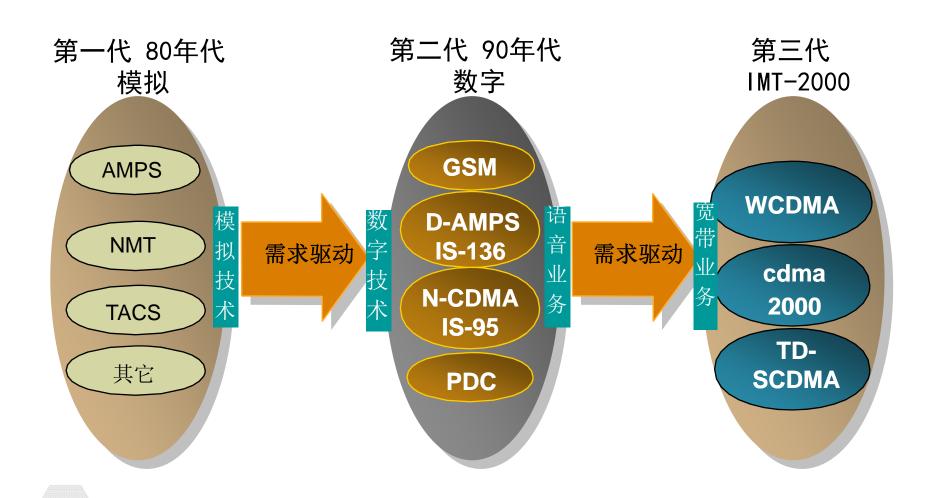
第八讲 2G蜂窝移动 通信系统



不同业务,不同技术





内容



- ◆第一代模拟移动通信系统
- ❖ 第二代数字GSM移动通信系统
- *第二代窄带CDMA移动通信系统

第1代模拟移动通信系统(1G)



- ❖ 第1个蜂窝移动电话出现在1973年4月 3号
 - 由 Motorola 公司开发
 - 每个电话重达850克





■ 北欧: NMT, 450/900MHz

■ 英国: TACS, 900MHz

■ 西德: C-Nez, 450MHz

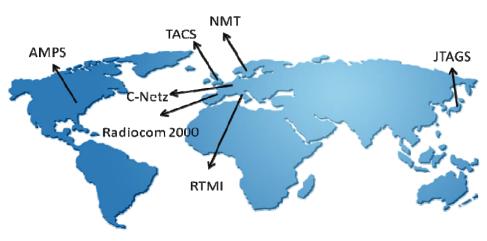
■ 法国: Radiocom 2000

■ 意大利: RTMI

■ 日本: JTAGS



马丁-库珀



模拟移动通信系统特点



- ❖采用模拟调制方式进行语音传输,逐步被数字蜂 窝移动通信所替代
 - 模拟蜂窝系统体制混杂,不能实现国际漫游;
 - 模拟蜂窝网业务形势单一,只能提供语音业务,不 能提供数据业务;
 - 模拟系统设备造价高,终端体积大,耗电量大,终端易被盗号;
 - 模拟网语音质量差,保密性差;
 - 模拟系统频谱利用率低,无法适应大容量的需求。

内容



- *第一代模拟移动通信系统
- ❖ 第二代数字GSM移动通信系统
- *第二代窄带CDMA移动通信系统

第2代数字移动通信系统(2G)



- *相对于1G系统的FDMA技术,2G系统主要采用TDMA和CDMA技术,同时也采用了数字调制技术,主要包括以下几种标准:
 - 1991年,美国提出的IS-136,即使数字AMPS (D-AMPS);
 - 1992年,欧洲推出的全球移动通信系统 (GSM);
 - 1993年, 日本提出的个人数字蜂窝 (PDC);
 - 1993年,美国提出的IS-95,即窄带CDMA (N-CDMA)。
- ❖ 与1G系统相比, 2G系统的主要优点:
 - 采用新的调制方式,频谱利用率高,有利于提高系统容量;
 - 抗噪声、抗干扰和抗多径衰落的能力强;
 - 具有较强的鉴权和加密功能,确保用户和网络的安全需求;
 - 可降低设备成本,减少用户设备的体积和质量。

第2代数字移动通信系统(2G)

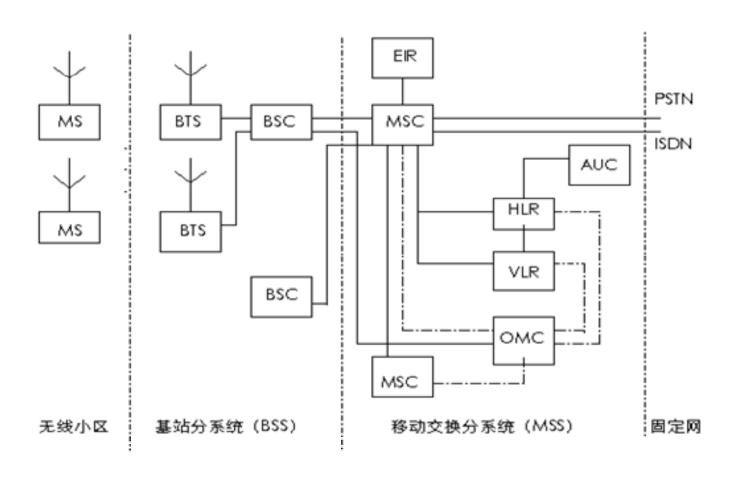


2G系统各种标准的主要参数

标准类型	GSM	IS-95	D-AMPS	PDC	
上行频段/MHz	890~915	824~849	824~849	810~830 或	
上1丁列权/MITZ	890~913	024~049	024~049	1429~1453	
工公居的 (A.G.)	935~960	869~894	960 904	940~960 或	
下行频段/MHz	955~900	009~094	869~894	1477~1501	
调制方式	CMCV	OQPSK(上行)	-/4 ODEV	-/4 ODEV	
	GMSK	QPSK(下行)	$\pi/4$ QPSK	π/4 QPSK	
载波带宽/kHz	200	1250	25	30	
语音编码方式	RELP - LTP	QCELP	VSELP	VSELP	
信道编码方式	CRC+卷积码	CRC+卷积码	CDC : MAIN	CDC + MEXITI	
	(r=1/2, k=5)	(r=1/2, k=5)	CRC+卷积码	CRC+卷积码	
信道数据速率/kbps	270.833	1228.8	1228.8 48.6		
语音编码速率/kbps	13	8	8	6.7	
多址方式	TDMA/FDMA	CDMA/FDMA	TDMA/FDMA	TDMA/FDMA	

GSM系统的总体结构





GSM系统的总体结构

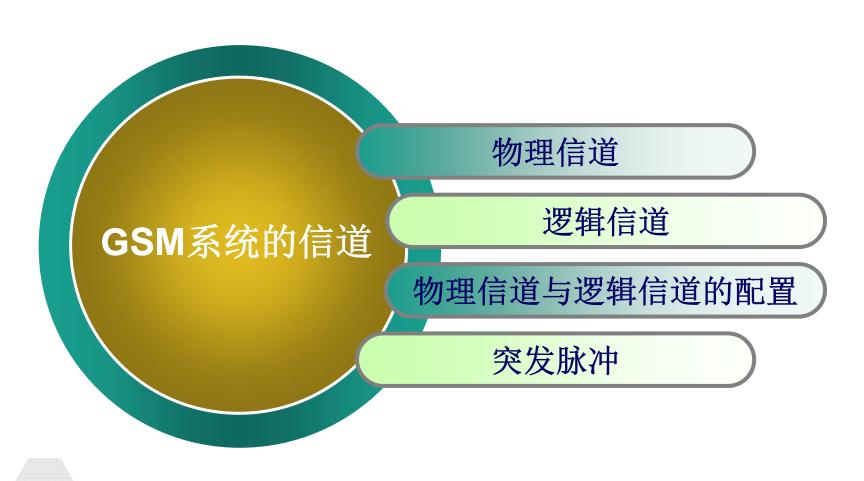
GSM系统的功能单元



子单元	功能		
MS(移动台)	包括ME (移动设备)和SIM (用户身份识别卡)		
BTS (基站收发系统)	为一个小区服务的无线收发设备,负责无线传输		
BSC (基站控制器)	对一个或者多个BTS进行控制和管理,包括信道分配和释放, 越区切换等		
MSC(移动业务交换中心)	实现移动用户与其它网络用户的联接,为此提供面向系统其它 功能实体的接口,到其它网络的接口以及其它MSC的接口		
VLR (拜访位置寄存器)	存储进入覆盖区的所有用户的相关信息,VLR是一个动态数据库,当移动用户离开覆盖区域,相关信息则被删除。VLR通常与MSC共存在一个物理实体上,避免频繁联系带来的接续时延。		
HLR (归属位置寄存器)	是系统的中央数据库,存放用户的所有信息,包括当前位置, 漫游权限,基本业务等,为MSC建立路由提供位置信息。一个 HLR可以覆盖几个移动交换中心甚至整个移动网络。		
EIR (设备识别寄存器)	存储与移动台的IMEI(国际移动设备识别号)相关的信息,可对移动台的合法性进行核查。		
AUC(鉴权中心)	存储用户的加密信息,包括鉴权信息与加密秘钥等。AUC与 HLR共存在一个物理实体上。		
OMC (操作维护中心)	操作维护GSM系统中的各功能实体		

GSM系统的信道



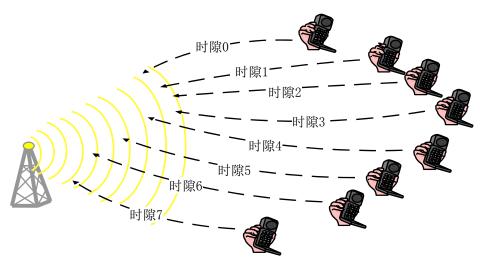


GSM的多址方式



→ GSM系统采用**FDMA**和**TDMA**混合多址接入技术

- → FDMA: 在GSM的900MHz频段(带宽2×25MHz)和1800MHz频段 (带宽2×75MHz)分别划分了124个和374个子信道,相邻子信道的载 频间隔为200kHz。
- → TDMA: GSM在每个子信道上再按时间划分为8个时段,每个时段称为一个时隙 (slot),而连续的8个时隙又组成一帧 (frame),称为"TDMA帧"。



时分多址接入原理示意图

GSM的工作频段



		900MHz频段	1800MHz频段		
	工作频段	890~915MHz 935~960MHz	1710~785MHz 1805~1880MHz		
	频道间隔	相邻频道间隔为200KHz 每个频道采用TDMA方式分为8个时隙,即8个物理信道			
等	频道序号	1 \sim 124	512 ~ 885		
间	频道数	124	374		
1_1_	频道序号和 频道中心频 率的关系	上行: $f_l(n)$ =890.200MHz+ $(n-1)$ ×0.200MHz 下行: $f_h(n)$ = $f_l(n)$ +45MHz 其中, n =1~124	$f_l(n) = 1710.200$ MHz+ $(n-512) \times 0.200$ MHz $f_h(n) = 95$ MHz+ $f_l(n)$ $n=512 \sim 885$		

GSM的频率复用方式



→ 若使用定向天线,应采用4×3的复用 方式

即 N=4,采用定向天线,每基站用3个120°的方向性天线构成3个扇形小区,如图1所示。

业务量较大的地区可采用其它的复用 方式

如3×3, 2×6, 1×3复用方式。

→ 若使用全向天线,应采用 N=7的复用 方式

其频率可从4×3复用方式的12组中任选7组, 频道不够用的小区可从剩余频率组中借用频道,但相邻频率组尽量不在相邻小区使用,如图2所示。

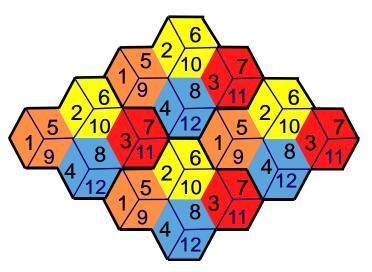


图1 4×3复用模式

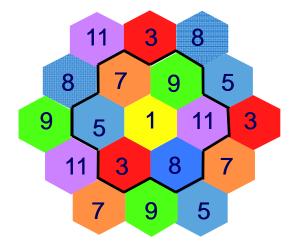


图2 7组复用模式

GSM的载波干扰比与保护频带要求



▶ 载波干扰比

干扰	参考载干比
同道干扰 <i>C/I_c</i>	9dB
200kHz邻道干扰 <i>C/I_{c1}</i>	−9dB
400kHz邻道干扰 <i>C/I_{c2}</i>	-41dB
600kHz邻道干扰 <i>C/I_{c3}</i>	-49dB

◆ 保护频带

原则:确保数字蜂窝移动通信系统能满足载波干扰比要求。

- ◆ 当某地GSM900系统与模拟蜂窝移动电话系统共存时,两系统之间 (频道中心频率之间)应有约400kHz的保护带宽。
- → 当某地GSM1800系统与其它无线电系统的频率相邻时,应考虑系统间的相互干扰情况,留出足够的保护频带。

GSM逻辑信道



→ 概念

逻辑信道是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或语音、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。

→ 分类

→ 公共信道

广播信道(BCH): "点对多点"的单向控制信道,用于基站向所有移动台广播入网和呼叫建立所需要的各种信息。

公共控制信道(CCCH): "点对多点"的双向控制信道,用于在呼叫接续阶段,传送链路连接所需要的信令消息和信道指配信息。

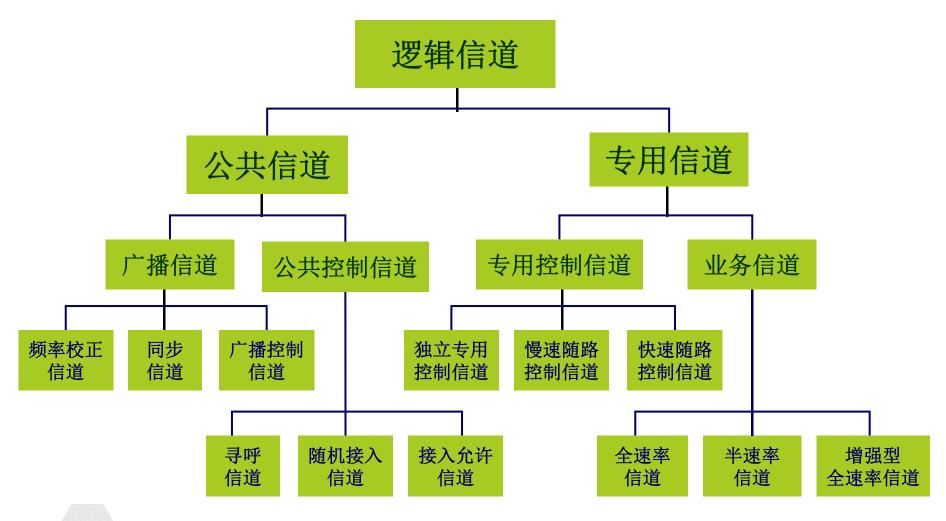
→ 专用信道

专用控制信道 (DCCH): "点对点"的双向控制信道,用于在呼叫接续阶段和在通信过程中,在移动台和基站之间传输必需的控制信息。

业务信道 (TCH): 面向特定移动台,用于携载语音或用户数据。

GSM的各种逻辑信道示意图





GSM定义的各种逻辑信道示意图

广播信道(BCH)



频率校正信道 FCCH

同步信道 SCH

广播控制信道 BCCH

给移动台传送校正移动台频率的 信息,移动台以此来校正自己的 时基频率。 给移动台传送帧同步(TDMA帧号)信息和基站识别码(BSIC)信息

单向下行信道,均为 点对多点的传播方式

每个基站广播公用的系统消息,移动台监听该信道获取如下信息:

- -本小区的载频信息
- -相邻小区的载频信息
- -区域识别信息
- -小区识别信息
- -功率控制信息等

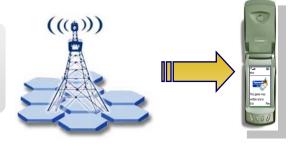
小区内的所有手机

公共控制信道 (CCCH)

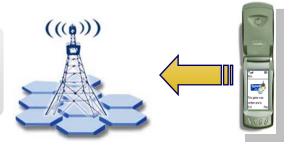


寻呼信道 PCH

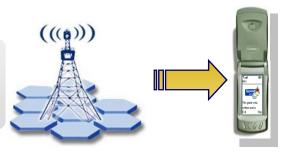
用于广播基站寻呼移动台的寻呼消息



随机接入信道 RACH 移动台随机接入网络时用此信道向基站发送接入请求,申请指配一独立专用控制信(SDCCH)



允许接入信道 AGCH 基站向随机接入成功的移动台发送指配了的独立专用控制信道(SDCCH)



专用控制信道(DCCH)



独立专用控制信道 SDCCH

- ▶ 传送基站和移动台间 的信令消息与信道指 配信息,如鉴权消息 、位置更新消息等;
- ➤ 在呼叫建立期间,该 信道支持双向数据传 输,以及短消息业务 的传送。

慢速随路控制信道 SACCH

- ▶ 基站向移动台传送功率 控制信息、帧调整等信息;
- ▶ 基站接收移动台发来的 移动台接收信号强度报 告和链路质量报告。

快速随路控制信道 FACCH

▶ 传送执行用户鉴权和越 区切换的信息。





业务信道 (TCH)



- → 业务信道用于携载语音或用户数据,可分为话音业务信道和数据业务信道。
 - → 话音业务信道

TCH/FS: 全速率语音信道, 13kbit/s

TCH/HS: 半速率语音信道, 5.6kbit/s

TCH/EFR: 增强型全速率语音信道, 12.2kbit/s

→ 数据业务信道

TCH/9.6: 全速率数据信道, 9.6kbit/s

TCH/4.8: 全(半)速率数据信道, 4.8kbit/s

TCH/2.4: 全(半)速率数据信道, 2.4kbit/s

逻辑信道与物理信道的映射关系



→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

▶ 将逻辑控制信道复用,即在一个或两个物理信道上复用逻辑控制信道。

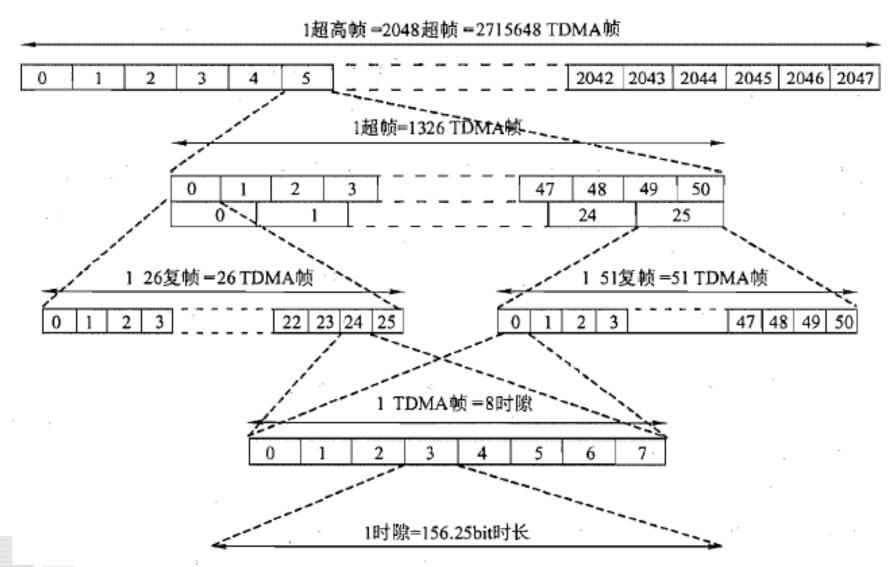
GSM的分级帧结构



- → 五个层次: 时隙、TDMA帧、复帧、超帧和超高帧
- → 时隙:物理信道的基本单元;
- **▼ TDMA帧**:包含8个时隙,整个帧长约为4.615ms;
- **▼ 复帧**(两种类型):
 - 连续的26个TDMA帧构成的复帧,称为26复帧,周期为120ms,用 于业务信道和随路控制信道(TCH与SACCH/FACCH);
 - 连续的51个TDMA帧构成的复帧,称为51复帧,周期为3060/13≈ 235.385ms,用于广播信道和公共控制信道(BCH与CCCH)。
- ▶ 超帧: 包含51个26复帧或者26个51复帧,一个超帧的持续时间为6.12s;

GSM的分级帧结构





逻辑信道与物理信道的映射关系



一个基站有N个载频,每个载频有8个时隙,于是定义

载频数为 f_0 、 f_1 、 f_2 、...、 f_{N-1} ;

时隙数为TSO、TS1、...、TS7。

- ★ f₀的TSO时隙→ f₀的TS1时隙

供控制信道使用

- → f₀的TS2~TS7时隙
 → f₁ ~f_{N-1}的TS0~TS7时隙

 \rightarrow 下面以 f_0 为例,说明物理信道和逻辑信道的映射关系。

供业务信道使用

f_0 的TS0时隙



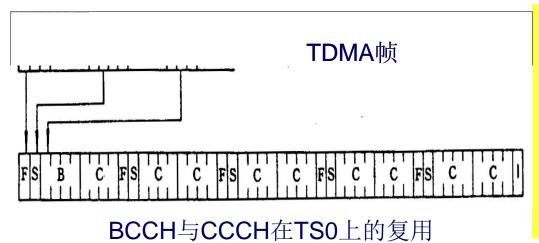
fo的TSO时隙用于映射广播信道 (BCH) 和公共控制信道 (CCCH),即

BCCH、FCCH、SCH、PCH、AGCH、RACH BCH CCCH

- → 下行链路(BCCH、FCCH、SCH、PCH、AGCH)
- → 上行链路 (RACH)

f_0 的TS0时隙——下行链路





F(FCCH): 移动台据此校正同步频率;

S(SCH): 移动台据此读TDMA帧号和基

站识别码(BSIC);

B(BCCH): 移动台据此读有关小区的公

用系统信息;

I(IDEL):空闲帧,不含任何信息,仅作

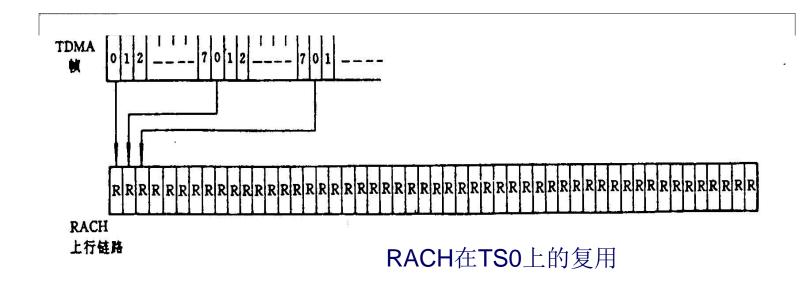
为复帧的结束标志;

C(CCCH): 移动台依此接受寻呼和接入。

- → 广播信道 (BCH) 和公共控制信道 (CCCH) 共占用51个TS0时隙,但从时间上共经历51个TDMA帧(即,51复帧);
- → 以每出现一个空闲帧作为复帧结束,在空闲帧之后,再从F、S开始进行 新的复帧,以此规律构成TDMA的复帧结构;
- ◆ 在没有寻呼或呼叫接入时,基站也总在f₀上发射信号,这使移动台能够 测试基站的信号强度以决定使用哪个小区更为合适。

f_0 的TS0时隙——上行链路



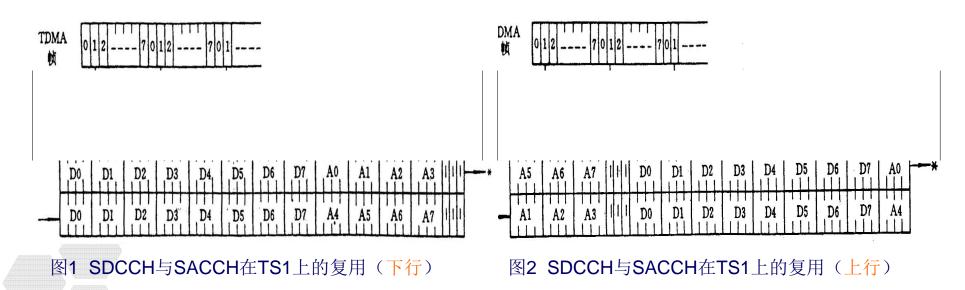


- → 只包含随机接入信道 (RACH),用于移动台的接入。
- → 上图为51个连续的TDMA帧的TS0 (51复帧)。

f_0 的TS1时隙



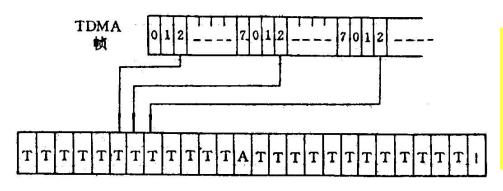
- → 用来映射专用控制信道,重复周期为2个51复帧。
- → 独立专用控制信道(SDCCH): Dx (x=0, 1, ..., 7)只在移动台x建立呼叫时使用,此时移动台x正在建立呼叫或更新位置或与基站交换系统参数。在移动台x转到业务信道(TCH)上开始通话或登记完释放后,Dx可用于其它移动台。
- ▶ 慢速随路控制信道(SACCH): Ax (A0, A1, ..., A7) 主要用于传送SDCCH的辅助信息,包括功率控制、帧调整、测量数据等信息。
- → 上、下行链路有相同结构,只是在时间上有一个偏移,即意味着一个 移动台可与基站实现双向连接。



fo的TS2~TS7时隙



→ 用来映射业务信道 (TCH), 重复周期为26个TDMA帧(26复帧)。

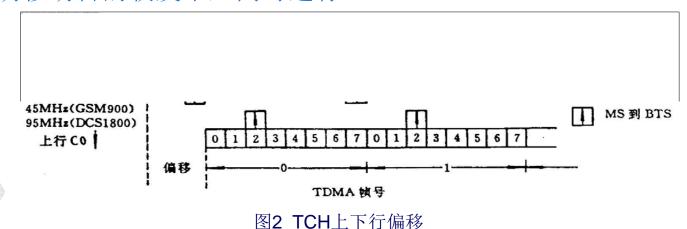


T (TCH业务信道):用于传送语音或数据; A(SACCH慢速随路信道):用于传送 TCH的辅助信息;

I(IDEL):空闲帧,它不含任何信息,用 于配合测量。

图1下行TCH的复用

→ 上、下行链路的TCH结构完全一样,只是有3个时隙的偏移,表明移动台的收发不必同时进行。



突发脉冲 (Burst)



普通突发脉冲序列:用于携带TCH、DCCH(SDCCH、FACCH、SACCH)、BCCH、PCH和AGCH信道的消息。

H,

同步突发脉冲序列: 用携带SCH信道的消息。

接入突发脉冲序列: 用于携带RACH信道 的消息。 TDMA信道上的一个时隙中的消息格式被称为突发脉冲序列。因为在特定突发脉冲上发送的消息内容不同,也就决定了它们格式的不同。

空闲突发脉冲序列: 当系 统没有任何具体的消息要 发送时就传送这种突发脉 冲序列。

频率校正突发脉冲序列: 用于携带FCCH信道的消息。

突发脉冲的结构



→ 普通突发脉冲(NB: Normal Burst)

TB	加密比特	F	训练序列	F	加密比特	TB	GP
3	57	1	26	1	57	3	8.25
•			0.577ms 156.25bit				

- ▶ 57个加密比特:加密语音、数据或控制信息;
- → 借用标志F: 表明快速随路控制(FACCH)借用一半的业务信道资源;
- ▶ 训练序列: 一串已知比特,供信道均衡使用;
- → 尾位TB: 总是000, 是突发脉冲开始与结尾的标志;
- ▶ 保护时间间隔:防止由于定时误差而造成突发脉冲间的重叠。
- → 频率校正突发脉冲 (FB: Frequency Correction Burst)



→ 固定比特: 142个全0比特,用于频率校正。

突发脉冲的结构



→ 同步突发脉冲(SB: Synchronization Burst)



- ▶ 由以下两部分构成: (1) 加密比特(2×39bit)包含TDMA帧号(TN)以及基站 识别码(BSIC); (2) 一个易被检测到的长同步序列。
- → 接入突发脉冲(AB: Access Burst)



→ 长保护时间间隔:适应移动台首次接入或切换到新基站时不知时间的提前量而设定的。

突发脉冲的结构



◆ 空闲突发脉冲(DB: Dummy Burst)

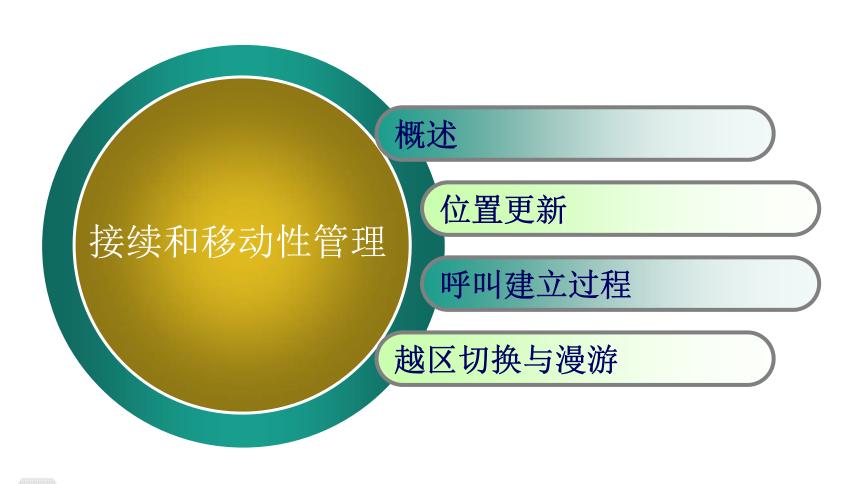
将普通突发脉冲中的加密信息比特换成固定比特

TB	固定比特	F	训练序列	F	固定比特	TB	GP
3	57	1	26	1	57	3	8.25
-	◆						

→ 当无用户信息传输时,用空闲突发脉冲替代普通突发脉冲在TDMA时隙中传送。

GSM的接续和移动性管理





概述



- ◆ 在移动蜂窝网中,为了建立一个呼叫连接需要解决的问题
 - → 定位用户的位置
 - → 用户的识别
 - ▶ 用户所需提供的业务
- ▶ 操作过程
 - ◆ 当一个移动用户在随机接入信道上发起呼叫时,移动蜂窝网就开始了一 系列的操作。这些操作设计到网络的各个单元,包括移动台、基站、移 动交换中心,各种数据库,以及网络的接口。



▶ 当移动用户进行越区切换时,同样会引起移动网的一系列操作:

各种位置寄存器中移动台位置信息的 登记、修改或删除

正在通话

越区转接

GSM移动用户的登记以及相关数据库

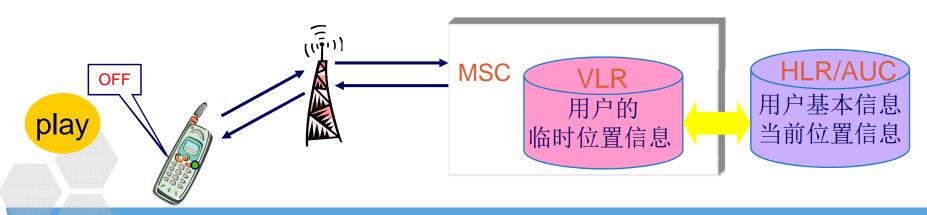


◆ SIM卡

- → 用户侧的重要数据库。一方面存储用户身份认证所需的信息,防止非法 用户入网;另一方面存储与网络和用户有关的管理数据。在网络侧来看, SIM卡就代表了用户,好像移动用户的"身份证",每次通话网络对用 户的鉴权实际上就是针对SIM卡的鉴权。
- → 网络运营部分在向用户提供SIM卡时,需要注入用户管理的有关信息, 包括用户的国际移动用户识别号(IMSI)、鉴权秘钥(Ki)、用户接入等级控制,以及用户注册的业务种类和相关的网络信息等内容。

▶ 鉴权登记

→ 当一个新用户在网络服务区开机登记时,登记信息通过空中接口送到网络端的VHL,并在此进行鉴权登记。通常MSC和VLR集成在一起。另外,网络内部的VHL和HLR要随时交换信息,更新彼此的数据。

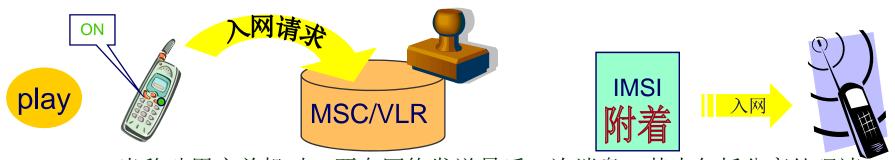


GSM移动用户的登记以及相关数据库



▶ 网络识别

当网络端允许一个新的用户接入网络时,网络对新用户的IMSI数据作"附着"标记,表明此用户是一个被激活的用户可以入网通信。



当移动用户关机时,要向网络发送最后一次消息,其中包括分离处理请求,MSC/VLR接收到请求消息后,就对该用户的相应的IMSI上做"分离"标记,去除"附着"。



GSM移动用户位置更新

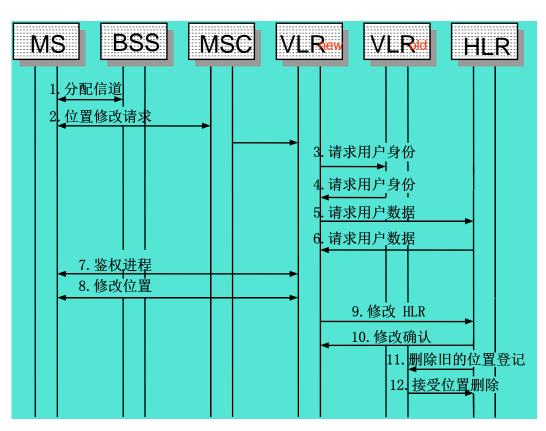


◆ 位置更新

移动用户从一个网络服务区到达另外一个网络服务区时,系统所进行的 位置更新操作。这种位置更新涉及了新、旧两个VLR。

→ 位置更新过程

- → 用户开机空闲状态时,通常锁 定在原小区的BCCH载频上, 随时接收网络发来的位置识别 信息;
- ▶ 移动台每次收到BCCH的位置 识别信息都与原来存储的信息 进行比较,如果两者不同则向 网络发出位置更新请求;
- → 网络端接收到请求信息后便将 移动台注册到新的VLR,同时 HLR要与新的VLR交换数据, 同时通知旧的VLR删除用户的 相关信息。



移动用户的周期位置更新



→ 问题

在某些特定条件下,由于无线链路质量很差,网络无法收到移动台的正确信息,因此网络无法知道移动台所处的状态。

▶ 解决方法

系统采取强制登记措施,要求移动台每隔一定时间,如一个小时,登记一次。

- → 周期位置更新由移动台内的一个定时器控制。定时器的定时值由 网络通过BCCH通知移动台;
- → 当定时值到时,移动台便向网络发送位置更新请求消息,从而启动位置更新过程;
- → 如果在一定时间内,网络接收不到某用户的周期位置更新请求, 则认为该移动台已经不在服务区或者电池耗尽,这是对其进行去 "附着"处理。



以固定网(公共开关电话网,PSTN)呼叫移动用户为例

1. 固定网的用户拨打移动用户的电话号码,即MSISDN MSISDN——移动用户的国际ISDN号码,其号码结构如下



- →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(区分运营商)
- →HLR识别号: H0 H1 H2 H3 (区分省份、城市)
- ◆SN (移动用户号): ABCD (区分用户)



2. PSTN交换机分析MSISDN号码

分析得出此用户要是接入移动用户网,则将接续转接到移动网的关口移动交换中心(GMSC)

3. GMSC分析MSISDN号码

由于被呼叫用户的地址信息只存放在用户登记的HLR/VLR中,因此GMSC分析 MSISDN号码可以得到被呼叫用户的HLR的地址,并给该地址发送一个携带 MSISDN号码的消息,以便得到被呼用户的路由信息,该过程也称为HLR查询。

4. HLR分析由GMSC发来的信息

HLR根据GMSC发来的信息,在数据库中找到被呼用户的位置信息,即被呼用户在哪一个VLR区登记的。

下面介绍一下HLR包含的内容?



→ HLR的内容:

MSISDN 、 IMSI 、 VLR的地址、用户的数据

→ 国际移动用户识别(IMSI): 移动用户的唯一识别号码(15位数字组成)

结构	识别对象	位数	中国	MCC	MNC		MSIN
MCC	移动国家号码	3	460		← 国内	移动用)	○识别 →
MNC	移动网号	2	中国移动为00 中国联通为01	■ 国内移动用户识别 ■■ 国际移动用户识别 ■			
MSIN	移动用户识别码	10	中国自行分配		IMSI的号	码结构	

此处不使用MSISDN号码的原因

- → 不同国家的MSISDN号码长度不同,主要是因为不同国家的国家码(CC)长度不同,如中国的CC为86,美国的CC为1,芬兰的CC为385。不同部分易混淆。
- → MSISDN号码用来识别不同的业务,也就是说同一个用户可以根据语音、 数据等不同的业务分配不同的MSISDN号码,但用户的IMSI号码全球唯一。



5. 由正在服务于被呼用户的MSC/VLR得到呼叫的路由信息

正在服务于被呼用户的MSC/VLR产生一个移动台漫游号码(MSRN),它包含被呼用户的路由信息。

6. MSC/VLR将呼叫的路由信息传送给HLR

HLR对此路由信息不做任何处理,直接将其传送给GMSC。

7. GMSC接收包含MSRN的路由信息

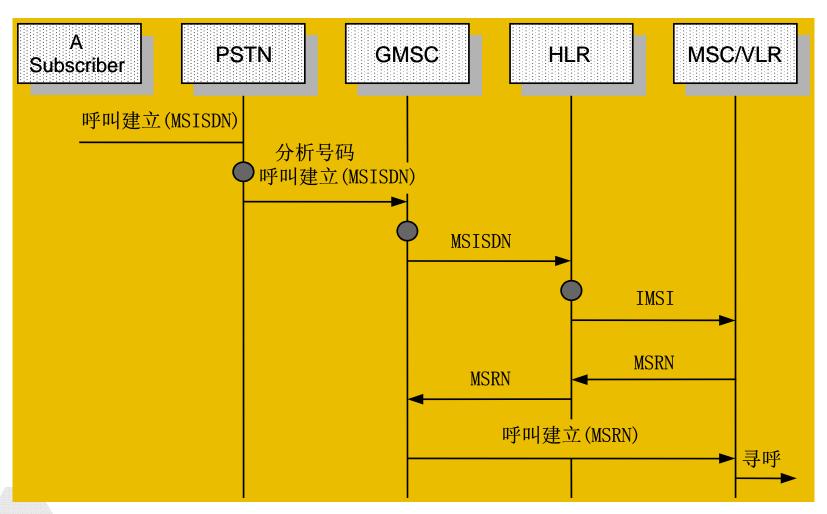
- ◆GMSC接收包含MSRN的路由信息,并分析MSRN,得到被叫的路由信息
- →向服务于被呼用户的MSC/VLR发送携有MSRN的呼叫建立请求消息
- →服务于被呼用户的MSC/VLR接到此消息,通过检查VLR识别被叫号码,找到 被叫用户

8. MSC/VLR定位被叫用户,开始寻呼过程

- →基站通过寻呼信道(PCH)发送寻呼信息
- ▶移动台识别出移动用户号码,便发出寻呼响应消息给网络
- ◆网络接到寻呼响应后,为用户分配一个业务信道,建立呼叫与被呼叫的连接

呼叫建立过程的简单步骤

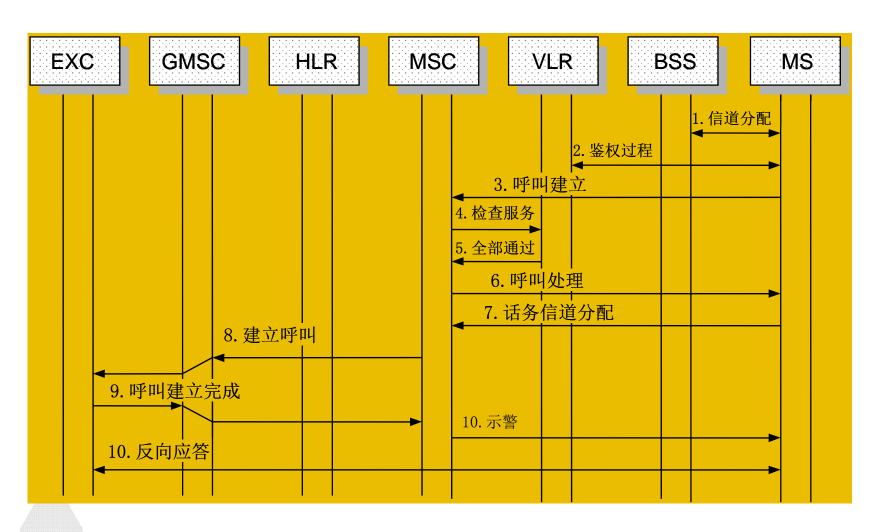




呼叫建立的简单步骤

移动台的始呼过程





移动台发起呼叫过程

越区切换的定义



切换(Handover):将正处于通话状态的移动台转移到新的、 业务信道上(新的小区)的过程。

- → 切换的目的 实现蜂窝移动通信的"无缝隙"覆盖,保证通信的连续性。
- → 实现切换的操作
 - → 识别新的小区
 - ◆ 在新的小区给移动台分配话音信道和控制信道
- → 引起切换的原因
 - → 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)

越区切换的策略



GSM系统中,切换的控制属于分散控制。移动台与基站均参与测量接收信号的强度(RSSI)和质量(BER)

- ▶ 移动台对不同基站RSSI进行测量,将测量结果报告给基站(两次/秒);
- → 基站对移动台所占用的业务信道(TCH)进行测量,并报告给基站控制器 (BSC);
- → 最后由基站控制器决定是否需要切换。

反映信道链路的指标	意义
WEI (word error indicator)	表明在移动台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的指标
QI (quality indicator)	在一个有效窗口内用载干比(S/I)加上信噪比 来估计信号的质量

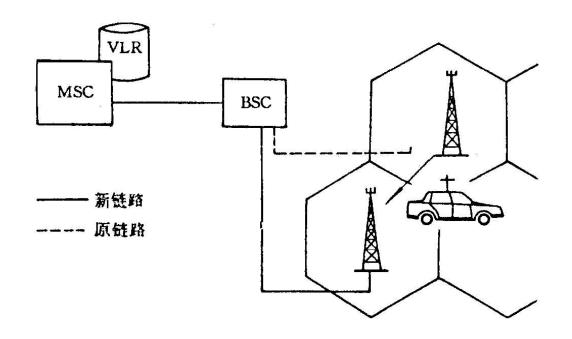
- ▶ 一般在决定是否切换时,主要根据上述两个指标: WEI和RSSI。
- → GSM采用"硬切换",即先断掉旧的的链路连接,然后建立新的链路连接。

越区切换的种类



同一基站控制器(BSC)内不同小区间的切换

- → BSC需要建立与新基站之间的链路,并在新的小区基站分配一个业务信道(TCH)。
- ▶ 移动业务交换中心(MSC)对这种切换不做控制。



越区切换的种类



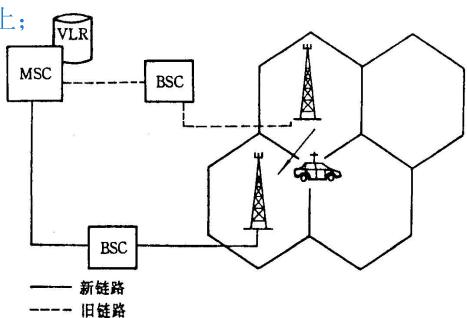
同一MSC/VLR内不同BSC控制的小区间的切换

MSC参与切换过程

- ◆ 原BSC向MSC请求切换;
- → 建立MSC与新的BSC、新的BTS的链路;
- → 选择并保留新小区空闲TCH供MS切换后使用;

→ 命令MS切换到新频率的新TCH上;

→ 切换成功后MS需要了解周围 小区的信息,若位置区域发 生了变化,呼叫完成后必须 进行位置更新。



越区切换的种类



- ▶ 不同MSC/VLR控制的小区间的切换
- ▶ 路由信息

当MS从正在为其服务的原MSC管辖的区域移动到目标MSC管辖的区域时,目标MSC要向原MSC提供一路由信息以建立两个移动交换中心的连接,这个路由信息是由一个切换号码提供。

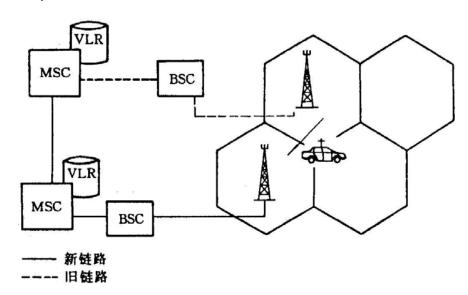
◆ 切换号码(HON, Handover Number)

HON = CC + NDC + SN

CC: 国家码

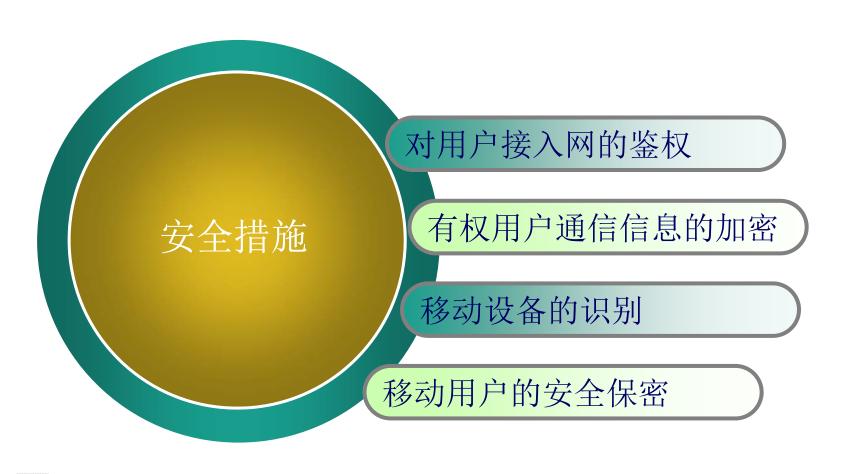
NDC: 数字蜂窝移动业务接入号

SN: 移动用户号



GSM的安全措施





对用户接入的网鉴



- → 作用
 - ▶ 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"
- → 原理: 基于GSM系统定义的鉴权键Ki
 - → 当移动用户在GSM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;
 - ◆ 鉴权的过程就是在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
- ▶ 解决方法:
 - → 在GSM系统中,为了鉴权和加密的目的应用了三种加密算法,即A3, A5 和A8算法。
 - → 用鉴权键Ki和AUC发来的伪随机数RAND通过算法A3加密算法产生加密的数据(符号响应(SRES))。移动终端向网络端发送SERS,通过与VLR的本地SRES进行对比完成验证。

鉴权键Ki+伪随机数RAND 符号响应SRES VLR

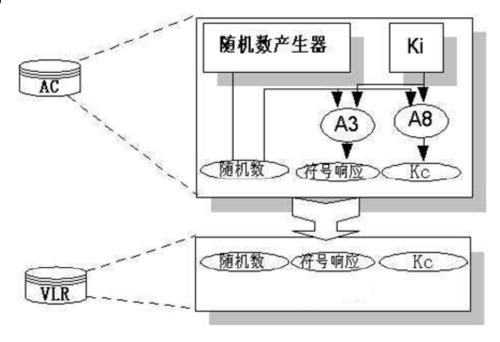
安全算法及鉴权三参数



→ 在GSM系统中,为了鉴权和 加密的目的应用了三种算法, 即A3,A5和A8算法。

算法	目 的
A3	产生SERS,鉴权
A8	产生供用户数据加密 使用的密钥 Kc
A 5	用户数据的加密

→ 在进行鉴权和加密时,GSM 系统要在其AUC产生鉴权三 参数: RAND、SERS和Kc。



鉴权三参数产生过程

鉴权的过程



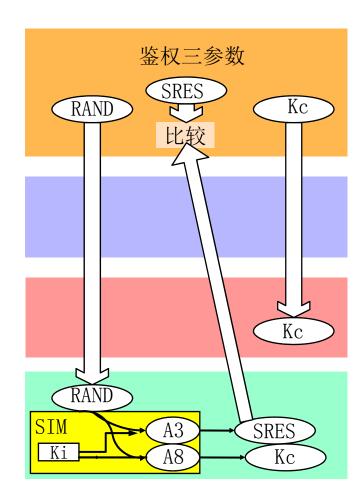
- → AC产生鉴权三参数后将其传送给 VLR;
- → 鉴 权 开 始 时 VLR 通 过 BSS 将 RAND发送给移动台的SIM卡。 SIM卡中具有与网络端相同的Ki 和A3、A8算法,可产生与网络端相同的SRES和Kc;
- → MS将SIM卡产生的SRES发给
 VLR,在VLR中进行鉴权验证;
- → 因为SRES是随机的,所以在空中传输时是加密的。











鉴权过程

无线链路上有权用户通信信息的加密

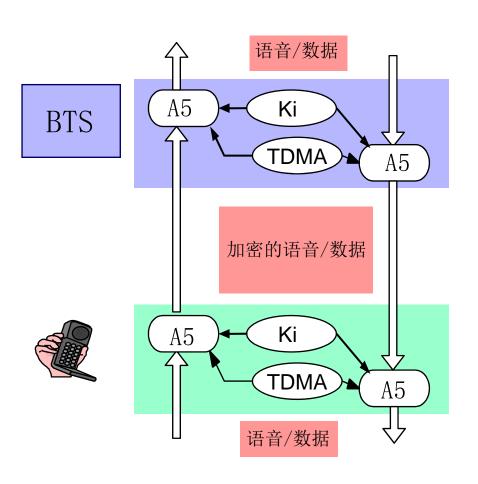


→ 目的

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 开始使用密钥Kc;
- ★ 在MS,由密钥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;
- → 在BTS,把从无线信道上收到的加密信息流、TDMA帧号和密钥 Kc,再经过A5算法解密后,传送给BSC和MSC;
- ◆ 上述过程反之亦然。



通信信息加密

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

→ 过程

- → 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, IER使用所定义的三个清单:

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。

移动用户的安全保密



用户的 临时识别码 TMSI 用户的 个人身份号 PIN

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(国际移动用户识别)或跟踪移动用户的位置。

→ 分配者

TMSI由MSC/VLR分配,并不断更换,更换周期由运营商决定。

▶ 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(PIN)



→ 位数

PIN是一个4~8位的个人身份号,用于控制对SIM卡的使用。

→ 使用过程

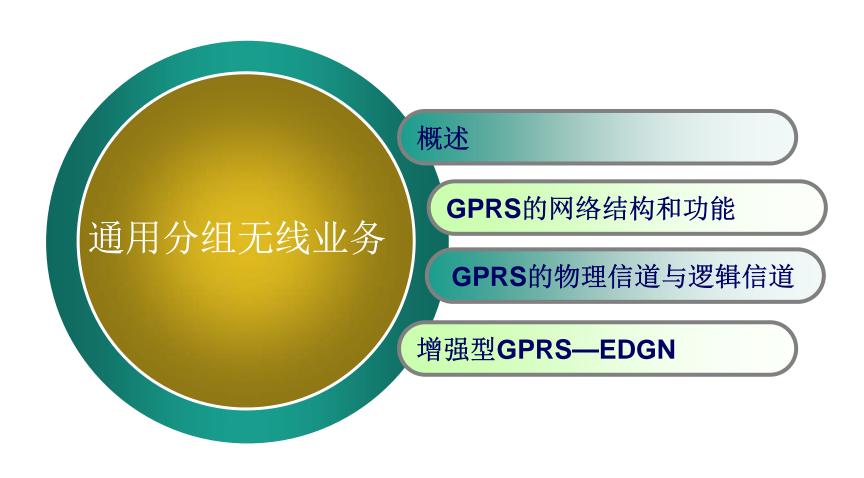
- → 只有PIN码认证通过,移动设备才能对SIM卡进行存取,读出相关 数据,并可以入网。
- ◆ 每次呼叫结束或移动设备正常关机时,所有的临时数据都会从移动设备传送到SIM卡中,再打开移动设备时要重新进行PIN码校验。

→ 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卡被阻塞, 须到网络运营商处消阻;
- → 连续十次不正确输入时,SIM卡会被永久阻塞,即作废。

通用分组无线业务 (GPRS)





GPRS概述

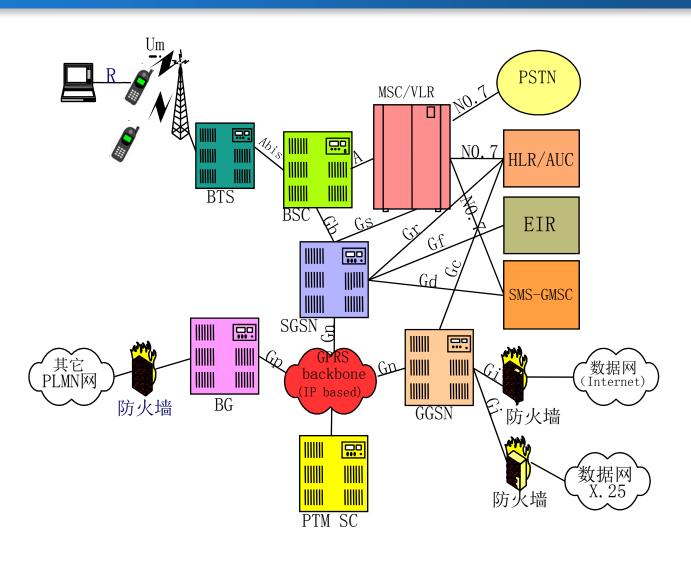


→ GSM

- ▶ 低数据速率,仅为9.6kbit/s,无法支持高速数据业务;
- → 只能为每个用户分配一个物理信道。
- → 高速电路交换数据(HSCSD)
 - ▶ 将多个业务信道复用在一起供一次数据业务使用,以提高无线接口数据的传输速率;
 - ★ HSCSD单个时隙的速率为14.4kbit/s; 4个时隙的速率为57.6kbit/s;
 8个时隙的速率为115.2kbit/s;
 - ▶ 根据分配的时隙数来计费。
- → 通用分组无线业务(GPRS)
 - ▶ 采用分组交换技术:
 - 按需动态占用资源:只在有数据传输时才分配无线资源,频谱利用 率较高;
 - ◆ 支持中、高速率的数据传输(9.05~171.2kbit/s);
 - ▶ 根据实际的数据传输量来计费;

GPRS的网络结构和功能





GPRS网络结构及其接口

GPRS的网络结构和功能



◆ SGSN: GPRS业务支持节点

SGSN的功能类似与GSM系统MSC/VLR,主要是对移动台进行鉴权、移动性管理和路由选择;建立移动台与GGSN直接的传输通道;进行业务统计与计费。

→ GGSN: GPRS网关支持节点

GGSN是GPRS网络对外部数据网络的网关或路由器。GGSN可以把GPRS的分组数据包进行协议转换,实现与外部的数据网络,如Internet网的互联。

→ BG: 边缘网关

实际上就是一个路由器,主要完成分属不同GPRS网络的SGSN、GGSN之间的路由以及安全性管理。

→ PTM SC: 点对多点业务中心

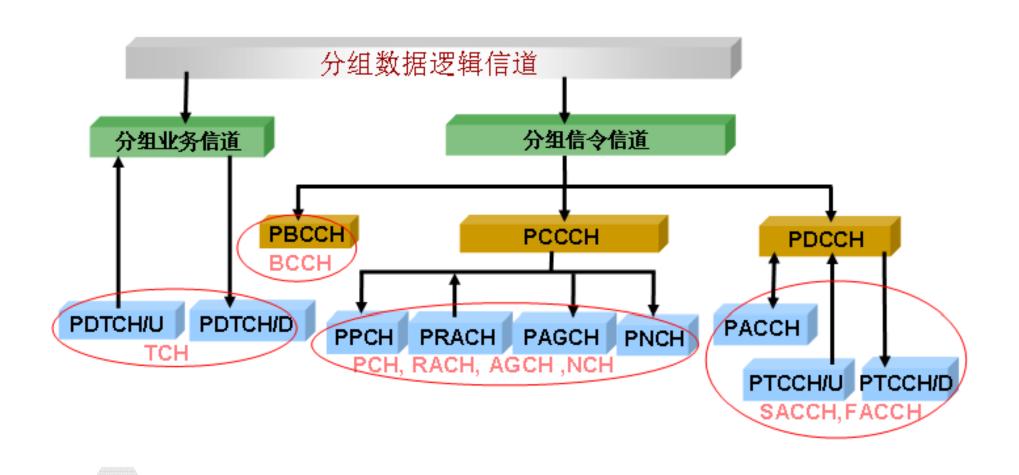
提供的点对多点数据业务,可根据某个业务请求者要求,把信息送给多个用户, 又可分为点对多点多信道 (PTM-M)广播业务、点对多点群呼 (PTM-G)业务等。

◆ GPRS 核心网

用于将SGSN、GGSN、BG等互联起来的IP专用网,用于传输GPRS的数据和信令。

GPRS的逻辑信道





GPRS的逻辑信道



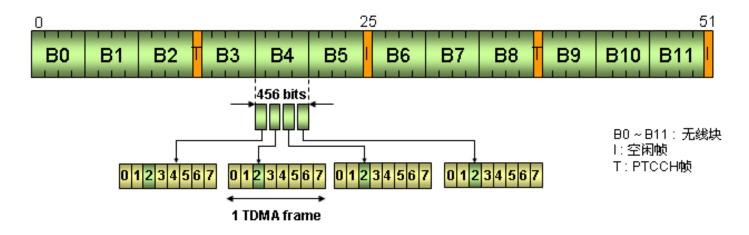
	逻辑信道分类	功能	上/下行
分组广播控制信道(PBCCH)		广播MS因分组业务接入网络所必需 的参数	下行
<i>(</i>) / H	分组寻呼信道(PPCH)	寻呼MS	下行
分组 公共	分组随机接入信道(PRACH)	请求分配一个或多个PDTCH	上行
控制信道	分组接入允许信道(PAGCH)	分配一个或多个PDTCH	下行
(PCCCH)	分组通知信道(PNCH)	告知MS有PTM-M(点对多点多信道) 广播业务	下行
分组	分组随路控制信道(PACCH)	在数据传送过程中传送分组信令	下行
专用	分组数据业务信道(PDTCH)	传送用户的分组数据	上/下行
控制 信道	· · · · · · · · · · · · · · · · · · ·	传送随机接入脉冲,以估计进行分组 业务的MS的时间提前量	上行
(PDCCH)	(PTCCH)	向移动台发送定时提前量的控制信息	下行

GPRS的物理信道



→ GPRS的物理信道称为分组数据信道(PDCH)。

在GPRS中,PDCH采用52帧复帧(约240ms)的结构,每4个帧组成一个无线块(Radio Block),因此一个无线信道共分为12个无线块。如下图所示:



每个时隙中的内容称为突发脉冲序列。

GPRS系统中共有4种不同的突发脉冲序列:

常规突发脉冲(NB), 承载所有业务信息和大部分信令信息;

接入突发脉冲(AB),用于MS建立与BTS的首次连接或越区切换;

频率校正突发脉冲(FB)以及同步突发脉冲(SB)。

增强型数据速率GSM演进技术(EDGE)

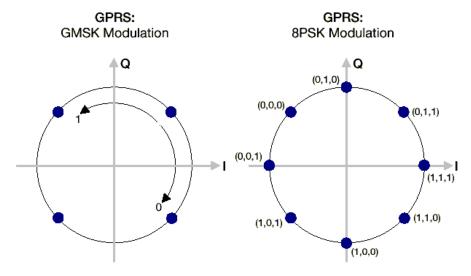


- → EDGE是英文Enhanced Data Rate for GSM Evolution 的缩写,即增强型数据速率GSM演进技术。一般认为EDGE是2G通往3G的一个过渡技术方案
- ★ 主要特点: 充分利用现有的GSM资源,特别是不需要大量改动或增加硬件,而只需对网络软件及硬件做一些较小的改动,就能够使运营商向移动用户提供高速率的数据业务,诸如互联网浏览、视频电话会议和高速电子邮件传输等无线多媒体服务。
- **→ 3项关键技术带来EDGE**速率的提升:
 - ▶ 8PSK调制方式:每个符号传送3比特;
 - ◆ 多种编码方案: 网络可以根据无线环境调整编码方式;
 - → 增量冗余(Incremental Redundancy: IR): 如果数据接收错误,则 通过重传增量冗余信息来提高解码成功率。

关键技术-EDGE的调制技术



EDGE引入了8PSK调制方式,通过信号的绝对相位来表示符号,其符号的可能性有8种,每个符号映射成3个比特。因此EDGE理论上可以达到GSM三倍的速率。



	GPRS	EDGE
调制方式	GMSK	8-PSK/GMSK
符号速率	270ksym/s	270ksym/s
比特速率	270kb/s	810kb/s
无线数据速率/时隙	22.8kbit/s	69.2kbit/s
最大用户速率/时隙	20kbit/s	59.2kbit/s
最大用户速率/8个时隙	160kbit/s	473.6kbit/s

关键技术-EDGE的编码方案



- ◆ EDGE共有9种不同的编码方式(MCS-1~MCS-9),其中MCS-1~MCS-4采用高斯最小键控(GMSK); MCS-5~MCS-9采用八进制相移键控(8PSK)。
- → 当采用MCS-9时EDGE系统达 到峰值传送速率,此时1个时隙 的传输速率为59.2kbps,每个 200kHz频点有8个时隙,那么 容易得到EDGE系统的理论峰值 速率为59.2*8=473.6kbps。
- → 当信道条件较好时,例如终端位于小区中心区域,可以采用速率较高的MCS-5~MCS-9;当信道条件恶劣时,例如终端位于小区边界,可以采用速率偏低的MCS-1~MCS-4。

方案	编码速率	调制方式	数据速率 kbp/s	分组
MCS-1	0.53	GMSK	8.8	С
MCS-2	0.66	GMSK	11.2	В
MSC-3	0.85	GMSK	14.8	A
MCS-4	1.0	GMSK	17.6	C
MCS-5	0.37	8-PSK	22.4	В
MCS-6	0.49	8-PSK	29.6	A
MCS-7	0.76	8-PSK	44.8	В
MCS-8	0.96	8-PSK	56.4	A
MCS-9	1.0	8-PSK	59.2	A

关键技术-链路质量控制



- → 所谓链路质量控制(LQC)就是指在数据传输过程中通过改变调制方式和编码方式,动态地适应无线传输环境,已达到提高链路质量的方法。EDGE采用了一套精心设计的、高效的LQC算法: 链路自适应(LA)和增量冗余(IR)。
 - → 链路自适应(LA):根据信道环境选择合适的MCS来获得最大的吞吐量。9种编码方式被分成3组,运营商可以自定义初始编码方式,在通信过程中,编码方式可以在同组内变化。这种方式与GPRS不同,在GPRS系统中数据重传时必须采用上一次的编码方式,无法根据信道环境的变换而调整。LA在保证传输质量的同时最高限度的使用了无线资源。
 - → 增量冗余(IR):数据传输采用速率兼容打孔卷积码(RCPC)的特定打孔模式,数据重传时采用不同的打孔模式,接收时原始数据和重传数据合并解码。在GPRS数据传输时,如果出现误码,该数据块进行重传,直至正确接收。而在EDGE网络中采用不同的打孔方案,接收端可以将每次重传的数据块进行重组,从而减少了重传的次数,提高了传输效率。

内容



- *第一代模拟移动通信系统
- ❖ 第二代数字GSM移动通信系统
- **❖**第二代窄带CDMA移动通信系统

窄带CDMA移动通信系统





窄带CDMA 移动通信系统 蜂窝小区构成及频率配置

IS-95 CDMA的信道划分

IS-95 CDMA的功率控制技术

IS-95 CDMA的软切换技术

概述



- → IS-95 CDMA系统由高通公司设计并于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。
- → IS-95是兼容AMPS模拟制式的双模标准,主要包括IS-95A和IS-95B两个系列标准,它们都属于第二代移动通信技术标准。
 - → IS-95A是1995年5月TIA正式颁布的窄带CDMA标准,在全球得到广泛应用,可提供最大9.6kb/s电路型数据接入。
 - → IS-95B标准是IS-95A的进一步发展,其主要目标是提高CDMA系统性能,满足更高比特速率业务的需求,IS-95B支持8个码信道的捆绑使用,可提供的理论最大比特速率为115kb/s。

→ IS-95 系统的工作频带

- → 上行(移动台->基站): 869~894MHz;
- → 下行(基站->移动台): 824~849MHz;
- → 双工间隔为45MHz;

IS-95 系统与蜂窝结构的关系



→ IS-95 CDMA的频谱带宽

- ▶ 陆地移动通信环境下的多径时延扩展通常为1μs或者更大,为了能分离多径信号要求扩频序列的码片速率至少为1MHz。扩频信号带宽越宽,可实现的多径分离也越精细,比如带宽为100MHz,可分离的多径信号时延为10ns,但是900MHz频段不能提供如此宽的频谱资源。
- → 考虑到可用频谱和设备复杂度的限制, IS-95 系统的载频间隔设置为 **1.25MHz**,码片的速率为1.2288Mc/s。为了与3G的WCDMA(载频间隔 5MHz)区别,通常称IS-95系统为**窄带CDMA系统**。

→ IS-95 CDMA与蜂窝小区和扇区的关系

- ◆ 在CDMA蜂窝系统,不同的DS-CDMA蜂窝系统可采用不同的载频区分,而 对同一个DS-CDMA蜂窝系统的某一个载频,则是采用地址码选择站址的, 即对不同的小区和扇区基站分配不同的码型。
- ◆ 在IS-95 CDMA系统中,这些不同的码型是由一个PN码序列生成的,PN序列周期为2¹⁵=32768个码片,并将此周期序列每隔64码片移位序列作为一个码,共可得到32768/64=512个码。即在1.25MHz带宽的CDMA蜂窝系统中,可区分多达512个基站(或扇区站)。
- → 在一个小区(或扇区)内,基站与移动台之间的信道,是在PN序列上再采用正交序列进行码分的信道。



→ 前向链路

前向链路指由基站发往移动台的无线通信链路,也称作下行链路。

→ 前向逻辑信道及其功能

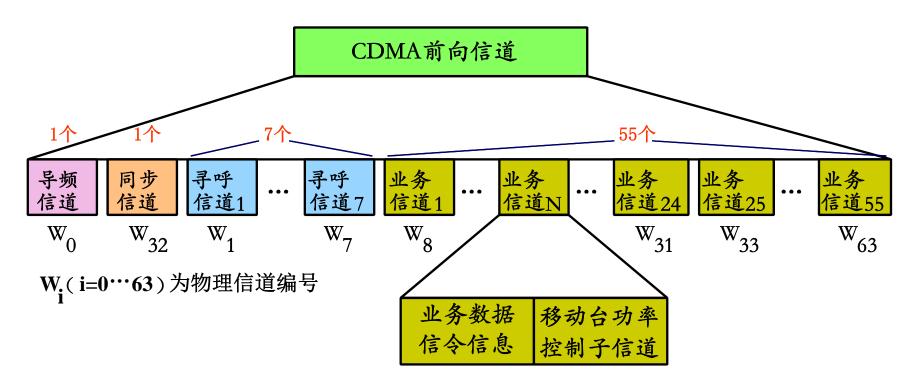
- → <mark>导频信道(Pilot Channel)</mark>: 基站在此信道发送导频信号(其信号功率比其 他信道高20dB)供移动台识别基站并引导移动台入网;
- **▼ 同步信道(Synchronizing Channel)**: 基站在此信道发送同步信息供移动台建立与系统的定时和同步;
- → 寻呼信道(Paging Channel): 基站在此信道寻呼移动台,发送有关寻呼指令 及业务信道指配信息;
- → 前向业务信道(Traffic Channel):供基站到移动台之间通信,用于传送用户业务数据和信令信息。该信道包含有业务数据子信道和功率控制子信道,前者传送用户信息和信令信息,后者用于传送功率控制信息。

→ 前向物理信道

→ 在IS-95中,基站和移动台之间的前向链路的码分物理信道,是在PN序列上再采用正交信号的码分信道,其正交信号是64位的Walsh码,记作 W_0 , W_1 , W_2 ,…, W_{63} ,可提供**64个码分物理信道**。



→ 前向逻辑信道与物理信道的映射关系



特殊情况: 当用户数过多,业务信道数目不够时,某几个寻呼信道可以临时用作业务信道;极端情况下,7个寻呼信道和1个同步信道都可用作业务信道。



▶ 反向链路

反向链路指由移动台发往基站的无线通信链路,也称作上行链路。

→ 反向逻辑信道及其功能

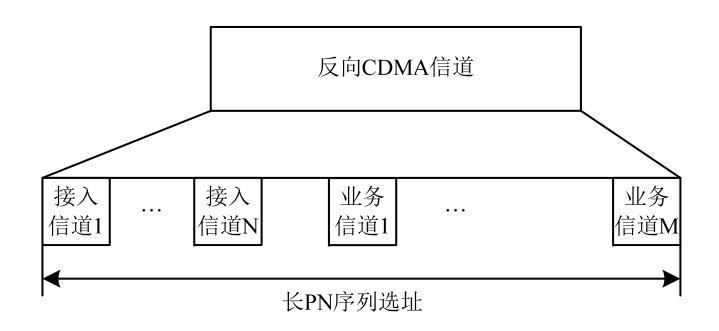
- → 接入信道(Access Channel): 与前向链路的寻呼信道相对应,其作用是在移动台没有占用业务信道之前,提供移动台至基站的传输通路,供移动台发起呼叫或者对基站的寻呼进行响应,以及向基站发送登记注册消息等。
- ▶ 反向业务信道(Reverse Traffic Channel): 与前向业务信道一样,反向业务信道用于传送用户业务数据,同时也传送信令信息。

→ 反向物理信道

- → 在IS-95中,反向链路的码分物理信道是由长度为2⁴²-1的长PN序列构成的。 使用长码的不同相位偏置来区分不同的用户。
- ★ 长码PN_A和PN_T序列分别为反向接入信道和业务信道提供码分物理信道,其中最多可设置的接入信道数N=32,对应于PN_{A1}~ PN_{AN};最多可设置的业务信道数M=64,对应于PN_{T1}~ PN_{TM}。



▶ 反向逻辑信道与物理信道的映射关系



◆ 长码PN_A和PN_T序列分别为反向接入信道和业务信道提供码分物理信道,其中最多可设置的接入信道数N=32,对应于PN_{A1}~PN_{AN};最多可设置的业务信道数M=64,对应于PN_{A1}~PN_{AM}。

IS-95 CDMA的功率控制



→ 功率控制的分类

◆ 功率控制分为前向功率控制和反向功率控制;

→ 前向功率控制

- ◆ 前向链路功率控制主要解决同频干扰问题。前向链路控制的目的是要使移动 台接收到的信噪比为所需的最小值,这种方式可使处于严重干扰区域的移动 台保持较好的通信质量,同时减少对其他信号的干扰。
- ◆ 在前向功率控制中,基站根据移动台提供的测量结果,调整对每个移动台的 发射功率,其目的是对路径衰落小的移动台分配较小的正向链路功率,而对 那些远离基站和误码率高的移动台分配较大的正向链路功率。通过在各个前 向业务信道上合理的分配功率可以确保各个用户的通信质量,同时使前向链 路容量达到最大。

→ 反向功率控制

- ▼ 反向功率控制主要解决远近效应,通过控制各移动台的发射功率的大小,保证基站接收到的小区内所有移动台信号功率相等,从而使各用户之间相互干扰最小。
- ▼ 反向功率控制又可分为仅由移动台参与的开环功率控制和移动台、基站同时 参与的闭环功率控制。

IS-95 CDMA的功率控制



→ 反向开环功率控制

- ▼ 它的前提条件是假设上行链路和下行链路传输损耗相同。移动台接收 并测量基站发来的信号强度,并估计下行传输损耗;然后根据这种估 计,移动台自行调整其发射功率,若接收信号增强,则移动台降低发 射功率;接收信号减弱,则移动台增加发射功率。
- → 开环功率控制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、节省开销、简单易行。但由于CDMA系统采用频分双工的通信方式,收发频率相差45MHz,已远远超过信道的相干带宽,使得这种直接依据前向信道信号电平来调节移动台发射功率的方法不能对功率进行完善的调节。为了解决这个问题,可采用闭环功率控制方法。

IS-95 CDMA的功率控制



→ 反向闭环功率控制

- ▶ 闭环功率控制是指移动台根据基站发送的功率控制指令(功率控制比特携带的信息)来调节移动台的发射功率的过程。闭环功率控制的设计目标是使基站对移动台的开环功率估计迅速做出纠正,以使移动台保持最理想的发射功率。
- ★ 在反向闭环功率控制中,基站起主导作用。基站测量所接收到的每一个移动台的信噪比,并与一个门限相比较,决定发给移动台的功率控制指令是增大还是减少它的发射功率。移动台将接收到的功率控制指令与移动台的开环估算相结合,来确定移动台闭环控制应发射的功率值。

IS-95 CDMA的软切换技术



→ 切换过程

在移动通信系统中,对于正在通信中的移动台,当它由一个基站的覆盖 区域移动到另外一个基站的覆盖区域时,为了保证通信的连续性,网络 控制系统会启动<mark>切换过程</mark>,将移动台与网络之间的通信链路从当前基站 转移到新的基站,以保证用户业务的连续传输。

→ 分类

根据切换发生时,移动台与原基站以及目标基站连接方式的不同,可以将切换分为硬切换与软切换两大类。

→ 硬切换

- ▼ 硬切換是指移动台先中断与原基站的联系,再去建立和新基站联系的 切换方式,在整个切换过程中移动台只能使用一个无线信道。
- ◆ 在硬切换过程中,可能存在原有的链路已经断开,但是新的链路没有 成功建立的情况,导致切换失败,通话中断。
- → 采用**不同频率的小区**之间只能采用硬切换,所以模拟系统和**TDMA**系统(如**GSM**系统)都是采用硬切换的方式。

IS-95 CDMA的软切换技术



▶ 软切换

- ◆ <mark>软切换</mark>是指移动台需要切换时,先与新的基站建立联系,再中断与原基站联系的切换方式。软切换可以有效地提高切换的可靠性,大大减少切换造成的掉话。
- ◆ 软切换只能在同一频率的信道间进行,因此,模拟系统、TDMA系统 不具有这种功能。
- → 软切换还可细分为:
 - **更软切换**是指发生在同一基站具有相同频率的不同扇区间的切换。 软切换过程中会伴随有新的通信链路的建立和旧的通信链路的删除 ,而更软切换的前后,使用的是相同的通信链路。更软切换由移动 台提出,由基站来完成,不需要MSC的参与,但要通知MSC。
 - 软/更软切换是移动台从一个小区的扇区进入相同载频的另外一个小区的扇区采用的过境切换。这种类型的切换网络资源包括小区A和B之间的双方软切换资源,加上小区B内的更软切换资源。

Thank You

