**文件编号：LTE-HeNB\_RRC\_REESTAB\_LJBG\_V1.0**

**TD-LTE HeNB协议栈软件系统**

**RRC连接重建立模块**

**理解报告说明书**

拟制：张瑞明

时间：2011-8-30

**中国科学院计算技术研究所**

**先进无线技术联合研究中心**

**软件组**

**LTE协议栈项目组**

修改记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 文件编号 | 版本号 | 拟制人/  修改人 | 拟制/修改日期 | 更改理由 | 主要更改内容  （写要点即可） |
|  |  | 张瑞明 | 2011-8-30 | 无 |  |
|  |  |  |  |  |  |
| 注1：每次更改归档文件（指归档到组内及研究室的文件）时，需填写此表。  注2：文件第一次归档时，“更改理由”、“主要更改内容”栏写“无”。 | | | | | |

修改列表：



### 本文档的程序或内容受版权法的保护，未经中科院计算所的书面许可，不得擅自泄漏、拷贝或复制本文档资料的全部或部分。

### **1 概述**

#### 1.1 UE 状态和状态转换（包括异系统之间）

当已经建立了RRC 连接，则UE处在RRC\_CONNECTED状态。如果没有建立RRC连接，即UE处在RRC\_IDLE状态,分类如下：

a) **RRC\_IDLE：**

* + 高层可以配置UE专用DRX；
  + UE控制的移动性；
  + 对于UE：
    - * 监控一个寻呼信道，进而检测到来的呼叫、系统信息改变、以及ETWS通知（仅对支持ETWS的UE）；
      * 进行邻区测量和小区选择（重选）；
      * 获取系统信息。

b) **RRC\_CONNECTED：**

* + 传输给/来自UE的单播数据传输。
  + 在低层，UE可以被配置为具有UE专用DRX。
  + 网络控制的移动性
  + 对于UE：
    - * 监控一个寻呼信道和/或SIB1的内容，进而检测系统消息更改，以及ETWS通知（仅适用于支持ETWS的UE）；
      * 监控与共享数据信道相关联的控制信道，进而决定是否为其准备数据；
      * 提供信道质量和反馈信息；
      * 进行邻区侧量和测量报告；
      * 获取系统信息。

#### 1.2 信令无线承载

“信令无线承载”（SRB）定义为仅仅用于RRC和NAS消息传输的无线承载（RB）。更具体地讲，定义如下三种SRB：

* + SRB0用于建立RRC 消息，使用CCCH逻辑信道；（说明：1，RRC消息包括RRC连接请求建立，RRC连接建立消息，RRC连接拒绝消息；RRC连接重建请求消息，RRC连接重建拒绝。2，CCCH UE与网络间用来传输控制信息的逻辑信道）
  + SRB1 用于传输RRC 消息（可能包括捎带的NAS消息）和建立先于SRB2的建立的NAS消息，使用DCCH逻辑信道；（说明：1，DCCH UE与网络间用来传输专用控制信息的点到点双向传输。2，下行捎带的NAS 消息仅仅作为一个流程（即关于连接成功/失败）：建立/修改/释放承载的依附。上行捎带的NAS消息仅仅用于在建立连接的过程中传输初始的NAS 消息。）
  + SRB2 用于传输 NAS消息，使用DCCH逻辑信道。（说明：SRB2要后于 SRB1建立，并且总是由E-UTRAN在安全激活后进行配置。）

注： NAS消息由SRB2传输的当然它也包含在RRC消息中，然而RRC消息中不包含任何RRC协议控制信息。

#### 1.3 关于UE的一些说明

UE将：

1> 由RRC对接收的消息进行按序处理，即在开始对后来的消息进行处理之前，应该完成对前面消息的处理；

注 1： 在接收前期触发过的UE响应之前，E-UTRAN可以促发后面的过程。（按时序触发,实时性）

1> 在每字节中按照过程描述中的顺序来执行步骤；

1> 在响应消息中如果包含（rrc-TransactionIdentifier）的话，将rrc-TransactionIdentifier设置为等于从E-UTRAN接收的触发响应消息中包含的值；

1> 当接收到一个设置为 ‘setup’的选择值时，有：

2> 采用相应的接收配置，以及开始使用相关的资源，除非有其它情况的明确说明；

1> 当接收到一个设置为 ‘release’的选择值时，有：

2> 清除相应的配置，以及停止使用相关的资源；

1>当切换到E-UTRA；或

1>当收到的RRCConnectionReconfiguration消息中包含fullConfig时，有：

2>使用在drb-ToAddModList中重配DRB时包含DRB/PDCP/RLC 建立的ASN.1的配置条件。

注 2： 在每个时间点，UE保持对每个变量只保持一个值，但为了在切换失败时回到以前的配置，在切换时UE可以临时保存原来的配置。总之：当UE重配一个变量时，除了切换，现有的值都要释放掉。

注3： 尽管没有明确指出，UE最初认为所有的功能将被去激活/释放直到这些功能被显式地建立/激活。相应地，UE最初认为列表是空的，例如无线承载列表，测量列表。

### **2 系统信息**

#### 2.1 概述

系统信息(Sl。System Information)是由eNB端的RRC层通过广播的方式发给UE的与整个通信系统相关的一些系统级参数，包括具有固定调度周期的SI和动态调度周期的SI。UE需维护SI窗口以接收Sl消息，在不同场景下获取不同的SI作为进行其后续行为的决策依据。

系统信息分成MasterInformationBlock(MIB)和多个SystemInformationBlocks (SIBs)。MIB包括有限个最重要、最常用的传输参数，其需要从该小区中获得其它的信息，同时其在 BCH上进行传输。

在SystemInformation (SI)消息中承载的是SIB，而不是SystemInformationBlockType1， SIB到SI消息的映射是灵活配置的，由在SystemInformationBlockType1中包含的schedulingInfoList进行配置，此外还有一些约束，即每个SIB仅仅包含在单个 SI消息中，仅仅具有相同调度要求（周期）的SIB能映射到相同的SI消息，并且SystemInformationBlockType2总是可以映射到对应于schedulingInfoList中SI消息列表第一个条目的SI消息。可能会有多个传输具有相同周期的SIB的SI消息。SystemInformationBlockType1和所有的SI消息是传输在DL-SCH。

系统信息（不是指 ETWS）的更改仅发生在特定的无线帧上，即引入一种更改周期的概念。当网络更改系统信息（或部分系统信息）时，首先它会首先把此更改通知UE，即可能会在整个更改周期中通知。在下一个更改周期中，网络传输更新的系统信息。

说明：寻呼（Paging）消息用于通知处在空闲状态的UE以及RRC\_CONNECTED状态的UE关于系统信息的更改。如果UE收到一条包括systemInfoModification的 Paging消息，表明系统信息将在下一个更改周期中进行更改。虽然UE可能被通知关于系统信息的更改，但是进一步的消息并没有提供

#### 2.2 系统信息获取



**图1系统信息获取，常规流程**

是E-UTRAN（发送端）通过广播方式（方式）发给UE（接收端）的与整个系统相关的一些系统级参数（可与Paging比较，更改参数），处于RRC\_IDLE和RRC\_CONNECTED状态的UE应用系统信息获取程序来获取E-UTRAN广播的接入层和非接入层系统信息。

#### 2.3 初始化

一旦小区选择（例如开机），或小区重选，或当从另一种RAT切换进入E-UTRA并完成时，或从没有覆盖的区域返回，或接收一个该系统信息已经改变的通知，或接收关于ETWS通知的指示，或接收关于CMAS通知的指示，或超出最大有效持续时间等，UE将应用系统信息获取流程。除非在该流程规范中有明确说明，否则系统信息获取流程将覆盖任一储存系统信息，即增量配置对于系统信息而言是不适用的，从证实该消息有效起经过3个小时后，删除任何存储的系统信息，除非有其它情况的描述。

#### 2.4 UE必需的系统信息

UE将：

1> 如果处在 RRC\_IDLE状态，那么：

2> *MasterInformationBlock*，*SystemInformationBlockType1*以及*SystemInformationBlockType2*~ *SystemInformationBlockType8*，取决于相关RAT的支持；

2>如果处在RRC\_CONNECTED状态，那么：

2> *MasterInformationBlock*，*SystemInformationBlockType1*，*SystemInformationBlockType2*，*SystemInformationBlockType8*，取决于 CDMA2000的支持；

### **3 连接控制**

#### 3.1 介绍

3.1.1 RRC 连接控制---- LTE使用无线承载(RB。Radio Bearer)分段映射的QoS体系结构，映射到相同RB上的服务数据流具有相同的传送等级，因而LTE系统通过RB实现了无线资源管理。连接控制过程实质是LTE系统中对RB控制的具体方式，实现了对数据无线承载(DRB，Data Radio Bearer)和信令无线承载(SRB。Signal Radio Bearer)的管理。

RRC 连接建立包括SRB1的建立。E-UTRAN在完成S1连接建立过程前，即在接收EPC发出的UE上下文信息之前，完成RRC连接的建立。因此，在RRC连接的初始阶段，AS安全将不会被激活。在RRC连接的初始阶段，E-UTRAN配置UE进行测量报告。不过，当AS安全被激活后，UE仅接受切换消息。

当接收到EPC发出的UE上下文后，E-UTRAN使用初始安全激活过程来激活安全（包括加密和完整性保护）。激活安全的RRC消息（命令与成功响应）会得到完整性保护，而加密只有当次过程完成后才开始。也就是说，激活安全消息的响应没有被加密，只有随后的消息有完整性保护和加密，比如建立SRB2和DRB的消息。

初始安全激活过程启动后，E-UTRAN发起SRB2和DRB的建立，也就是在接收到UE发出的初始安全激活确认前E-UTRAN 可以发起SRB2和DRB的建立。在任何情况下，E-UTRAN会对用于建立SRB2和DRB的RRC连接重配消息进行加密和完整性保护。如果初始安全激活和/或无线承载建立失败，E-UTRAN应释放RRC连接。

对于SRB2和DRB，安全总是在初始被激活，也就是说，E-UTRAN不会在激活安全之前建立这些承载。所以说，RRC层在RRC过程的执行中，完成对下层的管理和控制：

RRC通过连接(重)建立、连接配置和释放过程实现对RB的建立、修改和释放；

通过连接配置过程控制下层机制和行为。

另外RRC通过SI获取过程、安全激活过程对下层的基本参数进行配置

#### 3.1.2 安全性

AS 安全包括RRC信令的完整性保护，以及RRC信令和用户数据的加密。

RRC处理属于AS配置一部分的安全参数的配置，包括：完整性保护算法、加密算法以及两个参数（*keyChangeIndicator*和*nextHopChainingCount*）。*keyChangeIndicator*和*nextHopChainingCount*是UE用于在切换和/或连接重建立时，确定AS安全密钥的。(可能这些安全配置是由PDCP来完成，但是这些配置是由RRC来处理handle和应用的)

SRB1 和SRB2所使用的完整性保护算法是相同的。所有RB（SRB1、SRB2以及DRB）使用相同的加密算法。SRB0则没有完整性保护和加密。

完整性和加密算法(PDCP安全性的对象是C（control，控制）平面的信令以及U(user，用户)平面数据部分，完整性保护的对象仅针对C平面的信令部分，加密保护的对象仅针对U平面的信令部分，完整性保护在加密之前进行)仅能在切换时改变。每一次切换和连接重新建立，四个AS密钥（KeNB, KRRCint, KRRCenc和KUPenc）都会改变。keyChangeIndicator用于切换，且指示UE是否应使用与最近可用KASME密钥相关的密钥。当推演用于产生KRRCint, KRRCenc和KUPenc的新KeNB的时候，UE在切换和连接重建立使用nextHopChainingCount。

每个RB在每个方向都会保留一个独立的计数器。对于每个 DRB，该 COUNT被用作加密的输入。对于每个 SRB，该COUNT会被用作加密和完整性保护的输入。

#### 3.2 寻呼



图2寻呼流程

该流程的目的是：

-寻呼信息发送给RRC\_IDLE状态下的UE并将去往上层，从而发起RRC连接建立；（SRB0的建立）

- 通知处于RRC\_IDLE和RRC\_CONNECTED状态下的UE系统消息改变，是E-UTRAN（发送端）通过广播方式（方式）发给UE（接收端）的与整个系统相关的一些系统级更改参数。

该流程的时机是：E-UTRAN在UE寻呼时机，发送Paging 消息发起寻呼过程。

#### 3.3 RRC 连接建立



图3 RRC 连接建立，成功流程



图4 RRC 连接建立，网络拒绝流程

该流程的目的是：

- 该过程旨在建立一个RRC连接(SRB1的建立);

- 该过程也可用于从UE向E-UTRAN传输初始的NAS专用信息/消息。

该流程的时机是：

- 在RRC\_IDLE状态下，当上层请求建立RRC连接时（这个请求在Paging里，SRB0），UE将发起初始化过程来准备。在RRCConnectionRequest和RRCConnectionSetup之后，UE进入 RRC\_CONNECTED状态了，而在设置*RRCConnectionSetupComplete*消息内容时，设置*dedicatedInfoNAS*包含接收来自上层的信息（这句话说明了SRB1的建立，所以也说明了SRB1的建立是后于RRC\_CONNECTED状态的建立）

#### 3.4 初始安全激活



图5安全模式命令，成功流程



图6安全模式命令，失败流程

该流程的目的是：

* 该过程旨在在RRC连接建立上激活AS安全（SRB2的建立）；

该流程的时机是：

* 当接收到EPC发出的UE上下文后，E-UTRAN使用初始安全激活过程来激活安全，E-UTRAN 向处在RRC\_CONNECTED状态的UE初始化SecurityModeCommand。

一旦安全被激活，在SRB1和SRB2上所有的RRC消息，包括那些包含NAS或非3GPP消息，都由PDCP进行完整型保护和加密。NAS各自独立采用完整性保护和加密生成NAS消息。

建立SRB2和DRBs

在激活安全之后，E-UTRAN开始建立SRB2和DRBs。E-UTRAN在收到来自UE的安全激活确认之前就开始建立SRB2和DRBs，在这种情况下，用于建立SRB2和DRBs的RRC连接重配置消息使用完整性保护和加密。如果安全激活或者RB建立失败，E-UTRAN应该释放RRC连接（给出两个暗含的意义：RRC connection re-configuration实际是用来建立SRB2和DRBs；当bearers建立失败时使用RRC connection release消息）。

#### 3.5 RRC 连接重配置



图7 RRC 连接重配置，成功流程



图8 RRC 连接重配置，失败流程

该流程的目的是：

* 该过程旨在修改RRC连接，例如，建立/修改/释放RB，进行切换，准备/修改/释放测量。作为该过程的部分，NAS专用信息可以从 E-UTRAN 传输给UE。

该流程的时机是：

E-UTRAN对处在RRC\_CONNECTED状态下的UE发起RRC连接重配置过程，如下：

- 仅当AS安全已经被激活时，才包含mobilityControlInfo，并建立SRB2以及至少一个DRB，且不会挂起；

- 仅当AS安全已经被激活时，才包含RB的建立（与SRB1不同，在RRC连接建立时就建立过了）；

#### 3.6 RRC 连接重建立



图9 RRC 连接重建立，成功流程



图10 RRC 连接重建立，失败流程

该流程的目的是：

- 重配SRB1，且仅为其恢复数据传输；

- 重新激活AS安全不改变算法。（算法不变，但是基于不变算法的密钥要更新）

该流程的时机是：

处于RRC\_CONNECTED(连接状态不是SRB1建立的等价形式，他们甚至是独立的，没有太多约束对方的性质)状态的UE，安全已被激活，可发起该过程继续RRC连接。仅当相关小区是具有UE上下文的小区时，连接重建才会成功。假使E-UTRAN认可重建，SRB1的操作会恢复，而其它RB将继续保持挂起。它将初始化该进程来继续重建RRC连接。如果AS安全没有被激活，UE不会发起该过程，而直接转到RRC\_IDLE状态。（）

满足以下任一条件时，UE才发起初始化过程：

1> 检测到无线链路失败；或者

1> 切换失败；或者

1> E-UTRA侧移动性失败；或者

1> 底层制式完整性校验失败；或者

1> RRC连接重配失败

网络端接收到UE端发送的请求消息(先释放)后，作出响应，发送RRC连接重建立消息到UE，告知UE端可以进行RRC重建进程的操作。在接收到网络端的指示后（连接建立），LIE端的RRC将重建PDCP和RLC，并执行无线资源配置进程，利用先前配置的加密和完整性保护算法，更新密钥，配置低层以激活完整性保护和加密，执行相关测星，并将RRC连接重建完成消息传送到网络端。

### **RRC连接控制交互过程**



### **RRC重建立流程**





