



(12) 发明专利申请

(10) 申请公布号 CN 104469745 A

(43) 申请公布日 2015. 03. 25

(21) 申请号 201410692503. X

(22) 申请日 2014. 11. 26

(71) 申请人 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)

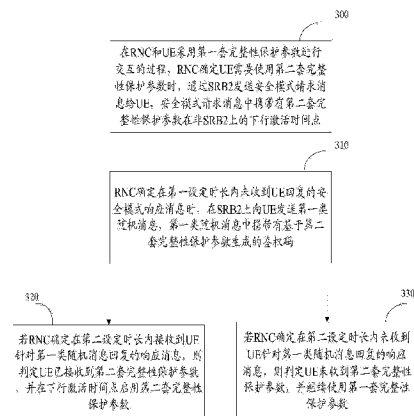
权利要求书3页 说明书14页 附图5页

(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。

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 所述的方法,其特征在于,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。

4. 如权利要求 1、2 或 3 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。

5. 如权利要求 1、2 或 3 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。

6. 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。

7. 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。

8. 如权利要求 7 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。

9. 如权利要求 7 所述的装置,其特征在于,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,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。

10. 如权利要求 7、8 或 9 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。

11. 如权利要求 7、8 或 9 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。

12. 如权利要求 7 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 (Mandatorily Preset, MP)		<p>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.</p> <p>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</p> <p>The value for RB1 shall be ignored if this IE was included in a RRC message sent on RB1.</p> <p>如果这个消息在 SRB1 上发送,这个 IE 可以忽略不被使用</p>

[0015]

信息 (Information Element/Group name)	需要 (Need)	类型和参考 (Type and reference)	语义解释 (Semantics description)
			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 空口处, 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 Indentity 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 Indentity 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

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。

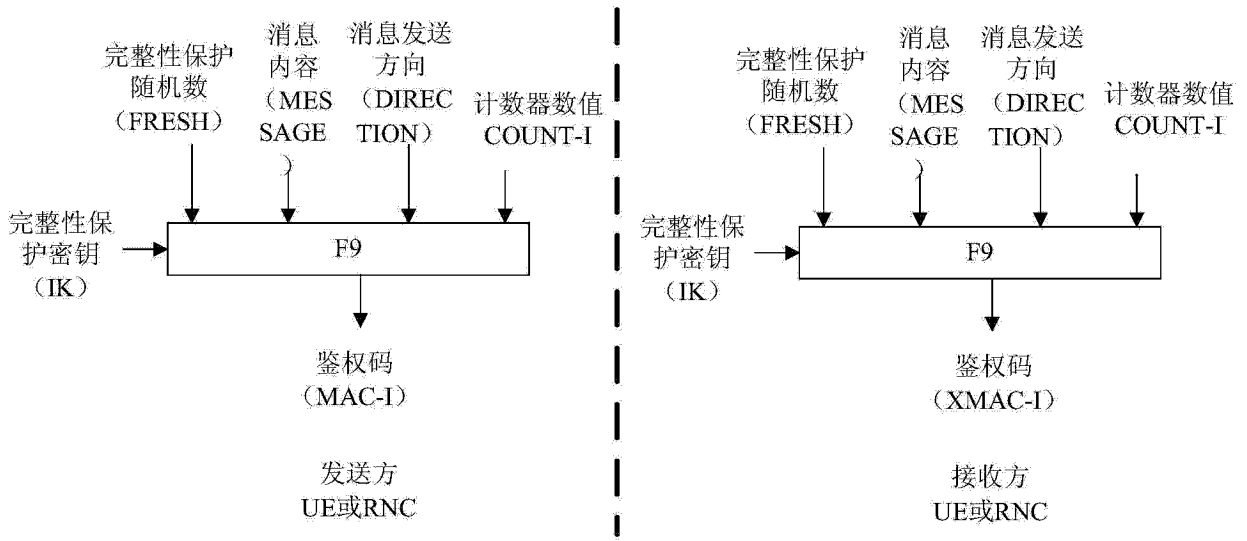


图 1

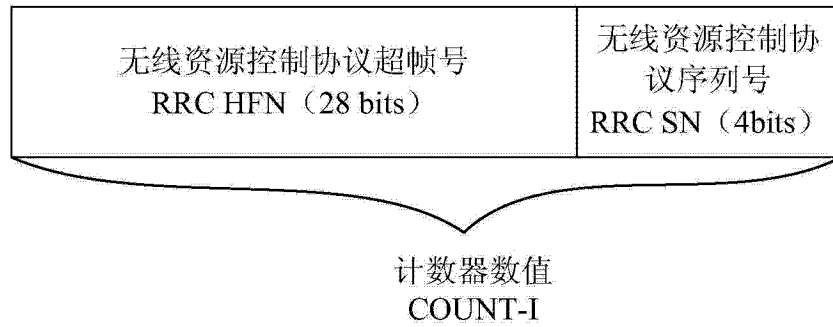


图 2

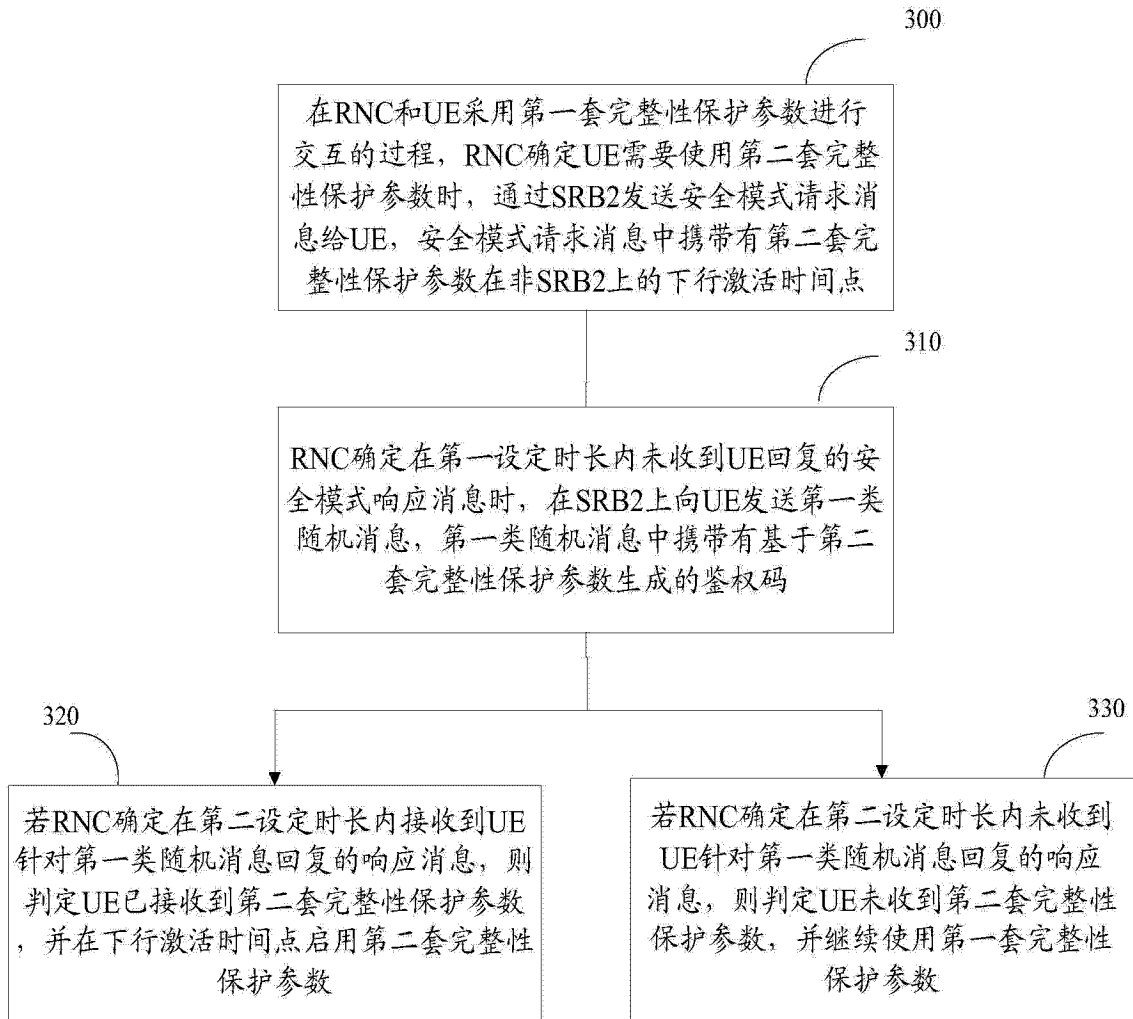


图 3



图 4

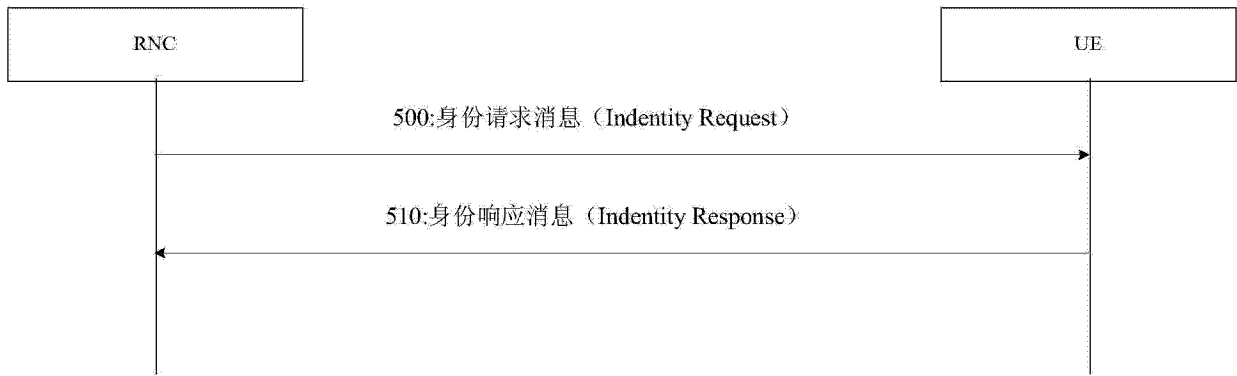


图 5

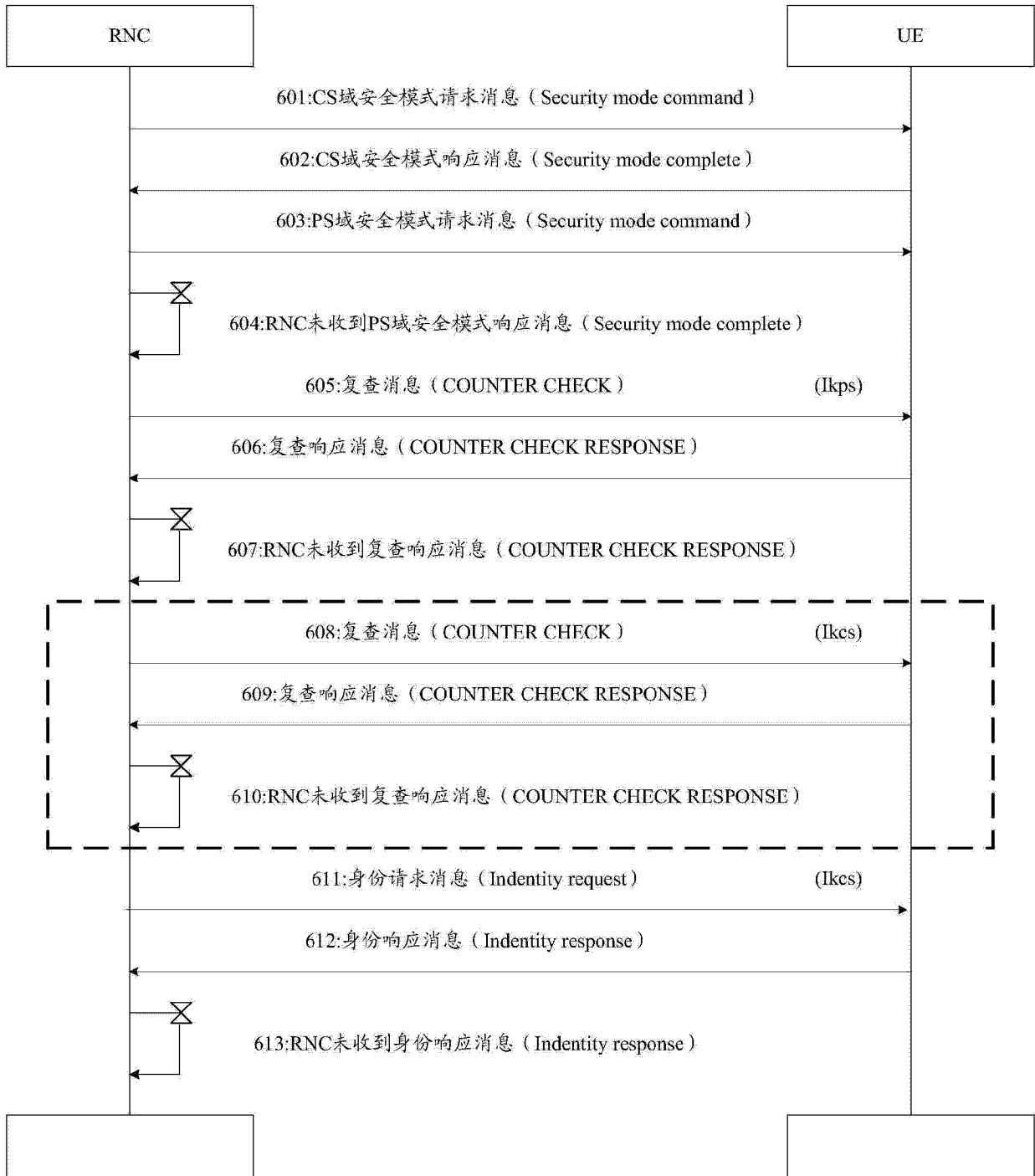


图 6

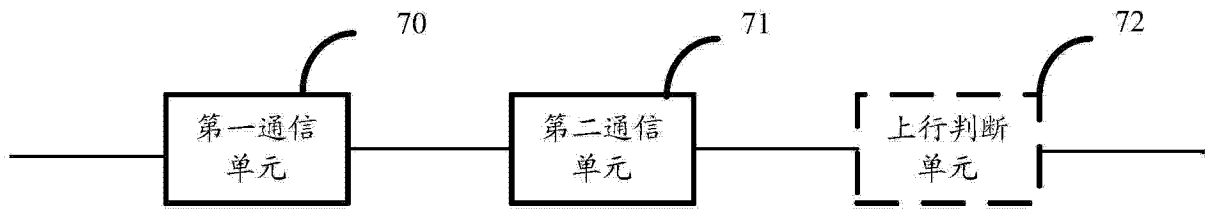


图 7