

摘要

随着无线通信系统的飞速发展, 3GPP 组织提出了 LTE 系统规范, 该系统具备高速率、低延迟的优势, 能够充分满足用户和运营商对速率和性能的需求。据全球移动设备供应协会预计, 未来 10 年全球移动宽带用户数将达到 50 亿, 因此抓住商机, 尽快研发 LTE 终端产品具有巨大的市场价值。非接入层作为 LTE 终端的重要组成部分, 其主要功能有: 移动管理、会话管理和连接管理, 其中会话管理功能决定着非接入层数据传输的速率、延迟以及稳定性。本文深入研究了会话管理功能从而实现了非接入层的数据传输功能。

首先, 基于对 LTE 系统构架的认识以及非接入层对于数据传输的要求, 本文深入探讨了 LTE 系统独有的 QoS 构架以及 TFT 在数据传输中的过滤功能, 重点研究了 LTE 系统中 PDN 连接过程、承载资源分配过程等会话管理流程, 并在此基础上对 LTE 系统从非接入层信令建立到用户数据传输的整个流程做了系统性的研究。

其次, 本文针对 LTE 终端非接入层数据传输的需求, 在对 LTE 协议深入分析研究的基础上, 结合 LTE 终端的会话管理功能, 设计并实现了一种非接入层数据传输方案: 设计了 LTE 终端的会话管理实体, 提出了一种会话管理实体的状态划分、状态跳转以及接口原语系统。之后, 对应会话管理实体系统, 详细设计了 LTE 终端会话管理流程。为减少终端和网络的交互异常, 重点设计了非接入层的重传机制。结合 TFT 的过滤功能, 实现了 LTE 终端正常情况和异常情况下的数据传输的设计流程。

最后, 本文选取具有代表性的测试用例, 运用协仿真测试方法和板级测试方法, 对本文提出的设计方案进行协议一致性测试。结合 3GPP 测试协议的要求, 通过对仿真结果图的深入分析, 证明了本文提出的关于非接入层数据传输方案的正确性和可行性。

关键词: LTE, 非接入层, 会话管理, 数据传输

Abstract

With the rapid development of wireless communication system, the 3GPP organization proposes LTE system specifications, it has the advantage of high-speed, low latency, and can fully meet the speed and performance needs of users and operators. According to the Global Mobile Device Supply Association, the number of global mobile broadband users will reach 5 billion in the following 10 years, so that it is of great market value to seize the opportunities to develop LTE Terminal products. Non-access layer, as an important part of LTE Terminal, its main functions are as follows: mobility management, session management and connection management, session management function of which determines transmission rate, delay, and the stability. This paper provides an in-depth study of session management function and explores and implements function of non-access layer data transmission.

First, based on LTE system framework and non-access layer data transmission, this paper conducts an in-depth discussion on the unique QoS framework of LTE system and filter function of TFT in data transmission, focuses on research of the PDN connection process and bearer resources distribution process of session management process in LTE system, and then it has a systemic research on the whole process from signalling establishment to data transmission in LTE system.

Secondly, this paper focuses on the requirement of non-access layer data transmission, combines with session management process, details in the design of the session management entity. Based on an analysis of the protocols, set states division, states transfer and interface primitives, and then it details in the design process of session management function. To reduce terminal and network interaction anomalies, it focuses on design of non-access layer retransmission mechanism and combines with filtration function of TFT, describes the design of data transmission process.

Finally, this paper selects a representative test cases, uses simulation and board-level test method, it conducts protocol conformance testing towards the proposed design. Combined with 3GPP test requirements protocols, it proves the correctness and the feasibility of data transmission design by in-depth analysis of simulation results.

Key words: LTE, Non-Access-Stratum (NAS), EPS Session Management (ESM), Data Transfer

缩略表

3G	3rd Generation mobile communication	第三代移动通信
3GPP	Third Generation Partnership Project	第三代合作项目
APN	Access Point Name	接入点名称
AS	Access Stratum	接入层
ASP	Abstract Service Primitives	抽象服务原语
ATS	Abstract Test Suite	抽象测试集
CMC	Connection Management Control	连接管理控制
COM	communication port	串行通讯端口
CS	Circuit Switched	电路交换
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DL	DownLink	下行
EPC	Evolved Packet Core	演进型包核心
EPS	Evolved Packet System	演进型包系统
ESM	EPS Session Management	EPS会话管理
EMM	EPS Mobility Management	EPS移动性管理
eNB	Evolved NodeB	演进型结点B
E-UTRAN	Evolved UTRAN	演进型UTRAN
FDD	Frequency Division Duplex	频分双工
GBR	Guaranteed Bit Rate	比特速率保障
GUTI	Globally Unique Temporary Identifier	全球唯一临时标识
HSS	Home Subscriber Server	归属用户服务器
Ipv4	Internet Protocol version 4	因特网协议版本4
Ipv6	Internet Protocol version 6	因特网协议版本6
IMS	IP Multimedia Subsystem	IP多媒体子系统
IUT	Implementation Under Test	被测实体
L1	Layer 1(Physical Layer)	层一（物理层）
LTE	Long Term Evolution	长期演进
MAC	Medium Access Control	媒体介入控制
MBMS	Multimedia Broadcast and Multicast Service	多媒体广播组播业务
MBWA	Mobile Broadband Wireless Access	移动宽带无线接入
MBR	Maximum Bit Rate	最大比特速率

MME	Mobility Management Entity	移动管理实体
MSC	Message Sequence Charts	消息序列图
NAS	Non-Access Stratum	非接入层
OFDM	Orthogonal Frequency Division Multiple	正交频分多址
P-GW	Packet Data Network Gateway	PDN 网关
PCO	Points of Control and Observation	控制观察点
PCRF	Policy and Charging Rules Function	策略和计费规则功能
PDB	Packet Delay Budget	数据包时延预算
PDCP	Packet Data Convergence Protocol	分组数据汇聚层数据
PDN	Packet Data Network	分组数据网
PLMN	Public Land Mobile Network	公共陆地移动通信网
PLR	Packet Loss Rate	数据包丢失率
PS	Packet Switched	分组交换
PTI	Procedure Transaction Identity	过程处理标识
QCI	QoS Class Identifier	QoS组标识
QoS	Quality of Service	服务质量
RABM	Radio Access Bearer Management	无线接入承载管理
RRC	Radio Resource Control	无线资源控制
RLC	Radio Link Control	无线链路控制
S-GW	Serving Gateway	服务网关
SAP	Service Access point	业务接入点
SDF	Service Data Flow	业务数据流
SDL	Specification Description Language	规范描述语言
SMC	Security mode control	安全模式控制
SPV	Service Provider	服务提供商
TAC	Tracking Area Code	跟踪域码
TAI	Tracking Area Identity	跟踪域标识
TDD	Time Division Duplex	时分双工
TFA	Traffic Flow Aggregates	传输流汇聚
TFT	Traffic Flow Template	业务流模板
TTCN	Tree and Tabular combined Notation	协议测试规格语言
UE	User Equipment	用户终端
UL	UpLink	上行

第一章 绪论

1.1 引言

随着个人移动通信需求的增加,无线通信技术不断向前演进,人们对移动通信业务的要求已经从单纯的语音业务扩展到多媒体业务。同时,用户的通信习惯也从以往的点到点通信演进到人到人通信。个人通信的迅猛发展极大地促进了个人通信设备的微型化和多样化,结合多媒体消息、在线游戏、视频点播、音乐下载和移动电视等数据业务的能力,无线性能得到很大的提高,但是在应对市场挑战和满足用户需求等领域,还有很多局限性,而3G厂商和运营商在专利问题上处处受到制肘,业界迫切需要改变这种不利局面^{[1][2]}。

对此,全球各大组织积极提出应对措施,推出了WiMAX、UMB、MBWA等先进技术。面对这种情况,3GPP标准化组织启动了LTE(Long Term Evolution, 长期演进)项目来应对WiMAX等移动通信技术的竞争压力,保证3GPP系统在未来10年中在行业内的竞争优势^{[3][4]}。

LTE系统将移动通信技术与宽带无线接入技术相融合,采用全新的扁平化网络架构,该架构基于全IP的PS域,取消了CS域,逐步趋近于典型的IP宽带网络结构,将原来的CS域业务全部经由PS域实现(比如通过VoIP等)。可以说LTE是3G技术的一场革命^[5]。

LTE系统的目的是研发一个高数据传输率、低延迟、为分组业务而优化的无线接入系统,这使得LTE系统主要集中在分组交换(Packet Switching, PS)域。3GPP组织从“系统性能要求”、“网络的部署场景”、“网络架构”、“业务支持能力”等方面对LTE系统进行了详细的描述,具体技术特征如下^[3]:

1, 通信速率有了极大的提高,下行峰值速率最高可达100Mbps、上行速率最高可达50Mbps。

2, 以分组域业务为主要目标,系统在整体架构上基于分组交换。

3, QoS保证,通过系统设计和严格的QoS机制,保证实时业务的服务质量。

4, 降低无线网络时延:子帧长度为1ms,解决了向下兼容的问题并降低了网络时延,时延可满足用户面(U-plane)<5ms、控制面(C-plane)<100ms。

5, 增加了小区边界比特速率,在保持目前基站位置不变的情况下增加小区边界比特速率。如MBMS(多媒体广播和组播业务)在小区边界可提供1 bit/s/Hz的数据速率。

6, 强调向下兼容, 支持已有的 3G 系统和非 3GPP 规范系统的协同运作。

此外在 LTE 系统中, 还规范了一些其他的要求, 比如与配置相关的要求、E-UTRAN 架构和移植性要求、无线资源管理要求、复杂性要求、成本相关要求以及业务相关要求等等。

1.2 研究现状

1.2.1 LTE 研究现状

就在全球数以亿计的移动通信用户还在享受第三代移动通信技术(3G)带给工作和生活巨大改变的时候, 3G 的长期演进方案——LTE 技术的研发和推广工作已经悄然展开。随着全球 3G 市场稳步增长, 2010 年我国的 TD-LTE 市场正式启动。据了解, TD-LTE 已经入选中国国家 16 个重大科技专项, “新一代宽带无线移动通信网”也将 TD-LTE 作为 ‘十一五’ 工作的重中之重。

2010 年 4 月, 全球首个 TD-LTE 演示网在上海世博园区开通。2010 年 6 月, 日本最大移动运营商 NTT DoCoMo 宣布开始正式检验其在东京地区新的 LTE 网络, 预计将在 2011 年中大规模推出超高速的 LTE 商用服务。2010 年 9 月, 由广东移动承建的 TD-LTE 试验网已经在广州、深圳两地建成 220 个站点, 并完成了网络的优化工作。与此同时, 非洲以及中国台湾地区 TD-LTE 试验网也相继开通。截止 2010 年底, 全球已建成 11 个 TD-LTE 试验网, 另有 8 个试验网计划于今明两年间相继开通。目前国内外企业广泛参与的 TD-LTE 产业链已初步形成, TD-LTE 技术试验工作已组织并开展。

2010 年 10 月, 在中国国际信息通信展览会上, 中国移动应用 TD-LTE 技术, 实现北京展会现场和上海世博会信息通信馆现场的互联互通, 使北京展会现场的操作手柄可以控制上海机器人的移动方向, 这给观众带来了全新的互动体验。目前包括华为、中兴、上海贝尔、大唐、爱立信等主流设备商均已参与并完成了 2.3GHz 室内设备测试, 2.6GHz 部分室外设备测试也正在筹划之中。据了解, 近期华为、中兴通讯、大唐、诺基亚西门子和上海贝尔等 5 家系统厂商, 海思、创毅视讯等 2 家芯片厂商将在北京、杭州、上海、南京、广州、深圳及厦门等 7 个城市开展为期一年半的规模基数实验。届时, 将对 LTE 的系统设备、终端性能、网络性能、组网性能等进行测试和验证, 使得 LTE 系统能够在试验区域达到基本的商用水平。综上所述, LTE 的商用已经启动, 4G 时代触手可及。

1.2.2 LTE 终端的发展

TD-LTE 要发展, 终端是首要解决的问题。终端设备数量、成熟度及价格将成为 TD-LTE 在 4G 市场决胜的关键。由于先前对 LTE 发展前景不确定, 大部分芯片厂商在过去很长一段时间都处于观望状态, 导致了 LTE 芯片跟不上网络发展速度, 使得大多数 TD-LTE 终端现在还停留在各厂商开发、改进阶段。2010 年 6 月初, 在上海世博会上, 中移动仅仅展示出 4 款 TD-LTE 上网卡, 远达不到需求^[6]。10 月底, 中国移动联合诺基亚展示一款 TD-LTE 上网本, 基于上海 TD-LTE 演示网进行了包括高清视频传输等在内的 TD-LTE 业务演示。目前只有海思、创毅视讯、Sequans、三星、中兴微电子五家芯片厂商提供了产品进行功能、性能、射频等参数的测试, 计划进行异系统互操作测试。

总体上, 相对于网络设备的蓬勃发展, LTE 终端芯片的发展相对滞后。距离大规模的设备互通测试阶段为时尚早, 还需要产业链更加努力加快发展。无论从技术实验还是到规模验证, 都需要三到五年的时间才能把它推向成熟。

虽然各大公司以及运营商都对 LTE 终端投入了比较大的精力, 但现在仍只有少数产品能够初步商用, 且由于商业机密等原因, 各大公司之间并不能很好的交流, 也在一定程度上影响了 LTE 终端的发展。本文对非接入层的数据传输进行了深入的研究, 为 LTE 终端进一步的发展, 加快 LTE 的发展进程做了一定的贡献。

1.3 论文安排

本文首先简要的介绍了 LTE 的发展现状和目标, 在此基础上介绍了 LTE 系统构架、LTE 终端模型以及和非接入层数据传输相关流程; 然后对非接入层数据传输技术进行了介绍; 接着对会话管理流程进行重点分析, 给出相应的解决方案, 并进行了测试。

论文的内容组织安排如下:

第一章: 绪论

本章对 LTE 的背景进行了介绍, 说明了 LTE 的研究现状, 介绍了论文的组织结构。

第二章: 非接入层数据传输的研究

本章主要对非接入层数据传输进行理论研究。首先对 LTE 系统构架、LTE 终端结构模型以及各个组成部分做了简单介绍; 然后详细介绍了数据传输的几个重要参数; 最后介绍了为非接入层数据传输准备的相关流程, 比如会话管理流程以及连接管理相关流程。

第三章: 非接入层数据传输的设计与实现

本章针对第二章的理论研究，粗略设计了开发平台以及总体设计方案；详细设计了各个模块的接口原语、状态定义；并针对会话管理流程以及数据传输流程做了详细的流程设计。

第四章：仿真与测试

首先，简要介绍协议测试原理、步骤以及协议测试工具 TTCN；然后，根据协议栈软件开发的需求，设计 TTCN 协仿真测试用例并测试；其次，选取有代表性的测试用例进行 TTCN 板级测试，通过对测试结果的详细分析，验证非接入层数据传输相关功能模块设计的正确性和有效性。最后，本章简单介绍了外场测试的情况。

第五章：结束语

总结全文，陈述了本论文所涉及工作的主要内容与贡献，并指出了继续进行的相关研究工作和未来可能的研究方向。

论文最后给出了致谢和参考文献。

第二章 非接入层数据传输的研究

2.1 LTE 系统总体框架

LTE 系统作为 3G 系统的演进，其特点为高数据传输率、低延迟、为分组业务优化。由于采用了基于 OFDM 技术的空中接口设计，LTE 系统比 3G 系统的空中接口技术有了很大的改进。LTE 系统基于分组交换的设计思想，仅仅使用共享信道，物理层不再提供专用信道。LTE 系统支持 FDD 和 TDD 两种双工方式，TD-LTE 系统即是我国自主研发的技术。早先的 3G 网络构架比较臃肿，网络的交互相对繁琐，不利于信息的快速传递，LTE 系统对传统 3G 网络架构进行了优化，采用了扁平化的网络结构，取消了不少不必要的节点，将相同或者类似的功能整合在一起，在接入网中只保留 eNB 构成的“单层”构架，使信息传递更加迅速快捷。图 2.1 描述了 LTE 系统总体框架^[7]。

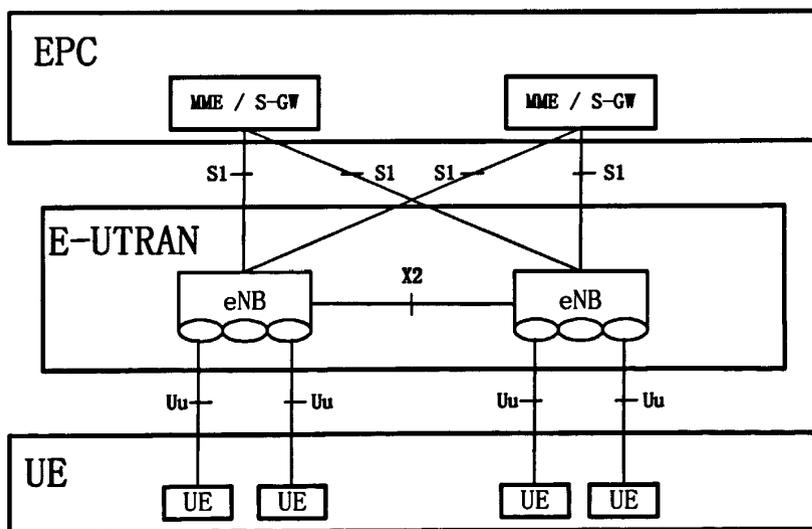


图 2.1 LTE 系统总体框架模型

如图 2.1 所示，整个 LTE 系统由核心网（EPC）、接入网（E-UTRAN）和用户设备（UE）3 部分组成。其中，EPC（Evolved Packet Core）负责核心网部分，EPC 信令处理部分称 MME，数据处理部分称为 SAE Gateway (S-GW)；E-UTRAN 节点为 eNB(eNodeB)；UE 指用户终端设备。E-UTRAN 与 EPC 通过 S1 接口连接；eNodeB 之间通过 X2 接口连接；eNodeB 与 UE 通过 Uu 接口连接。

MME 的功能包括：寻呼消息发送；安全控制；Idle 状态的移动性管理；SAE 承载管理；NAS 信令的加密及完整性保护等。

S-GW 的功能包括：数据的路由和传输，以及用户面数据的加密。

eNodeB 的功能包括：RRM 功能；IP 头压缩及用户数据流加密；UE 附着时的 MME 选择；寻呼信息的调度传输；广播信息的调度传输；设置和提供 eNB 的测量等。

LTE 系统的 EPS 网络架构相对于 UMTS 系统的变化主要体现为以下两个方面：

1, 全 IP 的扁平化网络架构。EPS 系统取消了 CS 域，代之以基于全 IP 的 PS 域。

2, 支持多种 3GPP、非 3GPP 无线系统的接入, 如 GERAN/UTRAN、E-UTRAN、WLAN 等。

图 2.2 给出了在非漫游场景下 UE 通过 E-UTRAN 接入 EPC 核心网的系统架构。其中, PDN-GW 可以通过 SGi 接口接入运营商网络, MME 用于信令的控制, S-GW 用于用户数据的传输, PCRF 实体负责通过 Gx 接口为 PDN-GW 提供相关的策略控制与计费规则, HSS 是用于存储用户签约信息的数据库。

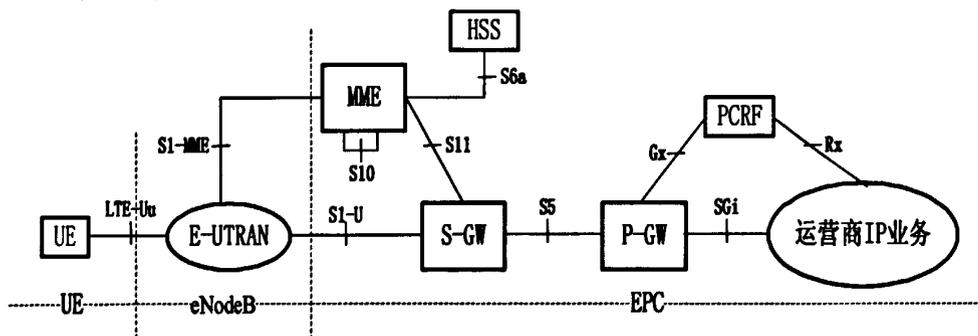


图 2.2 3GPP 接入架构

2.2 LTE 系统终端结构模型

根据 3GPP 协议中对 LTE 协议栈层次结构的描述, 可以将 LTE 系统终端协议栈划分为如图 2.3 所示的结构^[7]。

由底层到上层, 分别为: 物理层 (L1)、协议栈和应用层。分别对各个层进行描述:

物理层: 物理层向高层提供数据传输服务, 包括: 传输信道的错误检测, 前向纠错(Forward Error Correction, FEC)编码解码, 传输信道与物理信道之间的速率匹配, 传输信道与物理信道之间的映射, 物理信道的调制解调等服务。

协议栈: 协议栈通过解析物理层数据, 完成终端与网络之间的信令交互, 包括移动性管理、连接管理以及会话管理等; 同时对于应用层下发的数据, 经过加头、加密等操作传输到网络。

应用层：应用层与人机界面相结合，通过 AT 指令，向协议栈提出各种需求。同时，通过相关接口发送和接收用户的相关数据。

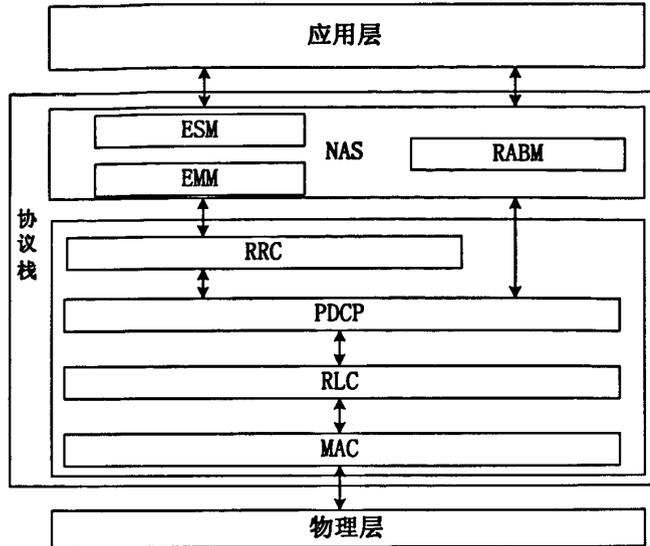


图 2.3 LTE 系统终端结构模型

如图 2.3 可以看到，协议栈分为接入层（AS）和非接入层（NAS）两部分。AS 主要由媒体访问控制（MAC）、无线链路控制（RLC）、分组数据汇聚（PDCP）和无线资源控制（RRC）四部分组成。NAS 主要由移动管理（EMM）、会话管理（ESM）和无线接入承载管理（RABM）三部分组成。

2.3 非接入层框架

NAS 层主要由 EMM、ESM 和 RABM 三部分构成。控制平面包括 EMM 和 ESM，数据平面包括 RABM。针对非接入层的数据传输，在控制平面主要由 ESM 负责，在数据平面主要由 RABM 负责^[8-10]。ESM 是一个多实例的模块，每一个实例管理一个 EPS 承载。ESM 主要提供会话管理功能，包括 EPS 承载的建立、修改和释放。RABM 向下层提供 EPS 承载与无线承载的映射，同时对上层完成一组 SDF(业务数据流)与 EPS 承载间的映射。

本文的研究目的是建立非接入层的数据传输。首先通过 ESM 的会话管理功能建立终端与核心网之间的信令连接，然后通过 RABM 传输用户数据。因而本文的研究重点也分为两点：ESM 的会话管理功能和 RABM 的用户数据传输功能。

由图 2.4 可以看到，ESM 子层处于协议栈 NAS 层的最上层，与应用层交互，向下与 EMM 相连，其主要作用是处理控制平面的会话管理相关信令。RABM 主要负责处理应用层数据平面(COM)的用户数据以及 PDCP 层发来的数据。

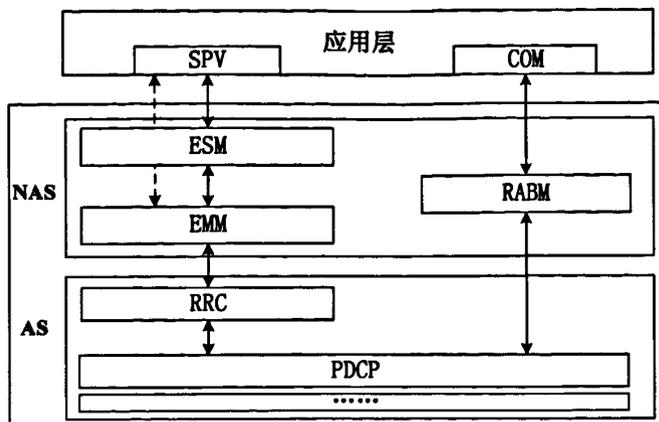


图 2.4 LTE 系统终端非接入层结构模型

下面对 ESM、RABM、EMM、PDCCP、应用层进行简单的描述，对非接入层数据传输有个大体的了解：

ESM 描述：ESM 模块是 LTE 终端的会话管理模块，其主要功能是对会话的建立、修改和释放进行控制。

RABM 描述：RABM 模块主要管理 EPS 承载与无线承载之间的映射关系。对于 SPV 传来的数据，根据相应的匹配规则发送给 PDCCP 层传输；对于 PDCCP 发来的数据，根据相应规则传输给 SPV。

EMM 描述：EMM 模块主要是为 PS 域的移动性和安全性进行管理，主要完成附着注册，位置更新，MM 连接建立等功能。

应用层描述：应用层负责多种业务，在控制平面，与 ESM 通信的主要是 SSM (SPV-ESM)模块；在数据平面，负责数据平面的 IP 数据包的下发和接收主要是 COM 模块。

PDCCP 描述^[7]：PDCCP 主要提供数据的头压缩业务、加密业务以及处理包头。对于上层 RABM 传来的数据进行头压缩、加密以及一致性保护；对于下层 RLC 发来的数据进行头解压缩、解密同时去除 PDCCP 包头。

2.4 数据传输重要参数

LTE 系统为应对高速的数据传输，合理分配网络资源，对 QoS 做了很大的改变，减少了由于 QoS 协商带来的时延，使 QoS 更加清晰，更易于实现。同时为了更好的应对不同数据对于网络资源的要求，LTE 系统对 TFT 做了更加详细的描述。

2.4.1 QoS 的研究

由于 LTE 系统在接入网结构上的优化,使得接入网结构更加扁平化,导致 LTE 系统 QoS 的结构也发生变化。为了使 UE 更好的实现“永远在线”,LTE 系统在 QoS 中引入了默认承载等相关概念。

在 LTE 系统中给出了以下 QoS 相关概念^[1]:

默认承载: 默认承载是在 UE 连接到 PDN 网络时建立的,并且在 UE 与 PDN 网络连接的整个期间都将被保留的承载。默认承载可以为 UE 提供连接到 PDN 网络的永远在线的 IP 连接。默认承载的初始承载级别 QoS 参数基于用户的签约数据,由网络分配。默认承载是一种提供尽力而为的 IP 连接的承载。

专有承载: 专有承载是 UE 在默认承载建立之后,为某种特定业务而建立的承载。一般情况下专有承载的 QoS 将要比默认承载的 QoS 高。专有承载在 UE 端关联了一个 UL 业务流模板(Traffic flow template, TFT),在 PDN-GW 管理一个 DL TFT, TFT 包含了业务流的过滤器,而这些过滤器只能匹配符合某些准则的分组数据,从而使得只有特定的数据才能通过专有承载传输。

GBR/Non-GBR 承载: 如果将某些保证比特速率(Guaranteed Bit Rate, GBR)相关的专用的网络资源在承载建立或修改的时候被永久分配给一个 EPS 承载(例如:通过 eNB 中的准入控制功能),则该 EPS 承载就是一个 GBR 承载。否则,该 EPS 承载是一个 Non-GBR 承载。

一般来说,默认承载是一个 Non-GBR 承载。其相关的专有承载根据其 QoS 的不同,可以是 GBR 承载也可以是 Non-GBR 承载。

2.4.1.1 QoS 概念和承载业务架构

一个 ESP 承载业务分层架构在图 2.5 中描述。

EPS 承载业务构架采用的是分层次、分区域的 QoS 体系结构。有图 2.4 可以看到,端到端的 QoS 业务可以分解为两部分:EPS 承载业务和外部承载业务。其中,外部承载业务用于连接 P-GW 与外部网络节点之间的业务承载。EPS 承载业务则可以分为无线接入承载业务和 S5/S8 承载业务。S5/S8 承载业务可以实现 MME 与 P-GW 之间的 EPS 承载业务数据单元的传送,同时提供端到端 IP 业务汇聚的 QoS 保证。无线接入承载又可分为无线承载和 S1 承载。EPS 无线承载业务可以实现 eNB 与 UE 之间的 EPS 业务数据单元的传送,其依据的是 UE 请求的 QoS 等级。同时无线承载业务可以提供 IP 头压缩、用户平面加密功能,并可以为 UE 提供映射及复用信息。S1 承载业务可以实现 eNB 与 MME 之间的 EPS 承载业务数据单元的传送。

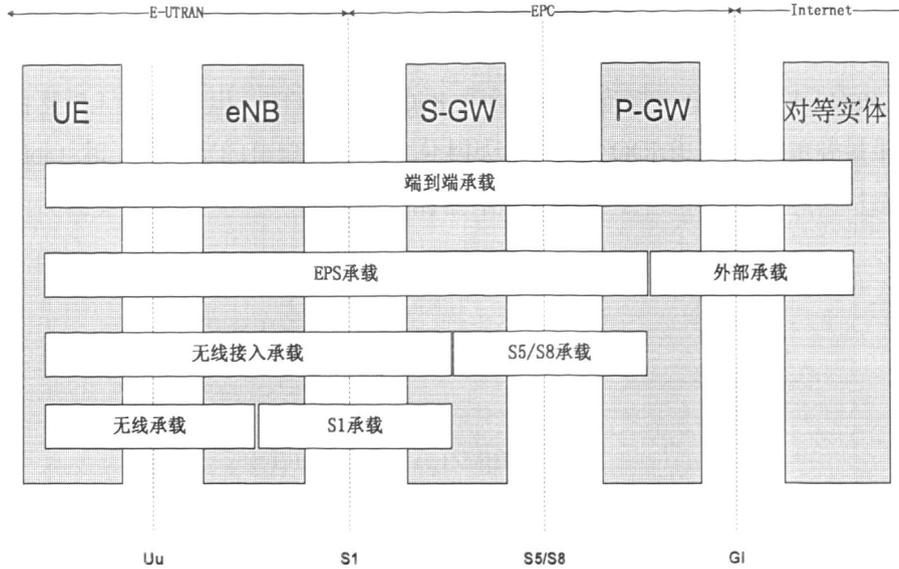


图 2.5 EPS 承载业务构架

2.4.1.2 承载级 QoS 参数及属性

由表 2.1 可以看出，LTE 系统 QoS 的结构非常简洁，仅由 QCI (QoS Class Identifier) 和一些限定的传输速率两部分构成。其中，QCI 作为 EPS 承载最重要的参数，代表了 EPS 系统整个 QoS 参数的整体指标。表 2.1 中*表示此项为可选项。

表 2.1 UE 端 QoS 信息单元

QoS信息单元标识	字节 1
QoS内容长度	字节 2
QCI	字节 3
上行最大比特率(UL-MBR)	字节 4*
下行最大比特率(DL-MBR)	字节 5*
上行保证比特率(UL-GBR)	字节 6*
下行保证比特率(DL-GBR)	字节 7*
扩展的上行最大比特率(UL-MBR-extended)	字节 8*
扩展的下行最大比特率(DL-MBR-extended)	字节 9*
扩展的上行保证比特率(UL-GBR-extended)	字节 10*
扩展的下行保证比特率(DL-GBR-extended)	字节 11*

QCI 可同时应用于 GBR 承载和 Non-GBR 承载。用于指定访问节点内定义的控制承载级分组转发方式，例如调度权重、接纳门限、队列管理门限、链路层协议配置等。在接口上使用 QCI 而不是传输一组 QoS 参数主要是为了减少接口上的控制

信令数据的传输量，并且使得不同设备、多系统间的互联更加容易。标准 QCI 属性如表 2.2 所示。

表 2.2 标准 QCI 属性

QCI	资源类型	优先级	数据包时延	数据包丢失率	典型业务
1	GBR	2	100 ms	10^{-2}	会话语音
2		4	150 ms	10^{-3}	会话视频(直播流媒体)
3		5	300 ms	10^{-6}	非会话视频(缓冲流媒体)
4		3	50 ms	10^{-3}	实时游戏
5	Non-GBR	1	100 ms	10^{-6}	IMS 信令
6		7	100 ms	10^{-3}	语音, 视频(直播流媒体), 交互式游戏
7		6	300 ms	10^{-6}	视频(缓冲流媒体), 基于 TCP 业务(例如 www, e-mail, ftp 等)
8		8			
9		9			

资源类型：表明其 QCI 对应的 QoS 是否为 GRB 承载，其相关的专有网络资源能否被恒定的分配。

优先级：用来区分相同或者不同 UE 的业务数据流集合。每个 QCI 对应一个优先级，其中优先级 1 是最高优先级级别。

数据包时延预算 (Packet Delay Budget, PDB)：用于表示数据包在 UE 和 PDN-GW 之间可能被延迟的时间，引入 PDB 参数的目的是支持时序和链路层功能的配置。对于同一个 QCI 等级，PDB 值在上行方向和下行方向相同。

数据包丢失率：(Packet Loss Rate, PLR)：定义为已经被发送端链路层处理但没有被接收端成功传送到上层 SDU 的比率，PLR 参数实际体现了非拥塞情况下数据包丢失率的上限。引入 PLR 参数的目的是考虑何时的链路层协议配置。对于某一个特定的 QCI 等级，PLR 值在上行方向和下行方向是相同的。

2.4.2 TFT 的研究^[11]

传输流模板 (Traffic flow template, TFT) 是一组业务数据流 (Service Data Flow, SDF) 的集合体。每个 SDF 对应 TFT 中的一个数据包过滤器，每一个 EPS 承载关联着一个 UE 的上行 TFT 和一个 PDN-GW 的下行 TFT。如图 2.6 所示。

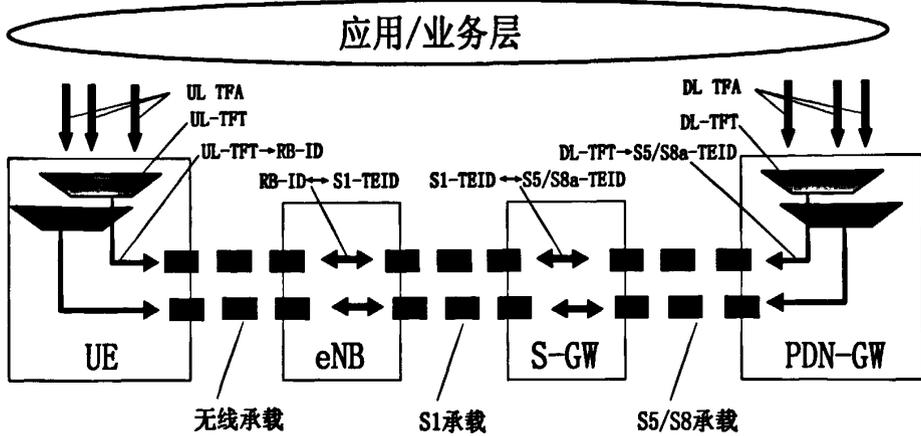


图 2.6 基于 GTP 协议的 EPS 承载

首先，UE 根据需求，将一个或多个上行 SDF 绑定成一个 EPS 承载，并发送给核心网。这组 SDF 集合称为传输流汇聚 (Traffic Flow Aggregates, TFA)。核心网同 UE 协商之后，在 S-GW 实现 S1 承载与 S5/S8 承载之间的映射，创建 S1 承载与 S5/S8 承载之间的绑定；在 eNodeB 实现无线承载与 S1 承载之间的一一映射，创建无线承载与 S1 承载之间的绑定；UE 实现 UL TFT 与无线承载之间的一一映射，创建 TFA 与无线承载之间的绑定。最终，EPS 承载数据通过无线承载、S1 承载以及 S5/S8 承载的级联，实现了 UE 对外部 PDN 网络之间 PDN 连接业务的支持。

TFT 作为业务数据流的集合体，由一组数据包过滤器(Packet filter)组成。每一个数据包过滤器的结构如下表所示：

表 2.3 TFT 结构

8	7	6	5	4	3	2	1	
0	0	direction		packet filter identifier				Octet 1
packet filter evaluation precedence								Octet 2
Length of Packet filter contents								Octet 3
packet filter contents itself								Octet 4
								Octet n

具体参数说明如下：

packet filter identifier: 用来标识这个 packet filter，长度为 4 个 bit。

direction: 表明此数据包过滤器应用的方向。具体的编码如下：

00 - pre Rel-7 TFT filter，兼容 TD TFT

01 - downlink only，用于网络端

10 - uplink only，用于 UE 端

11 - bidirectional，双向

packet filter evaluation precedence: packet filter 最重要的参数, 用来标识这个 packet filter 的优先级每个 packet filter 的优先级是不同的, RABM 依据优先级的不同, 将不同的数据做分组传送。

Length of Packet filter contents: 每个 Packet filter 有一个或多个组件构成, Length of Packet filter contents 表示各个组件的总长度。

packet filter contents itself: 详细描述每个组件的具体内容。每一种组件都代表一种特殊的含义。应用层传输的数据都要依据其优先级和是否与组件匹配来确定是否能够传输。

2.5 非接入层数据传输重要模块

2.5.1 会话管理模块^[12-15]

2.5.1.1 会话管理流程

ESM 层的主要功能是处理 UE 和 MME 之间 EPS 承载上下文。包括如下两种过程:

- 1, 网络激活、修改和释放 EPS 承载上下文。
- 2, UE 请求资源, 例如对一个 PDN 网络进行 IP 连接、专用承载资源等。

每一个 EPS 承载上下文描述一个 UE 和 PDN 网关之间的 EPS 承载。EPS 承载的激活与否不依赖于信令链接是否存在, 即当 UE 和 MME 之间的无线承载和 S1 承载释放时, EPS 承载上下文仍可以处于激活状态。

当 UE 连接到一个 PDN 网络时需要建立一个 EPS 承载, 并且在连接到 PDN 网络的整个过程期间建立的这个承载都将被保留, 这可以给 UE 提供到 PDN 网络的永远在线的 IP 连接, 这个承载就是默认承载。任何其他的连接到相同的 PDN 网络的 EPS 承载都是专用承载。默认承载的基于签约数据的初始承载级别 QoS 参数由网络分配, 决定建立或修改一个专用承载仅能由 EPC 执行, 并且承载级别 QoS 参数值一直由 EPC 分配。

为了能够真正实现永远在线的目的, LTE 系统在开机注册的时候会伴随有默认承载的建立。当用户发起业务, 需要特定的 QoS 和(或)TFT 时, UE 会发起承载资源分配或承载资源修改过程。网络也可以单独发起一个专用承载的建立、修改和释放。这些过程会在下面几节中具体描述。

ESM 过程只有在 UE 和 MME 间的 EMM 上下文建立后被执行。首次默认 EPS 承载上下文的建立在 EPS Attach 过程中执行。UE 成功 EPS Attach 后, 还能够进行

多 PDN 连接的建立。

UE 能够请求网络分配、修改或者释放额外的 EPS 承载资源。网络决定是否执行 UE 的请求。网络通过激活一个新的专有承载上下文或者修改现有 EPS 承载上下文来响应 UE 的请求。

大体上, ESM 过程分为网络发起的 ESM 过程和 UE 发起的 ESM 过程两种。具体过程如下所述。

A) 网络发起的 ESM 过程

此类过程由网络发起, 用于处理 EPS 承载上下文。

1, 默认承载建立过程

默认承载上下文激活过程的目的是在 UE 和 EPC 之间建立默认 EPS 承载上下文。网络发起默认 EPS 承载上下文激活过程, 来响应 UE 的 PDN CONNECTIVITY REQUEST 消息。如果默认承载上下文激活过程作为 EPS Attach 过程的一部分, 那么当 EPS Attach 过程失败时, UE 认为默认承载上下文激活过程也失败。

MME 通过发送 ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST 消息发起默认承载上下文激活过程, 首次默认承载在 EPS Attach 过程期间被激活。一旦 UE 成功附着之后, UE 便可以请求 MME 连接到额外的 PDN 网络。对于每一个额外的 PDN 连接, MME 需要激活单独的默认 EPS 承载。一个默认 EPS 承载在 PDN 连接期间一直处于激活状态。

当默认承载上下文作为 EPS Attach 过程的一部分被激活时, MME 将 ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST 组装到 ATTACH ACCEPT 消息中一同发送给 UE。

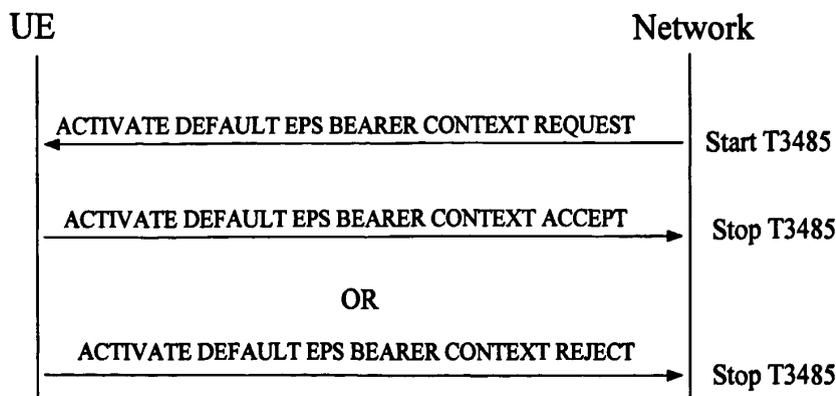


图 2.7 默认承载激活过程

收到 ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST 消息时, UE 发

送 ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT 消息给 MME。当默认承载作为 EPS Attach 过程的一部分被激活时，UE 将 ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT 组装到 ATTACH COMPLETE 消息中一同发送。

当默认承载激活请求是为了响应一个单独的 PDN CONNECTIVITY REQUEST 消息时，UE 将单独发送 ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT 消息。

2. 专用承载建立过程

专用承载上下文激活过程的目的是在 UE 和 EPC 之间,应用特定的 QoS 和 TFT 建立一个 EPS 承载上下文。网络能够单独发起专用 EPS 承载上下文激活过程, UE 可以依靠承载资源分配过程或承载资源修改过程请求此过程。专用承载上下文激活过程可以是 EPS Attach 过程的一部分, 如果 ATTACH 过程失败, UE 认为专用承载激活过程失败。

一个专有承载上下文总是和一个默认承载上下文相关联。专有承载上下文用于描述 UE 和 PDN 之间额外的 EPS 承载资源。网络可以在默认承载上下文建立或者之后的直至默认承载释放之前的任意时间发起专有承载激活过程。

专用 EPS 承载上下文可以在没有影响默认 EPS 承载上下文时被释放。当默认承载上下文被释放, 那么所有和它关联的专用承载上下文也将被释放。

专有 EPS 承载上下文激活过程可以由网络单独发起, 也可以作为承载资源分配过程或者承载资源修改过程的响应由 UE 触发。MME 通过发送 ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST 消息发起专用承载上下文激活过程, 此时会开启定时器 T3485。具体消息流程如图 2.8 所示。

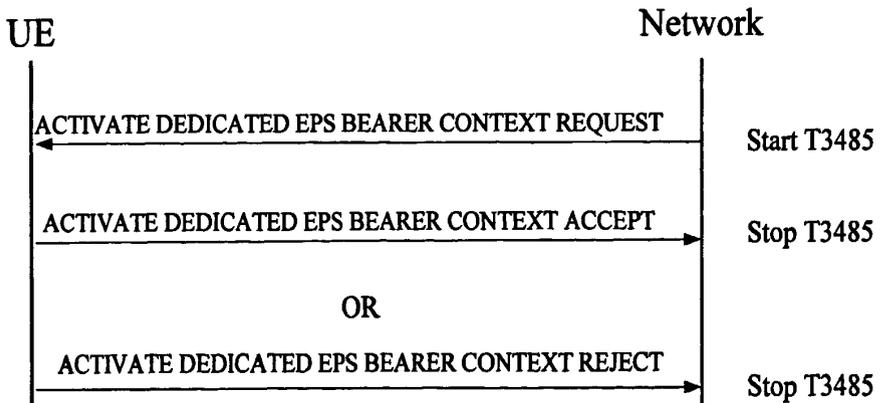


图 2.8 专用承载激活过程

收到 ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST 消息, UE 在应用此 EPS 承载前首先检查接收到的 TFT。确认无误后 UE 将发送 ACTIVATE

DEDICATED EPS BEARER CONTEXT ACCEPT 消息给网络。

ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST 消息包含两个重要参数：EPS bearer identity IE 和 linked EPS bearer identity IE，分别用来标识此 EPS 承载和其对应的默认 EPS 承载。

3, EPS 承载修改过程

EPS 承载上下文修改过程的目的是修改 EPS 承载上下文使其符合特定的 QoS 和 TFT。EPS 承载上下文修改过程是由网络发起的，但也可以作为承载资源分配过程或承载资源修改过程的一部分被激活。默认和专用 EPS 承载上下文都可以被修改。

EPS 承载上下文修改过程可以由网络单独发起，也可以作为承载资源分配过程或者承载资源修改过程的响应由 UE 触发。MME 通过发送 MODIFY EPS BEARER CONTEXT REQUEST 消息发起 EPS 承载上下文修改过程，此时会开启定时器 T3486。MME 在 MODIFY EPS BEARER CONTEXT REQUEST 消息里包含一个 EPS 承载标识来标识被修改的 EPS 承载。

收到 MODIFY EPS BEARER CONTEXT REQUEST 消息，UE 在应用此 EPS 承载前首先检查接收到的 TFT。确认无误后 UE 将发送 MODIFY EPS BEARER CONTEXT ACCEPT 消息给网络。MME 收到 MODIFY EPS BEARER CONTEXT ACCEPT 消息时，将停止定时器 T3486。

4, EPS 承载去激活过程

EPS 承载上下文去激活过程的目的是释放一个 EPS 承载上下文或通过去激活所有的 EPS 承载上下文，使其从 PDN 网络断开。EPS 承载上下文去激活过程是由网络发起，UE 可以通过承载资源修改过程或 PDN 去连接过程触发。

EPS 承载上下文去激活过程可以由网络单独发起，也可以作为承载资源修改过程或者 PDN 去连接过程的响应由 UE 触发。MME 通过发送 DEACTIVATE EPS BEARER CONTEXT REQUEST 消息发起 EPS 承载上下文去激活过程，此时会开启定时器 T3495。

收到 DEACTIVATE EPS BEARER CONTEXT REQUEST 消息，UE 根据消息中的 EPS 承载标识删除 EPS 承载上下文。在去激活相应的 EPS 承载上下文后，UE 回复 DEACTIVATE EPS BEARER CONTEXT ACCEPT 消息给 MME。当接收到 DEACTIVATE EPS BEARER CONTEXT ACCEPT 消息，MME 将停止定时器 T3495。

如果 DEACTIVATE EPS BEARER CONTEXT REQUEST 消息中指示的 EPS 承载标识是一个连接到 PDN 网络的默认承载，UE 将删除与此 PDN 连接相关的包括默认承载和专有承载在内的所有 EPS 承载上下文。

B) UE 发起的 ESM 过程

此类过程由 UE 发起,用于 UE 请求或释放承载资源。例如连接到一个新的 PDN 网络、请求专有承载资源或者从 PDN 网络断开。

1, PDN 连接过程

UE 请求 PDN 连接的目的是 UE 对 PDN 请求建立一个默认 EPS 承载。UE 通过发送 PDN CONNECTIVITY REQUEST 消息给网络来请求连接到一个 PDN 网络。如果网络接受,网络将发起默认承载上下文建立过程。该过程可被用于建立首次默认承载上下文(包含在最初的 ATTACH REQUEST 消息里),也可以在随后为额外 PDN 建立默认承载,用以允许 UE 并行接入多个 PDN 网络。

当 UE 连接到一个 PDN 网络时,UE 会发起一个 PDN 连接过程(PDN connectivity procedure)。UE 发送 PDN CONNECTIVITY REQUEST 消息给 MME,发起 PDN 连接过程。如果网络同意,网络会发起默认 EPS 承载上下文激活过程;如果网络拒绝,则发送 PDN 连接拒绝消息给 UE。其中,相关定时器的开启与关闭如图 2.9 所示。

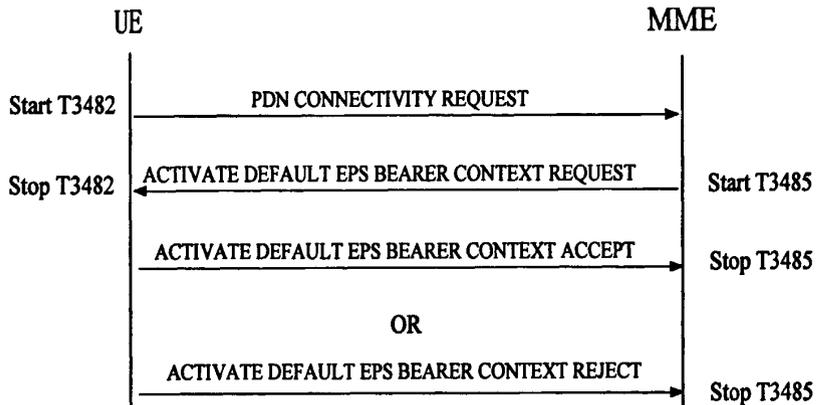


图 2.9 网络接受 PDN 连接过程

特殊的,在 UE 注册时会伴随有首次 PDN 连接的建立。此时 PDN 连接过程会伴随 ATTACH 过程同时进行。同时根据此 ESM 消息是否需要保护,网络会决定是否发起一个 ESM 信息请求 (ESM information request procedure) 过程。其中,相关定时器的开启与关闭如图 2.10 所示,其中虚线部分表示此消息是有条件发送的。

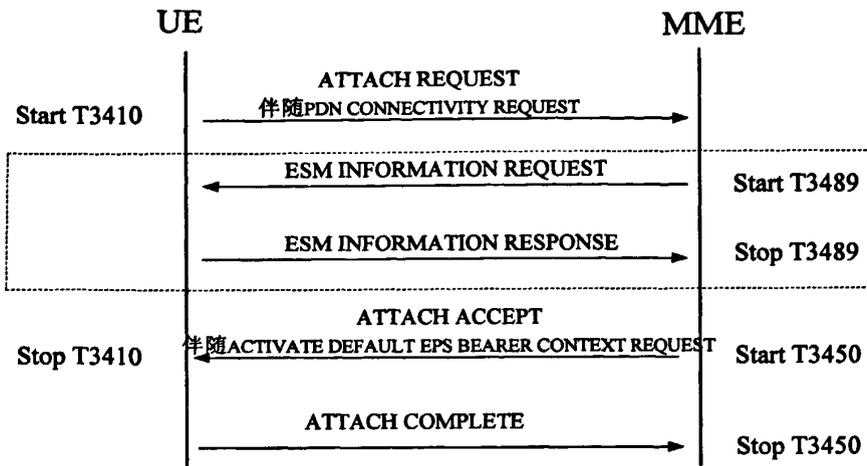


图 2.10 ATTACH 过程中的 PDN 连接过程

2. PDN 去连接过程

UE 请求 PDN 断开过程的目的是 UE 请求从一个 PDN 断开。当 UE 存在多个 PDN 网络连接时，可以发起此过程用于从一个特定的 PDN 网络断开。此时，对于所有的连接到此 PDN 网络的 EPS 承载上下文，包括专用 EPS 承载上下文都将被释放。

当 UE 从一个 PDN 网络断开时，UE 发送 PDN DISCONNECT REQUEST 消息给 MME，发起 PDN 去连接过程。当网络接受此请求，网络会发起 EPS 承载上下文去激活过程；如果网络拒绝此请求，则发送 PDN 去连接拒绝消息给 UE。其中，相关定时器的开启与关闭如图 2.11 所示。

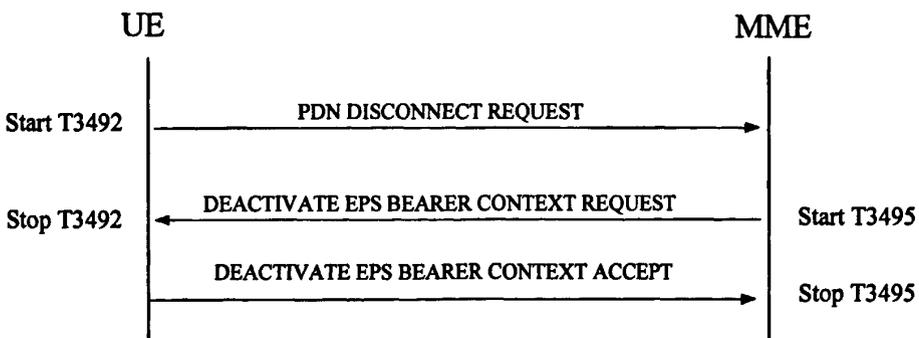


图 2.11 PDN 去连接过程 - 网络接受

3. 承载资源分配过程

UE 请求承载资源分配过程的目的是 UE 为一个 TFA(traffic flow aggregate)请求分配承载资源。UE 为一个新的 TFA 请求特定的 QoS demand(QCI)和 GBR 要求(可

选)。如果网络接受,那么网络会根据自身情况,调用专用承载激活过程或者是 EPS 承载上下文修改过程来响应 UE 的请求。

当 UE 请求分配新的承载资源时,UE 发送 BEARER RESOURCE ALLOCATION REQUEST 消息给 MME,发起承载资源分配过程。当网络接受此请求,网络根据当前激活的默认 EPS 承载上下文和 BEARER RESOURCE ALLOCATION REQUEST 消息的 Linked EPS bearer identity IE 中的 EPS 承载标识,发起专用 EPS 承载上下文激活过程或 EPS 承载上下文修改过程;当网络拒绝此请求,则发送承载资源分配拒绝消息给 UE。其中,相关定时器的开启与关闭如图 2.12 所示。

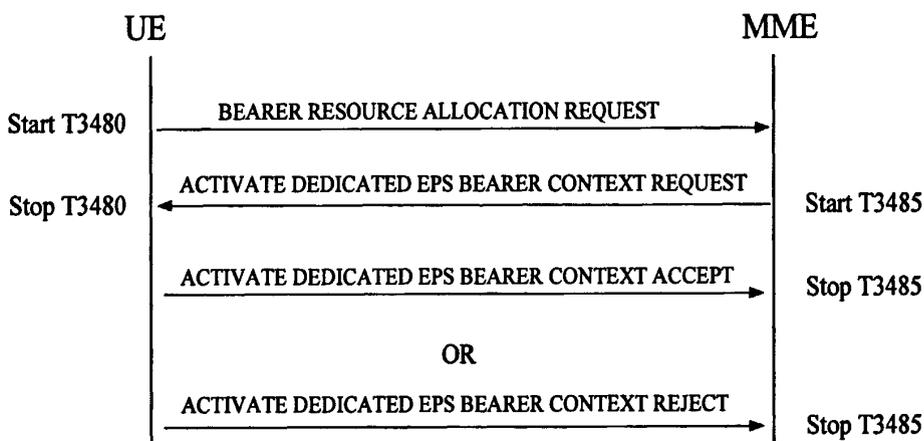


图 2.12 承载资源分配过程 --发起专用 EPS 承载激活

4. 承载资源修改过程

UE 请求承载资源修改程序的目的是 UE 为一个 TFA 请求修改或释放承载资源。当为一个 TFA 请求一个承载资源修改,UE 修改特定的 QoS demand (QCI)或现有的 GBR。如果网络接受,那么网络会根据自身情况,调用专用承载激活过程、EPS 承载上下文修改过程或者 EPS 承载上下文去激活过程来响应 UE 的请求。

当 UE 请求修改承载资源时,UE 发送 BEARER RESOURCE MODIFICATION REQUEST 消息给 MME,发起承载资源修改过程。当网络接受此请求,MME 检查 UE 请求的资源是否能够被建立或修改(通过核实 EPS bearer identity for packet filter IE 中的 EPS bearer identity),发起专用 EPS 承载上下文激活过程或 EPS 承载上下文修改过程或 EPS 承载上下文去激活过程;当网络拒绝此请求,则发送承载资源修改拒绝消息给 UE。其中,相关定时器的开启与关闭如图 2.13 所示。

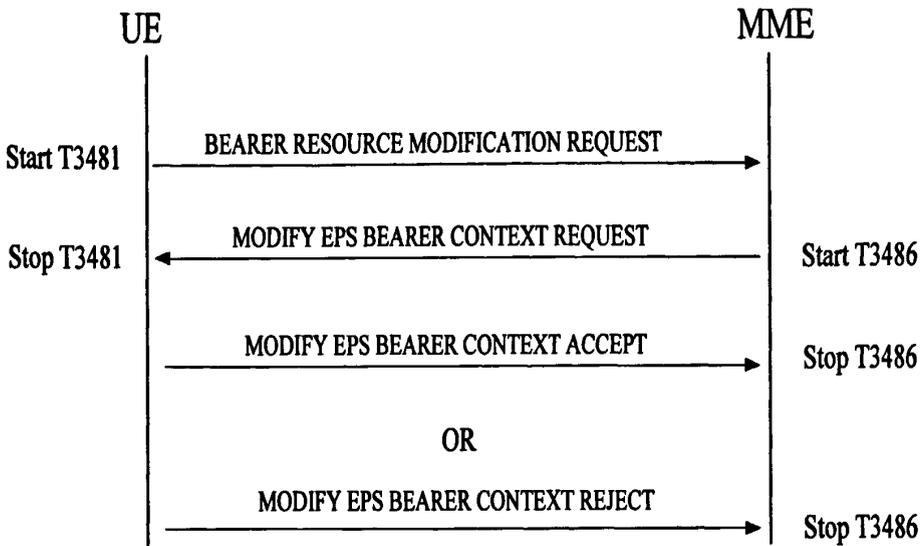


图 2.13 承载资源修改过程 --发起 EPS 承载修改过程

特殊的，UE 也可以通过承载资源修改相关过程去激活特定的 EPS 承载上下文。在此情况下，UE 需要将 ESM cause IE 的值设置为“regular deactivation”。其中，相关定时器的开启与关闭如图 2.14 所示。

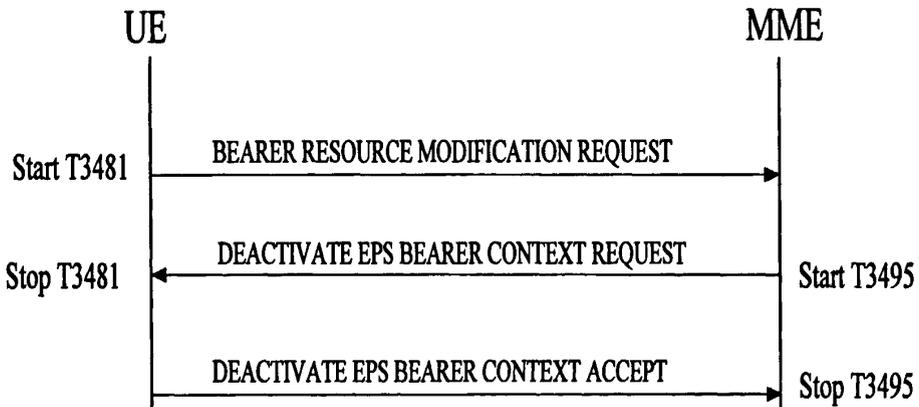


图 2.14 承载资源修改过程 --发起 EPS 承载去激活过程

2.5.1.2 IP 地址分配^{[12][17]}

UE 必须获得一个 IP 地址 (IPv4 或 IPv6) 才能接入到 PDN 网络。UE 获取 IP 地址可以在默认承载建立时进行，也可以在默认承载建立之后进行。如果在默认承载建立时 UE 没有获得 IP 地址，UE 可以通过 DHCP 方式获得 IP 地址。专用承载不单独分配的 IP 地址，使用其对应的默认承载的 IP 地址。

在激活默认承载时，网络可以通过两种方式为 UE 分配 IP 地址：分别为 P-GW

直接分配 IP 地址和 PDN 网络分配 IP 地址(外部 PDN 地址分配)。无论哪种方式,其分配的可以是动态的地址也可以是静态的地址。

当 UE 同时连接到多个 PDN 网络时,每个 PDN 的默认承载单独进行地址的分配。

UE 在申请默认承载激活时,可以指示网络以下三种 IP 类型: IPv4、IPv6、双栈。当 UE 申请双栈时,如果网络不支持双栈或者根据签约数据不允许用户使用双栈时,网络将把 IP 类型修改为 IPv4 或者 IPv6,只为 UE 分配一个版本的 IP 地址,并告知 UE 原因。在原因值为只支持单栈的情况下,UE 可以通过激活一个单栈的 PDN 连接来试图获得另一个版本的 IP 地址。网络只有在自己的能力和收到的 PDN 激活请求中 IP 类型都支持双栈时才给 UE 同时分配两个地址。

IPv4 地址的分配方法依赖于 UE 和网络的能力。不同于 2G/3G 系统,UE 在 PDN Address Allocation 参数中指示网络其所期望的 IPv4 地址获取方式:

1, UE 可以指示网络,它希望在激活默认承载的过程中得到 EPS 网络分配的 IPv4 地址

2, UE 也可以指示网络,它希望在默认承载建立以后通过 IETF 定义的各种流程来获得 IPv4 地址。在 EPS 网络允许的情况下,在默认承载的激活过程中,EPS 网络不直接分配 IPv4 地址给 UE。EPS 网络在给用户的消息中,将相应的地址地设置为 0.0.0.0 或不填。在默认承载建立完成后,UE 利用 EPS 承载来请求 DHCPv4 地址分配。

对于不能发送这种地址分配方式指示的早期 UE,网络应根据自己的策略决定具体的地址分配方式。

在得到一个 IPv6 前缀的情况下,UE 要能够通过无状态地址自动配置的方法来构造一个完整的 IPv6 地址。UE 收到 Attach Accept 消息以后,应忽略其中的 IPv6 前缀和接口地址,通过发送 Router Solicitation 消息从收到的 Router Advertisement 消息中获得 IPv6 前缀。该 IPv6 地址中的 64 位接口地址可以来自于网络,也可以由 UE 自己选定。

如果采用 DHCPv4/DHCPv6 分配方式,对 UE 而言 P-GW 是一个 DHCP 服务器。P-GW 可以从本地地址池中获取 IP,也可以作为 DHCP 客户端或者 Radius/Diameter 客户端从外部的 DHCP 服务器或者 Radius/Diameter 服务器获取 IP 地址和参数。UE 的标识信息,例如 IMSI/MSISDN 等,可以作为 DHCP/Radius/Diameter 地址分配的参数以尽量给 UE 分配相同的 IP 地址。

2.5.2 连接管理模块

2.5.2.1 附着管理^{[12][16]}

附着(ATTACH)过程的目的是使 EPS 服务的 PS 域业务附着到一个 EPC 中。在成功完成 ATTACH 过程后, 在 MME 中会建立一个 UE 的上下文, 并且在 UE 和 PDN-GW 之间建立了一个默认的承载, 使得“永远在线”的 IP 连接成为可能。网络也可以初始激活专有 EPS 承载作为 ATTACH 过程的一部分。

附着过程是 UE 获取 IP 连接能力的过程, 通常在 UE 开机, 或者做异系统切换时发起。附着过程是指用户在通过了接入层面的认证、授权之后, 完成移动 IP 注册的过程, 获取基本的 IP 连接能力。

2.5.2.2 业务请求

A) UE 发起的业务请求

对于注册状态下的 UE, 当处于 IDLE 模式且有 NAS 信令或者数据需要传输时, UE 将会触发业务请求过程。业务请求过程的目的是建立 NAS 信令连接, 即创建无线连接和 S1 连接。UE 将由 IDLE 状态迁移到 CONNECTED 状态。该过程由 UE 发起, 也可以由网络的寻呼请求触发。

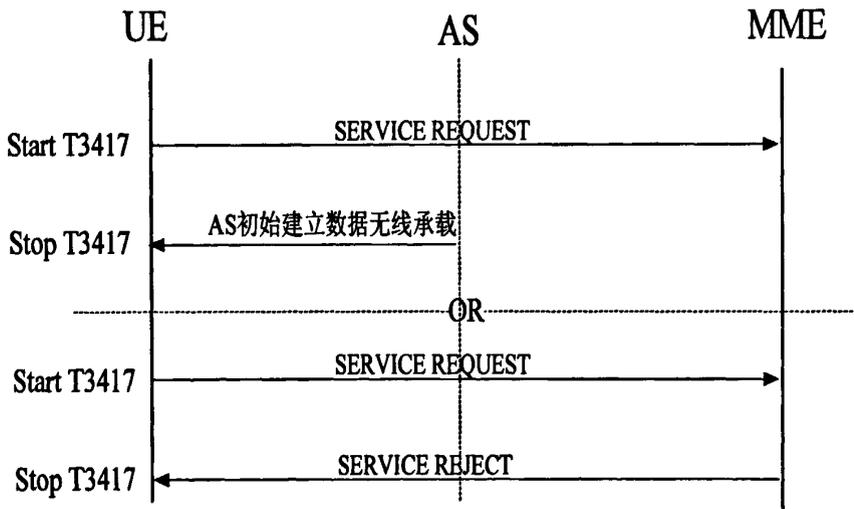


图 2.15 业务请求过程

如图 2.15 所示, IDLE 状态下 UE 发送业务请求消息给 MME, 为上层信令或者激活的承载预留资源而建立一条信令连接, 从而为后续的信令消息或者资源预留消息提供通道。

B) 网络发起的寻呼过程^{[12][18]}

寻呼过程作为网络主动发起的过程, 其目的如下:

- 1, 网络请求建立 NAS 信令。

- 2, 如果网络出现问题, 可以促使 UE 重附着。
- 3, 网络可以用寻呼来初始 MT CS fallback 过程。

网络端当有 NAS 信令, 或用户数据等待发送给 UE, 而此时 NAS 信令连接不存在, 网络将会初始一个用于 EPS 服务的寻呼过程。如图 2.16 所示, 为了初始寻呼过程, 网络侧的 EMM 实体会请求底层发起寻呼, 开启 T3413。UE 收到寻呼后, 将发起一个 SERVICE REQUEST 过程。如果 UE 接收到寻呼时正处于 EMM 特殊过程中, 或者业务请求过程中, UE 将会忽视该寻呼过程, 继续进行 EMM 特殊过程或者业务请求过程。

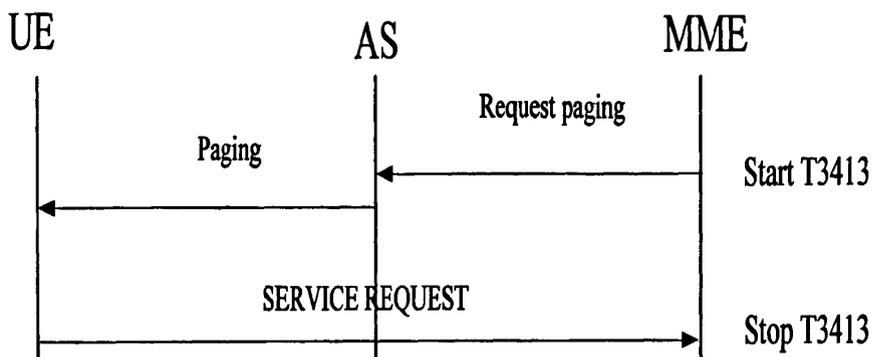


图 2.16 寻呼过程

2.6 数据传输框架^{[19][20]}

EPS 网络在 UE 和一个 PLMN 外部包数据网络 (PDN) 之间提供 IP 连接, 这就是 PDN 连接业务。在 PDN 连接业务存在期间会始终保持建立一个默认 EPS 承载, 来给 UE 提供永远在线的 IP 连接。连接到相同 PDN 的其他的 EPS 承载叫做专有承载。默认承载的建立过程包含在 ATTACH 过程中, ATTACH 和专有承载激活总体过程如图 2.17 所示。

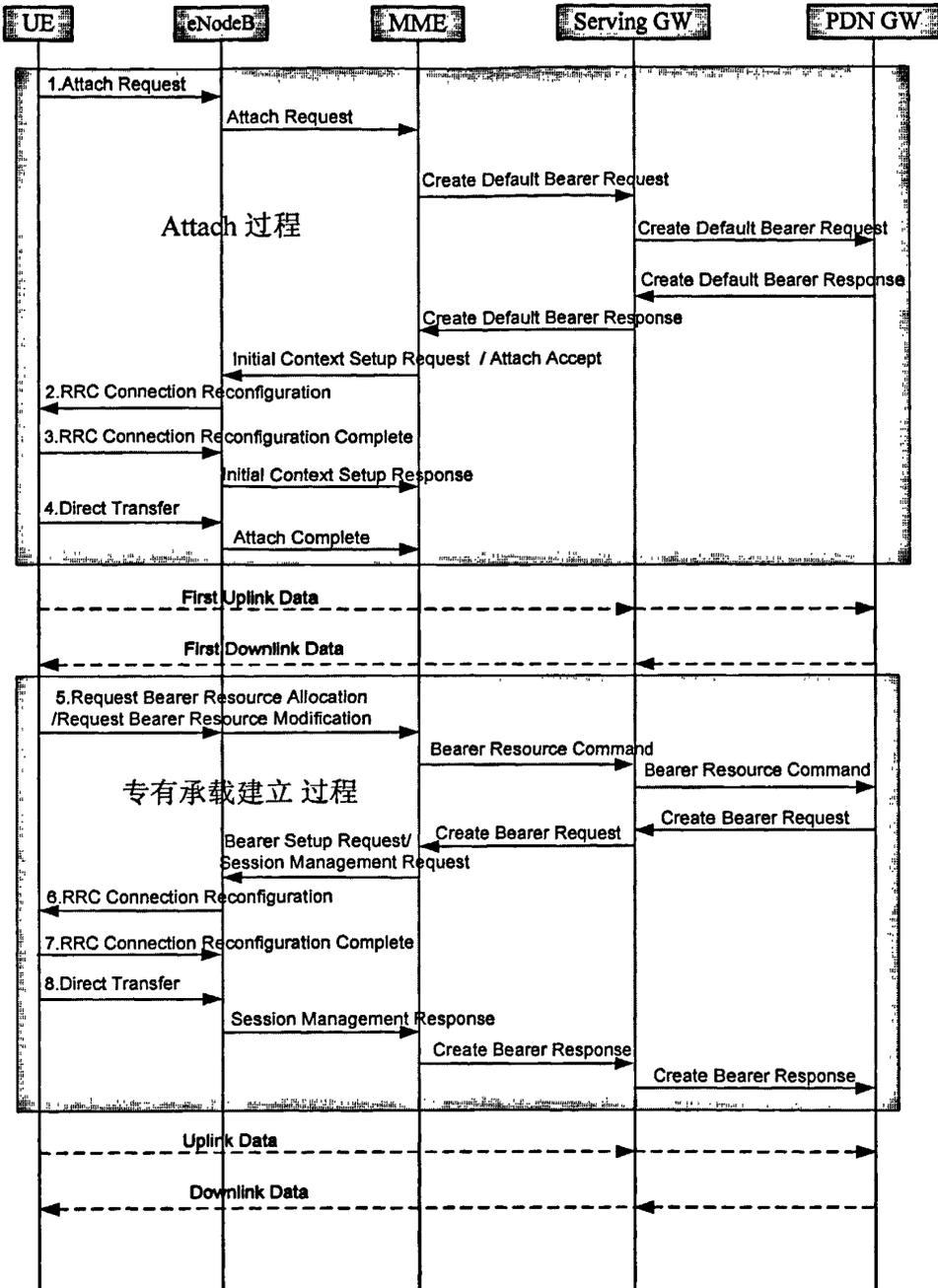


图 2.17 数据业务总体流程图

1, UE 发起附着请求消息以及网络选择指示给 eNB, 消息包含: IMSI 或旧的 GUTI,有效的上次访问的 TAI, UE 核心网络能力, UE 指定的 DRX 参数, PDN 类型, 协议配置选项 PCO, 加密选项传输标记, 附着类型, KSIASME, NAS 序列号, NAS-MAC 及附加的 GUTI。

2, eNodeB 发送 RRC 连接重配置消息给 UE, 其包含 EPS RB ID 和 Attach Accept 消息。

3, UE 发送 RRC 连接重配置完成消息给 eNodeB。

4, UE 发送一条 Direct Transfer 消息给 eNodeB, 该消息包含 Attach Complete (EPS Bearer Identity, NAS sequence number, NAS-MAC)消息。通过 Attach Complete 消息, UE 开始使用从 MME 指示的 NAS 安全算法。自此 ATTACH 过程结束, 默认承载建立完成, 可以使用默认承载来进行数据传输。

5, UE 发送一个 Request Bearer Resource Allocation 或 Request Bearer Resource Modification 消息给 MME, 请求承载资源分配。

6, eNodeB 将 EPS bearer QoS 匹配成 Radio Bearer QoS, 然后发送 RRC Connection Reconfiguration(Radio Bearer QoS, Session Management Request, EPS RB Identity)消息给 UE。UE 保存 Session Management Request 中的 QoS Negotiated, Radio Priority, Packet Flow Id 和 TI 信息, 以便 UE 在 GERAN 或者 UTRAN 接入时使用。UE NAS 保存 EPS Bearer Identity 并将该专有承载连接到 EBI 指示的缺省承载上。UE 使用 uplink packet filter (UL TFT)来决定业务数据流和无线承载之间的映射关系。

7, UE 发送 RRC Connection Reconfiguration Complete 消息给 eNodeB 确认无线承载的激活 radio bearer activation。

8, UE 发送 Direct Transfer (Session Management Response)消息给 eNodeB。Session Management Response 信元由 UE 在 NAS layer 构造, 其中包含 MME 分配的 EPS Bearer Identity。自此专有承载建立完成, 可以使用专有承载来进行数据传输。

2.7 本章小结

本章基于对 LTE 系统总体结构的介绍, 详细分析了 LTE 系统的各个组成部分。为实现非接入层数据传输, 详细描述了 LTE 系统 EPS 承载构架、QoS 构架和 TFT 构架等相关概念。之后详细介绍了会话管理相关过程、连接管理过程等为非接入层数据传输服务的相关过程。最后对从终端到网络端的整个的数据传输框架做了简单的描述, 为相关流程的设计提供依据。对于相关的流程的设计, 将在第三章展开。

第三章 非接入层数据传输的设计与实现

3.1 总体设计方案

依据图 2.3 对于 LTE 系统终端结构模的表述，设计 LTE 协议栈的结构如图 3.1 所示。

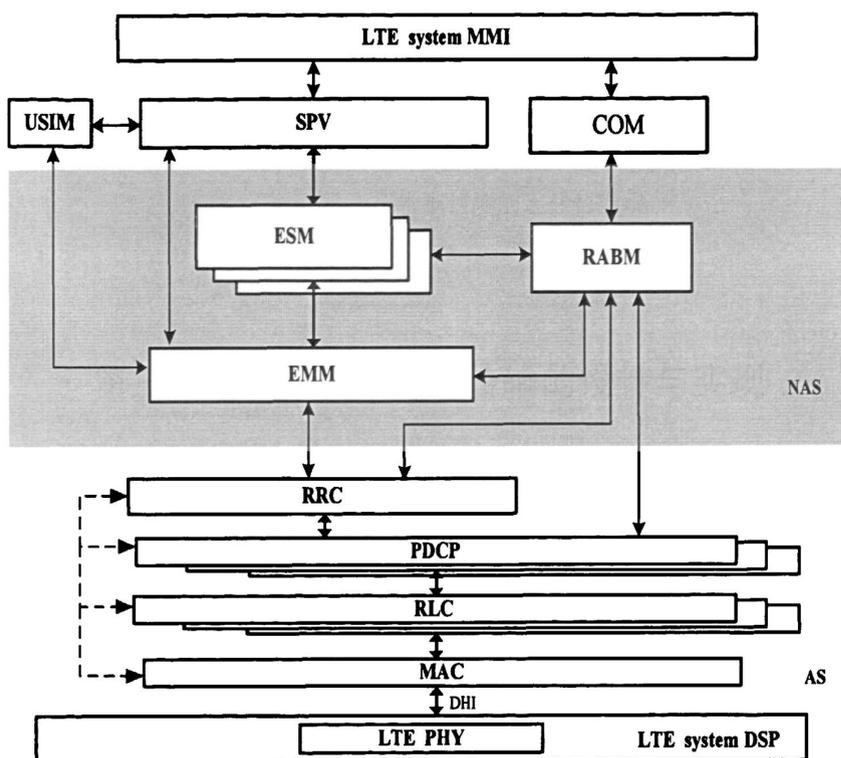


图 3.1 LTE 终端协议栈实现原理图

用户可以通过 MMI(人机接口)与 LTE 协议栈进行交互;LTE 协议栈经由 PHY(物理层)，通过空中接口协议与网络进行交互。

3.2 非接入层设计方案

为了更好的实现非接入层的数据传输，设计详细的非接入层结构很有必要。对于非接入层的数据传输，需求主要分为两部分：对会话的管理，以及建立 EPS 承载与 DRB 之间的映射关系。大体上，非接入层由 ESM、EMM 和 RABM 组成^{[9][19]}。RABM 主要负责建立 EPS 承载与 DRB 之间的映射关系，因而需要设计映射管理部

3.3.1 ESM 模块接口设计

依据协议 24.007 中关于 TD 接口相关原语的描述^[19]，设计 LTE 系统下 ESM 与 SSM、EMM 和 RABM 的相关接口。

由于 ESM 涉及的过程比较多，因而依据过程来设计接口原语可以使得接口原语内容明确，不易产生误解。把 ESM 相关接口的信号分为 PDN 连接相关信号、承载资源分配相关信号、承载资源修改相关信号、PDN 去连接相关信号、承载建立相关信号、承载修改相关信号、承载去激活相关信号等七类。详细的设计如下。

3.3.1.1 ESM_SSM 接口描述

ESM_SSM 接口主要是用来传输 PDN 连接与去连接请求、承载资源分配与修改请求、以及 EPS bearer context active、modify, deactivate 证实消息。

具体设计如表 3.1 所示：

表 3.1 ESM_SSM 接口信号

原语名	目标模块	信号用途说明
ESMREG_EPS_ACT_REQ	SSM→ESM	UE 发起 PDN 连接请求
ESMREG_EPS_ACT_ERR	ESM→SSM	网络拒绝 PDN 连接过程
ESMREG_EPS_ACT_IND	ESM→SSM	网络激活一个 EPS 承载
ESMREG_EPS_ACT_RSP	SSM→ESM	UE 同意 EPS 承载激活过程
ESMREG_EPS_ACT_REJ	SSM→ESM	UE 拒绝 EPS 承载激活过程
ESMREG_EPS_ALLOC_REQ	SSM→ESM	UE 发起承载资源分配请求
ESMREG_EPS_ALLOC_ERR	ESM→SSM	网络拒绝资源分配请求过程
ESMREG_EPS_MODIFY_REQ	SSM→ESM	UE 发起承载资源修改请求
ESMREG_EPS_MODIFY_ERR	ESM→SSM	网络拒绝承载资源修改请求
ESMREG_EPS_MODIFY_IND	ESM→SSM	网络发起一个 EPS 承载修改过程
ESMREG_EPS_MODIFY_RSP	SSM→ESM	UE 同意 EPS 承载修改过程
ESMREG_EPS_MODIFY_REJ	SSM→ESM	UE 拒绝 EPS 承载修改过程
ESMREG_EPS_DEACT_REQ	SSM→ESM	UE 发起 PDN 去连接过程
ESMREG_EPS_DEACT_ERR	ESM→SSM	网络拒绝 PDN 去连接过程
ESMREG_EPS_DEACT_IND	ESM→SSM	网络发起一个 EPS 承载去激活过程

根据协议规定，UE 必须接受网络发起的 EPS 承载去激活过程，因此在设计接口的时候并没有设计 UE 拒绝 EPS 承载去激活过程的相关接口。

3.3.1.2 EMM_ESM 接口描述

EMM_ESM 接口主要用来建立信令链路以及传输信令消息。

具体设计如表 3.2 所示：

表 3.2 EMM_ESM 接口信号

原语名	目标模块	信号用途说明
EMMESM_ESTABLISH_REQ	ESM→EMM	ESM 为激活一个 PDN 移动场景而要求建立一个 MM 连接。特殊的，在 ATTACH 过程中，此消息要携带 PDN CONNECTIVITY REQUEST 消息给 EMM
EMMESM_ESTABLISH_CNF	EMM→ESM	EMM 通知 ESM 已建立一个 MM 连接
EMMESM_ESTABLISH_REJ	EMM→ESM	EMM 通知 ESM 由于某种原因导致 EMM 上下文建立失败
EMMESM_RELEASE_IND	EMM→ESM	EMM 通知 ESM 释放正在激活或已经激活的 EPS 承载
EMMESM_DATA_REQ	ESM→EMM	ESM 向 EMM 传输信令数据
EMMESM_DATA_IND	EMM→ESM	EMM 向 ESM 传输信令数据

3.3.1.3 RABM_ESM 接口描述

RABM_ESM 接口主要是 ESM 通知 RABM, EPS bearer context 相关的信息变化。

具体设计如表 3.3 所示：

表 3.3 RABM_ESM 接口信号

原语名	目标模块	信号用途说明
RABMESM_ACTIVATE_IND	ESM→RABM	ESM 指示 RABM 激活的 EPS 承载
RABMESM_ACTIVATE_RSP	RABM→ESM	RABM 响应 ESM：由 ESM 指示的 EBI 已经开始使用，与该 EBI 相关的 DRB 已经建立
RABMESM_DEACT_IND	ESM→RABM	ESM 通知 RABM 该 EPS 承载已经被释放，以后不能使用
RABMESM_DEACTE_REQ	RABM→ESM	RABM 通知 ESM 由于 DRB 无效等原因需要去激活对应的 EPS 承载

3.3.2 RABM 子层接口设计

3.3.2.1 EMM_RABM 接口描述

EMM_RABM 之间的接口通信主要是为了进行 DRB 的重建, 该接口是在 EMM 模块与 RABM 模块之间, 用来定义与 EMM 信令传输相关的信号。

具体设计如表 3.4 所示:

表 3.4 EMM_RABM 接口信号

原语名	目标模块	信号用途说明
EMMRABM_REESTABLISH_REQ	RABM→EMM	RABM 实体请求 EMM 发起 SERVICE REQUEST 过程建立 DRB
EMMRABM_REESTABLISH_RSP	EMM→RABM	EMM 子层用来通知 RABM 实体: Service Request 消息已经被网络接收
EMMRABM_REESTABLISH_REJ	EMM→RABM	EMM 子层通知 RABM 实体: 使用 Service Request 过程重建 DRB 失败

3.3.2.2 RRC_RABM 接口描述

RRC_RABM 接口是在 RABM 模块与 ESM 模块之间, 用来定义与 ESM 信令传输相关的信号, 主要是指示 RABM 的建立情况。

具体设计如表 3.5 所示:

表 3.5 RRC_RABM 接口信号

原语名	目标模块	信号用途
RABMAS_ESTABLISH_IND	RRC→RABM	RRC 向 RABM 模块指示已建立的 DRB 列表
RABMAS_ESTABLISH_RSP	RABM→RRC	RABM 向 RRC 证实所建的 DRB 在上层所对应的 EBI 已激活情况
RABMAS_ESTABLISH_REJ	RABM→RRC	RABM 向 RRC 证实由于承载没有建立使得无线接入承载被拒绝
RABMAS_RELEASE_IND	RRC → RABM	RRC 向 RABM 指示由 EBI 所指的 DRB 被释放
RABMAS_RELEASE_RSP	RABM → RRC	RABM 通知 RRC 所建的 DRB 已被释放
RABMAS_STATUS_IND	RRC → RABM	RRC 模块通知 RABM 模块在数据

		传输中发生的错误情况
--	--	------------

3.3.2.3 RABM_COM 接口描述

RABM_COM 接口是在 RABM 模块与 COM 模块之间, 用来定义与数据传输相关的信号, 以及数据传输控制相关的信号。

具体设计如表 3.6 所示:

表 3.6 RABM-COM 接口信号

原语名	目标模块	信号用途说明
RABMCOM_DATA_REQ	COM→RABM	RABM 从 COM 接收数据
RABMCOM_DATA_IND	RABM→COM	RABM 收到下层数据传给 COM
RABMCOM_SUSPEND_IND	RABM→COM	RABM 通知 COM: 与 EPS 承载相关的 DRB 还未建立, 暂时不能传输数据
RABMCOM_RESUME_IND	RABM→COM	RABM 通知 COM: 与 EPS 承载相关的 DRB 建立完毕, 可以开始传输数据

3.3.2.4 PDCP_RABM 接口描述

PDCP_RABM 接口是 RABM 模块和 PDCP 模块之间的通信接口。该接口主要用来在用户平面传输用户数据。

具体设计如表 3.7 所示:

表 3.7 PDCP_RABM 接口信号

原语名	目标模块	信号用途
PDCPRABM_DATA_REQ	RAB→PDCP	RABM 请求将高层 PDU 传送给 PDCP
PDCPRABM_DATA_IND	PDCP→RAB	PDCP 将接收到的 PDCP PDU 传送给 RABM

3.4 ESM 详细设计

3.4.1 ESM 模块状态设计

3.4.1.1 状态划分

根据 EPS 承载所处的状态和 ESM 过程所处的状态, 并依据协议 24.301 中关于 ESM 状态的要求, 将 ESM 子层划分为如下 2 个状态:

BEARER CONTEXT INACTIVE: 表明现在不存在 EPS 承载上下文。

BEARER CONTEXT ACTIVE: 表明现在 EPS 承载上下文已经建立完成。

但在实际应用中, 如果按照这样的设计, 虽然状态机设计比较简单, 但由于每个状态的内容过于复杂, 不利于设计和实现。鉴于此, 将 BEARER CONTEXT ACTIVE 状态进行细化, 本文按照 ESM 实例的流程不同, 划分为 ACTIVE BEARER PENDING、MODIFY BEARER PENDING、BEARER RESOURCE ALLOC PENDING、BEARER RESOURCE MODIFY PENDING、PDN CONNECT PENDING、PDN DISCONNECT PENDING 六个状态, 使得能够更好的通过状态机来实现。

根据以上分析, ESM 状态划分如表 3.8 所示:

表 3.8 EPS 承载上下文状态划分

状态名称	简称	简述
BEARER CONTEXT INACTIVE	BCI	表示对应的承载还没有建立, 在该状态下终端可以发起 PDN 连接请求或者承载建立请求
BEARER CONTEXT ACTIVE	BCA	表示对应的承载已经建立完毕
ACTIVE BEARER PENDING	ABP	表示终端正在进行一个 EPS 承载的激活过程
MODIFY BEARER PENDING	MBP	表示终端正在进行一个 EPS 承载的修改过程。
BEARER RESOURCE ALLOC PENDING	RAP	表示终端正在进行一个承载资源分配请求
BEARER RESOURCE MODIFY PENDING	RMP	表示终端正在进行一个承载资源修改过程
PDN CONNECT PENDING	PCP	表示终端正在进行一个 PDN 连接过程
PDN DISCONNECT PENDING	PDP	表示终端正在进行一个 PDN 去连接过程

3.4.1.2 状态转换

由于 ESM 过程较多, 若总体设计会使工作量增大, 不利于细节的考虑。因此分为如下三部分分别考虑:

A) PDN 连接过程及承载建立相关状态跳转

与 PDN 连接过程及承载建立相关的状态包括: BCI、PCP、BCA、ABP 四个。其具体的跳转如图 3.3 所示。

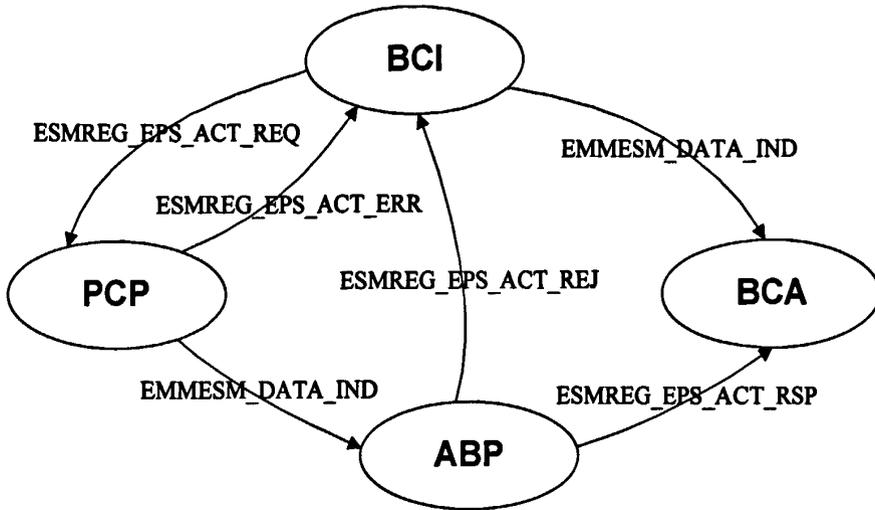


图 3.3 ESM 状态跳转 - 1

状态跳变说明：

1, 新创建的 ESM 实例处于 BCI 状态，当收到 ESMREG_EPS_ACT_REQ 信号后，表明将发起 PDN 连接过程，ESM 将跃迁到 PCP 状态。

2, 在 PDN 连接过程中，ESM 实例若收到 ESMREG_EPS_ACT_ERR 信号，表明 PDN 连接失败，则 ESM 跃迁到 BCI 状态，进而删除此 ESM 实例。

3, 在 PDN 连接过程中，ESM 实例若收到 EMMESM_DATA_IND 原语且原语中包含 ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST 消息时，ESM 进入 ABP 状态。

4, ESM 实例在 ABP 状态下，若收到 ESMREG_EPS_ACT_REJ 原语，表明 SSM 拒绝此承载的建立，ESM 实例将跃迁到 BCI 状态，进而删除此 ESM 实例。

5, ESM 实例在 ABP 状态下，若收到 ESMREG_EPS_ACT_RSP 原语，表明 SSM 同意建立此承载的建立，ESM 实例在通知 RABM 模块此承载建立完成之后跃迁到 BCA 状态。

6, ESM 实例在 BCI 状态下收到 EMMESM_DATA_IND 原语且原语中包含 ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST 消息时，ESM 进入 ABP 状态。

B) 承载资源分配过程、承载资源修改过程和 EPS 承载修改过程的相关状态跳转

与承载资源分配过程、承载资源修改过程和 EPS 承载修改过程相关的状态包括：BCA、RMP、MBP、MAP 四个。其具体的跳转如图 3.4 所示。

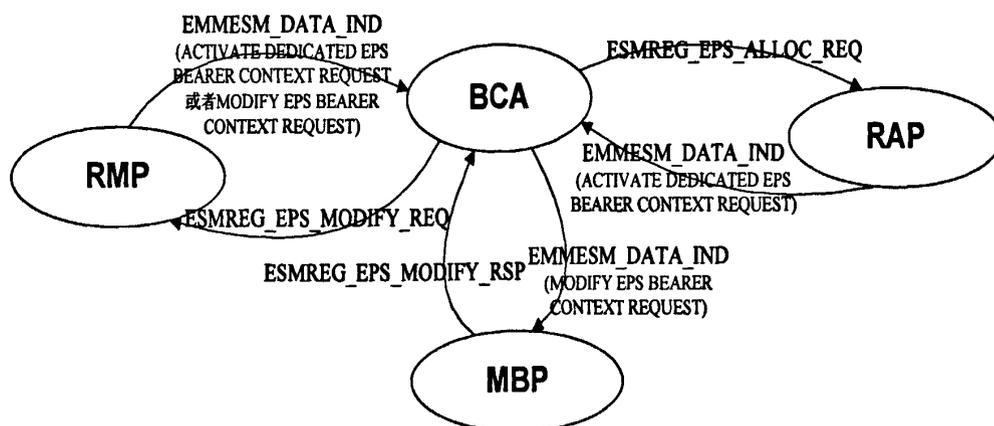


图 3.4 ESM 状态跳转 --2

状态跳变说明:

1, ESM 实例在 BCA 状态下收到 ESMREG_EPS_ALLOC_REQ 原语, 表明将发起承载资源分配过程, ESM 将跃迁到 RAP 状态。

2, ESM 实例在 RAP 状态下收到 EMMESM_DATA_IND 原语且原语中包含 ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST 消息时, 表明网络将要新建一个专有承载, 对于当前承载比不做改变。因而此 ESM 实例跃迁到 BCA 状态。

3, ESM 实例在 BCA 状态下收到 EMMESM_DATA_IND 原语且原语中包含 MODIFY EPS BEARER CONTEXT REQUEST 消息时, 表明网络发起修改 EPS 承载过程, 此时 ESM 实例跃迁到 MBP 状态。

4, ESM 实例在 MBP 状态下收到 ESMREG_EPS_MODIFY_RSP 原语或者 ESMREG_EPS_MODIFY_REJ 原语时, 表明 SSM 接受或者拒绝此 EPS 承载的修改。无论哪种情况, ESM 实例都将跃迁到 BCA 状态。

5, ESM 实例在 BCA 状态下收到 ESMREG_EPS_MODIFY_REQ 原语, 表明将发起承载资源修改过程, ESM 将跃迁到 RMP 状态。

6, ESM 实例在 RMP 状态下收到 EMMESM_DATA_IND 原语且原语中包含 ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST 消息或者 MODIFY EPS BEARER CONTEXT REQUEST 消息并且此 MODIFY EPS BEARER CONTEXT REQUEST 消息标明需要修改的并非此 EPS 承载时, 表明网络对于当前承载不做改变。因而此 ESM 实例跃迁到 BCA 状态。

特别的, ESM 实例在 RMP 状态下收到 EMMESM_DATA_IND 原语且原语中包含 DEACTIVATE EPS BEARER CONTEXT REQUEST 消息时, 表明网络将去激活当前 EPS 承载, 此 ESM 实例跃迁到 BCI 状态, 进而删除此 ESM 实例。

C) PDN 去连接过程及承载去激活相关状态跳转

与 PDN 去连接过程及承载去激活相关的状态包括：BCI、BCA、PDP 三个。其具体的跳转如图 3.5 所示。

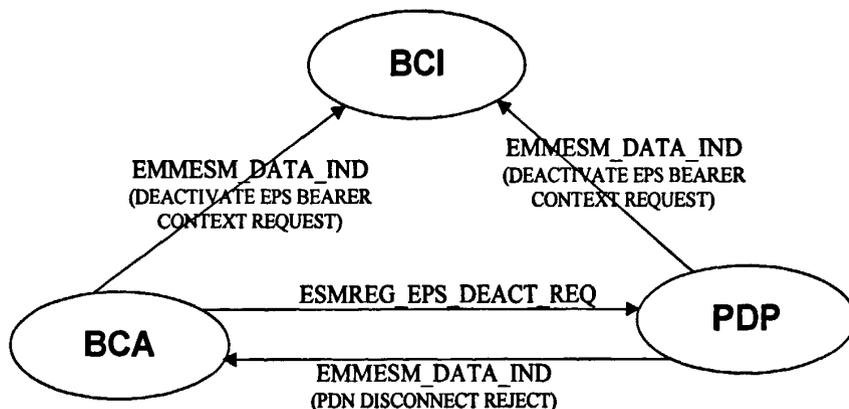


图 3.5 ESM 状态跳转 -- 3

状态跳变说明：

1, ESM 实例在 BCA 状态下收到 EMMESM_DATA_IND 原语且原语中包含 DEACTIVATE EPS BEARER CONTEXT REQUEST 消息时, ESM 进入 BCI 状态, 进而删除此 ESM 实例。

2, ESM 实例在 BCA 状态下收到 ESMREG_EPS_DEACT_REQ 原语, 表明将发起 PDN 去连接过程, ESM 将跃迁到 PDP 状态。

3, ESM 在 PDP 状态下收到 EMMESM_DATA_IND 原语且原语中包含 PDN DISCONNECT REJECT 消息时, 表明网络拒绝 PDN 去连接过程, 此时 ESM 实例进入 BCA 状态。

4, ESM 实例在 PDP 状态下收到 EMMESM_DATA_IND 原语且原语中包含 DEACTIVATE EPS BEARER CONTEXT REQUEST 消息时, ESM 实例进入 BCI 状态, 进而删除此 ESM 实例。

至此, 整个状态设计完成。

3.4.2 CMC 模块设计

由于 ESM 实体是多实例的, 如果整体考虑, 容易造成实例管理混乱等问题。为了更好地管理每一个 ESM 实例, 本文单独设计一个 CMC (Connection Management Control, 连接管理控制) 子模块, 它负责将发送到 ESM 模块的信号中转到相应的实例, 同时实现多个实例的创建、修改和删除。

在设计的时候本着简单易管理的原则, CMC 负责控制每个 ESM 实例, 使得所有发往 ESM 各实例的消息全部经由 CMC 转发。对于 ESMREG_EPS_ACT_REQ 等

没有确定实例发送的原语，全部发送到 CMC 模块，CMC 模块在收到 ESMREG_EPS_ACT_REQ 原语(以原语内容为 ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST 消息为例)的时候首先创建一个 ESM 实例，然后再将消息发送到这个新创建的实例。其结构如图 3.6 所示。

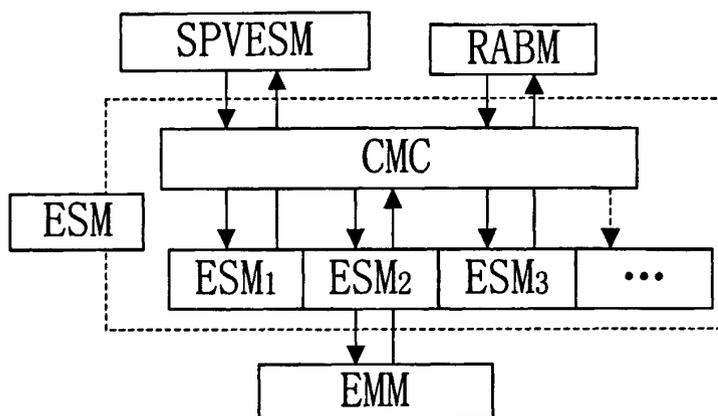


图 3.6 ESM 模块结构

3.5 会话管理流程设计

3.5.1 ATTACH 过程中的 PDN 连接流程设计

开机 ATTACH 过程是很多过程的综合体，为了描述方便，现将整个过程拆分为以下几个部分分别描述：

3.5.1.1 小区驻留

开机之后，系统首先初始化各个模块，包括：SPV、CMC、EMM、RRC 等。对于 ESM 模块，由于是多实例的，因而在开机时刻并不创建，使用的时候再行创建。限于篇幅以及本文的研究重点，本部分仅提及与 PDN 连接过程相关的内容。

具体流程如图 3.7 所示：

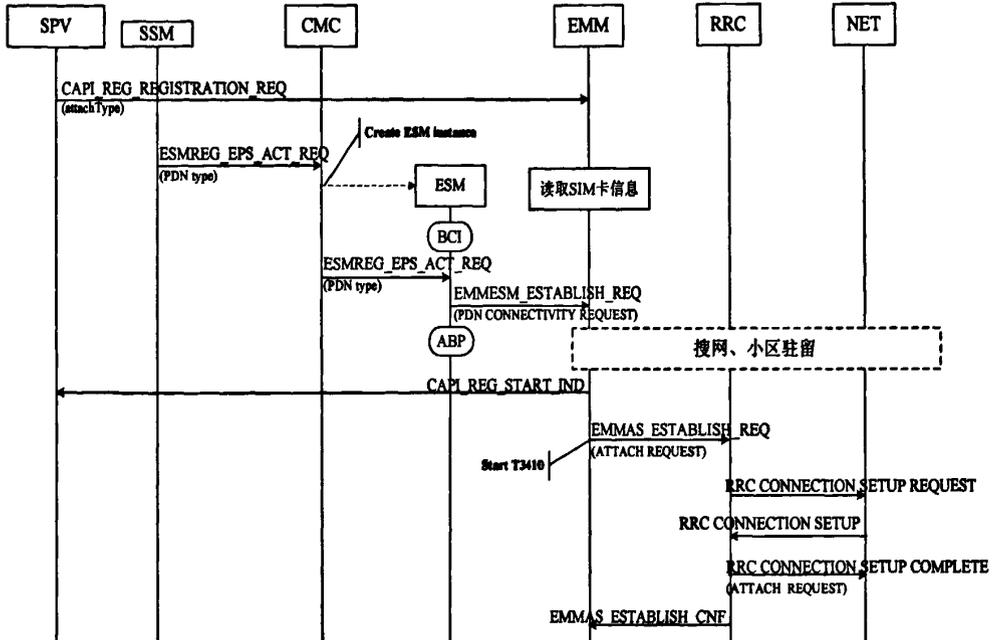


图 3.7 ATTACH 过程中的 PDN 连接过程-- 1

1, 开机之后 SPV 发送开机信号 CAPI_REQ_REGISTRATION_REQ 原语给 EMM, EMM 将读取 USIM 卡信息, 为 PLMN 选择以及小区驻留做准备; 同时 SPV 层的 SSM 子层发送 ESMREG_EPS_ACT_REQ 原语给 CMC. 为更好的表达, 将 SSM 独立于 SPV, 但 SSM 本质是仍然是 SPV 的一个子层。

2, CMC 创建一个 ESM 实例, 之后 CMC 将 ESMREG_EPS_ACT_REQ 原语发送给 ESM, ESM 发送 EMMESM_ESTABLISH_REQ 原语给 EMM, 在 EMMESM_ESTABLISH_REQ 原语中携带有 PDN CONNECTIVITY REQUEST 消息。

3, EMM 将引导执行搜网、小区驻留等过程。发送 CAPI_REG_START_IND 给 SPV 表明已经完成小区驻留。

4, EMM 将组装 ATTACH REQUEST 消息通过 RRC CONNECTION SETUP REQUEST 消息发送给网络。

至此, ATTACH 过程开始。

3.5.1.2 EMM 一般过程

ATTACH 过程开始之后, 网络将通过鉴权过程、身份认证过程以及安全模式控制过程, 确认 UE 的合法身份以及完成加密等操作, 具体流程如图 3.8 所示:

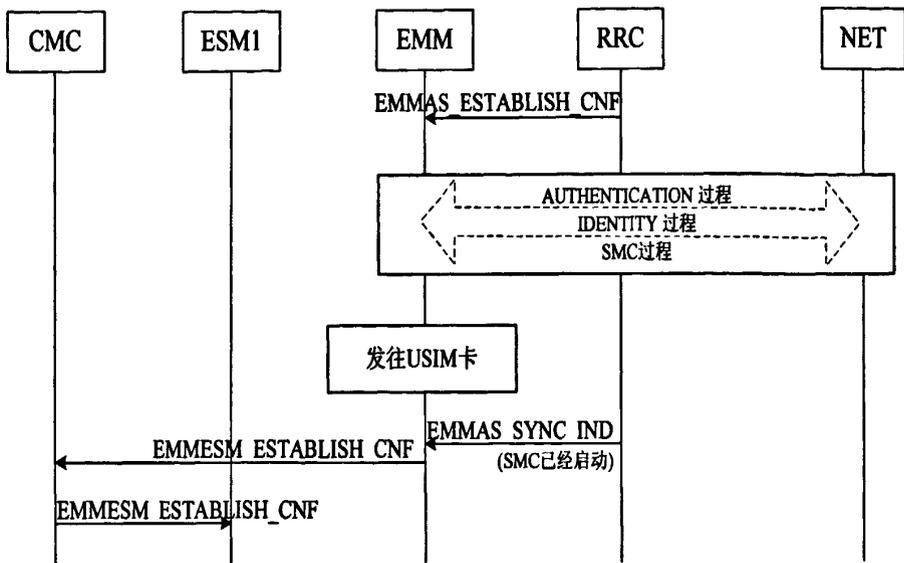


图 3.8 ATTACH 过程中的 PDN 连接过程--2

- 1, 鉴权过程、身份认证过程以及安全模式控制过程都是通过 EMM 来控制进行的。
- 2, EMM 收到 EMMAS_SYNC_IND 原语表明安全模式控制已经完成, 之后和网络的交互都要在加密的情况下进行。
- 3, 收到 EMMESM_ESTABLISH_CNF 原语之后, 表明一个 MM 连接已经建立。

3.5.1.3 建立 EPS 承载与 DRB 的映射关系

网络通过 RRC CONNECTION RECONFIGURATION 消息将 EPS 承载和 DRB 的映射关系通知给 UE, 同时将 ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST 消息通知 ESM。ESM 接收到 ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST 消息表明 PDN 连接过程已经结束, 默认承载建立过程即将开始。具体流程如图 3.9 所示:

- 1, 网络发送 RRC CONNECTION RECONFIGURATION 消息, RRC 解析其内容, 分别将 RABMAS_ESTABLISH_IND 原语和 EMMAS_DATA_IND 原语发送给 RABM 和 EMM。
- 2, RABM 根据 RABMAS_ESTABLISH_IND 原语的内容建立 EPS 承载和 DRB 的映射关系。
- 3, EMM 解析 EMMAS_DATA_IND 原语中的 ATTACH ACCEPT 消息, 之后将解析出来的 ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST 消息通过 CMC 发送给 ESM。

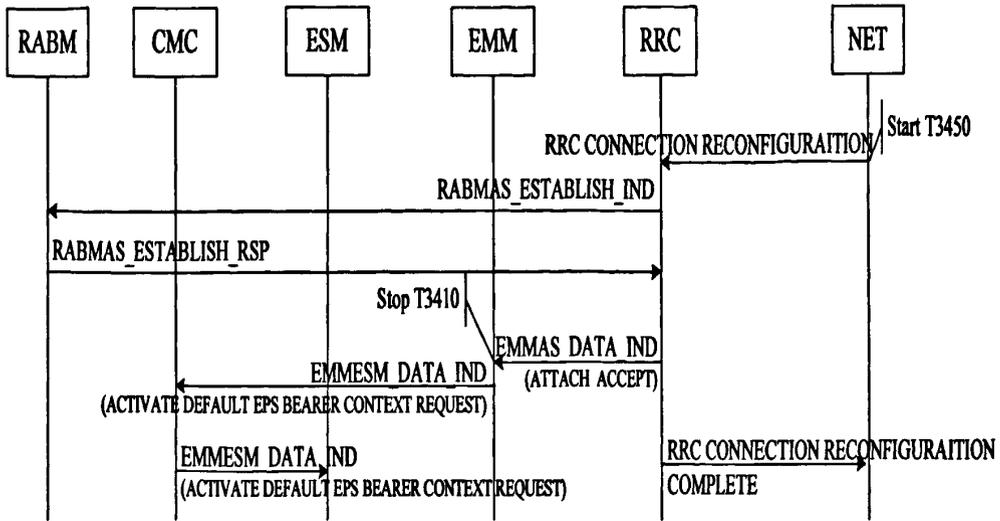


图 3.9 ATTACH 过程中的 PDN 连接过程-- 3

3.5.1.4 默认承载建立过程

默认承载建立可作为 ATTACH 过程的一部分。具体流程如图 3.10 所示：

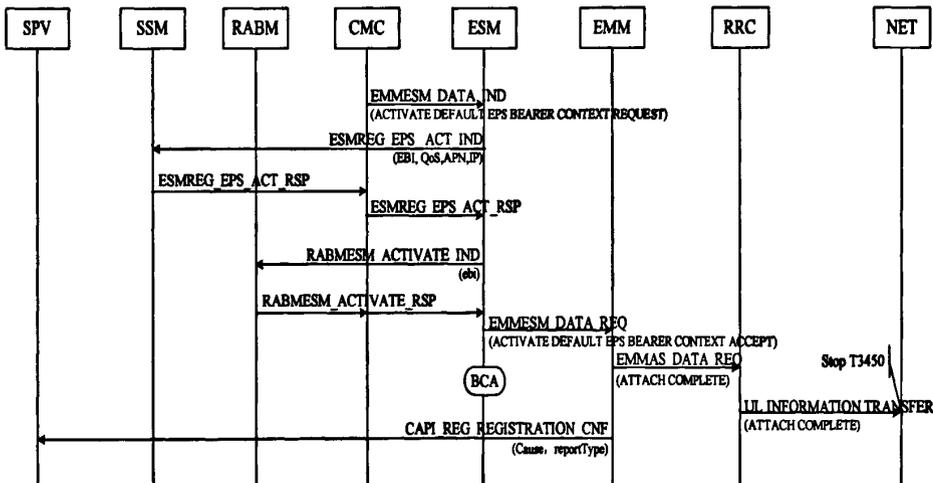


图 3.10 Attach 过程中的 PDN 连接过程-- 4

- 1, ESM 收到 ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST 消息后询问 SSM 默认承载是否能够建立。
- 2, 得到 SSM 的确认消息 ESMREG_EPS_ACT_RSP 后, 通知 RABM 建立的承载上下文。
- 3, 收到 RABM 的 RABMESM_ACTIVATE_RSP 消息, 表明 RABM 已经建立承载上下文与 DRB 之间的关系。
- 4, ESM 发送 ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT 消息, EMM 将此消息组装到 ATTACH COMPLETE 消息中通过 UL INFORMATION

TRANSFER 消息传送给网络。

自此，整个 ATTACH 过程结束，默认承载建立完成。

总结整个过程，有如下几点需要注意：

1，在 ATTACH 过程中，PDN CONNECTIVITY REQUEST 消息是组装到 ATTACH REQUEST 消息中发送的。

2，ATTACH REQUEST 消息是组装到 RRC CONNECTION RECONFIGURATION COMPLETE 消息中发送给网络的。

3，RRC CONNECTION RECONFIGURATION 消息包含有 EPS 承载于 DRB 的映射关系，以及 ATTACH ACCEPT 消息。

4，ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT 消息是组装到 ATTACH COMPLETE 消息中通过 UL INFORMATION TRANSFER 消息发送给网络的。

3.5.2 承载资源分配流程设计

UE 在建立 PDN 连接之后，对于特定的数据，需要申请特定的承载资源。此时，UE 将会发起承载资源分配过程。

对于承载资源分配过程，网络会根据当前资源的大小以及 UE 请求的资源的大小来决定是以专有承载建立过程还是 EPS 承载修改过程来响应 UE 的请求。

现以网络用专有承载建立过程来响应 UE 的请求为例来详细描述整个过程。

3.5.2.1 UE 发起承载资源分配过程

当 ESM 收到 SSM 发来的 ESMREG_EPS_ALLOC_REQ 原语时表明 UE 将发起承载资源分配过程。ESM 首先检查当前 MM 连接是否存在，如不存在则通过业务请求流程建立 MM 连接。具体流程如图 3.11 所示：

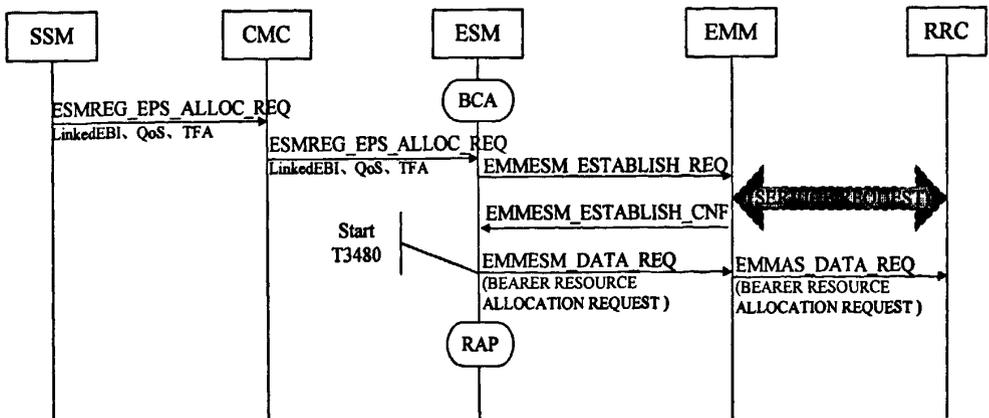


图 3.11 承载资源分配过程-UE 发起

1, 在 ESMREG_EPS_ALLOC_REQ 原语中包含有 UE 请求的承载资源, 包括 QoS、TFA 等内容。同时为了使网络能够区分不同 PDN 的默认承载, 因而在 ESMREG_EPS_ALLOC_REQ 原语中添加参数 LinkedEBI 来指明其默认承载。

2, ESM 实例在收到 ESMREG_EPS_ALLOC_REQ 原语后首先检查 MM 连接是否存在, 发送 EMMESM_ESTABLISH_REQ 原语给 EMM, 当 EMM 存在 MM 连接时响应 ESM 原语 EMMESM_ESTABLISH_CNF。此时 ESM 认为 MM 连接已经存在, 发送 EMMESM_DATA_REQ 给 EMM 通过空口发送给网络。

3.5.2.2 CMC 接收 EMMESM_DATA_IND 原语

CMC 收到 EMMESM_DATA_IND 原语后, 解析消息类型以及 LinkedEBI、PTI 等参数, 确定下一步的行为。整个过程如图 3.12 所示:

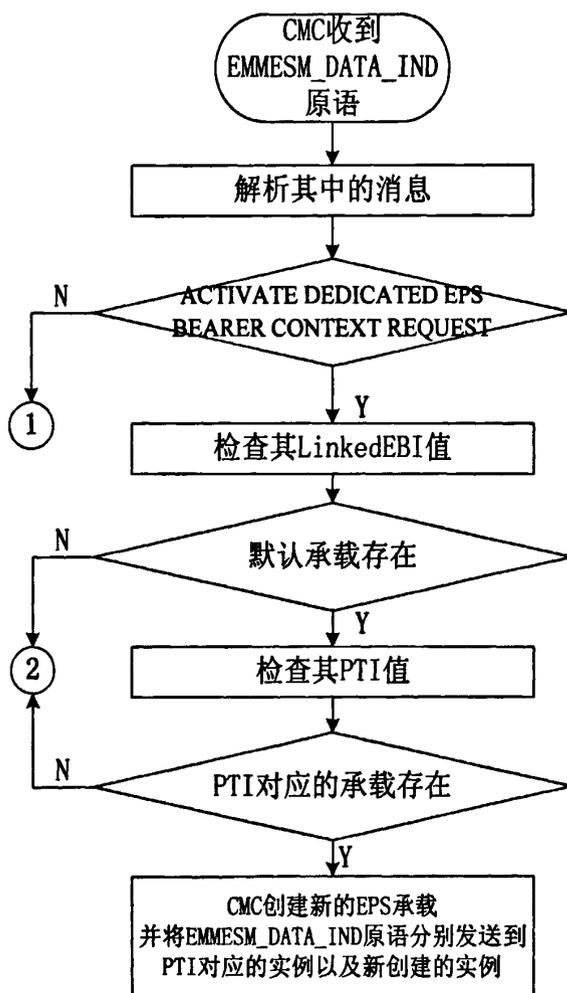


图 3.12 CMC 接收 EMMESM_DATA_IND 原语

对于①, CMC 将检查其消息类型是否为 MODIFY EPS BEARER CONTEXT REQUEST 消息。若是, 则将进行 EPS 修改刚才; 若不是, CMC 将忽略这条原语,

等待网络的再次响应。

对于②，CMC 由于检查不到其相关承载的存在，将直接回复 EMMESM_DATA_REQ 原语给 EMM，原语中包含消息 ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT 消息，其中原因值为 ESM cause #43 "invalid EPS bearer identity"或者#47 "PTI mismatch"。

CMC 接收 EMMESM_DATA_IND 原语后的行为如图 3.13 所示：

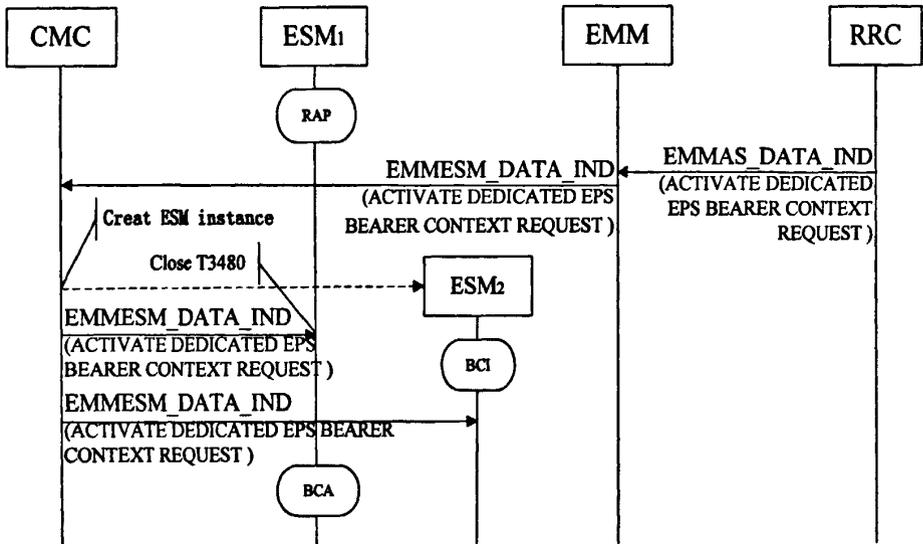


图 3.13 承载资源分配过程——CMC 的处理

3.5.2.3 专有承载建立

ESM 实例 1 收到 EMMESM_DATA_IND 原语后结束承载资源分配过程；ESM 实例 2 收到 EMMESM_DATA_IND 原语后进行专有承载建立过程。具体流程如图 3.14 所示。

1, ESM 实例 1 收到 EMMESM_DATA_IND 原语后结束承载资源分配过程，跃迁到 BCA 状态。

2, ESM 实例 2 收到 EMMESM_DATA_IND 原语后开启专有承载建立过程，发送 ESMREG_EPS_ACT_IND 原语给 SSM，发送 RABMESM_ACTIVATE_IND 原语给 RABM，发送 EMMESM_DATA_REQ 原语给 EMM，将 ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT 消息给网络。

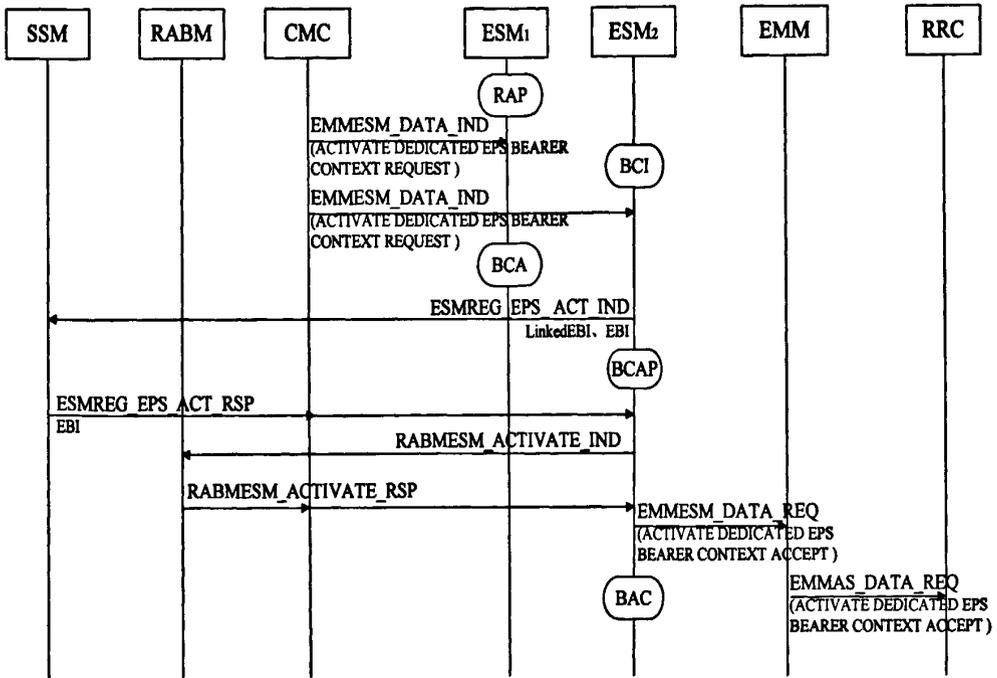


图 3.14 承载资源分配过程——专有承载建立

至此，整个过程结束，UE 和网络已经建立专用的承载资源。

3.5.2.4 网络拒绝承载资源分配请求被

由于 UE 非法、UE 请求的承载资源不能得到网络的响应等原因，网络会拒绝 UE 发起的承载资源分配请求，网络通过发送 BEARER RESOURCE ALLOCATION REJECT 消息来响应 UE 的请求。

其消息流程如图 3.15 所示：

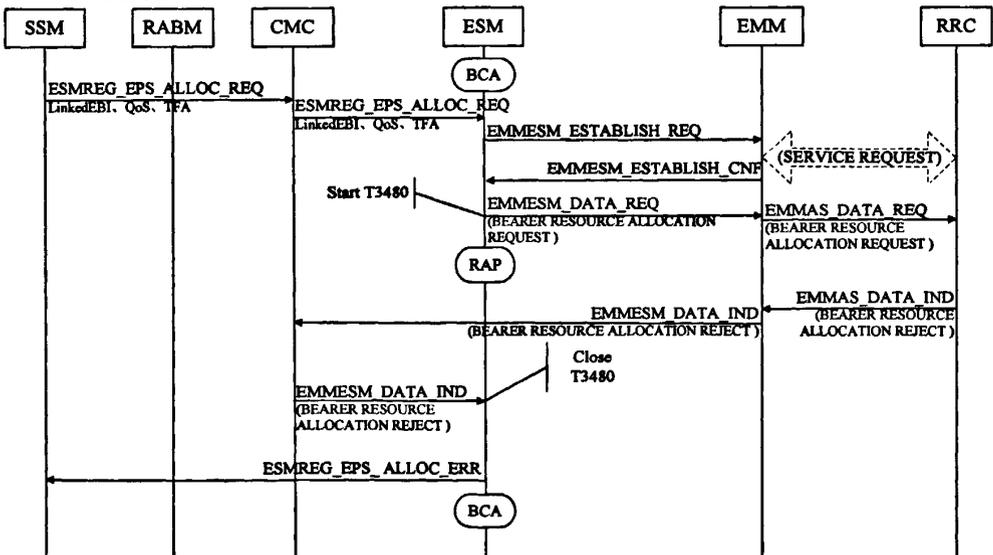


图 3.15 UE 发起的承载资源分配请求被网络拒绝

3.5.3 承载资源修改流程设计

UE 在建立默认承载以及专有承载之后，可以进行数据的传输，但由于用户需求的变化，当需要增加或者减小资源时，UE 将会发起承载资源修改过程。

对于承载资源修改过程，网络会根据当前资源的大小以及 UE 请求的内容来决定是以专有承载建立过程还是 EPS 承载修改过程或者 EPS 去激活过程来响应 UE 的请求。

现以网络用 EPS 承载修改过程来响应 UE 的请求为例来详细描述整个过程。

3.5.3.1 UE 发起承载资源分配过程

当 ESM 收到 SSM 发来的 ESMREG_EPS_MODIFY_REQ 原语时表明 UE 将发起承载资源修改过程。ESM 首先检查当前 MM 连接是否存在，如不存在则通过业务请求流程建立 MM 连接。具体流程如图 3.16 所示：

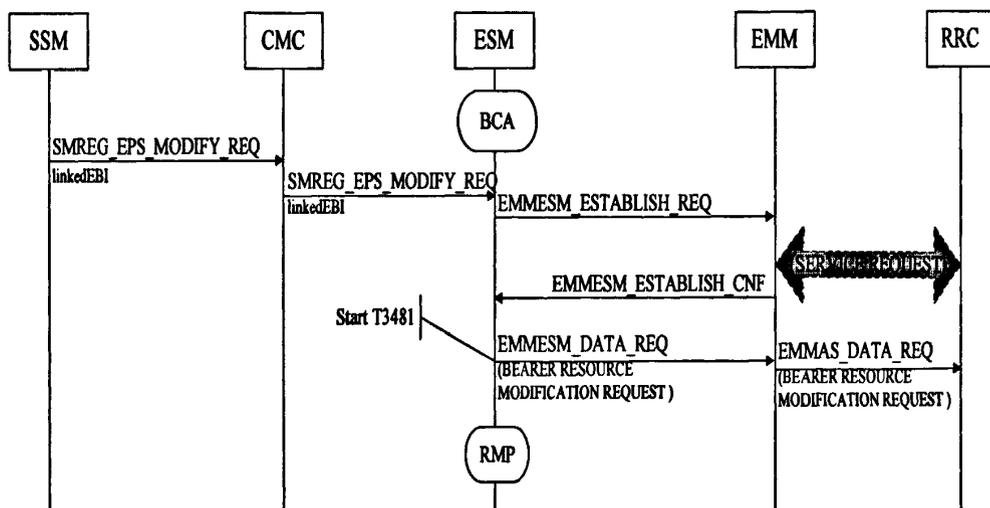


图 3.16 承载资源修改过程——UE 发起

3.5.3.2 CMC 接收 EMMESM_DATA_IND 原语

CMC 收到 EMMESM_DATA_IND 原语后，解析消息类型以及 LinkedEBI、PTI 等参数，确定下一步的行为。流程如图 3.17 所示：

- 1, ESM 在 RMP 状态下收到 MODIFY EPS BEARER CONTEXT REQUEST 消息，将发送 SMREG_EPS_MODIFY_IND 原语到 SSM，同时跃迁到 BMP 状态。
- 2, 收到 SMREG_EPS_MODIFY_REP 原语，ESM 发送(MODIFY EPS BEARER CONTEXT ACCEPT 消息给网络，接受网络的修改，并跃迁到 BCA 状态。

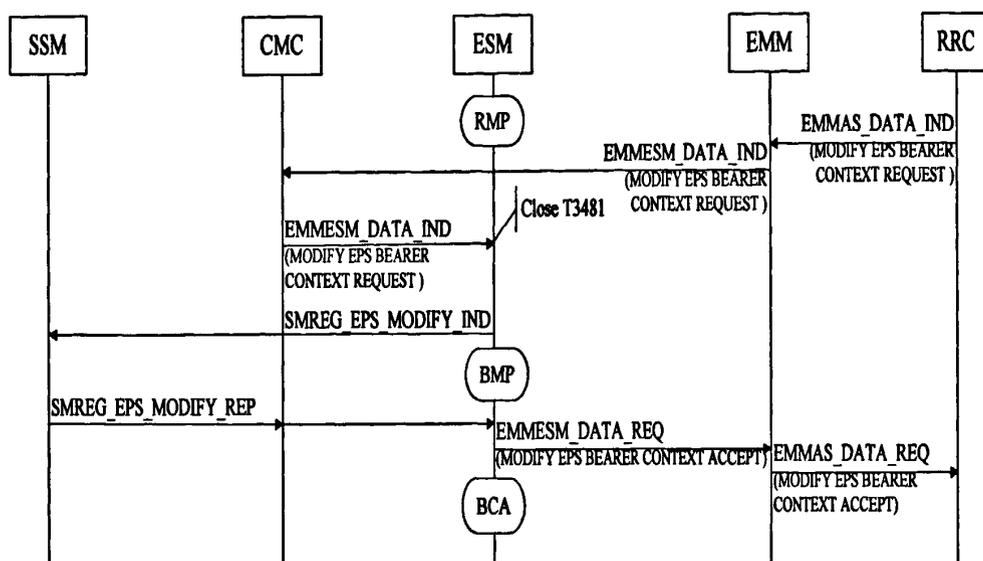


图 3.17 承载资源分配过程——CMC 的处理

至此，整个过程结束，UE 的承载已经被修改。

3.5.3.3 EPS 承载去激活设计

对于承载资源修改过程，UE 也可以用来删除一个专有承载上下文。具体做法是：

1, SSM 发送 SMREG_EPS_MODIFY_REQ 原语给 ESM，表明 UE 主动删除一个专有 EPS 承载，其中原语中携带 cause 值为#36: regular deactivation。

2, 发送 BEARER RESOURCE MODIFICATION REQUEST 消息后，网络回复 DEACTIVATE EPS BEARER CONTEXT REQUEST 消息。ESM 在发送 ESMREG_EPS_DEACT_IND、RABMESM_DEACT_IND 原语以及 DEACTIVATE EPS BEARER CONTEXT ACCEPT 消息后进入 BCI 状态，之后删除这个 ESM 实例。

其消息流程如图 3.18 所示：

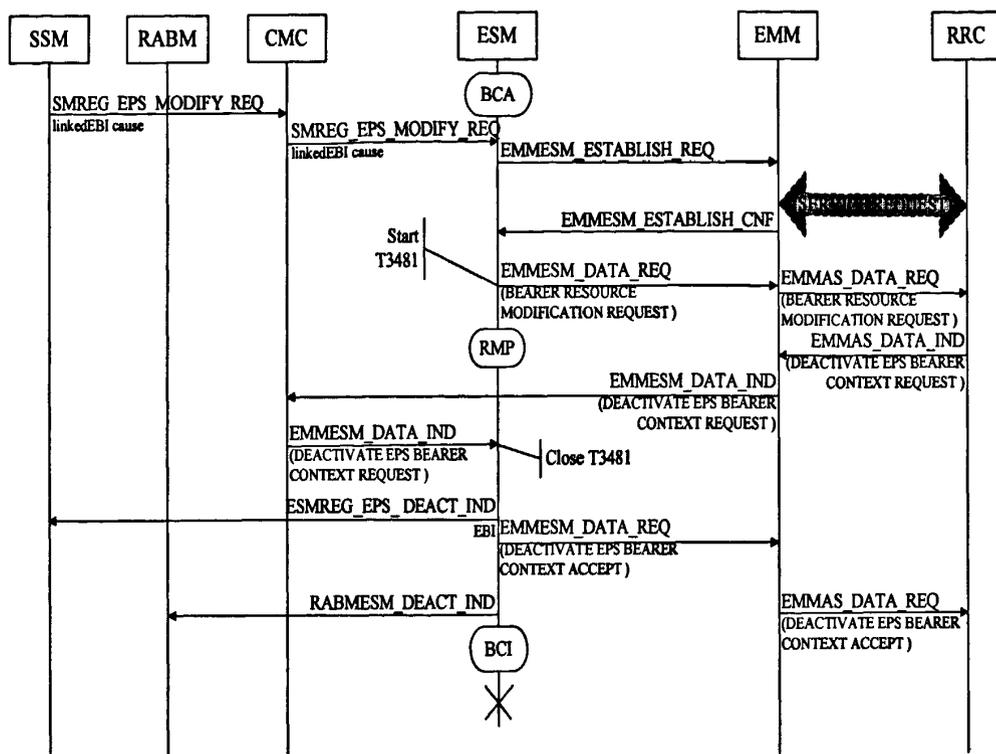


图 3.18 EPS 承载去激活

3.6 NAS 重传机制

由于底层传输出现异常，会导致NAS消息传输失败，进而使UE和网络对于NAS过程的处理不同，使得NAS过程失败，这会造成不必要的信息传输，影响UE和网络之间的信息交互的效率，降低用户的体验度。为消除这种情况的发生，LTE系统应用四重重传机制来确保消息的正确传输。这四重重传机制分别是：MAC子层的HARQ重传机制、RLC子层的ARQ重传机制、PDCP子层的重建时刻的重建机制以及NAS层的消息重传机制。

对于NAS消息的重传，主要在NAS的低层即EMM子层实现。当EMM子层发送NAS消息(此时的NAS消息包括EMM消息和ESM消息)的时候，EMM会记录消息的发送状态，用来标明消息在发送中还是已经发送成功。在等待网络的确认信息的过程中，若时限过长，导致网络定时器超时，将进入异常流程的处理，使得整个过程与设计不符，易造成不可预知的错误；若时限过短，网络还没来得及响应，NAS层就重传消息，会导致网络端多次收到消息，虽然不影响网络的处理，但对于设备的省电等不利。因而确定重传的时限非常重要。

鉴于此，设计重传时限与定时器超时的时限相等。使得重传的时限足够长，但又不会触发定时器超时。因为定时器超时的话，NAS过程将会与设计不符。以ESM子层BEARER RESOURCE ALLOCATION REQUEST消息的重传为例，具体的处理如图3.19所示：

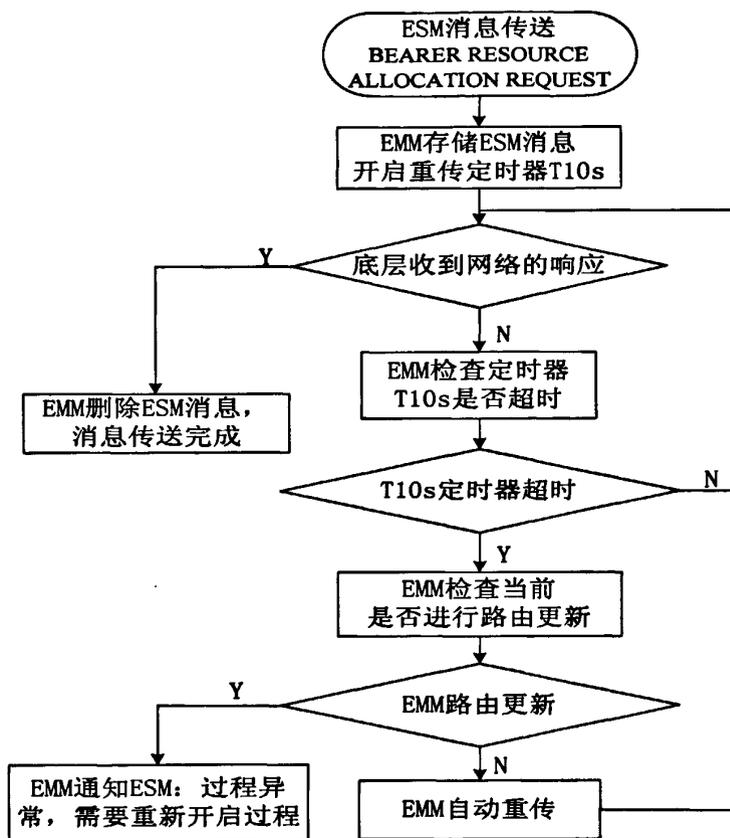


图 3.19 NAS 数据重传机制

- 1, 设定定时器T10s长度为10s, 与承载资源分配过程的定时器长度相同。
- 2, 在T10s超时前收到网络的响应, 则EMM删除存储的消息。
- 3, T10s超时, EMM检查当前是否需要需要进行路由更新。若需要路由更新, 则通知ESM重新开始过程; 若不需要路由更新, 则重传ESM消息, 并重新开启T10s。

3.7 用户数据传输流程设计

3.7.1 正常数据传输流程设计

对于正常的数据传输过程, 在非接入层主要由 RABM 负责。当 ESM 建立 EPS 承载完成且 RABM 建立 DRB 和 EPS 承载的映射关系完毕之后, 数据通路搭建完毕。

RABM 首先要依据 TFT 的滤过, 将数据映射到不同的数据无线承载上面。依据第二章 2.4.2 中的相关描述, 数据在通过 TFT 过滤传输的步骤如图 3.20 所示:

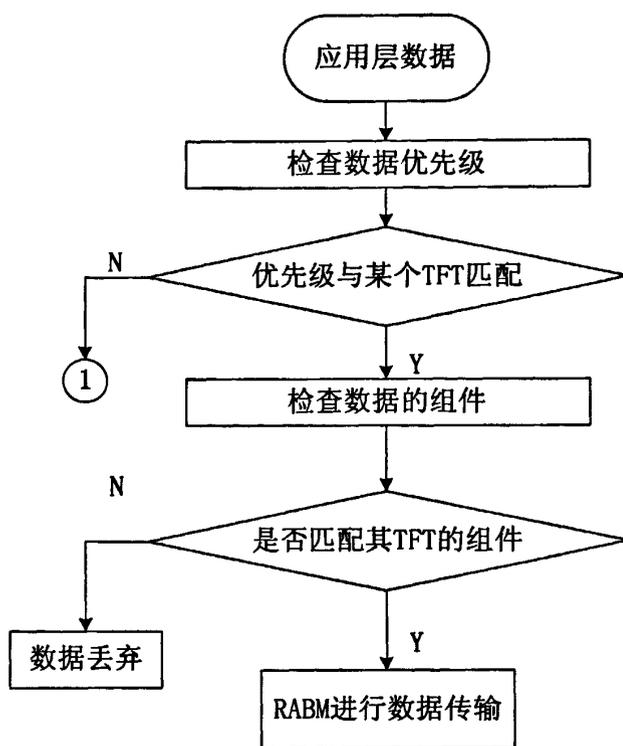


图 3.20 数据通过 TFT 过滤传输

对于①，若其默认承载不存在 TFT，则将数据通过默认承载传输；若默认承载存在 TFT，则丢弃该数据。

对于 UE 的上行数据，UE 通过 COM 口将 IP 数据下发到 RABM。RABM 解析 IP 数据包头，依据 TFT 的筛选原则进行筛选。其筛选原则如图 3.21 所示：

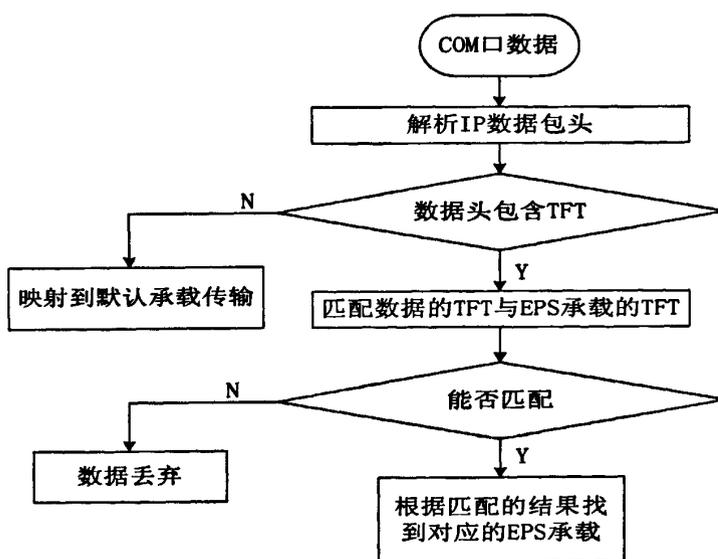


图 3.21 RABM 数据筛选原则

在找到数据对应的 EPS 承载之后, RABM 依据 EPS 承载与 DRB 的映射关系, 将数据映射到对应的 DRB 承载上, 进行数据传输。

对于来自网络的下行数据, PDCP 将数据传输到 RABM, RABM 再将数据传输到 COM。

具体的消息流程如图 3.22 所示:

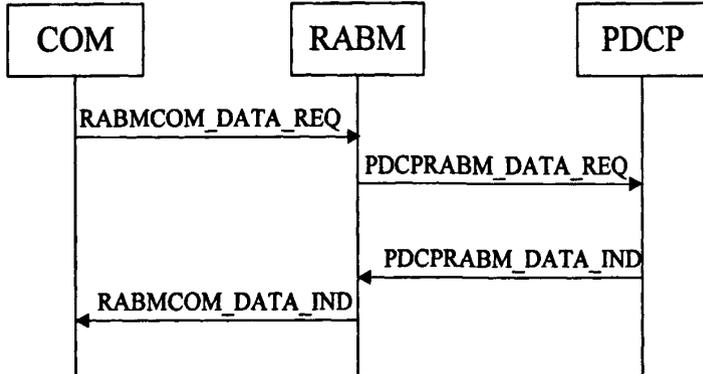


图 3.22 正常上行数据传输流程

3.7.2 DRB 重建流程设计

对于 EPS 承载, 可以看作是 UE 和 PDN-GW 之间的逻辑链路, 其有效性不依赖于实际链路是否存在。但对于 DRB 承载, 当 RRC 连接释放后 DRB 承载将会被删除。因而, 在 IDLE 模式下, 当 UE 发送上行数据时, RABM 将发起 DRB 重建流程。具体消息流程如图 3.23 所示:

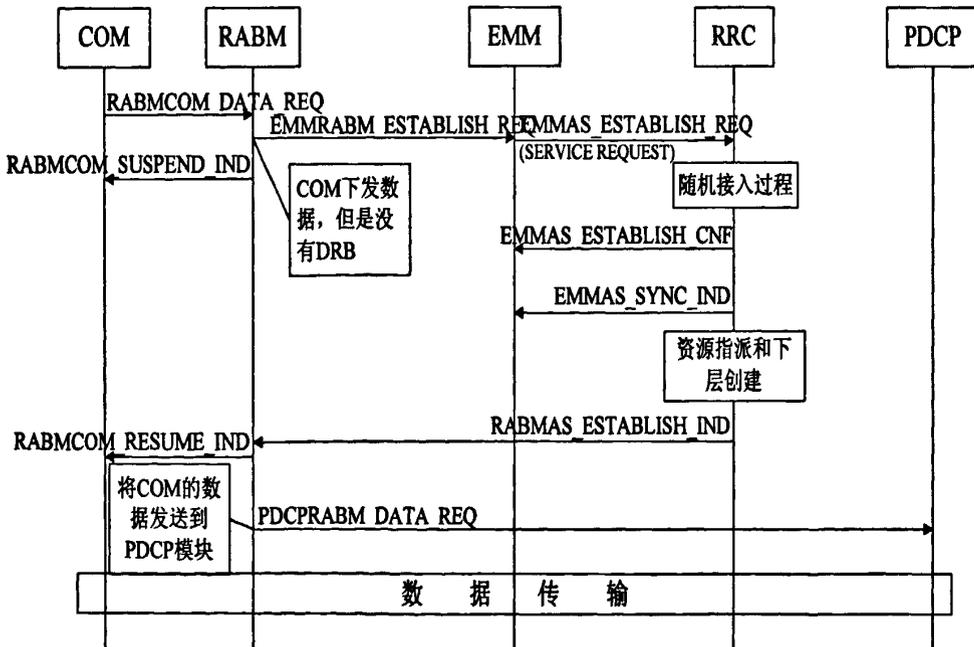


图 3.23 DRB 重建流程

RABM 发起 DRB 重建后首先应发送 RABMCOM_SUSPEND_IND 原语给 COM 挂起 COM 口数据，防止 RABM 一直接收 COM 口数据导致协议栈的数据缓冲区溢出，同时通知 EMM 进行 SERVICE REQUEST 过程，建立一个 MM 连接。

在建立 MM 连接后，RABM 收到 RRC 的 RABMAS_ESTABLISH_IND 原语，建立 EPS 承载和 DRB 的映射关系。之后发送 RABMCOM_RESUME_IND 原语给 COM，通知 COM 口链路已经建立完毕，可以进行数据的发送。

3.7.3 DRB 与 EPS 承载映射错误

网络延迟、核心网错误以及网络资源不足等原因会导致 RRCConnectionReconfiguration 消息中缺少部分 DRB 承载和 EPS 承载映射关系。当遇到这种问题的时候，RABM 根据 RABMAS_ESTABLISH_IND 原语的内容，保留 RABMAS_ESTABLISH_IND 原语指定的对应关系，将其余的 EPS 承载删除。具体的消息流程如图 3.24 所示。

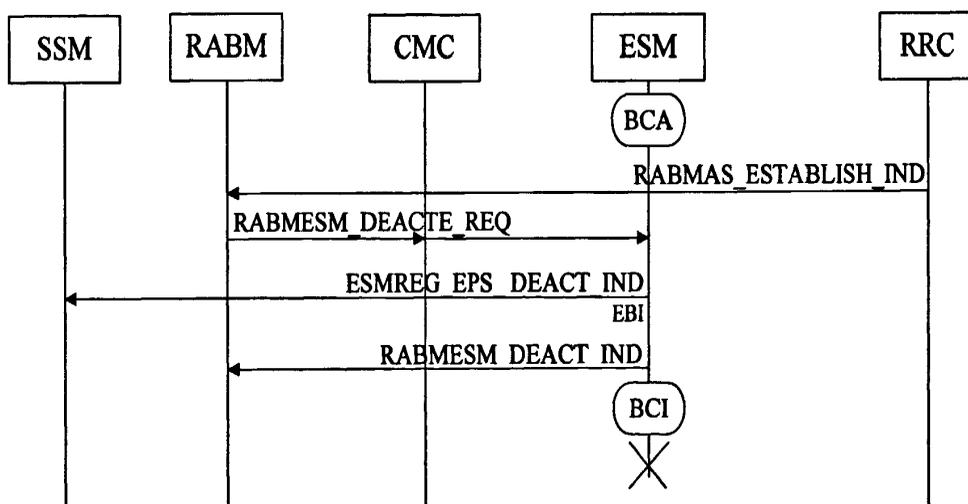


图 3.24 EPS 承载删除

1, RABM 收到 RABMAS_ESTABLISH_IND 原语后建立 DRB 与 EPS 承载之间的映射关系。RABM 检查当前 EPS 承载列表中不存在 DRB 映射关系的 EPS 承载，发送 RABMESM_DEACTE_REQ 原语给此承载对应的 ESM 实例。

2, ESM 实例在收到 RABMESM_DEACTE_REQ 原语后发送 ESMREG_EPS_DEACT_IND 原语给 SSM，发送 RABMESM_DEACT_IND 原语给 RABM，删除本实例。

3.8 本章小结

本章介绍了非接入层数据传输的设计方案以及实现。首先介绍了 LTE 的总体设计，详细设计了 LTE 非接入层构架；其次详细设计与非接入层数据传输相关各个接口；然后基于有限状态机的状态跳转机制，依据 ESM 过程的相关描述，对 ESM 的状态进行了划分，之后详细设计了 ESM 的状态跳转机制，为了更好的管理 ESM 实体，提出了 CMC 的设计；之后详细设计了会话管理流程，为保证消息传输的有效性，设计了 NAS 重传机制；最后根据 TFT 对于数据的滤过作用，设计了非接入层数据传输流程。对于设计的验证与仿真，将在第四章进行。

第四章 仿真与测试

仿真与测试的主要目的是发现并排除在分析、设计、编程等各个阶段中产生的各种类型的错误，以得到可正确运行的软件系统。软件测试工作的目标是尽可能的暴露软件中的潜在错误，能暴露更多的潜在错误的测试用例，便是成功的测试用例。

4.1 仿真测试原理

软件开发过程是一个自顶向下，逐步细化的过程：首先在软件设计阶段定义软件的作用域，确定软件的大体方案；然后进行软件的需求分析，建立软件的数据域、功能和性能需求、约束和一些有效性准则等一系列细节问题；接着进行软件的开发，首先是软件设计，然后再把设计用某种程序设计语言转换成程序代码。而测试过程则是依照相反的顺序进行的。测试工作是一个自底向上，逐步集成的过程。低一级测试为上一级测试准备条件。然而在特定的阶段不排除两者平行进行测试。

通用的测试顺序一般是：首先对每个程序模块进行单元测试，消除程序模块内部在逻辑上和功能上的错误和缺陷；然后在对照软件设计进行集成测试，检测和排除子系统结构上的错误；再次对照需求，进行确认测试；最后从系统全体出发，运行系统，查看系统最终是否满足要求^{[26][27]}。

4.1.1 测试方法分类

按照被测对象的控制观察方式进行分类^[28]，测试方法可以分为白盒法和黑盒法。

白盒法又称为结构化方法或者逻辑覆盖法。白盒法的基本思想是把程序看做是一个路径的集合。这样，对程序的测试便转化为对程序中某些路径的测试，要设法让被测程序的“各处”均被执行到，使潜伏在程序每一个角落的错误均有机会暴露出来。因此，白盒法实际上是一种选择通过制定路径的输入数据的分析方法。

黑盒法又称功能测试，是依据软件需求说明书上罗列的各项功能、性能指标，来构建测试用例的输入数据，实际执行被测软件，分析执行过程的行为与执行结构，以便监察被测软件的潜在错误。在黑盒法测试中，测试者可以完全不关心程序的内部结构。

由此可见，白盒法是一种逻辑驱动方法，而黑盒法是一种功能驱动方法。

无论是白盒法还是黑盒法测试，都不能进行穷举测试，因为即使测试所有路径的一个小的子集，也会导致需要大量的测试数据。因而在实际工作中，一般采用白

盒法和黑盒法相结合的技术，称为灰盒法。

测试用例设计的基本原则，是以尽可能小的代价确定一组最有可能发现某个错误或者某类错误的测试数据。灰盒法是一种合理的方法，它以产品的主要性能和功能为测试依据，根据产品的程序图、功能说明书以及测试者的实践经验来设计测试用例，不强调要在对程序中各语句处理内容完全了解的情况下进行。测试产品主要功能的同时也测试产品的主要性能，可以根据测试者的经验来选取，把容易发生错误的变量输入、流程图中关键路径和程序图等作为测试的内容，忽略掉不容易发生错误的变量输入和流程图中不影响或者不改变内部逻辑的细节。可以选取并测试数量有限的重要逻辑路径，对一些重要数据结构的正确性进行完全的检查。这样，不仅证实了软件接口的正确性，同时在某种程度上也保证了软件内部工作的正确性。

灰盒测试能最大限度的结合白盒测试和黑盒测试的优点，避免把测试工作分为两次进行，提高了测试效率，文章要介绍的就是一种灰盒测试的方法。

4.1.2 测试步骤

测试过程按四个步骤进行，即单元测试、集成测试、确认测试和系统测试。

1, 单元测试, 集中对代码中的每一个程序单元进行测试, 检查各个程序模块是否正确的实现了规定的功能。

2, 集成测试, 把已测试过的模块组装起来, 主要针对与设计相关的软件体系结构的构造进行测试, 再将一个一个实施了单元测试并确保无误的程序模块组装成软件系统的过程中, 集成测试能够对正确性和程序结构等方面做详细的检查。

3, 确认测试, 主要检查待测软件是否满足了需求规格说明书中确定了的各种需求, 以及软件配置是否完全、正确等。

4, 系统测试, 把经过确认了的软件纳入实际运行环境中, 与其他系统成分组合在一起进行测试。

协议测试是一种特殊的软件测试, 也具备一般软件测试的特点。

4.1.3 协议一致性测试

目前, 协议测试分成4个方面进行研究: 一致性测试(Conformance Testing)、互操作性测试(Interoperability Testing)、性能测试(Performance Testing)和稳定性测试(Robustness Testing)。

一致性测试主要测试协议的实现是否严格遵循相应的协议描述, 判断网络产品的协议实现是否符合协议的国际标准, 一致性测试是协议测试的最基本内容, 是其它三种测试的基础; 互操作性测试关注的是对于同一协议标准, 不同协议实现的互

连通问题；性能测试是用实验的方法来观测被测协议实现的各种性能参数，如吞吐量和传输延迟等等，其结果往往与输入负载有关；稳定性测试是检测协议实体或者系统在各种恶劣环境下运行的能力(如信道被切断、通信系统掉电、注入干扰报文等)。

一致性测试是由ISO9646国际标准定义的一个完善的测试方法。根据ISO9646一致性测试方法论的规定，测试标准包括三个部分：抽象测试集(ATS)，协议实现一致性说明(PICS)，协议实施附加信息(PIXIT)。可执行测试集(ETS)是在以上三部分的基础上生成的。一致性测试的主要步骤如图4-1所示。

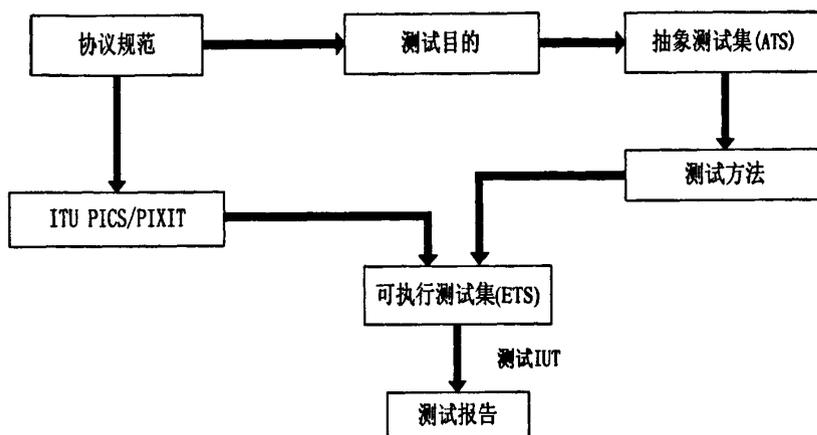


图 4.1 一致性测试的测试过程

ATS: 抽象测试集，是描述过程的文本，它提供测试项的规范。

PICS: 协议实现一致性说明，用来说明实施的要求，能力以及可选项实施的情况。

PIXIT: 协议实施附加信息，用来提供测试时必须标明的协议参数。

ETS: 可执行测试集，是测试集有软件实现体。

IUT: 被测协议实现，是指一个实际开放系统将要进行一致性测试的那部分，它应该是一个或多个 OSI 协议的实现。被测系统所包含的 IUT 可以是单层 IUT(被测系统只有一层被测试)或多层 IUT(被测系统中有一系列相邻层需要测试)，能力以及可选项实施的情况。

详细描述如下：

1. 根据协议规范，研究协议规范的每个特性，为每个特性编写测试目的。
2. 把每个测试目的转化为抽象测试用例(ATC)。覆盖协议规范所有特性的多个 ATC 集合就构成了该协议规范的 ATS。
3. 生成 PICS/PIXIT。PICS 用来说明实施的要求、能力及可选项实施的情况。PIXIT 用来提供测试时必须标明的协议参数。
4. 确定测试方法，针对不同的 IUT(被测实现)，用户应采用不同的测试方法。

- 5, 根据 PICS/PIXIT 和测试目的编写测试用例, 生成 ETS。
- 6, 使用生成的 ETS 测试 IUT。
- 7, 根据测试结果生成测试报告。

一致性测试实质上是利用一组特定的测试用例, 在一定的网络环境下, 对待测设备进行黑箱测试, 通过比较实际输出与预期输出的异同, 判定待测设备在多大的程度上与标准描述相一致, 并借此来保证通过一致性测试的设备在不同网络中的表现一致。

同一类待测设备只有在通过了一致性测试后, 才能保证在变化的环境中始终都做出同样的处理, 从而有效保证在同一个网络内的其他实体不会发生由此带来的异常处理, 确保了所有设备在公共部分实现的一致性。终端设备的一致性测试是对终端的全面验证测试, 能够考察终端设计方案与相应标准的符合性、一致性, 是终端产品成熟的重要标志。同时一致性测试能力的完善程度则是技术成熟、产业链健全度的主要体现。

4.2 协仿真测试

4.2.1 TTCN 测试模型

测试阶段所使用的测试语言为 SDL 语言(Specification Description Language)即规格和描述语言^[29-31]。它是 CCITT 推荐的规范描述语言。作为国际标准化的正式语言, SDL 的目的是用来描述电信系统的功能实体之间的交互行为。测试阶段用于生成测试用例的语言为 TTCN (Tree and Tabular Combined Notation) 即树表结合表示法, 它是一种标化的 ATS 描述语言, 获得了世界范围的标准化组织和测试委员会的认同, 被广泛的应用于通信协议的测试中^[32]。TTCN (Tree and Tabular Combined Notation) 具有明确的语法和语义, 用以表述独立于任何现实的通用测试集。这种语言最初是为了明确指定测试指令序列而开发的, 用于一致性测试集的测试表示法; 同时它也是独立于协议、测试方法和测试设备的抽象语言, 是一种非常有效的协议测试软件。目前 LTE 协议栈软件的开发中广泛应用了 TTCN 作为测试工具。

在对 LTE 高层软件进行测试时, TTCN 通过与 SDL 的联合使用(协仿真), 可以生成消息序列流图(MSC)。通过观察 IUT 内部和 IUT 与环境(测试系统)之间的消息序列和数据流, 达到查找错误的目的。

根据协议 3GPP TS 36.523 和 3GPP TS 36.508 对于一致性测试的描述^[33-35], 一致性测试模型如图 4.2 所示:

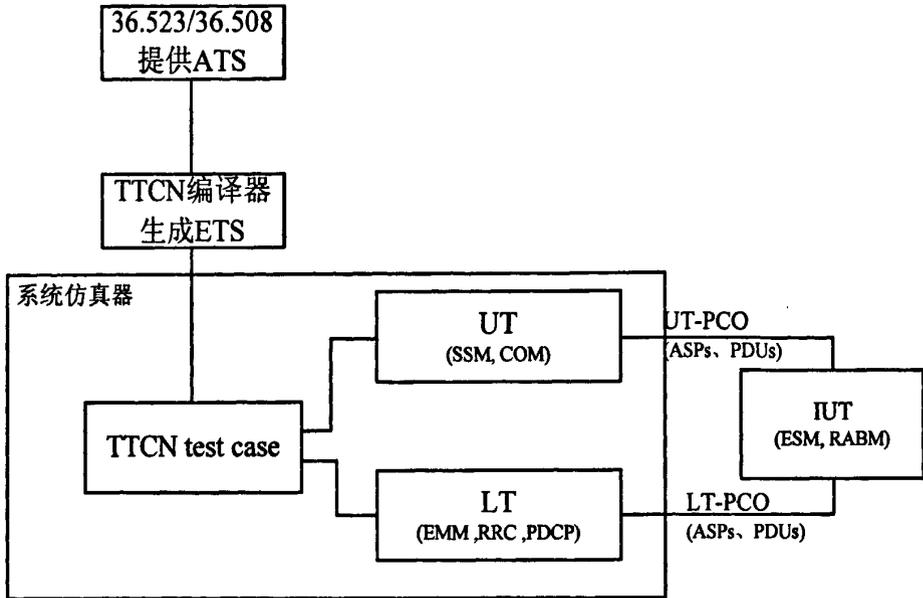


图4.2 系统仿真器与TTCN一致性测试

其中需要说明的是：

IUT：被测试实体。IUT 是一个或多个协议的实现，是使用 TTCN 来测试和验证的实体。在本论文中特指 ESM 和 RABM。

PCO：控制和观察点。PCO 是测试环境与 IUT 之间的一个观察点，在该点可以观察和控制测试事件的发生，通过观察和控制该点，也可以跟踪测试事件的发生。

ASP：抽象服务原语。ASP 主要描述服务提供者和服务用户在层间的交互信息。这些原语是协议规定的，与实现无关。

PDU：协议数据单元。PDU 是嵌套在 ASP 中的对等层间交换的信息单元。

UT、LT：上测试器和下测试器。对 UT 和 LT 的区分是相对于 IUT，PCO 的位置而言的。通常把放在 IUT 的上层观察和控制 IUT 的测试点，称为 UT-PCO；而把放在 IUT 的下层观察和控制 IUT 的测试点，称为 LT-PCO。

Test Suite：测试集。Test Suite 是由一套完整的测试用例(Test Case)组成，可包括嵌套的测试组 (Test Group)，用来执行一个或多个 OSI 协议的动态测试。

4.2.2 默认承载建立的协仿真测试

单元测试用是一种协仿真测试，能够很好的暴露流程性的问题和各模块之间配合性的问题，因而在测试之初经常使用。下面就以开机默认承载建立为例进行单元测试。

默认承载建立是UE开机的重要过程，其成功与否关系着UE能否在小区中完成注册过程。因而，默认承载建立成为测试的重点。

4.2.2.1 测试点

UE在开机ATTACH过程中，伴随有PDN连接过程，其目的就是为了在UE和PDN-GW之间建立默认承载上下文。

本测试用例的主要测试点如下：

- 1, 开机ATTACH过程中，UE首先发送ATTACH REQUEST消息。
- 2, 收到ATTACH ACCEPT消息后UE建立默认承载上下文。
- 3, 默认承载建立完毕后UE发送ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT 消息到网络。

4.2.2.2 测试用例构造

由于是开机过程，因此设定一些初始信息：

- 1, UE处于关机状态，进行初始EPS Attach。
- 2, CELLA信息：存在TAI列表(TAI-1), TAC = 1, MME Group ID = 32769, MME Code = 1。
- 3, UE先前已经注册在E-UTRAN，并能通过鉴权。

根据第三章设计的流程以及初始条件，构造测试用例如图4.3所示：

Nr	Label	Behaviour Description	Constraints Ref	Verdi
1	CH_SPYNET	CAPi_REG_REGISTRATION_REQ	CapiregRegistrationReq	
2	CH_SSM_CMC	ESMREG_EPS_ACT_REQ	EsmregEpsActReq	
3	READ_U SIM	CH_MDBI_EPM ? MODI_SAP_BINARY_READ_REQ(sim_index:=MODI_SAP_BINARY_READ_REQ_h_T_MDBI_SAP_BINARY_READ_REQ_i_SAP_BINARY_READ_REQ_i_MODI_SAP_BINARY_READ_REQ_indexId)	MobiSepBinaryReadReq	
4		*step_readLiteUsim_Normal ->READ_USIM		
5				
6	CH_SPYNET	CAPi_REG_START_IND	CapiregStartInd	
7	CH_EPM_RNC	EMMAS_ESTABLISH_REQ	EmmasEstablishReq	
8	CH_EPM_RNC	EMMAS_ESTABLISH_CNF	EmmasEstablishCnf	
9		*step_authentication		
10		*step_identity		
11		*step_securityModeCommand		
12	CH_RAD_RNC	RADMAS_ESTABLISH_IND	RabmasEstablishInd	
13	CH_RAD_RNC	RADMAS_ESTABLISH_RSP	RabmasEstablishRsp	
14	CH_EPM_RNC	EMMAS_DATA_IND	EmmasDataIndAttachAccept	
15	CH_ESM_SSM	ESMREG_EPS_ACT_IND	EsmregEpsActInd	
16	CH_SSM_CMC	ESMREG_EPS_ACT_RSP	EsmregEpsActRsp	
17	CH_EPM_RNC	EMMAS_DATA_REQ	EmmasDataReq	
18	CH_MDBI_EPM ?	MODI_SAP_BINARY_UPDATE_REQ(sim_index:=MODI_SAP_BINARY_UPDATE_REQ_h_T_MDBI_SAP_BINARY_UPDATE_REQ_i_SAP_BINARY_UPDATE_REQ_i_MODI_SAP_BINARY_UPDATE_REQ_indexId)	MobiSepBinaryUpdateReq	
19	CH_SPYNET	CAPi_REG_REGISTRATION_CNF	CapiregRegistrationCnf	
20	CH_ESM_SSM	ESMREG_EPS_ACT_CNF	EsmregEpsActCnf	
21	CH_EPM_RNC	EMMAS_DATA_CNF	EmmasDataCnf_04	
22	CH_RAD_RNC	RADMAS_RELEASE_IND	RabmasReleaseInd	
23	CH_RAD_RNC	RADMAS_RELEASE_RSP	RabmasReleaseRsp	
24	CH_EPM_RNC	EMMAS_RELEASE_IND	EmmasReleaseInd_NormalRelease_PASS	

图 4.3 LTE 终端默认承载建立测试用例

4.2.2.3 测试结果分析

根据编写的测试用例，应用 TTCN 生成可执行测试集，执行协仿真测试。测试完成之后 TTCN 会生成消息序列图(MSC 图)，MSC 图可以很直观的给出消息的交

互过程，同时也能显现出各个消息所携带的数据。根据消息交互流程以及消息携带的数据，我们可以深入分析从而得出分析结果。

限于篇幅，这里只截取了该测试用例测试 MSC 图的重要部分，该测试用例测试通过协仿真测试产生的 MSC 图如图 4.4、4.5 所示：

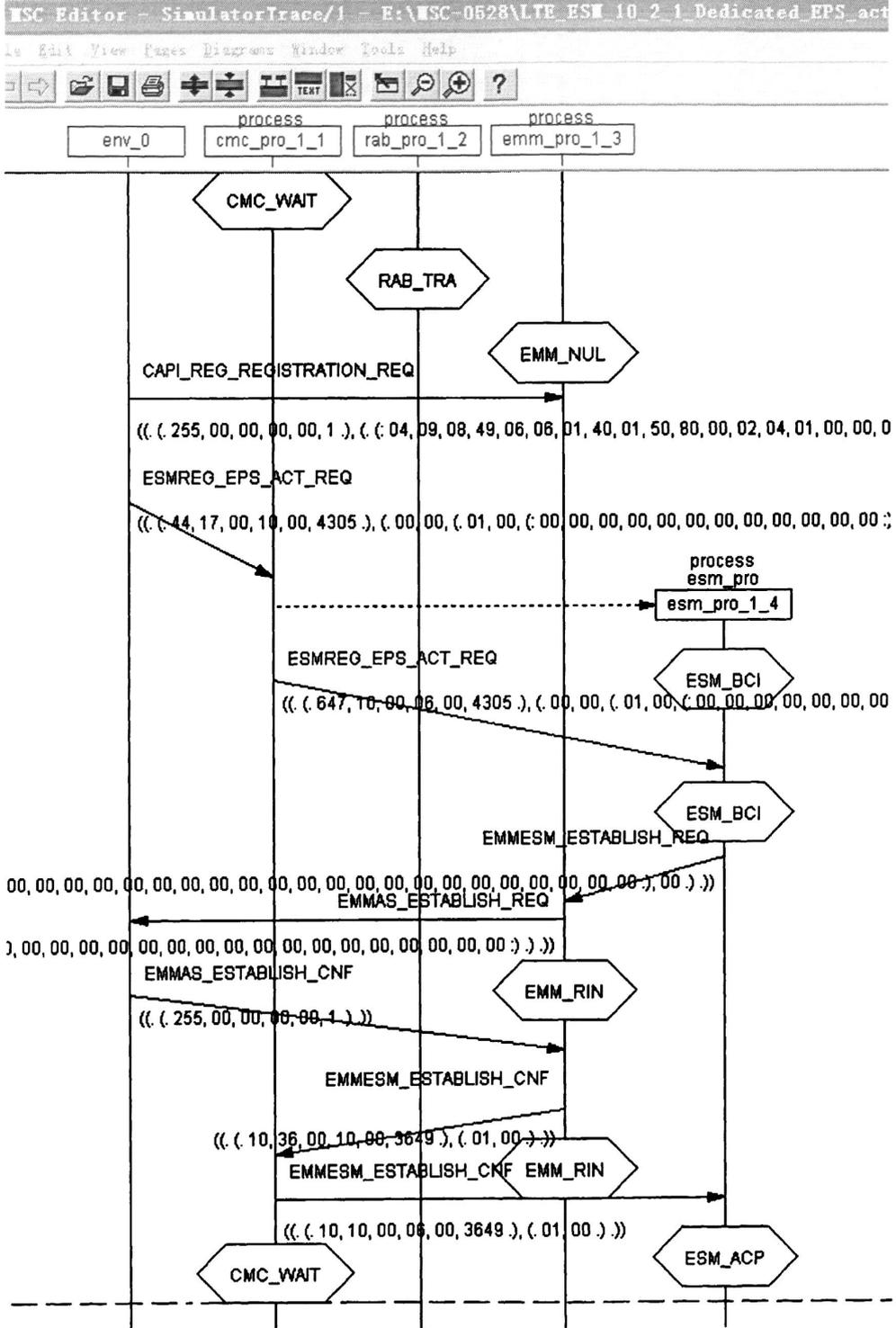


图4.4 LTE终端Attach过程测试MSC图（一）

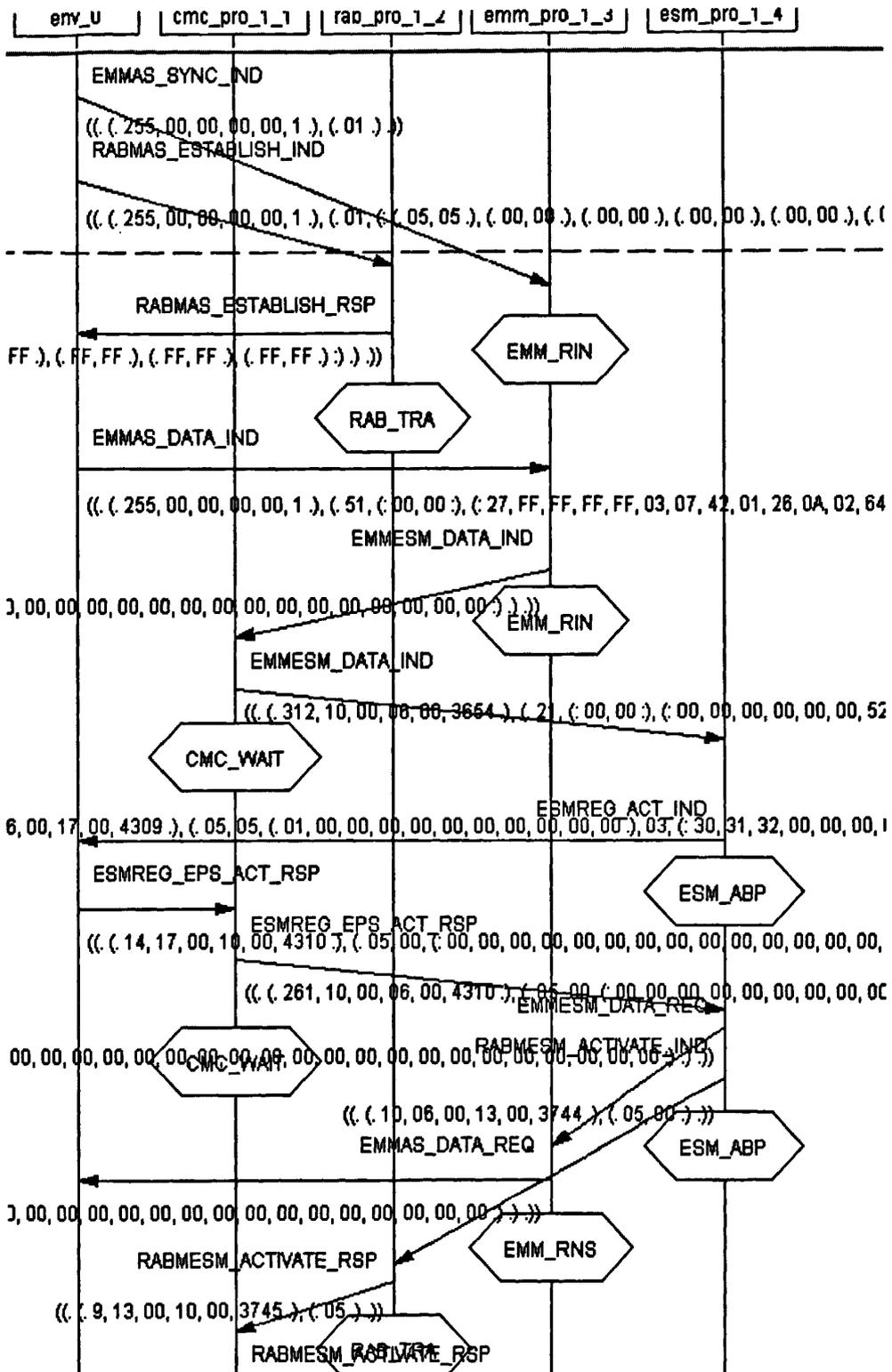


图4.5 LTE终端Attach过程测试MSC图(二)

图4.4显示在开机初始阶段,高层下发开机信号,CMC创建ESM实例,EMM建立MM连接。图4.5显示MM连接建立完毕后CMC通知ESM建立默认承载上下文。得到SSM的ESMREG_EPS_ACT_RSP后通知网络默认承载已经建立。整个测试流程符

合标准规范。可见仿真结果达到了预期的目的，验证了软件设计的正确性。

4.3 板级测试

协仿真虽然能够很好的暴露流程性的问题，但其实时性比较差，不能很好的模拟定时器、内存等实际情况，在协议栈软件开发的后期，面对越来越多的协议栈软件与操作系统相关、与硬件相关以及与定时器相关的很多问题，协仿真都不能很好的胜任。因而需要考虑新的测试方法。板级测试能够很好的完成这一工作。

4.3.1 板级测试模型

板级测试方法是一种非常有效的模拟现场测试的系统测试方法，其仍然采用 TTCN 模拟测试环境，编写测试用例，但是测试体 IUT 就不再是嵌入了 C 代码的 SDL，而是移植了源代码的 ARM 实验板，测试模型如图 5.6 所示。

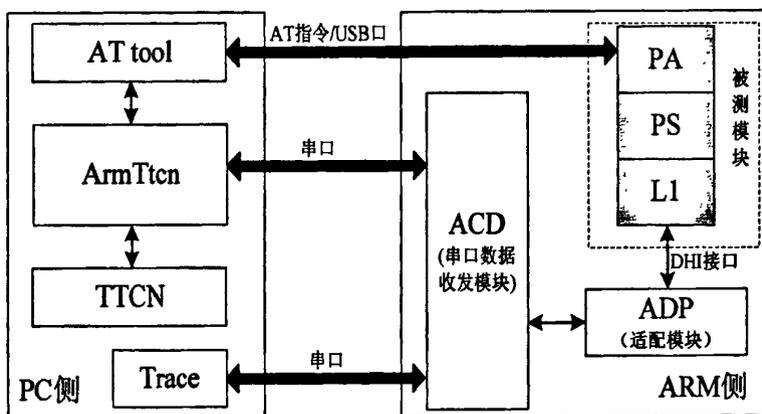


图 4.6 板级测试示意图

这里主要对 PC 端以及 ARM 端的主要模块及功能进行描述：

Trace: 主要负责跟踪打印。

TTCN: TTCN 测试软件，主要负责测试用例的编写、开发工作。

ArmTtcn: 测试环境，主要负责将 TTCN 编写的测试用例代码集成到 ArmTtcn 中，同时集成了串口通讯模块等代码，以便 PC 端的测试数据能够通过串口与 ARM 侧进行通讯。

ACD: 串口数据的收发模块，在 ARM 侧操作系统中作为一个高级中断服务程序存在。

ADP: 主要负责接收被测模块的消息数据，向 TTCN (PC 端) 发送；以及接收来自 TTCN 的测试数据，发送到被测模块。

AT tool: 模拟人机界面操作。将 TTCN 发送的 MMI 指令转化为 AT 指令通过真实的 AT 接口发送到数据卡协议栈 PA 模块, 并且可以将数据卡发出的 AY 指令发送到 TTCN 检查 AT 命令消息的正确性。

PA: 协议应用, 作为协议栈软件的一部分, 和 AT tool 传输 AT 指令, 通过 USB 口进行传输。

PS: 协议栈, 包括 AS 和 NAS 部分, 本论文的主要设计都是在这部分内。

L1: 物理层。与 ADP 适配模块通过 DHI 接口通信。

综上, 可以将 AT 指令传输点作为上观测点, 将 DHI 接口作为下观测点。

4.3.2 承载资源分配板级测试

本测试从开机开始, 包括默认操作建立, 之后 AT 指令请求新的资源来传送数据, 协议栈下发承载资源分配请求, 直至网络响应专有承载建立过程为止。检验在板级测试的环境下 UE 的开机过程以及承载资源分配过程。

4.3.2.1 测试点

该测试用例的主要测试点有如下几个, 分别是:

1, UE能否正常开机完成注册过程。

2, 当AT下发AT指令, 新建专有承载, 要求发起承载资源分配过程时, UE是否发送发送BEARER RESOURCE ALLOCATION REQUEST消息。

3, 收到网络的ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST后 UE是否回复网络ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT消息。

4.3.2.2 测试用例构造

在构造测试用例前要详细设计初始条件, 以便更好的编写测试用例。设置的初始信息如下:

1, UE处于注册状态, IDLE模式。

2, 在网络和UE之间存在一个默认承载上下文, EPS bearer identity为5。

本测试用例严格按照 3GPP 协议 36.523 中第十章 10.7.1 关于承载资源分配过程的测试标准进行编写。

1, 设置初始的小区条件, 编写开机流程, 然后进行 RRC 连接释放, 进入 IDLE 状态。

2, 然后应用 AT tools 工具发起 AT 命令。这两步主要为承载资源分配过程作铺垫。具体构造如图 4.7 所示:

Nr	Label	Behaviour Description	Constraints Ref	Verdict
1		(a_setIdCellRsrp := {70, 65535, 65535, 65535, 65535, 65535, 65535, 65535})		
2		+modifyUeInfoFromTtcnLTE		
3		DSP ! SET_L1_HARQ_IND_FROM_TTCN_LTE	cs_SET_L1_HARQ_IND_FROM_TTCN_LTE	
4		+state2(CELL1)		
5		(v_cid := 02'H)		
6		+maiNoBearerResourceallo		
7		(a_rrcConReconfig := a_rrcConReconfig_DRB_1_0, a_rrcConReq := [40'0,'10'0,'00'0,'00'0,'00'0,'00'0,*], a_brallocationReq := [02'H,'02'H,'04'H,'06'H,'15'H,'21'H,'31'H,'09'H,'15'H,'10'H,'06'H,'18'H,'08'H,'0C'H,'FF'H,'FF'H,'FF'H,'00'H,'30'H,'06'H,'51'H,'00'H,'01'H,'FF'H,'FF'H,'41'H,'00'H,'01'H,'FF'H,'FF'H,'05'H,'02'H,'A1'H,'A1'H,'A1'H,'A1'H,*])		
8		+BearerResourceAllocationAct_Allocation(cs_RRCConnectionSetup, cs_RRCConnectionReconfiguration)		
9		+waitExpired(3000)		

图 4.7 LTE 终端承载资源分配测试用例—1

对于承载资源分配过程，由于比较复杂，在设计的时候设置成了测试步进行重点描述。即图 4.7 中的 BearerResourceAllocationAct_Allocation 项。在此测试部中需要设计 RRC 连接、RRC 连接重配等流程，其构造如图 4.8 所示：

Nr	Label	Behaviour Description	Constraints Ref	Verdict
1		+rrcConnectionSetup_RRC_ServicReq(rrcSetup)		
2		+integrityProtectSuccessForAs_LTE		
3		+rrcConnectionReconfiguration(cs_RRCConnectionReconfiguration_noNAS)		
4		DSP ? NAS_PS_DATA_REQ	cr_bearerResourceAllocationRequest	
5		(v_waitFlag := '01'H)		
6		DSP ! NAS_PS_DATA_IND	cs_activateDedicatedEPSContextRequest	
7		(v_waitFlag := '00'H)		
8		DSP ! RRCConnectionReconfiguration	rrcReconfig	
9	1_001	DSP ? ELI_PHY_CONFIG_REQ	cr_EL1_PHY_CONFIG_REQ	
10		-> _001		
11		[v_regressionTest = 0]		
12		-> _001		
13		[v_regressionTest = 1]		
14		DSP ? RRCConnectionReconfigurationComplete	cr_RRCConnectionReconfigurationComplete	
15		DSP ? NAS_PS_DATA_REQ	cr_activateDedicatedEPSContextAccept	
16		DSP ? RRCConnectionReconfigurationComplete	cr_RRCConnectionReconfigurationComplete	
17		DSP ? NAS_PS_DATA_REQ	cr_activateDedicatedEPSContextAccept	

图 4.8 LTE 终端承载资源分配测试用例—2

4.3.2.3 测试结果分析

完成上述测试文档的输入以及测试过程的执行后，Trace 工具会将跟踪的结果输出为 LOG 保存在硬盘上。运用重邮信科公司开发的 Trace 工具即可查看整个层 3 消息流如图 4.9、4.10 和 4.11 所示：

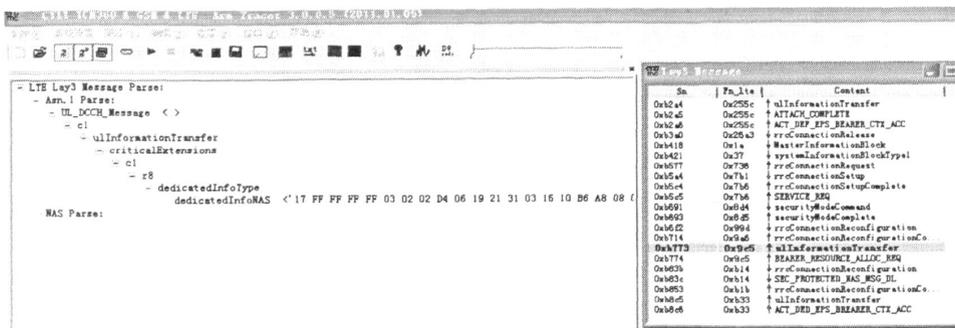


图 4.9 LTE 终端承载资源分配测试结果—1

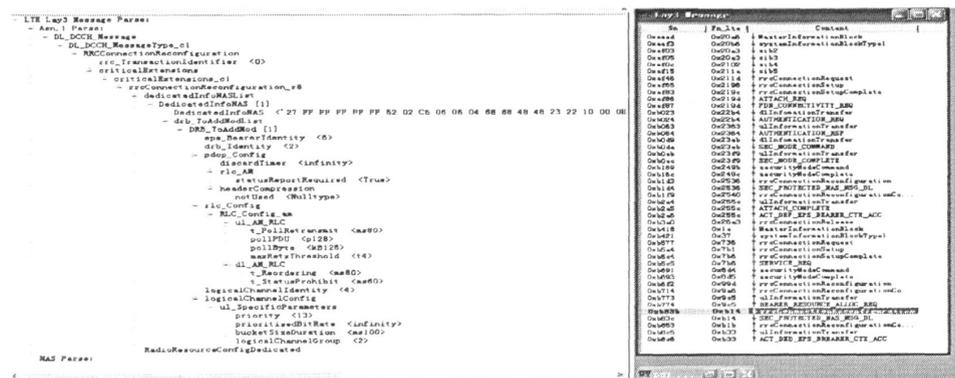


图 4.10 LTE 终端承载资源分配测试结果—2

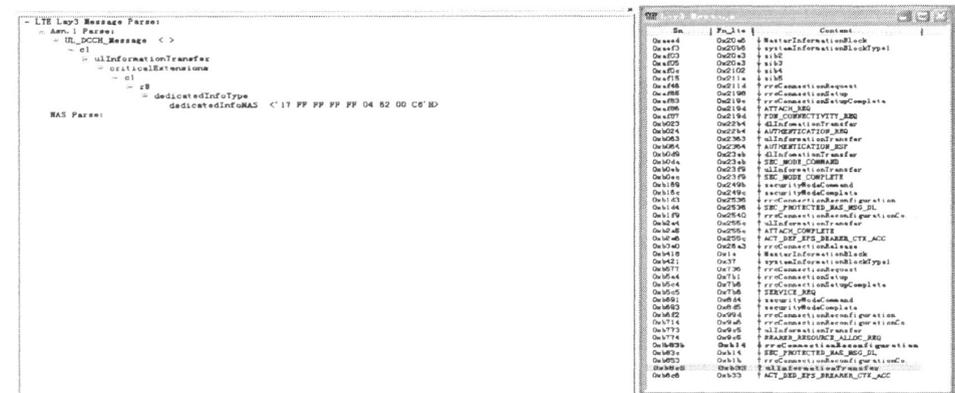


图 4.11 LTE 终端承载资源分配测试结果—3

从图中可以很清楚的看出，UE 完成了开机注册过程以及承载资源分配过程。

图 4.9 左侧列出了 ulInformationTransfer 消息，通过解析其中的 NAS 消息可以看出，其携带的消息即为 BEARER RESOURCE ALLOCATION REQUEST 消息。

图 4.10 左侧列出了 rrcConnectionReconfiguration 消息，通过解析其中的内容，其中 NAS 消息为 ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST 消息，同时新建立了 DRB。

图 4.11 列出了最后一条 ulInformationTransfer 消息，解析得到其中的 NAS 消息为 ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT。其流程完全符合设

为 ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT 消息。证实了 UE 在收到 ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST 消息后发送 BEARER RESOURCE ALLOCATION ACCEPT 消息给网络。

经过分析，证明了本测试结果与设计完全相符合，同时符合 3GPP 协议的规定。

通过两方面的验证，证实本设计得到了实现。按照 3GPP 协议的要求，本文共测试了九个大类的 21 个小项的测试用例，涵盖 PDN 连接过程、PDN 去连接过程、承载资源分配过程、承载资源修改过程、默认承载建立过程、专有承载建立过程、承载上下文修改过程、承载上下文去激活过程以及用户数据传输过程。对于这些测试，已经全部通过，证明了本文设计与 3GPP 协议完全符合，从另一方面证明了本设计的正确性和可行性。

4.4 本章小结

本章基于对测试方法的分类以及对 TTCN 测试原理的介绍，依据协议栈软件开发的需求，在开发的前期，运用协仿真测试方法进行相关测试用例的测试验证，证明过程实现的正确性和可行性；在开发的中后期，运用板级测试的测试方法，对典型的测试用例进行了测试，经过对测试结果仔细的分析检验，证明本设计完全达到标准的相关要求；最后简单的介绍了外场测试的情况。

第五章 论文工作总结及进一步的思考

5.1 论文工作总结

本文主要研究了 LTE 终端非接入层数据传输。作者在参与重邮信科国家重大专项—“TD-LTE 终端基带芯片研发”的过程中阅读了大量 3GPP 标准中关于 LTE 终端协议的相关内容，对协议结构中关于非接入层特别是会话管理流程部分做了详细的研究，对 LTE 终端会话管理和数据传输的要求和实现有了深入认识。在论文中首先分析了当前 LTE 系统的发展现状，引出非接入层数据传输的重要性，其次，简要介绍了 LTE 系统终端的相关结构以及协议栈总体构架。基于对会话管理和数据传输的理论研究，重点对会话的管理以及数据的传输进行了实现，主要包括协议栈总体设计、交互接口设计、状态跳转设计、会话管理的流程设计、非接入层数据传输流程设计等部分。最后，介绍了仿真测试原理，并通过协仿真测试以及板级测试对先前的设计进行了测试验证，验证结果显示本设计完全符合协议的要求，验证了本设计的正确性。

具体来说，本文作了如下工作：

1， 基于对 LTE 总体框架的认识以及本文的研究重点，详细的分析与描述了会话管理的相关协议，同时对从开机 ATTACH、专有承载建立直至进行数据传输的从终端到网络端的整个流程做了深入的研究。

2， 给出了非接入层数据传输的实现方案。在介绍 LTE 终端总体框架以及非接入层框架的基础上，详细设计了 ESM 和 RABM 的相关接口；基于有限状态机的原理，本着状态跳转清晰的原则，对 ESM 进行了状态划分，同时定义了状态跳转；重点设计了会话管理流程，NAS 重传机制，以及非接入层数据传输流程。

3， 在介绍协仿真测试原理的基础上，以默认承载建立过程为例，详细设计了测试步骤，仔细分析了测试结果，验证协仿真测试的正确性，以及本文设计的正确性。

4， 在介绍板级测试原理的基础上，以承载资源分配过程为例，详细设计了测试步骤，仔细分析了测试结果，从另一方面验证协仿真测试的正确性，以及本文设计的正确性和可行性。

5.2 展望

本论文主要设计并实现了非接入层数据传输的协议软件，处于 LTE 系统终端设计和实现的初级阶段，对于系统的稳定性和健壮性等还需要进一步的研究，而且对于系统间切换时会话的管理流程未进行研究；另外限于篇幅，对于会话管理过程的异常情况处理和许多具体设计细节未能一一具体描述；对于会话管理流程过程中的众多测试项目，未能一一列表说明；同时可能有些极个别情况没有考虑到。这些都是下一步需要考虑和解决的问题。

致 谢

在论文撰写过程中，除了自身的潜心专研和努力之外，也凝聚了很多人的心血。在这论文即将完成之际，谨向在论文撰写期间给予巨大帮助的老师 and 同学们表示最由衷的感谢。

首先，我要感谢我的导师王琼老师，感谢王导师在我攻读硕士学位的三年中对我的热心指导。王导师丰富的实践经验、渊博的专业知识、务实忘我的工作作风、宽以待人的处事态度使我受益匪浅。

感谢重邮信科协议栈软件部的周中立、杨黎明、陈吕洋、朴虎哲老师，正是他们的敬业精神和治学态度为我营造了良好的工作和求学环境。感谢周巧成、姜浩等员工在我工作和学习中给予我的很多中肯的意见以及在论文的编写过程中给与的宝贵意见和建议，在此深深的感谢你们的帮助。

感谢高攀、程运、邓江、赵国会、何海鹏、刘娜，谢谢你们在这三年中在生活和学习上对我的关心和帮助。

感谢所有给我帮助和建议的朋友们，感谢我的家人，感谢你们在生活、学习和工作方面给予我的关心和支持。

最后，感谢为本论文的审阅付出艰辛劳动的各位专家和教授。谢谢你们。

参考文献

- [1] 沈嘉,索士强.3GPP 长期演进(LTE)技术原理与系统设计.第一版.[M].北京.人民邮电出版社.2008.P1-30,P378-424
- [2] 张克平.LTE-B3G/4G 移动通信系统无线技术.[M].北京.电子工业出版社.2008.06. P1-92, P126-203
- [3] 黄韬,刘韵洁.LTE/SAE 移动通信网络技术.第一版.[M].北京.人民邮电出版社.2009.P1-36,P85-115
- [4] Stefania Sesia, Issam Toufik, Matthew Baker. LTE, The UMTS Long Term Evolution From Theory to Practice.[M].UK. Wiley.2009
- [5] Farooq Khan.LTE for 4G Mobile Broadband.[M].Cambridge.Cambridge University Press.2009
- [6] 康钊 .TD-LTE 城市示范网建设推迟缘于终端过于初级 . [J].<http://www.china-3g.com/Show.asp?id=32122>.2010.10
- [7] 3GPP TS 36.300 V9.5.0."Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description". [S].2010-09.P17-80
- [8] 3GPP TS 23.401 V9.6.0."Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access". [S] .2010-09.P14-71
- [9] LTE 系统中 PDN 连接过程的建立与实现.[J].电视技术.2010.第 34 卷第 12 期.P94-96
- [10] 周中立,李小文.TD-SCDMA 系统终端中 RAB 重建过程的实现.[J].重庆邮电学院学报 2005 第 17 卷第 4 期.P35-38
- [11] 3GPP TS 24.008 V9.4.0."Technical Specification Group Core Network and Terminals; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".[S].2010-09.P235-264,P445-447
- [12] 3GPP TS 24.301 V9.4.0."Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS) ". [S].2010-09.P131-166
- [13] 大唐移动通信技术有限公司.EPS 承载管理的方法、装置、MME 及通信系统.[P].

- 中国.CN 101394580A.2007
- [14] 北京三星通信技术研究有限公司.LTE 系统中的会话接入方法.[P].中国.CN 1933651A.2005
- [15] Jaewook Shin, Kwangryul Jung and Aesoon Park.Design of Session and Bearer Control Signaling in 3GPP LTE System. [J].IEEE.2008.Vol3.
- [16] 王泽宁,李传峰.LTE 研究.现代电信科技.[J].2009 年 10 月.第 10 期.P23-27
- [17] 大唐移动通信设备有限公司.一种为终端分配静态 IP 地址的方法、系统及装置.[P].中国.CN 101453492A.2009
- [18] 3GPP TS 36.331 V9.4.0."3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC);Protocol specification".[S]. 2010-09.P37-49
- [19] 3GPP TS 24.007 V9.0.0. "Technical Specification Group Core Network and Terminals; Mobile radio interface signalling layer 3". [S].2009-12.P28,P41 -47
- [20] Anna Larmo, Magnus Lindstrom.The LTE Link-Layer Design.[J].IEEE Communications Magazine.April 2009.vol04.P52-59.
- [21] Nokia, Ericsson. Pseudo-CR on Message header for EPS session management. [R].C1-081650.Cape Town, South Africa.3GPP.2008
- [22] Fredrik Presson. Voice over IP Realized for the 3GPP Long Term Evolution. Vehicular Technology Conference.[J].Baltimore.IEEE.2007.P1090-3038
- [23] 3GPP TR 21.905 V9.4.0."3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".[S].2009-12.P6-53
- [24] Kenneth A. Reek 著徐波 译.C 和 C++实务精选 C 和指针.[M].北京.人民邮电出版社.2003.P355-386
- [25] 彭木根.TD-SCDMA 移动通信系统.机械工业出版社.[M].机械工业出版社. 2009 年 7 月.P50-103
- [26] 李小文,李贵勇,陈贤亮.TD_SCDMA 第三代移动通信系统、信令及实现.[M]. 北京.人民邮电出版社.2003.1.P363-384
- [27] 郑人杰等.实用软件工程.[M].北京.清华大学出版社.1997.4.P207-209
- [28] 王文编著.软件工程学教程.[M].北京.科学出版社.2004.P175-179
- [29] 宋茂强.通信软件设计基础.[M].北京.北京邮电大学出版社.2001.10.P44-133
- [30] Telelogic tau AB.Telelogic tau SDL suite 4.0 Methodology Guidelines.[Z].2001
- [31] ITU-T Recommendation Z.100.CCITT SPECIFICATION AND DESCRIPTION

- LANGUAGE (SDL). [S].P34-47
- [32] 罗一静,段红光. 利用 TTCN 进行协议测试的一种方法[J].广东通信技术.2006. vol26 No.6.P41-45
- [33] 3GPP TS 36.508 V9.2.0."Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Packet Core (EPC); Common test environments for User Equipment (UE) conformance testing".[S].2010-09.P58-83
- [34] 3GPP TS 36.523-1 V9.1.1."3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Packet Core (EPC); User Equipment (UE) conformance specification; Part 1: Protocol conformance specification". [S].2010-06.P452-517
- [35] 3GPP TS 36.523-2 V9.1.2."3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Packet Core (EPC); User Equipment (UE) conformance specification; Part 2: Implementation Conformance Statement (ICS) proforma specification".[S].2010-06.P45

附录 攻硕期间从事的科研工作及取得的研究成果

学习期间参与的科研项目：

[1] TD-LTE 终端基带芯片研发，2009ZX03002-003-05，国家重大专项，新一代宽带无线移动通信网科技重大专项

[2] LTE TDD 终端基带芯片的开发及产业化，发改办高技[2008]2441 号，国家发改委，国家新一代宽带及网络通信产业化专项

[3] LTE TDD 终端基带芯片平台关键技术的研究与应用，CSTC2009AB2088 号，重庆市科委，重庆市科技攻关项目

学习期间发表的论文

[1] 刘毅,王琼. LTE 系统中 PDN 连接过程的建立与实现.[J].电视技术.2010 年第 12 期