**文件编号：LTE-HeNB\_RRC\_COUNTERCHECK\_LJBG\_V0.5**

**TD-LTE HeNB协议栈软件系统**

**CounterCheck**

**理解报告**

拟制：张瑞明

时间：2011.11.17

**中国科学院计算技术研究所**

**无线通信技术研究中心**

**软件组**

**LTE协议栈研发项目组**

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） |
|  | 0.5 |  | 2011-11-17 | 建立 |  |
|  | 0.6 |  | 2011-11-23 |  |  |
| 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：

后续版本对之前版本所做修改逐条说明清楚。



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。

**目录**

[1 引言 4](#_Toc309913177)

[1.1 编写目的4](#_Toc309913178)

[1.2 定义4](#_Toc309913179)

[1.3 参考资料4](#_Toc309913180)

[2 COUNTER CHECK 5](#_Toc309913181)

[2.1 COUNT5](#_Toc309913182)

[2.2 PDCP SN5](#_Toc309913183)

[2.3 HFN5](#_Toc309913184)

[2.4 Counter Check6](#_Toc309913185)

[2.4.1 COUNTERCHECK作用6](#_Toc309913186)

[2.4.2 ENB过程 6](#_Toc309913187)

[2.4.3 UE过程 7](#_Toc309913188)

[3 其他说明 10](#_Toc309913189)

**CounterCheck模块理解报告**

# 1 引言

## 1.1 编写目的

本文档将作为MAC接收模块的代码编写的依据，详细说明了本模块功能、结构、函数定义，以及与其它模块的接口。本说明书的读者为LTE HeNB端MAC接收模块设计、编码人员、测试人员、项目组负责人员、实验室主任及相关项目管理人员。

编写本说明书的目的在于

* 为开发人员提供依据。
* 为修改和维护本系统提供条件。
* 项目负责人将根据本文档计划和控制系统设计、开发的全过程。

## 1.2 定义

SN: Sequence Number

HFN: hyper frame number

## 1.3 参考资料

1. 《3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2"》；
2. 《3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification"》；
3. 《3GPP TS 33.4011: "3GPP System Architecture Evolution (SAE); Security architecture "》;

# 2 COUNTER CHECK

## 2.1 COUNT

长度：由32bit组成；

COUNT值用于LTE空口侧PDCP对数据和信令的加解密，以及对信令的完整性保护。它由HFN和PDCP SN组成，PDCP SN的长度由RRC配置，HFN的长度则等于32减去PDCP SN。



图1.COOUNT结构

## 2.2 PDCP SN

长度：由5,7或者12bit组成；

PDCP SN值用于标识业务的按序传输，且无线传送过程中SN被包含在PDU里。

表1.PDCP SN 长度

|  |  |
| --- | --- |
| Length | Description |
| 5 | SRBs |
| 7 | DRBs(*pdcp-SN-Size* [3]) |
| 12 | DRBs (*pdcp-SN-Size* [3]) |

## 2.3 HFN

HFN是一种溢出计数机制，被用于在eNB和UE之间以确保DRB的同步，更确切说，是一种确保安全的同步机制！同时以“SN位满便进位到HFN”的方式保证和限制SN的实际数量。

## 2.4 Counter Check



图3. eNB periodic local authentication procedure

### 2.4.1 COUNTERCHECK作用

E-UTRAN使用Counter Check消息来请求UE验证每个DRB上发送/接收的数据量。更具体来说，UE需要对每个DRB检查，判断COUNT的最高有效位是否与E-UTRAN指示的相同。

CounterCheck这个过程可以使E-UTRAN察觉非法的入侵，他可在COUNT达到任一个特定值时，E-UTRAN 通过发送一个CounterCheck消息来发起该过程。

### 2.4.2 ENB过程

eNB会随意可选（意为周期时间是可选的）的应运Counter Check来周期性的执行本地认证，周期确定以后，对HFN的检测会是当每有任何一位变化便同步一次，如HFN的某个固定位有变化。

该过程的目的是验证“在UTRAN和UE中，RRC连接期间双向链路（上行链路和下行链路）上所发送的数据量是相同的（来检测可能出现的入侵者的操作）”！如果，UE接收到了CounterCheck的请求消息，它会响应Counter Check Response消息。

eNB的PDCP会一直周期性监管联系着每个无线信令承载（更确切说是DRB）的COUNT值，所以只要监管到COUNT接收到一个特殊值（HFN的值的变化）便会促发countercheck过程。而这个周期的间隔力度被访网络定义。此过程中的所有消息会被完整性保护！

具体步骤如下：

1　当收到一个检测值（如，这个值的HFN的某个固定位被篡改），eNB会发送Counter Check消息，此消息中包含着来至每个DRB的PDCP COUNT值的MSB部分（它反映着数据的接收情况）；

2　UE在接收到Counter Check值后会与自己的每个DRB比较COUNTMSB值，异常的UE COUNT值会被包含在Counter Check Response反馈回去；

3　eNB接收到反馈来的Counter Check Response消息后，如果没有包含任何的异常PDCP COUNT值，则此过程结束；如果包含1个或者多个异常PDCP COUNT值，eNB会释放该DRB并且上报给MME（以释放对应的E-RAB）。

### 2.4.3 UE过程

接收到CounterCheck 消息，UE应：

1> 对于每个建立的DRB：

2>如果在一个给定的方向上（上行或者下行）没有COUNT， 因为已经建立的DRB是对应另一个方向配置的单向承载：

3>认为该方向的COUNT值是‘0’；

2>如果drb-CountMSB-InfoList中没有包含某个drb-Identity：

3>通过在CounterCheckResponse消息drb-CountInfoList中包含drb-Identity的方式包含该DRB，count-Uplink 和count-Downlink设置为相应COUNT的值；

2>否则，如果至少在一个方向上，COUNT的MSB与drb-CountMSB-InfoList指示的值不同：

3> 通过在drb-CountInfoList 的CounterCheckResponse消息中包含中drb-Identity的方式包含该DRB，count-Uplink 和count-Downlink设置为相应COUNT的值；

1>对于包含在CounterCheck消息的drb-CountMSB-InfoList还没有被建立的每一个DRB：

2> 在CounterCheckResponse 消息drb-CountInfoList中包含 drb-Identity的方式包含该DRB，把count-Uplink和count-Downlink 的MSB设置为drb-CountMSB-InfoList 一样的值，且LSB设置为0；

1> 将CounterCheckResponse 消息提交给底层传输，该过程结束；



图4.发送CounterCheck消息过程



图5.接收CounterCheckResponse消息过程

# 3 其他说明

方案1，确定周期时间，然后在周期之内将需要验证同步的DRBlist（包含多个有异常的count值）以CounterCheck消息传到对端，ue按协议处理之后，eNB收到CounterCheckResponse后，将没有包含在list的DRB验证，将包含在list且不同步的DRB释放；

方案2，不需要确定周期时间，只要count值有异常值便将此UE对应的所有DRB组成list传到对端（注意此list里面只有一个需验证，但是组成list的原因在于在UE接收到countercheck消息后同步时确保所有的DRB-id都有，也就不会出现协议中的“若countercheck消息中没有包含某个DRB-id”的情况），当ue同步完成以后传回给eNB 的response有且有最多一个不同步counter值，释放便可；

方案3，将方案1和2结合，确定周期且将所有DRBlist传输；

若按方案1，周期和HFN的特殊位的确定如下：以7位SN为例，则HFN是25位，即是从第8位到第32位，则将第8位作为HFN的特殊固定位，因为HFN的计数无论变化有多大都是从它的最低位开始的，也就是从第8位开始的，所以只要将SN从最小值变化到最大值传输的数据量所需的时间计算出来便是countercheck模块的最小周期时间！这样就保证了每个周期内都会有需要同步的HFN存在！