Contents

Chapter 1

GSM 移动通信系统

1.1 GSM 总体结构

1.1.1 系统结构

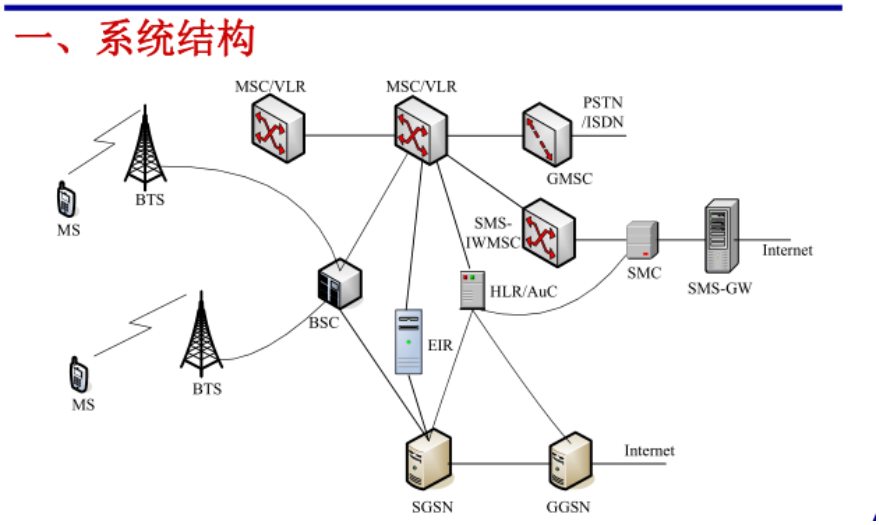


Figure 1.1:

GSM 网络由 MS，BSS，NSS 三部分组成。

- BSS: 包括 BTS 和 BSC
- NSS：包括核心网功能实体
  - 电路域，MSC/VLR，GMSC，SMS-IWMSC、SMC、SMS-GW、HLR/AuC 和 EIR
  - 分组域，SGSN，GGSN。

1.1.2 协议栈和接口

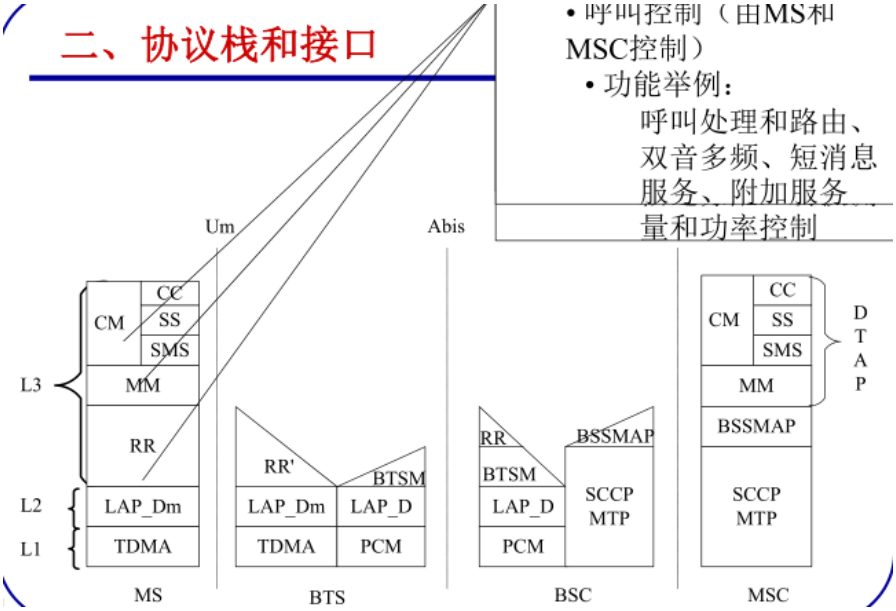


Figure 1.2:

1. Um 接口，是 MS 和 BTS 的空中接口，共三层（网络、数据链路和物理层）
   (a) CM，连接管理
   (b) MM, 移动性管理，包括位置登记和呼叫传递，在 MS 和 MSC 中实现。
   (c) RR, 无线资源管理。
2. Abis，BTS 和 BSC 之间的接口。
3. A,BSC 和 MSC 之间的接口。

1.2 无线信道

中国地区使用 900/1800MHz。其中以 900 为主，1800 不是到处都有。GSM 采用 FDD 工作方式，在 900MHz 时，双工收发间隔是 45MHz，在 1800MHz 双工收发间隔为 905Hz。一般地，**基站使用高频部分，补偿上下功率不平衡问题**。
在划分的上下行对称频段，按照 **200kHz** 间隔划分载波，每个载波采用 TDMA 方式，划分 8 个时隙（TS0-TS7），8 个时隙共占用 4.615ms。
载频间隔为 0.2Hz，频道序号为 n，则上下两频段中序号为 n 的载频可用下式计算：

$$\text{上行} f_{ul} = F_{ul0} + 0.2n \tag{1.1}$$
$$\text{下行} f_{dl} = F_{dl0} + 0.2n \tag{1.2}$$

1.2.1 干扰载波比

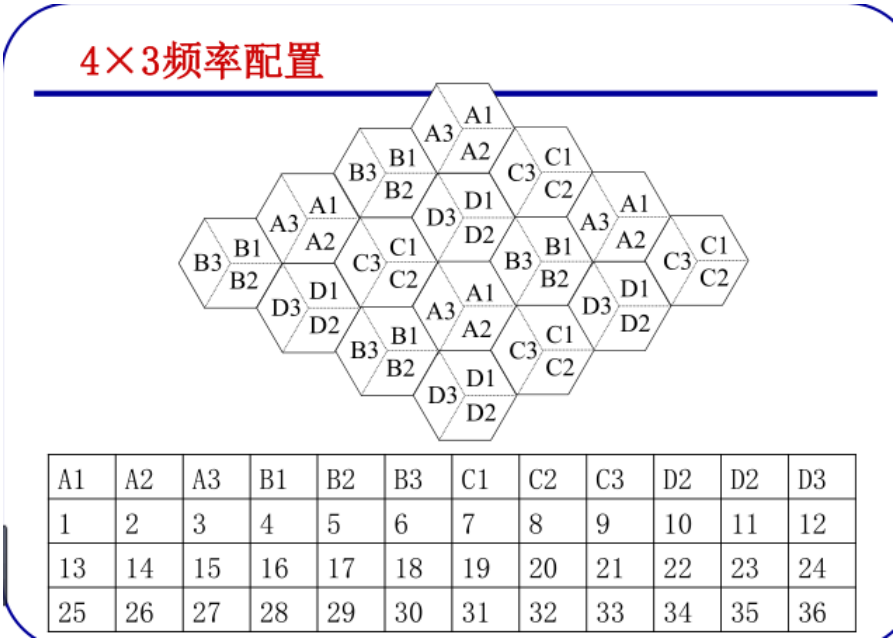
定义：波干扰保护比 C/I 就是指接收到的希望信号电平与非希望信号电平的比值。
GSM 采用**高斯最小频移键控 (GMSK)**、

1.2.2 频率复用方式

区群：将相邻若干的小区形成一个单元，在该单元内，所有小区不允许使用相同频率，且这种单元能无缝覆盖 GSM 业务提供去，单元之间频率符用。
小区个数：$N = i^2 + ij + j^2$

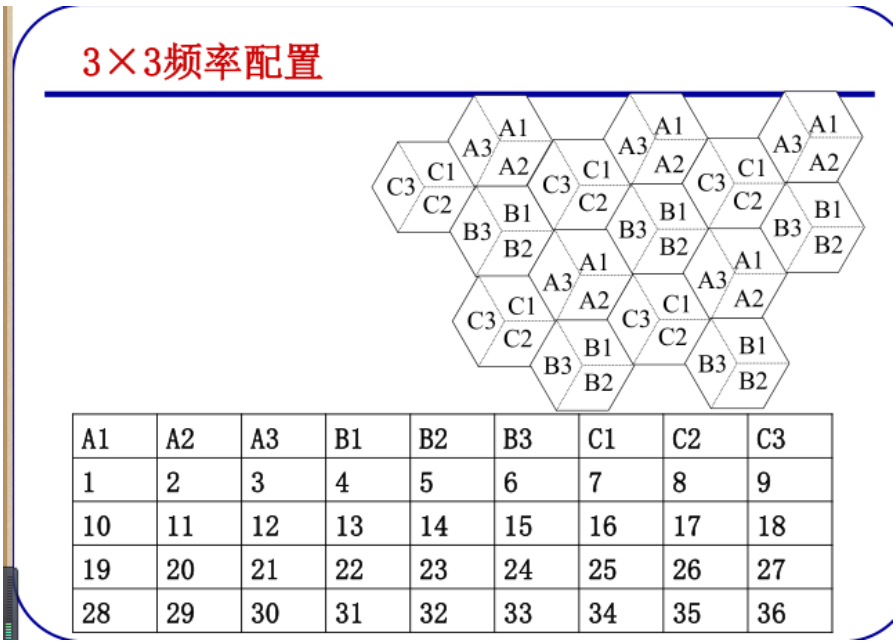
- 模拟蜂窝采用 7 小区，采用全向天线。
- GSM，采用 4 小区或者 3 小区，采用扇区天线。
- 采用 3 小区使，同频小区距离较小，采用跳频技术来躲避同频干扰。

1.2.2.1 4*3 和 3*3 的频点配置



A1	A2	A3	B1	B2	B3	C1	C2	C3	D2	D2	D3
1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36

Figure 1.3:



A1	A2	A3	B1	B2	B3	C1	C2	C3
1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	29	30	31	32	33	34	35	36

Figure 1.4:

为了提高系统容量

1. 提升频率复用系数，即减少单个小区个数，使得复用次数增多，不过同频干扰增大。
2. 小区分裂，减少原基站的覆盖半径，通过增加新基站来覆盖由于原基站覆盖半径减小而形成的盲区。基

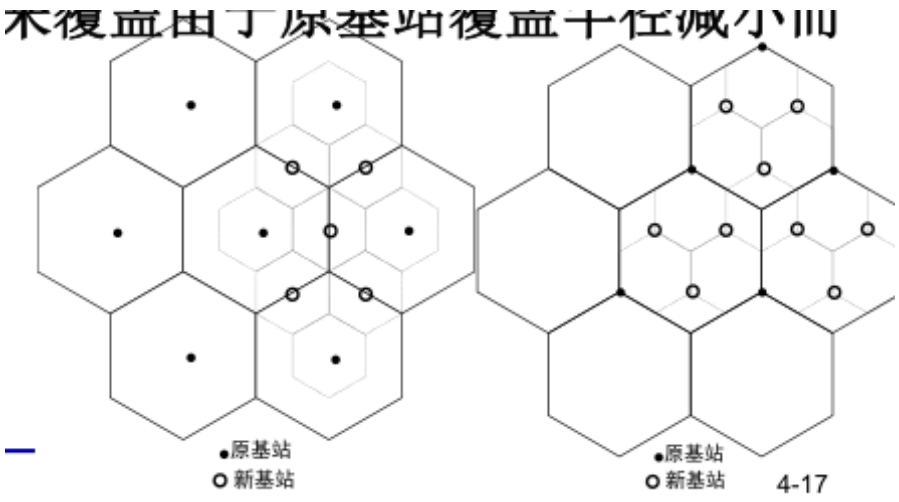


Figure 1.5:

站布置方式有中心激励（天线采用全向天线）和顶点激励（天线采用扇区天线），两种布置方式的覆盖面积和基站个数均相同。

1.2.3 无线帧结构

GSM 采用 TDMA 多址方式，在每载波上按时域划分为 TS0 ~ TS7 共 8 8 个时隙，时隙按 4.615ms 周期性的重复，每个时隙即是一个物理信道。
超高帧–超帧–复帧–TDMA。**MS 占用上下行频率的时隙号相同，但上行时隙相对于下行时隙延后 3 个时隙时间**。，原因

- MS 的收发信需要天线双工器来回倒换（对于只有一个天线的 MS 来说），倒换需要一定的时间。
- MS 处于随机移动状态，它与 BS 之间的距离和位置随机变化，为了防止在不同位置使用相同频率的 MS 发射的时隙在到达 BS 的时候出现重叠的情况，离 BS 远的 MS 应当适当提前它的发射时刻，TA（时间提前量）。

1.2.4 逻辑信道

1.2.4.1 TCH

传送语音数据和低速数据业务数据。

速度类型	语音编码速率	信道编码速率
全速率	13kb/s	22.8kb/s
半速率	6.5kb/s	11.4kb/s

1.2.4.2 CCH

传送信令数据以及短分组数据（短消息）。

BCH(广播控制信道) 一点对多点的下行控制信道；传送的内容主要使**移动台入网**和**呼叫建立**所需的有关信息。

1. 频率校正信道 (FCCH), 用于 MS 的频率矫正。
2. 同步信道 (SCH)，传送基站识别码 (BSIC，MS 可以区分使用相同频率的不同基站，BS 也可识别是否是连接到自身的 MS)，传送 TDMA 帧号（FN）。

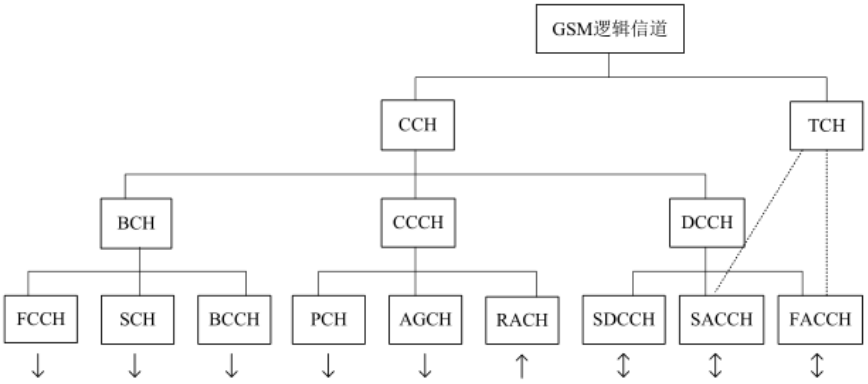


Figure 1.6:

3. 广播控制信道（BCCH），MS 由此获取各种系统参数（位置区识别 LAI); 同时，BS 以**最强且恒定**公里吧发射该信道，MS 通过检测该信道的信号质量作为越区切换判决用。

CCCH(公共控制信道) 双向控制信道，用于**呼叫接续**阶段传输链路连接所需的控制信令。

1. 寻呼信道 PCH，用于寻呼移动台。在寻呼信道上，可以组呼多个 MS，通过 **TMSI**，区分不同的 MS。
2. 随机接入信道 (RACH)，**上行**，用于移动台提出入网申请，请求分配 **SDCCH**。
3. 接入允许信道 AGCH，用于入网应答，分配一条 SDCCH。

DCCH 专用控制信道 ，双向，由基站分给某一特定的移动台专用

1. 独立专用控制信道 SDCCH，用于在分配 TCH 之前接续过程中传送系统信令，用于传递位置登记、鉴权、呼叫建立、**短消息**等信令信息。经过鉴权确认后，在分配 TCH。
2. 慢速辅助控制信道 SACCH
   - 与 SDCCH 联用，构成 SACCH-C，用于**周期性**传递 MS 对当前服务基站及周边基站信号的测量报告。
   - 与 TCH 联用，构成 SACCH-H，用于在**通话过程中**，传递 MS 对当前基站和周边基站的测量报告，用于网络判决 MS 是否需要越区切换。以及 TA 下发，功率调整下发。
3. 快速辅助控制信道 FACCG，与 TCH 联用。越区切换判决后，使用 FACCH 发送越区切换指令。

Figure 1.7:

1.2.5 时隙格式

GSM,8 时隙，时隙宽度 0.577ms, 包含 156.25bit。

频率校正突发

同步突发

接入突发, (AB) ，脉冲序列。用于 RACH ，在 MS 初始接入时，利用接入突发传送信道请求消息。由保护期长度，可计算小区覆盖半径。

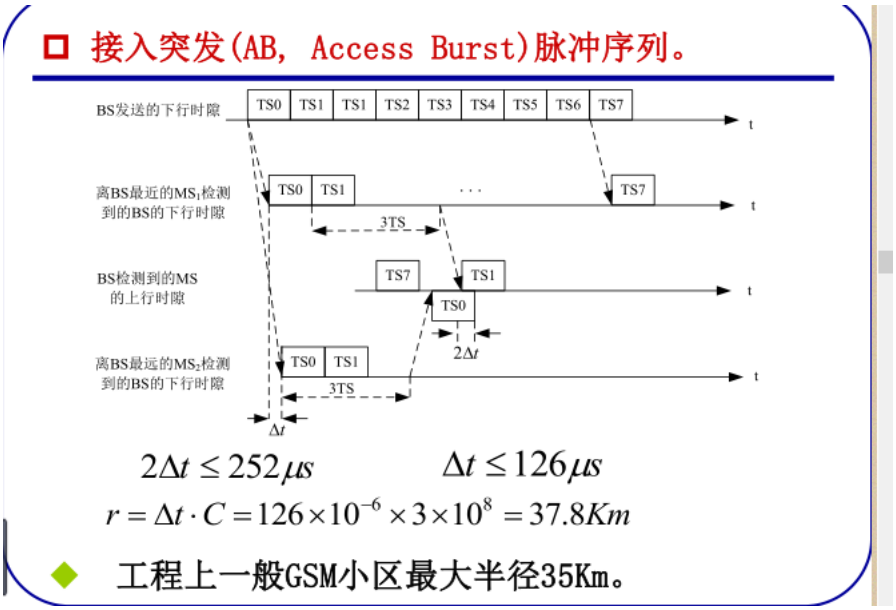


Figure 1.8:

常规突发 用于业务信道和专用控制信道。对于 BCCH 、PCH 、AGCH 、SDCCH 、SACCH 和 FACCH 信道，采用 LAPDm 协议

1.2.6 交织

对于全速率 TCH，GSM 手机将 20ms 的模拟话音数据编码成 260 个比特（所以全速率话音速率为 13kb/s)，经过卷积编码等最终输出 456bit。然后进行**块内和块间交织**。

块内交织 分为 8 个小块，每个小块 456/8=57bit。

块间交织 相邻两块数据进行二次交织，来自两个不同的 57bit 数据放入常规突发中。

1.2.7 逻辑信道与物理信道映射

对于多载频的情况下，系统会划分出主载频和副载频，**主载频上**的 TS0 和 TS1 用于映射控制信道，**主载频上的其余时隙和副载频上的所有时隙用于映射业务信道**。

1.2.7.1 BCH,CCCH

对于**上行链路**，TS0 只用于 MS 的接入 (RACH)，即 51 个 TDMA(TS0) 帧用于随机接入信道。

1.2.7.2 SDCCH、SACCH-C

下行链路 TS1 用于映射专用控制信道。

1.2.7.3 TCH

复诊含有 26 个 TDMA 帧。

T 编码话音或数据，用于通话，突发脉冲序列为 NB。

A SACCH, 信号强度检测，TA 下发，功率公职。

I 空闲帧。

1.2.7.4 FACCH

1.3 呼叫处理流程

1. MSISDN, 移动台综合业务数据网号码。存放于 HLV 中。平常拨打的手机号。
   - CC, 国家码。86
   - NDC, 国内地区码。131,139
   - SN, 用户号码。**H0H1H2H3**ABCD，加黑标识一个 HLR。
2. IMSI, 国际移动用户标识码。移动客户唯一标识码。绑定 SIM 和存放在 HLR/AuC。在位置登记和呼叫等过程中作为 MS 的身份标识。
3. TMSI, 临时移动用户标识，用于在 VLR 服务区内唯一标识一个移动用户，由 VLR 生成和管理。
4. IMEI 国际移动设备标识, 用于标识移动设备。
5. LAI, 位置区识别码。
6. MSRN, 移动台漫游号码，VLR 为 MS 生成。MSRN 用作原端交换机寻路目的交换机用
7. GCI, 全球小区识别。
8. BSIC ： 基站识别色码，用于区分使用相同载频的不同基站。
9. MSC/VLR Number, 路由选择时进行识别。
10. HLR Number, 用于主叫方交换机寻址被叫 MS 的 HLR.

1.4 通信安全

1. 鉴权
2. 加密
3. IMEI 查询, 网络判定 IMEI 的合法性，即判定移动台本身的合法性。

GSM 系统的鉴权是单向鉴权，即只有网络对 MS 的鉴权过程。在 3G 网络中引入了双向鉴权机制，增加了 MS 对网络的鉴权过程，有效的防范伪基站攻击