

## 5.1 第三代移动通信系统标准介绍

### 5.1.1 3G 的历史及特征

#### 1. 3G 的发展历程

3G 是第三代移动通信系统的简称,是早在 1985 年由国际电信联盟(ITU)率先提出并负责组织研究的、采用宽带码分多址数字技术的新一代通信系统,是现代移动通信技术和实践的总结和发展。3G 在当年提出时被命名为未来公众陆地移动通信系统(FPLMTS),1996 年更名为 IMT-2000,意指在 2000 年左右开始商用、工作在 2000MHz 频段上且数据传输速率达到 2000Kb/s 的国际移动通信系统。21 世纪初,全球 3G 业务快速成长,网络覆盖率迅速提升;随后,3G 增强型技术成为主流应用技术,绝大部分网络已升级到增强型技术;随着 3G 市场的成熟,全球 3G 用户数也进入规模增长阶段。3G 的发展经历了如下历程。

(1) 1991 年,ITU 正式成立 TG8/1 工作组,负责 FPLMTS 标准的制定。

(2) 1992 年,世界无线电行政大会(WARC)在 2000MHz 频段上分配了 230MHz 频段给 FPLMTS 使用,这次会议成为 3G 标准制定进程中的重要里程碑。

(3) 1997 年 4 月,ITU 在全球范围内征集 IMT-2000 无线传输方案。

(4) 1998 年 6 月,ITU 共收到 10 种地面无线传输方案。

(5) 1999 年 3 月,完成 IMT-2000 关键参数部分的标准化的。

(6) 1999 年 11 月,确定了 IMT-2000 的无线传输技术规范,将无线接口的标准明确为 5 个标准,如表 5-1 所示。

表 5-1 IMT-2000 无线接口标准

CDMA 技术	IMT-2000 CDMA DS	对应 WCDMA
	IMT-2000 CDMA MC	对应 CDMA 2000
	IMT-2000 CDMA TDD	对应 TD-SCDMA(UTRA TDD LCR)和 UTRA TDD(HCR)
TDMA 技术	IMT-2000 TDMA SC	对应北美 UNC-136
	IMT-2000 FDMA/TDMA	对应欧洲 EP-DECT

(7) 2000 年 5 月,完成 IMT-2000 的全部网络规范,其中包括美国 TIA 提交的 CDMA 2000、欧洲 ETSI 提交的 WCDMA 以及中国电信科学技术研究院(CATT)提交的 TD-SCDMA。

其中两种基于 TDMA 技术的标准分别适用于北美和个别欧洲地区,是区域性 3G 标准

规范；而基于 CDMA 技术的 3 种标准则成为 3G 主流标准，CDMA 技术也被公认为 3G 的主流技术。

基于共同的利益目标，以欧洲的 ETSI、日本的 ARIB/TTC、美国的 T1、韩国的 TTA 和中国的 CWTS 为核心发起成立了 3GPP(1998 年底成立，CWTS 在 1999 年加入)，专门研究如何从第二代的 GSM 向 IMT-2000 CDMA DS 和 IMT-2000 CDMA TDD 演进；以美国 TTA、日本的 ARIB/TTC、韩国的 TTA 和中国的 CWTS 为首成立的 3GPP2(1999 年 1 月成立，CWTS 在 1999 年 6 月加入)，则专门研究如何从 IS-95 CDMA 系统向 IMT-2000 MC 演进。3GPP 和 3GPP2 成立后，ITU 主要负责标准的正式制定和发布方面的管理工作，而 IMT-2000 的标准化研究工作则主要由 3GPP 和 3GPP2 承担。

3GPP 主要制定基于 GSM MAP 核心网，以 WCDMA、TD-SCDMA 为无线接口的标准，称为 UTRA(通用陆地无线接入)，同时也在无线接口上定义与 ANSI-41 核心网兼容的协议；3GPP2 主要制定基于 ANSI-41 核心网，以 CDMA 2000 为无线接口的标准，同时也在无线接口定义与 GSM MAP 核心网兼容的协议。

## 2. 3G 的特征

第三代移动通信系统中采用了 RAKE 接收、智能天线、高效信道编译码、多用户检测、功率控制和软件无线电等多项关键技术。总体来说，第三代移动通信系统具有如下特征。

(1) 全球化：3G 的目标是在全球采用统一标准、统一频段、统一大市场。IMT-2000 是一个全球性的系统，各个地区多种系统组成了一个 IMT-2000 家族，各系统在设计上具有很好的通用性，与此同时，3G 业务与固定网的业务也具有很好的兼容性；ITU 划分了 3G 的公共频段，全球各地区和国家在实际运用时基本上能遵从 ITU 的规定；全球 3G 运营商之间签署了广泛的协议，基本形成了大一统的市场。基于以上条件，3G 用户能在全球实现无缝漫游。

(2) 多媒体化：提供高质量的多媒体业务，如语音、可变速率数据、移动视频和高清晰图像等多种业务，实现多种信息一体化。

(3) 综合化：多环境、灵活性，能把现存的无绳、蜂窝(宏蜂窝、微蜂窝、微微蜂窝)、卫星移动等通信系统综合在统一的系统中(具有从小于 50m 的微微小区到大于 500km 的卫星小区)，与不同网络互通，提供无缝漫游和业务一致性；网络终端具有多样性；采用平滑过渡和渐进式演进方式，即能与第二代移动通信系统共存和互通，采用开放式结构，易于引入新技术；3G 的无线传输技术满足三种传输速率，即室外车载环境下为 144Kb/s，室外步行环境下为 384Kb/s，室内环境下为 2Mb/s。

(4) 智能化：主要表现在优化网络结构方面(引入智能网概念)和收发信机的软件无线电化。

(5) 个人化：用户可用唯一个人电号码(PTN)在任何终端上获取所需要的电信业务，这就超越了传统的终端移动性，但也需要足够的系统容量来支撑。

第三代移动通信系统除了具有上述基本特征之外，还具有高频谱效率、低成本、优质服务质量、高保密性及良好的安全性能、收费制度更合理等特点。

### 5.1.2 3G 的主流标准及无线技术对比分析

3G 的 3 大主流应用技术标准是 WCDMA(宽带码分多址接入)、CDMA 2000(多载波码分多址接入)和 TD-SCDMA(时分同步码分多址接入)，在 3 大标准中，WCDMA 和 CDMA

2000 采用 FDD 方式,需要成对的频率规划。WCDMA 的扩频码速率为 3.84Mc/s,载波带宽为 5MHz,而 CDMA 2000 采用单载波时扩频码速率为 1.2288Mc/s,载波带宽为 1.25MHz;另外,WCDMA 的基站间同步是可选的,而 CDMA 2000 的基站间同步是必需的,因此需要全球定位系统(GPS),以上两点是 WCDMA 和 CDMA 2000 最主要的区别。除此以外,在其他关键技术方面,例如,功率控制、软切换、扩频码以及所采用分集技术等基本都是相同的,只有很小的差别。

TD-SCDMA 的双工方式为 TDD,不需要为其分配成对的频带。扩频码速率为 1.28Mc/s,载波带宽为 1.6MHz,其基站间必须同步。与其他两种标准相比,TD-SCDMA 采用了智能天线、联合检测、上行同步及动态信道分配、接力切换等技术,具有频谱使用灵活、频谱利用率高等特点,适合非对称数据业务。

3 大主流标准的空中接口的具体参数对照如表 5-2 所示。

表 5-2 WCDMA、CDMA 2000 和 TD-SCDMA 空中接口参数对照

对照参数	WCDMA	CDMA 2000	TD-SCDMA
载波带宽	成对频带,单向 5MHz	成对频带,单向 1.25MHz(CDMA 2000 1x)/ 3.75MHz(CDMA 2000 3x)	上下行共享一个频带,共 1.6MHz
多址方式	DS-SSMA(5MHz)	DS-SSMA(1.25MHz) MC-SSMA(3.75MHz)	TDMA/DS-SSMA(1.6MHz) FDMA/TDMA/DS-SSMA (5MHz,3个载波)
双工模式	FDD(频分双工)	FDD(频分双工)	TDD(时分双工)
码片速率(Mc/s)	3.84	1.2288 3.6864	1.28
扩频码	OVSF	Walsh	OVSF
扩频因子	4~512	4~512	1,2,4,8,16
无线帧长	10ms	20ms,5ms	10ms(分为2个5ms的子帧)
时隙数	15个时隙/帧	—	10个时隙 (其中7个为业务时隙)/子帧
信道编码	卷积码,Turbo码	卷积码,Turbo码	卷积码,Turbo码
符号调制	上行:BIT/SK 下行:QPSK	上行:BIT/SK 下行:QPSK	上/下行:QPSK,8PSK
功率控制	开环、闭环(1500Hz)	开环、闭环(800Hz)	开环、闭环(200Hz)
接收机技术	RAKE	RAKE	联合检测,智能天线
同步要求	基站同步或异步	基站间GPS同步	基站间同步 多用户同步

3种标准的无线接口技术在发展成熟度上各具优势,但总体来看,WCDMA网络被更多运营商所接受,在全球商用网络中占有的份额大,因为其无线网络性能更胜一筹。以下是它的几点优势。

(1) 使用的带宽和码片速率是最宽的,因而能提供更大的多路径分集、更高的中继增益和更小的信号开销,此外,更高的码片速率也改善了接收机解决多径效应的能力。

(2) 小区站点同步设计可选用异步基站,不需要采用GPS同步,基站开设可兼顾室内、室外的覆盖。

(3) 功率控制速率最快,可保证更好的信号质量,并支持更多的用户。

(4) 在公共信道开销方面,其下行链路导频结构基于专用和公共导频符号,所以导频信道只需占下行链路总传输功率的约 10%;而 CDMA 2000 由于基于公共持续导频序列,故要占 20%左右。

### 5.1.3 3G 频段的划分

ITU 中协调全球无线电频段规划的部门是 WARC(世界无线电行政大会),在 ITU 改组后成为 WRC(世界无线电通信大会)。WARC-92 为 3G 划分了 230MHz 的核心频段,如图 5-1 所示。其后,WRC 后续的会议又为 3G 分配了新的频段,如 WRC-2000 为 3G 划分 1710~1885MHz 和 2500~2690MHz 频段为主要的附加频段,同时决定 3G 可以使用现 2G 业务频段,而 3G 卫星业务可使用 3G 以下现存移动卫星业务(MSS)频段。

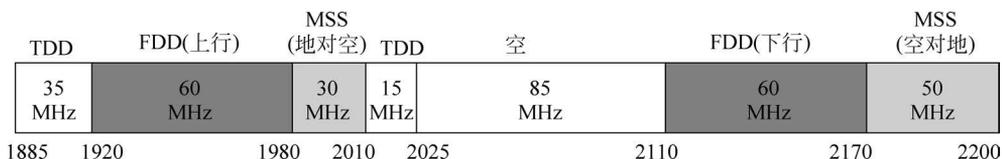


图 5-1 ITU 的 3G 频段划分建议

各国的实际使用情况与 ITU 的 3G 频段规划有少许差别,在欧洲和大部分亚洲地区,IMT-2000 的 2×60MHz 频段分配给 WCDMA-FDD 系统:上行频段为 1920~1980MHz,下行频段为 2110~2170MHz。留给 WCDMA-TDD 的频段较为零散:获得运营执照的 TDD 系统使用 1900~1920MHz 和 2020~2025MHz 共 25MHz 的频段;剩下的一个单独的频段 2110~2120MHz 则用于不需要执照的 TDD 业务。北美的情况较为复杂,ITU 建议的 3G 频段已经拍卖给 2G 系统的运营商,而且没有新的频段指定给 3G 系统。所以只能在 2G 的频段上使用部分频段来开展 3G 的业务。

我国的 3G 频段划分方案参照了 ITU 的建议,并和 ITU 基本保持了一致,如图 5-2 所示。具体方案如下:①主要工作频段:FDD 模式的上行频段为 1920~1980MHz,下行频段为 2110~2170MHz,而 TDD 模式的频段为 1880~1920MHz 和 2010~2025MHz;②补充工作频段:FDD 模式的上行频段为 1755~1785MHz,下行频段为 1850~1880MHz,而 TDD 模式的频段为 2300~2400MHz;③MSS 频段:地对空为 1980~2010MHz,空对地为 2170~2200MHz。这样我国 TDD 模式共获得了 155MHz 的频段,FDD 也获得了 180MHz 的频段,体现了我国支持自主知识产权及 FDD/TDD 有机互补与健康合理发展这一基本特征。需要说明的是,在 2007 年 11 月 ITU 举行 WRC-07 大会上,接受了我国提出的将 2300~2400MHz 频段作为全球统一频段的建议,这也就意味着为 TD-SCDMA 的国际漫游提供了可能。



图 5-2 我国的 3G 频段划分方案

### 5.1.4 3G 业务特点与分类

3G 业务是指所有能够在 3G 网络上承载的各种移动业务,它包括点对点基本移动语音业务和各类移动增值业务,3G 业务具有丰富的多媒体业务应用、高速率的数据承载、业务提供方式灵活和提供业务的 QoS 保证的特点。移动增值业务是移动运营商的主要利润增长点,也是发展 3G 业务的方向,3G 运营商在保留和增强 2G/2.5G 移动增值业务的同时,大量开发并提供了新的 3G 移动增值业务,它们具备互联网化、媒体化和生活化的特点。3G 移动增值业务中,成熟类的主要有短消息(SMS)、彩铃、WAP、IVR(交互式语音应答)等业务;成长类的主要有移动即时通信、移动音乐、MMS(彩信)、移动邮件、移动电子商务、移动位置服务(LBS)、手机媒体、移动企业应用、手机游戏、无线上网卡业务跟踪等业务;萌芽类主要有移动博客、手机电视、一键通(PTT)、移动数字家庭网络、移动搜索、移动 VoIP 等业务。

目前制定 3G 业务标准的标准化组织主要有 3GPP、3GPP2、OMA(开放移动联盟)等,为了适应新的业务模式,这些标准化组织的工作都集中在标准化业务体系框架和业务能力上,而对业务本身并不做规范。其中,3GPP 定义了框架业务能力特征(提供公共使用能力)和非框架业务能力特征(允许业务使用网络底层)两种业务能力特征;OMA 定义了公共业务引擎和专业业务引擎等各种技术引擎,专业业务引擎负责提供基本的业务能力特征。

对 3G 进行科学的分类,对业务发展是十分必要的。由于 3G 业务的多样性、用户使用特征的差异以及运营商情况的不同,对 3G 业务的分类也可以从多角度进行。总体来说,可按以下角度划分 3G 业务。

(1) 从承载网络来分,3G 业务可以分为电路域和分组域业务,其中电路域业务包括主语音、智能网业务、短信、彩铃、补充业务等;分组域业务包括数据业务、数据卡上网和 IMS 业务等。

(2) 从业务特征上分,3G 业务可以分为语音和非语音两大类,语音类包括基本语音和增强语音;非语音业务包括数据业务、数据卡上网、智能网业务和补充业务等。

(3) 从服务质量(QoS)来分,3GPP 提出了会话类、流媒体、交互类和后台类 4 种业务区分方式。会话类业务主要为语音通信和视频电话业务;流媒体业务可分为长流媒体和短流媒体业务,也可分为群组流体与个人流媒体业务,还可分为广播式流媒体和交互式流媒体业务;交互类业务包括基于定位的业务、网络游戏等;后台类业务有 E-mail、SMS、MMS 和下载业务等。会话类和流媒体业务对时延敏感,但允许较高的误码率;而交互类和后台类业务对时延要求低,但对误码率要求高。

(4) 从业务发展和继承方面考虑,3G 业务可以分为 2G/2.5G 继承业务及 3G 特色业务。

(5) 基于 3G 用户需求,3G 业务可分为通信类、消息类、交易类、娱乐类和移动互联网类。

3GPP 从承载网络和 QoS 两方面对 3G 业务进行了分类,前面已进行了介绍。需要说明的是,3GPP 定义了工具箱,如 CAMEL、MExE 和 USAT 等,运营商可利用这些工具箱或者外部解决方案来修改已有业务或者创建新业务。

随着移动业务的发展,3G 业务发展将面临一个截然不同的外部环境,其业务价值链分工将更加细化。其中,SP(服务提供商)的作用是开发和提供应用服务,它的主要工作包括需求评估、应用设计、应用模拟、实施和发布等;如果 SP 将应用设计的工作外包,则出现了

另一个独立的价值链环节——AP(应用提供商)。CP(内容提供商)的作用是开发和提供内容,并将其提供给 SP,其主要工作有制造内容、内容管理、内容发布和索引链接(门户)等。

## 5.2 WCDMA 系统

### 5.2.1 概述

#### 1. WCDMA 的发展和现状

ETSI 把 3G 技术统称为 UMTS(通用移动通信系统)。1998 年,日本和欧洲在宽带 CDMA 建议的关键参数上取得一致,使之正式成为 UMTS 体系中 FDD 频段的空中接口的入选方案,并由此通称为 WCDMA,后来它成了 ITU 的 IMT-2000 体系的 3 大主流标准之一。在欧洲,WCDMA 也称为 UMTS,或者叫 UTRA-FDD。

WCDMA 是最早,也是最完善的 3G 通信体制。3 大主流标准中,最早建成商用网络并开展 3G 业务的是 WCDMA。现阶段,WCDMA 是全球 3G 运营商在 3 大标准中选择最多的体制。

#### 2. WCDMA 的主要特点

概括起来,WCDMA 系统具有以下特点。

(1) 信道复杂,可适应多种业务需求。WCDMA 可通过公共信道/共享信道、接入信道和专用信道等不同类型的信道实现不同业务,适应不同时延和分布特点的要求,使资源的调配更加灵活。正是这种复杂的信道和灵活的资源调配方式,可使 WCDMA 能满足不同业务的 QoS。

(2) 大容量和高业务速率。WCDMA 系统的码片速率达 3.84Mc/s,载波带宽为 5MHz,相对于窄带 CDMA 系统,WCDMA 系统的带宽能够支持更高的速率,同时带来了无线电传播的频率分集;相对于速率大致相同的语音业务,具有更高的扩频增益,接收灵敏度更高。

(3) 功率控制完善。WCDMA 采用开环和闭环两种功率控制方式,当链路没有建立时,开环功率控制用来调节接入信道的发送功率;链路建立之后使用闭环功率控制。WCDMA 的上、下行均采用快速功率控制,频率为 1500Hz,在 3 类标准中是最快的,其快速功率控制速度比任何较明显的路径损耗的变化都要快,甚至比低速和中速移动的用户设备产生的瑞利衰落的速度还快,可以有效抵抗链路的功率不平衡现象和瑞利衰落,能够更好地控制系统内的干扰,提升网络覆盖、容量方面的性能。

(4) 支持基站异步操作。同步只是可选项,也就是说网络侧对同步没有要求,从而易于实现室内和密集小区的覆盖,但需要快速小区搜索技术。

(5) 切换机制健全,有更灵活的分层组网结构。WCDMA 系统既支持软切换,又支持不同载频间的硬切换,也可以采用压缩模式实现不同系统之间的硬切换;提供分层小区结构(HCS)组网,即分别选择宏小区、微小区、微微小区进行组网,以满足不同容量和覆盖需求。

(6) 优化的分组数据传输方式。支持帧间数据速率转换,允许不同 QoS 要求的业务复用,具有良好的资源调度机制。

(7) 上、下行链路均利用导频进行相干检测。和窄带 CDMA 系统相较,增加了反向导

频辅助的相干检测,扩大了覆盖范围。

### 3. WCDMA 系统的基本结构

WCDMA 系统的基本结构如图 5-3 所示,以模块来划分,整个 WCDMA 系统可分成 3 个功能实体:用户设备(UE)、无线接入网(RAN)和核心网(CN)。无线接入网也可以借用 UMTS 中地面 RAN 的概念,因此又可以简称为 UTRAN(UMTS 陆地无线接入网)。CN 可以和 PSTN、ISDN、其他运营商的 PLMN 和 Internet 等外部网络进行通信。WCDMA 系统中,无线接入网和核心网可以分开发展。无线接入网采用整体推进,使用 WCDMA 无线接口技术;而核心网可以从已有的 GSM/GPRS 核心网平台开始,以平滑演进的方式逐步过渡到全 IP 通信网络。

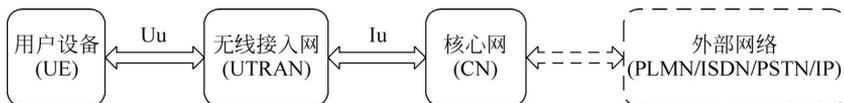


图 5-3 WCDMA 系统的基本结构

WCDMA 系统中的功能实体的具体组成和作用如下。

(1) UE 包括移动设备(ME)和 UMTS 用户识别模块(USIM)两部分。ME 是进行无线通信的设备;USIM 相当于 GSM 终端中的 SIM 智能卡,用于记载用户标识,可执行鉴权算法,并保存鉴权、密钥及终端所需的一些预约信息。

(2) UTRAN 的主要作用是实现无线接入和无线资源管理。UTRAN 的结构包含一个或几个无线网络子系统(RNS),一个 RNS 由一个无线网络控制器(RNC)和一个或多个节点 B(Node B)组成,如图 5-4 所示。RNC 在逻辑上对应于 GSM 网中 BSC,它控制辖区内的无线资源,是与之相连的 Node B 的管理者,也是无线接入网提供给 CN 的所有业务的接入点;Node B 在逻辑上对应于 GSM 网中的 BTS,它主要完成 Uu 接口的物理层的功能(信道编码、交织、速率匹配和扩频等),也完成部分无线资源控制(如功率控制)。

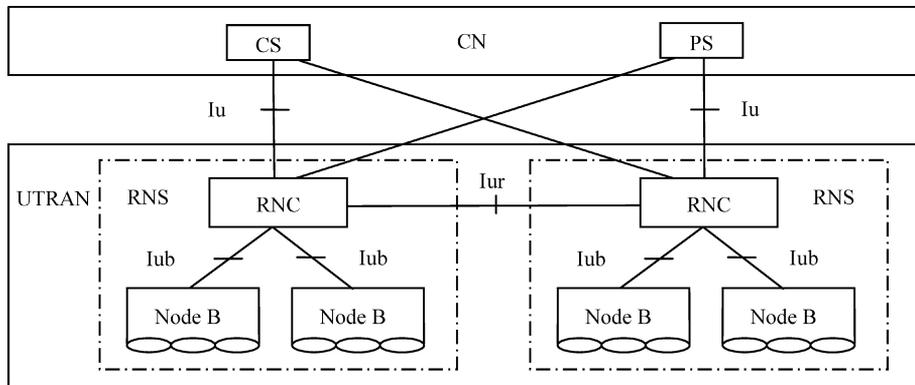


图 5-4 UTRAN 的结构

(3) CN 负责处理 WCDMA 系统内语音呼叫和数据连接,并实现与外部网络的交换和路由功能。

CN 从逻辑上分为电路交换(CS)域和分组交换(PS)域两部分,CS 主要负责语音等业务的传输与交换,而 PS 主要负责非语音类数据业务的传输与交换。

无线接入网与 UE 的接口为 Uu 接口,与核心网的接口是 Iu 接口。用户设备内部,ME

与 USIM 的接口为 Cn 接口；而在无线子系统内部，Node B 与 RNC 间的接口为 Iub 接口，RNC 之间的接口为 Iur 接口。

UTRAN 各个接口的协议结构是按照一个通用的协议模型来设计的，如图 5-5 所示，设计的原则是层间和平面间在逻辑上相互独立。

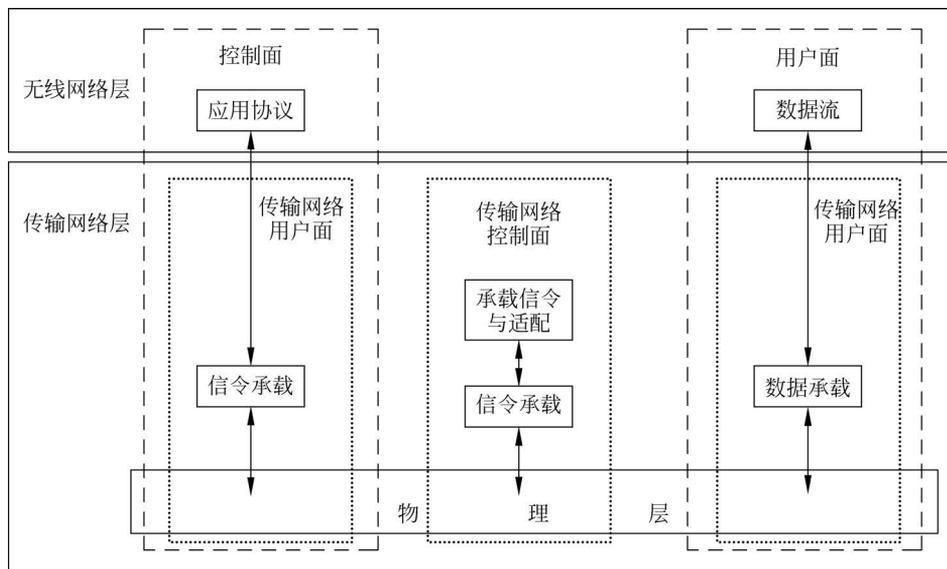


图 5-5 UTRAN 接口通用协议结构

从水平层面来看，协议结构主要包括两层，即无线网络层和传输网络层。所有 UTRAN 的相关问题只与无线网络层有关，传输网络层只是 UTRAN 采用的标准化的传输技术，与 UTRAN 特定功能无关。

从垂直平面来看，协议结构包括控制面、用户面、传输网络控制面和传输网络用户面，其中，控制面包括无线网络层的应用协议以及用于传输应用协议消息的信令承载；用户面包括数据流和用于传输数据流的数据承载；传输网络控制面在控制面和用户面之间，只在传输网络层上，它不包括任何无线网络层的信息；传输网络用户面提供用户面的数据承载和应用协议的数据承载。

## 5.2.2 WCDMA 的空中接口

WCDMA 的空中接口是 Uu 接口，它是系统最重要的开放接口，也是 WCDMA 技术的关键所在。Uu 接口协议层分为物理层、数据链路层和网络层。空中接口使用无线传输技术将用户设备接入系统固定网络部分，用来建立、重新配置和释放无线承载业务。

WCDMA 空中接口的整体逻辑协议结构如图 5-6 所示，它分为控制面 and 用户面，控制面由物理层、媒体接入控制(MAC)层、无线链路控制(RLC)层和无线资源控制(RRC)层等子层组成，在用户面的 RLC 子层之上有分组数据汇聚协议(PDCP)和广播/组播控制协议(BMC)。

### 1. 无线信道及功能

WCDMA 空中接口上有物理信道、传输信道和逻辑信道 3 种信道。物理层通过传输信



道向上层提供各种数据传输业务,而传输数据的类型与特征决定了传输信道的特征;MAC层通过逻辑信道向RLC层提供业务,逻辑信道的特征是由发送数据的类型来决定的。物理信道的属性由物理层来定义。3种信道之间的对应关系如图5-7所示。

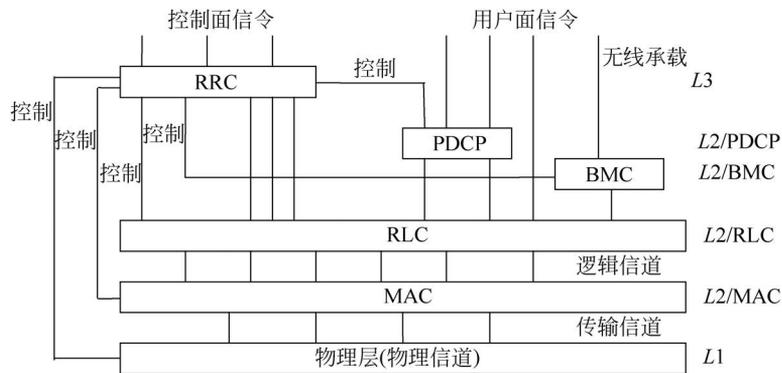


图 5-6 WCDMA 空中接口的整体逻辑协议结构

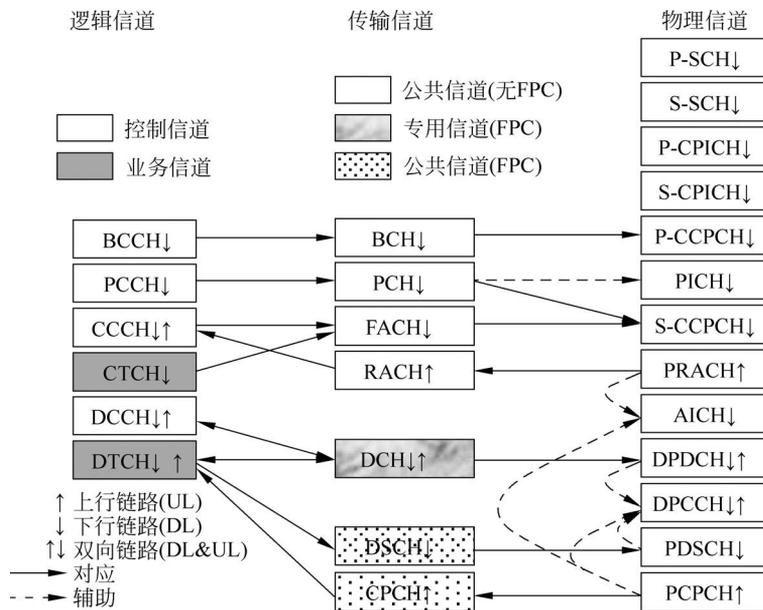


图 5-7 WCDMA 空中接口信道的对应关系

### 1) 逻辑信道

信息可以开始于协议堆栈的顶层,以逻辑信道的形式从RLC层传输到MAC层。MAC层在逻辑信道上提供数据传输业务,直接承载用户业务,逻辑信道类型集合根据MAC层提供的数据传输业务类型进行定义。根据承载的是控制面业务还是用户面业务,逻辑信道通常可以分成两类,控制信道和业务信道,控制信道用来传输控制面信息;业务信道用来传输用户面信息。

控制信道包含下列信道。

- (1) BCCH——广播控制信道(DL),用于在下行链路上广播系统的控制信息。
- (2) PCCH——寻呼控制信道(DL),用于在下行链路上发送寻呼信息。

(3) CCCH——公共控制信道(DL&UL),用于在网络和 UE 间发送控制信息(通常在 UE 没有与网络间建立 RRC 连接和重选后,UE 要接入新小区时使用)。

(4) DCCH——专用控制信道(DL&UL),用于传送专用控制信息的点对点的双向链路。

业务信道包含以下信道。

① DTCH——专用业务信道(DL&UL),针对一个 UE 点对点地进行用户信息的传送。

② CTCH——公共业务信道(DL),用于将特定的用户信息传送到全部或一组 UE 的对多点单向信道。

### 2) 传输信道

传输信道根据传输的是针对一个用户的专用信息还是针对所有用户的公共信息而分为专用信道和公共信道两大类,它们之间的主要区别在于公共信道资源可由小区内的所有用户或一组用户共同分配使用,而专用信道资源仅仅是为单个用户预留的,并采用特定频率的特定编码加以识别。

专用信道只有一种,即 DCH——专用传输信道(DL&UL),支持可变速率和多种业务,传送高层的所有用户信息,包括数据、即时业务和控制信息。对应于物理层的 DPDCH,它具有闭环功控、帧间快速速率改变、部分扇区发射和软切换等功能。

目前已定义的公共传输信道有 6 种,与 2G 不同的是,可以在公共信道和下行链路共享信道中传输分组数据;同时,公共信道不支持软切换,但一部分公共信道可以支持快速功率控制(FPC)。公共信道有以下几种。

(1) BCH——广播信道(DL),发送广播信息的控制信道。

(2) PCH——寻呼信道(DL),发送寻呼信息的控制信道。

(3) FACH——前向接入信道(DL),通过该下行控制信道,网络告知终端该选择哪个小区,并且可以用来传送少量的分组数据。

(4) DSCH——下行共享信道(DL),用于传送用户的数据和控制信息,可由多个用户同时共享。

(5) RACH——随机接入信道(UL),传送上行的控制信息,如建立 RRC 的请求等,也可以用来传送少量的分组数据信息。

(6) CPCH——公共分组信道,传送分组格式的用户数据,支持上行链路内环功控。

用于基本网络运营的公共传输信道有 RACH、FACH 和 PCH,而 DSCH 和 CPCH 是可选的,使用情况由网络决定。

### 3) 物理信道

物理信道是各种信息在无线接口传输时的最终体现形式,是物理层的承载信道。每一种使用特定的载波频率、码(扩频码和扰码)以及载波相对相位(0 或  $\pi/2$ ,只用于上行链路)的信道都可以理解为一类特定的信道。物理信道包含以下信道:

(1) DPCH——物理专用信道,对于下行链路又分为物理专用数据信道(DPDCH)和物理专用控制信道(DPCCH),提供可变速率业务承载信道,是主要的数据承载信道。对上行链路,为避免业务数据静默时出现纯控制信息形成的低频脉冲干扰,DPDCH 和 DPCCH 通过正交调制复用在一条信道;对下行链路,由于业务数据本身就是多用户时分复用,所以不存在以上问题,控制信息和数据信息也以时分的方式共用一条信道。

(2) CPICH——公共导频信道(DL),有主导频信道和辅助导频信道两种,用于区分扇区;在使用 DPCH 时,如果 CPICH 不能提供信道参考,则需要使用第二导频信道(或是使用 DPCH 中的导频位)以提供进一步的参考。

(3) CCPCH——公共控制信道(DL),有主控制信道和辅助控制信道两种;主控制信道与 BCH 对应,用于传送广播信息;辅助控制信道承载 FACH 和 PCH,完成接入控制(与 PRACH 一起)和寻呼。

(4) PDSCH——下行物理共享信道(DL),与传输层的 DSCH 信道对应,主要传送非实时的突发业务,可以通过正交码由多个用户共享;相对于 DPCH,PDSCH 没有软切换,所以对覆盖不太有利,但是可以解决码资源不足的问题。

(5) PICH——寻呼指示信道(DL),与 CCPCH 中包含的 PCH 一起,进行寻呼的控制,告诉终端是否该解调 CCPCH 信道,以了解寻呼信息。

(6) AICH——分配指示信道(DL),与上行链路的 PRACH 一起,完成终端的接入过程;在 Node B 收到并正确解调出上行 PRACH 中发送的探针 Preamble 后,回应相关指示信息。

(7) SCH——同步信道(DL),用于小区搜索过程同步,包括主同步信道、辅同步信道,分别用于小区同步和帧同步。

(8) PRACH——物理随机接入信道(UL),对应于传输层的 RACH,用于终端的接入。

(9) PCPCH——物理公共分组信道(UL),与 PDSCH 类似,作为数据传送的补充。相对于 DPCH,同样缺少软切换,但是接入时间短,而且可由多个用户共用,所以主要用于突发的数据,较长的数据仍由 DPCH 传送。

## 2. 物理层

物理层主要完成以下功能:在传输信道上进行前向纠错的编译码,对高层进行测量和指示,宏分集分解和合并,软切换,传输信道上纠错,传输信道复用和编码组合传输信道(CCTrCH)分离,速率匹配,将 CCTrCH 映射到物理信道上,频率和时间同步,闭环功率控制,物理信道的功率加权与组合,射频处理,波束赋形等。

### 1) 物理信道的帧结构

一般的物理信道包括 3 层结构:超帧、帧和时隙。超帧长度为 720ms,包括 72 个帧;每帧长为 10ms,对应的码片(chip)数为 38 400;每帧由 15 个时隙组成,一个时隙的长度为 2560chip。由于采用了正交可变扩频因子(OVSF)的扩频方式,每时隙中的传输位数取决于扩频因子的大小。

在每个无线链路(物理链接)的上行物理信道中,可能有 0、1 和若干上行 DPDCH,只有一个上行 DPCH,DPDCH 和 DPCH 通过并行码分复用的方式进行传输,它们的帧结构如图 5-8 所示。上行 DPDCH 承载第二层或更高层生成的专用数据,可提供逐帧改变速率的变速率服务;上行 DPCH 传送的物理层控制信息包括导频位、发送功率控制(TPC)命令、反馈信息(FBI)、可选的传输格式组合指示(TFCI)等。图 5-8 中参数  $k$  决定了上行 DPDCH 中每时隙的位数,它对应于物理信道的扩频因子  $SF=256/2^k$ 。 $k=0, \dots, 6$ ,对应的扩频因子为 256 到 4,对应的信道位速率为 15~960Kb/s;上行 DPCH 的扩频因子固定为 256,因此它每时隙传送 10 位的控制信息,其中的导频位决定使用的导频图案集,TFCI 用于指示当前帧中 DPDCH 的消息格式,FBI 用于支持 UE 与基站之间的反馈技术,TPC 用于

控制下行链路的发射功率。

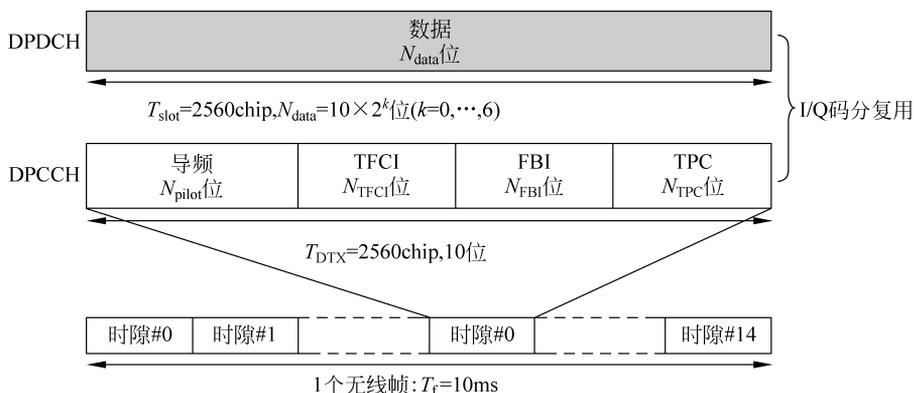


图 5-8 上行专用物理信道的帧结构

图 5-9 给出了下行专用物理信道的帧结构,可以看出,下行专用数据和控制信息在一个时隙内是时间复用传输的,参数  $k$  确定一个时隙内 DPCCH 和 DPDCH 的总位数。同样地,扩频因子  $SF = 512/2^k$ ,其范围由 512 到 4。在一个时隙内,需要确定表明不同域内位数的参数  $N_{pilot}$ 、 $N_{TPC}$ 、 $N_{TFCI}$  和  $N_{data}$ 。当在一个下行链路连接上传输的总的位速率超过一个下行物理信道最大位速率时,可采用多码传输,即一个或几个传输信道的信息经编码复接后,组成的 CCTrCH 可使用几个并行的扩频因子相同的下行 DPCH 进行传输。此时,为了降低干扰,物理层的控制信息仅放在第一个下行 DPCH 的 DPCCH 上,其他 DPCH 上不传输控制信息,即在 DPCCH 的传输时间不发送任何信息,也就是采用了不连续发射。多码传输也可用于采用不同码的不同传输信道上,在这种情况下,不同并行码可采用不同扩频因子,并且物理层控制信息在每一个信道上要独立传送。

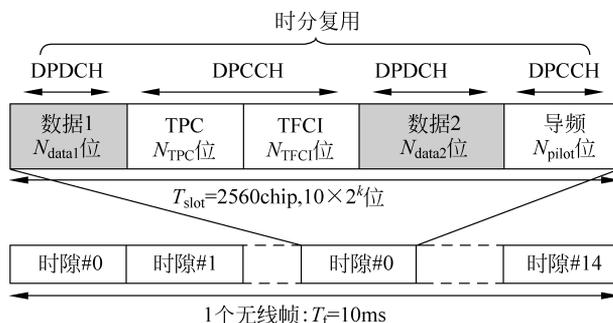


图 5-9 下行专用物理信道的帧结构

其他物理信道在时间上也基本上采用了三层式结构,但其帧结构和专用物理信道的帧结构不同,具体情况请参阅其他图书。

## 2) 扩频、扰码与调制

WCDMA 上行链路的扩频、扰码与调制的实施过程如图 5-10 所示,可以看出,上行 DPDCH 和 DPCCH 如前所述通过并行码分复用的方式进行传输。图中示意的是多数情况,一个连接配置一个 DPDCH,在各种业务联合交织并共享相同的 DPDCH 中,也可能分配多个 DPDCH。当使用多码传输时,几个(最多 6 个)并行的 DPDCH 用不同的信道编码

来传送,而每个连接只有一个 DPCH。上行物理信道先经信道码  $C_d$  或  $C_c$  扩频,扩频后速率达到码片速率,再分别调制到两个正交支路  $I$  和  $Q$  上,实现双信道 QPSK 调制,中间还要经过复数扰码。

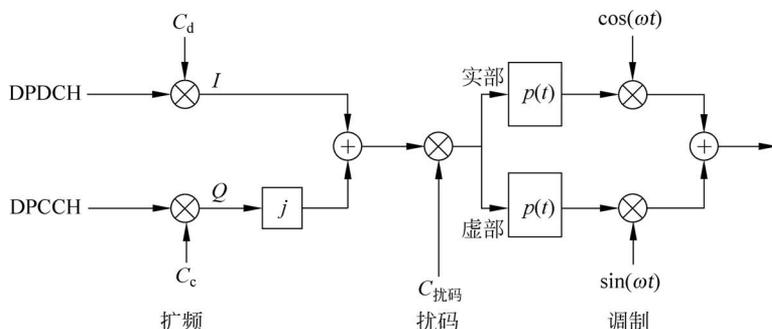


图 5-10 WCDMA 上行链路的扩频、扰码与调制的实施过程

在以上扩频过程,信道码用的是 OVFSF 码,它的作用是保证所有用户在不同物理信道之间的正交性。与 CDMA 2000 相同,OVFSF 码采用的是变长的 Walsh 码,它组成了树状结构的序列集合,如图 5-11 所示。可以验证,该树状结构中非衍生节点之间具有正交性。通常,处理高速数据业务,需要占用靠顶端的 OVFSF 码,此时,引起该节点下端的 OVFSF 码就不能再用,因此需要对码资源的分配和使用进行有效的管理。

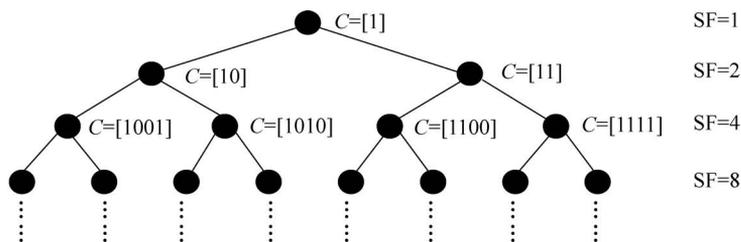


图 5-11 OVFSF 码树状结构的序列集合

WCDMA 中的扰码在下行中用于区分基站,而在上行中用于区分用户。上行链路的扰码可以选择长扰码和短扰码(应用多用户检测技术时采用短扰码),长码选用 Gold 序列,短码选用复数四相序列  $S(2)$ 。所有上行物理信道都采用同一复扰码序列进行扰码操作。上行长扰码(数量为  $2^{24}$  个)的实部和虚部所使用的基础序列  $C_1$  和  $C_2$  分别来自一个 25 阶的 Gold 序列, $C_1$  取 Gold 序列的前 38400 位(10ms,相当于一个无线帧), $C_2$  由  $C_1$  相移 16777232 码片后截取 38400 个码片得到。上行复数长扰码  $C_{扰码}$  按如下方式来定义。

设  $z$  为 25 阶的二进制 Gold 序列,并令

$$Z(i) = \begin{cases} +1, & z(i) = 0 \\ -1, & z(i) = 1 \end{cases} \quad i = 0, 1, \dots, 2^{25} - 2 \quad (5-1)$$

则有

$$C_1(i) = Z(i), \quad i = 0, 1, \dots, 2^{25} - 2 \quad (5-2)$$

$$C_2(i) = Z((i + 16\,777\,232) \bmod (2^{25} - 1)), \quad i = 0, 1, \dots, 2^{25} - 2 \quad (5-3)$$

$$C_{扰码}(i) = C_1(i)(1 + j(-1)^i C_2(2 \lfloor i/2 \rfloor)), \quad i = 0, 1, \dots, 2^{25} - 2 \quad (5-4)$$

其中,  $\lfloor \cdot \rfloor$  表示向下取整。

上行短扰码与上行长扰码相似,也是复数序列,且是由 3 个实数序列模 4 相加得到,但是在实现细节上有所不同。短码长度为 256 个码片。

WCDMA 下行链路的扩频、扰码与调制的实施过程如图 5-12 所示,扩频用的信道码同上行相同,为 OVSF 码。基本 CPICH 使用  $C_{256,0}$ ,PCCPCH 使用  $C_{256,1}$ ,其余信道的扩频码由网络决定。扰码使用长扰码,它是由 18 阶的 Gold 码为基础形成的复数扰码序列,具体形成方式同上行长扰码的方式近似,但只选用了其中的 8192 个,分成 512 个集合,每个集合包括 1 个主扰码和 15 个辅扰码,每个小区对应 512 个扰码集中的一个,512 个主扰码又分成 64 组,每组 8 个主扰码。对于同小区下行链路的不同信道,一般只使用一个扰码,即主扰码;辅扰码只对采用了波束定向的专用信道使用。下行扰码长度为 38400 个码片。下行链路的调制方式采用的是常规的平衡 QPSK 调制。

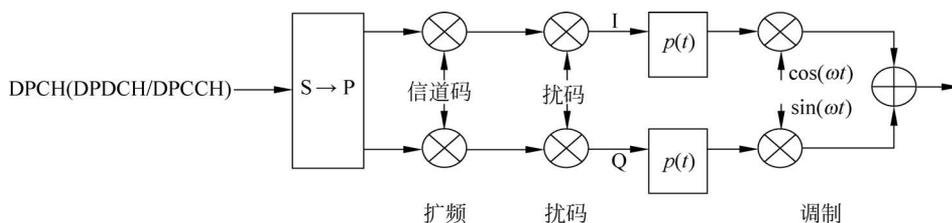


图 5-12 WCDMA 下行链路的扩频、扰码与调制的实施过程

### 3) 信道编码与复用

为实现一个连接上并行传送多业务,传输信道上的数据需要经过信道编码与复用处理才能映射到物理信道上。WCDMA 的上下行链路的信道编码与复用过程分别如图 5-13 和图 5-14 所示。其基本的过程包括:添加 CRC 校验比特、传输块(TrBk)级联和码组分段、信道编码、第一交织、无线帧分段、速率匹配、传输信道(TrCH)复接、物理信道分段、第二交织和物理信道映射等。在下行信道中还需插入不连续发送(DTX)比特。

物理层的信道编码包括检错编码、纠错编码、速率匹配和交织。CRC 为 24 位、16 位、12 位、8 位或 0 位。纠错编码可选的方案包括卷积编码(编码速率通常为 1/2 或 1/3)、Turbo 码(由于其译码的延时较长,通常用于高质量的高速率数据业务中)和不编码 3 种。速率匹配的的目的是使复用传输信道的信息速率与上行或下行物理信道的几个有限的速率相匹配。速率匹配分为两类:静态速率匹配和动态速率匹配。静态速率匹配在纠错编码后的码序列进行,可随时从一个连接中增加或去除一个传输信道业务;动态速率匹配是按帧进行的,它采用非均匀重复方式完成,且仅用于上行。在下行,处理复用后总瞬时速率与信道速率不匹配的方法是采用 DTX 方式。交织采用内外两次交织的形式。

### 4) 物理层的主要相关进程

WCDMA 的物理层包含了很多系统运作的关键进程,这些进程在 3GPP 的 TS25.214 物理层协议中都有所规范。下面介绍物理层的几个主要相关进程。

(1) 小区搜索与同步进程。WCDMA 支持基站间的异步操作,其终端与小区的同步主要借助下行链路的主、辅同步信道完成(主、辅同步信道都不进行扰码,在每个时隙中,两信道并行发送),同时获取目标小区的扰码信息,完成小区搜索。小区搜索(即同步)进程分为 3 个步骤。

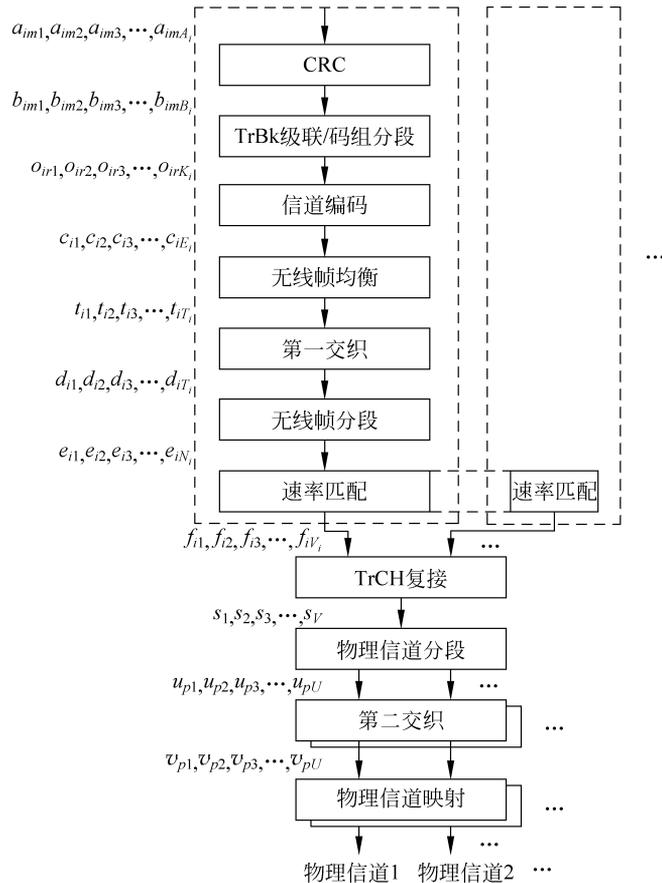


图 5-13 WCDMA 上行链路的信道编码与复用过程

第一步是时隙同步。由于主同步信道所在小区采用的是同一个 256 位码,而且在各时隙中的同一个位置重复发射。终端在接收到后,采用相关滤波器去匹配主同步信道,再检测滤波器输出的峰值,就可以获得各时隙的边界,实现时隙同步。

第二步是帧同步和扰码组的识别。在得到时隙的边界后,通过对比的方法,终端进一步识别辅同步信道中 256 位码组成的 15 种不同形状(检测最大相关值)及其在同一帧中不同时隙的位置,就可以确定小区的扰码组。由于同一小区每一帧中 15 个时隙的辅同步的码序列顺序是不变的,所以确定码的形状后,同时也就了解到了时隙的顺序,实现了帧同步。

第三步是扰码识别。由于每个扰码组中有 8 个扰码,在实现帧同步后,终端经过对扰码组内可能的 8 个主扰码与 P-CPICH 信道中实际采用的扰码逐个进行试探比较,可以找到匹配的主扰码。

(2) 功率控制进程。3GPP 按信道的种类、实际的进程定义了非常复杂、详细的功率控制模式。功率控制的方式有开环功控、内环功控(在 WCDMA 中称为快速闭环功控)和外环功控(在 WCDMA 中称为慢速功控)。

开环功控只用于 RACH 或 CPCH 传输的初始化过程。开环功控的精度一般在  $\pm 9\text{dB}$  之内,如在正常连接时使用开环功控会对链路质量带来影响,因此在正常连接模式下,WCDMA 系统不采用快速功控。

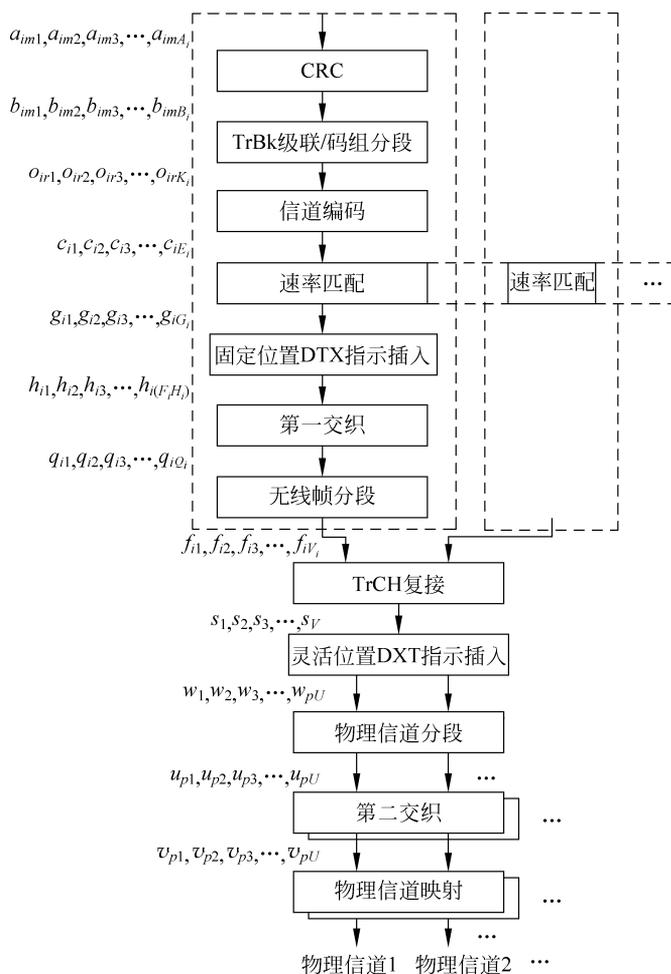


图 5-14 WCDMA 下行链路的信道编码与复用过程

内环功控通过快速调整发射功率使接收信号的 SIR 稳定在预设的目标值  $SIR_{target}$  上。每时隙派发一个功控指令，指令速度为 1500Hz，基本步长为 1dB(可选用 2dB)，对应的精度为  $\pm 0.5$ dB。内环功控要考虑软切换状态和压缩模式两种特殊情况下的功率控制方法。

外环功控为内环功控提供达到某一质量要求所需的目标 SIR 值。对于不同的业务速率、终端移动速度和无线环境，达到某一个 QoS 对 SIR 的要求也不同，所以内环的  $SIR_{target}$  需要根据业务速率和无线环境的变化在外环功控过程中来确定。外环功控速度为 10~100Hz。

(3) 下行链路发送分集进程。WCDMA 在下行链路使用开环和闭环两种类型的发送分集方式来提高数据的传输性能，在使用闭环发送分集时，基站使用两根天线来发送用户数据，这两根天线的工作状态根据 UE 在上行 DPCH 中反馈的 FBI 位来进行调整，闭环发送分集本身有两种工作模式：在模式 1 中，根据来自 UE 的反馈命令控制天线的相位，使 UE 接收功率最大；在模式 2 中，不仅要调整天线相位，还要调整天线幅度。闭环模式只在专用信道或伴随 DSCH 的专用信道中采用，而开环模式没有信道类型的限制。

(4) 切换控制进程。物理层中与切换有关的主要工作是：依据切换的种类(软切换、制式内硬切换和制式间硬切换)，配合支持相应的测量，解决测量方法和提出测量报告。软切

换时,可以在连接状态下,利用 ME 的多个 RAKE 接收机对同频的其他小区进行测量,但需要定时的支持;同频的硬切换测量与软切换测量方法相同,不同频或不同系统的硬切换的测量一般需要压缩模式的支持,产生发送和接收的间断,在其时隙内完成对其他频率和制式的测量。

### 3. 数据链路层

WCDMA 空中接口的数据链路层可分为若干子层,在控制面上,数据链路层包含 MAC 和 RLC 两个子层;在用户面上,除了 MAC 和 RLC 之外,还存在两个与特定业务有关的协议,即 PDCP 和 BMC。

#### 1) MAC 层

MAC 层的逻辑结构如图 5-15 所示,它包括 3 个逻辑实体:MAC-b、MAC-c/sh 和 MAC-d,用于逻辑信道到传输信道的映射,其中,MAC-b 负责广播信道的处理,MAC-c/sh 负责公共信道和共享信道的处理,MAC-d 负责在连接模式下处理分配给 UE 的专用信道。

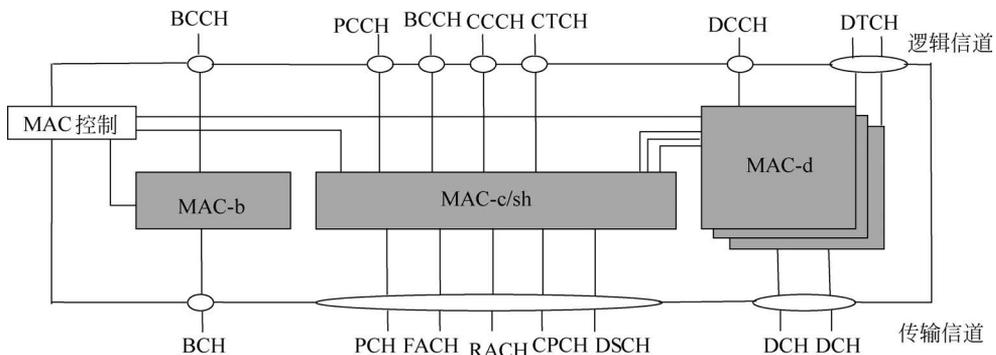


图 5-15 MAC 层的逻辑结构

MAC 层的功能包括:①逻辑信道和传输信道之间的映射;②根据瞬时源速率为每个传输信道选择合适的传输格式(TF);③对一个 UE 的数据流,通过选择“高速率”和“低速率”传输格式实现优先级调度;④在不同 UE 间进行优先调度;⑤在上层的传输块和公共或者专用传输信道之间进行复用和解复用;⑥进行业务流量监测,MAC 层将对应于一条传输信道的数据量与 RRC 设置的门限相比较,如果数据量太高或太低,MAC 层就发送一个关于业务量状态的测量报告给 RRC 层,RRC 层使用这些报告来引发对无线承载和传输信道参数的重新分配;⑦实现传输信道类型的转换,在来自 RRC 层的命令下,MAC 层执行公共传输信道和专用传输信道之间的切换;⑧实施加密,如果无线承载使用透明 RLC 模式,加密就在 MAC 层的子层(MAC-d 实体)进行;⑨在 RACH 发射时进行接入业务级别选择。

#### 2) RLC 层

RLC 层的结构如图 5-16 所示,它共有 3 种 RLC 实体类型,即透明模式(Tr)、确认模式(AM)和非确认模式(UM)。RLC 实体和它的服务接入点(SAP)相关联。需要说明的是,在透明模式和非确认模式下,RLC 实体都被定义成单向的,而确认模式的实体是双向的。

(1) 透明模式。不给高层区域增加任何开销,高层数据可以不进行分段而以数据流的形式发送,而错误的协议数据单元(PDU)可能被丢弃或者作错误标记。

(2) 非确认模式。不使用重传协议,传送的数据没有保护,接收到的错误数据根据配置被丢弃或者作标记。它用于小区广播业务和 VoIP(基于 IP 的语音通信)业务。

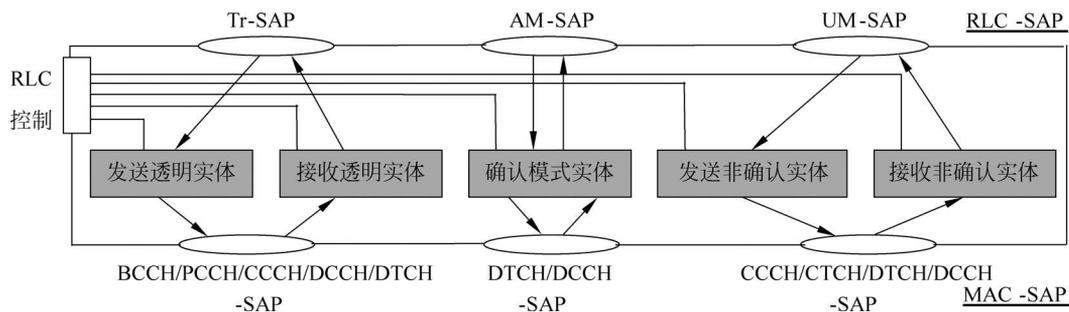


图 5-16 RLC 层的结构

(3) 确认模式。使用自动重传请求(ARQ)方案纠错,RLC 的质量及与其对应的延迟性能可由 RRC 控制。

RLC 层的功能和链路连接质量有很大的关系,其功能包括:①分段与重组,将不同长度的高层 PDU 进行分段与重组为较小的 RLC 负荷单元(PU),一个 RLC PDU 承载一个 PU,RLC PDU 的大小是按照使用 RLC 实体的业务可能的最小位速率设置的;②级联,若一个 RLC SDU(RLC 业务数据单元)的内容不能填满整数个 RLC PU,下一个 RLC SDU 的第一段可以放在该 RLC PU 中与前一个 RLC SDU 的最后一段级联在一起;③填充,当级联不适用并且剩余需要发送的数据不能填满一个给定大小的完整的 RLC PDU 时,数据域的剩余部分将用填充位填满;④数据传输,RLC 支持确认、非确认和透明模式数据传输,QoS 设置控制用户数据的传输;⑤错误检测,该功能在确认数据传输模式中通过自动重传请求提供纠错;⑥高层 PDU 的接序发送,该功能保持高层 PDU 的顺序,该顺序是 RLC 使用确认数据传输业务递交的传输顺序;⑦重复检测,检测收到 RLC PDU 备份,并保证合成的高层 PDU 只向上层发送一次;⑧流量控制,允许 RLC 接收端控制对等 RLC 发送实体发送信息的速率;⑨序列号检测,通过提供的一个检测恶化的 RLC SDU 的方法检查 RLC PDU 中序列号,恶化的 RLC SDU 将被丢弃,从而保证重组 PDU 的完整性;⑩协议错误检测和恢复,在 RLC 协议操作中检测错误并进行恢复;⑪加密,在 RLC 层中确认和非确认模式下进行加密;⑫数据传输的暂停和恢复,在安全模式控制过程需要传输暂停,因此对等实体就总是使用相同的密钥,暂停和继续都是由 RRC 通过控制接口命令实现的。

### 3) PDCP 层

PDCP 层只存在于用户面,并且只处理 PS 域业务。为了在无线上传输 IP 分组业务并获得更好的频谱效率,PDCP 包含了压缩方法。每个 PDCP 实体使用 0、1 或者多个报头压缩算法类型和可配置参数集合。算法类型和它们的参数在 RRC 无线承载建立和重新配置过程中被协商并且通过 PDCP 控制 SAP 指示给 PDCP。PDCP 负责 PDU 从一种网络协议到一种 RLC 实体间的映射,它支持透明模式和非透明模式(包括确认模式和非确认模式)的传输。在透明模式下,PDCP 没有改变数据单元,意味着没有增加报头,也无压缩功能,此时 PDCP 的功能有:用户数据的传输、PDCP 缓冲区的重新分配和 PDCP SDU 的缓存;在非透明模式下,则可能增加了报头并且执行了报头适配,此时 PDCP 的功能有:报头适配、用户数据传输、PDCP 缓冲区重新分配和 PDCP SDU 缓存、IP 数据流的适配。

### 4) BMC 层

BMC 层也只存在于用户面,服务于无线接口上的广播/组播业务(产生于广播域上)。

其功能有：①储存小区广播消息；②为小区广播业务(CBS)的业务监测和无线资源进行请求；③BMC消息的调度；④向 UE(终端)发送 BMC 消息；⑤向上层传送小区广播消息。

#### 4. 网络层

RRC 层协议是 WCDMA 无线接口中网络层协议的核心规范,其中包括 UE 和 UTRAN(UMTS 陆地无线接入网)之间传递的几乎所有的控制信令以及 UE 在各种状态下无线资源的使用情况、测量任务和执行的操作。

下层的一些测量报告可以为 RRC 分配无线资源提供参考,控制操作和测量报告将通过 RRC 与低层的接入点进行交互。RRC 与低层的交互动作如图 5-17 所示。

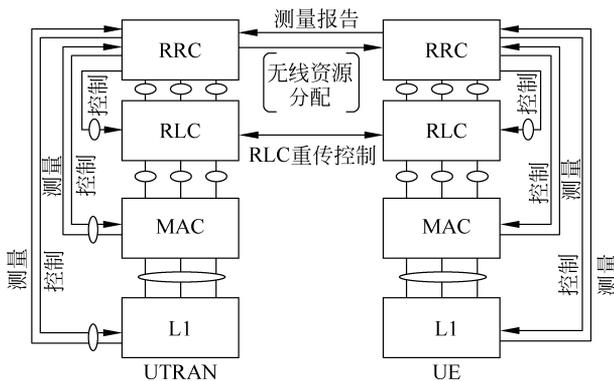


图 5-17 RRC 与低层的交互动作

RRC 层向上层提供信令连接以支持与上层之间的信息交流,信令连接可在 UE 和核心网之间传输高层信息。对每个核心网域,最多只能同时存在一个信令连接;对于一个 UE,同时最多也只能存在一个 RRC 连接。

UE 的两个基本的操作模式是空闲模式和连接模式。连接模式可以进一步分成不同的 RRC 业务状态:URA-PCH 状态、CELL-DCH 状态、CELL-PCH 状态和 CELL-FACH 状态,这些状态定义了 UE 使用的物理信道的种类。UE 可以在空闲模式和连接模式之间转移,也可以在连接模式的各个状态之间转移。

RRC 层的结构如图 5-18 所示,它可以用以下 4 个功能实体来描述。

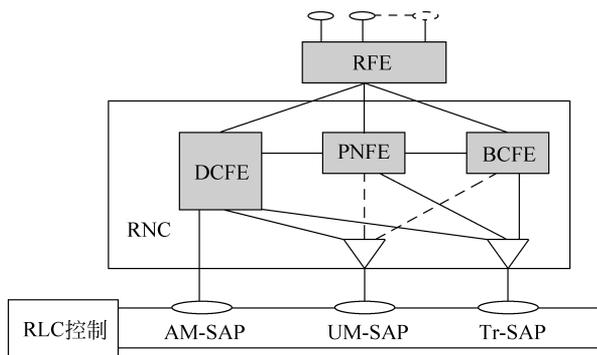


图 5-18 RRC 层的结构

- (1) 专用控制功能实体(DCFE)处理一个特定 UE 的所有功能和信令。
- (2) 寻呼及通告功能实体(PNFE)处理空闲模式中的 UE 的寻呼。

(3) 广播控制功能实体(BCFE)处理系统信息广播功能。

(4) 路由功能实体(RFE)处理不同 MM/CM 实体(UE 侧)或者不同的核心网域(UTRAN 侧)的高层消息的路由选择。

RRC 层的功能包括: ①广播对应非接入层和接入层的系统信息; ②寻呼; ③空闲模式下初始小区的选取和重选; ④RRC 连接的建立、维护和释放; ⑤无线承载、传输信道和物理信道的控制; ⑥安全功能控制; ⑦信令完整性保护; ⑧UE 测量报告和控制; ⑨RRC 连接移动性管理; ⑩SRNC(服务 RNC)重定位的支持; ⑪对下行链路外环功控的支持; ⑫对开环功控的支持; ⑬小区广播业务相应的功能; ⑭UE 定位相应的功能。

### 5.2.3 WCDMA 核心网的演进

3GPP 已制定了 R99、R4、R5、R6、R7、R8、R9、R10、R11、R12、R13 等多个核心网(CN)网络结构的版本,自 R5 进入了 HSPA(高速分组接入)阶段,为 WCDMA 的提高版; R8 对应 LTE(长期演进计划),为准 4G 版; R10 对应 LTE-Advanced(LTE 演进版),即 4G 版。

#### 1. R99 网络结构

R99(又称为 R3)是 WCDMA 的第一个版本,因此它的网络设计考虑了 2G、3G 的兼容问题,支持 GSM→GPRS/EDGE→WCDMA 的平滑过渡,其网络结构如图 5-19 所示。

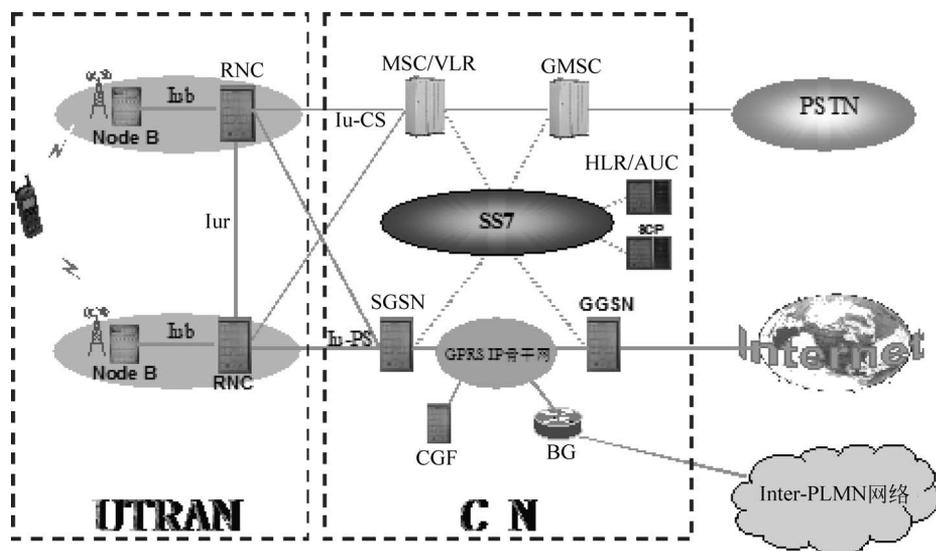


图 5-19 R99 网络结构

总体来说,R99 采用了基于 GSM/GPRS 的核心网络,无线接入则引入了新的 WCDMA 接入网(即 UTRAN)。在无线接入部分,除了支持新引入的 UTRAN 的 RNS 之外,也支持 GSM/GPRS 的 BSS(在图 5-19 中未画出)。

在 R99 的核心网络中,CS 域和 PS 域是并列的,CS 域的功能实体包括 MSC、VLR、GMSC(移动交换中心网关)和 IWF(互通功能)等;PS 域特有的功能实体包括 SGSN(GPRS 服务支持节点)、GGSN(GPRS 网关支持节点)、BG(边界网关)和 CGF(收费网关功能)等;而 HLR、AUC、SCP(智能网业务控制点)和 EIR 等为 CS 域和 PS 域共用设备。R99 的 CS 域是基于 TDM 技术的,并仍采用分级组网模式,通过 GMSC 和外部网络相连;PS 域

基于 IP 组网,通过 GGSN 接入外部分组网络。核心网与接入网之间的 Iu 接口采用 ATM 技术来传输,核心网可以和智能网相连,定义了 CAMEL3(移动网络增强逻辑的客户化应用 3)规范,以增强对智能业务的支持。

## 2. R4 网络结构

继 R99 之后,3GPP 又推出了 R4,其 PLMN 基本网络结构如图 5-20 所示。在无线接入技术方面,R4 只是提出一些改进,以增进系统性能,但把 TD-SCDMA 技术列入了补充的无线接入标准。

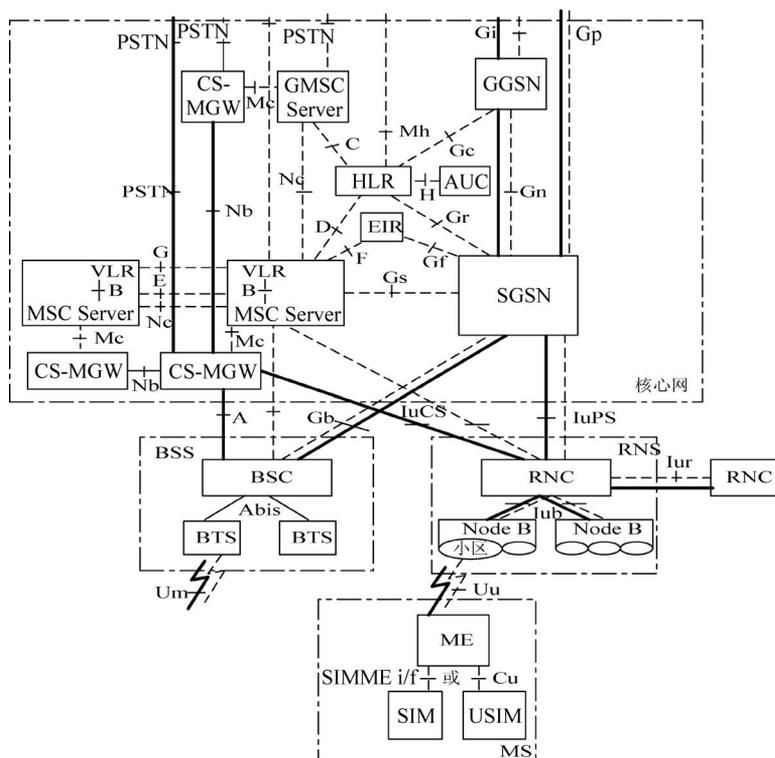


图 5-20 R4 的 PLMN 基本网络结构

在核心网方面,R4 的 PS 域与 R99 相比变化不大,主要是增加了部分与 QoS 相关的协议标准。但 R4 的 CS 域变化比较大,主要是采用了承载与控制相分离的软交换思想,有利于运营商降低建网和运营的成本。在 CS 域的功能实体中,(G)MSC 被两个独立的功能实体(G)MAC Server(MSC 服务器)和 MGW(媒体网关)替代,(G)MSC Server 完成呼叫控制和移动管理功能,MGW 提供承载信道;HLR 也可以替换为 HSS(归属用户服务器);SG(信令网关)是新增加的网络实体,用于完成基于 IP 的 7 号信令和基于 TDM 的 7 号信令之间的消息格式转换。R4 的 CS 域中的网络实体间可以采用 TDM/ATM/IP 技术组网,这样,运营商有多种选择,如果采用 IP 组网,可以组建结构更为简化的信令网和平面化的承载网。

## 3. R5 网络结构

R5 版本的网络结构的目标是构造全 IP 移动网络,在研究过程中分化为 R5、R6 两个版本。R5 主要定义了全 IP 网络的架构,R6 的重点集中于业务增强以及与其他网络的互通方面。R5 的具体网络结构如图 5-21 所示。



全、计费等其他功能增强。

R7 版本主要继续 R6 未完成的标准和业务制定工作,如多天线技术,包括 MIMO 技术的实现。将考虑支持通过 CS 域承载 IMS 语音、通过 PS/IMS 域提供紧急服务、提供基于 WLAN 的 IMS 语音与 GSM 网络的 CS 域的互通、提供 xDSL(数字用户线路)和有线调制器等固定接入方式,同时引入 OFDM,完善 HSDPA 和 HSUPA 标准。

## 5.2.4 WCDMA 的移动性管理

### 1. 概述

WCDMA 的移动性管理是从 GSM/GPRS 的移动性管理演进的,从而具有很多 GSM 基于电路交换的移动性管理特征。但 WCDMA 系统中存在大量分组业务,特别是 WCDMA 的后期版本中,采用了全 IP 架构,因此简单采用传统的 HLR/VLR 为主控制的移动性管理,显然不能满足要求,为此需要引入移动 IP 技术。

传统的移动性管理过程在链路层完成,而移动 IP 技术是基于网络层上的移动管理,因此,WCDMA 系统的移动性管理可以分为基于链路层的移动性管理和基于网络层的移动性管理两个方面。其中基于链路层的移动性管理包括位置管理和会话管理两部分,基于网络层的移动性管理从作用范围来看可以分为宏移动性管理和微移动性管理。

### 2. 基于链路层的移动性管理

#### 1) 位置管理

位置管理是移动性管理的关键。为了有效地进行移动性管理,WCDMA 定义了一些区域。除了在 GSM/GPRS 中已定义的路由区域(RA)和位置区域(LA)外,WCDMA 还定义了 UTRAN 登记区域(URA)和蜂窝区域。RA 是核心网中 PS 域使用的概念,SGSN 使用 RA 来寻呼 UE; LA 是核心网中 CS 域使用的概念; URA 和蜂窝区域只在 UTRAN 中可见。区域之间的关系是严格分层的,LA 属于一个 3G-MSC; RA 属于一个 3G-SGSN; URA 属于 RNC。它们之间的关系如图 5-22 所示。

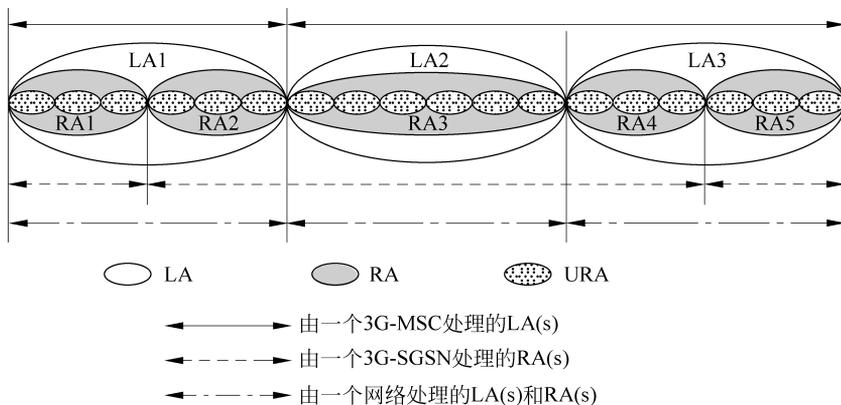


图 5-22 WCDMA 中不同区域之间的关系

LA 包含一个或多个小区。在 CS 域,当 UE 处于 IDLE(空闲)状态时,通过 MM(移动性管理)过程,网络侧可以知道 UE 所在的 LA,LA 主要用于 3G-MSC/VLR 寻呼 UE。RA 包含一个或多个小区,一个 RA 总包含于一个 LA 之中,一个 LA 可以包含多个 RA。在 PS 域,当 UE 处于 IDLE 状态时,通过 MM 过程,网络侧可以知道 UE 所在的 RA。RA 主要用

于 3G-SGSN 寻呼 UE, 当一个 UE 同时注册了 PS 和 CS 业务时, 由于 RA 较小, 在 UE 发起 RA 更新过程的同时可以顺带完成 LA 更新过程, 也可以通过 RA 来为 CS 业务寻呼 UE。

在 UE 和 UTRAN 之间只有一条 RRC 连接, 统一分配用户面和控制面数据传输所需要的所有无线资源。无线资源的控制和管理完全由 UTRAN 实现, 与核心网无关。在 UTRAN 中, RRC 的状态和移动性管理的状态密切相关, RRC 有两种状态: RRC 连接状态和 RRC 空闲状态。RRC 的状态决定了网络层识别 UE 的标识, 处于 RRC 空闲状态时, 通过和 CN 有关的身份(如 IMSI)识别 UE; 处于 RRC 连接状态时, 通过在公共传输信道上分配给 UE 的无线网络临时标识号(RNTI)来识别 UE; 当 UE 被分配了专用传输信道后, 就使用由这些传输信道所提供的内部地址来识别 UE。

处于 RRC 空闲状态时, UTRAN 不为 UE 分配无线资源, UTRAN 中没有关于 UE 的信息, 两者之间无信令交互。此时, UTRAN 不参与 UE 的定位, UE 只能通过监听广播信道判断自己的位置, 在位置更新时向核心网节点(MSC, SGSN 和 GGSN)发送位置更新消息。

处于 RRC 连接状态时, UTRAN 为 UE 分配了无线资源, UTRAN 中存储了关于 UE 的信息。UE 和网络进行移动性管理消息的交互, 核心网知道 UE 的位置(LA/RA 级或小区级)。UTRAN 至少知道 UE 位于哪一个 URA(处于会话连接状态时知道 UE 所处的小区), UTRAN 为 UE 分配一个 RNTI 作为 UE 在传输信道上的标识。在 RRC 连接状态, UE 的位置是由 UTRAN 确定的(UE 可以辅助 UTRAN), UE 无须监听广播信道。UTRAN 通过 RRC 连接通知 UE 所处的位置, 当发生 RA 或 LA 更新时, UTRAN 将通过 RRC 连接通知 UE 向核心网发起 RA 或 LA 更新过程。在该状态下, URA 的更新过程将提供移动性管理功能。

一般来说, 一个 RA 由几个 URA 组成, 但 URA 的具体大小可以由网络管理者定义, 例如可以把 URA 定义得比较小, 这样寻呼的范围可以比较小, 但在一次会话连接结束后的较短时间内 RRC 连接就要被释放。也可以定义 URA 比较大, 这样寻呼范围也比较大, 但 RRC 连接可以在会话连接结束后保持较长的时间。

WCDMA 核心网中每一个业务域(CS 域和 PS 域)都有自己的 MM 状态, MM 的状态主要有 DETACHED(分离态)、IDLE(空闲态)和 CONNECTED(连接态)。WCDMA 的 MM 状态和 GPRS 是类似的, 但具体定义有所不同。

(1) 处于 CS-DETACHED 状态和 PS-DETACHED 状态时, UE 不发送任何位置更新消息, 它的位置对于网络是不可知的。

(2) 处于 CS-IDLE 状态和 PS-IDLE 状态时, UE 和网络之间没有数据传输, UE 此时处于 RRC 空闲状态。UE 通过监听广播信道判断自己的位置, 跨越 RA 或 LA 时要向网络发送位置更新消息(CS 域是 LA 更新消息, PS 域是 RA 更新消息), 即使没有跨越 RA 或 LA, 也要定期发送位置更新消息使网络知道 UE 处于哪一个 RA 或 LA。

(3) 处于 CS-CONNECTED 状态时, UE 和网络之间进行实时业务传输, 在信令信道发送位置更新等移动性管理消息。此时网络精确知道 UE 处于哪一个小区, UE 必然处于 RRC 连接状态。

(4) 处于 PS-CONNECTED 状态时, UE 和网络之间进行数据传输, 或者数据传输的可能性很大, 在信令信道发送位置更新等移动性管理消息, 此时 UE 必然处于 RRC 连接状态。当进行数据传输时, 网络精确知道 UE 处于哪一个小区, 当没有进行数据传输但数据传输的

可能性很大时,网络要知道 UE 所处的 URA。

CS 域和 PS 域的移动性管理可以分开进行,当同时使用 CS 域和 PS 域两种业务时,两个域的移动性管理可以同时进行。例如 UE 发送 RA 更新消息后,由于 RA 小于 LA,不仅 RA 位置信息可以被更新,CS 域的 LA 位置信息也可以被更新。在位置更新过程中,有下面几个重要的特征。

(1) 在 MM 过程中,都要以 IMSI 作为公共用户身份,所有对用户的安全验证都是基于 IMSI 的。

(2) 在 RA 更新过程中,UE 将旧的参数向新的 SGSN 注册,新 SGSN 向旧的 SGSN 发送获取 UE 的 MM 和 PDP(分组数据协议)信息的请求,旧的 SGSN 进行响应。UE、新 SGSN 和 HLR 之间进行安全保密验证,不符合的用户是不能接入网内的。

(3) 在 RNC 和 RA 更新过程中,有一整套的过程来保护 PDU 数据的完整性,并且可以保证在 SGSN 切换时不影响 QoS,其中最为重要的是不影响 Gn 接口的 GTP(GPRS 隧道协议)。而且 PS 域和 CS 域可以通过 Gs 接口进行联合更新过程。

(4) 所有的移动性管理的信息只存在于 WCDMA 核心网内,PS 域更新过程需要 HLR、UE、RNC、SGSN 和 GGSN 的参与。

(5) PS 域内的基于链路层的移动性管理可以切换不同的 UTRAN 和 SGSN,但是访问外部分组数据网的 GGSN 是不会改变的。在 UE 漫游时,这样的移动性并不是分组数据传输的最佳路径。

## 2) 会话管理

会话管理(SM)是移动性管理的重要组成部分,SM 子层主要用于支持用户终端的 PDP 上下文操作,包括 PDP 上下文的激活、修改和去除激活。

PDP 是外部分组数据网与 WCDMA/GPRS 接口所用的网络协议,PDP 上下文是在 UE 和 GGSN 节点中存储的与 SM 有关的信息,该信息可分为两类。

(1) 预定信息,如 IMSI、QoS 层次(预定、请求、协商等)和无线优先权等。

(2) 位置信息,如 NSAPI(网络业务接入点)、LLC-SAPI(逻辑链路控制业务接入点)、GTP 序号、当前 GGSN 地址、PDP 地址和 APN(接入点名)等参数。

这些信息主要是为分组数据在 WCDMA/GPRS 无线接入网和核心网中选择路由时提供路由信息,WCDMA 的 SM 的功能和 GPRS 的 SM 功能基本相同,WCDMA 分别在 UE 侧和网络侧定义了几类 SM 状态,如表 5-3 所示。

表 5-3 WCDMA 定义的 SM 状态

UE 侧 SM 状态		网络侧 SM 状态	
SM 状态名	说 明	SM 状态名	说 明
PDP-INACTIVE	没有 PDP 上下文存在	PDP-INACTIVE	没有 PDP 上下文存在
PDP-ACTIVE-PENDING	UE 正在请求激活 PDP 上下文	PDP-ACTIVE-PENDING	UE 正在请求激活 PDP 上下文
PDP-INACTIVE-PENDING	UE 正在请求去除激活 PDP 上下文	PDP-INACTIVE-PENDING	UE 正在请求去除激活 PDP 上下文
PDP-ACTIVE	已经激活 PDP 上下文	PDP-ACTIVE	已经激活 PDP 上下文
		PDP-MODIFY-PENDING	网络正在请求修改 PDP 上下文

最常用的 SM 过程有 PDP 上下文激活过程、PDP 上下文修改过程和 PDP 上下文去除激活过程。

当一个 UE 附着到 PS 业务时,可自愿建立 PDP 上下文。如果 UE 没有建立 PDP 上下文(SM-Inactive),则没有无线接入载体来建立 PS 业务,只有其处于 CS-CONNECTED 状态或者 PS-CONNECTED 状态(即有一条 PS 信令连接存在)时才处于 RRC 连接状态,否则将处于 RRC 空闲状态。

当 UE 建立了至少一个 PDP 上下文(即处于 SM-Inactive)时,UE 可以处于 PS-CONNECTED 状态或者 PS-IDLE 状态。PDP 上下文的状态不会因为 RRC 连接的释放而改变,除非 RRC 失败导致了实时业务的 QoS 要求不能满足而致使上下文被修改。

### 3. 基于网络层的移动性管理

由上面的基于链路层的移动性管理可以看出,所有的基于网络层的业务都不会因为 UE 的移动而使通信中断或者质量下降。但是,基于链路层的移动性管理有时候并不是一个最好的方法。移动 IP 是从网络层开始解决移动性问题,而屏蔽了底层的具体承载技术。可以说,引入移动 IP 技术弥补了链路层移动管理的缺陷,比如,链路层移动管理不能解决 IP 地址的移动性问题,这一点对于 IP 网络的数据通信非常重要,而移动 IP 中的移动 IPv4 可使移动终端在不同数据网络中使用相同的 IP 地址,并提供 PUSH 业务,移动 IPv6 技术在这方面能力更强。

从作用范围来看,基于网络层的移动性管理可分为宏移动性管理和微移动性管理。宏移动性管理主要处理大范围的移动性,如不同网络之间的漫游,当用户从一个网络漫游至另一个网络时,仍然可以不间断通信;微移动性管理主要处理小范围内的移动性,如同一个网络内部的移动。为提高有效性,需要综合采用宏移动性管理和微移动性管理。目前已提出的微移动性协议可分为两大类:一类是基于路由的方案,如朗讯公司提出的 HAWAII 协议和哥伦比亚大学提出的蜂窝 IP(Cellular IP)协议等;另一类是基于隧道的方案,如移动区域注册(MIP-RR)。在基于路由的方案中,所有的移动代理组成一个严格的树状结构,去往任何一个移动节点的数据包都由移动代理根据其对应于该移动节点的路由来发送。基于隧道的方案则通过多级的移动代理使用所记录的转交地址来将数据包封装,通过隧道沿移动代理逐级往下传送到目标移动节点。

## 5.2.5 HSPA 技术

### 1. 概述

HSPA 是高速下行分组接入(HSDPA)和高速上行分组接入(HSUPA)两种技术的统称,HSPA 是为了支持更高速率的数据业务、更低的时延、更高的吞吐量和频谱利用率、对高数据速率业务的更好覆盖而提出的。在 3GPP 中,HSPA 作为 WCDMA 的增强型无线技术推出,其中,HSDPA 在 R5 中进行标准化,可以在一个小区中支持 14.4Mb/s 的峰值数据速率;HSUPA 在 R6 中进行标准化,可以在一个小区中支持 5.76Mb/s 的峰值数据速率。HSDPA 和 HSUPA 的性能在 3GPP 的后续版本中继续完善和演化,其增强型技术称为 HSPA+。

实现 HSPA 功能主要是对基站修改比较大,对 RNC 主要是修改算法协议软件,硬件影响很小。如果在原有设备中考虑了 HSPA 功能升级要求,一般来讲实现 HSPA 功能不需要硬件升级,只要软件升级即可。要特别说明的一点是,HSPA 技术不仅可用于 WCDMA 系

统中,也可以用于 TD-SCDMA 系统中。

## 2. HSPA 新增物理信道

### 1) HSDPA 新增物理信道

HSDPA 在物理层引入了 3 种新的物理信道,即 HS-PDSCH、HS-SCCH 和 HS-DPCCH。在用户数据传输方面引入了高速下行链路共享物理信道(HS-PDSCH),在伴随的信令消息方面引入了高速共享控制信道(HS-SCCH)和高速专用物理控制信道(HS-DPCCH)。HS-SCCH 信道用于下行链路,负责传输 HS-DSCH 信道解码所必需的控制信息;HS-DPCCH 信道用于上行链路,负责传输必要的控制信息。HSDPA 新增物理信道的相关信息如表 5-4 所示。

表 5-4 HSDPA 新增物理信道的相关信息

缩写	名称	方向	调制方式	功能
HS-PDSCH	高速下行链路共享物理信道	下行	QPSK、16QAM	承载下行链路数据
HS-SCCH	高速共享控制信道	上行	QPSK	为 HS-DPSCH 控制信息:正确解码所需信息、调制方式和 HARQ 进程等
HS-DPCCH	高速专用物理控制信道	上行	BIT/SK	承载上行链路物理层的反馈信息: HARQ 反馈信息、CQI

### 2) HSUPA 新增物理信道

在上行信道方面,HSUPA 增加了增强专用物理数据信道(E-DPCCH)和增强专用物理控制信道(E-DPDCH),E-DPDCH 用于承载用户上行数据,E-DPCCH 承载伴随信令,包括 E-TFCI、重传序列号(RSN)和满意位信息。在下行信道方面,HSUPA 增加了绝对授权信道(E-AGCH)、相对授权信道(E-RGCH)、HARQ 确认指示信道(E-HICH)。E-AGCH 为公共信道,用来传送用户终端最大可用传输速率的数据;E-RGCH 为专用信道,用来传送递增或递减的调度指令,最快可按 2ms TTI(传输时间间隔)调整用户终端的上行传输速率;E-HICH 为专用信道,承载标识用户接收进程是否正确的 ACK/NACK 信息。HSUPA 新增物理信道的相关信息如表 5-5 所示。

表 5-5 HSUPA 新增物理信道的相关信息

缩写	名称	方向	调制方式	功能
E-DPDCH	增强专用物理数据信道	上行	BIT/SK	承载用户上行链路数据
E-DPCCH	增强专用物理控制信道	上行	BIT/SK	为 E-DPDCH 承载控制信息,包括 E-TFCI
E-AGCH	绝对授权信道	下行	QPSK	为上行 E-DCH 调度提供绝对授权
E-RGCH	相对授权信道	下行	QPSK	为上行 E-DCH 调度提供相对授权
E-HICH	HARQ 确认指示信道	下行	QPSK	承载 HARQ 反馈信息

## 3. HSPA 关键技术

### 1) 混合自动重传请求(HARQ)

HARQ 是 ARQ 和前向纠错编码(FEC)的综合利用,HSDPA 和 HSUPA 在物理层都采用了这一技术,都支持两种合并方式——Chase 合并(CC)和增量冗余技术(IR)。CC 方式重发的数据包与原数据包完全相同,接收端把每个包中的对应位一一相加,再送入译码器。而 IR 技术每次重发的数据包里包含更多纠错码的编码方式,因而含有更多的冗余信

息量,可以适应信道条件恶劣的情况。

不同于 R99 的数据包重传,HSDPA 和 HSUPA 的数据包重传避开了 Iub 接口,大大减少了重传时延。HSDPA 和 HSUPA 唯一的差别为 HSDPA 采用了异步的 HARQ,而 HSUPA 采用了同步的 HARQ。

#### 2) 基于 Node B 的快速调度

与 R99 不同,HSDPA 和 HSUPA 的分组调度都是直接由 Node B 控制,而不是由 RNC 控制。在 HSDPA 中,调度主要由 Node B 中的新增实体 MAC-hs 来完成,负责为多个用户分配 HS-DSCH 资源(包括时隙和码字),以达到最大化利用系统资源的目的。在 HSUPA 中,调度主要由 Node B 中新增的 MAC-e 功能实体完成,负责为各个 E-DCH 用户分配所需要的尽可能多的发射功率,同时避免过多的 UE 接入,尽可能地抑制上行干扰。在 HSUPA 中,服务小区将对调度起主要作用。

#### 3) 自适应编码调制(AMC)

HSDPA 引入了比 WCDMA 的 QPSK 更高阶的 16QAM 调制方式以提高下行数据速率,HSDPA 采用 AMC 作为基本的链路自适应技术对调制编码方式进行选择。

在调制方式上,HSUPA 的 R6 中没有引入新的调制方案,而是使用与 WCDMA 上行同样的双 BIT/SK 调制(HPSK 扩展)。同时,为了简化 HSUPA 终端复杂的硬件结构和处理机制,E-HICH 的功能虽然与 HSDPA 的 HS-DPCCH 类似,即提供 HARQ 反馈信息 ACK/NACK,但是 E-HICH 的承载信息中不包含 CQI(信道质量指示)信息,因此 HSUPA 不支持自适应编码调制 AMC。

#### 4) 2ms TTI 短帧传输

R99 中 DCH 的传输时间间隔(TTI)为 10ms、20ms、40ms、80ms。HSDPA 使用 2ms TTI,可以大大减小 HARQ 进程的往返时间,提高快速调度响应能力。HSUPA 同时采用 10ms TTI 和 2ms TTI。保留 10ms TTI,一方面是考虑标准实现后向兼容,另一方面是因为基于 2ms TTI 的短帧传输不适合工作于小区的边缘;而 2ms 的 TTI 为可选,可以大大减小传输时延,获得更高的系统吞吐量。

## 5.3 CDMA 2000 系统

### 5.3.1 概述

#### 1. CDMA 2000 的演进路径

CDMA 2000 是在 CDMA One(包括 IS-95A 和 IS-95B)基础上发展起来的 3G 技术,它是由美国 TIA 等标准化组织向 ITU 提交并被 ITU 接纳的 3G 标准之一,它实现平滑演进,其系列标准由 3GPP2 制定。与 CDMA One 相比,CDMA 2000 增加了分组域网元,引入了分组数据业务;在空中接口上进行了重大改进,并获得了更大的容量、更高的速率和质量。

CDMA 2000 的具体演进路径如图 5-23 所示。CDMA 2000 1x 以后的是 3G 标准,而 CDMA 2000 1x 在习惯上被看作 2.5G(因为这一点,所以将它放在第 4 章介绍),当然 3GPP2 并未明确这一说法。CDMA 2000 1x 之后有两条演进路径,其中之一是发展到 CDMA 2000 3x,它在前向链路上可选多载波(3 个 CDMA 载频捆绑,每载波扩频码片速率为 1.2288Mc/s)或直扩(1 个载波,扩频码片速率为 3.6864Mc/s),反向链路采用直扩

(3.6864Mc/s 码片速率)。这种标准由于技术复杂,通常系统成本较高。另一条演进路径就是 CDMA 2000 1xEV(在 CDMA 2000 1x 基础上的增强),它又分为 CDMA 2000 1xEV-DO 和 CDMA 2000 1xEV-DV,DO 的含意是指仅支持数据增强,而 DV 的含意是指数据信道和语音信道合一,都得到增强,该方案得到了多数厂商和运营商的支持。

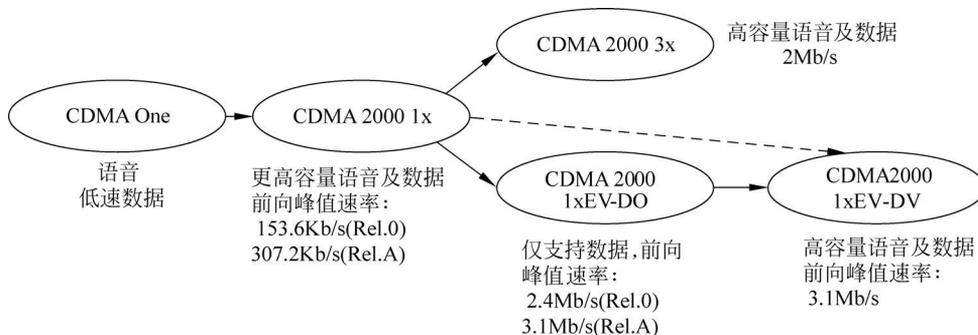


图 5-23 CDMA 2000 的具体演进路径

3GPP2 为 CDMA 2000 制定了 0、A、B、C、D、E、F 共 7 个版本(Release),但 CDMA 2000 的 Release 通常仅仅指无线接口和 A 接口,核心网是独立的。CDMA 2000 1xEV 的不同版本的业务性能如图 5-24 所示。需要说明的是, EV-DO 的 Rel. B 版本通过捆绑几个 Rel. A 载波以实现多载波,如果是捆绑 3 个载波,峰值速率下行达到 9.3Mb/s,上行 5.4Mb/s;最多可捆绑 15 个载波,此时峰值速度下行达到 73.5Mb/s,上行 27Mb/s。

仅用于分组数据业务,全 IP 架构	CDMA 2000 1xEV-DO	
	Rel. 0	Rel. A
	前向峰值速率为 2.4Mb/s,反向峰值速率为 153.6Kb/s,增强时支持 QoS、多播、均衡、接收分集	前向峰值速率为 3.1Mb/s; 反向峰值速率为 1.8Mb/s



同时支持语音及数据	CDMA 2000 1x			CDMA 2000 1xEV-DV	
	Rel. 0	Rel. A	Rel. B	Rel. C	Rel. D
	前向峰值速率为 153.6Kb/s,分组业务与语音	前向峰值速率为 307.2Kb/s,分组业务与语音		前向峰值速率为 3.1Mb/s; 反向峰值速率为 451Kb/s	前向峰值速率为 3.1Mb/s; 反向峰值速率为 1.8Mb/s

图 5-24 CDMA 2000 1xEV 的不同版本的业务性能

CDMA 2000 演进的主要特点是: ①模块化划分,各个模块按照自己的技术发展道路向前演进,尽可能减小对其他模块的影响,这和 WCDMA 强调系统整体推进不一样(虽然无线接入网和核心网也可以分别整体推进),而且这种模块化的演进方式不仅使得 CDMA 2000 系统的升级具有平滑性,也使得 CDMA 2000 网络更具灵活性; ②CDMA 2000 系统经常利用现有的成熟技术,降低了标准的编写复杂度,加快了标准的制定进程。CDMA 系统自身独特的演进方式,使得系统具有完备的前后兼容性,升级成本低,风险小,技术复杂度低。

### 2. CDMA 2000 的主要特点

与 CDMA One 相比,CDMA 2000 具有以下主要特点。

- (1) 多种信道带宽,高扩频增益,前向链路上支持多载波和直扩两种方式,反向链路仅支持直扩方式;也支持可变扩频因子,扩频长度为 4~512,扩频码长度较大时,可获得高扩频增益。
- (2) 前后向兼容,可实现平滑过渡。
- (3) 核心网协议可使用 IS-41、GSM-MAP 以及 IP 骨干网标准。
- (4) 宽松的性能范围,从语音到低速数据,到高速的分组和电路数据业务。
- (5) 提供多种复合的业务,包括只传送语音,同时传送语音和数据,只传送数据和定位业务等。
- (6) 具有先进的多媒体 QoS 控制能力,支持多路语音、高速分组数据同时传送。
- (7) 在同步方式上,沿用 IS-95 CDMA 方式,采用 GPS 使基站间严格同步,以取得较高的组网与频谱利用效率,有效地使用无线资源。
- (8) 由于采用新技术,在提高系统性能和容量上有明显的优势。

### 3. CDMA 2000 的系统结构

简化的 CDMA 2000 系统结构如图 5-25 所示。它主要包括无线部分、核心网和外部网络,其中核心网包括核心网电路域、核心网分组域、智能网、MC、定位模块和 WAP 等几部分。CDMA 2000 的无线部分、MC、定位模块、核心网电路域、智能网以及 WAP 的基本要求和 CDMA One 一样,只是技术更先进一些,并且任何模块只要技术发展了,都可以独立更新。核心网分组域是新增的,包括 PCF、PDSN、AAA、HA 和 FA 等功能实体。其中 PCF

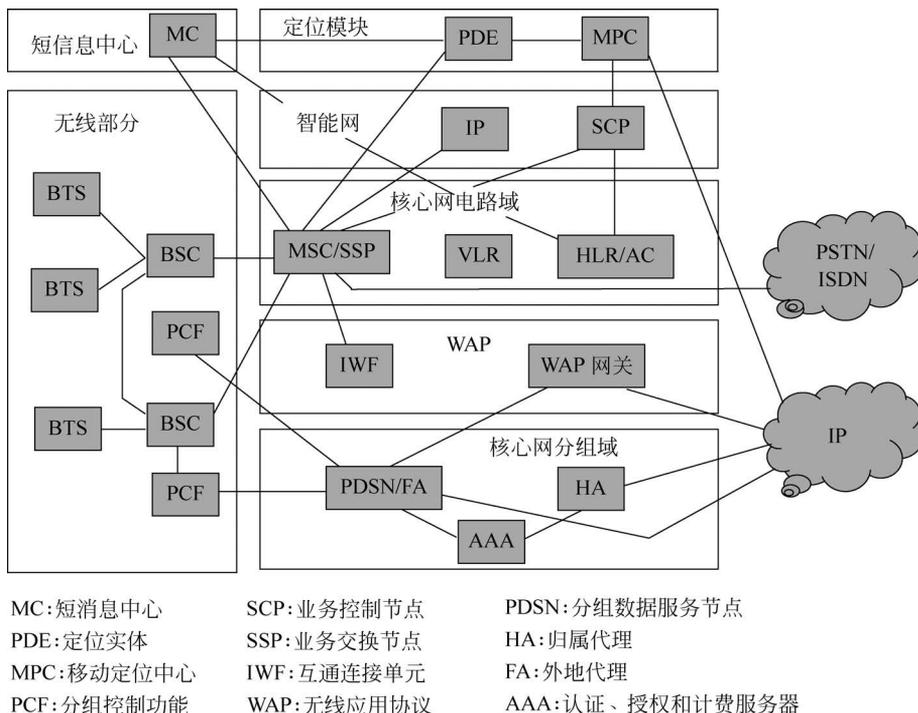


图 5-25 简化的 CDMA 2000 系统结构

负责与 BSC 配合,完成与分组数据有关的无线信道控制功能,虽然它的物理实体通常和 BSC 在一起,但属于核心网分组域;PDSN 负责管理用户通信状态,转发数据;AAA 负责管理用户,包括权限、开通的业务等;当使用移动 IP 协议时,分组域还应在简单 IP 基础上增加 HA,HA 负责将分组数据通过隧道技术送给移动用户,并实现 PDSN 之间的宏移动性管理,同时,PDSN 还应增加外地代理(FA)功能,负责提供隧道出口,并将数据解封装后发往移动台。

A 接口是基站子系统与核心网之间的接口,由于核心网增加了分组域,因此 CDMA 2000 的 A 接口进行了分化,部分网络参考模型如图 5-26 所示。CDMA 2000 的 A 接口包括 4 个组成部分:A1/A2/A5、A3/A7、A8/A9 和 A10/A11。各子接口的主要功能如表 5-6 所示。

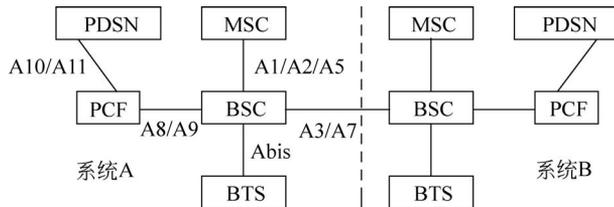


图 5-26 CDMA 2000 的 A 接口部分网络参考模型

表 5-6 CDMA 2000 的 A 接口各子接口的主要功能

接口	接口的主要功能
A1	用于传输 MSC 和 BSC 之间的信令消息,使用 SS7 中消息传递部分(MTP)和信令连接控制部分(SCCP)来承载
A2	传输采用 64KPCM 电路的语音部分
A3	传输 BSC 和 SDU 之间的用户话务(语音与数据)和信令,A3 接口包括独立的信令和话务子信道
A5	传输 IWF 和 SDU(交换数据单元)之间的全双工数据流
A7	传输 BSC 之间的信令,支持 BSC 之间的软切换
A8	传输 BS 和 PCF 之间的用户业务
A9	传输 BS 和 PCF 之间的信令业务
A10	传输 PDSN 和 PCF 之间的用户业务
A11	传输 PDSN 和 PCF 之间的信令业务

#### 4. IP 技术在 CDMA 2000 系统中的应用

CDMA 2000 提供了简单 IP 和移动 IP 两种分组服务接入方式。

##### 1) 简单 IP(SIP)方式

类似于传统的拨号接入,PDSN 为移动台动态分配一个 IP 地址,该 IP 地址一直保持到该移动台移出该 PDSN 的服务范围,或者移动台终止简单 IP 的分组接入。当移动台跨 PDSN 间切换时,一般通信发生中断,该移动台的所有通信需重新建立,重新建立通信后通常 IP 地址也会发生变更,但若网络提供 PDSN 间的快速切换功能(通过 PDSN 间的可选 P-P 接口来实现),则其 IP 地址也可保持不变。由于用户每次连接的 IP 地址不能确保固定,所以 SIP 只能提供用户主动发起的业务,而不能提供网络侧发起的业务。SIP 可支持 IPv4 和 IPv6。移动台在其归属地和访问地都可以采用 SIP 接入方式。

##### 2) 移动 IP(MIP)方式

移动台使用的 IP 地址是其归属网络分配的,不管移动台漫游到哪里,它的归属 IP 地址均保持不变,这样移动台就可以用一个相对固定的 IP 地址和其他节点进行通信了。简单地

说,移动 IP 提供了一种特殊的 IP 路由机制,使得移动台可以以一个永久的 IP 地址连接到任何链路上。移动 IP 的实现,主要通过三个步骤来完成:代理搜索、注册、数据包的选路。代理搜索过程如下:移动代理(含 HA 和 FA)通过代理广播消息向用户广播它们的存在,当移动节点(MN)收到广播后就能确定它目前是处于本地网还是在外地网。注册过程如下:当 MN 确定其处于本地网时,若还没有注册,则 MN 应首先到 HA 进行注册,然后再进行正常通信;当 MN 确定目前位置已移至外地网时,它就在本地网中获得一个转交地址,MM 再用外地转交地址向 HA 注册。数据包的选择路径(选路)过程如下:当 MN 处于本地网时,数据包的选择和固定节点的选择原理相同;当 MN 处于外地网时,启动 MIP 机制进行选路,数据的上行是先由 MN 发给 PDSN/FA,PDSN 再将数据包直接路由转发到目标设备,而在下行方向上,凡传送给 MN 的数据包首先要被 HA 截获,然后再通过专用隧道(这个专用隧道可优化)送至 MN 的转交地址并达到隧道的终点。

### 3) 简单 IP 和移动 IP 的差异

SIP 与 MIP 的区别首先体现在对移动用户的移动性支持上。在 CDMA 2000 网络中,分组数据用户的移动性体现为三个层次:蜂窝移动性、PCF 到 PDSN 的移动性、IP 级的移动性。由于 SIP 模式中移动用户的 IP 地址由 PDSN 分配,所以 SIP 模式只支持二级移动性,而不能对 IP 级移动性提供支持,相对应的是 MIP 能支持三级移动性。其他差异还体现在移动终端的支持性、配置方式、专网接入方式等方面。

## 5.3.2 CDMA 2000 1xEV-DO 系统

### 1. 概述

CDMA 2000 1xEV-DO 技术起源于美国 Qualcomm 公司提出的高速率数据(HDR)技术。1997年8月,Qualcomm 公司向 CDMA 发展组织(CDG)提出了 HDR 的概念,在随后的几年中,该技术逐渐成熟。2000年10月,CDMA 2000 1xEV-DO 的标准在 3GPP2 中获得通过,后来,3GPP2 又将其定名为高速分组数据(HDPR)。

CDMA 2000 1xEV-DO 实际上是 CDMA 2000 1x 和 HDR 技术的结合,它的实现思路是:利用分组数据业务和语音业务对资源的需求不同这一特点,将数据业务和语音业务相分离,在独立于 CDMA 2000 1x 语音业务的载波上提供分组数据业务。具体的方法是:在一个或几个载波上用 HDR 技术传输高速分组数据业务,即在 CDMA 的基础上引入了 TDMA 技术的一些特点,“时分”使得“速率控制”容易实现,从而大幅度提高了数据业务的性能;在另外的一个或几个载波上用 CDMA 2000 1x 技术传输语音业务。

CDMA 2000 1xEV-DO 现有 Rel. 0 和 Rel. A 两个版本,可以在 1.25MHz 带宽内提供高达 2.4Mb/s(Rel. 0)和 3.1Mb/s(Rel. A)的前向峰值速率,频谱利用率非常高。现阶段,CDMA 2000 1xEV-DO 已在全球得到了大规模的商用。

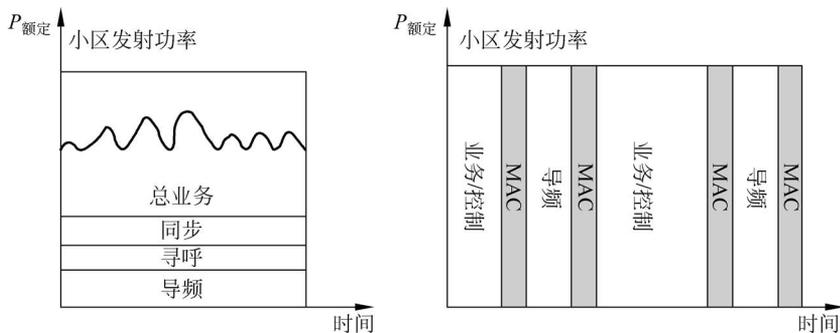
### 2. CDMA 2000 1xEV-DO 的技术特点

与 CDMA 2000 1x 相比,CDMA 2000 1xEV-DO 具有峰值速率高、平均吞吐量大和频谱利用率高的优势。为达到这些要求,CDMA 2000 1xEV-DO 在技术实现上出现了许多变化,其具体的技术特点如下。

(1) 前向链路时分复用,反向链路码分复用。CDMA 2000 1xEV-DO 充分利用了数据通信业务的不对称性(下行流量大于上行)和数据业务对实时性要求不高的特征,前向链路



设计为时分复用 CDMA 信道。也就是说,在 CDMA 2000 1xEV-DO 中,一个时刻只有一个用户在接受服务,不同用户在不同的时刻接受服务,这样,当用户没有数据传输的时候,就不必给用户分配信道。但是,原来的 CDMA 技术仍然保留在 CDMA 2000 1xEV-DO 的调制解调和扩频方式中,这样就保留了原来 CDMA 技术抗多径干扰的特性。另外,不管是传输控制信息还是传输业务信息,CDMA 2000 1x EV-DO 的前向链路载波总是以全功率发射。它的前向链路功率示意图如图 5-27 所示。



(a) IS-95CDMA/CDMA2000 1x前向链路功率示意图 (b) 1xEV-DO前向链路功率示意图

图 5-27 IS-95 CDMA、CDMA 2000 1x 和 CDMA 2000 1xEV-DO 前向链路功率示意图

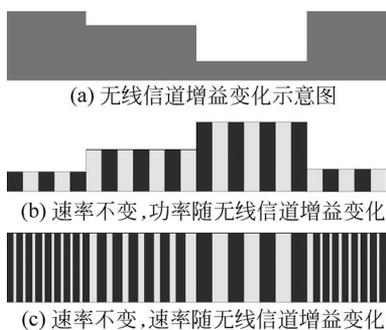


图 5-28 无线环境变化时的功率控制与速率控制过程

(2) 动态速率控制。在前向链路上,发射功率保持不变,即不再采用功率控制,转而采用速率控制。这是因为在某一时刻,只有一个用户将得到前向载波的全部功率,不必考虑其他用户受到干扰而采取功率控制;此外,用户在不同的无线环境下,其得到的数据服务速率不同。CDMA 2000 1xEV-DO 采用了动态速率控制,根据用户的不同环境,快速调整数据发送速率(最小调度单位为 1.667ms),保证用户尽可能快速地接收信息。图 5-28 给出了无线环境变化时功率控制和速率控制的过程,可以从中看出功率控制和速率控制处理方法的差异。

在反向链路上,CDMA 2000 1xEV-DO 的 Rel. 0 采用功率控制;而 Rel. A 则采用快速动态功率控制,此外,移动台根据基站返回的反向链路负荷情况指示采用随机化算法来调节移动终端的数据发送速率,这种速率控制可对反向链路的负荷进行调节,它和前向链路的速率控制还是有差别的。

(3) 自适应调制编码。系统能够根据信道的变化情况快速调整编码调制方案(Turbo 编码率可选 2/3、1/3 和 1/5,调制可选 QPSK、8PSK 和 16QAM)来获得任何时刻所能达到的最大传输速率,从而能够充分利用空中链路资源,满足用户需求。

(4) 前向虚拟软切换。在软切换状态,移动台同时与两个或两个以上的基站联系,所以软切换需要占用多个基站的资源。而在 CDMA 2000 1xEV-DO 的前向链路中,由于具有速率高、功率大和实时数据业务等特点,如果采用类似语音的软切换将会极大地浪费资源,所以在前向链路的业务信道上采用了虚拟软切换,它是快速小区交换技术,即选择信号质量最好的基站,信息通过这个质量最好的基站发送给移动台,由于只需要一个基站,从而降低了

对系统资源的需求。

在前向链路的控制信道以及反向链路上,系统仍旧采用软切换技术,以保证较好的通信质量。

(5) 灵活的调度算法。在基站中,由一种调度算法来决定下一个时隙分配给具体哪一个用户使用。由于每个时隙中只有一个用户在接受服务,显然,为了提高系统的性能,系统应当优先向无线环境比较好的用户提供服务,利用这种多用户分集增益使扇区吞吐量最大化。但是,无线环境较差的用户可能长时间得不到服务,因此,在保证系统综合性能最大的同时,通过调度,也使所有用户都能获得适当的服务。

(6) 支持广播和组播业务。为了充分利用带宽,使得类似于电视节目的广播服务能够更有效地在移动通信网络中传输,CDMA 2000 1xEV-DO 引入了广播和组播业务(BCMCS)技术。BCMCS 可以使组播 IP 流在空中只传输一份复本,多个用户接收,从而大大节省空中链路带宽,有效地提高服务质量和整体吞吐量,同时也能将费用降低到用户可以接受的水平。

(7) 核心网基于无线 IP。CDMA 2000 1xEV-DO 的核心网是基于无线 IP 的网络结构,采用 IP 协议实现从互联网或其他 IP 网络到移动终端的数据传输,支持和 CDMA 2000 1x 之间的切换。

### 3. CDMA 2000 1xEV-DO 的网络结构

CDMA 2000 1xEV-DO 的网络参考模型如图 5-29 所示。其中引入了 AT(接入终端)、AN(接入网络)和 AN AAA 三个网络元素。AT 相当于传统的移动台,用户可以将计算机与 AT 相连(AT 相当于 Modem)或直接使用支持分组数据业务的 AT 接入分组数据网;AN 相当于传统的基站,它一方面通过空中接口连接 AT,另一方面通过 A 接口与分组数据网相连;AN AAA 作为网络侧的一个鉴权机构,它主要用于对终端的认证,其功能类似于核心网电路域中的 HLR,在通过升级建成的网络中,它可以省略,其功能由核心网分组域的 AAA 来完成。其他网元和 CDMA 2000 1x 系统中相应网元相同。

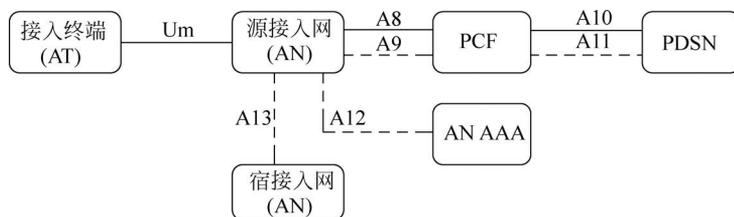


图 5-29 CDMA 2000 1xEV-DO 的网络参考模型

网络模型中,A 接口新增了两个子接口:A12 接口和 A13 接口。A12 接口是 AN 与 AN AAA 之间的接口,用于传递鉴权信息;A13 接口是两个 AN 之间的接口,用于支持 AN 之间的切换。

### 4. CDMA 2000 1xEV-DO 的物理信道

系统的空中接口定义了 7 层协议,在每一层协议中又定义了若干协议子层。这 7 层协议由上到下包括应用层、流层、会话层、连接层、安全层、媒体接入控制层和物理层,需要说明的是,这 7 层只是 OSI 协议模型中的物理层和数据链路层的扩展。

在物理层中定义了前向/反向链路的信道(前向/反向物理信道),以及这些信道的结构、编码、调制、功率输出特性和频率等。

## 1) 前向物理信道

CDMA 2000 1xEV-DO 的 Rel. A 规定的前向物理信道分类如图 5-30 所示。

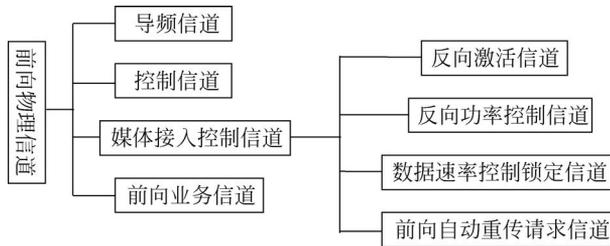


图 5-30 CDMA 2000 1xEV-DO 前向物理信道分类

各个前向物理信道的主要功能如下：

(1) 导频信道,主要用于系统捕获及信道质量测量。

(2) 媒体接入控制(MAC)信道,其中,反向激活(RA)信道用于指示终端是否增加或降低传输速率;反向功率控制(RPC)信道则负责对反向链路进行功率控制,调整终端的功率;数据速率控制锁定(DRCLock)信道主要用于接入网向终端声明是否收到数据速率控制信息。为了支持反向 HARQ 功能,相应的前向链路新增了自动重传请求(ARQ)信道,对接收到的反向数据包进行确认。

(3) 控制信道,主要负责向终端发送一些控制消息,诸如终端控制区(TCA)消息和扇区参数消息,其功能类似于 CDMA 2000 1x 中的寻呼信道。

(4) 前向业务信道,主要负责向终端发送业务数据,会话建立后的参数配置消息也在前向业务信道发送,它进一步可划分为前缀部分和数据部分。

## 2) 反向物理信道

CDMA 2000 1xEV-DO 的 Rel. A 规定的反向物理信道包括反向业务信道和接入信道两大类,如图 5-31 所示。

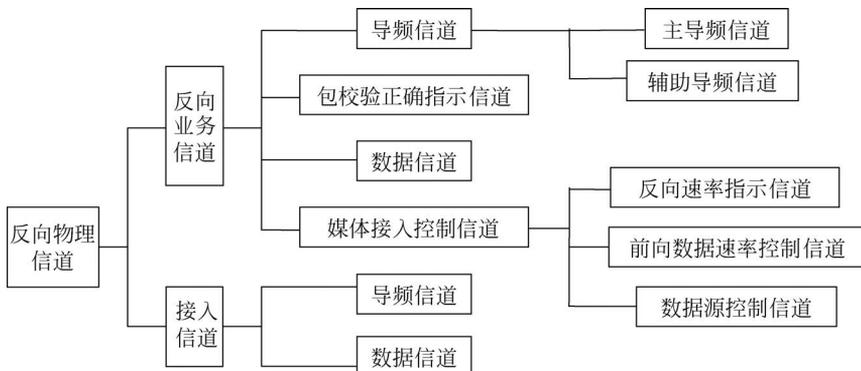


图 5-31 CDMA 2000 1xEV-DO 反向物理信道分类

各反向物理信道功能描述如下。

(1) 反向业务信道中,导频信道用于接入网对终端的捕获;包校验正确指示(ACK)信道用于向接入网发出响应,表明终端已经正确收到了接入网所发送的数据;媒体接入控制信道中的反向速率指示(RRI)信道用于通知接入网目前终端数据信道的传输速率,反向速率指示信道与导频信道以时分方式进行复用;前向数据速率控制(DRC)信道根据对各扇区

的导频信道测量的结果,选定导频信号最强扇区并与之通信,同时要求该扇区按终端规定好的速率进行传输,从而实现对前向链路的速率控制;为减小干扰,前向数据速率控制信道信号在发送时可以采用门控与非门控两种方式传输;数据源控制信道主要是提高切换功率,减少业务中断,具体过程是——终端提前一定时间将自己需要切换的目标小区信息通过数据源控制信道提前通知基站,基站收到消息后做切换准备;辅助导频信道主要是为了辅助基站对高速数据进行解调,提高反向吞吐量。

(2) 接入信道,用于 AT 向 AN 发起呼叫或响应 AN 发出的指令信息,接入信道中的导频信道作为前缀(用于提供反向相干解调),后面紧跟接入的数据包(即数据信道)。

### 5.3.3 CDMA 2000 1xEV-DV 系统

#### 1. CDMA 2000 1xEV-DV 标准的产生

在 CDMA 2000 1xEV-DO 系统中,语音和数据业务使用不同的载波,并使用了一系列新技术。这种方案的优点是控制资源简单、语音业务和数据业务互不影响、数据业务还达到了很高的传输率;但与此同时,也带来了该方案固有的缺点,即语音业务和数据业务中任何一方有空闲资源时,并不能用来支持对方,这样整个系统资源利用率低;另外,CDMA 2000 1x 和 CDMA 2000 1xEV-DO 双模手机在切换时,前向链路语音和数据切换方式不一样,管理难度大大增加。

针对以上情况,3GPP2 提出了新的系统方案,即将语音和高速分组数据业务合并到一个载波上传输,这就是 CDMA 2000 1xEV-DV。其目标是系统能够在同载波上传输实时性业务和非实时性业务以及这两种业务的混合业务。

3GPP2 分别在 2002 年和 2004 年发布了 Rel. C 和 Rel. D 版本两套标准,对应于 CDMA 2000 1xEV-DV 发展的两个阶段。Rel. C 主要是在前向链路进行了加强,使前向峰值数据速率达到了 3.1Mb/s;而 Rel. D 主要是在反向链路进行加强,使反向峰值数据速率也达到了 1.8Mb/s。不过这两个版本在语音容量上并无显著提高(语音容量的提高成为后续版本 Rel. E 的目标之一)。

#### 2. CDMA 2000 1xEV-DV 的 Rel. C 技术特点

Rel. C 标准具有更高的前向容量、后向兼容 CDMA 2000 1x、可支持多种业务组合以及更有效支持数据业务的特性。其具体的技术特点如下。

(1) 新增物理信道。为了在和语音业务相同的载波上支持高速分组数据业务,Rel. C 标准在维持 CDMA 2000 1x 原有物理信道的基础上新增了 4 种物理信道。

在前向信道中,增加了前向分组数据信道(F-PDCH)和前向分组数据控制信道(F-PDCCCH),F-PDCH 用于传送高速分组数据,在同一个扇区的不同用户之间,F-PDCH 以时分的方式快速复用;此外,同一时刻 F-PDCH 信道允许不同用户码分复用,也就是 TDM/CDM 方式,但同一时刻 PDCH 码分复用的用户数量不能太多,否则将大大增加 TDM/CDM 的信令开销,同时增加终端的复杂性和处理负担,Rel. C 中允许 PDCH 同一时刻最多两个用户码分复用。F-PDCCCH 用于传输用户的 F-PDCH 控制信息。

为了配合前向链路的增强,Rel. C 的反向信道新增了反向确认信道(R-ACKCH)和信道质量指示信道(R-CQICH),ACK 信道用于支持前向 HARQ,对接收到的前向子分组进行确认,CQICH 用于向基站反馈前向信道质量,通过 Walsh Cover 指示目标基站,基站基于

这个信息确定下一个发送子分组的调制和编码方式。

(2) 分组数据控制保持模式。Rel. C 在分组数据激活和休眠模式的基础上增加了控制保持模式,控制保持模式介于激活模式和休眠模式之间,当处于控制保持模式时,移动台不解调 F-PDCH 但解调 F-PDCCH,对反向导频进行 1/2 或者 1/4 门控,信道质量指示(CQI)报告进行 1/2 或 1/4 门控,或不报告 CQI,这样,在不进入休眠的时间内节约了移动台的耗电量。

(3) 功率控制与速率控制相结合。在前向链路上采用功率控制和速率控制相结合的控制方案,首先通过快速功率分配,以 800Hz 的频率估计语音等用户需要的功率,并把剩余功率分配给使用 F-PDCH 的分组数据用户,并根据分配给数据用户的功率,进行速率控制。这样就充分利用了语音激活、功率控制以及低话务量时间段基站所富余出来的系统资源,从而提高了整个系统的资源利用率。图 5-32 展示了 CDMA 2000 1xEV-DV 的功率控制与速率控制相结合的控制过程,具体步骤是图中的(1)→(2)、(2')→(3)、(3')→(4)→(5)、(5')→(6)。

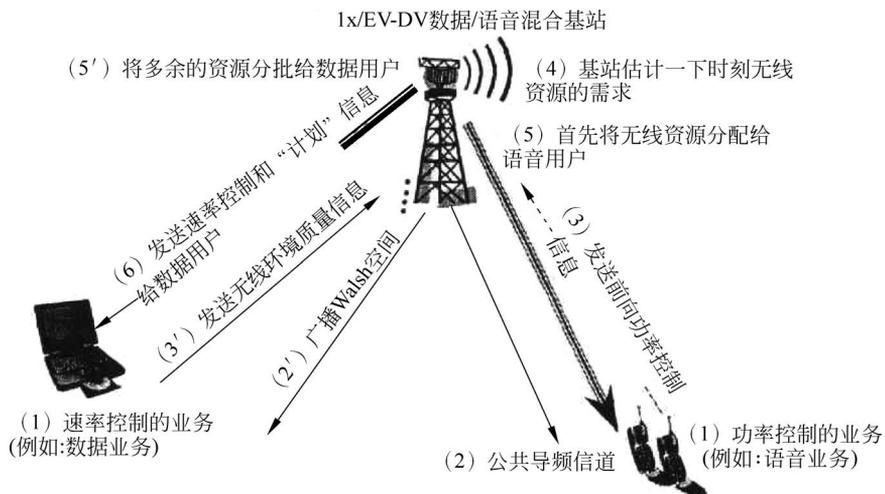


图 5-32 CDMA 2000 1xEV-DV 的控制过程

(4) 快速呼叫建立。快速呼叫建立主要针对分组数据的呼叫建立过程进行了增强,减小呼叫建立的时延,也可以用于其他业务的呼叫建立,便于对呼叫建立时间有特殊要求业务的开展,如 PTT。Rel. C 对呼叫建立过程的增强主要体现在以下几个方面,即信道分配时指示已保存业务配置,可以重新存储某个业务配置,短重连接消息。

除以上技术外,Rel. C 还通过自适应调制和编码、前向 HARQ 进行前向链路增强。另外,由于在 F-PDCH 信道上要传输高速数据,所以在该信道采用小区交换技术,其他信道继续采用软切换。

### 3. CDMA 2000 1xEV-DV 的 Rel. D 技术特点

Rel. D 的反向链路得到增强以后具有如下特性: ①完全保留了 CDMA 2000 1x 信道的信令结构; ②控制方式灵活; ③反向调度和速率控制的速度加快; ④物理层分组帧长固定为 10ms,10 种固定分组大小; ⑤采用同步 4 信道 HARQ 技术,提高链路效率; ⑥采用自适应调制和编码技术; ⑦移动台可以基于 QoS 要求在时延和吞吐量之间选择; ⑧QoS 改善,不同业务区分接入优先级,基于 Buffer(缓存)和功率申请资源。

Rel. D 的具体技术特点如下。

(1) 新增物理信道。Rel. D 在反向物理信道中新增加了 RC7 和相应的 4 个反向物理信道,分别为反向辅助导频信道(R-SPICH)、反向请求信道(R-REQCH)、反向分组数据信道(R-PDCH)和反向分组数据控制信道(R-PDCCH)。为了支持反向链路的增强,并进一步提高系统容量,Rel. D 在前向物理信道中新增加了 RC7 和相应的 3 个前向物理信道,分别为前向许可信道(F-GCH)、前向确认信道(F-ACKCH)和前向指示信道(F-ICCH)。

(2) 快速呼叫建立。在 Rel. C 的基础上,Rel. D 通过直接信道分配、减小时隙周期索引(SCD)、业务信道初始化增强和跟踪区域报告等技术,进一步增强了快速呼叫建立。

(3) 新的移动台设备标识(MEID)。目前移动台都是以其硬件决定的 32 位电子序列号(ESN)来唯一标识移动台的,随着移动通信用户数的不断增加,32 位的 ESN 的资源日益紧张。为解决 ESN 资源不足的瓶颈问题,3GPP2 组织开始研究一种 ESN 的替代方案,来扩展移动台可用的标识资源,并决定将这种 ESN 替代方案正式写入 CDMA 2000 1xEV-DV 的 Rel. D 版本中,形成新的 MEID。

移动台可以使用 32 位的 ESN 或者 56 位的 MEID 的两者之一(不能同时)。ESN 和 MEID 是用来唯一标识一个移动台的(相当于移动台的硬件号码),若移动台的版本号(MOB\_P\_REVP)小于 7,将使用 ESN,否则使用 MEID。为了后向兼容,若移动台支持 MEID,则根据 MEID 推导出 32 位的伪 ESN,再使用伪 ESN 来替换 ESN。32 位伪 ESN 的高 8 位设置为 0X80,低 24 位为 MEID 经过 SHA-1 算法后取其 24 位。MEID 与伪 ESN 的映射是固定的,不同的 MEID 会映射出同一个伪 ESN,ESN 不是唯一的。因而在 Rel. D 中支持 PLCM(公共长码掩码)32,避免由于 ESN 的冲撞导致的串音现象。

从以上所述的 CDMA 2000 1x EV-DV 两个版本的特点也可以看出,Rel. D 版本更便于多样化业务的开发,在上、下行对称业务(如 E-mail、可视电话等业务)的支持方面有更多的优势,与 Rel. C 相比,具有更强的竞争力,但 Rel. D 的技术更复杂,实现难度更大。

### 5.3.4 CDMA 2000 核心网的演进

#### 1. CDMA 2000 核心网的演进路线

3G 系统的核心网有一个共同的演进方向:最终到达基于 IMS 的 ALL IP(全 IP)架构。具体对于 CDMA 2000 系统来说,在无线侧不断演进的同时,核心网也经历了一个逐渐演进的过程,即从非开放内部接口,到半开放的 ATM 接口,最终到完全开放的 IP 接口,也就是 CDMA 2000 ALL IP 网络。CDMA 2000 网络侧演进将是逐步的和后向兼容的。

3GPP2 发布了一个演进标准 S. R0038,制定了 CDMA 2000 核心网从现有网络向 ALL IP 的演进路线,如图 5-33 所示。ALL IP 网络的演进分为 4 个阶段(Phase),其中,Phase 2 对应于 LMSD(传统移动终端域)阶段,可细分为 Step 1、Step 2、……、Step  $n$ ; Phase 3 对应 MMD(多媒体域)阶段,又可细分为 Step 1、Step 2、……、Step  $n$ 。

在 CDMA 2000 核心网的演进路线中,Phase 0 是演进的起点;Phase 1 是演进过程中的增强型网络,分组网络能力扩大,信令用 IP 进行传输;Phase 2 是向 ALL IP 网络演进的第一步,引入了软交换的思想,信令和承载开始独立演变并采用 IP 进行传输,核心网和接入网也开始分离,这个阶段引入了 LMSD(移动软交换系统),在 IP 核心网中支持传统的终端以及 IMS 中的一些实体,空中接口仍采用 CDMA 2000 系列标准;Phase 3 是 ALL IP 网络的最终目标,空中接口将 IP 化,LMSD 域将逐渐消失,最终由 IMS 完全取代,3GPP2 称此阶段为 MMD(移动多媒体系统)。

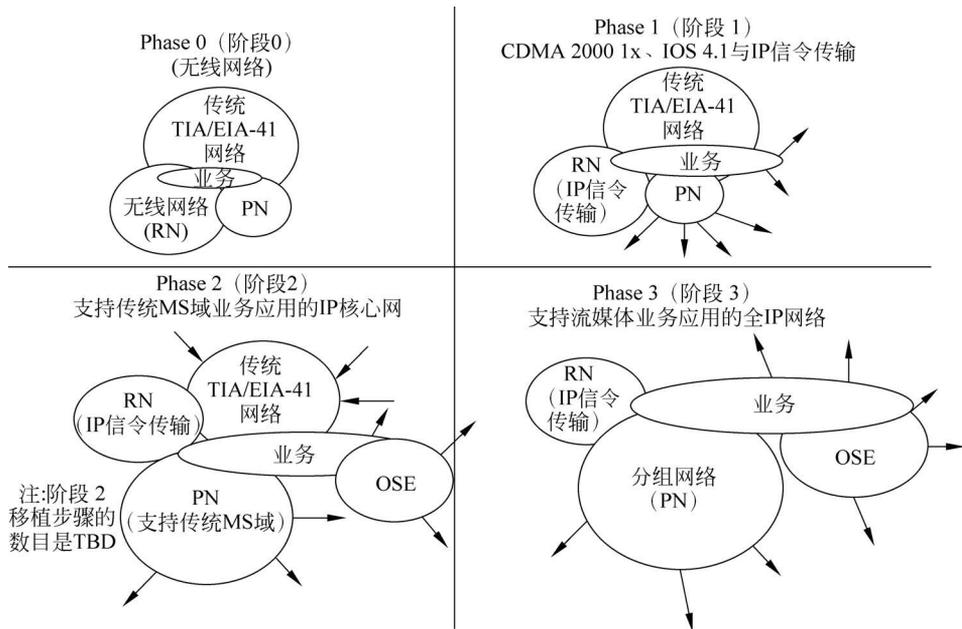


图 5-33 CDMA 2000 核心网演进路线

网络演进到 MMD 之后,核心网提供对各种接入技术的支持,3G 业务统一基于一个 ALL IP 架构上来实现,业务的实现形式也变得更加容易和丰富。可以说 Phase 3 为网络融合提供了很好的契机,分别基于 3GPP2 和 3GPP 标准的移动网络可以实现融合,而且移动网络也可以实现与固定网络的融合。

## 2. Phase 0

Phase 0 是 CDMA 2000 核心网演进的起点,是基于电路交换的传统网络,Phase 0 中网络各部分具有如下特征。

(1) 核心网电路域基于 IS41D 协议。

(2) 核心网分组域 PS 的结构由 P. R0001 定义,引入了 PCF 和 PDSN,使用简单 IP 和移动 IP 作为分组数据业务的接入方式,并使用 RADIUS(远程认证拨号用户服务)服务器或 AAA 提供鉴权和计费。

(3) A 接口由 IOS4.0 来定义。其中,A3、A7、A8、A9、A10 和 A11 已经实现了信令链路与数据承载分开。

## 3. Phase 1

与 Phase 0 相比,Phase 1 的主要发展包括支持分组数据话路的切换,支持语音与分组数据的并发等;其网络结构没有太多的变化,主要是业务功能有所增强。可以说 Phase 0 和 Phase 1 还都属于网络演进过程中的传统域阶段。Phase 1 中网络各部分具有如下特征:

(1) 核心网中电路域在 IS41D 的基础上增加了 IS880 协议,以支持与分组数据相关的功能,如切换、用户属性信息、分组数据业务选项等。

(2) 无线接入网中 A 接口采用 IOS4.1 协议,但无线接入网的网络结构与 Phase 0 相比没有什么变化。

## 4. Phase 2

Phase 2 是向 ALL-IP 网络发展的第一步,这一阶段也称为 LMSD 阶段。LMSD 在基

于 IP 协议的核心网中提供对传统终端(IS-95A、IS-95B 和 IS-2000 等)的兼容功能,支持传统 IS41D 网络中的业务和功能,并且对用户是透明的,新的业务和功能由 IP 核心网提供给使用新终端的用户。LMSD 阶段整体网络架构仍然是传统意义上的集中控制架构,为典型的主从模式协议。LMSD 阶段是向 IMS 阶段过渡的一个阶梯,IMS 阶段更多地体现了客户—服务器理念,终端和网关具备更多的主动性和智能性。可以说,LMSD 阶段既兼顾了运营商原来的投资利益,同时也可以保证向 ALL IP 网络顺利迈进,为二者之间找到了一个平衡点。LMSD 分  $n$  个步骤来演进,目前 3GPP2 已经明确了的是 Step 1 和 Step 2。

#### 1) LMSD Step 1

LMSD Step 1 的网络结构与 Phase 0 和 Phase 1 的网络结构相比,主要的变化是将 MSC 分成了 MSCe(移动交换中心仿真)、MGW(媒体网关)与 MRFP(多媒体资源功能处理器),实现电路域中传统交换机中的信令与承载分离。MSCe、HLRe(HLR 仿真)和 SCPe(SCP 仿真)等支持传统电路域的实体构成了支持传统域的系统(LMSDS),负责信令的处理。新增的 MGW 和 MRFP 负责与承载相关的媒体处理。增加新的实体之后,相应地在新实体之间定义了新的接口,即 MRFP 与 LMSDS 之间的 xx 接口、两个 MGW 之间的 yy 接口、两个 LMSDS 之间的 zz 接口以及 MGW 与 LMSDS 之间的 39 接口。图 5-34 是 LMSD Step 1 的网络结构。

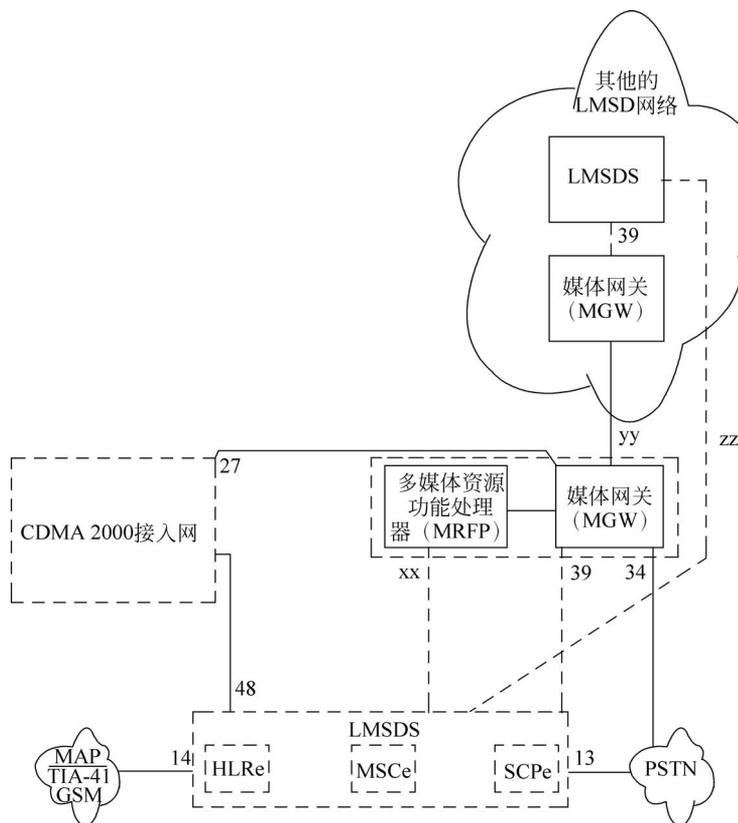


图 5-34 LMSD Step 1 的网络结构

从图 5-34 可以看出, LMSD Step 1 的核心网主要设备与 2G 相比发生了如下变化。

(1) Phase 0、Phase 1 的 MSC、HLR、SCP 不见了,取而代之的是承载和控制分离的两

块：一块是控制相关的部分合在一起，成为 LMSDs，包括 MSCe、HLRe、SCPe；另一块是承载相关的部分，包括 MGW 和 MRFP。

(2) 增加了一些新的接口。其中 13 接口、14 接口、27 接口和 34 接口继续采用 Phase 0、Phase 1 阶段已有的接口规范，而 39 接口、xx、yy 以及 zz 接口则是全新的接口，制定了新的接口规范。

### 2) LMSD Step 2

LMSD Step 2 的网络结构如图 5-35 所示。

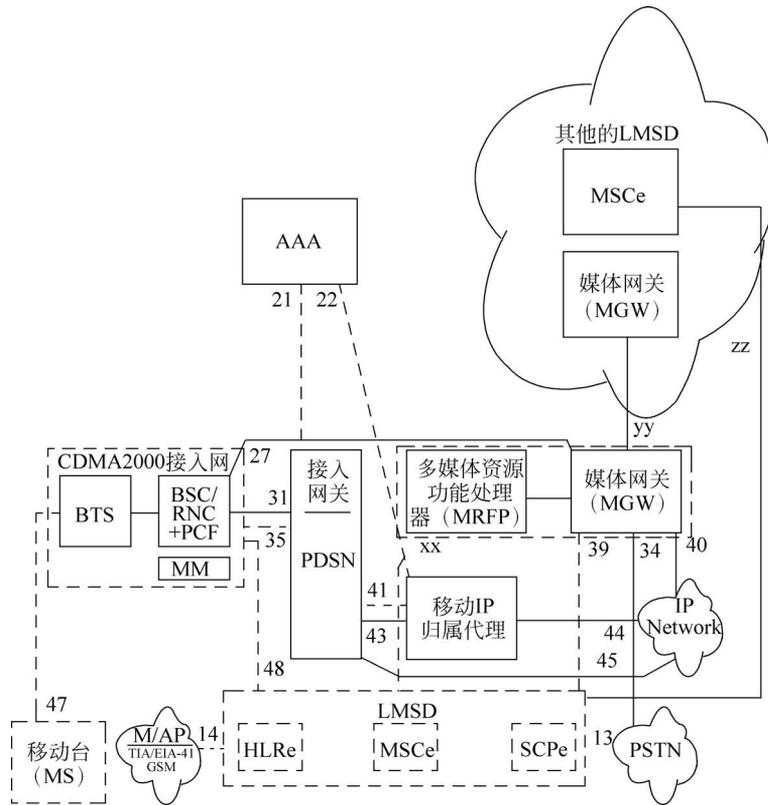


图 5-35 LMSD Step 2 的网络结构

从图 5-35 中可以看出，LMSD Step 2 阶段只是增加了 PS 域的一些网元；但在 CS 域中并没有新增网元，只是功能上有所扩展。

- (1) 支持 3GPP2 参考点 48 (CDMA 2000 接入网和 LMSD MSCe 之间的信令)，即 A1p 接口。
- (2) 支持 3GPP2 参考点 27 (CDMA 2000 接入网和 MGW 之间的承载业务)，即 A2p 接口。
- (3) 支持 TrFO (无码转换器操作)/RTO (极少码转换器操作)。

为了保护运营商的投资，保证网络平滑演进，在 LMSD 阶段，2G 的 BSS 通过 A1 接口和 A2 接口接入 3G 核心网中，A1 和 A2 接口均基于 TDM 传输技术，3G 基站系统通过 A1p 接口和 A2p 接口接入 3G 核心网系统中，A1p 和 A2p 接口均基于 IP 传输技术。当 2G 基站系统接入核心网时，具体实现方案可以采用 MGW 内置信令网关功能，A1 接口的 BSAP 信令在 MGW 和 MSCe 之间通过 IP 承载传输。

### 3) LMSD Step n

LMSD Step n 是向 MMD 域演进的最后一步，引入了与 MMD 域相同的网络实体和架

构,同时支持传统的移动台。这一阶段的网络全网支持基于 IP 的传输方式,并采用更高传输效率的 TrFO/RTO 等功能。该阶段的网络结构比较复杂,其网络实体可以分成业务相关的实体(OSA 应用服务器、SIP 应用服务器等)、IMS 相关的实体(如 CSCF、MRFC、MRFP、MGW 和 PDF 等)、核心网 PS 域(如 AGW、FA 等)、核心网 CS 域(LMSDS)和 RAN(如 BTS、BSC/PCF 等)。LMSD Step *n* 的核心网络支持基于 IP 传输的信令和载体接口。网络支持传统的 IS41D 网络的业务以及语音和其他数据业务之间的交互(如语音优先、呼叫等待等),该阶段下的网络支持与传统的 IS41D 网络之间的漫游和切换等操作。LMSD Step *n* 的核心网具有如下主要特征。

- (1) 信令和承载分离。
- (2) 信令和承载将基于 IP 传输。
- (3) 支持开放的业务架构,提供新的基于 IP 的业务。

LMSD Step *n* 网络结构如图 5-36 所示。

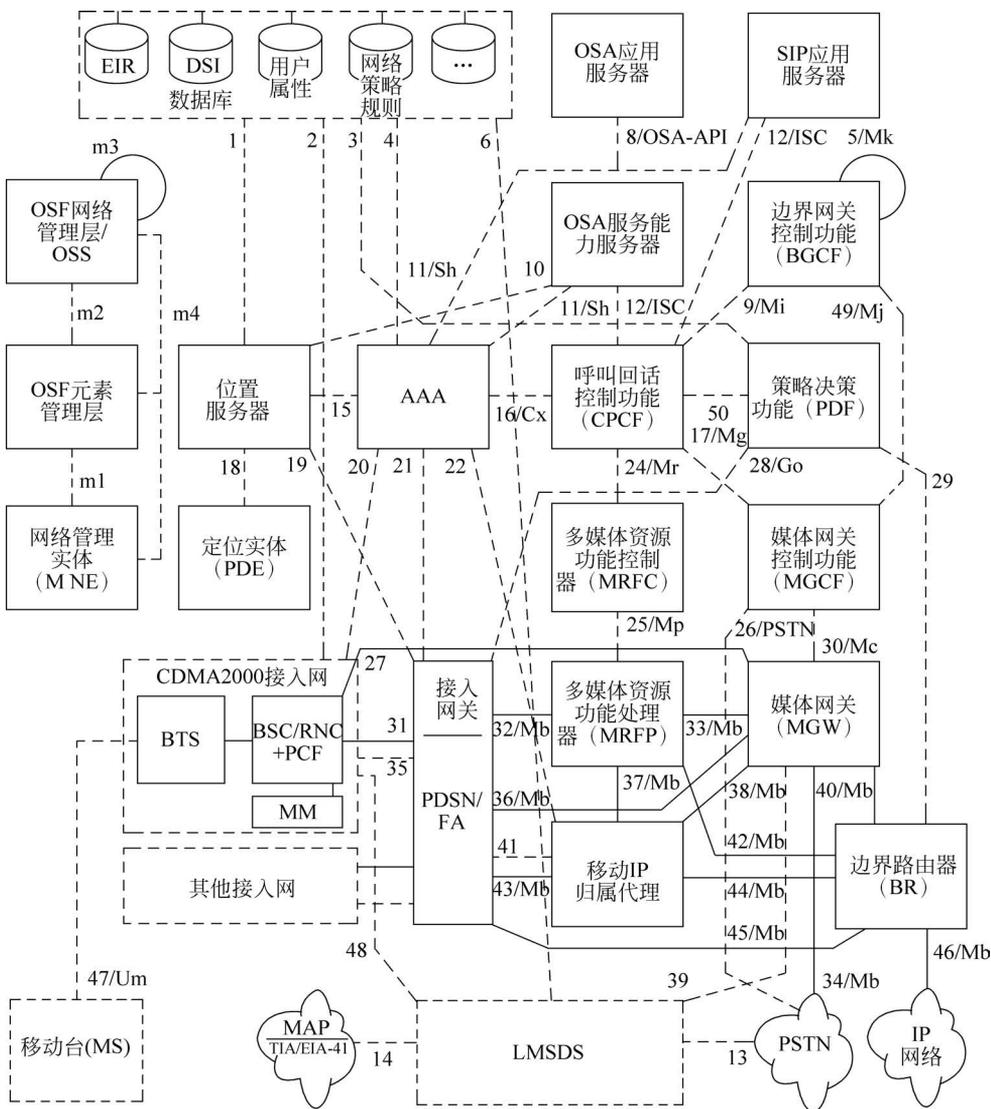


图 5-36 LMSD Step *n* 的网络结构

### 5. Phase 3

Phase 3(阶段 3)又称为多媒体域阶段,即 MMD 阶段,包含两个子系统,即分组数据子系统(PDS)和 IMS。PDS 为 IMS 提供可靠的 IP 承载通道;IMS 为 CDMA 2000 网络提供丰富多彩的移动多媒体相关业务。在 Phase 3,已经彻底抛弃了 LMSDS。其网络结构如图 5-37 所示。Phase 3 的网络是向 ALL-IP 网络演进路线的终点,该阶段以实现基于 IP 的空中接口为标志,而最终达到全网实现基于 IP 传输。Phase 3 的发展也可以分成几个步骤,其网络结构与 LMSD Step *n* 的网络基本相同,只是没有 LMSDS 部分。

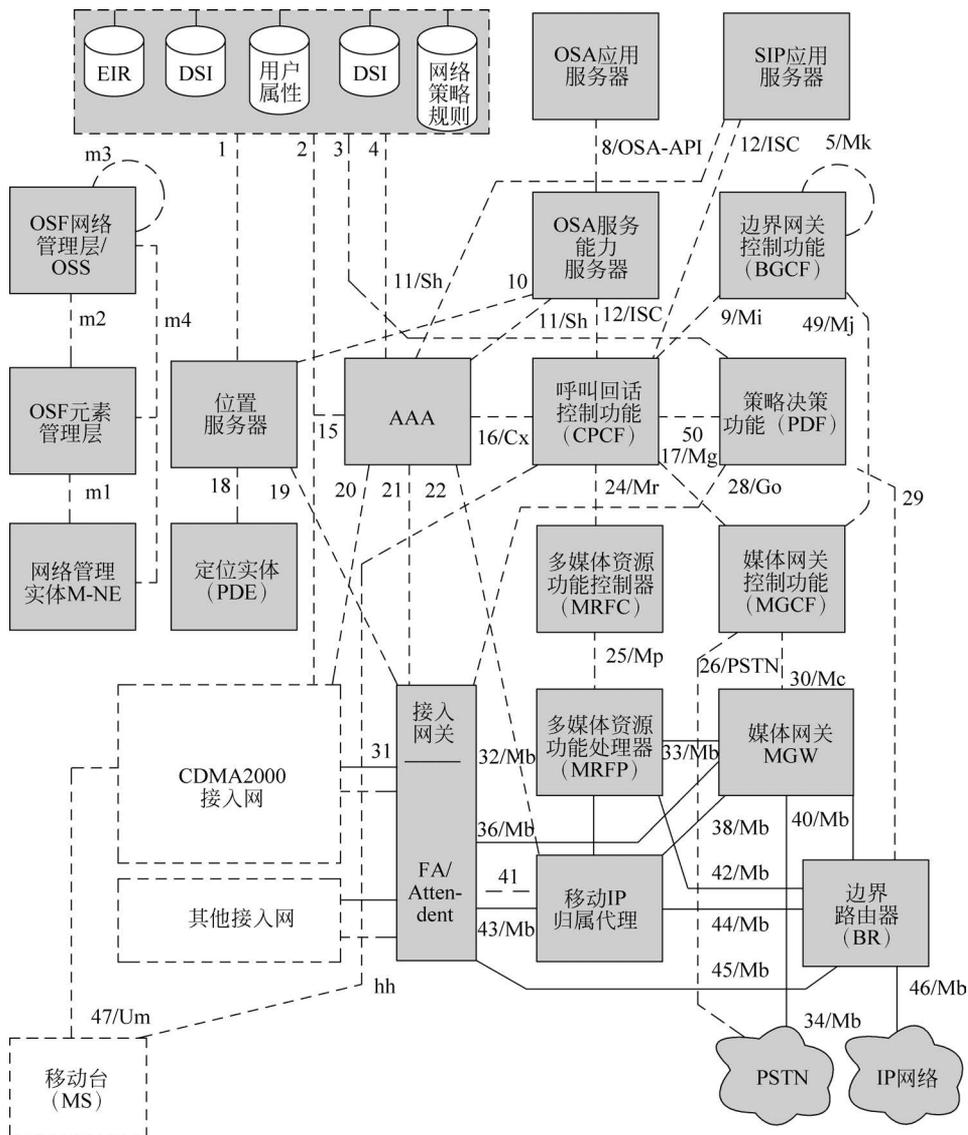


图 5-37 MMD 的网络结构

(1) 核心网。Phase 3 的网络将支持 3GPP2 的 MMD/IMS 规范系列——X. P0013,并支持基于 IP 的多媒体业务。对于传统移动台的支持,Phase 3 的网络可以通过 Phase 2 的 LMSDS(或更早阶段的网络)实现。

(2) 无线接入网。在 Phase 3 中,用于支持 LMSD 的接入网将支持基于 IP 传输的信令链路和媒体流,用于支持 IMS 的接入网在业务和 QoS 方面将具有更强的功能。

(3) 空中接口。Phase 3 中的空中接口,只支持基于 IP 传输的信令和承载。

## 5.4 TD-SCDMA 系统

### 5.4.1 概述

#### 1. TD-SCDMA 的发展与现状

TD-SCDMA 的含意是时分同步码分多址接入,是 ITU 发布的 3G 标准之一,它也是第一个由中国提出、拥有自主知识产权、被国际上广泛接受和认可的无线通信国际标准。自 TD-SCDMA 成为 3G 正式标准十几年来,中国的通信研究机构、标准化组织、生产商与运营商在政府的大力支持下对 TD-SCDMA 的技术研究、标准制定、产品开发和商用推动进行了不懈的努力,也取得了丰硕的成果。2000 年在人民大会堂宣布成立了“TD-SCDMA 技术论坛”(2009 年更名为“TD 技术论坛”)组织,其国内外成员众多,该组织在开展国际技术合作与交流方面作出了突出贡献;2002 年同样是在人民大会堂宣布成立了“TD-SCDMA 产业联盟”,最初的成员是 8 家,2008 年 7 月随着中国移动等 10 家通信产业关键企业的加入,组织发展迅速,现有上百家企业成员,覆盖了 TD-SCDMA 产业链从系统、芯片、终端到测试仪表的各个环节,该组织在 TD-SCDMA 的研发与产业化进程中发挥了组织协调作用。

由于 TD-SCDMA 的成熟度较其他两个 3G 标准要差,因此其产业化进程相对缓慢。TD-SCDMA 采用 TDD 模式,具有频谱效率高的独特优势。与此同时,它采用了大量的新技术,在技术与性能上与 WCDMA 和 CDMA 2000 相比并未显示出明显的劣势,再加上中国政府的全力支持和中国巨大的市场需求,TD-SCDMA 已在 3G 市场上占有一席之地。TD-SCDMA 网络在全球范围内得到了部署,截至 2014 年,中国移动的 TD-SCDMA 用户数已突破 2 亿,正全面使用 TD-SCDMA 增强型技术。

#### 2. TD-SCDMA 的主要特点

TD-SCDMA 综合了 TDD 和 CDMA 的技术优势,具有灵活的空中接口,采用了智能天线等诸多先进技术,因而在系统容量、频谱利用率和抗干扰能力等方面具有很强的优势。TD-SCDMA 的主要特点表现在如下几方面。

(1) 采用 TDD 模式并拥有 TDD 模式系统的优点。TD-SCDMA 系统采用 TDD 工作模式,其上下行共享一个频带,仅需要 1.6MHz 的最小带宽,若系统带宽为 5MHz,则支持 3 个载波,就可以在一个地区组成蜂窝网运营,频谱使用非常灵活,频谱利用率也很高;由于 TDD 系统上下行使用相同载波频率,可以通过对上行链路的估值获得上下行电波传播特性,便于使用诸如智能天线、预 Rake 接收等技术以提高系统性能;TD-SCDMA 由于其特有的帧结构和 TDD 工作模式,可以根据业务的不同而任意调整上下行时隙转换点,适用于不对称的上下行数据传输速率,尤其适合 IP 分组型数据业务。这里需要说明的是,TDD 也有其固有的缺点,由于采用不连续发送和接收,因而在对抗多径衰落和多普勒频移方面不如 FDD。但在 TD-SCDMA 系统中,由于采用智能天线技术加上联合检测技术克服了 TDD 模式的缺点,在小区覆盖方面和 WCDMA 相当,支持的移动速度也达到 250km/h。

(2) 上行同步。在 CDMA 移动通信系统中,下行链路的主径都是同步的。同步 CDMA

指上行同步,要求来自不同用户终端的上行信号(每帧)能同步到达基站,上行链路各个用户发出的信号在基站解调器处完全同步。在 TD-SCDMA 系统中,上行同步是基于帧结构来实现的,并使用一套开环和闭环控制的技术来保持。同步 CDMA 可以使正交扩频码的各个码道在解扩时是完全正交的,相互间不会产生多址干扰,克服了异步 CDMA 多址技术由于每个移动台发射的不同码道的信号到达基站的时间的不同而造成的码信道非正交所带来的干扰问题,提高了 TD-SCDMA 系统的容量和频谱利用率,还可以简化硬件电路,降低成本。

(3) 接力切换。GSM 等传统移动通信系统在用户终端切换中都采用硬切换,对数据传输是不利的。IS-95 CDMA 系统采用了软切换,是一个大的进步。但采用软切换要付出占用更多网络资源及无线信道作为代价,特别当所有无线信道资源都可以作为业务使用时,使用软切换的代价就太高了。

接力切换的概念是充分利用 TDD 模式的特点,即不连续接收和发射。另外。由于在 TDD 系统中,上下行链路的电波传播特性相同,可以通过开环控制实现同步。这样,当终端在切换前,首先和目标基站实现同步,并获得开环测量的功率和同步所需要的参数。切换时,原基站和目标基站同时和此终端通信(通断几乎同时),在不产生任何中断情况下就实现了切换。这样,接力切换具有软切换的主要优点,但又克服了软切换的缺点;而且接力切换可以在工作载波频率不同的基站间进行,比软切换的适用范围更广了。

(4) 动态信道分配(DCA)。TDD 系统中的动态信道分配是一项重要技术,它不是将无线资源固定分配给小区,而是根据需要进行集中分配使用。TD-SCDMA 系统中的动态信道分配技术分为慢速 DCA 和快速 DCA 两种。慢速 DCA 根据小区内业务的不对称性的变化,动态地划分上下行时隙,使上下行时隙的传输能力和上下行业务负载的比例关系相匹配,以获得最佳的频谱效率;快速 DCA 为申请接入的用户分配满足要求的无线信道资源,并根据系统状态对已分配的资源进行调整。另外,在 TD-SCDMA 系统中,将 DCA 和智能天线波束赋形结合进行考虑,部分引入空分多址(SDMA)概念,将使 DCA 的手段大大增强,这对相邻小区使用不同上下行比例业务有非常明显的效果。

(5) 使用新技术提高系统性能。TD-SCDMA 系统使用了智能天线技术、联合检测技术、空时编码技术和软件无线电技术等许多移动通信中先进的技术来提高系统性能,这既是为了维持系统的先进性,也是为了克服系统固有缺点必须采取的措施(比如载波码片速率不高,高速率业务时扩频增益小,抗干扰能力下降;再比如 TDD 模式抗多径衰落能力差等)。这些新技术在其他两个 3G 系统中是可选技术,而在 TD-SCDMA 系统中是写进标准中的必选技术。

### 3. TD-SCDMA 的系统结构

TD-SCDMA 系统作为 ITU 第三代移动通信标准之一,其网络结构遵循 ITU 统一要求,通过 3GPP 组织内融合后,TD-SCDMA 与 WCDMA 的网络结构基本相同(请参阅 5.2 节),相应接口定义也基本一致,但接口的部分功能和信令有一些差异,特别是空中接口的物理层,两个标准各有自身的特色。

3GPP 移动通信网按照其功能划分由四部分,即用户识别模块域、移动设备域、无线接入网域和核心网域组成,如图 5-38 所示。这种采用模块化结构的网络设计是 IMT-2000 的一大特点,它不仅允许符合 IMT-2000 家族概念的网络设备接入系统,而且可以方便地通过一组标准化接口将各种不同的现有网络与 IMT-2000 的组件连在一起,因此,这也为网络运

营商指出了一条向 IMT-2000 演化的途径。

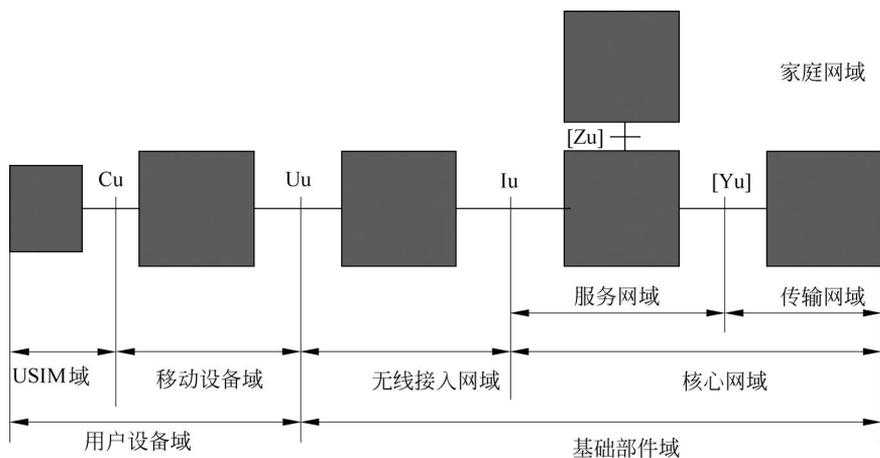


图 5-38 3GPP 的网络结构与功能域

#### 4. TD-SCDMA 的演进路线

因为技术和市场的不确定因素,TD-SCDMA 的标准制定与其他两种 3G 标准相比,思路不够明确,方案不够完善,但基本方向还是确定的。

3GPP 在制定 R4 版本时将 TD-SCDMA 列入为它的可选无线接入标准,从此 TD-SCDMA 和 WCDMA 演进就基本处于同步状态。与 WCDMA 一样,TD-SCDMA 在 R5 版本中推出了 HSDPA 技术。采用 HSDPA 后,TD-SCDMA 增加了 1 种传输信道、3 种物理信道,还增加了 16QAM 调制技术。采用 HSDPA 技术可以让 TD-SCDMA 系统下行链路的数据传输速率有很大的提高,单载波支持数据传输速率达到 2.8Mb/s。WCDMA 在 R6 版本中完成了 HSUPA 标准的制定并引入了 MBMS,TD-SCDMA 在这方面的技术研究较晚,一直到 2007 年 9 月才在 R7 中完成 TD-SCDMA 的 HSUPA 和 MBMS 的标准制定;同样地,WCDMA 已在 R7 中基本完成 HSPA+(HSPA 增强技术,HSPA 是 HSDPA 和 HSUPA 的合称)标准的制定,TD-SCDMA 在 R8 中才完成这一标准的制定工作。TD-SCDMA 最后将进入 TD-SCDMA LTE(TD-SCDMA 长期演进阶段)。

### 5.4.2 TD-SCDMA 的空中接口

#### 1. TD-SCDMA 空中接口的结构

TD-SCDMA 系统的空中接口,即 UE 和 UTRAN 之间的 Uu 接口,主要由物理层(L1)、数据链路层(L2)和网络层组成,如图 5-39 所示。

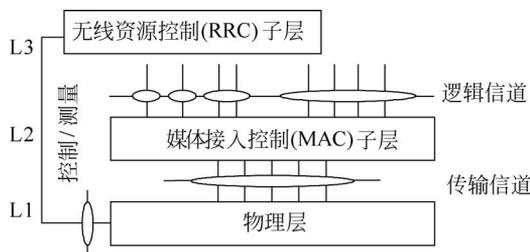


图 5-39 TD-SCDMA 系统的空中接口结构



微课视频 20

L2 又由 MAC 子层、RLC 子层、PDCP 子层和 BMC 子层组成；而 L3 由 RRC 子层、MM 子层和 CM 子层组成。总体来说，TD-SCDMA 的空中接口各子层功能与协议和 WCDMA 的空中接口是基本相同的，区别就在物理层上。

## 2. 信道对应关系

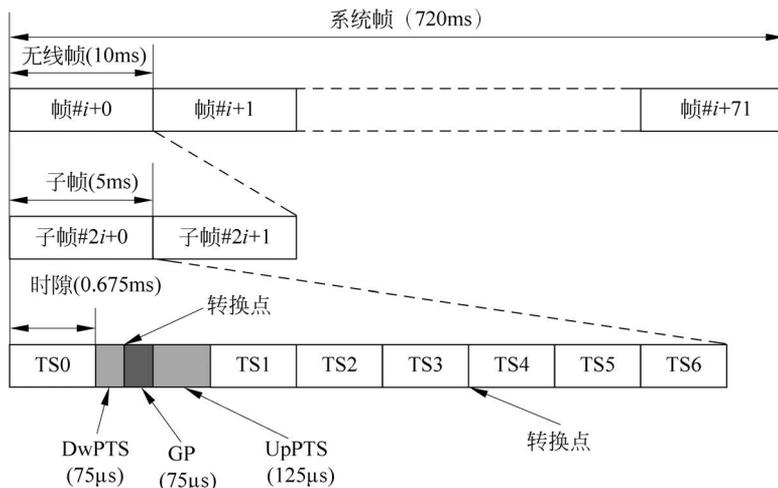
在 TD-SCDMA 系统中，定义了逻辑信道、传输信道和物理信道。具体的信道类型和 WCDMA 基本相同，逻辑信道增加了共享控制信道(SHCCH)；物理信道增加了下行导频信道(DwPCH)、上行导频信道(U<sub>p</sub>PCH)和快速物理接入信道(FPACH)；传输信道没有 WCDMA 特有的公共分组信道(CPCH)，但增加了 TD-SCDMA 特有的上行共享信道(USCH)。逻辑信道和传输信道的对应关系和 WCDMA 基本相同，而 TD-SCDMA 传输信道和物理信道的映射关系如表 5-7 所示。

表 5-7 TD-SCDMA 传输信道和物理信道的映射关系

传输信道	物理信道
专用信道(DCH)	专用物理信道(DPCH)
广播信道(BCH)	主公共控制物理信道(P-CCPCH)
寻呼信道(PCH)	主公共控制物理信道(P-CCPCH)
	辅助公共控制物理信道(S-CCPCH)
前向接入信道(FACH)	主公共控制物理信道(P-CCPCH)
	辅助公共控制物理信道(S-CCPCH)
随机接入信道(RACH)	物理随机接入信道(PRACH)
上行共享信道(USCH)	物理上行共享信道(PUSCH)
下行共享信道(DSCH)	物理下行共享信道(PDSCH)
	下行导频信道(DwPCH)
	上行导频信道(U <sub>p</sub> PCH)
	寻呼指示信道(PICH)
	快速物理接入信道(FPACH)
高速下行共享信道(HS-DSCH)	高速物理下行共享信道(HS-PDSCH)
	HS-DSCCH 共享控制信道
	HS-DSTCH 共享信息信道

## 3. 物理信道及其帧结构

TD-SCDMA 系统中，物理信道是由频率、时隙、信道码、训练序列位移和无线帧分配等诸多参数来共同定义的。其扩频带宽为 1.6MHz，码片速率为 1.28Mb/s；信道码采用 OVSF 码，扩频因子取值范围为 1~16，不算太大，这是由于系统 TD-SCDMA 采用了联合检测技术，而联合检测算法的复杂度随扩频信道数的 2 次方以上的速度增加，为使联合检测算法的复杂度适中，扩频因子取值不宜过高；物理信道在时间上采用系统帧(超帧)、无线帧、子帧和时隙/码字这样一个特殊的 4 层式的结构。一个系统帧号由 72 个无线帧组成，时长为 720ms；一个无线帧由 2 个 5ms 的子帧组成，时长为 10ms；每个子帧又是由 3 个特殊时隙(下行导频时隙 DwPTS、上行导频时隙 U<sub>p</sub>PTS 和保护间隔 GP)和 7 个 675μs 的常规时隙(TS0~TS6)组成，时长为 5ms。其物理信道帧结构如图 5-40 所示。虽然和 WCDMA 一样采用了 10ms 的无线帧，但无线帧又划分为 2 个完全相同的子帧，其目的是支持智能天线的使用。



说明：传码率为1.28Mb/s时，每无线帧为6400chip，每时隙为864 chip，每DwPTS为96 chip，每UpPTS为160chip，每GP为96 chip

图 5-40 TD-SCDMA 的物理信道帧结构

每个子帧中，UpPTS 和 DwPTS 是为上下行导频和同步而设计的，主保护时隙 GP 为发射和接收转换提供保护间隔，防止上下行信号相互之间的干扰。在 7 个常规时隙中，TS0 总是分给下行，而 TS1 总是分给上行。上行时隙和下行时隙之间由转换点分开，一个子帧有两个转换点(DL 到 UL 和 UL 到 DL)。通过灵活配置上下行时隙的个数，可使 TD-SCDMA 系统适用于上下行对称和非对称业务模式。其子帧结构如图 5-41 所示，分别给出了上下行时隙对称和不对称分配的示例。

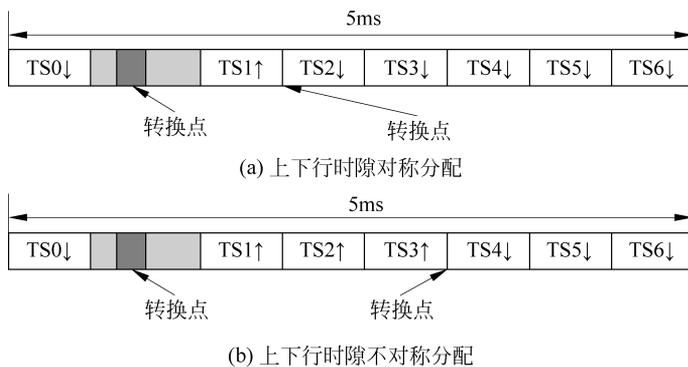


图 5-41 TD-SCDMA 的子帧结构

#### 4. 特殊时隙结构

DwPTS 由 Node B 以最大功率在全方向或在某一扇区上发射，该时隙通常由长为 64chip 的下行同步序列 (SYNC-DL) 和长为 32chip 的保护间隔 (GP) 组成，其时隙结构如图 5-42(a)所示。图中 SYNC-DL 是一组 PN 码，用于区分相邻小区。系统中定义了 32 个码组，每组对应一个 SYNC-DL 序列，SYNC-DL PN 码集在蜂窝网络中可以复用。将 DwPTS 放在单独的时隙，便于下行同步的迅速获取，同时也可以减小对其他下行信号的干扰。

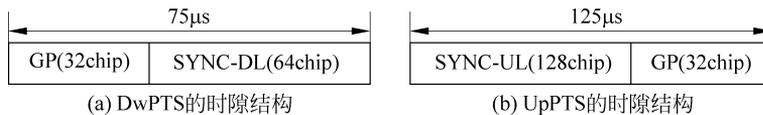


图 5-42 DwPTS 和 UpPTS 的时隙结构

UpPTS 时隙通常由长为 128chip 的上行同步序列(SYNC-UL)和长为 32chip 的保护间隔组成,其时隙结构如图 5-42(b)所示。图中 SYNC-UL 是一组 PN 码,用于在接入过程中区分不同的 UE。当 UE 处于空中登记和随机接入状态时,它将首先发射 UpPTS,当得到网络的应答后,发射 RACH。

### 5. 突发结构

通常,将时分系统中的一个基本业务单元,即一个常规时隙称为一个突发,TD-SCDMA 系统的突发结构如图 5-43 所示,将两个长为 352chip 的数据符号安放在突发的两边;中间设计了长为 144chip 的中间码(训练序列),应用于同步及信道估计,是为使用联合检测而准备的。中间码设计时已达到要求的码片速率,不需要进行扩频和加扰;数据符号数和扩频因子有关。

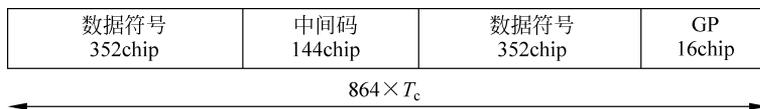


图 5-43 TD-SCDMA 系统的突发结构

TD-SCDMA 系统的突发结构传送的物理层控制信令包括传输格式合成指示(TFCI)、发射功率控制(TPC)和同步偏移(SS)。物理层控制信令在相应物理信道的数据部分发送,即物理层控制信令和数据比特具有相同的扩频操作。由于物理层信令缺少保护和纠错,因此将其放在靠近中间码两端的数据部分。物理层控制信令的结构如图 5-44 所示,图中的 SS 和 TPC 部分可以不发送。

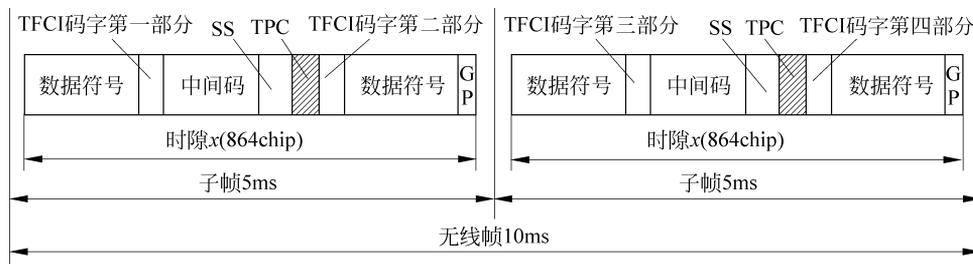


图 5-44 物理层控制信令的结构

对于每个用户,TFCI 信息将在每 10ms 无线帧里发送一次。编码后的 TFCI 符号分为 4 部分,在子帧内和数据块内都是均匀分布的。TFCI 的发送是由高层信令配置的。

对于每个用户,TPC 信息在每 5ms 子帧里发送一次,这使得 TD-SCDMA 系统可以进行快速功率控制。

对于每个用户,SS 信息在每 5ms 子帧里发送一次。SS 用于命令终端每  $M$  帧进行一次时序调整,调整步长为  $(k/8)T_c$ 。其中,  $T_c$  为码片周期,  $M$  值和  $k$  值由网络设置,并在小区中进行广播。上行突发中没有 SS 信息,但是 SS 位置予以保留,以备将来使用。

## 6. 扩频与调制

TD-SCDMA 系统的数据调制通常采用 QPSK,在提供 2Mb/s 业务时采用了 8PSK 调制方式,为支持 HSDPA 下行可以用 16QAM。扩频后的码片速率为 1.28Mc/s,扩频因子的范围是 1~16,调制符号的速率为 80.0ks/s~1.28Ms/s。由于扩频采用 OVSF 码,再加上采用了上行同步技术,码的正交性较好,从而使信道间干扰较小。码片经扩频与调制以后,需经脉冲成形滤波器  $RC_0(t)$  成形,并且在发送方和接收方都要使用,该滤波器采用的是平方根升余弦滤波器,其冲激响应为

$$RC_0(t) = \frac{\sin\left[\pi\frac{t}{T_c}(1-a)\right] + 4a\frac{t}{T_c}\cos\left[\pi\frac{t}{T_c}(1+a)\right]}{\pi\frac{t}{T_c}\left[1 - \left(4a\frac{t}{T_c}\right)^2\right]} \quad (5-5)$$

式中,滚降系数  $a=0.22$ ,码片周期  $T_c=0.78125\mu\text{s}$ 。

## 7. 链路功率控制

TD-SCDMA 系统中采用的功率控制方案是上行采用开环+闭环功率控制,下行采用闭环功率控制,其功率控制参数如表 5-8 所示。

表 5-8 TD-SCDMA 的功率控制参数

参 数	上 行	下 行
功率控制速度	可变 闭环: 0~200 次/s 开环: 延时 200~3575 $\mu\text{s}$	可变 闭环: 0~200 次/s
步长	1dB、2dB、3dB(闭环)	1dB、2dB、3dB(闭环)

与 WCDMA、CDMA 2000 相比,其功率控制速度有所降低,这是因为 TD-SCDMA 系统采用了智能天线技术和上行 CDMA 同步技术后同信道干扰降低,对功率控制的要求有所降低,所以其功率控制速度不需要太高。

## 5.4.3 TD-SCDMA 的关键技术

TD-SCDMA 系统中的关键技术在本章 5.4.1 节做了一般性介绍,这一节主要介绍其不同于其他系统的关键技术。

### 1. 智能天线技术

#### 1) TD-SCDMA 系统采用智能天线技术的必要性

智能天线技术是目前 TD-SCDMA 标准的必选技术,也是其具有优势的核心技术之一。TD-SCDMA 系统很多物理层方面的设计(如帧结构)就是依赖智能天线实现的,如果不采用智能天线,整个 TD-SCDMA 系统标准必须重新设计。由于采用了智能天线技术,TD-SCDMA 系统可将频分复用、时分复用、码分复用和空分复用交叠应用。TD-SCDMA 系统中 6 大关键技术(智能天线技术、联合检测技术、动态信道分配技术、接力切换技术、功率控制技术和上行同步技术)中,其他 5 项技术都要与智能天线技术联合应用才能发挥出最大效果。

#### 2) 智能天线技术原理

智能天线技术的基本原理是:天线以多个高增益窄波束动态地跟踪多个期望用户,在



接收模式下,来自窄波束之外的信号被抑制;在发射模式下,能使期望用户接收的信号功率最大,同时使窄波束照射范围以外的非期望用户受到的干扰最小。智能天线可利用用户空间位置的不同来区分不同用户,完成空分复用。

根据采用的天线方向图形状,可以将智能天线分为两类:自适应智能天线和多波束智能天线。多波束智能天线的方向图形状不变,利用多个并行波束覆盖整个用户区,每个波束的指向是固定的。当用户在小区中移动时,它通过测向确定用户信号的到达方向,然后根据信号的到达方向选取合适的阵元加权,将方向图的主瓣指向用户方向,从而提高用户的信噪比。这类智能天线简单、稳定且响应速度快,但智能性不够,因此只作接收天线用。

自适应智能天线是智能天线的主要类型,其方向图没有固定的形状,随着信号及干扰而变化,可实现最佳接收与发送。图 5-45 给出了自适应智能天线基本原理图,自适应智能天线系统包括天线阵列、模/数转换和波束形成网络 3 部分。图中介绍的是智能天线接收时的结构,当用它进行发射时,结构稍有变化,加权器和加权网络置于天线之前,也没有相加合并器。天线阵列一般采用 4~16 天线阵元结构,阵元间距为半个波长。天线阵元分布方式有直线形、圆形和平面形。波束形成网络主要是由数字信号处理器依据一定的算法,即准则(主要有最小均方误差准则、最大信噪比准则和最小方差准则)给出最佳加权系数  $w_1, w_2, \dots, w_n$ ,从而形成符合要求的最佳波束。

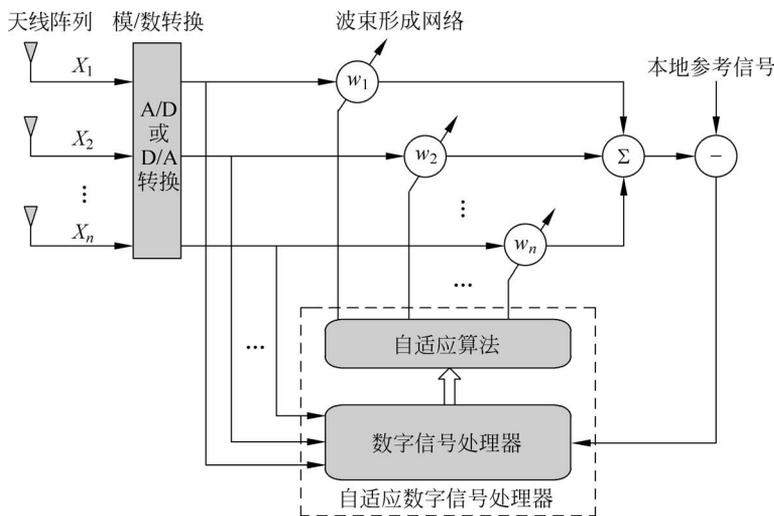


图 5-45 自适应智能天线的原理图

在实际应用中,环境是不断变化的,要求实时地更新权矢量,因此需要利用自适应算法来递归地获得实时的权矢量,而自适应算法不仅决定了算法的收敛速度,而且决定了算法硬件实现的复杂度,由此可见,选择合适的自适应算法对智能天线系统来说是很重要的。自适应算法分为非盲算法、盲算法和半盲算法。非盲算法是指需要借助参考信号(导频序列或导频信道)的算法,此时接收端知道发送的是什么,按一定准则确定或逐渐调整权值,使智能天线输出与已知输入最大相关。非盲算法主要有最小均方误差算法(LMS)和递归最小二乘算法(RLS)等。盲算法是无须发射端传送已知的导频信号,一般利用调制信号本身固有的、与具体承载的信息无关的一些特征,如恒模、子空间、有限符号集和循环平稳等,并调整权值,使输出满足这种特性,常见的是基于梯度的使用不同约束量的算法。非盲算法相对盲算

法而言,通常误差较小,收敛速度也较快,但常常浪费一定的系统资源。将二者结合产生的半盲算法,先用非盲算法确定初始权值,再用盲算法进行跟踪和调整,常常达到更好的效果。

### 3) 智能天线技术在 TD-SCDMA 系统中的应用

TD-SCDMA 系统由于采用 TDD 模式,上下行频率一致,可直接测量上行信号强度并对下行信号的传播进行估计,不需要采用反馈闭环方案测量下行传播特性;另外,TD-SCDMA 系统采用了短帧结构,且子帧中安排了训练序列用于智能天线。所有这些特性都有利于 TD-SCDMA 应用智能天线技术。

在现有 TD-SCDMA 商用系统基站采用的智能天线中,天线阵列一般采用如图 5-46(a)所示的 8 个天线单元组成的圆阵(用于全向赋形)或如图 5-46(b)所示的 8 个天线单元组成的线阵(用于定向赋形),各阵元间距为  $\lambda/2$ 。其处理过程如图 5-47 所示。从上行链路来看,天线阵 RF 前端接收到在第一个时隙来自各个终端

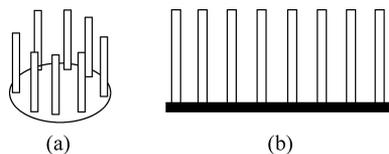


图 5-46 8 天线单元组成的圆阵和线阵示意图

的上行信号,这个组合信号被放大、滤波、下变频、A/D 转换后,数字合路器完成上行同步、解扩等处理,然后提取每个用户的空间参数,并进行上行波束成型(空间滤波)。下行链路大致是上行链路的逆过程,下行波束成型用上行链路提取的空间参数,并在第 2 个时隙将要发送的信号进行波束成形。

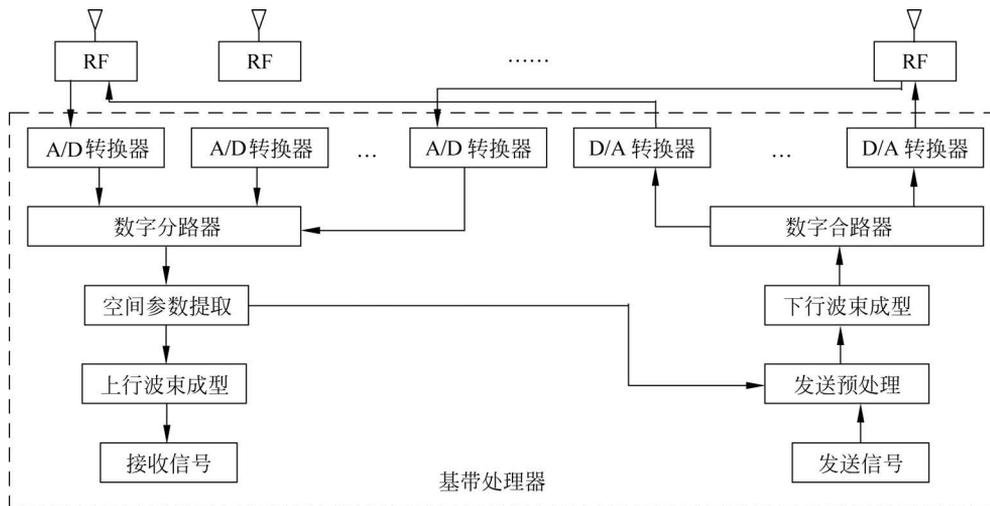


图 5-47 TD-SCDMA 系统基站采用的智能天线的处理过程

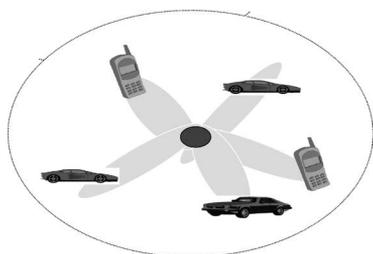


图 5-48 TD-SCDMA 智能天线小区可完成的覆盖

采用了智能天线的小区可完成如图 5-48 所示的覆盖,智能天线的主要作用有: ①提高基站接收机的灵敏度; ②提高基站发射机的等效发射功率; ③降低系统的干扰,增加了 CDMA 系统的容量; ④改进小区的覆盖,并提高了频谱利用率; ⑤降低无线基站的成本; ⑥实现移动台定位。

智能天线的引入可以极大地提升 TD-SCDMA 系统的性能,但对系统其他技术的控制算法和控制过程也带

来了影响。在 DCA 进行信道分配时,要尽量把相同方向上的用户分散到不同时隙中,使得在同一个时隙内的用户分布在不同的方向上,这样可以充分发挥智能天线的空分功效,使多址干扰降至最小。但要达到这一目的,需要增加 DCA 对用户空间信息的获取和处理能力。引入智能天线后,系统分组调度算法发生改变,新的调度方式主要将包括时分与空分结合方式、码分与空分结合方式、时分-码分-空分三者相结合的混合方式。智能天线对功率控制的影响表现在:①功率控制流程发生变化;②功率控制精度可降低;③功率控制的平衡点方程变得复杂。智能天线为切换提供一些有用的位置参考信息,可以提高系统资源利用率、缩短切换时间、降低掉话率、减少信令交互、提高切换成功率,另外,还可以采用接力切换技术。当然,智能天线也增加了切换的复杂性,如在物理信道分配的过程中,当发生冲突需要进行信道调整和切换时,由于判决维数增加,使用的切换算法要比只有一种资源的情况下复杂,用户的切换管理也要复杂得多。

## 2. 软件无线电技术

软件无线电技术是在通用芯片上用软件实现专用芯片的功能。其优势有:①可克服微电子技术的不足,通过软件方式,灵活完成硬件/专用 ASIC 的功能,在同一硬件平台上利用软件处理基带信号,通过加载不同的软件,可实现不同的业务性能;②系统增加功能通过软件升级来实现,具有良好的灵活性及可编程性,对环境的适应性好,不会老化;③可代替昂贵的硬件电路,实现复杂的功能,减少用户设备费用支出。

由于 TD-SCDMA 系统的 TDD 模式和低码片速率的特点,使得数字信号处理量大大降低,适合采用软件无线电技术。正是因为软件无线电的优势,使得 TD-SCDMA 系统在发展相对 WCDMA 和 CDMA2000 滞后的情况下,采用软件无线电技术,成功完成了试验样机和初步商用产品的开发,给 TD-SCDMA 系统的发展赢得了时间和空间。

## 3. 联合检测技术

根据对多址干扰(MAI)处理方法的不同,多用户检测(MUD)技术可以分为干扰抵消(IC)和联合检测(JD)两种。JD 的性能优于 IC,但 JD 的算法复杂度高于 IC,因此在 TD-SCDMA 中,基站采用 JD 技术,终端采用 IC 技术。联合检测技术的思想是充分利用 MAI,将所有的用户信号都分离开来,联合检测算法使用的前提是能得到所有用户的扩谱码和冲击响应,因此在 TD-SCDMA 系统中的帧结构中设置了用来进行信道估计的训练序列(Midamble),根据接收到的训练序列部分信号和已知的训练序列就可以估算出信道冲击响应,而扩谱码也是确知的,从而达到估计用户原始信号的目的。

在 TD-SCDMA 系统中,通常将联合检测技术与智能天线技术结合使用,以便发挥两者的优势,弥补各自的不足。图 5-49 是两者结合的流程示意图,这样能在上行获得分集接收的好处,下行实现波束成型。

## 4. 接力切换技术

接力切换技术是 TD-SCDMA 移动通信系统的核心技术之一,其设计思想是利用智能天线和上行同步等技术,在对 UE 的距离和方位进行定位的基础上,根据 UE 方位和距离信息作为辅助信息来判断目前 UE 是否移动到了可进行切换的相邻基站的临近区域。

### 1) 接力切换技术的特点

接力切换技术是介于硬切换和软切换之间的一种新的切换技术,与软切换相比,两者都有较高的切换成功率、较低的掉话率以及较小的上行干扰等优点,它们的不同之处在于接力

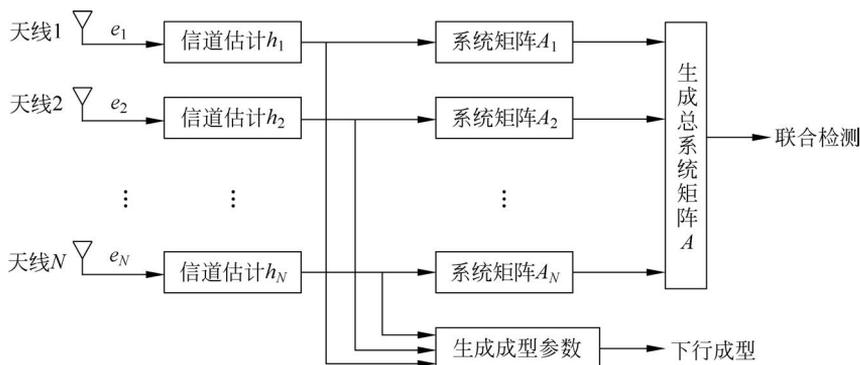


图 5-49 TD-SCDMA 联合检测技术与智能天线技术结合的流程示意图

切换并不需要同时有多个基站为一个移动台提供服务,因而克服了软切换需要占用的信道资源较多,信令复杂导致系统负荷加重,以及增加下行链路干扰等缺点;与硬切换相比,两者都具有较高的资源利用率,较为简单的算法以及系统相对较轻的信令负荷等优点,不同之处在于接力切换断开原基站和与目标基站建立通信链路几乎是同时进行的,因而克服了传统硬切换掉话率较高,切换成功率较低的缺点。接力切换的突出优点是切换高成功率和信道高利用率。接力切换可以在不同扇区的主频点间进行,也可以在不同扇区的主频点与辅频点、辅频点之间进行,有效地支持了多频点组网。

## 2) 接力切换算法

TD-SCDMA 系统中接力切换算法由切换判决准则、切换执行准则组成。

常用的具有滞后余量和限定门限的相对信号强度切换判决准则为仅允许移动台在新小区的导频信号强度比原小区导频信号强度强到一定程度(即大于滞后余量  $RSCP\_DL\_COMP$ )并且保持一定时间的情况下才进行越区切换,公式表示如下

$$PCCPCH\_RSCP_{neighbour} - PCCPCH\_RSCP_{serving} > RSCP\_DL\_COMP \quad (5-6)$$

这样可以防止由于信号波动引起的在两个小区之间的来回切换(乒乓效应)。同时仅允许移动台在当前小区的信号低于规定门限  $RSCP\_DL\_DROP$ (简称  $DROP$ ),并且新小区的信号强度高于当前小区给定的滞后余量时,才进行切换。

接力切换的判决相对于软切换来说要求比较严格,基于 TD-SCDMA 系统的特点,进行接力切换的 UE 上下行链路在与目标基站建立通信的时候是分别断开与原基站的连接,因此在满足正常通信质量的情况下,要尽可能地降低系统的切换率,表现在原服务小区(简称原小区)的  $RSCP\_DL\_DROP$  门限在保证一定的掉话率的同时尽可能地接近小区边缘的平均信号强度,而目标服务小区(简称目标小区)的  $RSCP\_DL\_ADD$  门限不能设置过高从而引起候选小区数量下降而导致掉话率过高,当然此门限亦不能过低从而失去设置此门限参数的意义。

当系统判决进行切换后,系统可以执行多种切换方式,如执行小区内切换、小区间切换、频率内切换、频率间切换、系统内切换、系统间切换等。因为不同的切换方式有不同的切换性能和复杂性,如切换率、切换成功率、切换延时和网络负荷等,一般按照小区内、小区间、RNC 内、RNC 间、系统内、系统间的顺序安排切换优先级,可以减少接口间的信令交互,减轻 RNC 的处理负担并加快切换的执行过程。在执行上述切换类型时,一般是频内切换的优先级高于频间切换的优先级。

### 3) 接力切换过程

接力切换分为 4 个过程,即测量过程、预同步过程、判决过程和执行过程,切换过程见图 5-50。

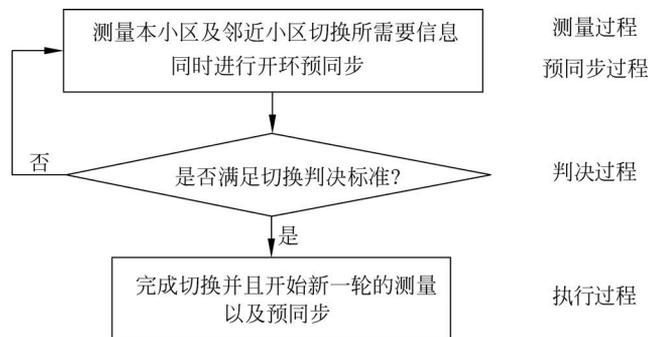


图 5-50 接力切换过程

在 UE 和基站通信过程中,UE 需要对本小区基站和相邻小区基站的导频信号强度进行测量。UE 的测量是由 RNC 指定的,可以是周期性进行,也可以由事件触发进行。

接力切换的预同步过程属于开环预同步,在 UE 对本小区基站和相邻小区基站的导频信号强度进行测量的同时记录来自各邻近小区基站的信号与来自本小区基站信号的时延差,预先取得与目标小区的同步参数,并通过开环方式保持与目标小区的同步。

接力切换的判决过程是根据各种测量信息并综合系统信息,依据一定的准则和算法判断 UE 是否应当切换和如何进行切换。

RNC 在收到 UE 的测量报告后,首先对 PCCPCH\_RSCP 最大的候选目标小区进行判断,如果大于设定的门限值 RSCP\_DL\_ADD(简称 ADD),则在此小区中进行接纳判决,反之进入下一个候选目标小区,直至最后一个候选目标小区。如果所有目标小区都不满足,则 UE 停留在原小区。目标小区确定后,RNC 根据目标小区与原小区的关系判决是硬切换(归属不同的 RNC)还是接力切换(归属同一个 RNC)。在接纳判决成功后,RNC 通知目标小区为 UE 分配无线资源并且将相关信息通知 UE。

RNC 的切换判决完成后,将执行接力切换。首先对目标小区发送无线链路建立请求。当 RNC 收到目标小区的无线链路建立完成之后,将向原小区和目标小区同时发送业务数据承载(此时目标小区并不向 UE 发送下行数据),同时 RNC 向 UE 发送物理信道重配置消息命令。

终端应根据是否携带 FPACH 信息来判断是否为接力切换,即接到切换命令后,首先判断切换类型,如果携带 FPACH 信息,则判断为硬切换,重新在目标小区做接入;如果没有携带 FPACH 信息,则判断为接力切换。

然后,UE 由原小区接收下行承载业务及信令而由目标小区发射上行的承载业务和信令。此分别收发的过程持续非常短的一段时间后,将接收来自目标小区的智能天线下行波束赋形数据,实现闭环功率和同步控制,中断和原基站的通信,完成切换过程。

## 5.5 第三代移动通信系统安全机制

### 5.5.1 3G 面临的安全威胁和攻击方法

3G 是一个在全球范围内覆盖与使用的网络系统,信息的传输既经过全开放的无线链路

亦经过开放的全球有线网络。3G 提供的业务包括语音、多媒体、数据、电子商务、电子贸易、互联网服务等多种信息,它为用户提供开放式应用程序接口以满足用户的个性化需求。网络的开放性以及无线传输的特性,使 3G 面临多种安全威胁,概括起来有如下几点。

- (1) 非法获取敏感数据来攻击系统的保密信息。
- (2) 非法操作敏感数据来攻击完整信息。
- (3) 非法访问服务。
- (4) 滥用、干扰 3G 服务降低系统服务质量或拒绝服务。
- (5) 网络或用户否认曾经发生的动作。

针对 3G 系统的攻击方法主要有针对系统核心网的攻击、针对系统无线接口的攻击和针对终端的攻击 3 种方式。

针对系统核心网的攻击手段包括以下几种。

(1) 入侵者进入网内窃听用户、信令以及控制数据,非法访问系统网络单元数据,甚至进行主动或被动流量分析。

(2) 入侵者篡改用户信令、业务数据等,或以非法身份修改通信数据或网络单元内存储的数据。

(3) 通过对在物理上或协议上的控制数据、信令数据或用户数据在网络中的传输进行异常干扰,实现网络中的拒绝服务攻击,或通过假冒某一网络单元来阻止合法用户的各种数据,干扰合法用户正常的网络服务请求。

(4) 用户否认业务费用、数据来源或接收到的其他用户的数据,网络单元否认发出信令或控制数据,否认收到其他网络单元发出的信令或控制数据。

(5) 入侵者模仿合法用户使用网络服务,或假冒服务网以利用合法用户的接入尝试获得网络服务,抑或假冒归属网以获取使他能够假冒某一方用户所需的信息。

针对 3G 系统无线接口的主要攻击方法如下。

(1) 入侵者窃听无线链路上的用户、信令和控制数据,进行流量分析;篡改无线链路上合法用户的数据和信令数据。

(2) 通过在物理上或协议上干扰用户数据、信令数据或控制数据在无线链路上的正确传输,来实现无线链路上的拒绝服务攻击。

(3) 攻击者伪装其他合法用户身份,非法访问网络,或切入用户与网络之间,进行中间攻击。

(4) 攻击者伪装成服务网络,对目标用户发身份请求,从而捕获用户明文形式的永久身份信息;压制目标用户与攻击者之间的加密流程,使之失效。

针对终端的攻击主要是攻击 USIM 和终端,主要是使用非法 USIM 或终端;非法获取其间存储的数据;篡改其中数据或窃听其间通信;以非法身份获取其间的交互信息等。

### 5.5.2 3G 系统的安全架构

为应对以上阐述的安全威胁和攻击,3G 系统所采用的安全架构如图 5-51 所示。它以 2G 安全系统为基础,保留了 2G 中被证明是必要和有效的安全功能,同时考虑了与 2G 的兼容,也增加了新的安全功能。它从 3 个层面,定义了 5 个安全特征组,每一类安全特征组针对一定的安全威胁进行设计,实现相应的安全防护。5 个安全特征组基本情况如下。

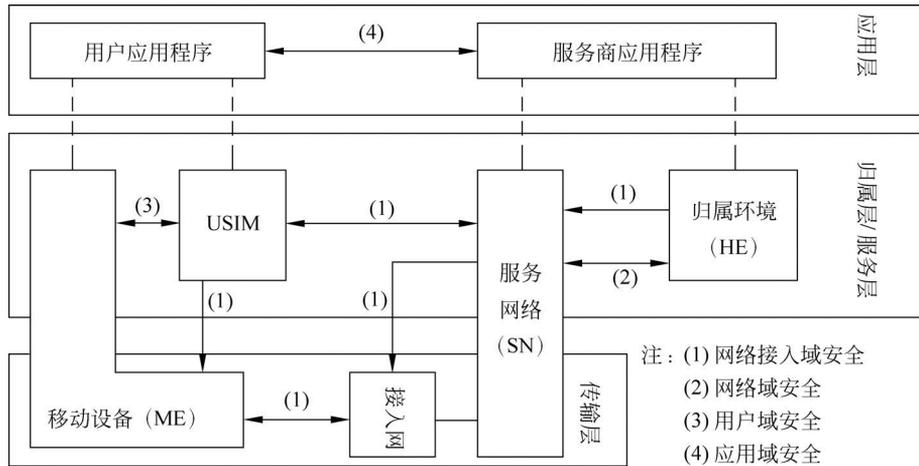


图 5-51 3G 系统所采用的安全架构

### 1. 网络接入域安全

网络接入域安全提供如下 4 个方面的安全特性。

(1) 用户标识的保密性：包括用户标识的保密、用户位置的保密以及用户的不可追踪性；

(2) 实体认证：包括用户认证和网络认证；

(3) 加密：包括加密算法协商、加密密钥协商、用户数据的加密和信令数据的加密；

(4) 数据完整性：包括完整性算法协商、完整性密钥协商、数据完整性和数据源认证。

### 2. 网络域安全

网络域安全分为以下 3 个层次。

(1) 第 1 层(密钥建立)：密钥管理中心产生并存储非对称密钥对,保存其他网络的公开密钥,产生、存储并分配用于加密信息的对称会话密钥,接收并分配来自其他网络的用于加密信息的对称会话密钥。

(2) 第 2 层(密钥分配)：为网络中的节点分配会话密钥。

(3) 第 3 层(安全通信)：使用对称密钥实现数据加密、数据源认证和数据完整性保护。

### 3. 用户域安全

用户域安全提供以下 2 个方面的安全特性。

(1) 用户到用户服务身份模块(USIM)的认证。用户接入 USIM 之前必须经过 USIM 的认证,确保接入 USIM 的用户为已授权用户。

(2) USIM 到终端的连接。确保只有授权的 USIM 才能接入终端或其他用户环境。

### 4. 应用域安全

应用域安全是指 USIM 应用程序为操作员或第三方运营商提供了创建驻留应用程序的功能,这就需要确保通过网络向 USIM 应用程序传输信息的安全性,其安全级别可由网络操作员或应用程序提供商根据需要选择。

### 5. 安全可见度与安全可配置性

安全可见度是指通常情况下,安全特性对用户是透明的。第三代移动通信系统中,对一些特定事件或按照用户需求提供了更大的安全特性操作可见度。

(1) 接入网络加密提示,通知用户是否保护传输的数据,特别在用户建立非加密的呼叫连接时进行提示。

(2) 安全级别提示,通知用户被访问网络是什么样的安全级别,特别是当用户被递交或漫游到低安全级别的网络(如 3G 到 2G)时进行提示。

安全可配置性是指用户可对安全特性进行配置。这些安全特性包括允许或不允许用户到 USIM 的认证,接收或不接收未加密的呼叫,建立或不建立非加密的呼叫,接收或拒绝使用某种加密算法。

### 5.5.3 3G 网络接入安全机制

3GPP 网络接入安全机制有 3 种:①根据临时身份(TMSI)识别;②使用永久身份(IMSI)识别;③认证和密钥协商(AKA)机制。

AKA 机制完成移动设备(ME)和网络的相互认证,并建立新的加密密钥和完整性密钥,3GPP 网络 AKA 运行过程如图 5-52 所示。AKA 机制的执行分为 2 个阶段:第 1 阶段是认证向量(AV)从归属环境(HE)到服务网络(SN)的传送;第 2 阶段是 SGSN/VLR 和移动台执行询问应答程序取得相互认证。归属环境包括 HLR 和鉴权中心(AUC)。认证向量含有与认证和密钥分配有关的敏感信息,在网络域的传送使用基于 7 号信令的 MAPsec 协议,该协议提供了数据来源认证、数据完整性、抗重放和机密性保护等功能。

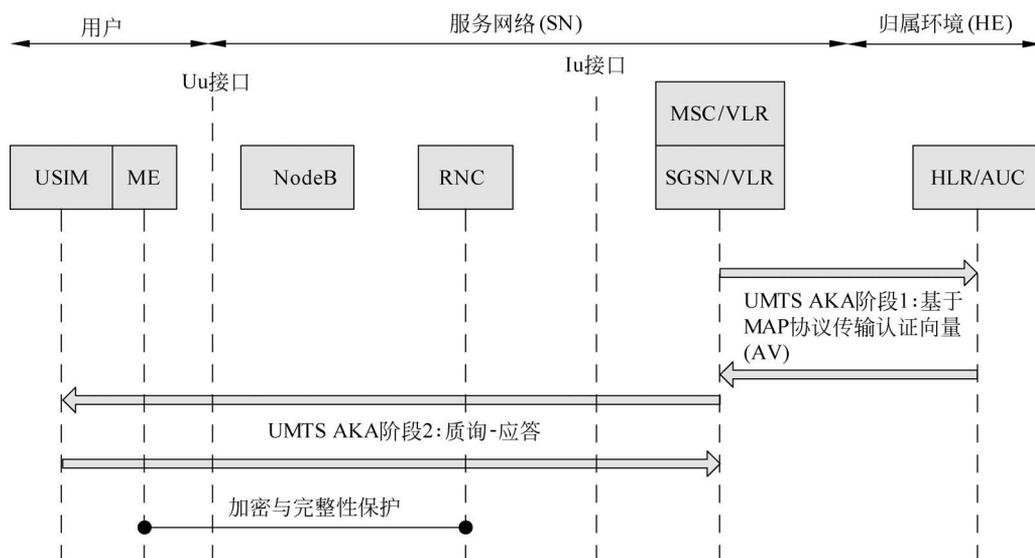


图 5-52 3GPP 网络 AKA 运行过程

3GPP 为 3G 系统定义了 12 种安全算法:  $f_0$ 、 $f_1$ 、 $f_2$ 、 $f_3$ 、 $f_4$ 、 $f_5$ 、 $f_6$ 、 $f_7$ 、 $f_8$ 、 $f_9$ 、 $f_{1^*}$ 、 $f_{5^*}$ , 应用于不同的安全服务。身份认证与密钥分配方案中移动用户登记和认证参数的调用过程与 GSM 网络基本相同,不同之处在于 3GPP 认证向量是 5 元组,包括随机数(RAND)、期望响应(XRES)、加密密钥(CK)、完整性密钥(IK)和认证令牌(AUTN),并实现了用户对网络的认证。AKA 利用  $f_0 \sim f_{5^*}$  算法,安全服务内容如表 5-9 所示,这些算法仅在鉴权中心和用户的 USIM 中执行。AKA 由 SGSN/VLR 发起,在鉴权中心中产生认证向量  $AV = (RAND, XRES, CK, IK, AUTN)$  和认证令牌  $AUTN = SQN[AAK] || AMF || MAC-A$ ,其中 AMF 为

认证密钥管理范围。VLR 发送 RAND 和 AUTN 至用户身份识别模块。用户身份识别模块计算  $XMAC-A=f_{1K}(SQN||RAND||AMF)$ ,若等于 AUTN 中的 MAC-A,并且 SQN 在有效范围内,则认为对网络鉴权成功,计算 RES、CK、IK,发送 RES 至 VLR。VLR 验证 RES,若与 XRES 相符,则认为对移动台鉴权成功;否则,拒绝移动台接入。当 SQN 不在有效范围内时,用户身份识别模块和鉴权中心利用  $f_{1^*}$  算法进入重新同步程序,SGSN/VLR 向 HLR/AUC 请求新的认证向量。

表 5-9 AKA 运行过程中所用安全算法的安全服务内容

序号	算法	安全服务内容	序号	算法	安全服务内容
1	f0	仅在鉴权中心执行,用于产生随机数 RAND	4	f3	用于产生加密密钥(CK)
2	f1	算法用于产生消息认证码(鉴权中心中为 MAC-A,用户身份识别模块中为 XMAC-A)	5	f4	用于产生消息完整性密钥(IK)
	$f_{1^*}$	重同步消息认证算法,用于产生 MAC-S	6	f5	用于产生匿名密钥(AK)和对序列号(SQN)加解密,以防止被位置跟踪
3	f2	用于产生期望的认证应答(鉴权中心中为 XRES,用户身份识别模块中为 RES)		$f_{5^*}$	重同步时的匿名密钥生成算法

3GPP 的数据加密机制将加密保护延长至 RNC。数据加密使用 f8 算法,生成密钥流块 KEYSTREAM。对于移动台和网络间发送的控制信令信息,使用算法 f9 来验证信令消息的完整性;对于用户数据和语音不给予完整性保护。移动台和网络相互认证成功后,用户身份识别模块和 VLR 分别将 CK 和 IK 传给移动设备和 RNC,在移动设备和 RNC 之间建立起保密链路。f8 和 f9 算法都是以分组密码算法 KASUMI 构造的,KASUMI 算法的输入和输出都是 64 位;密钥是 128 位;KASUMI 算法在设计上具有对抗差分和线性密码分析的可证明的安全性。

与 3GPP 网络类似,CDMA 2000 系统也采用了双向认证技术与 AKA 协议作为接入安全结构的基础,这样一方面可以克服 IS-95 CDMA 系统的安全漏洞,又有利于 3GPP 和 3GPP2 两种体制之间的漫游。机密性算法由 CMEA 增强为 ECMEA;所有密钥长度均采用 128 位。和 WCDMA 相比,由于两个系统的技术参数、系统架构与实现细节的差异,导致两者的安全技术略有不同。

## 本章小结

3G 是第三代移动通信系统的简称,3G 具有全球化、多媒体化、综合化、智能化和个人化的特征,3G 采用了 RAKE 接收、智能天线、高效信道编译码、多用户检测、功率控制和软件无线电等多项关键技术。ITU 制定的 3 大主流 3G 标准是 WCDMA、CDMA 2000 和 TD-SCDMA。

3 大标准中,WCDMA 和 CDMA 2000 采用 FDD 方式,需要成对的频率规划。WCDMA 的扩频码速率为 3.84Mc/s,载波带宽为 5MHz,而 CDMA 2000 采用单载波时扩频码速率为 1.2288Mc/s,载波带宽为 1.25MHz;另外,WCDMA 的基站间同步是可选的,而 CDMA 2000 的基站间同步是必需的,因此需要全球定位系统(GPS),以上两点是 WCDMA 和

CDMA 2000 最主要的区别。除此以外,在其他关键技术方面,例如功率控制、软切换、扩频码以及所采用分集技术等基本都是相同的,只有很小的差别。

TD-SCDMA 的双工方式为 TDD,不需要为其分配成对的频带。扩频码速率为 1.28Mc/s,载波带宽为 1.6MHz,其基站间必须同步。与其他两种标准相比,TD-SCDMA 采用了智能天线、联合检测、上行同步及动态信道分配、接力切换等技术,具有频谱使用灵活、频谱利用率高等特点,适合非对称数据业务。

WCDMA 标准由 3GPP 组织制定,已有 R99、R4、R5、R6、R7、R8、R9、R10、R11、R12、R13 等多个核心网网络结构的版本,自 R5 进入了 HSPA(高速分组接入)阶段,为 WCDMA 的提高版;R8 对应 LTE(长期演进计划),为准 4G 版;R10 对应 LTE-Advanced(LTE 演进版),即 4G 版。其中 R99 版本的主要特点是无线接入网采用 WCDMA 技术,核心网分为电路域和分组域,分别支持语音业务和数据业务。R4 版本是向全分组化演进的过渡版本,与 R99 相比其主要的变化是在电路域中引入了软交换的概念,将控制与承载分离,语音通过分组域传递。另外 R4 提出了信令的分组化方案,包括基于 ATM 和 IP 的两种可选方式。R5 和 R6 是全分组化的网络,在 R5 中提出了高速下行分组接入(HSDPA)方案,可以使最高下行速率达到 10Mb/s,在核心网上增加了 IP 多媒体子系统(IMS);R6 增加了 MBMS(多媒体广播组播业务)功能。R7 引入了 OFDM、MIMO(多人多出)技术。

CDMA 2000 标准由 3GPP2 组织制定,目前已制定了 0、A、B、C、D、E 和 F 共 7 个支持 CDMA 2000 1x 及其增强型技术的版本(CDMA 2000 1x EV-DO 和 CDMA 2000 1x EV-DV)。

3GPP 在制定 R4 版本时将 TD-SCDMA 列入它的可选无线接入标准,从此 TD-SCDMA 和 WCDMA 的发展就基本处于同步状态。与 WCDMA 一样,TD-SCDMA 在 R5 版本中推出了 HSDPA 技术。采用 HSDPA 后,TD-SCDMA 增加了 1 种传输信道、3 种物理信道,还增加了 16QAM 调制技术。采用 HSDPA 技术可以让 TD-SCDMA 系统下行链路的数据传输速率有很大的提高,单载波支持数据传输速率达到 2.8Mb/s。WCDMA 在 R6 版本中完成了 HSUPA 标准的制定并引入了 MBMS,TD-SCDMA 在这方面的技术研究较晚,一直到 2007 年 9 月才在 R7 中完成 TD-SCDMA 的 HSUPA 和 MBMS 的标准制定;同样地,WCDMA 已在 R7 中基本完成 HSPA+(HSPA 增强技术,HSPA 是 HSDPA 和 HSUPA 的合称)标准的制定,TD-SCDMA 在 R8 中才完成这一标准的制定工作。

第三代移动通信系统的 3 大标准都采用了平滑演进的方式,在无线网络中逐步采用增强型技术,从核心网络逐步过渡到全 IP 网络,最终进入的长期演进阶段目标(3GPP 制定的是 LTE,3GPP2 制定的是 AIE)是一致的,能最终融合到 B3G/4G 系统,进入下一代网络。

3G 业务是指所有能够在 3G 网络上承载的各种移动业务,它包括点对点基本移动语音业务和各类移动增值业务。3G 业务网络由传统的多业务分离的垂直的结构,发展成为分层的业务和控制分离的网络,形成了统一的业务平台,便于 3G 业务的生成和管理。

从服务质量(QoS)来分,3GPP 提出了会话类、流媒体、交互类和背景类 4 种业务。

由于网络的开放性以及无线传输的特性,使 3G 面临多种安全威胁,主要包括非法获取敏感数据来攻击系统的保密信息,非法操作敏感数据来攻击完整信息,非法访问服务,滥用干扰 3G 服务降低系统服务质量或拒绝服务,网络或用户否认曾经发生的动作。3GPP 网络接入安全机制有 3 种:①根据临时身份(TMSI)识别;②使用永久身份(IMSI)识别;③认证和密钥协商(AKA)机制。

## 习题

5-1 为什么要在 2G/2.5G 的基础上发展 3G 技术? 3G 在 2G/2.5G 的基础上有了哪些进步? 在满足用户需求方面,3G 系统还存在哪些不足? 以所掌握的知识讲述 3G 系统应从哪些方面来提高。

5-2 简述 3G 的发展历程。

5-3 第三代移动通信系统具有哪些特征? 其关键技术是什么?

5-4 对 WCDMA、CDMA 2000 和 TD-SCDMA 这 3 种 3G 系统的空中接口技术、标准的稳定性、系统性能、设备成熟度、漫游能力、业务提供能力以及所涉知识产权进行简要分析与比较。针对这 3 种系统的特点,我国在部署这些系统时应采用什么样的策略?

5-5 3GPP 和 3GPP2 分别是什么组织? 我国基于什么原因要分别加入这两个组织? 我国可以在这两个组织中发挥什么样的作用? 又可以得到什么样的好处?

5-6 ITU 和我国分别如何来划分 3G 的频段? 为什么说我国 3G 频段的划分体现了对 TD-SCDMA 的支持? 从 ITU 对 3G 频段的划分角度看,TD-SCDMA 能否实现全球漫游?

5-7 3G 的主流多址技术为什么是 CDMA 而不是 TDMA? 但在 TD-SCDMA 中又引入了时分技术,又是基于什么考虑?

5-8 3G 系统采用了什么语音编码技术? 3G 系统又采用了什么信道编码技术?

5-9 在 3G 网络中,实施承载与控制分离的结构有什么好处?

5-10 试述 WCDMA 系统的特点及网络结构组成。

5-11 3GPP R5 版本为什么要引入 IMS 域?

5-12 为什么 CDMA 系统需要进行网络同步? WCDMA 终端是如何实现与系统同步的? 其同步方式和 CDMA 2000 的同步方式有什么差异?

5-13 WCDMA 承载分组数据的传输信道有哪些? WCDMA 系统中物理信道的功率分配方式是什么?

5-14 2G 中的 SIM 卡和 3G 中的 USIM 长是什么关系? 试对两者的功能进行比较。

5-15 WCDMA 如何处理基站侧信号? 信号交织、复用后,同原信号相比有什么区别? I、Q 信号是如何产生的? I、Q 信号复用的作用又是什么?

5-16 画出 4~16 阶变长正交 Walsh 码(即 OVVSF 码)的码树,说明在取码过程中的原则。

5-17 什么是高速分组下行技术(HSDPA)?

5-18 CDMA 2000 系统是如何进行演进的? 其演进方式和 WCDMA 系统有什么差异? 为什么一般不将 CDMA 2000 1x 系统归于 3G?

5-19 CDMA 2000 1xEV-DO 和 CDMA 2000 1xEV-DV 各有什么特点? 它们分别采用了哪些关键技术?

5-20 试述 CDMA 2000 核心网的演进。3GPP2 为其制定的 Release 标准关注的是什么? 如何判断是否是核心网?

5-21 什么是 SIP 和 MIP? 比较这两种 IP 技术。

5-22 什么是速率控制? 速率控制和功率控制相比,各自有什么优缺点? 阐述速率控

制在 CDMA 2000 中的使用情况。

5-23 TD-SCDMA 系统的特点是什么? 其演进路线如何展开?

5-24 TD-SCDMA 帧结构如何设置? 为什么要采用这种结构? 其突发结构如下图所示, 试述这样安排是基于什么考虑? 如果要传输物理层控制信令, 应放置在突发结构的什么位置? 说出理由。



5-25 从概念、技术方案、特点和使用范围等几方面全面比较硬切换、软切换、更软切换、虚拟软切换(快速小区交换)和接力切换的不同。

5-26 智能天线可分为哪几类? 有什么作用? 阐述智能天线在 TD-SCDMA 中的使用情况。

5-27 3G 业务可依据哪些准则进行分类? 试述 3GPP 的 3G 业务分类方法。

5-28 3G 网络可能遭受的安全威胁和攻击手段有哪些?

5-29 画图说明 3G 系统的安全架构, 其采用的接入安全机制有哪几种?

5-30 HSPA 系统新增了哪些物理信道? 它采用的增强型技术有哪些?