.048Mbps PCM 数字传输链路来实现,此接口传送的信息包括对移动台及基站的管理、移动性和呼叫接续管理等。

Abis 接口。Abis 接口定义为基站子系统的基站控制器与基站收发信机两个功能实体之间的通信接口,用于 BTS(不与 BSC 放在一处)与 BSC 之间的远端互连方式。该接口支持所有向用户提供的服务,并支持对 BTS 无线设备的控制和无线频率的分配。

Um 接口。又称为空中接口，定义为移动台与基站收发信机之间的无线通信接口，它是GSM 系统中最重要、最复杂的接口，此接口传递的信息包括无线资源管理、移动性管理和接续管理等。

B 接口。B 接口定义为移动交换中心与访问位置寄存器之间的内部接口，用于 MSC 向VLR 询问有关移动台当前位置信息或者通知 VLR 有关 MS 的位置更新信息等。

C 接口。C 接口定义为 MSC 与 HLR 之间的接口，用于传递路由选择和管理信息，两者之间是采用标准的 2.048Mbps PCM 数字传输链路实现的。

D 接口。D 接口定义为 HLR 与 VLR 之间的接口，用于交换移动台位置和用户管理的信息，保证移动台在整个服务区内能建立和接收呼叫。由于 VLR 综合于 MSC 中，因此 D 接口的物理链路与 C 接口相同。

E 接口。E 接口为相邻区域的不同移动交换中心之间的接口，用于移动台从一个 MSC 控制区到另一个 MSC 控制区时交换有关信息，以完成越区切换。

F 接口。F 接口定义为 MSC 与 EIR 之间的接口，用于交换相关的管理信息。

G 接口。G 接口定义为两个 VLR 之间的接口，当采用临时移动用户识别码(TMSI)时，此接口用于向分配 TMSI 的 VLR 询问此移动用户的国际移动用户识别码(IMSI)的信息。

GSM 系统通过 MSC 与其他公用电信网互连，一般采用 SS7 号信令系统接口，其物理链接方式是通过在 MSC 与 PSTN 或 ISDN 交换机之间采用 2.048Mbps PCM 数字传输链路实现。

3.1.2　GSM 的区域和识别号码

1. 区域的划分

GSM 通信系统服务区域划分如图 3-2 所示。各类区域的定义如下。

(1) GSM 服务区。是指移动台可获得服务的区域，这些服务区具有完全一致的 MS－BS 接口。一个服务区可包含一个或多个公用陆地移动通信网(PLMN)，从地域上说，可对应一个国家或多个国家，也可以是一个国家的一部分。

(2) PLMN。可由一个或多个移动交换中心组成，该区具有共同的编号制度和路由计划，其网路与公众交换电话网互连，形成整个地区或国家规模的通信网。

(3) MSC 区。是指 MSC 所覆盖的服务区，提供信号交换功能及和系统内其他功能的连接，从位置上看，包含多个位置区。

(4) 位置区。一般由若干个基站区组成，移动台在位置区内移动时无须进行位置的登记或更新。

(5) 基站区。指基站提供服务的所有的区域，也叫作小区。

(6) 扇区。当基站收发天线采用定向天线时，基站区可分为若干个扇区；若采用 120°定向天线，一个小区分为 3 个扇区；若为 60°，则为 6 个扇区。

GSM 移动通信网在整个服务区内，具有控制、交换功能，以实现位置更新、呼叫接续、越区切换及漫游功能。而实现这些功能和各类区域的具体划分密切相关。

2. GSM 系统中的各种识别号码

GSM 网络比较复杂，包括无线和有线信道，移动用户之间或与其他多种网络的用户都

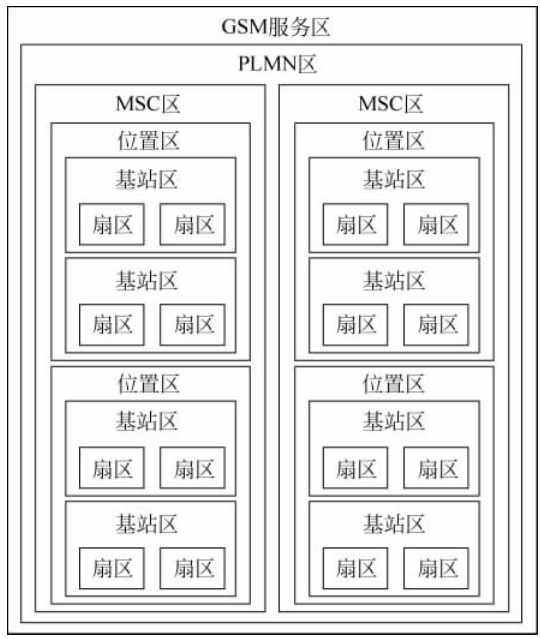

图 3-2　GSM 的区域定义

能够建立连接，例如市话网用户，综合业务数字网用户，公用数据网，因此要想能准确无误地呼叫连接上某个移动用户，一个移动用户就必须具备多种识别号码，用于识别不同的移动用户和移动设备。下面具体介绍一下各种号码。

1）MSISDN（移动台国际身份号码）

MSISDN 号码是在公共电话网交换网络编号计划中，唯一能识别移动用户的号码。

根据 CCITT（国际电报电话咨询委员会）的建议，MSISDN 由以下部分组成（见图 3-3），即

$$\text{MSISDN} = \text{CC} + \text{NDC} + \text{SN} \tag{3-1}$$

其中，CC（国家码）表示用户注册在哪个国家（中国为 86）；NDC（国内目的码）是国家特定的 PLMN 所确定的目标国家码；SN（用户号码）是由运营者自由授予的用户号码。

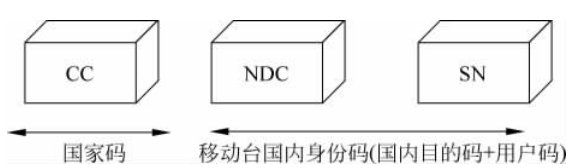

图 3-3　移动台国际身份号码的格式

若在以上号码中用国家码 CC 去除，就成了移动台的国内身份号码，也就是我们日常所说的“手机号码”。目前，我国 GSM 的国内身份号码为 11 位，每个 GSM 的网络均分配一个国内目的码（NDC），也可以要求分配两个以上的 NDC 号。MSISDN 的号长是可变的（取决于网络结构与编号计划），不包括字冠，最长可以达到 15 位。

NDC 包括接入号 N1N2N3，用于识别网络；SN 的前 4 位为 HLR 的识别号 H1H2H3H4（H1H2H3 全国统一分配，H4 省内分配），表示用户归属的 HLR，也表示移动业务本地网号。

2) IMSI(国际移动用户识别码)

国际上为唯一识别一个移动用户所分配的号码,此码在所有位置都是有效的,在呼叫建立和位置更新时需要使用 IMSI。IMSI 总共不超过 15 位,其结构如图 3-4 所示。

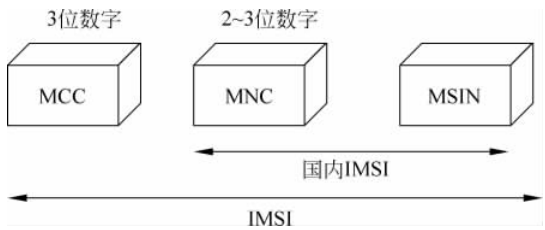

图 3-4　国际移动用户识别码的格式

MCC(移动国家码):表示移动用户驻在国,共 3 位,中国为 460。

MNC(移动网络码):即移动用户所属的 PLMN 网号,一般 2 位,中国移动为 00,中国联通为 01。

MSIN(移动用户标识):共有 10 位,用来识别某一移动通信网中的移动用户。

IMSI 组成关系式为

$$\text{IMSI} = \text{MCC} + \text{MNC} + \text{MSIN} \tag{3-2}$$

从式(3-2)中可以看出 IMSI 在 MSIN 号码前加了 MCC,以便于区别出每个用户来自的国家,因此可以实现国际漫游。

3) MSRN(移动台漫游号码)

这是针对移动台的移动特性所使用的号码。每次呼叫发生时,HLR 知道目前用户处在哪一个 MSC/VLR 服务区内,为了向接口交换机提供一个本次路由选择的临时号码,HLR 请当前的 MSC/VLR 分配一个移动台漫游号码(MSRN)给被叫用户,并将此号码传给 HLR;HLR 再将此号码转发给接口交换机,就能根据此号码将主叫用户接至所在的 MSC/VLR。

漫游号码的组成格式与移动台国际(或国内)ISDN 号码相同。另外,当进行 MSC 交换局间切换时为选择路由切换目的地 MSC(即目标 MSC)临时分配给来访移动用户一个切换号码(HON),HON 格式等同 MSRN,只不过 MSRN 后 3 位为 000～499,HON 后 3 位为 500～900。

4) TMSI(临时移动用户识别码)

为了保证移动用户识别码的安全性,在无线信道中需传输移动用户识别码时,一般用 TMSI 来代替 IMSI,这样就不会把用户的 IMSI 暴露给非法用户。TMSI 是由 VLR 分配的,与 IMSI 之间可按一定的算法互相转换。TMSI 可用于位置更新、切换、呼叫、寻呼等业务,并且在每次鉴权成功后都被重新分配,这样可以有效地防止他人窃取用户的通信内容,或非法盗取合法用户的 IMSI。

TMSI 的结构可由运营商自行决定,长度不超过 4 个字节。

5) IMEI(国际移动台设备识别码)

IMEI 是由 15 位数字组成的"电子串号"(见图 3-5),它与每台手机一一对应,而且该码是全球范围内唯一的。每一台手机在组装完成后都将被赋予全球唯一的一个号码,这个号

码从生产到交付使用都将被制造生产的厂商所记录，移动设备输入“＊＃06＃”也可显示该号码。

该码作为移动台设备的标志，可用于监控被窃或无效的移动。

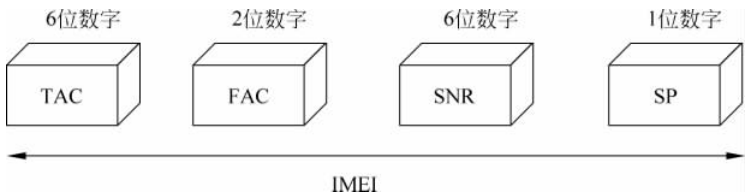

图 3-5　国际移动台设备识别码的格式

IMEI 的组成关系式为

$$\text{IMEI} = \text{TAC} + \text{FAC} + \text{SNR} + \text{SP} \tag{3-3}$$

TAC(型号核准号码)：一般代表机型。

FAC(最后装配号)：一般代表装配厂家号码。

SNR(串号)：一般代表生产顺序号。

SP(Spare)：通常是“0”，为检验码，目前暂备用。

6) LAI(位置区识别码)

LAI 用于移动用户的位置更新，其结构组成如图 3-6 所示。

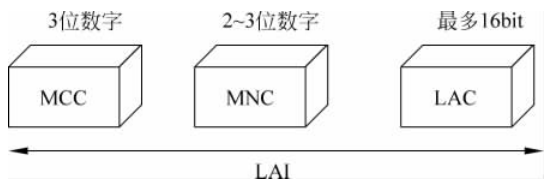

图 3-6　位置区识别码的格式

LAI 的组成关系式为

$$\text{LAI} = \text{MCC} + \text{MNC} + \text{LAC} \tag{3-4}$$

MCC：移动国家号，与 IMSI 中的 MCC 一样具有 3 个数字，用于识别一个国家，中国为 460。

MNC：移动网号，识别国内 GSM 网，与 IMSI 中的 MNC 的值是一样的。

LAC(位置区号码)：识别一个 GSM 网中的位置区。LAC 最大长度为 16bit，理论上可以在一个 GSM/VLR 内定义 65 536 个位置区。

7) CGI(小区全球识别码)

用于识别一个位置区的小区。CGI 组成如图 3-7 所示。

CGI 的组成关系式为

$$\text{CGI} = \text{MCC} + \text{MNC} + \text{LAC} + \text{CI} \tag{3-5}$$

CI：是小区识别代码。

MCC、MNC 和 LAC 与位置区识别码中的是一样的含义。

8) BSIC(基站识别码)

BSIC 用于识别相邻的、具有相同载频的不同基站，特别是用于区别不同国家的边界地

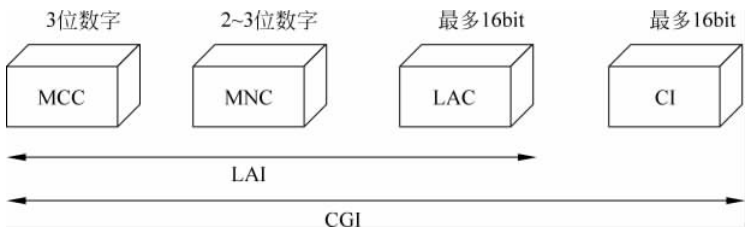

图 3-7　小区全球识别码的格式

区采用相同载频且相邻的基站，BSIC 是一个 6bit 号码，其组成如图 3-8 所示。

BGIC 的关系式为

$$\text{BSIC} = \text{NCC} + \text{BCC} \tag{3-6}$$

NCC(网络色码)：用于识别 GSM 移动网。

BCC(基站色码)：用于识别基站。

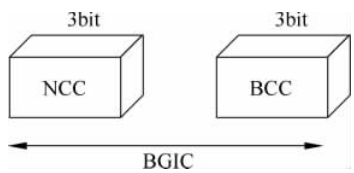

图 3-8　基站识别码的格式

3. GSM 业务

GSM 系统定义的所有业务是建立在综合业务数字网(ISDN)概念基础上，并考虑移动特点进行了必要修改。GSM 业务主要包含两类，即基本业务和补充业务，其中基本业务按功能又可分为电信业务和承载业务，是独立的通信业务。

(1) 电信业务，主要指包括电话、紧急呼叫、传真和短消息服务等。

(2) 承载业务，不仅支持语音业务，还支持数据业务。

(3) 补充业务，是对基本业务的改进和补充，非单独的，需和基本业务一起提供服务。主要包括呼叫前转、呼叫限制、呼叫等待、会议电话和计费通知等。

3.2　GSM 的空中接口

在 GSM 系统中，其空中接口就是指 MS 和 BSS 之间的接口，又称 Um 接口。空中接口是借助无线电波传递信息的，连接的用户众多，而且随着用户终端的多样性和环境的复杂多变，空中接口呈现广泛性和多样性。

3.2.1　技术参数

GSM 系统是 FDMA 和 TDMA 混合接入方式，FDMA 是指在一定的频段上分配 n 个载波频率，TDMA 是指在一个载频上分为 8 个时隙。GSM 系统主要有 GSM900、GSM1800 和 GSM1900 3 类，都是 FDD 工作方式，目前我国主要的两大 GSM 系统为 GSM900 及 GSM1800，其特性如表 3-1 所示。

表 3-1 我国 GSM 系统的主要技术参数

特　　性	GSM900	GSM1800
频段(MHz)	890～915(上行) 935～960(下行)	1710～1785(上行) 1805～1880(下行)
工作频带(MHz)	25	75
每帧 TDMA 的时隙数	8	8
上下行隔离(MHz)	45	95
频道间隔(kHz)	200	200
频道数	124	374

GSM 系统在上下行频段安排中,上行频段频率低于下行频段,主要是考虑到上下不对称的传输能力。频率越高,覆盖同样的范围需要更大的发射功率,而基站能比移动台提供更大的发射功率,所以采取上述频段安排方式。

3.2.2 空中接口的物理结构

1. 空中接口的帧结构

在 GSM 系统中,每个载频,在时间上被定义为一个个 TDMA 帧(简称为帧)相连接,每个 TDMA 帧包括 8 个时隙(TS0～TS7),所有 TDMA 帧中同号时隙提供一个物理信道,如图 3-9 所示。空中的传输速率为 270.833Kbps,每个时隙占用 576.9μs,相当于承载 156.25bit 的数据,一帧的时间为 4.615ms。

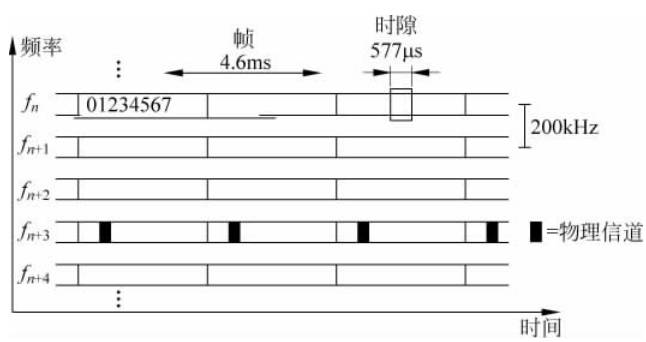

图 3-9 GSM 的 TDMA/FDMA 接入方式

复帧结构如图 3-10 所示,包括 26 帧和 51 帧两种。

(1) 26 帧的复帧,包含 26 个 TDMA 帧,持续时长为 120ms,用于传输业务信息。

(2) 51 帧的复帧,包括 51 个 TDMA 帧,持续时长为 235.385ms,用于传输控制信息。

超帧主要包括两类,即 26 个 51 帧的复帧和 51 个 26 帧的复帧组成的结构;一个超高帧包含 2048 个超帧,所包含的帧数为 2048×51×26=2 715 648。帧的编号以超高帧为周期,从 0～2 715 647。

通常,上行 TDMA 帧比下行 TDMA 帧固定落后 3 个时隙,这样方便移动台利用这段时间进行帧调整以及对收发信机进行调谐和转换。

2. 突发脉冲序列

GSM 系统空中接口的时隙上有 4 种不同功能的突发脉冲,即普通突发脉冲、频率校正

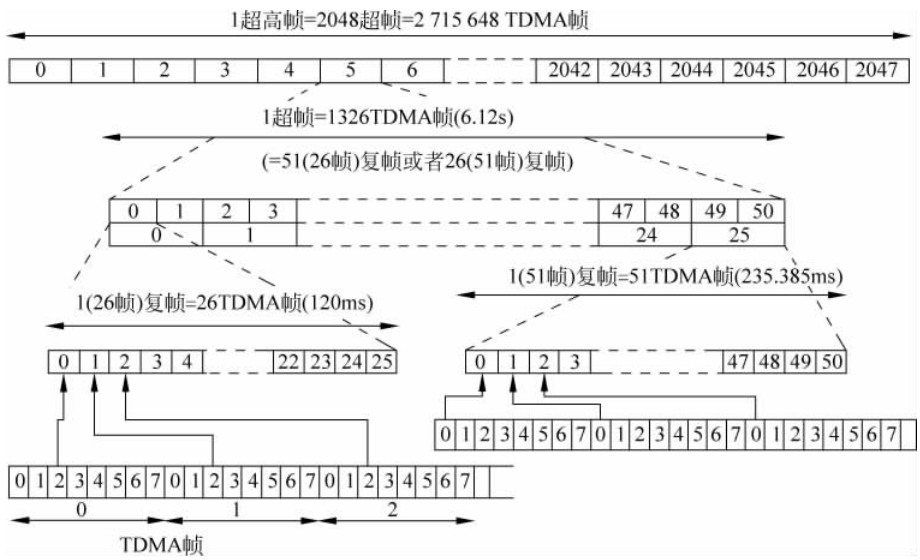

图 3-10　GSM 系统的各种帧及时隙的格式

突发脉冲、同步突发脉冲和接入突发脉冲，其格式如图 3-11 所示。

（1）普通突发脉冲：携带业务信息和控制信息。

（2）频率校正突发脉冲：携带频率校正信息。

（3）同步突发脉冲：携带系统的同步信息。

（4）接入突发脉冲：携带随机接入信息。

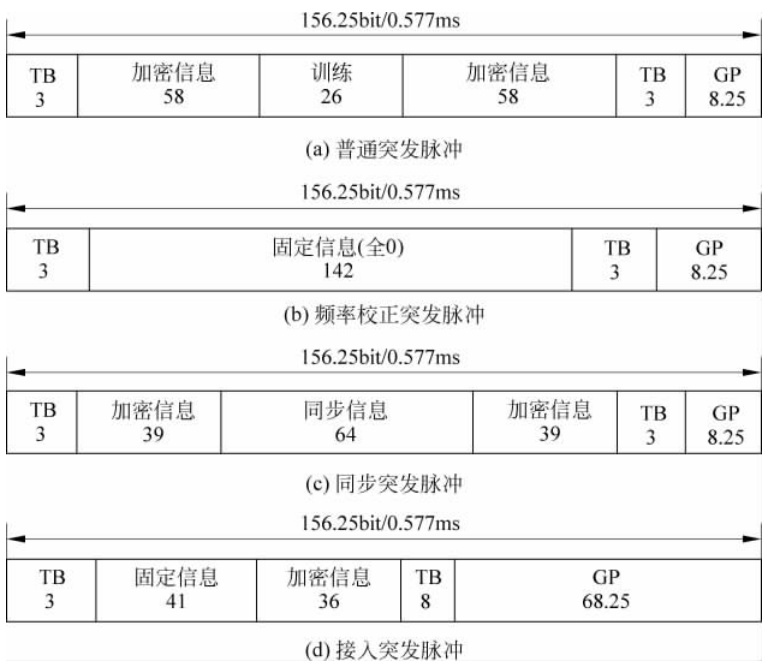

图 3-11　4 种不同功能突发序列的格式

图中 TB 是结尾标志，总是“000”；GP 是保护时间，防止由于定时误差而造成突发脉冲间的重叠。常规突发序列中，在两段信息码之间插入了 26bit 的训练序列，用作自适应均衡器的训练序列，以消除多径效应产生的码间干扰。GSM 系统共有 8 种训练序列，可分别用于邻近的同频小区，由于选择了互相关系数很小的训练序列，因此接收端很容易辨别各自所需的训练序列，产生信道模型，作为时延补偿的参照。

3. GSM 信道

1）GSM 信道分类

GSM 信道分为物理信道和逻辑信道两种。

GSM 系统需提供不同业务服务，因此要在物理信道上安排相应的逻辑信道。突发脉冲以不同的信息格式携带不同的信息就构成了不同的逻辑信道，因此在一个物理信道上可以承载多种逻辑信道。GSM 系统具体的逻辑信道见图 3-12，主要分为控制信道和业务信道两大类。各逻辑信道的功能见表 3-2。

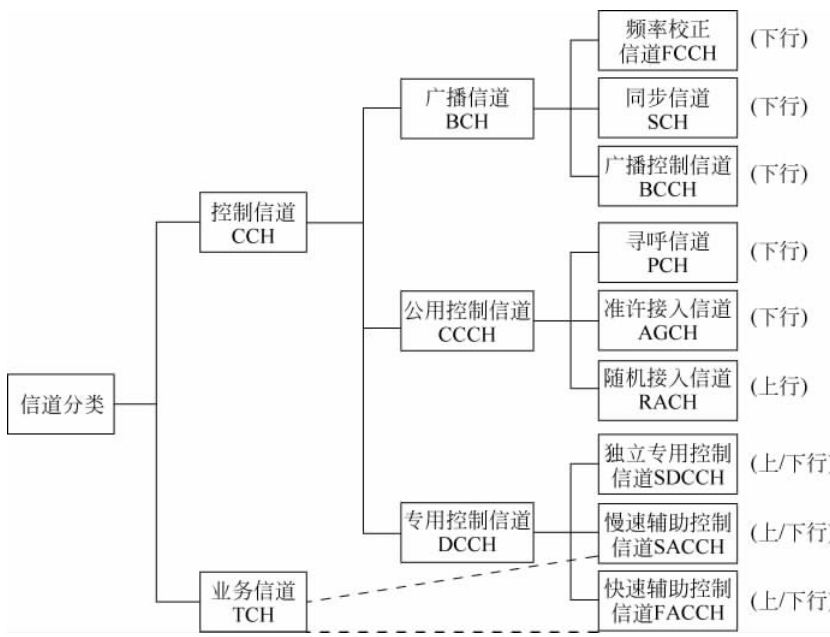

图 3-12　GSM 系统的逻辑信道分类

表 3-2　GSM 系统各逻辑信道的功能表

逻辑信道	突发脉冲方式	方向	功　能
频率校正信道	频率校正	BS→MS	广播用于校正终端频率的信息
同步信道	同步	BS→MS	广播帧同步和基站识别码信息
广播控制信道	普通	BS→MS	广播一般信息
寻呼信道	普通	BS→MS	传输基站寻呼移动台信息
随机接入信道	接入	BS←MS	用于终端随机提出入网申请，即请求分配一个 SDCCH

续表

逻辑信道	突发脉冲方式	方向	功　能
准许接入信道	普通	BS→MS	用于基站对终端的入网请求作出应答，即分配一个 SDCCH 或 TCH
独立专用控制信道	普通	BS↔MS	用于分配 TCH 之前传送信息
慢速辅助控制信道	普通	BS↔MS	伴随 TCH 或 SDCCH，双向传输信息
快速辅助控制信道	普通	BS↔MS	传输与 SDCCH 相同的信息，只是在没有分配 SDCCH 时才使用
业务信道	普通	BS↔MS	主要传输数字话音或数据，其次还可传输少量的控制信息

2）逻辑信道到物理信道的映射

用于呼叫处理的各种逻辑信道和信令，实际上是以突发脉冲的形式在物理信道上传递的。由前面的分析知道，GSM 的逻辑信道数远多于 1 个载频所提供的 8 个物理信道，为确保信道利用率，也不可能用 1 个物理信道承载 1 个逻辑信道（业务信道除外），因此，有必要讨论一下逻辑信道是怎样映射到物理信道上去的。

假设一个小区有 n 个载频，为 F_0、F_1、F_2、F_3、…、F_{n-1}，时隙数为 TS0、TS1、…、TS7。通常，将 F_0 载频中的 TS0 用作将公共信道承载广播信道和公用控制信道，如 BCCH、FCCH、SCH、PCH、AGCH 及 RACH 复用；TS1 承载专用控制信道，如 SDCCH、SACCH 复用。F_0 的 TS2…TS7，及 F_1…F_{n-1} 中的时隙都用来承载 TCH。在小容量地区和建站初期，也可以考虑采用 F_0 载频中的 TS0 承载全部控制信道，包括广播信道、公用控制信道和专用控制信道，这里只讨论前一种情况。

（1）控制信道的映射。物理信道采用 51 帧组成的复帧来传输控制信息，控制信道随突发脉冲不同，其组合的方式不同，并且上行传输和下行传输也不一样。

通常，BCH 和 CCCH 主要映射在 F_0 的 TS0 上，其在下行链路上的映射方式如图 3-13 所示。

图 3-13　BCH 和 CCCH 在下行链路上的复用方式

BCH 和 CCCH 共占用 51 个 TS0 时隙，当出现空闲帧时复帧结束，虽然只占用了每帧的 TS0 时隙，所以序列是以 51 个 TDMA 帧为一个周期。

在没有寻呼或接入信息时，基站也在 F_0 发射 F、S 和 B，便于移动台能测试基站信号的强度，能及时调整使用哪个小区，只是此时 C（CCCH）用空位突发脉冲代替。

对于上行链路，F_0 上的 TS0 只用于移动台的接入，51 个 TDMA 帧均映射 RACH，其

关系如图 3-14 所示。

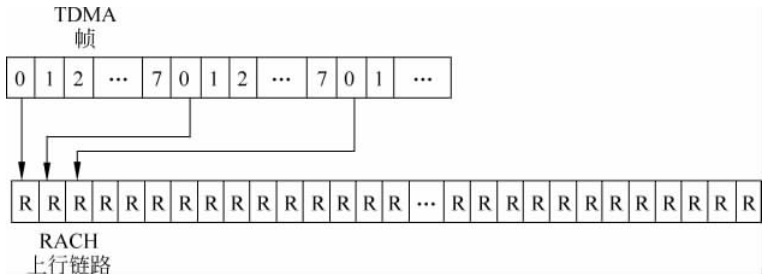

图 3-14　上行链路中，TS0 上 RACH 的复用

载频 F_0 上的 TS1 时隙用于将 DCCH 映射到物理信道上，其在下行链路上的映射关系如图 3-15 所示。

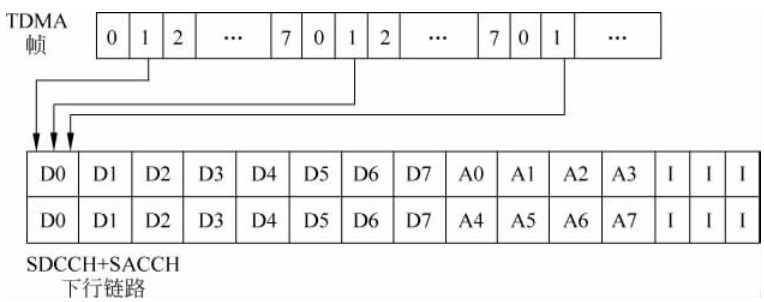

图 3-15　SDCCH 和 SACCH 在 TS1 上的复用

下行链路占用 102 个 TS1 时隙，时间上占了 102 个 TDMA 帧。由于呼叫建立和入网登记时比特率较低，所以可在 1 个时隙上放置 8 个专用控制信道，以提高时隙的利用率。

D0～D7 代表 SDCCH，其中每个 Dx 占 8 个时隙，只在移动台建立呼叫的时候使用，当移动台转移到业务信道（TCH）上开始通话或登记完后，Dx 就被释放用于其他的移动台。

A0～A7 代表 SACCH，每个 Ax 占用 4 个时隙，主要用于传输必要的控制信息。

用于专用控制信道时，上行链路 F_0 上的 TS1 与下行链路 F_0 上的 TS1 组织结构是相同的，只是它们在时间上有一个偏差。

（2）业务信道的映射。F_0 的 TS2……TS7，及 $F_1 \cdots F_{n-1}$ 中的时隙都用作 TCH。物理信道采用 26 帧组成的复帧来传输业务信息。TCH 到物理信道的映射如图 3-16 所示。

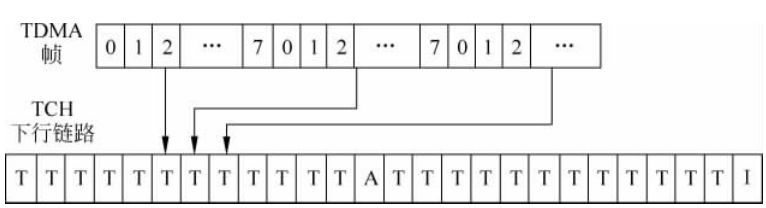

图 3-16　TCH 的复用方式

图中只给了 TS2 时隙的复用关系，其中 T 代表 TCH，主要用于传输数据和语音；A 代表 SACCH，传输控制信令；I 为 IDLE 空闲帧。

4. GSM 中的信道特性和抗衰落技术

1）信道特性

在移动通信中，经过处理的话音信号都是借助于无线信道来传播交换的，但是由于移动通信信道是一种极其复杂的时变信道，电波通过移动无线信道后，信号在时域或频域出现不同程度的交叠，从而产生了衰落失真，无线传播中出现的衰落特性主要有 3 种。

（1）多径衰落。在无线通信领域，多径指无线电信号从发射天线经过多个路径抵达接收天线的传播现象。大气层对电波的散射、电离层对电波的反射和折射以及山峦、建筑等地表物体对电波的反射都会造成多径传播。多径会导致信号的衰落和相移，例如多径传输会带来额外的路径损耗，导致信号传输的突发性错误和码间干扰。

（2）阴影衰落。移动通信中，阴影衰落是由障碍物阻挡造成的阴影效应，接收信号强度下降，但该强度值会随地理改变缓慢变化，又称慢衰落。

（3）时延扩展。移动信道的多径环境引起的信号多径衰落可从时域角度方面进行描述：各路径长度不同使得信号到达时间不同，基站发送一个脉冲信号，则接收信号中不仅含有该信号，还包含有它的各个时延信号，这种由于多径效应使接收信号脉冲宽度扩展的现象，称为时延扩展。时延扩展会导致接收信号中一个码元的扩展到其他的码元周期，引起码间干扰。

2）抗衰落技术

GSM 系统采用了多种抗衰落技术来提高系统的传输性能，主要的措施如下：

（1）信道编码。信道编码的本质是为了提高通信的可靠性，其过程是通过某种约定在源数据码流中加插一些码元，接收端解码时利用这些冗余信息检测误码并纠正错误，从而达到改善传输质量的目的。在 GSM 系统中，将 20ms 语音帧的信息比特分为两类，第一类是 182bit 对差错敏感的信息码；第二类是对差错不敏感的 78bit 信息码。对第二类比特不进行信道编码，对第一类比特加入奇偶校验比特和尾比特，再使用(2,1,5)结构的卷积编码器进行编码。

（2）交织编码。交织编码的目的是把一个较长的突发差错离散成随机差错，再用纠正随机差错的编码技术消除随机差错。交织深度越大，则离散度越大，抗突发差错能力也就越强，但交织深度越大，交织编码处理时间越长，从而造成数据传输时延增大，也就是说，交织编码是以时间为代价的，因此，交织编码属于时间隐分集。GSM 系统的交织跨度为 40ms，使用 8×114 的交织矩阵。

（3）均衡和分集接收。均衡是指对信道特性的均衡，即接收端的均衡器产生与信道相反的特性，用来抵消信道的时变多径传播特性引起的码间干扰。GSM 的实际传输带宽为 200kHz，高于信道的相干带宽(150kHz 左右)，因此，GSM 系统需要采用均衡器去除频率选择性衰落的影响，均衡的算法有很多种，目前在 GSM 中使用最多的是 Viterbi 均衡算法。

分集接收是抗衰落的一种有效措施，GSM 系统可选多天线接收(基站)和多径 RAKE 接收(手机)两种分集接收方式。

（4）跳频技术。跳频是把一个宽频段分成若干个频率间隔(称为频道或频隙)，由一个伪随机序列控制发射机在某一特定的驻留时间发送信号的载波频率。跳频分为快跳频和慢跳频，在 GSM 中采用的是慢跳频技术，因为在 GSM 中要求在整个突发脉冲期间传输的频隙保持不变，所以 GSM 每隔 4.615ms 改变一次载波频率，图 3-17 给出了 GSM 跳频示意图。

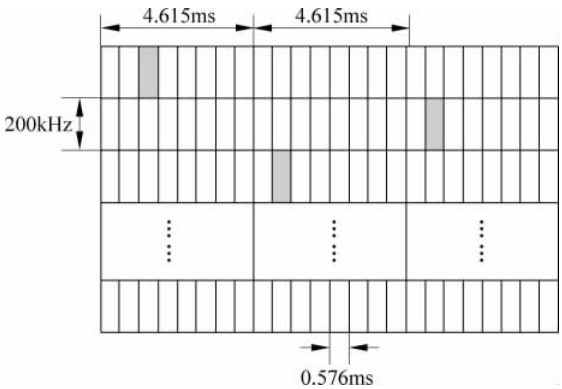

图 3-17　GSM 系统的跳频示意图

跳频技术与直接序列扩频技术完全不同，是另外一种意义上的扩频。跳频的载频受一个伪随机码的控制，在其工作带宽范围内，其频率合成器按 PN 码的随机规律不断改变频率，这样可以将连续的同频干扰转变为间断的同频干扰，减少瑞利衰落的相关性，所以采用跳频技术可以进一步增强系统的抗干扰能力。

跳频虽然是 GSM 系统的可选项，但在实际运营系统中得到了广泛的应用。需要说明的是，BCCH 和 CCCH 信道不使用跳频技术。

(5) 语音激活与功率控制。GSM 系统中采用语音激活和功率控制技术可以有效地减少同信道的干扰。

语音激活技术也称为间断传输(DTx)技术，其基本原则是只在有话音信号时才打开发射机，其余时间都是关闭的，一方面可以减少干扰，提高了系统容量；另一方面减少移动台的电能消耗。

功率控制的目的是保证通信质量良好的前提下，使发射机的发射功率最小，平均功率的减少就会相应地降低同信道干扰。移动台在小区内移动时，当它离基站较近时，就降低发射功率，以减少对其他用户的干扰，当它离基站较远时，就相应地增加功率，来补偿远距离的路径衰耗。

GSM 系统总的功率控制范围为 30dB，调节的步长为 2dB，一共有 16 个等级，每改变一个等级需要 60ms。

3.3　GSM 系统控制与管理

GSM 系统是一个庞大的通信网络，结构复杂且功能繁多，为了保证移动用户能够方便、快捷、安全地通信，这就需要对各种设备和服务进行有效的控制和管理，其中控制和管理的主要内容有以下几个方面。

3.3.1　位置的登记和更新

GSM 通信系统的整个网络可以分为不同的位置区，并有相应位置区标志号，对于其中的移动用户，存储移动台位置信息的是 VLR 和 HLR。VLR 主要存放用户的临时位置信息，而 HLR 中存放着用户的基本信息，是永久性的，还有从 VLR 得到的临时数据。

对于新入网的用户，首先需通过 MSC 在相应的 HLR 中登记注册，移动台在移动过程中引起位置变化的信息需在 VLR 登记，这样便于通信网对移动台的监控。

移动用户位置信息的更新主要存在两种情况下，第一种情况，当移动用户从一个网络服务区到另外一个网络服务区，移动台将向新区中的网络发送更新请求信息，网络端将移动台注册在新区的 VLR 中，同时 HLR 也随着 VLR 的信息进行更新，并通知旧区中的 VLR 删除用户的有关信息；第二种情况，移动台周期性的更新。当网络在一定的时间内没有收到移动台的任何信息时，那么网络可能无法获知移动台的状况，为了随时掌控移动台的信息，系统就要求移动台在一定的时间内登记一次。

3.3.2　越区切换

所谓越区切换是指移动用户在通话期间从一个小区移动到另外一个小区，网络能实时控制将移动台从原来的信道切换到新小区的某个信道，并且保持通话不间断。在 GSM 系统中对切换的控制是由 BS 和 MS 相互检测决定的。一般引起切换的原因有两个，一个原因是当移动台的信号强度或质量下降到系统规定的参数以下，移动台将被切换到信号较强的小区；另一个原因是由于某小区的业务信道被全部占用或几乎全被占用，那么移动台将被切换到有空闲业务信道的相邻小区，不过前者是由移动台发起的，后者是由系统发起的。

越区切换主要分为 3 大类：

(1) 同一 BSC 控制区内不同小区之间的切换，这种切换是最简单的。由 MS 发送信号强度报告，BSC 发出切换命令，MS 切换到新 TCH 信道后告知 BSC，再由 BSC 通知 MSC，即可完成切换。切换过程如图 3-18 所示。

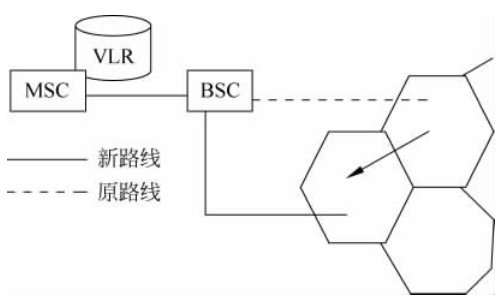

图 3-18　同一 BSC 控制区内不同小区之间的切换过程

(2) 同一 MSC/VLR 内不同 BSC 控制小区间的切换。要完成此类切换，需有网络的参与。MS 向原 BSC 发送数据，再由 BSC 向 MSC 发送切换请求，待 MSC 与新区的 BSC 和 BTS 建立链路，并给 MS 分配新的业务信道后，再命令 MS 切换到新区中，切换成功后 MSC 向原 BSC 发出“清除命令”，并释放原占用的信道，呼叫完成后还需要进行位置的更新。这一类切换的过程如图 3-19 所示。

(3) 不同 MSC/VLR 控制的小区间的切换。这是一种最复杂的切换，因为移动台从一个 MSC 切换到另一个 MSC 中，需要进行很多次信息的传递。整个切换过程如图 3-20 所示。

当移动台检测到所在区的信号强度很弱，而邻区的信号较强时，即可通过本区的 BSC_1

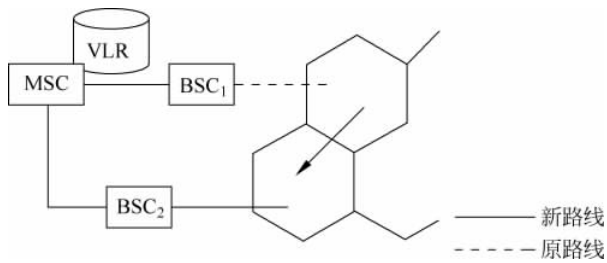

图 3-19　同一 MSC/VLR 内不同 BSC 控制小区间的切换过程

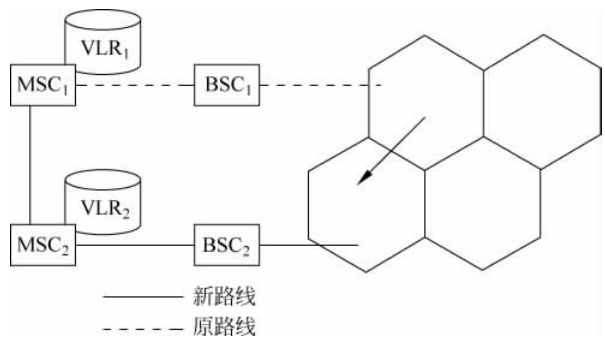

图 3-20　不同 MSC/VLR 控制的小区间的切换

向 MSC_1 发送切换区域请求。接着由 MSC_1 向另一新的 MSC_2 转发切换请求，此请求信息中包含该 MS 的标志号和目标 BSC_2 的标志号。MSC_2 收到请求后通知 VLR_2 给 MS 分配“切换号码”和“无线信道”，然后向 MSC_1 回复“切换号码”，如果无空闲信道，那么 MSC_2 通知 MSC_1 结束此次切换。

MSC_1 收到“切换号码”后，在 MSC_1 和 MSC_2 之间建立“地面有线链路”。

MSC_2 向 BSC_2 发出“切换命令”，MSC_1 向 MS 发送“切换命令”，MS 收到命令后就切换到新的业务信道上，而 BSC_2 向 MSC_2 发送“切换证实”信息，MSC_2 收到信息后就通知 MSC_1 结束切换，MSC_1 释放 MS 原来占用的信道。

3.3.3　鉴权与加密

移动通信网络受到的安全威胁主要来自两方面：一是空中接口，包括窃听、假冒、重放、跟踪、数据完整性侵犯和业务流分析；其次是网络和数据库，包括网络内部攻击、数据库非法访问和对业务的否认。后者是所有通信网络面临的问题，解决措施是相同的；前者是因为移动网络收发无线电波引起的。通常，无线传输比固定线路传输更易受到窃听和欺骗，所以移动通信系统首先必须解决两个问题：第一，对用户进行认证，防止未注册用户的欺骗性接入；第二，对无线路径加密，以防止第三方窃听。为了保证用户的安全通信，GSM 系统采用了鉴权和加密技术来保护网络的安全。鉴权可以确认用户的合法性，防止非法用户的“入侵”，加密是防止第三者的窃听，保护用户的私密性。

GSM 系统中，为鉴权和加密提供了 3 种算法，即 A3、A5 和 A8 算法，鉴权中心（AUC）为鉴权和加密提供了一个 3 参数组，即随机数（RAND）、符号响应（SRES）和加密密钥

(K_c),其产生过程如图 3-21 所示。对于新入网的用户,系统为其分配一个 128bit 的鉴权密钥 K_i 和一个 15 位的 IMSI,均存储在 AUC 和 SIM 卡中。在 HLR 的请求下,AUC 中首先产生一个 128bit 的随机数(RAND);然后通过鉴权算法 A3 和加密算法 A8,用 RAND 和 K_i 分别计算出 32bit 的 SRES 和 64bit 的 Kc;最后将 RAND、SRES 和 Kc 送至 HLR。

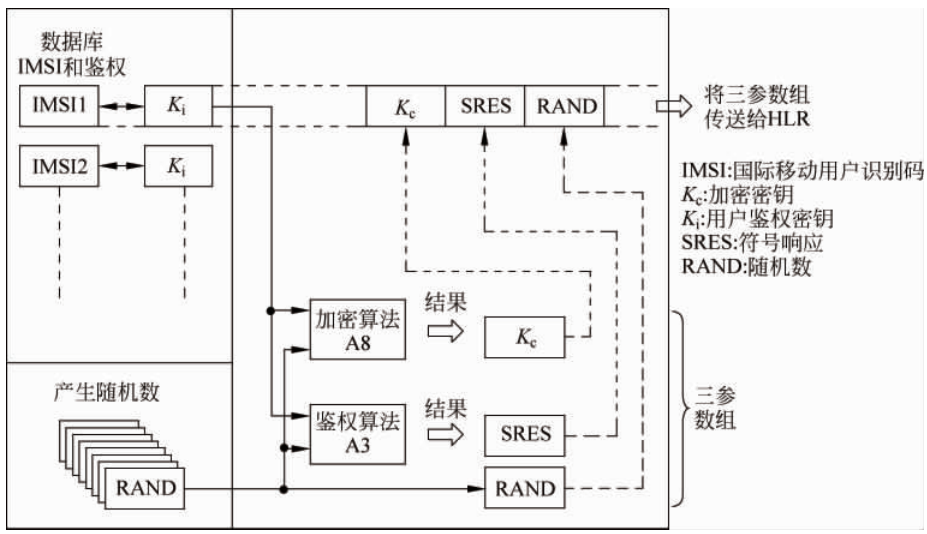

图 3-21　AUC 中产生 3 参数组的过程

将 GSM 系统采用的安全措施描述如下。

1. 鉴权

移动台的主叫和被叫过程中都存在鉴权流程,当 MS 请求入网时,首先需进行鉴权,VLR 通过 BSS 向 MS 发送 RAND,MS 使用该 RAND 和 K_i 通过算法 A3 计算出 SRES,然后把 SRES 回送给 VLR,与网络端的 SRES 比较,验证其合法性。GSM 系统中,IMSI 和 K_i 一起构成了网络借以鉴别用户的重要“身份证件”,网络对用户的认证协议采用典型的“问-答”机制。

2. 加密

为确保 BTS 和 MS 之间交换信息(包括信令和数据)的私密性,在此过程中采用了一个加密程序。在鉴权计算 SRES 的同时,MS 利用算法 A8 计算出了 K_c,加密开始时,根据 MSC/VLR 发出的加密模式命令,在 MS 侧,将 K_c、TDMA 帧号通过加密算法 A5,对用户信 s 息数据加密,并将加密信息回送到 BTS 中,BTS 再根据帧号和 K_c,利用 A5 算法将加密信息解密,如无错误则告知 MSC/VLR。GSM 系统对上下行传输信息进行双向加密,过程如图 3-22 所示,22bit 的 TDMA 帧号和 64bit 的 K_c 通过 A5 算法产生两个 114bit 的块 BLOCK1 和 BLOCK2,BLOCK1 与发送出去的 114bit 数据相异或以加密,BLOCK2 与接收到的 114bit 数据相异或以解密。

3. 移动设备识别

移动设备识别的目的是确保系统中使用的移动设备不是盗用或非法的设备,对于每个移动台,都有唯一的一个移动设备识别码(IMEI),在 EIR 中存储了所有的移动台的 IMEI。EIR 中定义了 3 种设备清单:

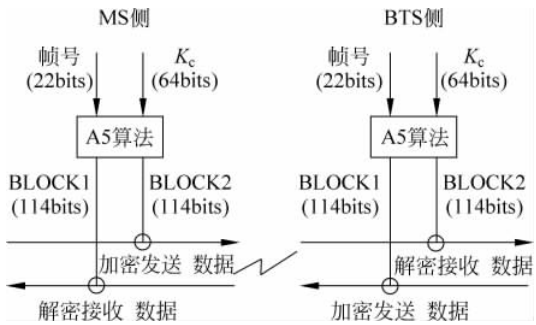

图 3-22 GSM 加密模式传输

(1) 白名单。合法的移动设备识别号。

(2) 灰名单。是否允许使用由运营者决定,例如包括有故障或未经型号认证的移动设备识别号。

(3) 黑名单。被禁止使用的移动设备识别号。

当 MS 发出呼叫请求时,MSC/VLR 要求其发送 IMEI,获得 MS 的 IMEI 后,将 IMEI 发送给 EIR,进行名单核对,EIR 将鉴定的结果传送给 MSC/VLR,由其决定是否允许 MS 建立呼叫。

4. 国际用户识别码(IMSI)保密

为了防止他人非法监听和盗用 IMSI,当 MS 向系统请求某种服务,例如位置的更新、呼叫建立或业务激活,需要在无线链路上传输 IMSI 时,MSC/VLR 将给 MS 分配一个临时的 TMSI 代替 IMSI,仅在位置更新错误或 MS 得不到 TMSI 时才使用 IMSI。IMSI 是唯一且不变的,而 TMSI 是不断更新的,这种更新在每一次移动性管理过程都发生,因此确保了 IMSI 的安全性。

3.4 IS-95 CDMA 系统概述

IS-95 CDMA 系统是由美国高通公司设计并于 1995 年投入运营的窄带 CDMA 系统,美国通信工业协会(TIA)基于该窄带 CDMA 系统颁布了 IS-95 CDMA 标准系统,因此,它与 GSM 都是第二代移动通信的主要系统。

IS-95 标准全称是“双模式宽带扩频蜂窝系统的移动台-基站兼容标准”,IS-95 标准提出了“双模系统”,该系统可以兼容模拟和数字操作,从而易于模拟蜂窝系统和数字系统之间的转换。

IS-95 CDMA 系统由 3 个独立的子系统组成,即移动台(MS)、基站子系统(BSS)和网络交换子系统(NSS),如图 3-23 所示。总体来看,其网络结构和 GSM 是相近的。

移动台是双模移动台,与 AMPS 模拟 FDMA 系统兼容。基站子系统是设于某一地点、服务于一个或几个蜂窝小区的全部无线设备及无线信道控制设备的总称,主要包括集中基站控制器(CBSC)和若干个基站收发信机(BTS),CBSC 由码转换器(XC)和移动管理器(MM)组成。

网络交换子系统包括移动交换中心(MSC)、归属位置寄存器(HLR)、访问位置寄存器

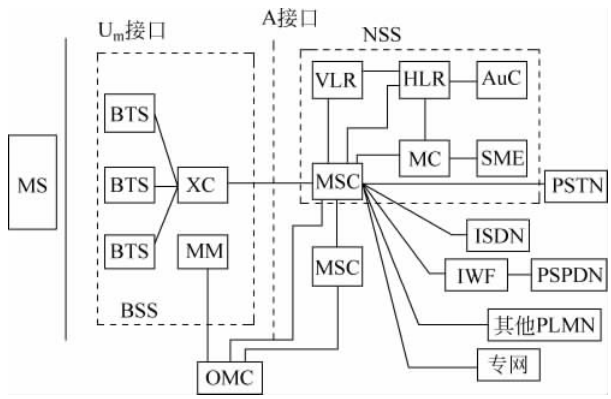

图 3-23　IS-95 CDMA 系统网络结构

(VLR)、鉴权中心(AuC)、消息中心(MC)、短消息实体(SME)和操作维护中心(OMC)。MSC 是完成对位于它所服务的区域中的移动台进行控制、交换的功能实体,也是蜂窝网与其他公用交换网或其他 MSC 之间的用户话务的自动设备。VLR 是 MSC 作为检索信息用的位置登记器,例如:它可以处理发至或来自一个拜访用户的呼叫信息。HLR 是为了记录注册用户身份特征的位置登记器,登记的内容是用户信息,例如 ESN、DN、IMSI(MIN)、服务项目信息、当前位置、批准有效时间段等。AuC 是一个管理与移动台相关的鉴权信息的功能实体。MC 是一个存储和传送信息的实体。SME 是一个合成和分解短消息的实体。

该系统是一种直接序列扩频 CDMA 系统,它允许同一小区内的用户使用相同的无线信道,完全取消了对频率规划的要求。工作频段为 1.2288MHz,可提供 64 个码道。为了克服多径效应,采用了 RAKE 接收、交织和天线分集技术。CDMA 系统具有频率资源共享的特点,具有越区软切换能力。为了减少远近效应,采用了严格的功率控制技术。前向链路和反向链路采用不同的调制扩频技术,在前向链路上,基站通过采用不同的扩频序列同时发送小区内全部用户的用户数据,同时还要发送一个导频码,使得所有移动台在估计信道条件时,可以使用相干载波检测;在反向链路上,所有移动台以异步方式响应,并且由于基站的功率控制,理想情况下,每个移动台具有相同的信号电平值。

IS-95 CDMA 蜂窝系统开发的声码器采用码激励线性预测(CELP)编码算法,也称为 QCELP 算法,其基本速率是 8Kbps,但是可随输入话音消息的特征而动态地分为 4 种,即 8Kbps、4Kbps、2Kbps、1Kbps,可以 9.6Kbps、4.8Kbps、2.4Kbps、1.2Kbps 的信道速率分别传输。

在数字蜂窝通信系统中,全网必须具有统一的时间标准,这种统一而精确的时间基准对 CDMA 蜂窝系统来说尤为重要。

CDMA 蜂窝系统利用“全球定位系统”(GPS)的时标,GPS 的时间和“世界协调时间”(UTC)是同步的,二者之差是秒的整倍数。

各基站都配有 GPS 接收机,保持系统中各基站有统一的时间基准,称为 CDMA 系统的公共时间基准。移动台通常利用最先到达并用于解调的多径信号分量建立时间基准。如果另一条多径分量变成了最先到达并用于解调的多径分量,则移动台的时间基准要跟踪到这个新的多径分量。

3.5 IS-95 CDMA 的空中接口

3.5.1 IS-95 CDMA 的正向信道

1. 正向传输逻辑信道

IS-95 定义的正向传输逻辑信道如图 3-24 所示，包含 1 个导频信道、1 个同步信道、7 个寻呼信道和 55 个业务信道。

导频信道：导频信道传输由基站连续发送的导频信号，导频信号是一种无调制的直接序列扩频信号，使移动台可迅速而精确地捕获信道的定时信息，并提取相干载波进行信号的解调。移动台通过对周围不同基站的导频信号进行检测与比较，可以决定什么时候需要进行过区切换。

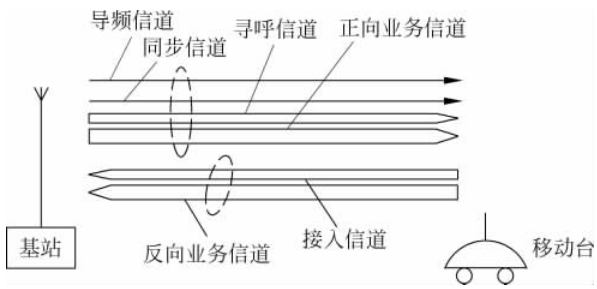

图 3-24 IS-95 CDMA 蜂窝系统的信道示意图

同步信道：同步信道主要传输同步信息，在同步期间，移动台利用此同步信息进行同步调整；一旦同步完成，它通常不再使用同步信道，但当设备关机重新开机时，还需要重新进行同步。当通信业务量很多，所有业务信道均被占用而不敷用时，此同步信道也可临时改作业务信道使用。

寻呼信道：寻呼信道在呼叫接续阶段传输寻呼移动台的信息。移动台通常在建立同步后，接着就选择一个寻呼信道来监听系统发出的寻呼信息和其他指令。在需要时，寻呼信道可以改作业务信道使用，直至全部用完。

正向业务信道：正向业务信道共有 4 种传输速率（9600bps、4800bps、2400bps、1200bps）。业务速率可以逐帧（20ms）改变，以动态地适应通信者的话音特征。例如，发音时传输速率提高，停顿时传输速率降低，这样做，有利于减少 CDMA 系统的多址干扰，以提高系统容量。在业务信道中，还要插入其他的控制信息，如链路功率控制和过区切换指令等。

2. 正向传输

IS-95 CDMA 正向信道传输的结构图如图 3-25 所示。

（1）数据速率

同步信道的数据速率为 1200bps，寻呼信道为 9600bps 或 4800bps，正向业务信道为 9600bps、4800bps、2400bps 和 1200bps。正向业务信道的数据在每帧（20ms）末尾有 8bit，称为编码器尾比特，它的作用是把卷积编码器置于规定的状态。此外，在 9600bps 和 4800bps 的数据中都含有帧质量指示比特（即 CRC 检验比特），前者为 12bit，后者为 8bit。因此，正向业务信道的信息速率分别是 8.6Kbps、4.0Kbps、2.0Kbps 和 0.8Kbps。

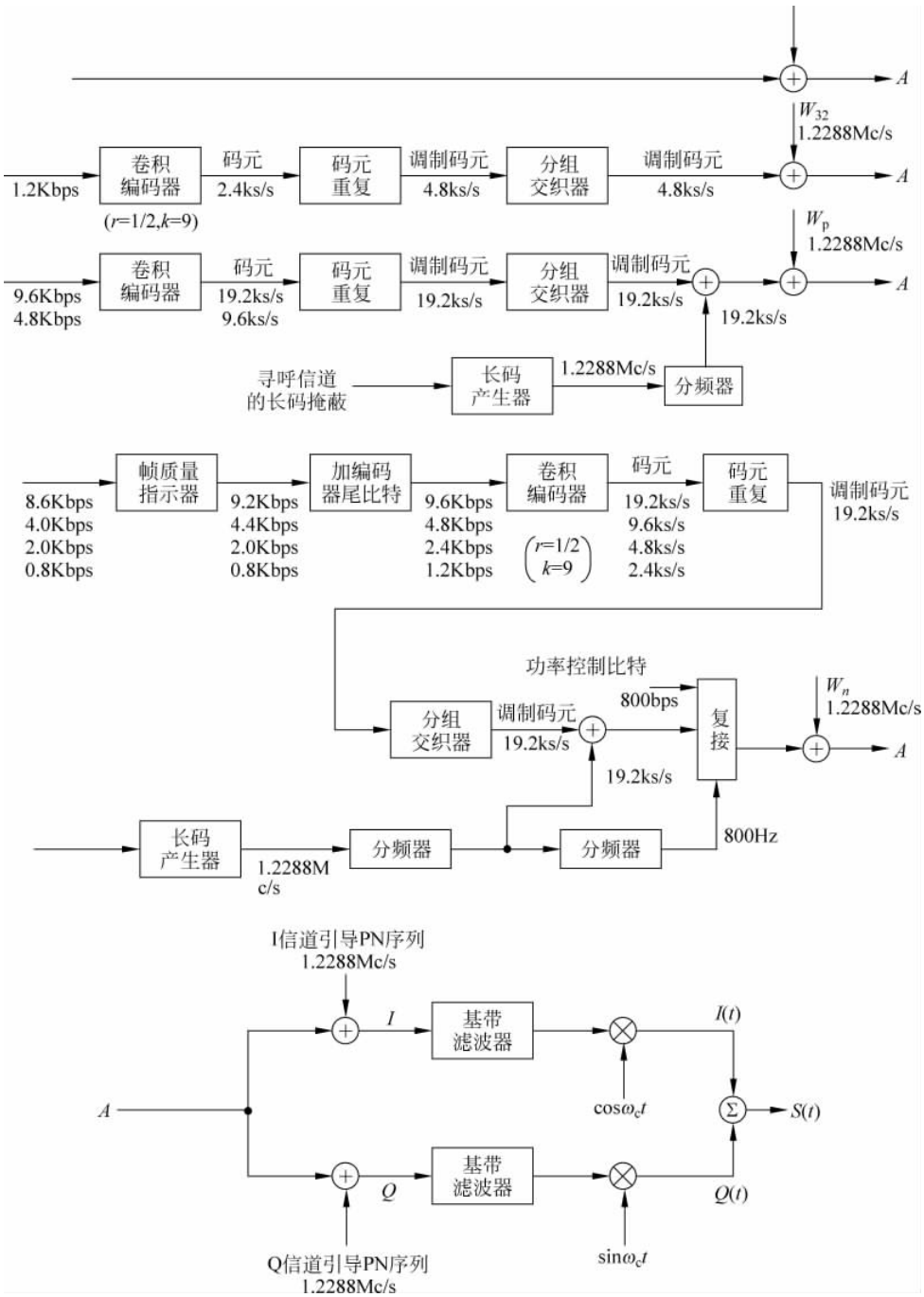

图 3-25　CDMA 正向信道传输的结构图

(2) 卷积编码

数据在传输之前都要进行卷积编码,卷积码的码率为 1/2,约束长度为 9。

(3) 码元重复

对于同步信道,经过卷积编码后的各个码元,在分组交织之前,都要重复一次(每个码元

连续出现 2 次)。对于寻呼信道和正向业务信道,只要数据率低于 9600bps,在分组交织之前都要重复。速率为 4800bps 时,各码元要重复一次(每码元连续出现 2 次);速率为 2400bps,各码元要重复 3 次(每码元连续出现 4 次);速率为 1200bps,各码元要重复 7 次(每码元连续出现 8 次)。这样做可以使各种信息速率均变成相同的调制码元速率,即 19 200 个调制码元每秒。

(4) 分组交织

所有码元在重复之后都要进行分组交织,同步信号所用的交织跨度等于 26.666ms,相当于码元速率为 4800s/s 时的 128 个调制码元宽度。交织器组成的阵列是 8 行×16 列(即 128 个单元)。寻呼信道和正向业务信道所用的交织跨度等于 20ms,这相当于码元速率为 19 200b/s 时的 384 个调制码元宽度。交织器组成的阵列是 24 行×16 列(即 384 个单元)。

(5) 数据掩蔽

数据掩蔽用于寻呼信道和正向业务信道,其作用是为通信提供保密。掩码器把交织器输出的码元流和按用户编址的 PN 序列进行模 2 加。这种 PN 序列是工作在时钟为 1.2288MHz 的长码,每一调制码元长度为 $1.2288\times10^6/19\,200=64$ 个 PN 子码宽度。长码经分频后,其速率变为 19 200s/s,因而送入模 2 相加器进行数据掩蔽的是每 64 个子码中的第一个子码起作用。

(6) 正交扩频

为了使正向传输的各个信道之间具有正交性,在正向 CDMA 信道中传输的所有信道都要用 64 进制的 Walsh 函数进行扩展。号码为 0 的 Walsh 函数 W0 分配给导频信道,号码为 32 的 Walsh 函数 W32 分配给同步信道。号码为 1～7 的 Walsh 函数 W1～W7 分配给寻呼信道,其余 Walsh 函数分配给正向业务信道。Walsh 函数的子码速率为 1.2288Mc/s,并以 52.083μs($64/1.2288\times10^6$)为周期重复,此周期就是正向业务信道调制码元的宽度。

(7) 四相扩展

在正交扩展之后,各种信号都要进行四相扩展。四相扩展所用的序列为引导 PN 序列,引导 PN 序列的作用是给不同基站发出的信号赋予不同的特征,便于移动台识别所需的基站。不同的基站使用相同的 PN 序列,但各自采用不同的时间偏置。不同的时间偏置用偏置系数表示,偏置系数共 512 个,编号从 0～511。偏置时间等于偏置系数乘以 64,单位是 PN 序列子码数目。引导 PN 序列的周期长度是 $32\,768/1\,228\,800=26.66$ms,即每 2 秒有 75 个 PN 序列周期。

(8) 信道参数

表 3-3～表 3-5 分别是 IS-95 CDMA 系统的同步信道参数、寻呼信道参数和正向业务信道参数。

表 3-3 同步信道参数

参　　数	数据率 1200bps
PN 子码速率(Mc/s)	1.2288
卷积编码码率	1/2
码元重复后出现次数	2
调制码元速率(s/s)	4800
每调制码元子码数	256
每比特的子码数	1024

表 3-4　寻呼信道参数

参　　数	数据率(bps)	
	9600	4800
PN 子码速率(Mc/s)	1.2288	1.2288
卷积编码码率	1/2	1/2
码元重复后出现次数	1	2
调制码元速率(s/s)	19 200	19 200
每调制码元子码数	64	64
每比特的子码数	128	256

表 3-5　正向业务信道参数

参　　数	数据率(bps)			
	9600	4800	2400	1200
PN 子码速率(Mc/s)	1.2288	1.2288	1.2288	1.2288
卷积编码码率	1/2	1/2	1/2	1/2
码元重复后出现次数	1	2	4	8
调制码元速率(s/s)	19 200	19 200	19 200	19 200
每调制码元子码数	64	64	64	64
每比特的子码数	128	256	512	1024

3.5.2　IS-95 CDMA 的反向信道

1. 反向传输逻辑信道

接入信道：当移动台没有使用业务信道时，接入信道提供移动台到基站的传输通路，在其中发起呼叫，对寻呼进行响应以及传送登记注册等短信息。接入信道和正向传输中的寻呼信道相对应，以相互传送指令、应答和其他有关的信息。

反向业务信道：与正向业务信道相对应。

2. 反向传输

IS-95CDMA 反向信道传输的结构图如图 3-26 所示。

(1) 数据速率

接入信道用 4800bps 的固定速率。反向业务信道用 9600bps、4800bps、2400bps 和 1200bps 的可变速率。两种信道的数据中均加入编码器尾比特，用于把卷积编码器复位到规定的状态。

(2) 卷积编码

接入信道和反向业务信道所传输的数据都要进行卷积编码，卷积码的码率为 1/3，约束长度为 9。

(3) 码元重复

反向业务信道的码元重复方法和正向业务信道一样，数据率为 9600bps 时，码元不重复；数据率为 4800bps、2400bps 和 1200bps 时，码元分别重复 1 次、3 次和 7 次(每一码元连续出现 2 次、4 次和 8 次)。这样就使得各种速率的数据都变换成 28 800 码元每秒。

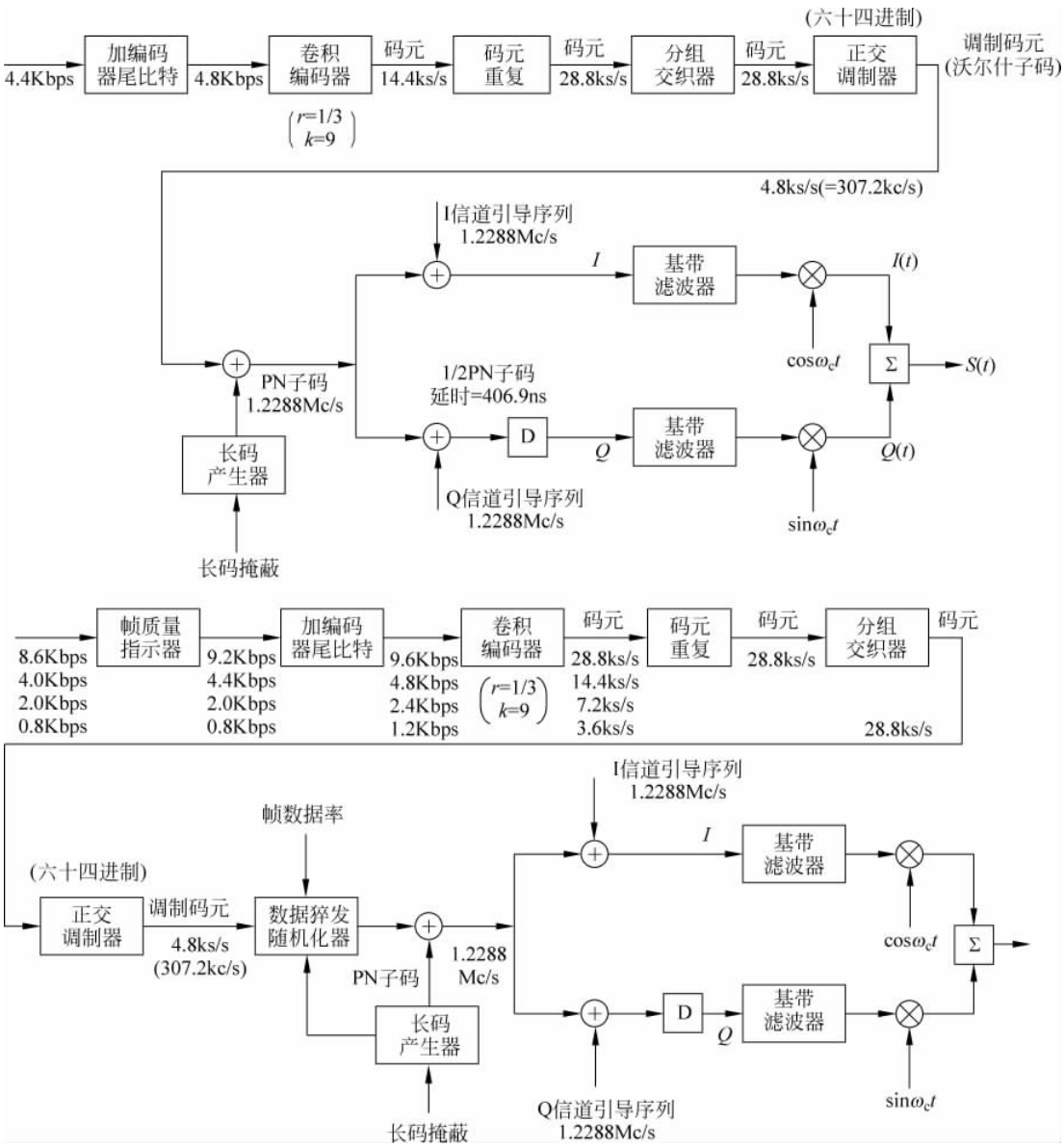

图 3-26　IS-95 CDMA 反向信道传输的结构图

(4) 分组交织

所有码元重复之前都要进行分组交织，分组交织的跨度为 20ms，交织器组成的阵列是 32 行×18 列(即 576 个单元)。

(5) 可变数据速率传输

为了减少移动台的功耗和减小它对 CDMA 信道产生的干扰，对交织器输出的码元用一时间滤波器进行选通，只允许所需码元输出，而删除其他重复的码元。

(6) 正交多进制调制

在反向 CDMA 信道中，把交织器输出的码元每 6 个作为 1 组，用 $2^6=64$ 进制的 Walsh

函数之一进行传输。调制码元的传输速率为 28 800/6＝4800s/s，调制码元的时间宽度为 1/4800＝208.333μs，每 1 调制码元含 6 个子码，因此 Walsh 函数的子码速率为 64×4800＝307.2kc/s，相应的子码宽度为 3.255μs。

(7) 直接序列扩展

在反向业务信道和接入信道传输的信号都要用长码进行扩展，前者是数据猝发随机化产生器输出的码流与长码模 2 加；后者是 64 进制正交调制器输出的码流和长码模 2 加。

(8) 四相扩展

反向 CDMA 信道四相扩展所用的序列就是正向 CDMA 信道所用的 I 与 Q 引导 PN 序列，经过 PN 序列扩展之后，Q 支路的信号要经过一个延迟电路，把时间延迟 1/2 个子码宽度(409.901ns)，再送入基带滤波器。

(9) 信道参数

表 3-6 和表 3-7 分别给出了 IS-95 CDMA 系统的反向业务信道和接入信道参数。

表 3-6　反向业务信道参数

参　　数	数据率(bps)			
	9600	4800	2400	1200
PN 子码速率(Mc/s)	1.2288	1.2288	1.2288	1.2288
卷积编码码率	1/3	1/3	1/3	1/3
传输占空比(%)	100	50	25	12.5
码元速率(s/s)	28 800	28 800	28 800	28 800
每调制码元的码元数	6	6	6	6
调制码元的速率(s/s)	4800	4800	4800	4800
沃尔什子码速率(kc/s)	370.20	370.20	370.20	370.20
调制码元宽度(μs)	208.33	208.33	208.33	208.33
每码元的 PN 子码数	42.67	42.67	42.67	42.67
每调制码元的 PN 子码数	256	256	256	256
每沃尔什子码的 PN 子码数	4	4	4	4

表 3-7　接入信道参数

参　　数	数据率 4800bps
PN 子码速率(Mc/s)	1.2288
卷积编码码率	1/3
码元重复出现次数	2
传输占空比(%)	100
码元速率(s/s)	28 800
每调制码元的码元数	6
调制码元的速率(s/s)	4800
沃尔什子码速率(kc/s)	370.20
调制码元宽度(μs)	208.33
每码元的 PN 子码数	42.67
每调制码元的 PN 子码数	256
每沃尔什子码的 PN 子码数	4

3.6 IS-95 CDMA 的控制功能

3.6.1 软切换

软切换是指移动台开始与新的基站通信但不立即中断它和原来基站通信的一种切换方式，软切换只能在同一频率的 CDMA 信道中进行。软切换是 CDMA 蜂窝系统独有的切换方式，可有效地提高切换的可靠性，而且若移动台处于两个小区的交界处，软切换能提供正向业务信道分集，也能提供反向业务信道的分集，从而保证通信质量；如采用硬切换，两个小区的基站在该处的信号电平都较弱而且有起伏变化，这会导致移动台在两个基站之间反复要求切换（即“乒乓”现象），从而重复地往返传送切换信息，使系统控制的负荷加重，或引起过载，并增加了中断通信的可能性。

同样，软切换的前提是要及时了解各基站发射的信号到达移动台接收地点的强度。因此，移动台必须对基站发出的导频信号不断进行测量，并把测量结果通知基站。

基站发出的导频信号在使用相同频率时，只由引导 PN 序列的不同偏置来区分，每一可用导频要与它同一 CDMA 信道中的正向业务信道配合才有效。当移动台检测到一个足够强的导频而它未与任何一个正向业务信道相配合时，就向基站发送一导频测量报告，于是基站就给移动台指定一正向业务信道和该导频相对应，这样的导频称为激活导频或称有效导频。

同一 CDMA 信道的导频分为 4 类。

（1）激活组：和分配给移动台的正向业务信道结合的导频。

（2）候补组：未列入激活组，但具有足够的强度表明它与正向业务信道结合并能成功地被解调。

（3）邻近组：未列入激活组和候补组，但可作为切换的备用导频。

（4）剩余组：未列入上述 3 组的导频。

当移动台驶向一基站，然后又离开该基站时，移动台收到该基站的导频强度先由弱变强，接着又由强变弱，因而该导频信号可能由邻近组和候补组进入激活组，然后又返回邻近组，如图 3-27 所示。在此期间，移动台和基站之间的信息交换如下：

（1）导频强度超过门限（上），移动台向基站发送一导频强度测量消息，并把导频转换到候补组；

（2）基站向移动台发送一切换引导消息；

（3）移动台把导频转换到激活组，并向基站发送一切换完成消息；

（4）导频强度降低到门限（下）之下，移动台启动切换下降计时器；

（5）切换下降计时器终止；移动台向基站发送一导频测量消息；

（6）基站向移动台发送一切换消息；

（7）移动台把导频从激活组转移到邻近组，并向基站发送一切换完成消息。

3.6.2 软容量

在 FDMA、TDMA 系统中，当小区服务的用户数达到最大信道数，已满载的系统绝对无法再增添一个信号，此时若有新的呼叫，该用户只能听到忙音。而在 CDMA 系统中，用户

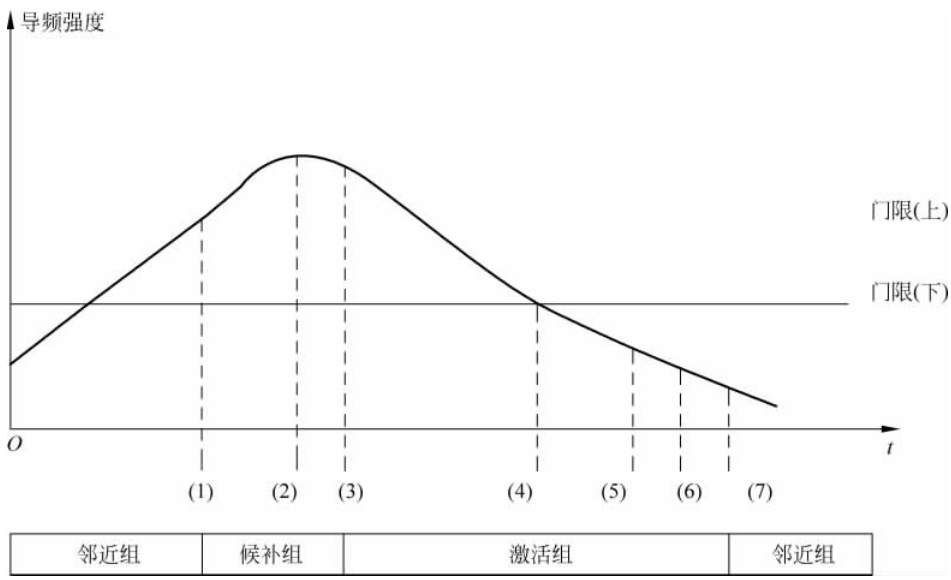

图 3-27　软切换过程

数目和服务质量之间可以相互折中，灵活确定。例如系统经营者可以在话务量高峰期将误帧率稍微提高，从而增加可用信道数。同时，当相邻小区的负荷较轻时，本小区受到的干扰减少，容量就可适当增加。

体现软容量的另一种形式是小区呼吸功能，所谓小区呼吸功能就是指各个小区的覆盖大小是动态的，当相邻两个小区负荷一轻一重时，负荷重的小区通过减小导频发射功率，使本小区的边缘用户由于导频强度不够，切换到相邻小区，使负荷分担，即相当于增加了容量。这项功能对切换也特别有用，可避免信道紧缺而导致呼叫中断。在模拟系统和数字 TDMA 系统中，如果一条信道不可用，呼叫必须重新被分配到另一条信道，或者在切换时中断。但是在 CDMA 系统中，在一个呼叫结束前，可以接纳另一个呼叫。

3.6.3　功率控制

1. 功率控制功能

CDMA 系统中所有的移动台在相同的频段工作，所以其中任意一个用户的通信信号对其他用户的通信都是一个干扰。通话的用户数越多，互相之间的干扰就越大，解调器输入端的信噪比就越低。当干扰达到一定的限度时，系统就不能正常工作了，就 CDMA 系统的容量来说，是干扰受限系统(FDMA 和 TDMA 是频率受限系统)。为了获得大容量、高质量的通信，CDMA 移动通信系统必须具有功率控制功能。

功率控制包括反向链路的功率控制和正向链路的功率控制，反向链路的功率控制是分布式控制，用来控制移动台的发射功率大小，使得基站接收到的所有移动台发射到基站的信号功率基本相等。反向链路的功率控制使得各个用户之间相互干扰最小，并能达到克服“远近效应”(指当基站同时接收两个距离不同而发射功率相同的移动台发来的信号时，由于距离基站较近的移动台信号较强，距离较远的移动台信号较弱，则距离基站近的移动台的强信号将对另一移动台信号产生严重的干扰)的目的。正向链路功率控制是调整基站向移动台

发射的功率，是集中式功率控制，使任一移动台无论处于蜂窝小区中的任何位置上，收到基站发来的信号电平都恰好达到信干比所要求的门限值。做到这一点，就可以避免基站向距离近的移动台辐射过大的信号功率，也可以防止或减小由于移动台进入传播条件恶劣或背景干扰过强的地区而发生误码率增大或通信质量下降的现象。

2. 反向功率控制方法

进行反向功率控制的办法可以是在移动台接收并测量基站发来的信号强度，并估计正向传输损耗，然后根据这种估计来调节移动台的反向发射功率。如果接收信号增强，就降低其发射功率；若接收信号减弱，就增加其发射功率。

功率控制的原则是：当信道的传播条件突然改善时，功率控制应作出快速反应，以防止信号突然增强而对其他用户产生附加干扰；相反，当传播条件突然变坏时，功率调整的速度可以相对慢一些。也就是说，宁可单个用户的信号质量短时间恶化，也要防止许多用户的背景干扰都增大。

这种功率控制方式也称开环功率控制法，其优点是方法简单、直接，不需要在移动台和基站之间交换控制信息，因而控制速度快并且节省开销。这种方法对于某些情况，例如车载移动台快速驶入（或驶出）地形起伏区或高大建筑物遮蔽区所引起的信号变化是十分有效的，但是对于信号因多径传播而引起的瑞利衰落变化则效果不好。这是指正向传输和反向传输使用的频率不同，通常两个频率的间隔大大超过信道的相干带宽，因此不能认为移动台在正向信道上测得的衰落特性就等于反向信道上的衰落特性。为了解决这个问题，可采用闭环功率控制法，即由基站检测来自移动台的信号强度，并根据测得的结果形成功率调整指令，通知移动台，使移动台根据此调整指令来调节其发射功率。

为了使反向功率控制有效而可靠，开环功率控制法和闭环功率控制法可以结合使用。

3. 正向功率控制方法

和反向功率控制的方法类似，正向功率控制可以由移动台检测其接收信号的强度，并不断比较信号电平和干扰电平的比值。如果此比值小于预定的门限值，移动台就向基站发出增加功率的请求；如果此比值超过了预定的门限值，移动台就向基站发出减小功率的请求。基站收到调整功率的请求后，即按一定的调整量改变相应的发射功率。同样，正向功率控制也可在基站检测来自移动台的信号强度，以估计反向传输的损耗并相应调整其发射功率。

3.6.4 安全机制

第二代移动通信系统的 CDMA 网络无线接入安全机制采用 4 种安全算法：①蜂窝鉴权与语音加密（CAVE）算法，这是北美系统标准，用于查询/响应鉴权协议和密钥生成；②专用长码掩码（PLCM）算法，用于控制扩频序列，然后将扩频序列与语音数据异或实现语音保密；③基于线性反馈移位寄存器（LFSR）的流密码 ORYX（由 4 个发明者名字的首字母命名）算法，用于无线用户数据加密服务；④增强的分组加密算法（ECMEA），对称密码，用于加密信令消息，包括短消息。

1. 鉴权

IS-95 系统提供网络对移动台的单向鉴权，一个成功的鉴权需要移动台和网络端处理一组完全相同的共享秘密数据（SSD）。现有的规范中定义了两种主要的鉴权过程——全局查询鉴权和唯一查询鉴权，全局查询鉴权在移动台主呼、移动台被呼和移动台位置登记时执

行，又称为共用 RAND 方式；唯一查询鉴权由基站在下列情况下发起，即全局查询鉴权失败、切换、在语音信道上鉴权、移动台闪动请求、SSD 更新。上述鉴权过程都包括了查询响应过程和 SSD 更新过程。

鉴权过程涉及的主要参数有如下：

(1) ESN(电子序列号)，长 32bit，是移动终端的唯一标识，由手机制造商分配；

(2) IMSI_S，是由 IMSI 得来的，并由 10 位数字(34bit)组成的号码；

(3) A_ Key，长 64bit，是根密钥，保存在移动台和 HLR/AuC 中；

(4) SSD，长 128bit，可分为 SSD_A 和 SSD_B 两部分，各为 64bit，分别用于鉴权和产生子密钥；

(5) COUNT，长 16bit，其中低 6 位有效，用来记录移动台接入网络总数。

查询响应过程和 SSD 更新过程涉及的其他相关参数如表 3-8 所示。

表 3-8　鉴权过程涉及的部分参数

参 数 名 称	参数长度(位)	参数简要说明
RANDC	8	全局查询响应过程使用的随机数
AUTHR	18	全局查询响应过程的输出参数
RANDU	24	唯一查询响应过程使用的随机数
AUTHU	18	唯一查询响应过程的输出参数
RANDSSD	56	SSD 更新过程使用的随机数
RANDBS	32	SSD 更新过程使用的随机数
AUTHBS	18	SSD 更新过程的输出参数

(1) 全局查询响应过程

移动台 MS 首先向基站 BS 发起接入请求，接着 MS 根据 BS 的 RANDC 计算得到 AUTHR，即 AUTHR＝CAVE(IMSI，ESN，SSD_A，RANDC)，同时，基站使用相同的 RANDC 进行相同计算得到一个 AUTHR。如果 MS 和 BS 拥有相同的 RANDC、AUTHR 和 COUNT，则鉴权成功，认为此 MS 是合法的；否则就发起唯一查询响应或更新 SSD。

(2) 唯一查询响应过程

首先 BS 生成 RANDU 发送给 MS，接着 MS 将其作为 CAVE 算法的输入参数并执行算法，即 AUTHR＝CAVE(IMSI，ESN，SSD_A，RANDU)。然后 MS 将计算结果 AUTHU 发送给基站，BS 使用它内部的 SSD_A 值与 MS 相同的算法计算出 AUTHU，两者 AUTHU 相比较，若相同，则鉴权成功；若不相同，则 BS 拒绝访问或发起 SSD 更新。

(3) SSD 更新过程

SSD 是存储在移动台用户识别 UIM 卡中半永久性 128bit 的共享秘密数据，其产生框图如图 3-28 所示。SSD 更新成功后，BS 会发起唯一查询响应。执行两次 CAVE 算法，计算输出用于验证的结果值 AUTHBS。第一次 CAVE 算法中以 A_ Key，ESN 及 RANDSSD 为参数，计算得到 SSD_new，输出 SSD_A_new、SSD_B_new。然后 MS 选择随机数 RANDBS 并在反向信道上发送给 BS。BS 和 MS 各以 RANDBS 为输入参数并执行第二次 CAVE 算法，分别得到用于验证的结果值 AUTHBS。

2. 加密

IS-95 系统采用两类加密模式：一是信源消息加密，又包括外部加密方式和内部加密方

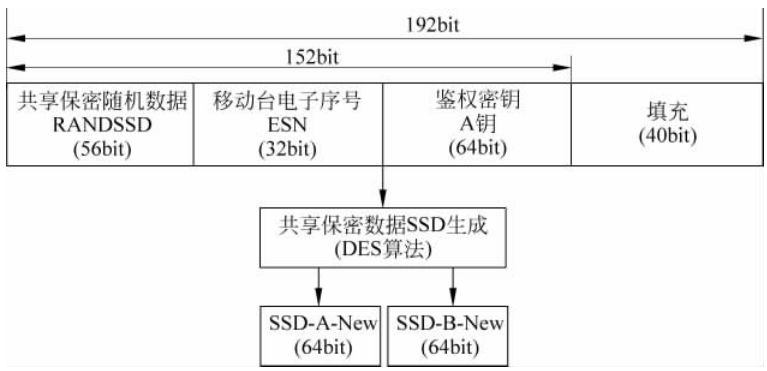

图 3-28　SSD 产生过程框图

式；二是信道输入信号加密。IS-95 系统可以对下列不同业务加密。

(1) 语音加密。

IS-95 系统中语音加密是通过长码掩码 PLCM 进行 PN 扩频实现的，终端利用 SSD_B 和 CAVE 算法产生专用长码掩码、64bit 的 CMEA 密钥、32bit 的数据加密密钥。终端和网络利用专用长码掩码来改变 PN 码的特性，改变后的 PN 码用于语音置乱，进一步增强了 IS-95 空中接口的保密性。

(2) 信令信息加密。

为了加强鉴权过程和保护用户的敏感信息，需要对信令信息的某些字段进行加密；终端和网络利用 CMEA 密钥和 CMEA 算法来加密解密空中接口的信令信息。

(3) 用户数据保密。

ORYX 是基于 LSFR 的流密码，用于用户数据加密，由于出口限制，密钥长度被限制在 32bit 以内。ORYX 被证明是不安全的。

3. 与 GSM 安全机制的比较

GSM 系统鉴权技术相对于 CDMA 系统鉴权技术而言要简单得多，所有场合下的鉴权都一视同仁，处理机制完全相同。由此可知，CDMA 系统的鉴权机制和规程相对于 GSM 要复杂得多，这主要是由 CDMA 的安全保密体制及其算法本身决定的。GSM 和 CDMA 的安全机制都基于私钥密码技术，都具有一个主密钥；都提供匿名性，认证和保密服务，所有算法秘密设计，没有经过公开的安全论证就投入使用。GSM 系统中，主密钥 K_i 直接用于产生认证签名。CDMA 系统中，主密钥 A_Key 并不直接用于认证，而是由它生成中间密钥 SSD，再由 SSD 产生认证签名和子密钥，这是 CDMA 系统的一个优点。

GSM 和 IS-95 都只对移动台采用单向鉴权，对来自网络的攻击和假冒没有防范功能。加密密钥都采用私钥机制，加密复杂度有待加强。

本章小结

GSM 系统由移动台、基站子系统和网络子系统组成，网络子系统由 MSC(移动交换中心)和 OMC(操作维护中心)以及 HLR(归属位置寄存器)、VLR(访问位置寄存器)、AUC(鉴权中心)和 EIR(设备标志寄存)等组成。

在GSM系统中，每个载频，在时间上被定义为一个个TDMA帧（简称为帧）相连接，每个TDMA帧包括8个时隙（TS0～TS7），所有TDMA帧中同号时隙提供一个物理信道。

GSM系统采用的抗衰落技术包括信道编码、交织编码、均衡技术、分集接收、跳频技术、语音激活技术和功率控制技术等。

GSM系统采用的安全措施有：鉴权、加密、EMSI的使用和IMSI保护等。

CDMA是以扩频通信技术为基础的数字移动通信中的一种多址接入方式，可以在系统中使用多种先进的信号处理技术，为系统带来了许多优点：软容量、软切换、高的话音质量和低发射功率、抗干扰能力强、保密。

就系统容量而言，CDMA系统是干扰受限的系统，而FDMA和TDMA是带宽受限的系统。

功率控制技术对移动通信来说是一项重要的技术，它对CDMA系统显得尤为重要，它是克服“远近效应”的有力措施。

第2代移动通信系统的CDMA网络无线接入安全机制采用4种安全算法：①蜂窝鉴权与语音加密（CASE）算法，这是北美系统标准，用于查询/响应鉴权协议和密钥生成；②专用长码掩码（PLCM）算法，用于控制扩频序列，然后将扩频序列与语音数据异或实现语音保密；③基于线性反馈移位寄存器（LSFR）的流密码ORYX（由4个发明者名字的首字母命名）算法，用于无线用户数据加密服务；④增强的分组加密算法（E_CMEA），对称密码，用于加密信令消息，包括短消息。

习题

3-1　移动台国际身份号码和国际移动用户识别码之间有什么区别？它们各自有什么用途？试画出它们的格式结构。

3-2　GSM系统中，常规突发序列中的训练序列的作用是什么？为什么要将其放在突发序列的中间？如果放在两端，会出现什么效果？

3-3　GSM系统的逻辑信道有哪些？说明其逻辑信道映射到物理信道的一般规律。

3-4　GSM系统采用了哪些抗衰落技术？简要说明这些技术的原理。

3-5　GSM系统在通信安全性方面采取了哪些措施？

3-6　说明CDMA蜂窝系统比TDMA蜂窝系统获得更大容量的原因。

3-7　为什么说CDMA系统具有软切换和软容量的特点？它们各自有什么好处？

3-8　GSM系统为什么要采用均衡技术？CDMA系统为什么又不需要采用均衡技术？

3-9　IS-95 CDMA系统有哪些物理信道？这些信道各自完成什么功能？

3-10　试说明IS-95 CDMA系统的正向信道的传输结构和反向信道的传输结构。

3-11　IS-95 CDMA系统中，下行引导PN序列是为了区分什么？上行引导PN序列又是为了区分什么？对于下行引导PN序列，不同的基站使用相同的PN序列，但各自采用不同的时间偏置，如果两个基站的偏置系数相差10，则相差的PN码元数为多少？偏置时间相差多少？

3-12　IS-95 CDMA系统中，为什么上行的卷积码的码率比下行的大？

3-13 解释 IS-95 CDMA 反向传输中的正交多进制调制过程。

3-14 CDAM 系统为什么要采用功率控制技术？按照技术特点功率控制技术如何分类？

3-15 第 2 代移动通信系统的 CDMA 网络无线接入安全机制采用哪 4 种算法？试比较 GSM 和 IS-95 CDMA 系统的安全机制。