



(12)发明专利

(10)授权公告号 CN 104469745 B

(45)授权公告日 2018.05.01

(21)申请号 201410692503.X

(22)申请日 2014.11.26

(65)同一申请的已公布的文献号

申请公布号 CN 104469745 A

(43)申请公布日 2015.03.25

(73)专利权人 大唐移动通信设备有限公司

地址 100083 北京市海淀区学院路29号

(72)发明人 程岳

(74)专利代理机构 北京同达信恒知识产权代理

有限公司 11291

代理人 朱佳

(51)Int.Cl.

H04W 8/24(2009.01)

H04W 12/06(2009.01)

H04W 12/10(2009.01)

(56)对比文件

CN 102833741 A,2012.12.19,

CN 1863397 A,2006.11.15,

CN 102316455 A,2012.01.11,

CN 1960374 A,2007.05.09,

CN 101610506 A,2009.12.23,

苏燕.由于安全模式超时导致PS域掉线的问题解决案例.《移动通信》.2013,(第14期),第24-27页.

审查员 彭聪

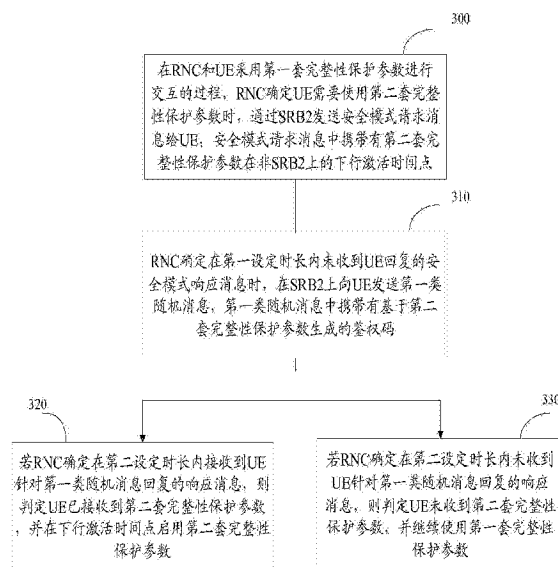
权利要求书3页 说明书14页 附图5页

(54)发明名称

一种完整性保护参数的应用方法及装置

(57)摘要

本发明涉及通信领域,特别是涉及一种完整性保护参数的应用方法及装置,用以保证用户的感知并提升KPI指标。该方法为,RNC在SRB2上发送携带用第二套完整性保护参数计算的鉴权码的下行随机消息,若UE对该随机消息进行响应,说明UE采用采用了第二套完整性保护参数,并在下行激活时间点启用第二套完整性保护参数;若UE未对该消息进行响应,则继续使用第一套完整性保护参数,以此来稽核UE和RNC使用的完整性保护参数的一致性,且稽核过程不会引起对呼叫流程的影响,有效地避免了CS域语音业务掉话和UE资源挂住的问题,保证了用户的感知,提升了KPI指标。



1. 一种完整性保护参数的应用方法,其特征在于,包括:

在无线网络控制器RNC和用户设备UE采用第一套完整性保护参数进行交互的过程中,RNC确定UE需要使用第二套完整性保护参数时,通过第二类无线承载SRB2发送安全模式请求消息给UE,所述安全模式请求消息中携带有所述第二套完整性保护参数在非SRB2上的下行激活时间点;

RNC确定在第一设定时长内未收到所述UE回复的安全模式响应消息时,在SRB2上向所述UE发送第一类随机消息,所述第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码;

若RNC确定在第二设定时长内接收到UE针对所述第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并在所述下行激活时间点启用所述第二套完整性保护参数;

若RNC确定在第二设定时长内未收到UE针对所述第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并继续使用所述第一套完整性保护参数;

其中,RNC确定在第一设定时长内未收到所述UE回复的安全模式响应消息时,在SRB2上向所述UE发送第一类随机消息,所述第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码,具体包括:

RNC确定在第一设定时长内未收到所述UE回复的安全模式响应消息时,在所述第二套完整性保护参数在非SRB2上的下行激活时间点到达之前,采用预设的发送次数和发送时间间隔,在SRB2上向所述UE发送第一类随机消息,所述第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码。

2. 如权利要求1所述的方法,其特征在于,RNC确定UE需要使用第二套完整性保护参数时,具体包括:

RNC获知UE在当前域中所采用的第一套完整性保护参数需要更改时,确定UE需要使用第二套完整性保护参数;

RNC获知UE在与当前应用域不同的另一域中发起相应业务时,确定UE需要使用第二套完整性保护参数。

3. 如权利要求1或2所述的方法,其特征在于,若RNC确定在第二设定时长内接收到UE针对所述第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并在所述下行激活时间点启用所述第二套完整性保护参数,具体包括:

若RNC确定在第二设定时长内接收到UE针对所述第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并直接在所述下行激活时间点启用所述第二套完整性保护参数;

或者,

若RNC确定在第二设定时长内接收到UE针对所述第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并进一步在所述下行激活时间点之前,在非SRB2上向所述UE发送第二类随机消息,所述第二类随机消息中携带有基于第一套完整性保护参数生成的鉴权码;以及在第三设定时长内接收到UE针对所述第二类随机消息回复的响应消息时,判定UE已经获知第二套完整性保护参数在非SRB2上的下行激活时间点,并在所述下行激活时间点启用所述第二套完整性保护参数。

4. 如权利要求1或2所述的方法,其特征在于,若RNC确定在第二设定时长内未收到UE针对所述第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并继续使用所述第一套完整性保护参数,具体包括:

若RNC确定在第二设定时长内未收到UE针对所述第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并直接继续使用所述第一套完整性保护参数;

或者,

若RNC确定在第二设定时长内RNC未收到UE针对所述第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并进一步在SRB2上向所述UE发送第二类随机消息,所述第二类随机消息中携带有基于第一套完整性保护参数生成的鉴权码,以及在第四设定时长内接收到UE针对所述第二类随机消息回复的响应消息时,判定UE未收到第二套完整性保护参数,并继续使用所述第一套完整性保护参数。

5. 如权利要求1所述的方法,其特征在于,进一步包括:

当RNC接收到所述UE在任一SRB上发送的上行消息时,RNC先采用第一套完整性保护参数对所述上行消息进行鉴权;

若鉴权未通过,RNC继续采用所述第二套完整性保护参数对所述上行消息进行鉴权,若采用所述第二套完整性保护参数鉴权通过,确定达到所述第二套完整性保护参数在所述任一SRB上的上行激活时间点,并直接删除所述第一套完整性保护参数,后续使用所述第二套完整性保护参数;

若鉴权通过,则确定还未达到所述第二套完整性保护参数在所述任一SRB上的上行激活时间点。

6. 一种完整性保护参数应用的装置,其特征在于,包括:

第一通信单元,用于在RNC和UE采用第一套完整性保护参数进行交互的过程中,确定UE需要使用第二套完整性保护参数时,通过SRB2发送安全模式请求消息给UE,所述安全模式请求消息中携带有所述第二套完整性保护参数在非SRB2上的下行激活时间点;

第二通信单元,用于确定在第一设定时长内未收到所述UE回复的安全模式响应消息时,在SRB2上向所述UE发送第一类随机消息,所述第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码;

以及若确定在第二设定时长内接收到UE针对所述第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并在所述下行激活时间点启用所述第二套完整性保护参数;若确定在第二设定时长内未收到UE针对所述第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并继续使用所述第一套完整性保护参数;

其中,确定在第一设定时长内未收到所述UE回复的安全模式响应消息时,在SRB2上向所述UE发送第一类随机消息,所述第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码,所述第二通信单元具体用于:

确定在第一设定时长内未收到所述UE回复的安全模式响应消息时,在所述第二套完整性保护参数在非SRB2上的下行激活时间点到达之前,采用预设的发送次数和发送时间间隔,在SRB2上向所述UE发送第一类随机消息,所述第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码。

7. 如权利要求6所述的装置,其特征在于,确定UE需要使用第二套完整性保护参数时,

所述第一通信单元具体用于：

获知UE在当前域中所采用的第一套完整性保护参数需要更改时，确定UE需要使用第二套完整性保护参数；

获知UE在与当前应用域不同的另一域中发起相应业务时，确定UE需要使用第二套完整性保护参数。

8. 如权利要求6或7所述的装置，其特征在于，若确定在第二设定时长内接收到UE针对所述第一类随机消息回复的响应消息，则判定UE已接收到第二套完整性保护参数，并在所述下行激活时间点启用所述第二套完整性保护参数，所述第二通信单元具体用于：

若确定在第二设定时长内接收到UE针对所述第一类随机消息回复的响应消息，则判定UE已接收到第二套完整性保护参数，并直接在所述下行激活时间点启用所述第二套完整性保护参数；

或者，

若确定在第二设定时长内接收到UE针对所述第一类随机消息回复的响应消息，则判定UE已接收到第二套完整性保护参数，并进一步在所述下行激活时间点之前，在非SRB2上向所述UE发送第二类随机消息，所述第二类随机消息中携带有基于第一套完整性保护参数生成的鉴权码；以及在第三设定时长内接收到UE针对所述第二类随机消息回复的响应消息时，判定UE已经获知第二套完整性保护参数在非SRB2上的下行激活时间点，并在所述下行激活时间点启用所述第二套完整性保护参数。

9. 如权利要求6或7所述的装置，其特征在于，若确定在第二设定时长内未收到UE针对所述第一类随机消息回复的响应消息，则判定UE未收到第二套完整性保护参数，并继续使用所述第一套完整性保护参数，所述第二通信单元具体用于：

若确定在第二设定时长内未收到UE针对所述第一类随机消息回复的响应消息，则判定UE未收到第二套完整性保护参数，并直接继续使用所述第一套完整性保护参数；

或者，

若确定在第二设定时长内RNC未收到UE针对所述第一类随机消息回复的响应消息，则判定UE未收到第二套完整性保护参数，并进一步在SRB2上向所述UE发送第二类随机消息，所述第二类随机消息中携带有基于第一套完整性保护参数生成的鉴权码，以及在第四设定时长内接收到UE针对所述第二类随机消息回复的响应消息时，判定UE未收到第二套完整性保护参数，并继续使用所述第一套完整性保护参数。

10. 如权利要求6所述的装置，其特征在于，进一步包括：

上行判断单元，用于当接收到所述UE在任一SRB上发送的上行消息时，先采用第一套完整性保护参数对所述上行消息进行鉴权；

以及若鉴权未通过，继续采用所述第二套完整性保护参数对所述上行消息进行鉴权，若采用所述第二套完整性保护参数鉴权通过，确定达到所述第二套完整性保护参数在所述任一SRB上的上行激活时间点，并直接删除所述第一套完整性保护参数，后续使用所述第二套完整性保护参数；若鉴权通过，则确定还未达到所述第二套完整性保护参数在所述任一SRB上的上行激活时间点。

一种完整性保护参数的应用方法及装置

技术领域

[0001] 本发明涉及通信领域,特别是涉及一种完整性保护参数的应用方法及装置

背景技术

[0002] 为了确保空中接口的信息安全,避免空中接口所传递的无线资源控制协议(Radio Resource Control, RRC)信令消息被非法截获、破坏或者攻击,3GPP规范中规定使用F9算法对空中接口RRC信令消息进行完整性保护(Integrity Protection)。完整性保护需要无线网络控制器(Radio Network Controller, RNC)和用户设备(User Equipment, UE)使用相同的F9算法参数集,具体的,RNC和UE通过安全模式过程协商F9算法参数集的同步及生效时间点,对空中接口RRC信令消息进行完整性保护。此外,RRC消息的完整性检查也需要执行F9算法。

[0003] F9算法的输入参数为:完整性保护密钥(Integrity protection Key, IK)、完整性保护随机数(Integrity protection initialisation number, FRESH)、计数器数值(COUNT-I),消息发送方向(DIRECTION)、UU口消息(MESSAGE),具体如图1所示:

[0004] IK值是由UE和核心网(Core Network, CN)鉴权过程协商后保存在终端的全球用户识别卡(Universal Subscriber Identity Module, USIM)中。CN通过无线接入网络应用部分(Radio Access Network Application Part, RANAP)消息中的安全模式请求(SEcurity MODE COMMAND)消息通知RNC不同终端的IK值。此外,对于不同的域,IK值也不相同。

[0005] FRESH值由RNC随机产生,并通过安全模式过程中UU口RRC协议中的SECURITY MODE COMMAND消息通知终端。

[0006] COUNT-I由超帧号(Hyper Frame Number, HFN)和信令无线承载(Signalling Radio Bearers, SRB)的序列号(SN)组成,参阅图2所示,根据是否收到新的IK, RNC将COUNT-I的HFN部分初始化为0或START值。START值在初始直传消息或者链路承载(Radio Bear, RB)消息中由终端计算后携带给RNC。每个SRB维护一个上行SN,和一个下行SN,在发送消息后SN递增。

[0007] MESSAGE为RNC或者UE发送和接收的消息内容。

[0008] DIRECTION指上行或者下行。

[0009] 在完整性保护过程中,UE在接入网络时,通过鉴权过程同核心网协商IK、通过IU和UU口安全模式过程在RNC和UE间启动完整性保护参数。在完整性保护参数同步后,继续进行UU口RRC层消息的完整性检查过程。完整性保护机制是指发送方(UE或RNC)基于将要传送的MESSAGE,采用完整性保护参数(如,密钥IK、FRESH、COUNT-I等)经过F9算法计算获得消息鉴权码(Message authentication code, MAC)-I,再将该消息码附加在要传送的MESSAGE的报文头中,接收方(RNC或UE)收到消息后,采用同样的方法计算得到XMAC-I。接收方把收到的MAC-I和计算的XMAC-I进行比较,如果两者相等,说明收到的MESSAGE是完整的,在传输过程中没有被修改。

[0010] UE在RRC连接建立完成后,在进行语音业务前,同电路交换(Circuit Switching,

CS) 核心网进行鉴权和安全模式过程,并在RNC侧生成F9算法需要的完整性保护参数集合: {IK_{CS},COUNT-I (STARTVALUE_{CS},KEYSTATUS_{CS},FRESH)}。由于IK_{CS}需要定期更新,因而RNC需要根据CS域的IK_{CS}新旧状态KEYSTATUS_{CS}使用0或者CS域START值更新COUNT-I的HFN。

[0011] 在UE继续发起PS业务时,UE会同分组交换(packet switching,PS) 核心网进行鉴权和安全模式过程生成新的完整性保护参数: {IK_{PS},COUNT-I (STARTVALUE_{PS},KEYSTATUS_{PS},FRESH)}。由于IK_{PS}需要定期更新,因而RNC根据PS域的IK_{PS}新旧状态KEYSTATUS_{PS}使用0或者PS域START值更新SRB2的HFN。

[0012] 实际应用中,UE和RNC之间通常采用五个SRB进行交互,其中,SRB2可以立即激活新的完整性保护参数配置,而SRB0、SRB1、SRB3、SRB4需要配置新完整性保护参数和启动激活时间(也称激活时间点),激活时间点为非SRB2的当前SN+OFFSET (OFFSET>0)。其中,激活时间点为非SRB2发送RRC消息的序列号,上下行分别维护。RNC和UE通过非SRB2在上下行各自对应的激活时间点,使用IK_{PS}和最近一次PS域的START值或者0更新COUNT-I的HFN计算MAC-I和XMAC-I,即RNC和UE的5个SRB始终是同步生效F9算法需要的关键参数,具体如表1所示。

[0013] 表1

[0014]

信息 (Information Element/Group name)	需要 (Need)	类型和参 考 (Type and reference)	语义解释 (Semantics description)
RRC 消息序列号 (RRC message sequence number list)	必 选 (Manda torily Preset , MP)		The RRC sequence number when a new integrity protection configuration shall be applied, for signalling radio bearers in the order RB0, RB1, RB2, RB3, RB4. 新完整性保护配置应用时, 对信令 SRB0、SRB1、SRB2、SRB3、SRB4 来说 RRC 序列号应该被使用 The value for RB1 shall be ignored if this IE was included in a RRC message sent on RB1. 如果这个消息在 SRB1 上发送, 这个 IE 可以忽略不被使用

信息 (Information Element/Group name)	需要 (Need)	类型和参考 (Type and reference)	语义解释 (Semantics description)
[0015]			The value for RB2 shall be ignored if this IE was included in a RRC message sent on RB2. 如果这个消息在 SRB2 上发送, 这个 IE 可以忽略不被使用
RRC 消息序列号>RRC message sequence number	MP	整数 Integer (0..15)	

[0016] 因此,RNC在UE需要采用PS域的新完整性保护参数时,RNC需要将非SRB2上的下行消息的新完整性保护参数的启动激活时间用Security mode command消息通知UE,相应的,UE需要将非SRB2上的上行消息的新完整性保护参数的启动激活时间用安全模式完成(Security mode complete)消息通知RNC,其中,Security mode command消息和Security mode complete消息是使用IKps和最近一次PS域的START值或者0更新COUNT-I的HFN计算MAC-I和XMAC-I。

[0017] 在UE和RNC同步这些完整性保护参数后,发送方(RNC或者UE)发送RRC消息计算MAC-I和接收方(UE或者RNC)接收RRC消息计算XMAC-I使用相同的完整性保护参数,MAC-I和XMAC-I计算结果相同,完整性保护检查通过。如果参数不匹配,MAC-I和XMAC-I不同,RNC和UE丢弃消息导致信令流程中断。

[0018] 在发起任一种业务之前,TS24.008协议要求必须进行安全模式过程,由于CS域核心网和PS域核心网彼此独立,因此CS域和PS域分别独立和UE进行可能的鉴权和安全模式过程。此外,在UE同网络连接的过程中,CS域核心网和PS域核心网均可能由于密钥使用过长重新生成密钥而进行安全模式更改过程,即生成新的一套完整性保护参数。因此,在UU接口处,最多可能会存在3套完整性保护参数,即正在使用的保护UU口信令消息的完整性保护参数,CS域将要使用的完整性保护参数,PS域将要使用的完整性保护参数。

[0019] 在现网中经常出现多域并发的情况(例如,UE在同一时刻分别同CS域和PS域的核心网建立IU连接)。而在进行第二个域的UU口安全模式过程时,若RNC因网络超时未收到UE发送的Security mode complete消息,则将导致释放UE进而引起呼损和其他问题,如,对于长期演进技术(Long Term Evolution,LTE)单卡双待手机,PS域业务支持LTE,即4G网络,语音业务支持时分同步的码分多址技术(Time Division-Synchronous Code Division Multiple Access,TD-SCDMA)网络,即3G网络,则UE在TD-SCDMA网络进行CS通话状态下,逐渐移向LTE弱覆盖区域至脱网(TD-SCDMA信号良好),则UE将向TD-SCDMA网络侧发起PS域路由去更新请求(即在TD网络下重新申请PS域业务),PS域核心网将对终端身份进行认证,进

行安全模式过程;此时,若RNC未收到UE返回的Security mode complete消息引起空口超时(即可能出现UE丢弃掉Security mode command消息不响应或RNC未收到Security mode complete消息的情况),语音业务(即CS域业务)和数据业务(PS域业务)将同时被拆链,从而产生掉话,进而严重影响语音服务质量。即使在3G网络覆盖情况下,以RNC为单位设置位置区和路由区,在CS业务重定位成功后,必然进行PS域的路由区更新过程,如果PS域路由区更新时安全模式过程由于空口超时未成功定位,则必将导致CS域业务释放。此外,智能终端在CS域业务进行过程中,PS域业务可能由于保持背景心跳的缘故,反复释放和重建,在PS域业务每次重建过程中,都要进行PS域的安全模式过程,如果PS域的安全模式过程超时,RNC释放UE也会引起CS域业务释放。

[0020] 由于上述原因,在RNC同UE的信令交互过程中,很有可能由于启用某一套完整性保护参数而造成安全模式过程超时,从而造成双方使用的完整性保护参数不同而导致发送方和接收方计算的MAC-I和XMAC-I不同,交互的消息会因完整性检查将不能通过而被丢弃,从而进一步引起后续信令交互过程失败,呼叫流程中止。

[0021] 因此,在现有技术中,RNC同UE的信令交互过程失败后,RNC释放UE,导致用户感知差,由于产生在线CS域业务掉话,于是导致关键绩效指标(Key performance Indicator, KPI)指标差。此外,由于语音业务释放且在释放UE时,RNC发送给UE的RRC CONNECTION RELEASE消息的完整性保护采用PS域的完整性保护参数,但此时UE可能未收到或者由于协议原因丢弃Security mode command消息,UE使用的是CS域的完整性保护参数,因此UE计算的XMAC-I和RNC计算的MAC-I不同,UE丢弃RRC CONNECTION RELEASE消息引起UE不能被释放,但此时RNC侧资源已经释放掉但UE仍处于业务连接态导致UE资源挂住。随着3G、4G网络建设的发展,由核心网之间传递密钥的原因导致安全模式流程超时的情况呈上升趋势,出现大量CS域业务掉话和UE资源挂住的问题。

发明内容

[0022] 本发明实施例提供一种完整性保护参数的应用方法及装置,用以解决现有技术中在多域并发时造成的大量CS域语音业务掉话和UE资源挂住的问题。

[0023] 本发明实施例提供的具体技术方案如下:

[0024] 一种完整性保护参数的应用方法,包括:

[0025] 在RNC和UE采用第一套完整性保护参数进行交互的过程中,RNC确定UE需要使用第二套完整性保护参数时,通过SRB2发送安全模式请求消息给UE,安全模式请求消息中携带有第二套完整性保护参数在非SRB2上的下行激活时间点;

[0026] RNC确定在第一设定时长内未收到UE回复的安全模式响应消息时,在SRB2上向UE发送第一类随机消息,第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码;

[0027] 若RNC确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并在下行激活时间点启用第二套完整性保护参数;

[0028] 若RNC确定在第二设定时长内未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并继续使用第一套完整性保护参数。

[0029] 有效地避免了CS域语音业务掉话和UE资源挂住的问题。相对于原有的释放UE的策略,避免了UE和RNC丢弃交互的信令消息导致呼叫流程中断,保证了用户的感知,提升了KPI指标。

[0030] 较佳的,RNC确定UE需要使用第二套完整性保护参数时,具体包括:

[0031] RNC获知UE在当前域中所采用的第一套完整性保护参数需要更改时,确定UE需要使用第二套完整性保护参数;

[0032] RNC获知UE在与当前应用域不同的另一域中发起相应业务时,确定UE需要使用第二套完整性保护参数。

[0033] 较佳的,RNC确定在第一设定时长内未收到UE回复的安全模式响应消息时,在SRB2上向UE发送第一类随机消息,第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码,具体包括:

[0034] RNC确定在第一设定时长内未收到UE回复的安全模式响应消息时,在第二套完整性保护参数在非SRB2上的下行激活时间点到达之前,采用预设的发送次数和发送时间间隔,在SRB2上向UE发送第一类随机消息,第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码。

[0035] 较佳的,若RNC确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并在下行激活时间点启用第二套完整性保护参数,具体包括:

[0036] 若RNC确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并直接在下行激活时间点启用第二套完整性保护参数;

[0037] 或者,

[0038] 若RNC确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并进一步在下行激活时间点之前,在非SRB2上向UE发送第二类随机消息,第二类随机消息中携带有基于第一套完整性保护参数生成的鉴权码;以及在第三设定时长内接收到UE针对第二类随机消息回复的响应消息时,判定UE已经获知第二套完整性保护参数在非SRB2上的下行激活时间点,并在下行激活时间点启用第二套完整性保护参数。

[0039] 对于有激活时间的SRB下行方向,RNC发送携带携带第一套完整性保护参数鉴权码的随机消息,若收到UE的响应消息,进一步保证了UE已经获知第二套完整性保护参数在非SRB2上的下行激活时间点。

[0040] 较佳的,若RNC确定在第二设定时长内未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并继续使用第一套完整性保护参数,具体包括:

[0041] 若RNC确定在第二设定时长内未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并直接继续使用第一套完整性保护参数;

[0042] 或者,

[0043] 若RNC确定在第二设定时长内RNC未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并进一步在SRB2上向UE发送第二类随机消息,第

二类随机消息中携带有基于第一套完整性保护参数生成的鉴权码,以及在第四设定时长内接收到UE针对第二类随机消息回复的响应消息时,判定UE未收到第二套完整性保护参数,并继续使用第一套完整性保护参数。

[0044] 较佳的,进一步包括:

[0045] 当RNC接收到UE在任一SRB上发送的上行消息时,RNC先采用第一套完整性保护参数对上行消息进行鉴权;

[0046] 若鉴权未通过,RNC继续采用第二套完整性保护参数对上行消息进行鉴权,若采用第二套完整性保护参数鉴权通过,确定达到第二套完整性保护参数在任一SRB上的上行激活时间点,并直接删除第一套完整性保护参数,后续使用第二套完整性保护参数;

[0047] 若鉴权通过,则确定还未达到所述第二套完整性保护参数在所述任一SRB上的上行激活时间点。

[0048] 一种完整性保护参数应用的装置,包括:

[0049] 第一通信单元,用于在RNC和UE采用第一套完整性保护参数进行交互的过程中,确定UE需要使用第二套完整性保护参数时,通过SRB2发送安全模式请求消息给UE,安全模式请求消息中携带有第二套完整性保护参数在非SRB2上的下行激活时间点;

[0050] 第二通信单元,用于确定在第一设定时长内未收到UE回复的安全模式响应消息时,在SRB2上向UE发送第一类随机消息,第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码;

[0051] 以及若确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并在下行激活时间点启用第二套完整性保护参数;若确定在第二设定时长内未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并继续使用第一套完整性保护参数。

[0052] 有效地避免了CS域语音业务掉话和UE资源挂住的问题。相对于原有的释放UE的策略,避免了UE和RNC丢弃交互的信令消息导致呼叫流程中断,保证了用户的感知,提升了KPI指标。

[0053] 较佳的,确定UE需要使用第二套完整性保护参数时,第一通信单元具体用于:

[0054] 获知UE在当前域中所采用的第一套完整性保护参数需要更改时,确定UE需要使用第二套完整性保护参数;

[0055] 获知UE在与当前应用域不同的另一域中发起相应业务时,确定UE需要使用第二套完整性保护参数。

[0056] 较佳的,在确定在第一设定时长内未收到UE回复的安全模式响应消息时,在SRB2上向UE发送第一类随机消息,第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码,第二通信单元具体用于:

[0057] 确定在第一设定时长内未收到UE回复的安全模式响应消息时,在第二套完整性保护参数在非SRB2上的下行激活时间点到达之前,采用预设的发送次数和发送时间间隔,在SRB2上向UE发送第一类随机消息,第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码。

[0058] 较佳的,若确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并在下行激活时间点启用第二套完整性保

护参数,第二通信单元具体用于:

[0059] 若确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并直接在下行激活时间点启用第二套完整性保护参数;

[0060] 或者,

[0061] 若确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并进一步在下行激活时间点之前,在非SRB2上向UE发送第二类随机消息,第二类随机消息中携带有基于第一套完整性保护参数生成的鉴权码;以及在第三设定时长内接收到UE针对第二类随机消息回复的响应消息时,判定UE已经获知第二套完整性保护参数在非SRB2上的下行激活时间点,并在下行激活时间点启用第二套完整性保护参数。

[0062] 对于有激活时间的SRB下行方向,RNC发送携带携带第一套完整性保护参数鉴权码的随机消息,若收到UE的响应消息,进一步保证了UE已经获知第二套完整性保护参数在非SRB2上的下行激活时间点。

[0063] 较佳的,若确定在第二设定时长内未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并继续使用第一套完整性保护参数,第二通信单元具体用于:

[0064] 若确定在第二设定时长内未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并直接继续使用第一套完整性保护参数;

[0065] 或者,

[0066] 若确定在第二设定时长内RNC未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并进一步在SRB2上向UE发送第二类随机消息,第二类随机消息中携带有基于第一套完整性保护参数生成的鉴权码,以及在第四设定时长内接收到UE针对第二类随机消息回复的响应消息时,判定UE未收到第二套完整性保护参数,并继续使用第一套完整性保护参数。

[0067] 较佳的,进一步包括:

[0068] 上行判断单元,用于当接收到UE在任一SRB上发送的上行消息时,先采用第一套完整性保护参数对上行消息进行鉴权;

[0069] 以及若鉴权未通过,继续采用第二套完整性保护参数对上行消息进行鉴权,若采用第二套完整性保护参数鉴权通过,确定达到第二套完整性保护参数在任一SRB上的上行激活时间点,并直接删除第一套完整性保护参数,后续使用第二套完整性保护参数;若鉴权通过,则确定还未达到所述第二套完整性保护参数在所述任一SRB上的上行激活时间点。

附图说明

[0070] 图1为本发明背景技术中F9算法的输入参数示意图;

[0071] 图2为本发明背景技术中COUNT-1参数的构成示意图;

[0072] 图3为本发明实施例中完整性保护参数的应用方法的概述流程图;

[0073] 图4为本发明实施例中采用COUNTER CHECK消息和COUNTER CHECK RESPONSE消息稽核完整性保护参数的概述流程图;

[0074] 图5为本发明实施例中采用Identity Request消息和Identity Response消息稽核完整性保护参数的概述流程图；

[0075] 图6为本发明实施例中完整性保护参数稽核的具体流程图；

[0076] 图7为本发明实施例中完整性保护参数的应用装置的结构示意图。

具体实施方式

[0077] 为解决现有技术中在多域并发时出现的CS域语音业务掉话和UE资源挂住的问题，本申请实施例中提出多域并发造成UU口安全模式超时情况发生时不释放UE的策略，在RNC未收到UE发送Security mode complete响应消息时，RNC在SRB2上向UE发送携带第二套完整性保护参数鉴权码的随机消息，若RNC在设定时长内接收到UE针对该随机消息回复的响应消息，则判定UE已经收到第二套完整性保护参数并在下行激活时间点启用第二套完整性保护参数；若RNC在设定时长内没有收到UE对该随机消息回复的响应消息，则判定UE未收到第二套完整性保护参数并继续使用第一套完整性保护参数。

[0078] 下面结合附图对本申请优选的实施方式进行详细说明。

[0079] 参阅图3所示，本申请实施例中，对完整性保护参数的应用方法的具体流程如下：

[0080] 步骤300：在RNC和UE采用第一套完整性保护参数进行交互的过程中，RNC确定UE需要使用第二套完整性保护参数时，通过SRB2发送安全模式请求消息给UE，安全模式请求消息中携带有第二套完整性保护参数在非SRB2上的下行激活时间点。

[0081] 在RNC和UE采用第一套完整性保护参数进行交互的过程中，RNC确定UE需要使用第二套完整性保护参数具体包括两种情况：其一，UE在当前域中所采用的第一套完整性保护参数需要更改；其二，UE在与当前应用域不同的另一域中发起业务。

[0082] 例如，当前UE正在使用CS域的语音业务，RNC采用CS域的完整性保护参数与UE进行交互，在UE发起PS域的业务时，UE同PS域核心网进行鉴权和安全模式过程生成新的完整性保护参数，此时，RNC确定UE需要使用第二套完整性，RNC通过SRB2发送Security mode command消息给UE，该消息中携带有第二套完整性保护参数在非SRB2上的下行激活时间点。

[0083] 步骤310：RNC确定在第一设定时长内未收到UE回复的安全模式响应消息时，在SRB2上向UE发送第一类随机消息，第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码，若RNC确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息，执行步骤320；若RNC确定在第二设定时长内未收到UE针对第一类随机消息回复的响应消息，执行步骤330；

[0084] 正常情况下，在RNC通过SRB2发送Security mode command消息给UE后，UE会回复Security mode complete响应消息给RNC，该响应消息中携带有第二套完整性保护参数在非SRB2上的上行激活时间点。

[0085] 如果RNC在第一设定时长内未收到UE回复的Security mode complete消息，即在空口超时的情况下，RNC在SRB2上向UE发送第一类随机消息，稽核UE是否收到第二套完整性保护参数，第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码。

[0086] 此外，RNC确定在第一设定时长内未收到UE回复的安全模式响应消息时，在第二套完整性保护参数在非SRB2上的下行激活时间点到达之前，可以根据预设的发送次数和发送时间间隔多次发送第一类随机消息。

[0087] 步骤320:RNC确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并在下行激活时间点启用第二套完整性保护参数。

[0088] 由于SRB2可以立即激活第二套完整性保护参数,UE在收到RNC在SRB2上发送第一类随机消息后,如果UE已经获知第二套完整性保护参数那么就可以立即采用第二套完整性保护参数对RNC发送的消息进行鉴权,若鉴权通过,UE向RNC发送针对第一类随机消息的响应消息。

[0089] 因此,若RNC在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则表明UE采用第二套完整性保护参数对RNC发送的第一类随机消息鉴权通过,因此RNC判定UE已接收到第二套完整性保护参数,并在下行激活时间点启用第二套完整性保护参数。

[0090] 在实际应用过程中,具体的包括两种情况:

[0091] 其一,若RNC确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并直接在下行激活时间点启用第二套完整性保护参数;

[0092] 其二,若RNC确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,在下行激活时间点之前,进一步判断UE是否已经获知第二套完整性保护参数在非SRB2上的下行激活时间点。

[0093] 因此,RNC在非SRB2上向UE发送第二类随机消息,第二类随机消息中携带有基于第一套完整性保护参数生成的鉴权码,进一步包括两种情况:

[0094] 其一,若RNC在第三设定时长内接收到UE针对第二类随机消息回复的响应消息时,则判定UE已经获知第二套完整性保护参数在非SRB2上的下行激活时间点,并在下行激活时间点启用第二套完整性保护参数。

[0095] 其二,若RNC在第三设定时长内未收到UE针对第二类随机消息回复的响应消息时,则判定UE已接收到第二套完整性保护参数,并在下行激活时间点启用第二套完整性保护参数。

[0096] 步骤330:RNC确定在第二设定时长内未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并继续使用第一套完整性保护参数。

[0097] 若RNC确定在第二设定时长内未收到UE针对第一类随机消息回复的响应消息,表明UE采用第二套完整性保护参数对RNC发送的第一类随机消息鉴权失败,则判定UE未收到第二套完整性保护参数,并继续使用第一套完整性保护参数。

[0098] 在实际应用过程中,具体的包括两种情况:

[0099] 其一,若RNC确定在第二设定时长内未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并直接继续使用第一套完整性保护参数;

[0100] 其二,若RNC确定在第二设定时长内RNC未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并进一步确认UE正在使用第一套完整性保护参数对RNC的下行消息进行鉴权。

[0101] 因此,RNC在SRB2上向UE发送第二类随机消息,第二类随机消息中携带有基于第一套完整性保护参数生成的鉴权码。若在第四设定时长内接收到UE针对第二类随机消息回复的响应消息时,表明UE使用第一套完整性保护参数对RNC的下行消息鉴权通过,判定UE未收

到第二套完整性保护参数,并继续使用第一套完整性保护参数。

[0102] 此外,当RNC接收到UE在任一SRB上发送的上行消息时,RNC先采用第一套完整性保护参数对该上行消息进行鉴权。

[0103] 如果鉴权未通过,RNC继续采用第二套完整性保护参数对该上行消息进行鉴权。若采用第二套完整性保护参数鉴权通过,确定达到第二套完整性保护参数在任一SRB上的上行激活时间点,并直接删除第一套完整性保护参数,后续使用第二套完整性保护参数。

[0104] 如果鉴权通过,则确定还未达到第二套完整性保护参数在任一SRB上的上行激活时间点。

[0105] 参阅图4所示,以复查COUNTER CHECK消息为例,对完整性保护参数的应用方法进行具体说明,其中,COUNTER CHECK消息具体用来检测任一RB在RNC侧的流量统计结果与UE侧对应RB的流量统计结果是否一致,本实施例中,RNC采用该消息对第二套完整性保护参数进行检查稽核。

[0106] 步骤400:RNC确定在第一设定时长内未收到UE回复的Security mode complete消息时,在SRB2上向UE发送COUNTER CHECK消息并启动定时器。

[0107] 由于此时UE侧并没有建立第二套完整性保护参数的RB,因此RNC在COUNTER CHECK消息中携带一个RB identity并采用第二套完整性保护参数计算鉴权码添加到消息头中,其中,该RB为非SRB和非第一套完整性保护参数使用的RB identity。

[0108] 步骤410:RNC确定在设定的时长内接收到UE回复的COUNTER CHECK RESPONSE消息,则判定UE已接收到第二套完整性保护参数,并在下行激活时间点启用第二套完整性保护参数。

[0109] UE接收到RNC发送的COUNTER CHECK消息,判断COUNTER CHECK消息中携带的RB identity未建立,UE在COUNTER CHECK RESPONSE消息中携带RB identity发送给RNC。在设定时长内,RNC接收到UE回复的COUNTER CHECK RESPONSE消息,则判定UE已接收到第二套完整性保护参数,并在下行激活时间点启用第二套完整性保护参数。

[0110] 另一方面,如果RNC未收到UE回复的COUNTER CHECK RESPONSE消息,且在第二套完整性保护参数下行激活时间点到达之前,此时可以根据预设的发送次数和发送时间间隔,在SRB2上向UE多次发送第一类随机消息。

[0111] 如果超过设定时长RNC仍然没有收到UE的COUNTER CHECK RESPONSE响应消息,表明UE没有收到第二套完整性保护参数并继续使用第一套完整性保护参数。

[0112] RNC为了进一步确认UE仍然采用第一套完整性保护参数,此时RNC采用第一套完整性保护参数计算鉴权码在SRB2上发送COUNTER CHECK消息给UE,如果在设定时长内收到UE的COUNTER CHECK RESPONSE响应消息,表明UE没有收到第二套完整性保护参数,RNC清除保存的第二套完整性保护参数,第二套完整性保护参数的检查稽核过程结束。

[0113] 进一步地,如果RNC收到由UE发送的携带有第二套完整性保护参数鉴权码的COUNTER CHECK RESPONSE响应消息,可以继续确认UE是否已经获知第二套完整性保护参数在非SRB2上的下行激活时间点。参阅图5所示,以身份请求消息(Identity Request)和身份响应消息(Identity Response)为例,对RNC如何进一步确认UE是否已经获知第二套完整性保护参数在非SRB2上的下行激活时间点进行详细说明。

[0114] 由于SRB2可以立即激活第二套完整性保护参数,而SRB0,SRB1,SRB3,SRB4存在上

下行激活时间,这里以SRB3为例进行具体说明。

[0115] 步骤500:RNC在SRB3上向UE发送携带有第一套完整性保护参数鉴权码的Identity Request消息。

[0116] 步骤510:RNC在SRB3上接收到UE发送的携带有第一套完整性保护参数鉴权码的Identity Response消息,确定UE已经获知第二套完整性保护参数在非SRB2上的下行激活时间点。

[0117] 参阅图6所示,本发明实施例中,RNC和UE稽核完整性保护参数的整体流程具体如下:

[0118] 本实施例中,假设在RNC和UE采用CS域完整性保护参数进行交互的过程中,RNC确定UE即将建立PS域业务,需要使用新的PS域完整性保护参数。

[0119] 步骤601:UE发起CS域业务,CS域业务安全模式过程开始进行,RNC在SRB2上发送Security mode command消息并启动第一定时器,该消息携带非SRB2的下行CS域完整性保护参数激活时间点。

[0120] 步骤602:在第一设定时长内,UE在SRB2上回复Security mode complete消息,该消息携带非SRB2的上行CS域完整性保护参数激活时间点,CS域业务安全模式建立成功,RNC与UE在SRB上的交互使用CS域完整性保护参数计算消息的鉴权码。

[0121] 步骤603:UE发起PS域业务,PS域业务安全模式过程开始进行,RNC在SRB2上发送Security mode command消息并启动第一定时器,该消息携带非SRB2的下行PS域完整性保护参数激活时间点。

[0122] 步骤604:RNC超过第一设定时长未收到UE回复的Security mode complete消息。

[0123] 步骤605:RNC在SRB2上向UE发送COUNTER CHECK消息并启动第二定时器,其中,COUNTER CHECK消息中携带非SRB和非CS域的RB identity且消息头中鉴权码采用PS域完整性保护参数计算。若在第二设定时长内,RNC在SRB2上接收到UE回复的COUNTER CHECK RESPONSE消息,执行步骤606;若RNC超过第二设定时长在SRB2上未收到UE回复的COUNTER CHECK RESPONSE消息,执行步骤607。

[0124] 步骤606:在第二设定时长内,RNC在SRB2上接收到UE回复的COUNTER CHECK RESPONSE消息,确认UE已收到PS域的完整性保护参数,继续执行步骤611。

[0125] 在定时器未超过第二设定时长期间,若RNC在SRB2上未接收到UE回复的COUNTER CHECK RESPONSE消息,RNC可按预设的发送次数和发送间隔继续向UE发送COUNTER CHECK消息。

[0126] 步骤607:RNC超过第二设定时长在SRB2上未接收到UE回复的COUNTER CHECK RESPONSE消息,执行步骤608。

[0127] 步骤608:RNC在SRB2上向UE发送COUNTER CHECK消息并启动第四定时器,其中,COUNTER CHECK消息中携带非SRB和CS域的RB且消息头中鉴权码采用CS域完整性保护参数计算。若在第四设定时长内,RNC在SRB2上接收到UE回复的COUNTER CHECK RESPONSE消息,执行步骤609。若RNC超过第四设定时长在SRB2上未收到UE回复的COUNTER CHECK RESPONSE消息,执行步骤610。

[0128] 步骤609:在第四设定时长内,RNC在SRB2上接收到UE回复的COUNTER CHECK RESPONSE消息,确认UE未收到PS域的完整性保护参数,RNC删除PS域的完整性保护参数且释

放PS域连接。

[0129] 步骤610:RNC超过第四设定时长在SRB2上未收到UE回复的COUNTER CHECK RESPONSE消息,流程结束,执行原有UE释放流程。

[0130] 步骤611:RNC在SRB3上向UE发送IDENTITY REQUEST消息并启动第三定时器,且消息头中的鉴权码采用CS域完整性保护参数计算。若在第三设定时长内,RNC在SRB3上接收到UE回复的IDENTITY RESPONSE消息,执行步骤612。若RNC超过第三设定时长在SRB3上未收到UE回复的IDENTITY RESPONSE消息,执行步骤613。

[0131] 步骤612:RNC在SRB3上接收到UE回复的IDENTITY RESPONSE消息,确认UE已经获知PS域完整性保护参数在非SRB2上的下行激活时间点,流程结束。

[0132] 步骤613:RNC超过第三设定时长在SRB3上未收到UE回复的IDENTITY RESPONSE消息,由于SRB2上已确定UE激活PS域的安全模式,RNC在非SRB2上按激活时间点执行正常的完整性检查流程。

[0133] 参阅图7所示,对完整性保护参数应用的装置,具体包括:

[0134] 第一通信单元70,用于在RNC和UE采用第一套完整性保护参数进行交互的过程中,确定UE需要使用第二套完整性保护参数时,通过SRB2发送安全模式请求消息给UE,安全模式请求消息中携带有第二套完整性保护参数在非SRB2上的下行激活时间点;

[0135] 第二通信单元71,用于确定在第一设定时长内未收到UE回复的安全模式响应消息时,在SRB2上向UE发送第一类随机消息,第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码;

[0136] 以及若确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并在下行激活时间点启用第二套完整性保护参数;若确定在第二设定时长内未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并继续使用第一套完整性保护参数。

[0137] 较佳的,确定UE需要使用第二套完整性保护参数时,第一通信单元70具体用于:

[0138] 获知UE在当前域中所采用的第一套完整性保护参数需要更改时,确定UE需要使用第二套完整性保护参数;

[0139] 获知UE在与当前应用域不同的另一域中发起相应业务时,确定UE需要使用第二套完整性保护参数。

[0140] 较佳的,在确定在第一设定时长内未收到UE回复的安全模式响应消息时,在SRB2上向UE发送第一类随机消息,第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码,第二通信单元71具体用于:

[0141] 确定在第一设定时长内未收到UE回复的安全模式响应消息时,在第二套完整性保护参数在非SRB2上的下行激活时间点到达之前,采用预设的发送次数和发送时间间隔,在SRB2上向UE发送第一类随机消息,第一类随机消息中携带有基于第二套完整性保护参数生成的鉴权码。

[0142] 较佳的,若确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并在下行激活时间点启用第二套完整性保护参数,第二通信单元71具体用于:

[0143] 若确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定

UE已接收到第二套完整性保护参数,并直接在下行激活时间点启用第二套完整性保护参数;

[0144] 或者,

[0145] 若确定在第二设定时长内接收到UE针对第一类随机消息回复的响应消息,则判定UE已接收到第二套完整性保护参数,并进一步在下行激活时间点之前,在非SRB2上向UE发送第二类随机消息,第二类随机消息中携带有基于第一套完整性保护参数生成的鉴权码;以及在第三设定时长内接收到UE针对第二类随机消息回复的响应消息时,判定UE已经获知第二套完整性保护参数在非SRB2上的下行激活时间点,并在下行激活时间点启用第二套完整性保护参数。

[0146] 较佳的,若确定在第二设定时长内未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并继续使用第一套完整性保护参数,第二通信单元71具体用于:

[0147] 若确定在第二设定时长内未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并直接继续使用第一套完整性保护参数;

[0148] 或者,

[0149] 若确定在第二设定时长内RNC未收到UE针对第一类随机消息回复的响应消息,则判定UE未收到第二套完整性保护参数,并进一步在SRB2上向UE发送第二类随机消息,第二类随机消息中携带有基于第一套完整性保护参数生成的鉴权码,以及在第四设定时长内接收到UE针对第二类随机消息回复的响应消息时,判定UE未收到第二套完整性保护参数,并继续使用第一套完整性保护参数。

[0150] 较佳的,进一步包括:

[0151] 上行判断单元72,用于当接收到UE在任一SRB上发送的上行消息时,先采用第一套完整性保护参数对上行消息进行鉴权;

[0152] 以及若鉴权未通过,继续采用第二套完整性保护参数对上行消息进行鉴权,若采用第二套完整性保护参数鉴权通过,确定达到第二套完整性保护参数在任一SRB上的上行激活时间点,并直接删除第一套完整性保护参数,后续使用第二套完整性保护参数;若鉴权通过,则确定还未达到所述第二套完整性保护参数在所述任一SRB上的上行激活时间点。

[0153] 综上,本发明提出在多域并发安全模式超时情况发生时不释放UE的策略,RNC在SRB2上发送携带第二套完整性保护参数的鉴权码的下行随机消息,若UE对该随机消息进行响应,说明UE采用采用了第二套完整性保护参数,若UE未对该消息进行响应,则继续使用第一套完整性保护参数,以此来稽核UE和RNC使用的完整性保护参数的一致性,且稽核完整性保护参数的UU口消息的过程不会引起对呼叫流程的影响,有效地避免了CS域语音业务掉话和UE资源挂住的问题。相对于原有的释放UE的策略,避免了UE和RNC丢弃交互的信令消息导致呼叫流程中断,保证了用户的感知,提升了KPI指标。

[0154] 此外,对于有激活时间的SRB下行方向,RNC发送携带携带第一套完整性保护参数鉴权码的随机消息,若收到UE的响应消息,进一步保证了UE已经获知第二套完整性保护参数在非SRB2上的下行激活时间点。对有激活时间点的SRB上行方向,通过在RNC侧存贮的新旧两套核心网域的完整性保护参数尝试计算UE发送的上行消息,在某条消息第二域完整性保护参数计算成功后,说明UE在这个时刻点启动第二套完整性保护参数。

[0155] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0156] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0157] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0158] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0159] 尽管已描述了本发明的优选实施例,但本领域内的技术人员一旦得知了基本创造性概念,则可对这些实施例作出另外的变更和修改。所以,所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0160] 显然,本领域的技术人员可以对本发明实施例进行各种改动和变型而不脱离本发明实施例的精神和范围。这样,倘若本发明实施例的这些修改和变型属于本发明权利要求及其等同技术的范围之内,则本发明也意图包含这些改动和变型在内。

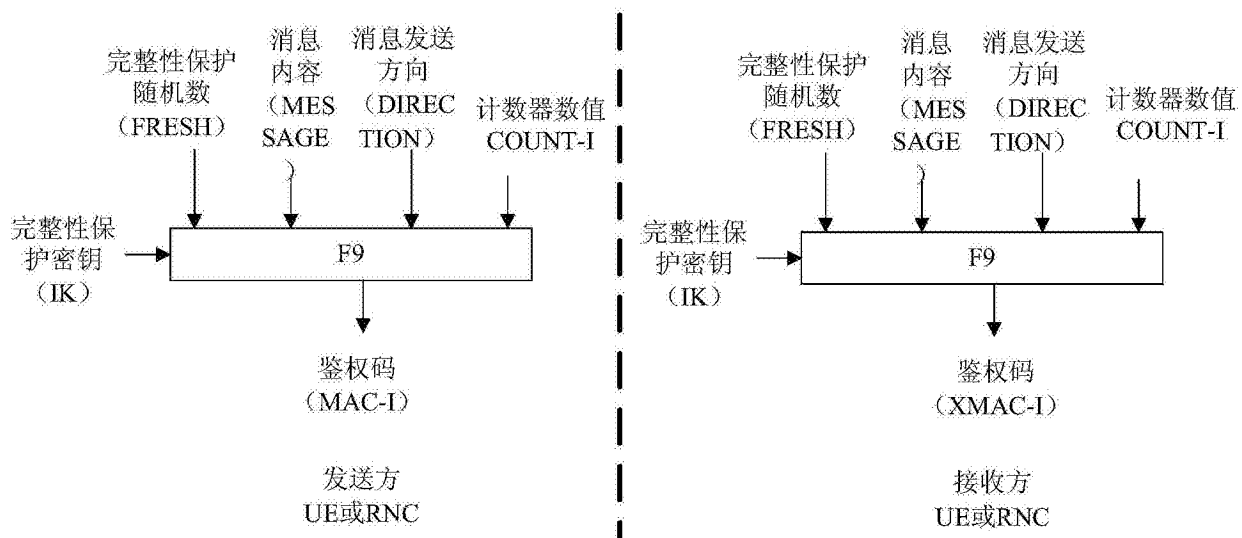


图1

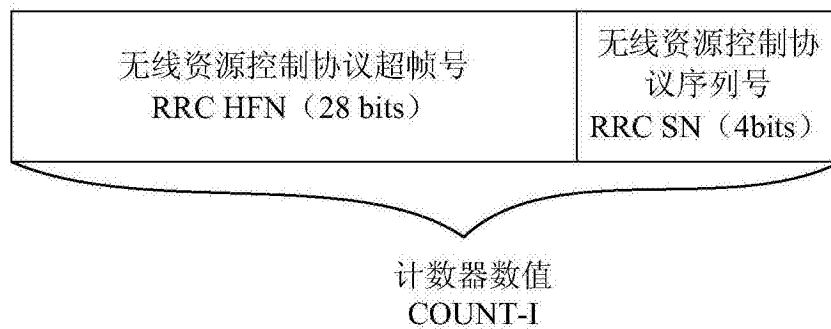


图2

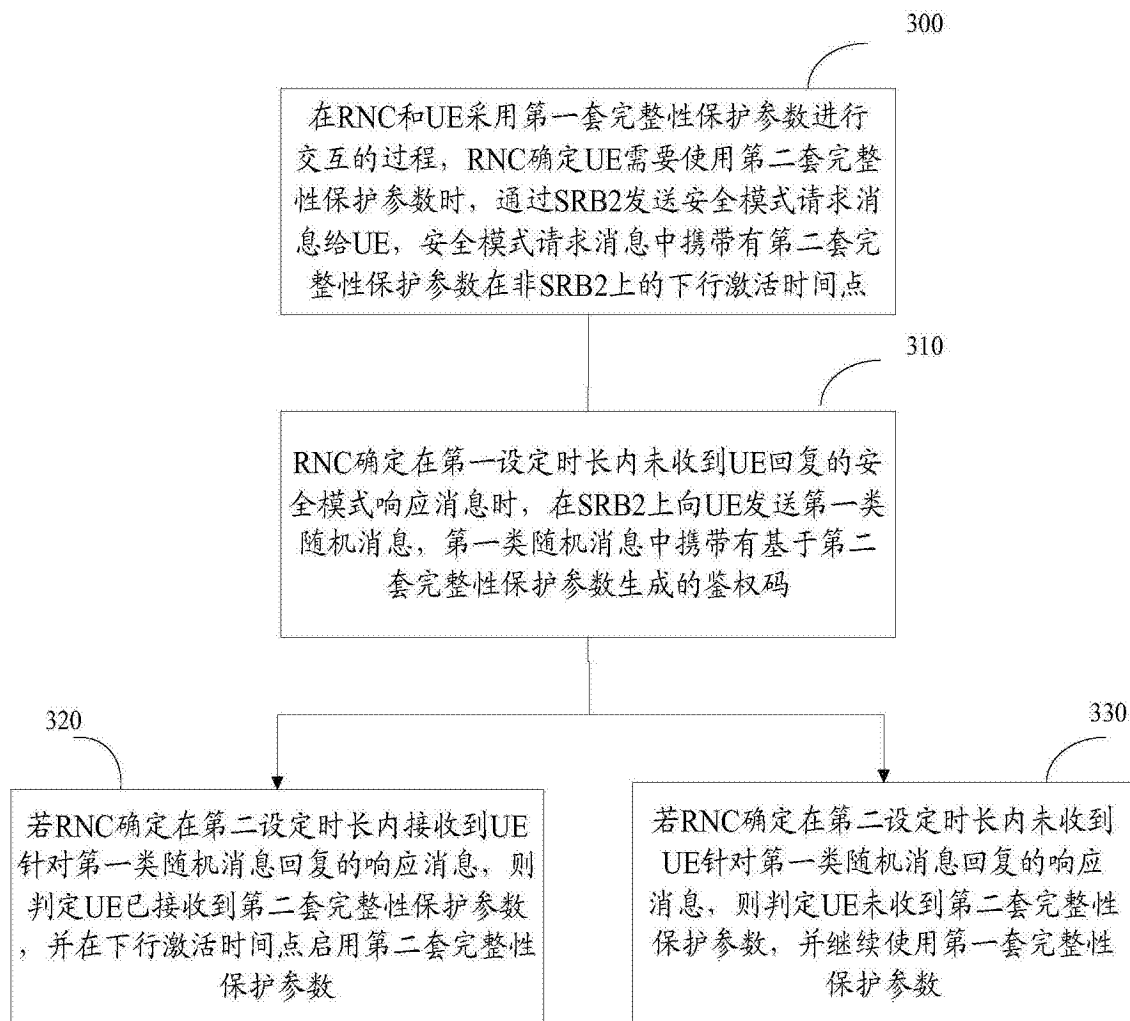


图3



图4

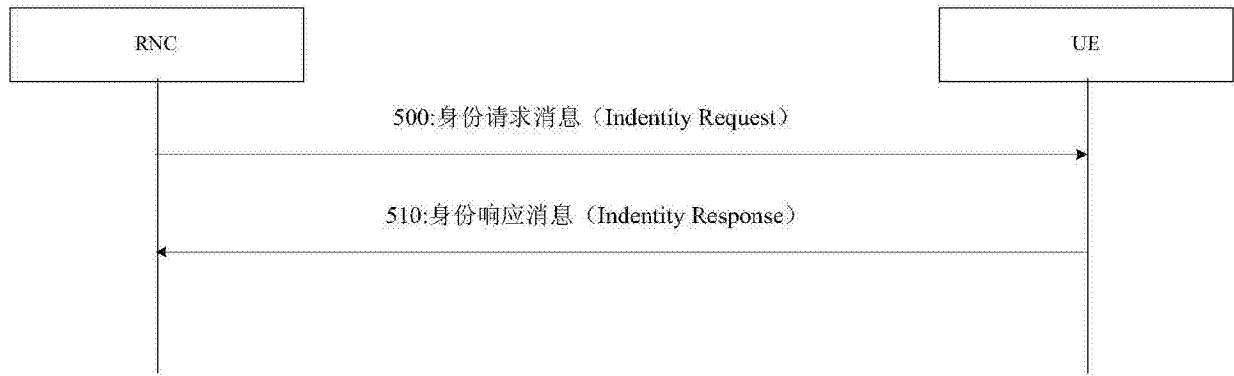


图5

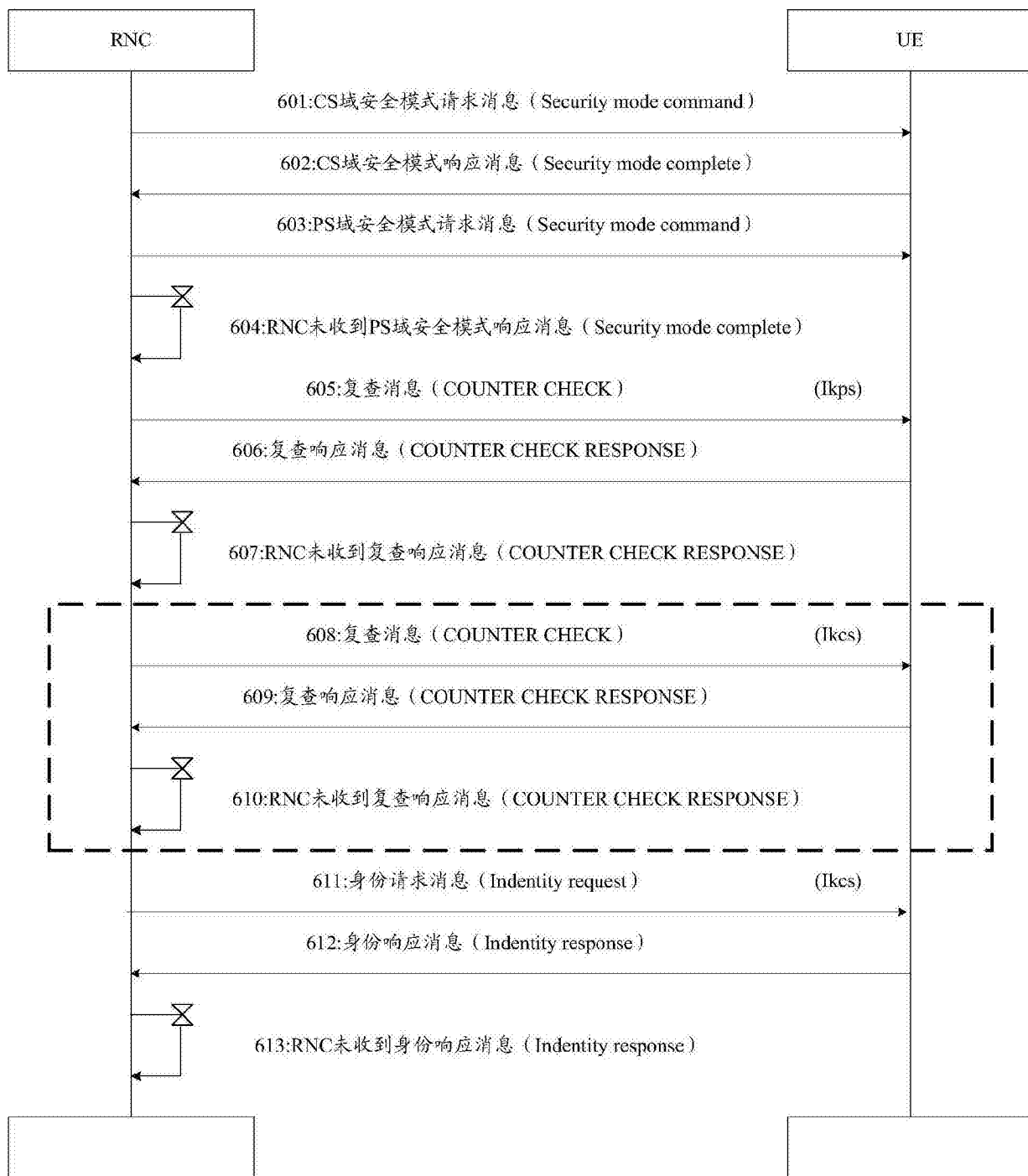


图6

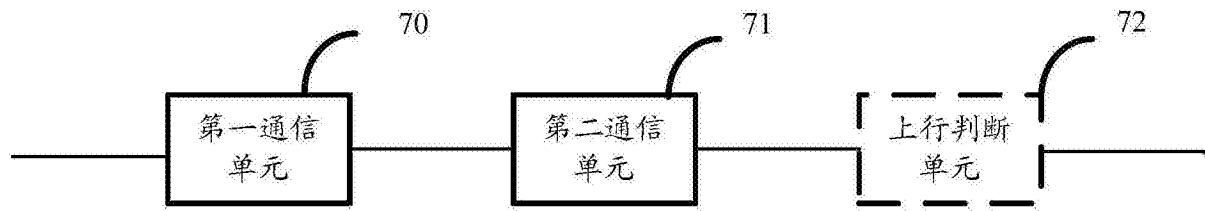


图7