移动通信原理与系统

第六章 GSM 系统

Xiuhua Fu

2019 年 5 月 6 日

contents

GSM 系统发展 I

- 1982 年，当时来自欧共体 11 国的代表在欧洲邮电管理委员会（CEPT）组织下成立了一个特别移动小组（Group Special Mobile），简称 GSM，其任务是制订一种泛欧 900MHz 的移动通信标准，以满足欧洲各国间跨国漫游通信的需求。
- 1988 年欧洲电信标准协会（ETSI）成立，GSM 和其它标准化工作一起转人这个新机构下。1991 年 GSM 阶段 1 的技术规范全部完成，它包括 12 系列，130 多个建议。同年底，世界上第一个 GSM 网络开始运营，将 GSM 正式更名为“全球移动通信系统”（Glboal System for Mobile Communication）。
- 同年，ETSI 还完成了制定 1800MHz 频段的公共欧洲电信业务的规范，名为 DCS1800 系统。该系统与 GSM900 具有同样的基本功能，常将 DCS1800 称为 GSM1800，和 GSM900 通称为 GSM 系统。
- 1995 年，GSM 系统进入中国市场。

GSM 系统发展 II

- 2000 年开始，GSM 规范转交至 3GPP（3rd Generation Partnership Project，第三代合作伙伴计划）组织。3GPP 主要负责 3G 移动通信系统技术规范制定和报告发布，2000 年后的 GSM 规范修订主要集中在制定 GPRS 和 EDGE 上。

GSM 频带划分 I

- GSM 是 FDMA + TDMA 系统, 其一个 TDMA 帧分成 8 个时隙, 每个时隙对应一个用户, 即 GSM 的一个载频上可提供 8 个物理信道
- 工作频段

图: 我国 GSM 网络的频段分配

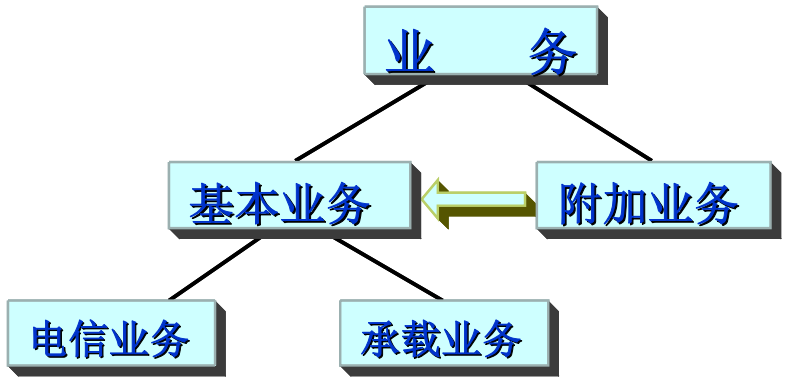
- 频道间隔:200kHz
- 双工间隔:900MHz 频段为 45MHz,1800MHz 频段为 95MHz,
- 频道配置: 采用等间隔配置方式
  - 在 900MHz 频段, 频道序号为 $1 \sim 124$, 共 124 个频道. 频道序号与频道标称中心频率的关系为:
    - 移动台发, 基站收 $f_l(n) = 890.200MHz + (n-1) \times 0.200MHz$
    - 基站发, 移动台收 $f_h(n) = f_l(n) + 45MHz, n = 1 \sim 124$

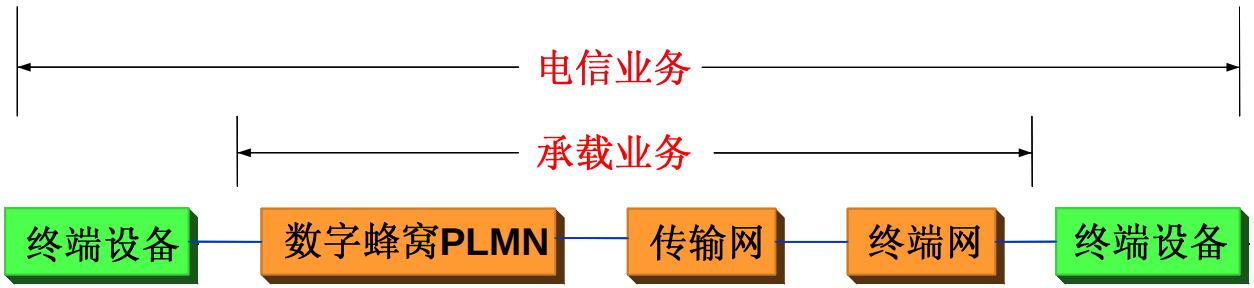
GSM 频带划分 II

- 在 1800MHz 频段, 频道序号为 512∼885, 共 374 个频道. 频道序号与频道标称中心频率的关系为:
  - 移动台发, 基站收
    $f_l(n) = 1710.200MHz + (n - 512) \times 0.200MHz$
  - 基站发, 移动台收
    $f_h(n) = f_l(n) + 95MHz, n = 512 \sim 885$

GSM 系统的业务及其特征 I

- GSM 业务:GSM 系统为了满足用户的通信要求而向用户提供的服务.
- 分类





GSM 系统的业务及其特征 II

- 电信业务: 为用户通信提供包括终端设备功能在内的完整能力
- 承载业务: 提供用户接入点（也称“用户/网络”接口）间信号传输的能力
  - 注 1. 承载业务 61 和 81 中的数据为 3.1KHz 信息传送能力的承载业务 21-34
  - 2. 表中“T”表示透明；“NT”表示不透明
- 附加业务: 基本电信业务增强或补充
  - 计费提示-AOC
  - 交替线业务 (ALS) - 个人或商业
  - 来话限制 - BAIC
  - 当漫游在 HPLMN 之外时，限制所有来话
  - 在国外时限制来话

GSM 系统的业务及其特征 III

- 呼出限制 - BOC
- .....

contents

GSM 系统的结构 I

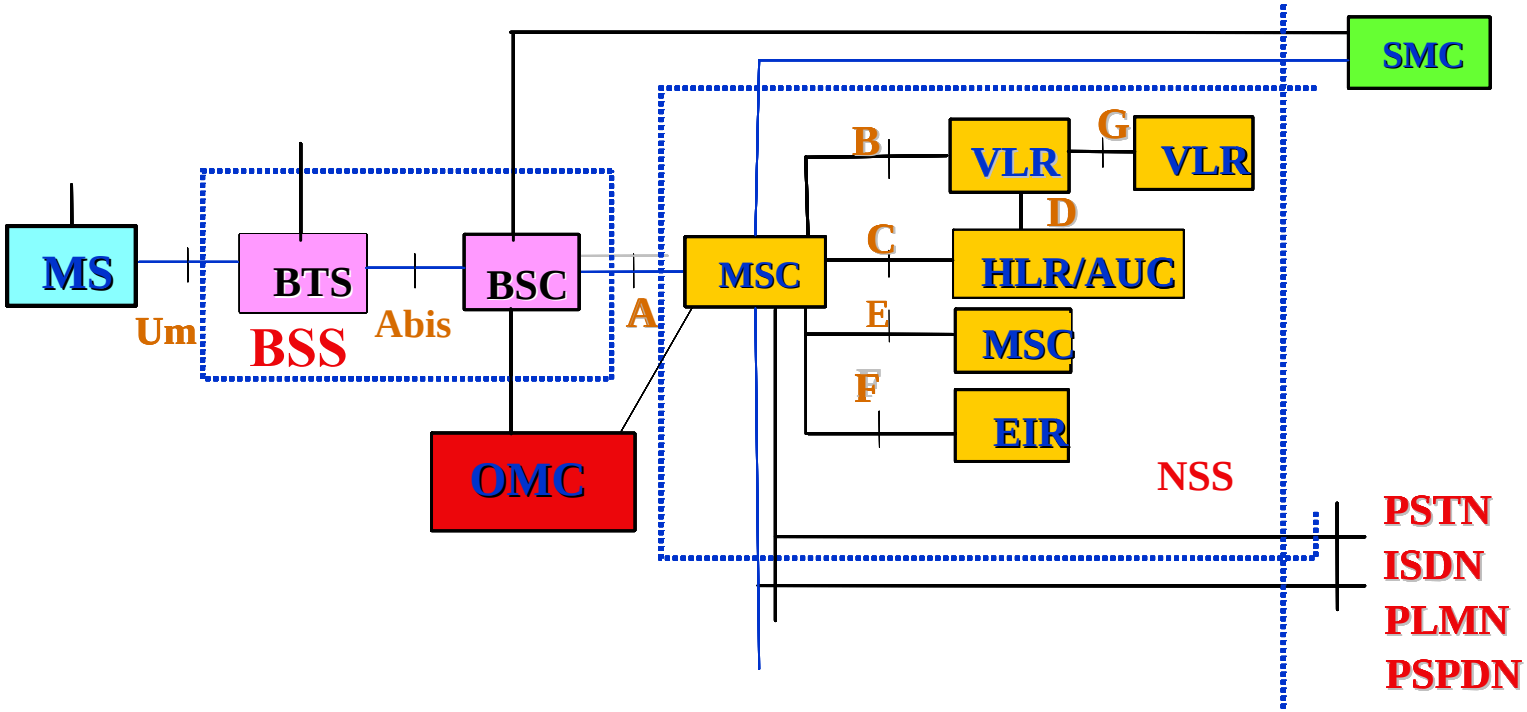


图: GSM 系统的总体结构

- 移动台子系统（MSS）

GSM 系统的结构 II

- MS 系统是移动系统的用户设备, 它由两部分组成, 移动终端和用户识别卡.
- 移动终端就是“机”, 它可完成话音编/解码、信道编/解码、信息加密/解密、信息的调制/解调、信息发射/接收等功能.
- 用户识别卡就是“人”, 存有认证和管理用户身份所需的所有信息, 并能执行一些与安全保密有关的重要信息, 以防止非法用户入网.

- 基站子系统（BSS）
  - 基站子系统 BSS 提供并管理移动台和 NSS 之间的无线传输通道
  - 它分为两个部分: 一部分是通过无线接口与移动台通信的基站收发信台（BTS）; 另一部分是与移动交换中心相连的基站控制器（BSC）
  - BTS 负责无线传输、BSC 负责无线资源控制与管理
- 网络子系统（NSS）
  - 主要完成移动通信系统的交换功能、用户数据管理和移动性管理、移动用户之间的通信以及移动用户与其他通信网用户之间的通信. 即 NSS 负责呼叫控制功能, 所有呼叫都经由 NSS 建立连接, 是移动网的核心子系统.

GSM 系统的结构 III

- 移动交换中心（MSC）
  - 完成呼叫接续、频道切换和无线资源管理等功能;
  - 是移动网的核心部件;
  - 是与外部网络设备的接口
- 归属地位置寄存器（HLR）
  - 归属地: 移动用户开户登记的移动电话局
  - HLR 存储的内容: 移动用户识别号码; 移动台的类型和参数; 用户服务类别; 与移动有关的用户位置信息; 路由选择信息; 计费信息等
- 拜访地位置寄存器（VLR）
  - 拜访地: 移动用户进入了非归属地地区的移动业务区时, 称其进入了拜访地. 拜访者有时称为漫游用户.
  - VLR 存储的内容是进入本地区的、与拜访者有关的信息和数据.
  - 拜访者的数据取自拜访者的 HLR/VLR,MSC 要处理对拜访者的呼叫时, 就从 VLR 中检索数据.
- 鉴权中心（AUC 或 AC）
  - 用于检验移动用户的合法性, 决定是否允许某个移动用户入网
  - 物理上通常与 HLR 放置在一起

GSM 系统的结构 IV

- 设备识别寄存器（EIR）
  - 系统进行设备鉴权时使用
  - 存储内容: 移动台的设备号; 移动台使用的合法信息等.
- 短消息中心（SC）
  - 对短消息进行接收、存储、转发, 是短消息业务的核心功能实体
- 操作支持子系统 OSS
  - 操作支持子系统是完成对 BSS 和 NSS 进行操作与维护管理任务, 主要设备是操作与维护中心（OMC）
  - OSS 的功能实体主要包括有网络管理中心 NMC、安全性管理中心 SEMC、用于用户识别卡管理的个人化中心 PCS、用于集中计费管理的数据后处理系统 DPPS、管理无线设备的 OMC-R、管理交换设备的 OMC-S 等
- 移动通信系统的网络接口
  - Um —无线接口
    - 传送数字话音或数据
    - 传送控制信息（信令信息）

GSM 系统的结构 V

- A 接口－ MSC 与 BSC 之间的接口
  - 传送数字语音或数据
  - 与移动呼叫有关的信息, 基站管理、移动台管理和信道管理等信息
- B 接口－ MSC 与 VLR 之间的接口
  - MSC 通过这个接口查询漫游用户的位置信息
  - 呼叫建立时向 VLR 查询漫游用户的有关数据
  - 一般情况下，MSC 与 VLR 在物理上同处在一个地方
  - 只传送信令信息
- C 接口－ MSC 与 HLR 之间的接口
  - 建立呼叫连接时, 查询移动台的选路信息
  - 呼叫完成时, 向 HLR 发送计费信息
  - 只传送信令信息

contents

逻辑信道 I

- 逻辑信道: 指在物理信道所传输的内容, 即依据移动网通信的需要, 为所传送的各种控制信令和语音或数据业务在 TDMA 的 8 个时隙分配的控制逻辑信道或语音/数据逻辑信道.
- 形式:GSM 数字系统在物理信道上传输的信息是大约由 100 多个调制比特组成的脉冲串，称为突发脉冲序列（Burst）. 以不同的“Burst”信息格式携带不同类型的信息内容来表示不同的逻辑信道.

逻辑信道 II

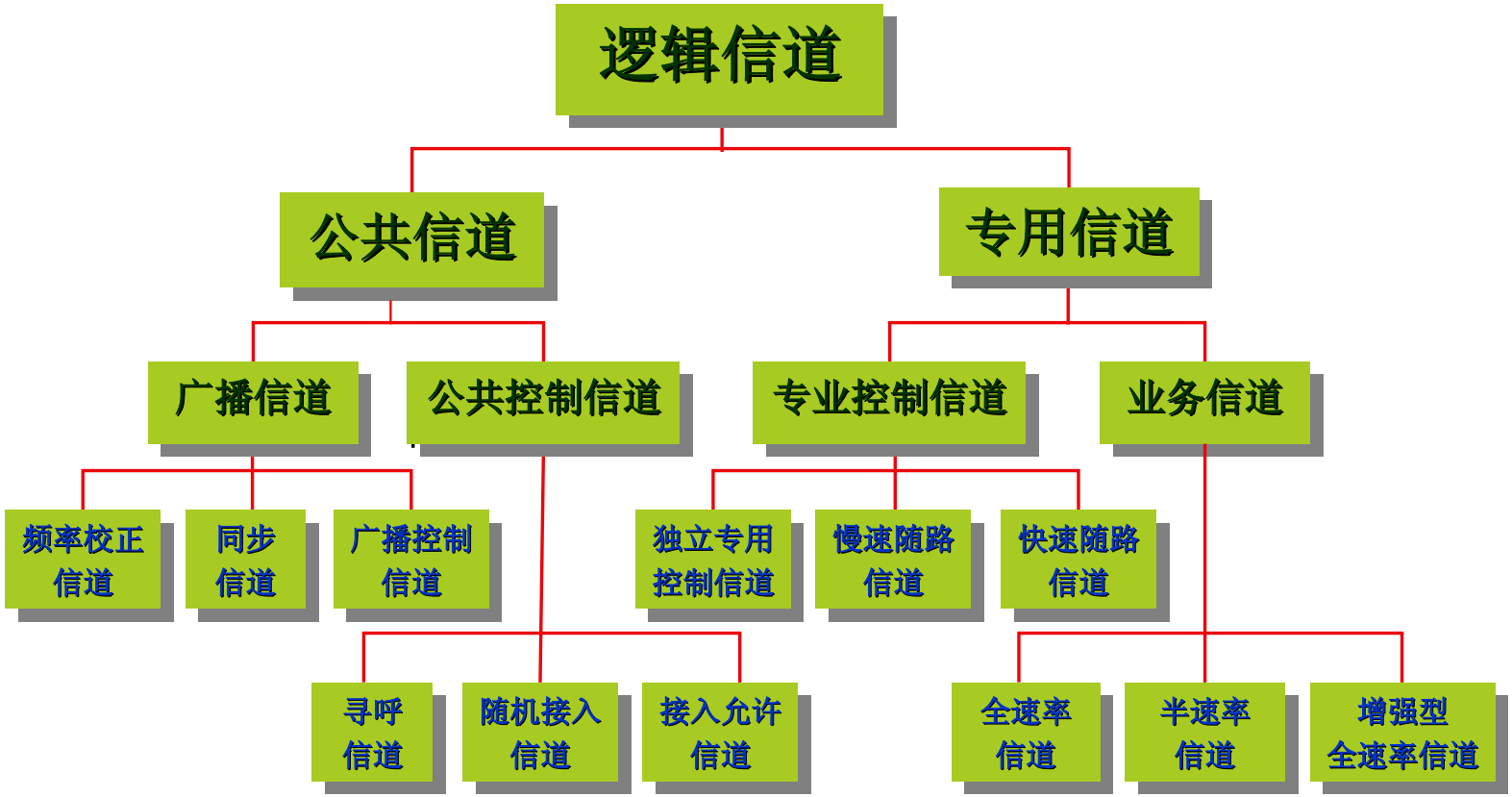


图: GSM 定义的各种逻辑信道示意图

- 公共信道: 用于传送基站向移动台广播消息的广播控制信道和用于传送 MSC 与 MS 间建立连接所需的双向信号的公共控制信道.

逻辑信道 III

- 广播信道 (BCH): 单向
- 公共控制信道（CCCH）: 双向

- 专用信道: 用于传送用户语音或数据的业务信道，另外还包括一些用于控制的专用控制信道.
  - 专用控制信道
  - 业务信道
    - 业务信道 (TCH) 传输话音和数据
    - 话音业务信道按速率的不同, 可分为全速率话音业务信道 (TCH/FS,13kbps) 和半速率话音业务信道 (TCH/HS,6.5kbps)
    - 数据业务信道按速率的不同，也分为全速率数据业务信道 (TCH/F9.6,TCH/F4.8,TCH/F2.4) 和半速率数据业务信道 (TCH/H4.8,TCH/H2.4)

逻辑信道 IV

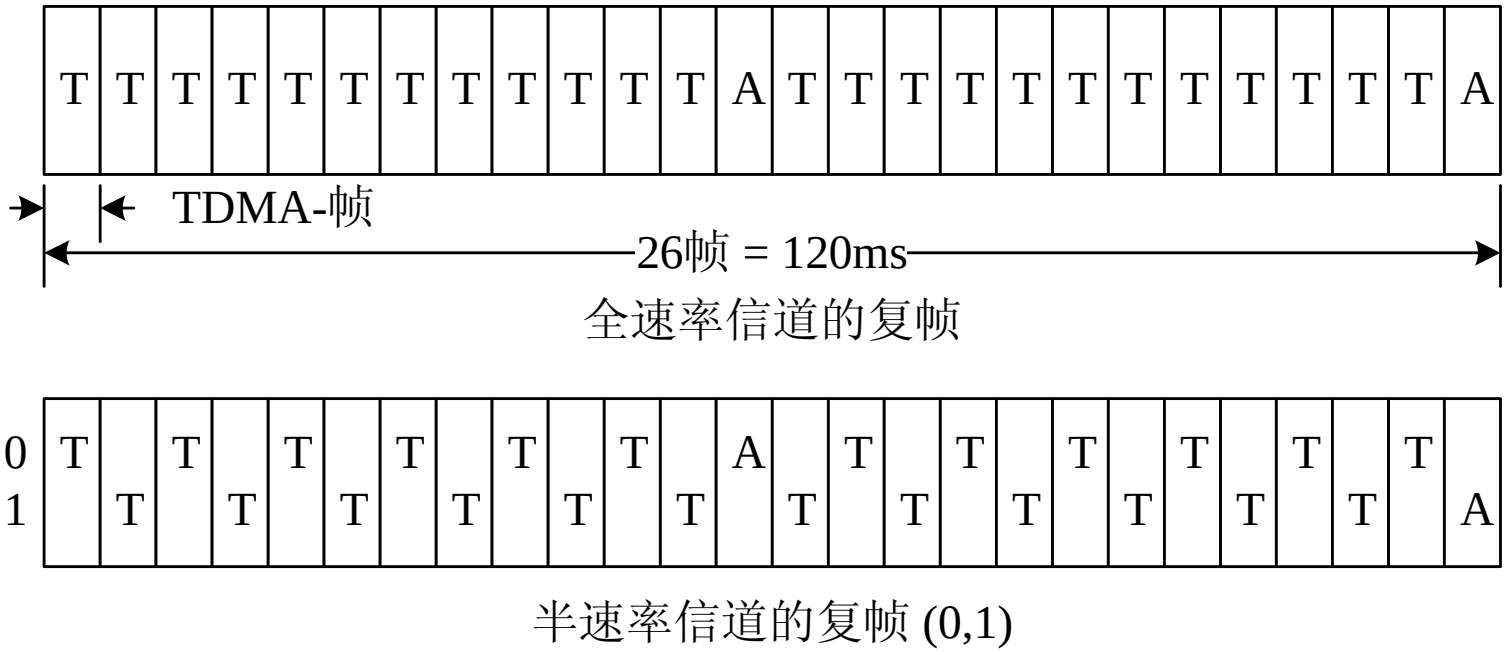
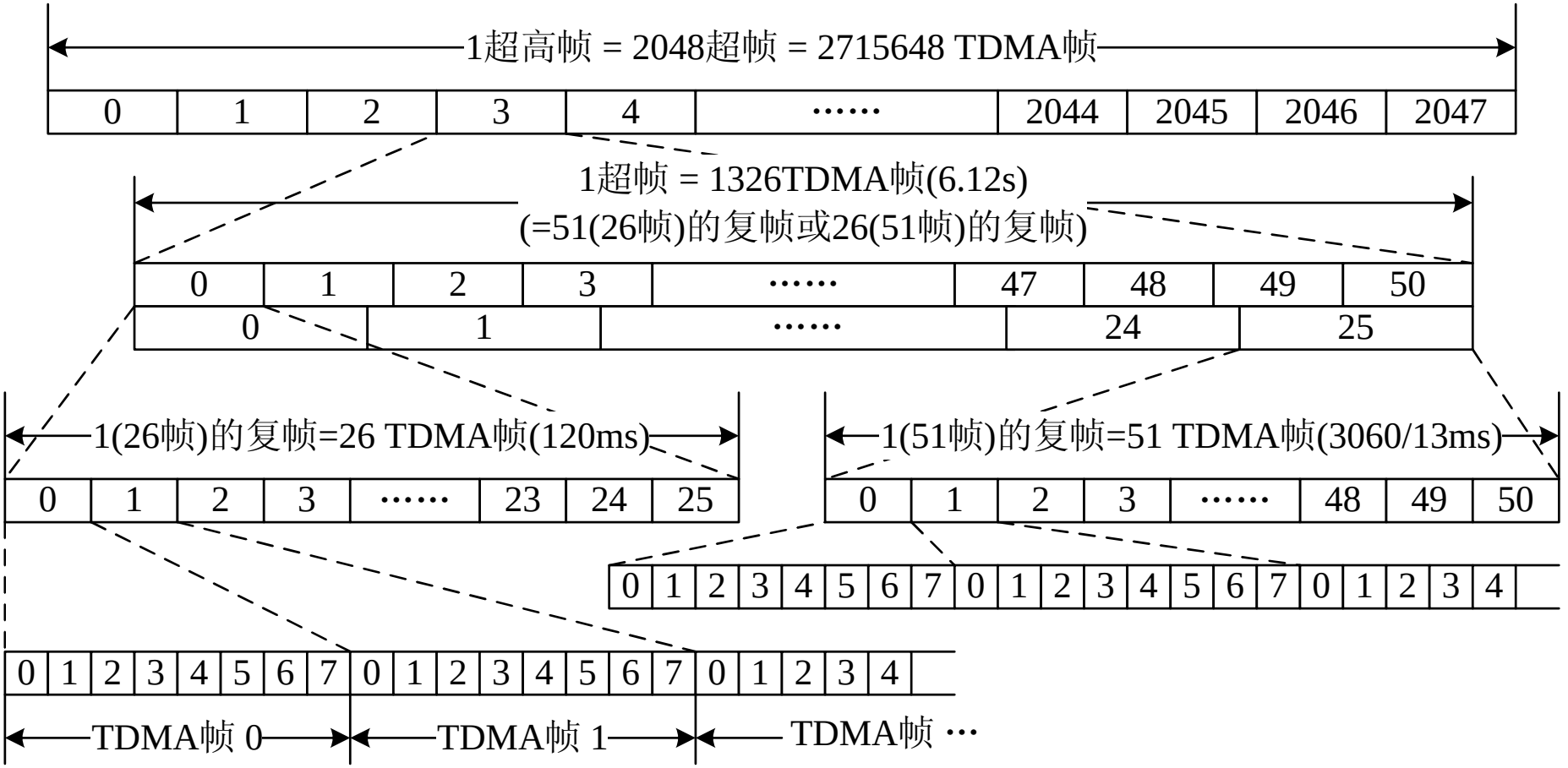


图: 全速率信道和半速率信道

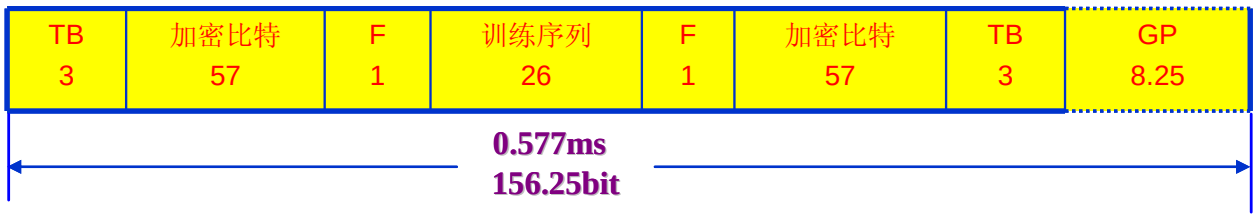
GSM 帧结构 I


1超高帧 = 2048超帧 = 2715648 TDMA帧
0 1 2 3 4 …… 2044 2045 2046 2047
1超帧 = 1326TDMA帧(6.12s)
(=51(26帧)的复帧或26(51帧)的复帧)
0 1 2 3 …… 47 48 49 50
0 1 …… 24 25
1(26帧)的复帧=26 TDMA帧(120ms)
0 1 2 3 …… 23 24 25
1(51帧)的复帧=51 TDMA帧(3060/13ms)
0 1 2 3 …… 48 49 50
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4
TDMA帧 0
TDMA帧 1
TDMA帧 …

突发脉冲 I

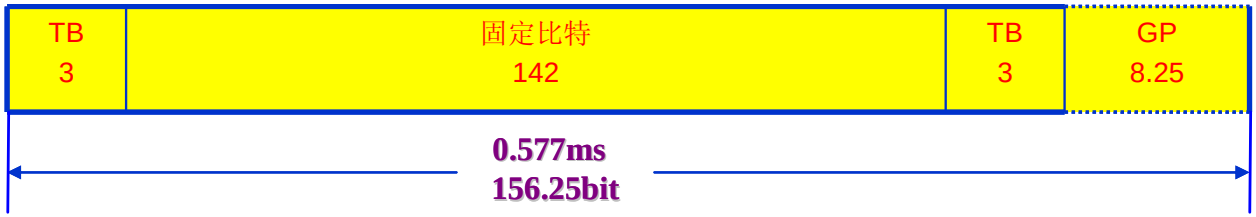
- 突发脉冲是以不同的信息格式携带不同逻辑信道, 是在一个时隙内传输的, 由 156.25 个调制比特组成的脉冲序列, 可看成是逻辑信道在物理信道传输的载体.
- 分类

- 普通突发脉冲（NB：Normal Burst）

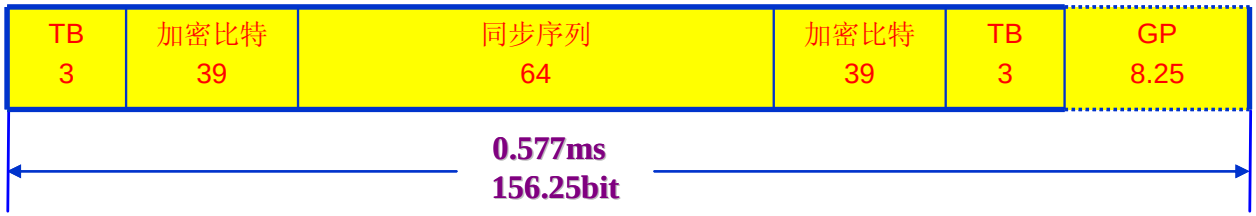


- 频率校正突发脉冲（FB：Frequency Correction Burst）

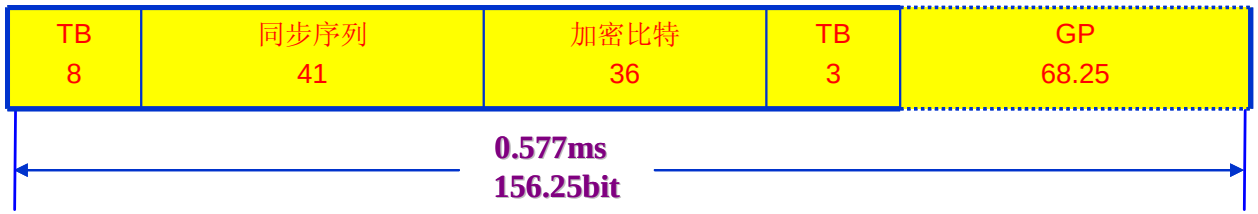
突发脉冲 II



- 同步突发脉冲（SB：Synchronization Burst）

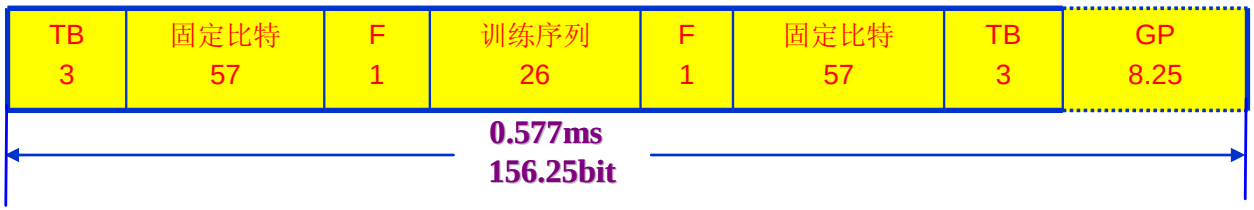


- 接入突发脉冲（AB：Access Burst）



- 空闲突发脉冲（DB：Dummy Burst）

突发脉冲 III



物理信道与逻辑信道的配置 I

- 问题
  - GSM 系统的逻辑信道数超过了一个载频所提供的 8 个物理信道
  - 通信的根本任务是利用业务信道传送语音或数据，而按照一对一的信道配置方法，在一个载频上已经没有业务信道的时隙了
- 解决方法: 将公共控制信道复用，即在一个或两个物理信道上复用公共控制信道

物理信道与逻辑信道的配置 II

- 映射对应关系
  - 一个基站有 N个载频，每个载频有 8 个时隙. 定义载频数为 f_0、f_1、f_2 、…、f_{N-1}, 每个载频有 8 个时隙, 分别用 $TS_0, TS_1, ..., TS_7$表示. 其中,f_0称为主载频. 逻辑信道到物理信道的映射关系为:f_0上的 TS_0 用于装载广播信道和公共控制信道,f_0上的 TS_1用于装载专用控制信道, 而 f_0上的 $TS_2 \sim TS_7$以及 $f_1 \sim f_{N-1}$上的全部时隙全部用于装载业务信道.
  - BCCH 和 CCCH 在 TS_0上的复用 (构成一个 51 个 TDMA 帧长的控制复帧)

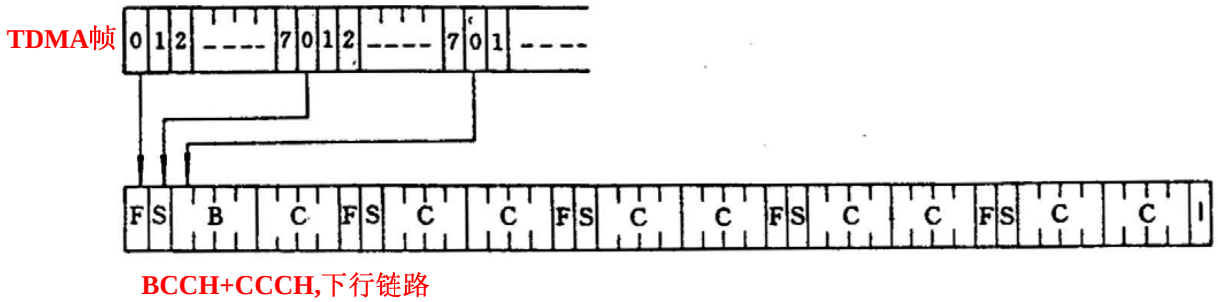


图: BCCH 和 CCCH 在 TS_0上的复用

物理信道与逻辑信道的配置 III

- RACH 在 TS_0上的复用 (公共控制信道中唯一的一个上行信道)

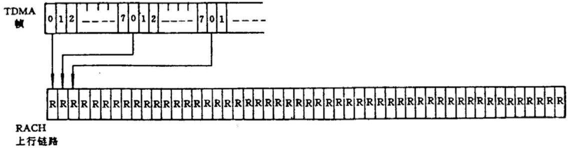


图: TS_0上 RACH 的复用

- 专用控制信道映射

物理信道与逻辑信道的配置 IV

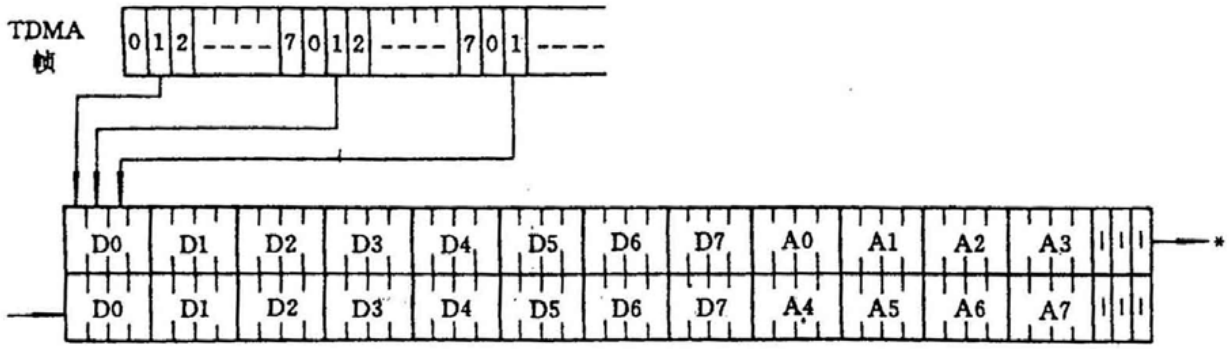


图: SDCCH 与 SACCH 在 TS_1 上的复用（下行）

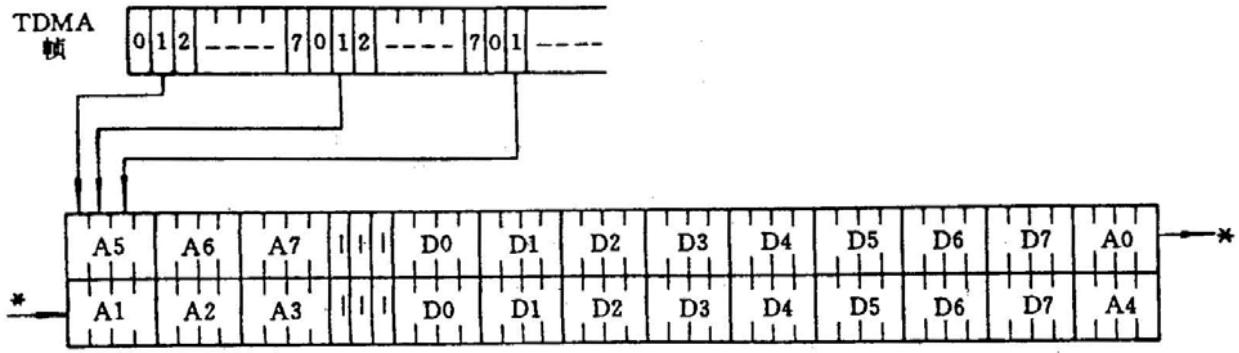


图: SDCCH 与 SACCH 在 TS1 上的复用（上行）

物理信道与逻辑信道的配置 V

- 业务信道映射 (构成一个 26 个 TDMA 帧长的业务复帧)

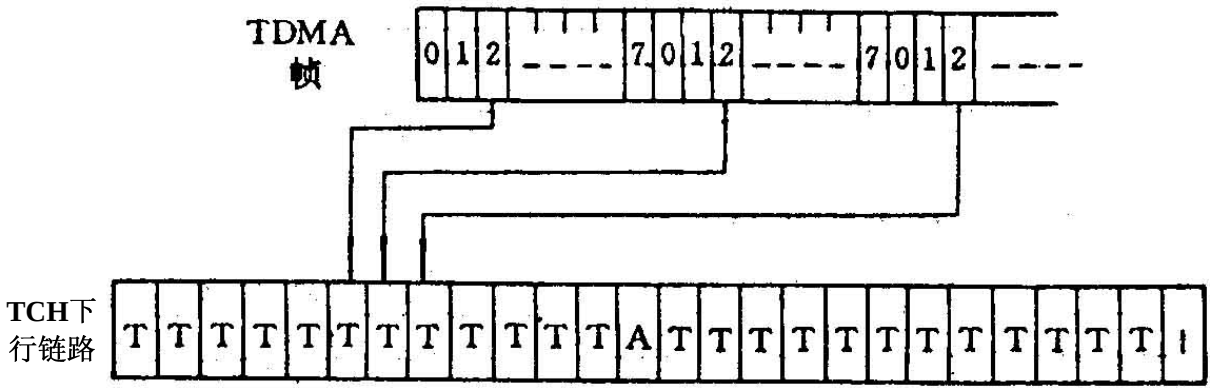


图: TCH 的复用

物理信道与逻辑信道的配置 VI

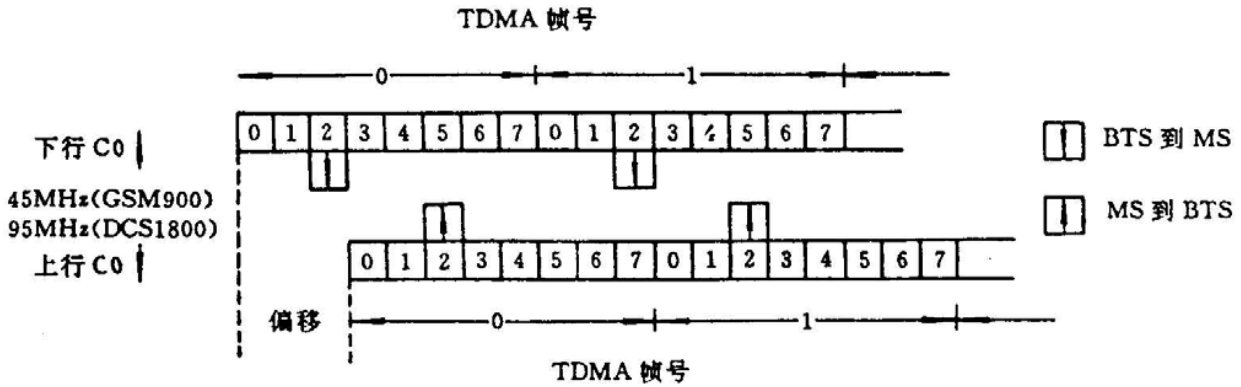


图: TCH 的上下行偏移

- 小结
  - TS_0：逻辑控制信道，重复周期为 51 个 TS
  - TS_1：逻辑控制信道，重复周期为 102 个 TS
  - $TS_2 \sim TS_7$：逻辑业务信道，重复周期为 26 个 TS
  - 其它 $f_1 \sim f_{N-1}$个载频的 $TS_0 \sim TS_7$时隙全部是业务信道

帧偏离、定时提前量与半速率信道 I

- 帧偏离
  - 前向信道的 TDMA 帧定时与反向信道的 TDMA 帧定时的固定偏差为 3 个时隙
  - 目的: 简化设计, 避免移动台在同一时隙收发, 从而保证收发的时隙号不变

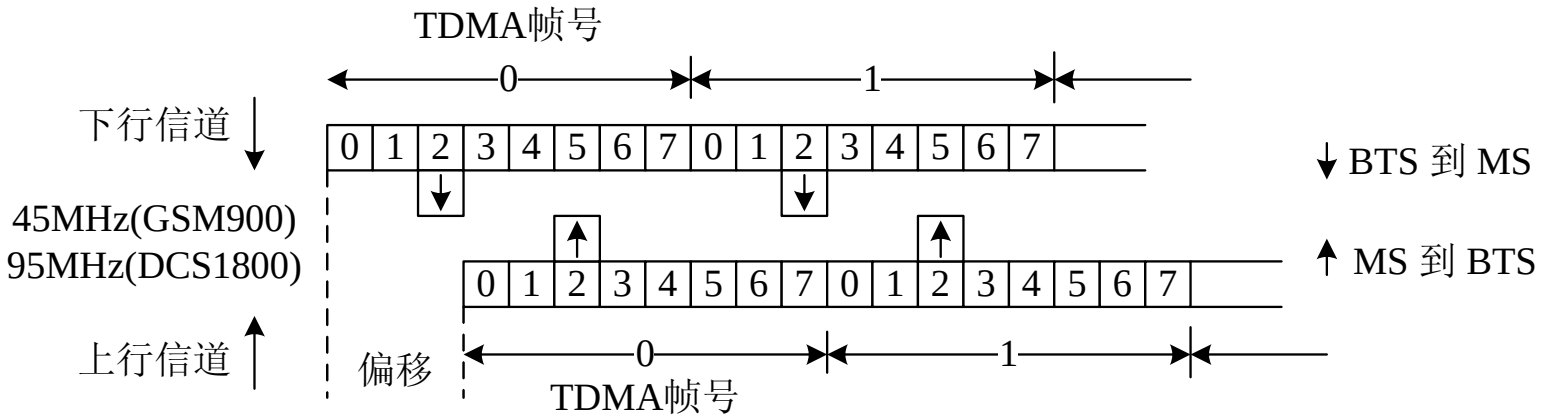
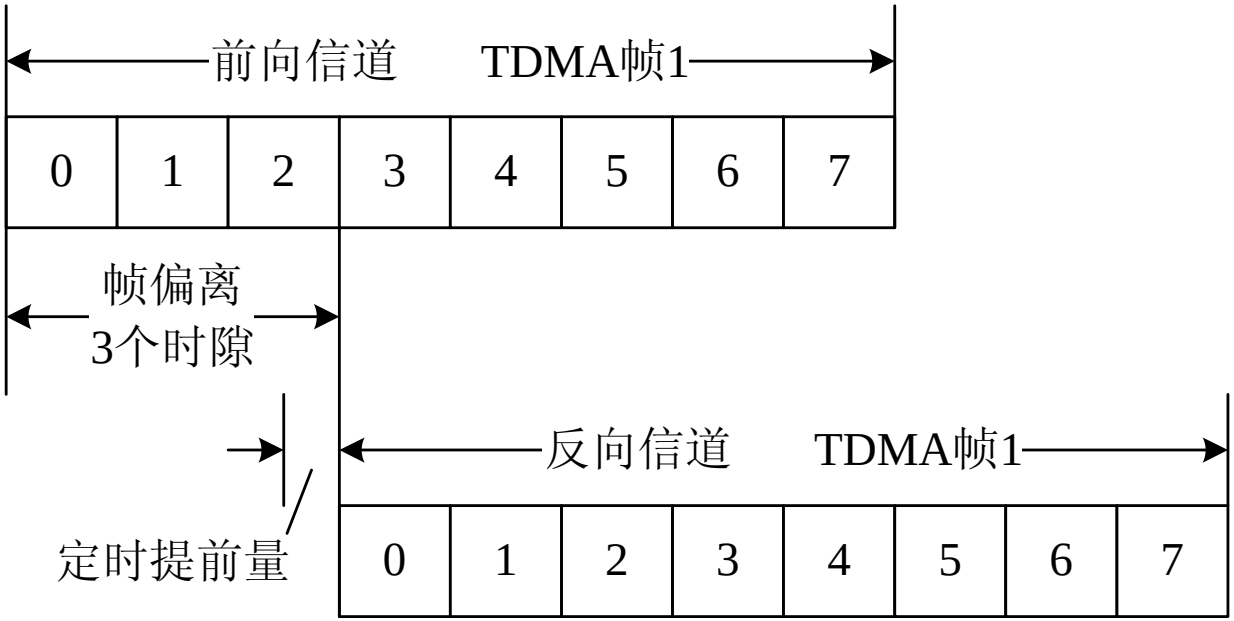


图: TCH 的上下行偏移

- 定时提前量

帧偏离、定时提前量与半速率信道 II

- 基站指示移动台以一定的提前量发送突发脉冲, 以补偿传播时延.
- 目的: 克服由突发脉冲的传输延时所带来的定时的不确定
- 方法:BTS 根据自己脉冲时隙与接收到的 MS 时隙之间的时间偏移测量值，在 SACCH 上通知 MS 所要求的时间提前量. 正常通话中, 当 MS 接近基站时, 基站就会通知 MS 减小时间提前量; 而当 MS 远离小区中心时, 基站就会要求 MS 加大时间提前量.



帧偏离、定时提前量与半速率信道 III

图: GSM 帧偏离与定时提前量

contents

GSM 系统无线信道的衰落特性 I

- 多径衰落
- 阴影衰落
- 问题: 信号衰落, 信号传输差错 (突发性错误), 时延扩展, 码间干扰

GSM 系统中的抗衰落技术 I

- 信道编码与交织
  - 编码方案: 混合编码, 有块卷积码, 纠错循环码, 奇偶码
  - 交织方法
    - 输入码流是 20ms 的帧, 每帧含 456bit. 每两帧（40ms）共 912bit, 按每行 8 位写入, 共写入 114 行
    - 输出按列输出, 每次读出 114bit, 恰好对应 GSM 的一个 TDMA 时隙
    - 当前帧的 456bit 分别与第 n-1 帧后半帧的 228bit 和第 n+1 帧前半帧的 228bit 交织 (即,GSM 采用了二次交织的方法)

GSM 系统中的抗衰落技术 II

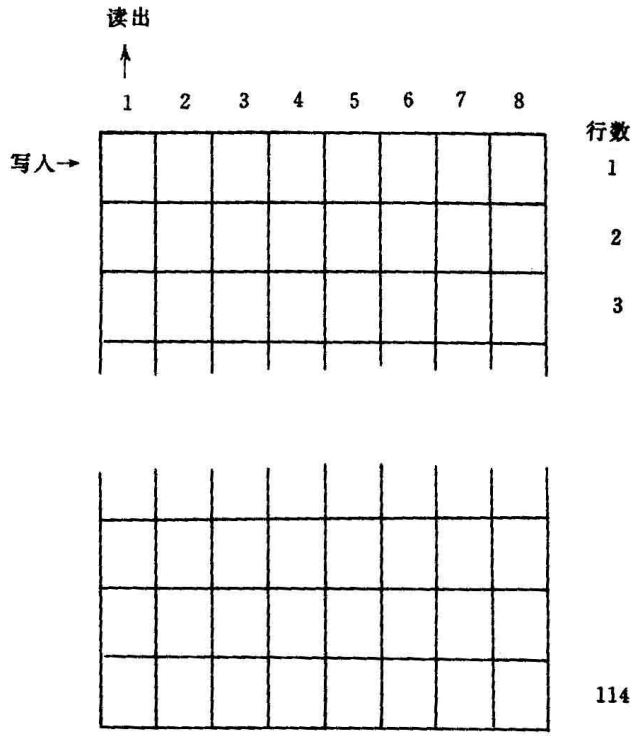
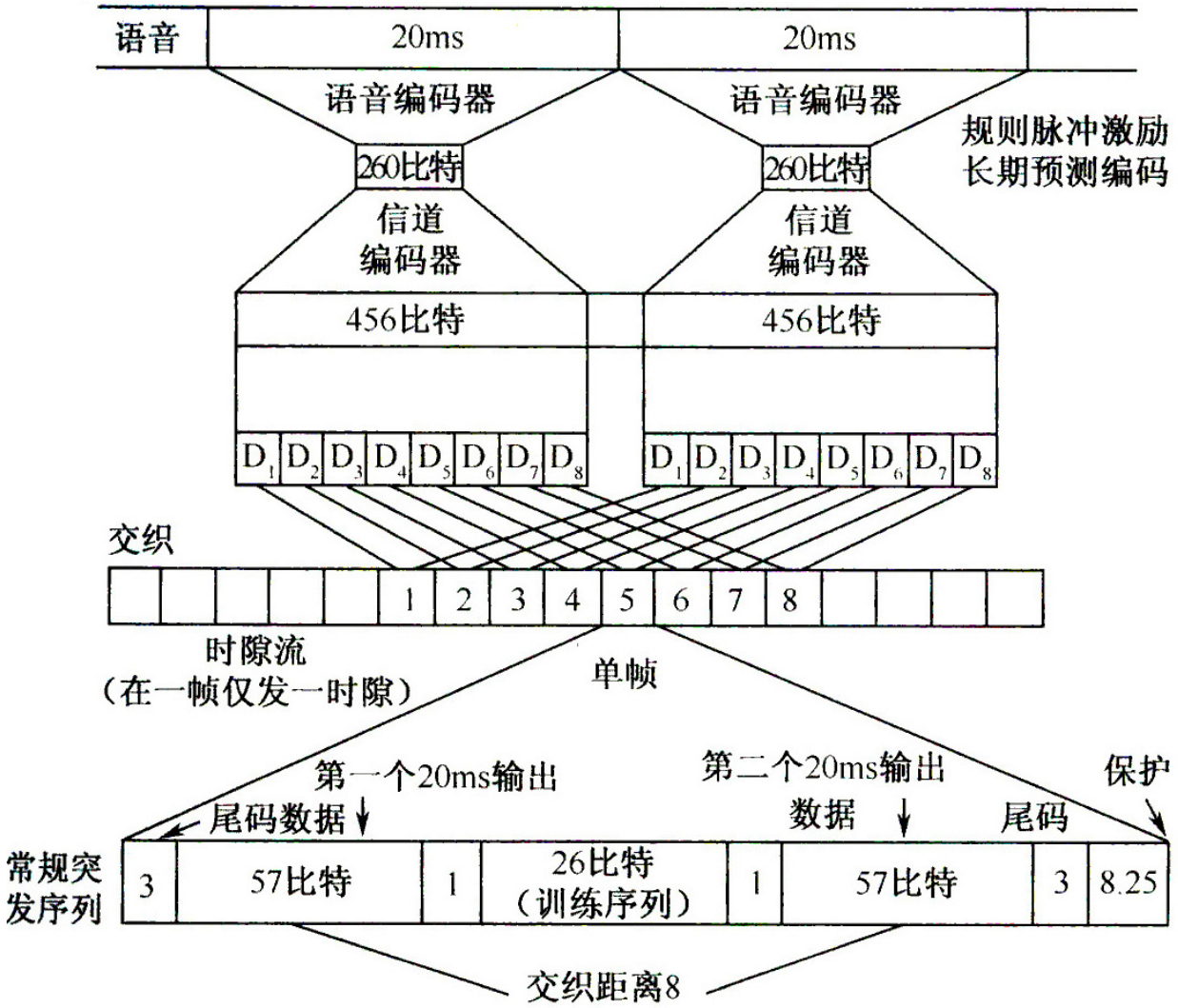


图: 交织编码矩阵

GSM 系统中的抗衰落技术 III



GSM 系统中的抗衰落技术 IV

图: GSM 的二次交织技术

- 维特比 (Viterbi) 均衡与天线分集
  - GSM 标准中并没有对采用哪种均衡算法做出规定, 大多数 GSM 系统中采用 Viterbi 均衡算法来对抗码间干扰.
  - GSM 采用天线分集技术对抗多径衰落.
- 跳频技术
  - GSM 采用每帧改变频率的方法, 即每隔 4.615ms 跳频一次, 属于慢跳频.
  - GSM 跳频在时隙和频隙上进行, 即在一定的时间间隔不断地在不同的频隙上跳频

GSM 系统中的抗衰落技术 V

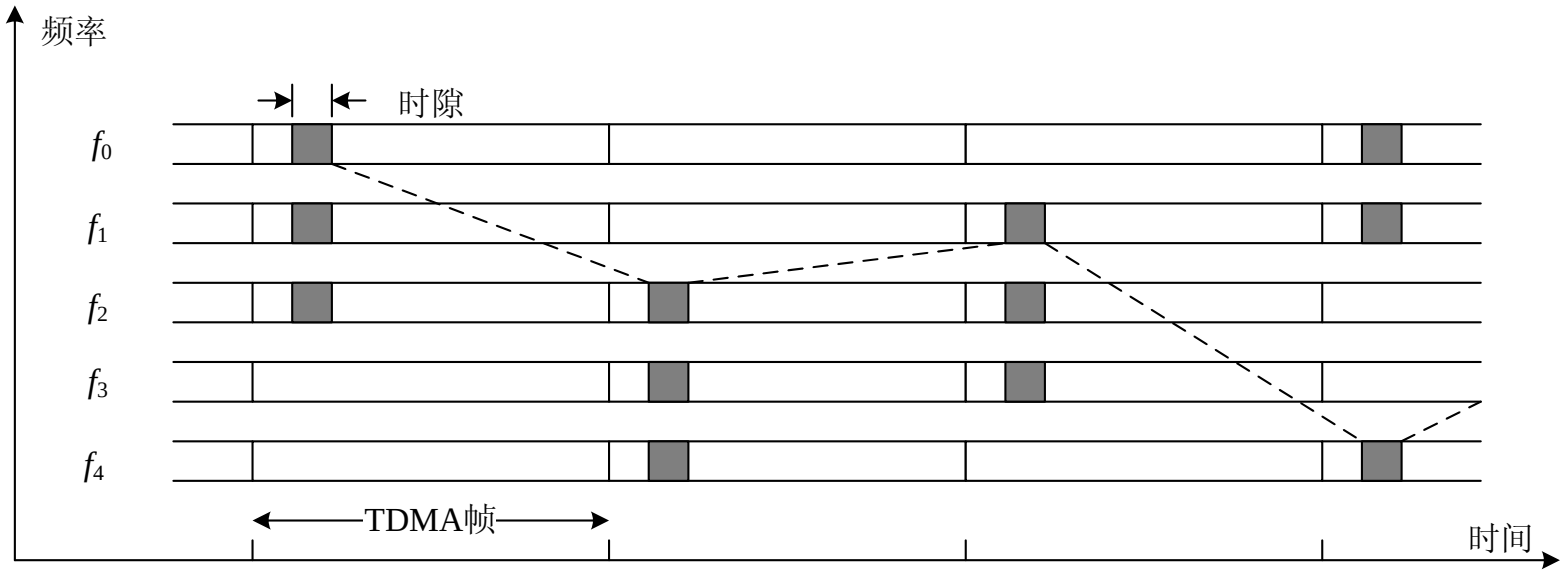


图: GSM 慢跳频示意图

- 跳频只在业务信道上进行, 在公共信道（广播控制信道和公共控制信道）上必须使用固定频率.

GSM 系统中的抗衰落技术 VI

- 在一个频道上,GSM 最多有 64 种不同的跳频序列, 描述参数: 跳频序列号 (HSN) 和移动指配偏置度 (MAIO).HSN（0～63）是规定跳频时采用哪种算法进行循环, 而 MAIO（取值要根据跳频集内的频点数决定）则是从哪个频点开始循环的指示, 即起跳点.
  例：Cell A 的频点集 MA=1,4,7,10,13,⋯,HSN 的取值是 0-63,0 为循环序列,1-63 为随机序列.
  - HSN ＝ 0，跳频次序＝ 1,4,7,10,13,⋯
  - HSN ＝ 2，跳频次序＝ 1,10,4,13,7,⋯
    使用 MAIO ＝ 0, 跳频次序＝ 1,10,4,13,7,⋯
    使用 MAIO ＝ 1, 跳频次序＝ 10,4,13,7,16,⋯
    使用 MAIO ＝ 2, 跳频次序＝ 4,13,7,16,19,⋯

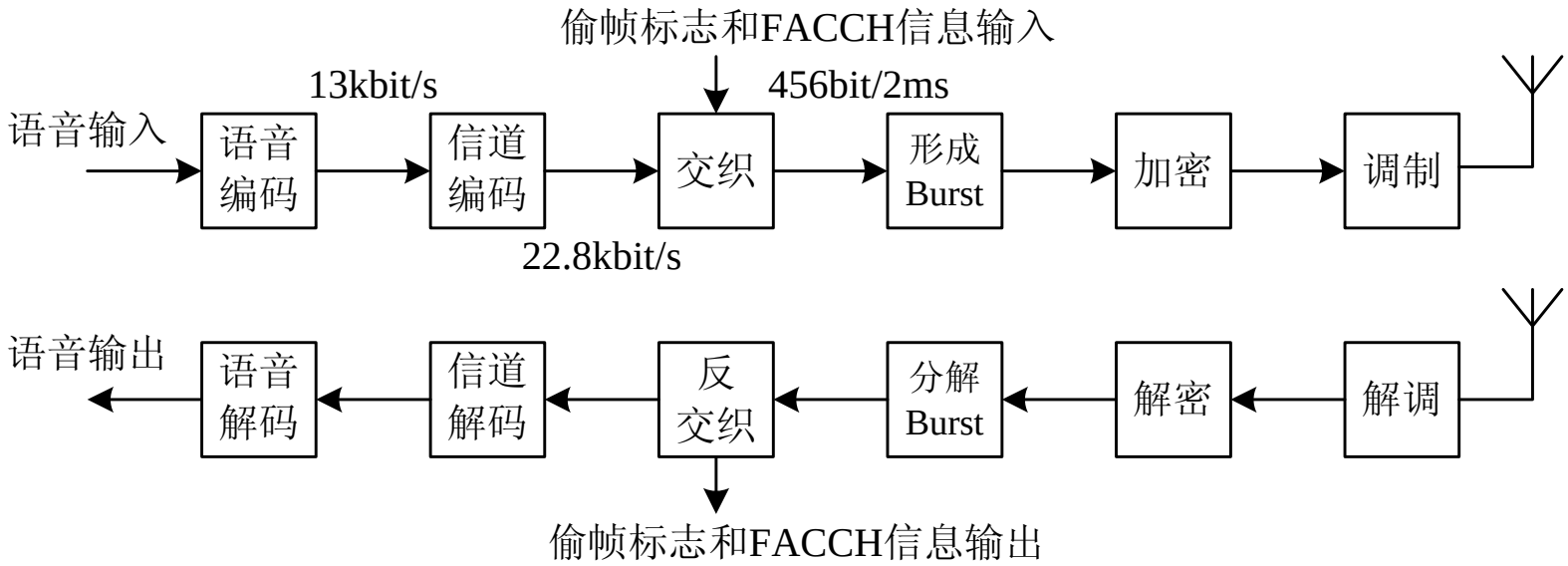
  注意: 同一个小区内,HSN 取值相同, 仅仅给每个用户分配不同的 MAIO; 对于同频邻区, 一定要保证 HSN 不同, 这样可以最大程度的减小同频干扰.
- 话音激活与功率控制
  - 目的: 有效地减少同道干扰

GSM 系统中的抗衰落技术 VII

- 话音激活控制就是采用非连续发射 (DTX), 在发送端有一个话音激活检测器 (VAD), 检测是否有话音或仅仅是噪声, 在发射机和接收机上还分别有舒适噪声发生器.
- GSM 功率控制, 支持基站和移动台各自独立地进行发射功率控制, 总的控制范围是 30dB，每步调节范围是 20dB，从 20mW 到 20W 之间的 16 个功率电平，每步精度为 ±3dB，最大功率电平的精度为 ±1.5dB.
- 功率控制过程: 移动台测量信号强度和信号质量, 并定期向基站报告，基站按预置的门限参数与之相比较，然后确定发射功率的增减量. 同理，移动台按预置的门限参数与之相比较，然后确定发射功率的增减量.
- 在实际应用中, 主要是对移动台的发射功率进行控制.

GSM 系统中的话音处理过程 I

- 语音编码方案:13kbit/s RPE-LTP 码（规则脉冲激励长期预测）
- 抽样频率 8kHz，A 率量化，把语音分成 20ms 为单位的段，每个段编成 260bit 的数据块，然后对每个小段分别编码。编码速率 13kbps（全速率）。



contents

概述 I

- 移动通信中, 为了建立一个呼叫连接需要解决的问题有:
  - 用户所在的位置
  - 用户识别
  - 用户所需提供的业务
- 主要操作过程
  - 网络附着/分离（位置登记/删除）
  - 位置更新
  - 越区切换
  - 安全保密
  - 呼叫接续
- 区域划分
  - 小区 (Cell): 移动网的最小单元
  - 基站区: 一个基站控制的区域

概述 II

- 采用全向天线, 一个基站只包含一个小区
- 采用定向天线, 一个基站可能包含几个扇形小区

- 位置区：可由几个基站区组成
  - 设立位置区是为了缩小寻呼范围, 不必在 MSC 所辖的所有小区中寻呼
- 移动业务交换区: 一个 MSC 管辖的区域
  - 可由若干个位置区组成
  - 一个公众移动网通常包含多个移动业务区
- PLMN 区: 一个 PLMN 能够覆盖的区域
- 服务区: 移动通信网络覆盖到的区域
  - 在这个区域中, 用户可以直接拨叫移动台, 不必知道移动台的实际位置

- 号码与地址识别
  - 移动台 ISDN 号码 (MSISDN)

概述 III

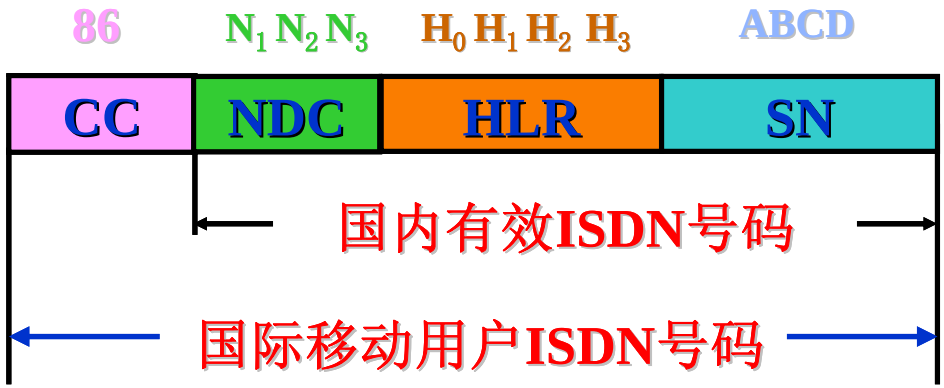


图: MSISDN 的号码结构

- CC 为国家代码，我国为 86. 国内有效 ISDN 号码,11 位
- NDC 数字蜂窝移动业务接入号,13S(S = 9、8、7、6、5 移动通信公司), 联通公司目前的接入网号为 (130,131)
- HLR 识别号:H0 H1 H2 H3
- SN(移动用户号), 由各 HLR 自行分配

- 国际移动客户识别码 (IMSI)
  - 移动用户的唯一识别号码 (15 位数字组成), 在无线信道上唯一能识别用户身份的就是 IMSI

概述 IV

- IMSI 是系统内部对每个用户的标识, 手机号码 MSISDN 在系统中是被转换成 IMSI 进行通信的

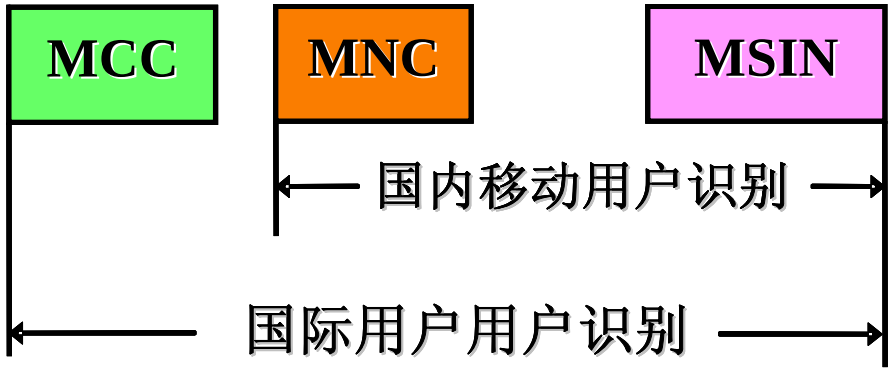


图: IMSI 的号码结构

  - MCC, 移动国家号码, 我国为 460. 移动网号 MNC,2 位, 识别移动用户归属的移动网. 移动用户识别码 MSIN,10 位, 由各国自行分配
- 移动客户漫游号码 (MSRN）
  - 正在服务于被呼用户的 MSC/VLR 产生一个移动台漫游号码 MSRN
  - MSC/VLR 将呼叫的路由信息传送给 HLR，用于 GMSC 寻址 VMSC 所用，在接续完成后立即释放
- 位置区识别码 (LAI)

概述 V

- 结构:MCC(3 位)+MNC(2 位)+LAC(16 位)
- 在检测位置更新时, 要使用位置区识别 LAI

- 全球小区识别码 (CGI)
  - 结构:MCC+MNC+LAC+CI(16 位)
  - 是所有 GSM PLMN 中小区的唯一标识, 是在位置区识别 LAI 的基础上再加上小区识别 CI 构成
- 基站识别码 (BSIC)
  - 结构:NCC(网络色码 2 位)+BCC(基站色码,2 位)
  - 用于移动台识别相邻的、采用相同载频的、不同的基站收发信台（BTS）, 特别用于识别在不同国家的边界地区采用相同载频的相邻 BTS

位置更新 I

- 网络附着和分离
  - 目的: 使网络能够掌握 MS 当前所处位置, 并将其位置信息保存起来, 以便在需要时能够迅速连接上移动台、实现正常通信. 通常, 移动台的位置信息存储在归属位置寄存器 (HLR) 和访问位置寄存器 (VLR) 这两个功能实体中.
  - MS 第一次开机 (首次登记)
    当一个移动用户首次入网时, 由于在其 SIM 卡中找不到位置区识别码 (LAI), 它会立即申请接入网络, 向 MSC 发送“位置更新请求”信息, 通知 GSM 这是一个该位置区内的新用户.MSC 根据该移动台发送的 IMSI 中的信息, 向该移动台的归属位置寄存器发送“位置更新请求”信息.HLR 把发送请求的 MSC 的号码记录下来, 并向该 MSC 回送“位置更新接受”信息. 至此, MSC 认为此移动台已被激活, 便要求访问位置寄存器 (VLR) 对该移动台作“附着”标记, 并向移动台发送“位置更新证实”信息, 移动台会在其 SIM 卡中把信息中的位置区识别码存储起来, 以备后用.

位置更新 II

- MS 不是第一次开机 (重新开机)
  移动台每次一开机, 就会收到来自于其所在位置区中的广播控制信道 (BCCH) 发出的位置区识别码 (LAI), 它自动将该识别码与自身存储器中的位置区识别码 (上次开机所处位置区的编码) 相比较. 若相同, 则说明该移动台的位置未发生改变, 无需位置更新, 只需要在 VLR 中对该用户作“附着”标记. 否则, 认为移动台已由原来位置区移动到了一个新的位置区中, 必须进行位置更新.
  此时, 又可以有两种情况，即前后位置区是否属于同一个 VLR 控制区。若是，则只需要在 VLR 中更改成新的 LAI 并进行 IMSI“附着”即可; 若不是，则需要向 HLR 发起“位置更新请求”，以便由其 HLR 通知原位置区中的 VLR 删除该移动台的相关信息.
- MS 关机, 从网络中” 分离”
  当移动台由激活（开机）转换为非激活（关机）状态时，应启动 IMSI 分离进程，在相关的 HLR 和 VLR 中设置标志，使得网络拒绝对该移动台的呼叫, 不再浪费无线信道发送呼叫信息.
- 周期性登记

位置更新 III

- 为了防止某些意外情况的发生, 进一步保证网络对移动台所处位置及状态的确知性, 而强制移动台以固定的时间间隔周期性地向网络进行的位置登记.
- 可能发生的意外情况如: 当移动台向网络发送“IMSI 分离”信息时, 由于无线信道中的信号衰落或受噪声干扰等原因, 可能导致 GSM 系统不能正确译码, 这就意味着系统仍认为该移动台处于附着状态. 再如, 当移动台在开机状态移动到系统覆盖区以外的地方, 即盲区之内时, GSM 系统会认为该移动台仍处于附着状态.

- 位置更新
  - 目的: 移动台向网络登记其新的位置区, 使网络能够跟踪移动台的运动, 以保证在有此移动台的呼叫时网络能够正常接续到该移动台
  - 同 MSC/VLR 内的位置更新
  - 不同 MSC / VLR 之间的位置更新 (越局位置更新)

位置更新 IV

图中, 移动台由 cell3 移动到 cell4 中的情况, 就属于同 MSC (MSCA) 中不同位置区的位置更新; 移动台由 cell3 移动到 cell5 中的情况, 就属于不同 MSC(MSCA 和 MSCB) 之间不同位置区的位置更新.

- 位置更新过程

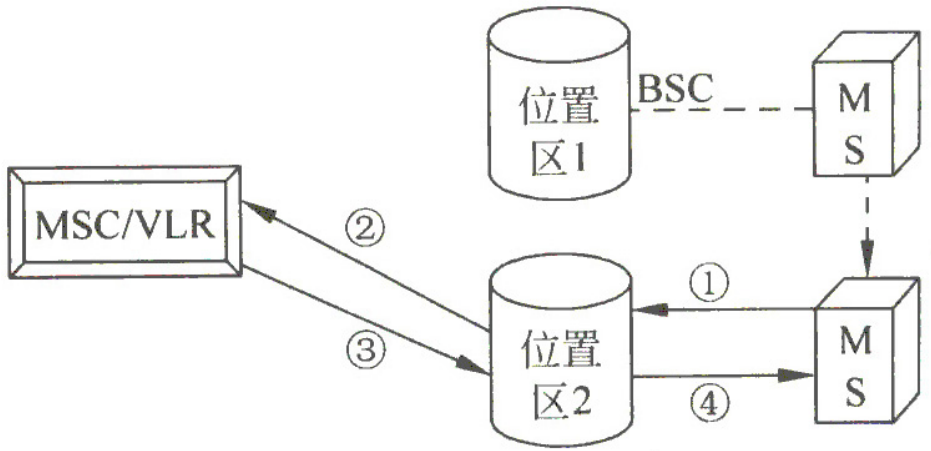


图: 同一 MSC 局内位置更新

位置更新 V

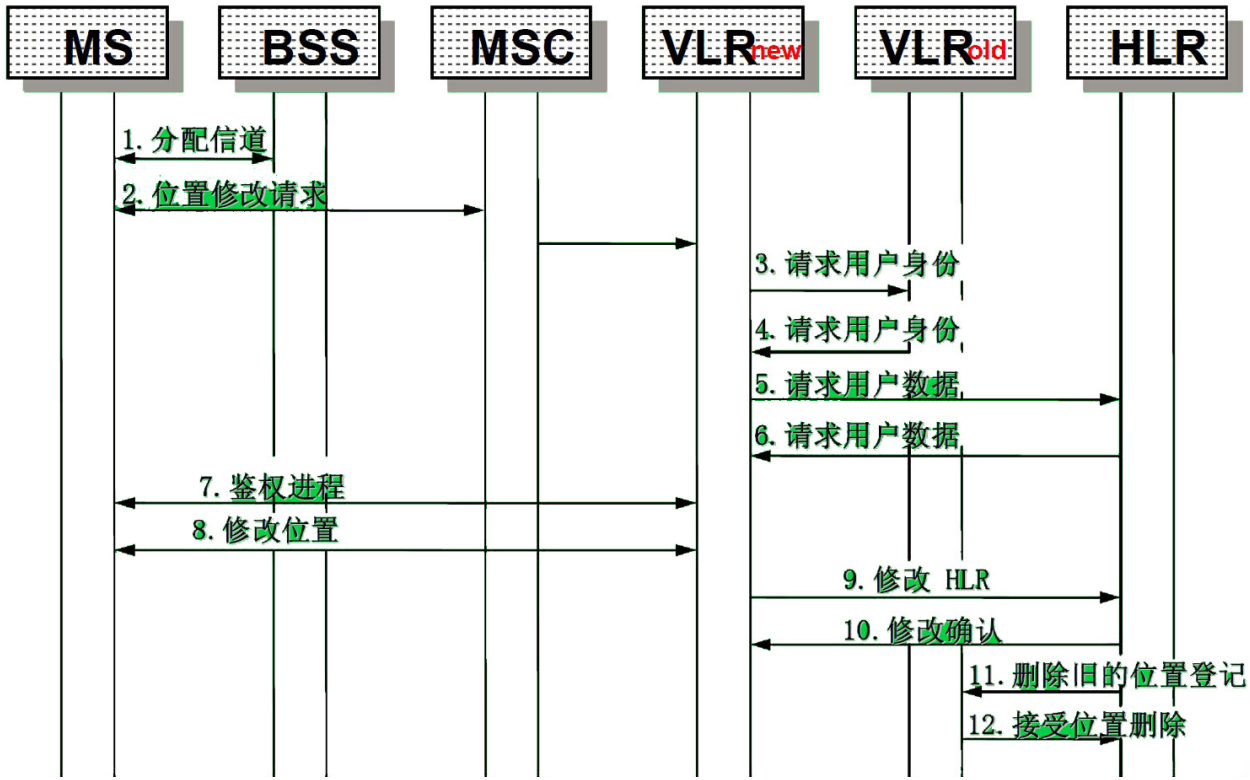


图: 越局位置更新过程

越区切换与漫游 I

- 将正处于通话状态的 MS 转移到新的业务信道上（新的小区）的过程, 保证通信的连续性
- 原因
  - 信号强度或质量下降到门限以下, 此时移动台被切换到信号强度较强的相邻小区, 由移动台发起
  - 由于某小区业务信道容量全被占用或几乎全被占用, 这时移动台被切换到业务信道容量较空闲的相邻小区, 由上级实体发起
- 操作
  - 识别和确定新的目标小区
  - 分配给移动台在新小区的话音信道和控制信道
- GSM 越区切换策略
  - 硬切换, 分散控制, 移动台与基站均参与测量接受信号的强度 (RSSI) 和质量 (BER)
- 信道链路指标

越区切换与漫游 II

  - WEI(word error indicator), 表明在 MS 侧当前的突发脉冲是否得到正确解调
  - RSSI (received signal strength indicator), 反映信道间干扰和噪声
  - QI(quality indicator), 在一个有效窗口内用载干比 (S/I) 加上信噪比来估计无线信号质量
- 越区切换的种类
  - 同一 BSC 内不同小区间的切换
  - 同一 MSC/VLR 内不同 BSC 控制的小区间的切换
  - 不同 MSC/VLR 控制的小区间的切换
- 同一 BSC 内不同小区间的切换

图: 同 BSC 内 BTS 间的切换

越区切换与漫游 III

(1)BSC 预订新的 BTS 激活一个 TCH;
(2)BSC 通过旧 BTS 发送一个包括频率、时隙及发射功率参数的信息至 MS, 此信息在 FACCH 上传送;
(3)MS 在规定新频率上发送一个切换接入突发脉冲, 通过 FACCH 发送;
(4) 新 BTS 收到此突发脉冲后, 将时间提前量信息通过 FACCH 回送 MS;
(5)MS 通过新 BTS 向 BSC 发送一切换成功信息;
(6)BSC 要求旧 BTS 释放 TCH

越区切换与漫游 IV

- 同一 MSC/VLR 内不同 BSC 控制的小区间的切换

图: 同 MSC/VLR 内不同 BSC 的切换

(1) 旧 BSC 把切换请求及切换目的小区标识一起发给 MSC;
(2)MSC 判断是哪个 BSC 控制的 BTS, 并向新 BSC 发送切换请求;
(3) 新 BSC 预订目标 BTS 激活一个 TCH;
(4) 新 BSC 把包含有频率时隙及发射功率的参数通过 MSC, 旧 BSC 和旧 BTS 传到 MS;
(5)MS 在新频率上通过 FACCH 发送接入突发脉冲;
(6) 新 BTS 收到此脉冲后回送时间提前量信息至 MS;
(7)MS 发送切换成功信息通过新 BSC 传至 MSC;
(8)MSC 命令旧 BSC 去释放 TCH;
(9)BSC 转发 MSC 命令至 BTS 并执行

越区切换与漫游 V

- 不同 MSC/VLR 控制的小区间的切换

图: 不同 MSC/VLR 控制的小区间的切换

(1) 旧 BSC 把切换目标小区标志和切换请求发至旧 MSC;
(2) 旧 MSC 判断出小区属另一 MSC 管辖;
(3) 新 MSC 分配一个切换号 (路由呼叫用) 并向新 BSC 发送切换请求;
(4) 新 BSC 激活 BTS 的一个 TCH;
(5) 新 MSC 收到 BSC 回送信息并与切换号一起转至旧 MSC;
(6) 一个 MSC 间的连接建立也许会通过 PSTN 网;
(7) 旧 MSC 通过旧 BSC 向 MS 发送切换命令其中包含频率时隙和发射功率;
(8)MS 在新频率上通过 FACCH 发一接入突发脉冲;

越区切换与漫游 VI

(9) 新 BTS 收到后通过 FACCH 回送时间提前量信息;
(10)MS 通过新 BSC 和新 MSC 向旧 MSC 发送切换成功信息

安全措施 I

- 对用户接入网的鉴权
  - 目的
    - 保护网络, 防止非法盗用;
    - 保护用户, 拒绝假冒合法用户的” 入侵”;
    - 通过鉴权, 系统可以为合法的用户提供服务, 对不合法的用户拒绝服务
  - 鉴权场合
    - 移动用户发起呼叫 (不含紧急呼叫);
    - 移动用户接受呼叫;
    - 移动台位置登记;
    - 移动用户进行补充业务操作
    - 切换
  - 鉴权原理: 基于 GSM 系统定义的鉴权键 Ki
    - 当客户在网络上注册登记时, 会被分配一个 MSISDN、一个 IMSI 及一个与 IMSI 对应的移动用户鉴权键 Ki;
    - Ki 被分别存放在网络端的鉴权中心 AUC 中和移动用户的 SIM 卡中;
    - 最简单的鉴权就是在 VLR 中验证网络端和用户端的 Ki 是否相同;
    - 问题: 用户将鉴权键 Ki 传输给网络时可能被人截获;

安全措施 II

- 解决方法: 用鉴权算法 A3 产生鉴权数据—符号响应 (SRES,Signed Response)

- 鉴权三元组（三参数）, 在鉴权中心 AUC 中产生
  - 随机数 RAND
  - 符号响应 SRES
  - 密钥 Kc
- 鉴权和加密算法
  - A3 算法: 鉴权
  - A8 算法: 产生一个供用户数据加密使用的密钥 Kc
  - A5 算法: 用户数据加密

安全措施 III

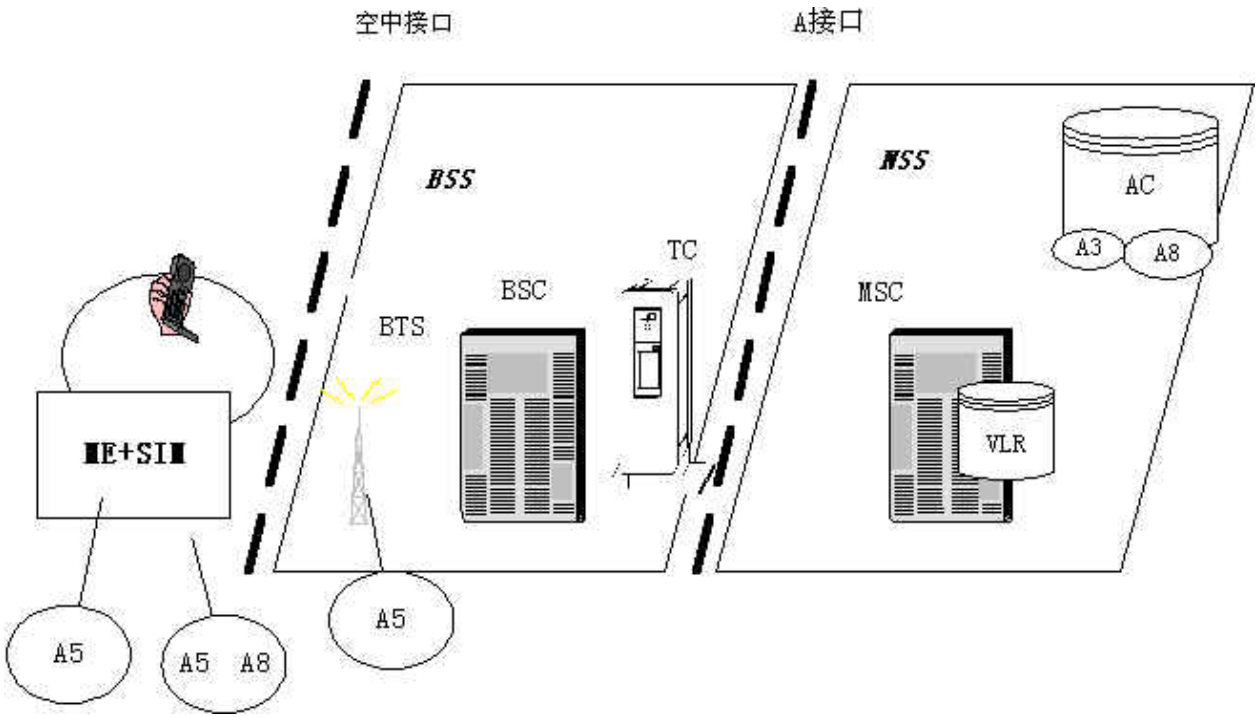


图: 安全算法的位置

安全措施 IV

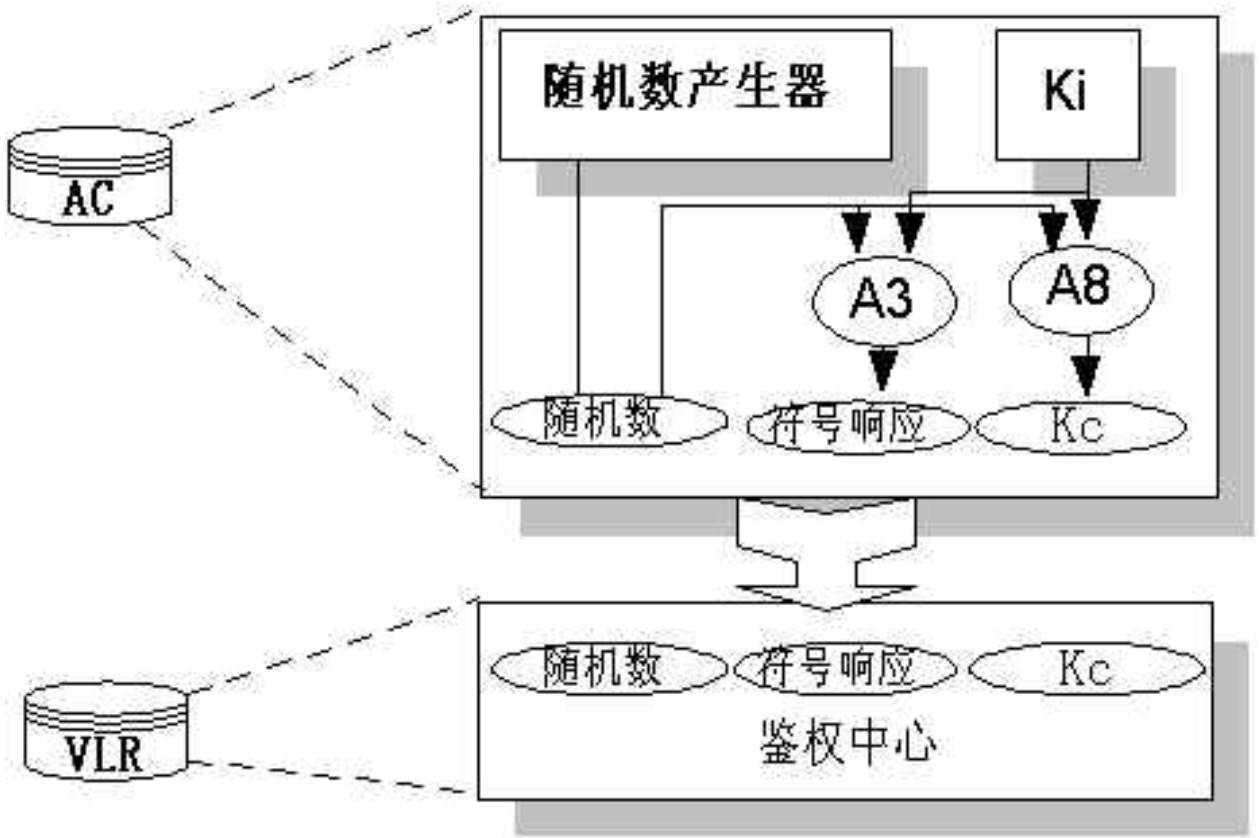


图: 鉴权三参数产生过程

安全措施 V

- 鉴权过程
  1.MSC、VLR 传送 RAND 至 MS;
  2.MS 用 RAND 和 Ki 算出 SRES 并返回 MSC/VLR
  3.MSC/VLR 把收到的 SRES 与存储在其中的 SRES 比较

安全措施 VI

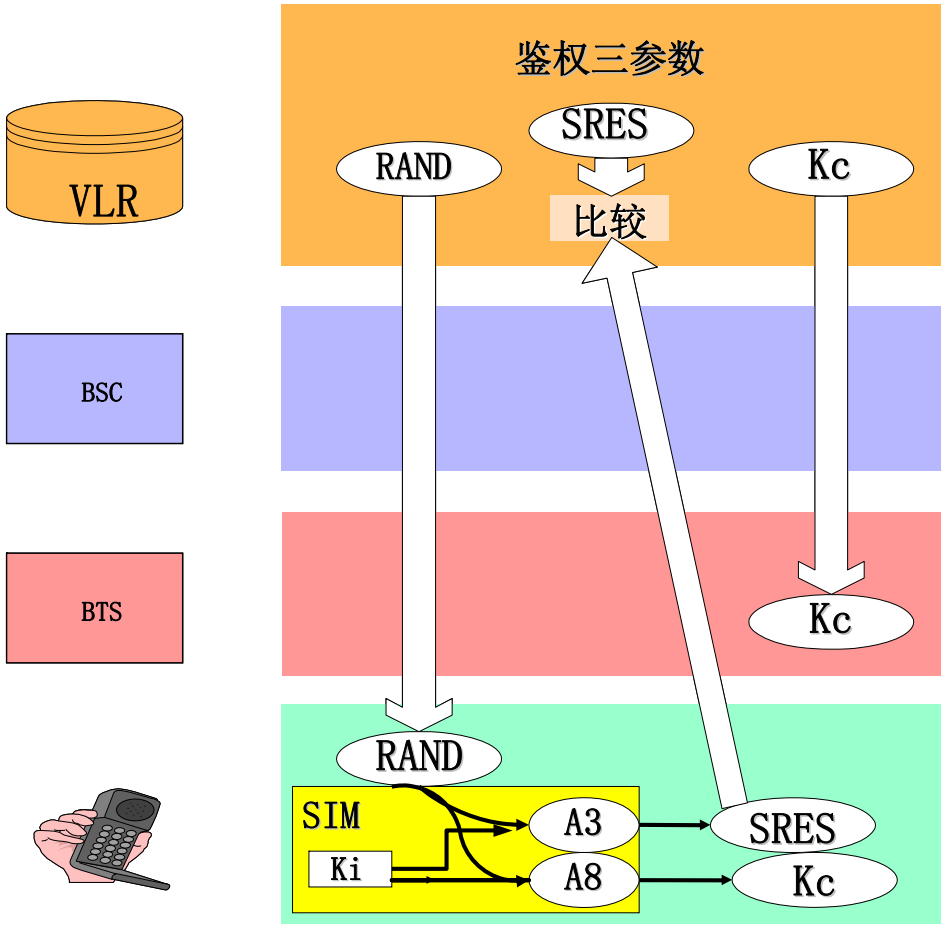


图: 鉴权过程

安全措施 VII

关于鉴权的几点说明:
(1) 由于鉴权中心提供的三参数组总是与每个用户相关连的, 因此通常 AUC 与 HLR 是合在同一个实体 (HLR/AUC) 中, 或者 AUC 直接与 HLR 相连
(2)MSC/VLR 在每次呼叫过程中通过检查系统所提供的和用户响应的三参数是否一致来鉴定用户身份的合法性
(3) 一般情况下, AUC 一次能产生这样的 5 个三参数组.AUC 会把这些三参数组传送给用户的 HLR, HLR 自动存储, 以备后用. 对一个用户, HLR 最多可存储 10 组三参数. 当 MSC / VLR 向 HLR 请求传送三参数组时,HLR 会一次性地向 MSC / VLR 传送 5 组三参数组.MSC / VLR 一组一组地用, 当用到只剩 2 组时, 就向 HLR 请求再次传送. 这样做的一大好处是鉴权算法程序的执行时间不占用移动用户实时业务的处理时间, 有利于提高呼叫接续速度.
(4) 鉴权算法 (A3) 和加密算法 (A5 和 A8) 都由泛欧移动通信谅解备忘录组织 (即 GSM 的 MOU 组织) 进行统一管理, GSM 运营部

安全措施 VIII

门需与 MOU 签署相应的保密协定后方可获得具体算法, 用户识别卡 (SIM 卡) 的制作商也需签定协议后才能将算法写到 SIM 卡中.

- 无线链路上信息的加密
  - 目的: 在空中对用户数据和信令的保密
  - 过程
    - 加密开始时根据 MSC/VLR 发出的加密指令,BTS 侧和 MS 侧均开始使用 Kc
    - MS 侧, 由 Kc、TDMA 帧号一起经 A5 算法, 对用户信息数据流加密, 在无线路径上传输
    - BTS 侧, 把从无线信道上收到的加密信息流、TDMA 帧号和 Kc, 再经过 A5 算法解密后, 传送给 BSC 和 MSC
    - 上述过程反之亦然

安全措施 IX

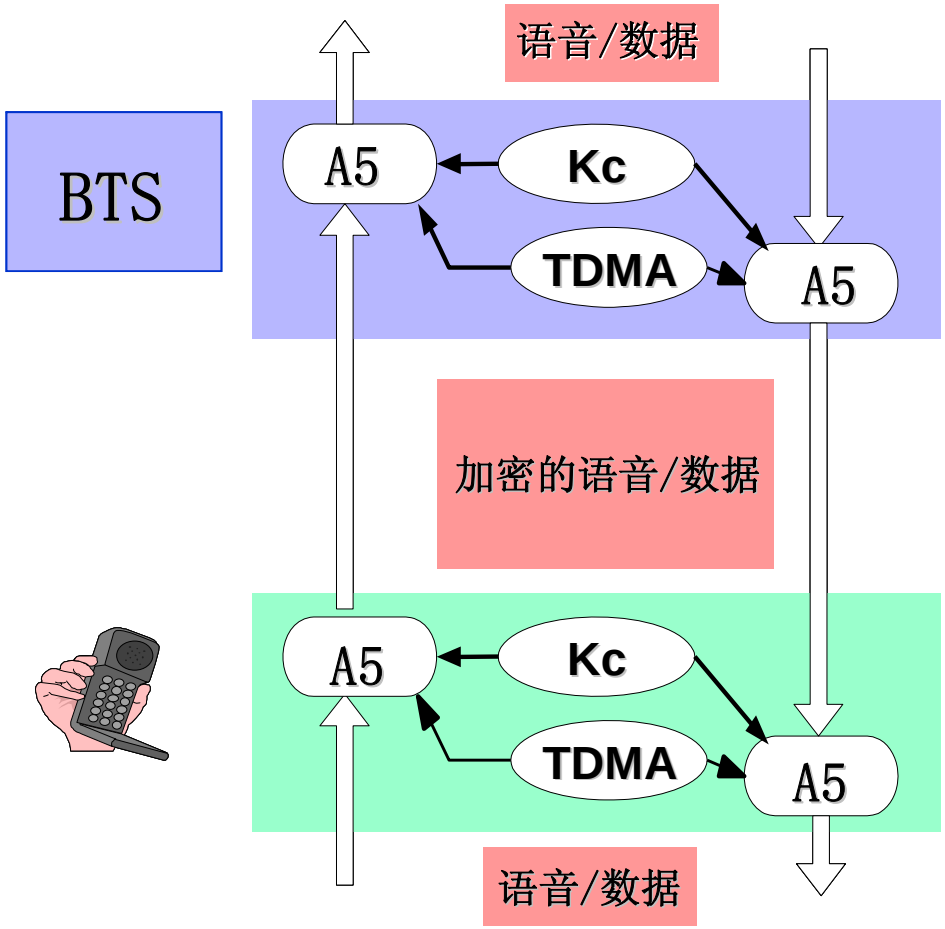


图: 空中接口用户信息加密

安全措施 X

- 移动设备的识别
  - 目的: 确保系统中使用的移动设备不是盗用或非法的设备
  - MSC/VLR 向移动用户请求 IMEI(国际移动台设备识别码) 并将 IMEI 发送给 EIR(设备识别寄存器)
  - 收到 IMEI 后,EIR 使用的三个清单
    - 白名单: 包括已分配给参加运营者的所有设备识别序列号码
    - 黑名单: 包括所有被禁止使用的设备识别
    - 灰名单: 由运营者决定, 例如包括有故障的及未经型号认证的移动设备
  - 将设备鉴定结果送给 MSC/VLR, 以决定是否允许入网
- 移动用户身份的安全保密
  - 用户的临时识别码 (TMSI)
    - 目的: 防止非法个人和团体通过监听无线路径上的信令交换而窃得移动用户的真实 IMSI 或跟踪移动用户的位置
    - 由 MSC/VLR 分配, 并不断更新, 更换周期由网络运营者决定

安全措施 XI

- 使用过程: 每当 MS 用 IMSI 向系统请求位置更新、呼叫建立或业务激活时,MSC/VLR 对它进行鉴权. 允许入网后，MSC/VLR 产生一个新 TMSI, 通过给 IMSI 分配 TMSI 的信令将其传送给 MS, 写入用户的 SIM 卡. 此后,MSC/VLR 和 MS 之间的信令交换就使用 TMSI, 而用户的 IMSI 不在无线路径上传送.

- 用户的个人身份号
  - 位数:4～8 位
  - 目的: 控制对 SIM 卡的使用
  - 使用过程: 只有 PIN 码认证通过, 移动设备才能对 SIM 卡进行存取, 读出相关数据, 并可以入网. 每次呼叫结束或移动设备正常关机时, 所有的临时数据都会从移动设备传送到 SIM 卡中, 再打开移动设备时要重新进行 PIN 码校验.
  - 错误输入处理: 如果输入不正确的 PIN 码, 用户可以再连续输入两次. 超过三次不正确,SIM 卡被闭锁, 须到网络运营商处解锁. 连续十次不正确输入时,SIM 卡回被永久闭锁, 即作废.

呼叫建立过程 I

- 端到端的呼叫流程
  - 移动呼移动 (主, 被叫在同一 MSC)
  - 移动呼移动 (主, 被叫不在同一 MSC)
  - 移动呼固定
  - 固定呼移动（被叫在 GMSC）
  - 固定呼移动（被叫不在 GMSC）
- 移动台的被呼过程 (以 PSTN 用户呼叫移动用户为例)

呼叫建立过程 II

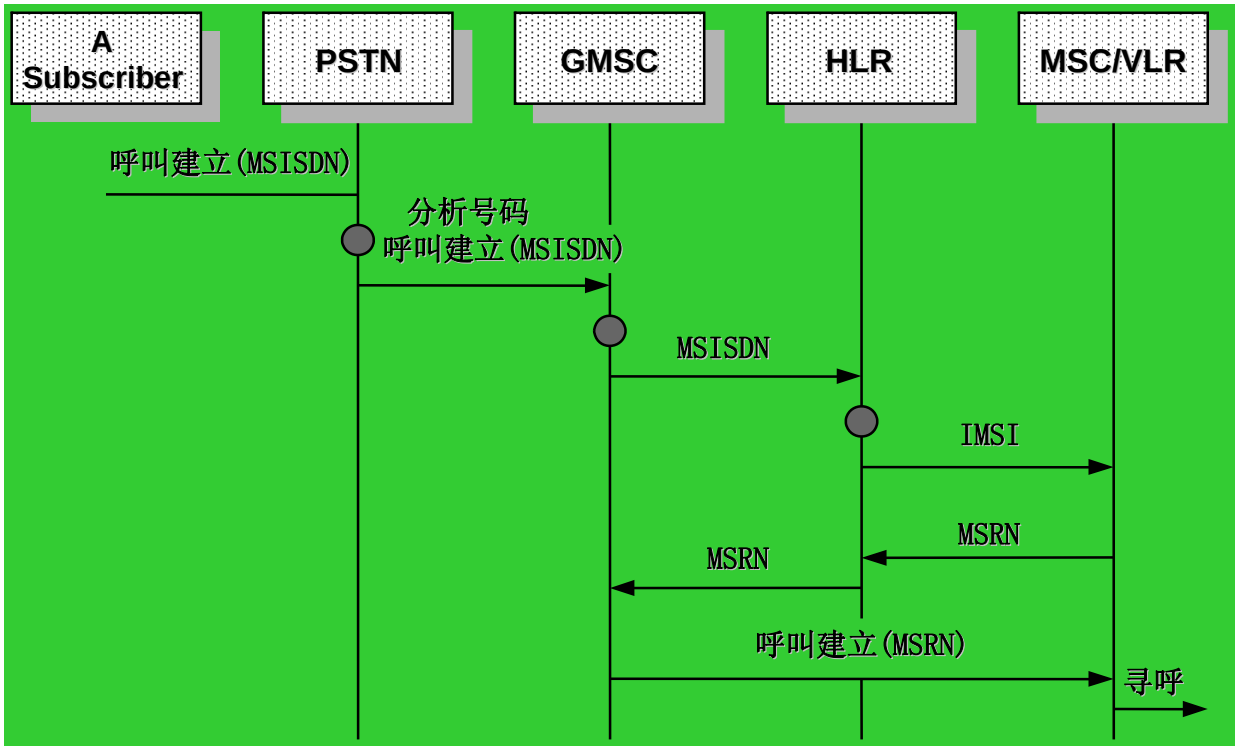


图: PSTN 用户呼叫 GSM 移动用户

呼叫建立过程 III

(1) 固定网的用户拨打移动用户的电话号码 MSISDN
(2)PSTN 交换机分析 MSISDN 号码
(3)GMSC 分析 MSISDN 号码
(4)HLR 分析由 GMSC 发来的信息
(5)HLR 查询当前为被呼移动用户服务的 MSC/VLR
(6) 由服务于被呼用户的 MSC/VLR 得到呼叫的路由信息
(7)MSC/VLR 将呼叫的路由信息传送给 HLR
(8)GMSC 接收包含 MSRN 的路由信息
(9)GMSC 把呼叫接续到服务的 MSC/VLR, 后者在被叫用户的位置区内进行寻呼
(10) 被叫用户响应寻呼, 网络为其分配控制信道和业务信道, 建立呼叫连接, 完成一次呼叫建立

- 移动台的始呼过程

呼叫建立过程 IV

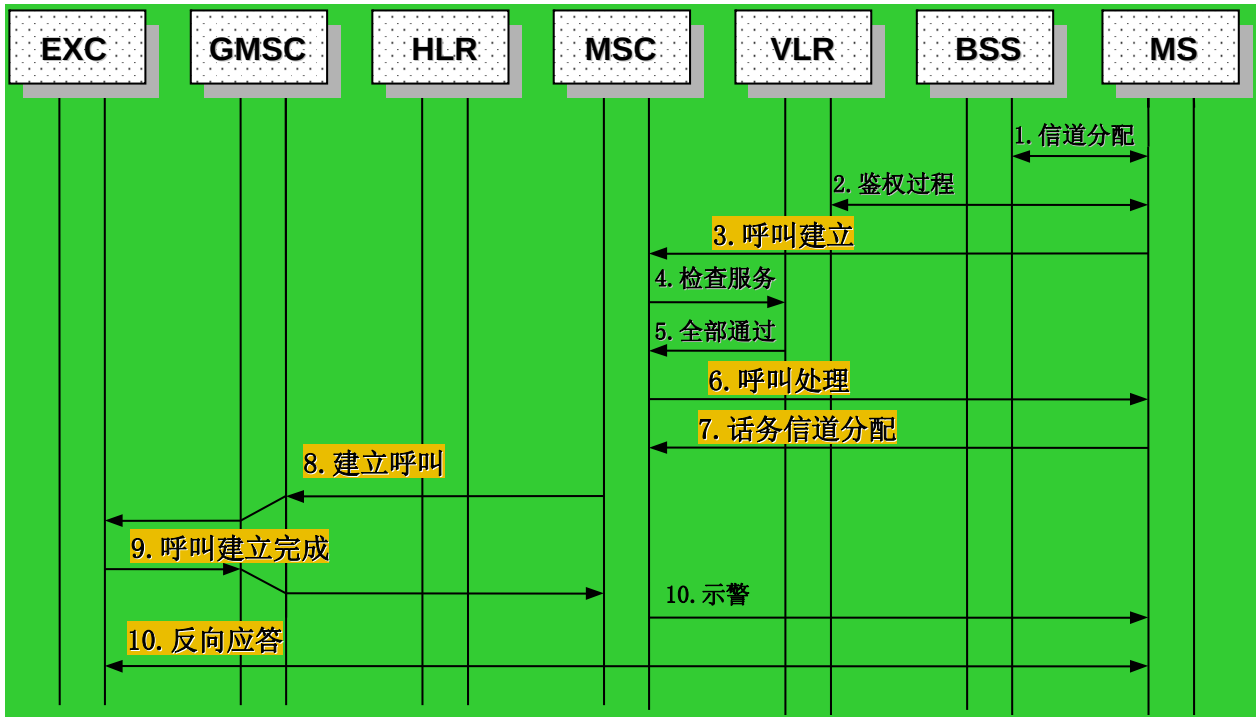


图: 移动台发起呼叫过程