



(12) 发明专利

(10) 授权公告号 CN 109644354 B

(45) 授权公告日 2021. 10. 26

(21) 申请号 201880002951.9

(72) 发明人 杨宁

(22) 申请日 2018.03.20

(74) 专利代理机构 北京派特恩知识产权代理有限公司 11270

(65) 同一申请的已公布的文献号
申请公布号 CN 109644354 A

代理人 陈宇 张颖玲

(43) 申请公布日 2019.04.16

(51) Int.Cl.

(85) PCT国际申请进入国家阶段日
2019.01.28

H04W 24/02 (2009.01)

H04W 76/19 (2018.01)

H04W 76/27 (2018.01)

(86) PCT国际申请的申请数据
PCT/CN2018/079684 2018.03.20

(56) 对比文件

CN 101848536 A, 2010.09.29

CN 102487507 A, 2012.06.06

CN 102238542 A, 2011.11.09

US 2011077010 A1, 2011.03.31

(87) PCT国际申请的公布数据
W02019/178755 ZH 2019.09.26

(73) 专利权人 OPPO广东移动通信有限公司
地址 523860 广东省东莞市长安镇乌沙海
滨路18号

审查员 张枫

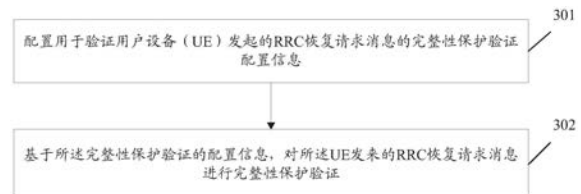
权利要求书4页 说明书11页 附图4页

(54) 发明名称

一种完整性验证方法、网络设备、UE及计算机存储介质

(57) 摘要

本发明公开了一种完整性验证方法、网络设备、用户设备(UE)及计算机存储介质,其中方法包括:配置用于验证用户设备UE发起的RRC恢复请求消息的完整性保护验证配置信息;基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证。



1. 一种完整性验证方法,应用于第一网络设备,所述方法包括:

在用户设备UE进入非激活状态之前,接收服务UE的原服务基站发送的用于验证所述UE发起的RRC恢复请求消息的完整性保护验证配置信息;

基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证;

所述完整性保护验证配置信息包括:所述第一网络设备管理的目标小区中频域范围包含的至少一个同步信息块SSB所对应的SSB的标识信息;

所述第一网络设备为当前为UE提供服务的基站。

2. 根据权利要求1所述的方法,其中,所述完整性保护验证配置信息,包括以下至少之一:至少一个短MAC-I、UE上下文标识I-RNTI。

3. 根据权利要求2所述的方法,其中,

所述至少一个短MAC-I,与所述至少一个SSB的标识信息相对应。

4. 根据权利要求1所述的方法,其中,所述完整性保护验证配置信息,包括以下至少之一:至少一个密钥、UE上下文标识I-RNTI、安全算法、原服务基站的PCI、原服务基站的C-RNTI。

5. 根据权利要求4所述的方法,其中,

所述至少一个密钥,与所述至少一个SSB的标识信息相对应。

6. 根据权利要求1-5任一项所述的方法,其中,基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证,还包括:

接收所述UE发来的RRC恢复请求消息;

当存在所述UE对应的完整性保护验证配置信息时,基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证;

当不存在所述UE对应的完整性保护验证配置信息时,寻址所述UE对应的锚基站,使得所述锚基站对RRC恢复请求消息进行完整性保护验证。

7. 根据权利要求1-3任一项所述的方法,其中,所述对所述UE发来的RRC恢复请求消息进行完整性保护验证,还包括:

根据所述RRC恢复请求消息中所携带的UE标识信息,寻找存储的短MAC-I;

基于所述短MAC-I进行完整性保护验证;

当验证成功时,为所述UE寻址目标网络设备,进行UE上下文获取;

当验证失败时,拒绝所述UE。

8. 根据权利要求1、4或5任一项所述的方法,其中,所述对所述UE发来的RRC恢复请求消息进行完整性保护验证,还包括:

根据所述RRC恢复请求消息中所携带的标识信息,寻找存储的密钥;

至少基于所述密钥和安全算法计算得到短MAC-I;

基于计算得到的所述短MAC-I进行完整性保护验证;

当验证成功时,为所述UE寻址目标网络设备,进行UE上下文获取;

当验证失败时,拒绝所述UE。

9. 一种完整性验证方法,应用于第二网络设备,所述方法包括:

当作为UE的原服务基站、且保存所述UE的上下文时,在释放所述UE进入非激活状态之

前,向当前为所述UE服务的基站发送关于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息;

所述完整性保护验证配置信息包括:第一网络设备管理的目标小区中频域范围包含的至少一个同步信息块SSB所对应的SSB的标识信息;

所述第一网络设备为当前为UE提供服务的基站。

10.根据权利要求9所述的方法,其中,所述第一网络设备及所述第一网络设备管理的小区,为RAN通知区域内的全部基站及所述全部基站管理的小区中的至少部分基站及小区中之一的基站及小区。

11.根据权利要求10所述的方法,其中,所述完整性保护验证配置信息,包括以下至少之一:至少一个短MAC-I、UE上下文标识I-RNTI。

12.根据权利要求11所述的方法,其中,

所述至少一个短MAC-I,与所述至少一个SSB的标识信息相对应。

13.根据权利要求10所述的方法,其中,所述完整性保护验证配置信息,包括以下至少之一:至少一个密钥、UE上下文标识I-RNTI、安全算法、原服务基站的PCI、原服务基站的C-RNTI。

14.根据权利要求13所述的方法,其中

所述至少一个密钥,与所述至少一个SSB的标识信息相对应。

15.根据权利要求9-14任一项所述的方法,向第一网络设备发送关于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息之前,所述方法还包括:

根据邻区的频域SSB配置信息计算至少一个SSB对应的密钥,以及对应的短MAC-I;

或者

根据邻区的频域SSB配置信息计算至少一个SSB对应的密钥。

16.一种第一网络设备,包括:

第一通信单元,在用户设备UE进入非激活状态之前,接收服务用户设备UE的原服务基站发送的用于验证所述UE发起的RRC恢复请求消息的完整性保护验证配置信息;

第一处理单元,基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证;

所述完整性保护验证配置信息包括:所述第一网络设备管理的目标小区中频域范围包含的至少一个同步信息块SSB所对应的SSB的标识信息;

所述第一网络设备为当前为UE提供服务的基站。

17.根据权利要求16所述的第一网络设备,其中,所述完整性保护验证配置信息,包括以下至少之一:至少一个短MAC-I、UE上下文标识I-RNTI。

18.根据权利要求17所述的第一网络设备,其中,

所述至少一个短MAC-I,与所述至少一个SSB的标识信息相对应。

19.根据权利要求16所述的第一网络设备,其中,所述完整性保护验证配置信息,包括以下至少之一:至少一个密钥、UE上下文标识I-RNTI、安全算法、原服务基站的PCI、原服务基站的C-RNTI。

20.根据权利要求19所述的第一网络设备,其中,

所述至少一个密钥,与所述至少一个SSB的标识信息相对应。

21. 根据权利要求16-20任一项所述的第一网络设备,其中,所述第一通信单元,接收所述UE发来的RRC恢复请求消息;

第一处理单元,当存在所述UE对应的完整性保护验证配置信息时,基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证;

当不存在所述UE对应的完整性保护验证配置信息时,寻址所述UE对应的锚基站,使得所述锚基站对RRC恢复请求消息进行完整性保护验证。

22. 根据权利要求16-18任一项所述的第一网络设备,其中,所述第一处理单元,根据所述RRC恢复请求消息中所携带的UE标识信息,寻找存储的短MAC-I;基于所述短MAC-I进行完整性保护验证;当验证成功时,为所述UE寻址目标网络设备,进行UE上下文获取;当验证失败时,拒绝所述UE。

23. 根据权利要求16、19或20任一项所述的第一网络设备,其中,所述第一处理单元,根据所述RRC恢复请求消息中所携带的标识信息,寻找存储的密钥;至少基于所述密钥和安全算法计算得到短MAC-I;基于计算得到的所述短MAC-I进行完整性保护验证;当验证成功时,为所述UE寻址目标网络设备,进行UE上下文获取;当验证失败时,拒绝所述UE。

24. 一种第二网络设备,包括:

第二处理单元,当所述第二网络设备作为UE的原服务基站、且保存所述UE的上下文时,在释放所述UE进入非激活状态之前,通过第二通信单元向当前为所述UE服务的基站发送关于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息;

第二通信单元,向第一网络设备发送所述完整性保护验证配置信息;

所述完整性保护验证配置信息包括:所述第一网络设备管理的目标小区中频域范围包含的至少一个同步信息块SSB所对应的SSB的标识信息;

所述第一网络设备为当前为UE提供服务的基站。

25. 根据权利要求24所述的第二网络设备,其中,所述第一网络设备及所述第一网络设备管理的小区,为RAN通知区域内的全部基站及所述全部基站管理的小区中的至少部分基站及小区中之一的基站及小区。

26. 根据权利要求25所述的第二网络设备,其中,所述完整性保护验证配置信息,包括以下至少之一:至少一个短MAC-I、UE上下文标识I-RNTI。

27. 根据权利要求26所述的第二网络设备,其中,

所述至少一个短MAC-I,与所述至少一个SSB的标识信息相对应。

28. 根据权利要求25所述的第二网络设备,其中,所述完整性保护验证配置信息,包括以下至少之一:至少一个密钥、UE上下文标识I-RNTI、安全算法、原服务基站的PCI、原服务基站的C-RNTI。

29. 根据权利要求28所述的第二网络设备,其中,

所述至少一个密钥,与所述至少一个SSB的标识信息相对应。

30. 根据权利要求24-29任一项所述的第二网络设备,第二处理单元,根据邻区的频域SSB配置信息计算至少一个SSB对应的密钥,以及对应的短MAC-I;

或者

根据邻区的频域SSB配置信息计算至少一个SSB对应的密钥。

31. 一种网络设备,包括:处理器和用于存储能够在处理器上运行的计算机程序的存储

器，

其中，所述处理器用于运行所述计算机程序时，执行权利要求1-15任一项所述方法的步骤。

32. 一种计算机存储介质，所述计算机存储介质存储有计算机可执行指令，所述计算机可执行指令被执行时实现权利要求1-15任一项所述的方法步骤。

一种完整性验证方法、网络设备、UE及计算机存储介质

技术领域

[0001] 本发明涉及信息处理技术领域,尤其涉及一种完整性验证方法、网络设备、用户设备(UE)及计算机存储介质。

背景技术

[0002] 当UE处于RRC_INACTIVE状态,网络侧会给UE配置RAN的寻呼区域,当UE在该寻呼区域内移动时不用通知网络侧,遵循idle下移动性行为,即小区选择重选原则。当UE移动出RAN配置的寻呼区域时,会触发UE恢复RRC连接并重新获取RAN配置的寻呼区域。

[0003] 现有技术中,RRC Resume request恢复请求消息(MSG3)的完整性保护验证是在原基站来执行的,比如图1所示,即服务基站将收到的RRC Resume request消息中的ShortMAC-I和UE上下文标识信息发给原基站,原基站进行完整性保护验证,如果完整性保护验证通过,则原基站转发该UE的AS上下文给服务基站,使得服务基站可以恢复UE的上下文进而恢复RRC连接。但是如果RRC Resume request消息的完整性保护验证失败,则原基站不发送安全上下文,但是Xn接口的信令还是要存在的。对于如果存在假UE尝试破坏网络侧,不停的发送RRC Resume request消息给基站,则基站会不停的尝试获取该假UE的安全上下文,使得网络消耗过多资源处理无意义的处理,甚至导致网络瘫痪。

发明内容

[0004] 为解决上述技术问题,本发明实施例提供了一种完整性验证方法、网络设备、用户设备(UE)及计算机存储介质。

[0005] 本发明实施例提供了一种完整性验证方法,应用于第一网络设备,所述方法包括:

[0006] 配置用于验证用户设备UE发起的RRC恢复请求消息的完整性保护验证配置信息;

[0007] 基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证。

[0008] 本发明实施例提供一种完整性验证方法,应用于第二网络设备,所述方法包括:

[0009] 当作为UE的原服务基站、且保存所述UE的上下文时,在释放所述UE进入非激活状态之前,向第一网络设备发送关于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息。

[0010] 本发明实施例提供一种完整性验证方法,应用于UE,所述方法包括:

[0011] 向第一网络设备发送RRC恢复请求消息。

[0012] 本发明实施例提供了一种第一网络设备,包括:

[0013] 第一通信单元,配置用于验证用户设备UE发起的RRC恢复请求消息的完整性保护验证配置信息;

[0014] 第一处理单元,基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证。

[0015] 本发明实施例提供一种第二网络设备,包括:

[0016] 第二处理单元,当作为UE的原服务基站、且保存所述UE的上下文时,在释放所述UE进入非激活状态之前,通过第二通信单元向第一网络设备发送关于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息;

[0017] 第二通信单元,向第一网络设备发送所述完整性保护验证配置信息。

[0018] 本发明实施例提供一种UE,包括:

[0019] 第三通信单元,向第一网络设备发送RRC恢复请求消息。

[0020] 本发明实施例提供的一种网络设备,包括:处理器和用于存储能够在处理器上运行的计算机程序的存储器,

[0021] 其中,所述处理器用于运行所述计算机程序时,执行前述方法的步骤。

[0022] 本发明实施例提供的一种UE,包括:处理器和用于存储能够在处理器上运行的计算机程序的存储器,

[0023] 其中,所述处理器用于运行所述计算机程序时,执行前述方法的步骤。

[0024] 本发明实施例提供的一种计算机存储介质,所述计算机存储介质存储有计算机可执行指令,所述计算机可执行指令被执行时实现前述方法步骤。

[0025] 本发明实施例的技术方案,就能够通过预先配置RRC连接恢复请求消息完整性保护验证的配置信息,使得第一网络设备可以进行完整性保护验证;如此,就能够降低第一网络设备尤其是服务基站和锚基站之间进行信令交互所带来的数据传输,特别是能够避免系统中存在假UE攻击网络的场景。

附图说明

[0026] 图1为RRC恢复连接的处理流程示意图;

[0027] 图2为一种网络结构示意图;

[0028] 图3为本发明实施例完整性验证方法流程示意图1;

[0029] 图4为本发明实施例完整性验证方法流程示意图2;

[0030] 图5为本发明实施例完整性验证方法流程示意图3;

[0031] 图6为本发明实施例完整性验证方法流程示意图4;

[0032] 图7为本发明实施例第一网络设备组成结构示意图;

[0033] 图8为本发明实施例第二网络设备组成结构示意图;

[0034] 图9为本发明实施例UE组成结构示意图;

[0035] 图10为本发明实施例的一种硬件架构示意图。

具体实施方式

[0036] 为了能够更加详尽地了解本发明实施例的特点与技术内容,下面结合附图对本发明实施例的实现进行详细阐述,所附附图仅供参考说明之用,并非用来限定本发明实施例。

[0037] 参考图2描述其中根据本发明的UE与网络设备进行通信的通信系统。

[0038] 这样的通信系统可以使用不同的空中接口和/或物理层。例如,由通信系统使用的空中接口包括例如频分多址(FDMA)、时分多址(TDMA)、码分多址(CDMA)和通用移动通信系统(UMTS)(特别地,长期演进(LTE))、全球移动通信系统(GSM)等等。作为非限制性示例,下面的描述涉及CDMA通信系统,但是这样的教导同样适用于其它类型的系统。

[0039] 参考图2,CDMA无线通信系统可以包括多个UE100、多个网络设备,比如图中的基站(BS) 270、基站控制器(BSC) 275和移动交换中心(MSC) 280等。MSC280被构造为与公共电话交换网络(PSTN) 290形成接口。MSC280还被构造为与可以经由回程线路耦接到基站270的BSC275形成接口。回程线路可以根据若干已知的接口中的任一种来构造,所述接口包括例如E1/T1、ATM、IP、PPP、帧中继、HDSL、ADSL或xDSL。将理解的是,如图2中所示的系统可以包括多个BSC275。

[0040] 在图2中,还描绘了多个卫星300,但是理解的是,可以利用任何数目的卫星获得有用的定位信息。作为无线通信系统的一个典型操作,BS270接收来自各种UE100的反向链路信号。UE100通常参与通话、消息收发和其它类型的通信。特定基站270接收的每个反向链路信号被在特定BS270内进行处理。获得的数据被转发给相关的BSC275。BSC提供通话资源分配和包括BS270之间的软切换过程的协调的移动管理功能。BSC275还将接收到的数据路由到MSC280,其提供用于与PSTN290形成接口的额外的路由服务。类似地,PSTN290与MSC280形成接口,MSC与BSC275形成接口,并且BSC275相应地控制BS270以将正向链路信号发送到UE100。

[0041] 实施例一、

[0042] 本发明实施例提供了一种完整性验证方法,应用于第一网络设备,如图3所示,包括:

[0043] 步骤301:配置用于验证用户设备(UE)发起的RRC恢复请求消息的完整性保护验证配置信息;

[0044] 步骤302:基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证。

[0045] 本实施例中所述第一网络设备,可以为当前为UE提供服务的基站。

[0046] 本实施例可以存在以下两种处理场景,分别说明如下:

[0047] 场景1、

[0048] 所述第一网络设备还会预先获取到UE之前的一个服务基站(第二网络设备)发来的完整性保护验证配置信息,具体包括:

[0049] 接收第二网络设备发来的关于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息;其中,所述第二网络设备为服务所述UE的原服务基站,且当所述第二网络设备在释放所述UE进入非激活态前,向所述第一网络设备发送用于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息。

[0050] 在第二网络设备侧还会进行以下处理:在发送配置信息之前(也就是说,向邻基站发送关于验证UE发起的RRC Resume request消息的完整性保护验证配置信息之前),所述第二网络设备根据邻区的频域SSB配置信息计算对应的 K_{gNB} *(密钥),以及对应的shortMAC-I。

[0051] 所述完整性保护验证配置信息,包括以下至少之一:至少一个短MAC-I、UE上下文标识I-RNTI。

[0052] 如果目标小区是一个频域范围包含多个SSBs的wideband carrier。则所述完整性保护验证配置信息包括每个SSB对应的ShortMAC-I以及对应的SSB标识信息。

[0053] 也就是说,当存在多个SSB的时候,所述完整性保护验证配置信息,还包括:所述第

一网络设备管理的目标小区中频域范围包含的至少一个SSB所对应的SSB的标识信息;并且,所述至少一个短MAC-I,与所述至少一个SSB的标识信息相对应。

[0054] 前述网络侧完成配置处理,然后所述UE会进行RRC恢复请求,在向目标发起RRC Resume request消息之前,UE根据当前SSB的ARFCN和PCI信息更新密钥并计算ShortMAC-I。

[0055] 相应的,所述第一网络设备侧基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证,还包括:

[0056] 接收所述UE发来的RRC恢复请求消息;

[0057] 当存在所述UE对应的完整性保护验证配置信息时,基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证;

[0058] 或者,

[0059] 当不存在所述UE对应的完整性保护验证配置信息时,寻址所述UE对应的锚基站,使得所述锚基站执行对RRC恢复请求消息进行完整性保护验证。

[0060] 也就是说,UE向某个基站发起RRC Resume request消息,如果该基站存在该UE对应的完整性保护验证配置信息,则执行RRC Resume request消息的完整性保护验证。否则寻址anchor gNB,让anchor gNB执行RRC Resume request消息的完整性保护验证。

[0061] 根据所述RRC恢复请求消息中所携带的UE标识信息,寻找存储的短MAC-I;基于所述短MAC-I进行完整性保护验证;当验证成功时,为所述UE寻址目标网络设备,进行所述UE上下文获取;当验证失败时,拒绝所述UE。

[0062] 也就是说,如果当前基站可以执行RRC Resume request消息的完整性保护验证,如果验证成功则寻址目标基站,进行UE上下文索取,否则直接拒绝UE。

[0063] 本场景可以进一步参见图4、5,其中图4中示意出,锚基站可以为UE连接的源基站,T-gNB可以理解为UE当前的服务基站;锚基站与服务基站之间通过Xn接口获取完整性保护验证配置信息;然后,锚基站向UE发送RRC连接释放消息,或者RRC暂停消息;UE驻留在目标gNB,保留RRC连接。UE至少基于C-RNTI、源PCI以及目标小区标识等信息计算短MAC-I;UE向目标基站发送RRC连接恢复请求消息,其中至少包括(ShortMAC-I and I-RNTI);目标基站基于RRC连接恢复请求消息中的I-RNTI查找到短MAC-I,然后目标基站根据短MAC-I进行完整性校验保护;如果当前基站也就是目标基站可以执行RRC Resume request消息的完整性保护验证,如果验证成功则寻址目标基站,进行UE上下文索取,否则直接拒绝UE。

[0064] 图5中示意出,1、锚基站(也就是本实施例中的第二网络设备)首先计算得到密钥,并且每一个SSB对应一个密钥,然后确定ARFCN以及PCI;基于每一个SSB对应的KRRCint,以及旧安全算法计算得到每一个SSB对应的ShortMAC-I,也就是图中所示的ShortMAC-I-1、ShortMAC-I-2、ShortMAC-I-3;

[0065] 2、锚基站向目标基站(也就是本实施例中的第一网络设备),发送每一个SSB对应的密钥、ShortMAC-I以及I-RNTI;

[0066] 3、在UE发送RRC恢复请求之前,UE可以确定其驻留小区为SSB2;并且计算得到密钥KgNB*,并从SSB2中提取ARFCN以及PCI,然后获取KRRCint,基于获取到的信息以及旧安全算法计算得到ShortMAC-I;

[0067] 4、目标基站在收到UE发来的RRC恢复请求的时候,基于RRC恢复请求中的I-RNTI找到对应的ShortMAC-I,然后进行安全性校验。

[0068] 场景2、

[0069] 所述第一网络设备还会预先获取到UE之前的一个服务基站(第二网络设备)发来的完整性保护验证配置信息,具体包括:

[0070] 接收第二网络设备发来的关于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息;其中,所述第二网络设备为服务所述UE的原服务基站,且当所述第二网络设备在释放所述UE进入非激活态前,向所述第一网络设备发送用于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息。

[0071] 在第二网络设备侧还会进行以下处理:在发送配置信息之前(也就是说,向邻基站发送关于验证UE发起的RRC Resume request消息的完整性保护验证配置信息之前),所述第二网络设备根据邻区的频域SSB配置信息计算对应的KgNB*。

[0072] 所述完整性保护验证配置信息,包括以下至少之一:至少一个密钥、UE上下文标识I-RNTI、安全算法、原服务基站的PCI、原服务基站的C-RNTI。

[0073] 如果包括有多个SSB的时候,还可以包括:

[0074] 所述第一网络设备管理的目标小区中频域范围包含的至少一个SSB所对应的SSB的标识信息;并且,所述至少一个密钥,与所述至少一个SSB的标识信息相对应。

[0075] 所述完整性保护验证配置信息包括KgNB*,UE上下文标识I-RNTI,存储的安全算法,原侧的PCI和C-RNTI。如果目标小区是一个频域范围包含多个SSBs的wideband carrier。则所述完整性保护验证配置信息包括每个SSB对应的KgNB*以及对应的SSB标识信息。

[0076] 前述网络侧完成配置处理,然后所述UE会进行RRC恢复请求,在向目标发起RRC Resume request消息之前,UE根据当前SSB的ARFCN和PCI信息更新密钥并计算ShortMAC-I。

[0077] 相应的,所述第一网络设备侧基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证,还包括:

[0078] 接收所述UE发来的RRC恢复请求消息;

[0079] 当存在所述UE对应的完整性保护验证配置信息时,基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证;

[0080] 或者,

[0081] 当不存在所述UE对应的完整性保护验证配置信息时,寻址所述UE对应的锚基站,使得所述锚基站执行对RRC恢复请求消息进行完整性保护验证。

[0082] 也就是说,UE向某个基站发起RRC Resume request消息,如果该基站存在该UE对应的完整性保护验证配置信息,则执行RRC Resume request消息的完整性保护验证。否则寻址anchor gNB,让anchor gNB执行RRC Resume request消息的完整性保护验证。

[0083] 根据所述RRC恢复请求消息中所携带的标识信息,寻找存储的密钥;至少基于所述密钥和所述安全算法计算得到短MAC-I;基于计算得到的所述短MAC-I进行完整性保护验证;当验证成功时,为所述UE寻址目标网络设备,进行所述UE上下文获取;当验证失败时,拒绝所述UE。

[0084] 也就是说,目标基站根据RRC resume request消息所携带的信息,寻找存储的KgNB*,然后计算shortMAC-I。如果当前基站可以执行RRC Resume request消息的完整性保护验证,如果验证成功则寻址目标基站,进行UE上下文索取,否则直接拒绝UE。

[0085] 本场景可以进一步参见图4、6,其中图4中示意出,锚基站可以为UE连接的源基站,T-gNB可以理解为UE当前的服务基站;锚基站与服务基站之间通过Xn接口获取完整性保护验证配置信息;然后,锚基站向UE发送RRC连接释放消息,或者RRC暂停消息;UE驻留在目标gNB,保留RRC连接。UE至少基于C-RNTI、源PCI以及目标小区标识等信息计算短MAC-I;UE向目标基站发送RRC连接恢复请求消息,其中至少包括(ShortMAC-I and I-RNTI);目标基站基于RRC连接恢复请求消息中的I-RNTI查找到短MAC-I,然后目标基站根据短MAC-I进行完整性校验保护;如果当前基站也就是目标基站可以执行RRC Resume request消息的完整性保护验证,如果验证成功则寻址目标基站,进行UE上下文索取,否则直接拒绝UE。

[0086] 图6中示意出,1、锚基站(也就是本实施例中的第二网络设备)首先计算得到密钥,并且每一个SSB对应一个密钥、ARFCN以及PCI;

[0087] 2、锚基站向目标基站(也就是本实施例中的第一网络设备),发送每一个SSB对应的密钥、I-RNTI、源PCI和源C-RNTI、以及安全算法;

[0088] 3、在UE发送RRC恢复请求之前,UE可以确定其驻留小区为SSB2;并且计算得到密钥KgNB*,并从SSB2中提取ARFCN以及PCI,然后获取KRRCint,基于获取到的信息以及旧安全算法计算得到ShortMAC-I;

[0089] 4、目标基站在收到UE发来的RRC恢复请求的时候,先计算得到ShortMAC-I,然后进行安全性校验。

[0090] 可见,通过采用上述方案,就能够通过预先配置RRC连接恢复请求消息完整性保护验证的配置信息,使得第一网络设备可以进行完整性保护验证;如此,就能够降低第一网络设备尤其是服务基站和锚基站之间进行信令交互所带来的数据传输,特别是能够避免系统中存在假UE攻击网络的场景。

[0091] 实施例二、

[0092] 本发明实施例提供了一种完整性验证方法,应用于第二网络设备,包括:当作为UE的原服务基站、且保存所述UE的上下文时,在释放所述UE进入非激活状态之前,向第一网络设备发送关于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息。

[0093] 本实施例中所述第二网络设备,可以为当前为UE对应的原服务基站。其中,所述第一网络设备及小区,为RAN通知区域内的全部基站及其小区中的至少部分基站及小区中之一的基站及小区。或者可以理解为第一网络设备为UE的当前服务基站;该第一网络设备管理的某一个小区为UE的目标小区。

[0094] 本实施例也可以存在以下两种处理场景,分别说明如下:

[0095] 场景1、

[0096] 在发送配置信息之前(也就是说,向邻基站发送关于验证UE发起的RRC Resume request消息的完整性保护验证配置信息之前),所述第二网络设备根据邻区的频域SSB配置信息计算对应的KgNB*(密钥),以及对应的shortMAC-I。

[0097] 所述完整性保护验证配置信息,包括以下至少之一:至少一个短MAC-I、UE上下文标识I-RNTI。

[0098] 如果目标小区是一个频域范围包含多个SSBs的wideband carrier。则所述完整性保护验证配置信息包括每个SSB对应的ShortMAC-I以及对应的SSB标识信息。

[0099] 也就是说,当存在多个SSB的时候,所述完整性保护验证配置信息,还包括:目标小

区中频域范围包含的至少一个SSB所对应的SSB的标识信息;并且,所述至少一个短MAC-I,与所述至少一个SSB的标识信息相对应。

[0100] 前述网络侧完成配置处理,然后所述UE会进行RRC恢复请求,在向目标发起RRC Resume request消息之前,UE根据当前SSB的ARFCN和PCI信息更新密钥并计算ShortMAC-I。

[0101] 场景2、

[0102] 在第二网络设备侧还会进行以下处理:在发送配置信息之前(也就是说,向邻基站发送关于验证UE发起的RRC Resume request消息的完整性保护验证配置信息之前),所述第二网络设备根据邻区的频域SSB配置信息计算至少一个SSB对应的密钥。

[0103] 所述完整性保护验证配置信息,包括以下至少之一:至少一个密钥、UE上下文标识I-RNTI、安全算法、原服务基站的PCI、原服务基站的C-RNTI。

[0104] 如果包括有多个SSB的时候,还可以包括:

[0105] 所述第一网络设备管理的目标小区中频域范围包含的至少一个SSB所对应的SSB的标识信息;并且,所述至少一个密钥,与所述至少一个SSB的标识信息相对应。

[0106] 所述完整性保护验证配置信息包括KgNB*,UE上下文标识I-RNTI,存储的安全算法,原侧的PCI和C-RNTI。如果目标小区是一个频域范围包含多个SSBs的wideband carrier。则所述完整性保护验证配置信息包括每个SSB对应的KgNB*以及对应的SSB标识信息。

[0107] 前述网络侧完成配置处理,然后所述UE会进行RRC恢复请求,在向目标发起RRC Resume request消息之前,UE根据当前SSB的ARFCN和PCI信息更新密钥并计算ShortMAC-I。

[0108] 可见,通过采用上述方案,就能够通过预先配置RRC连接恢复请求消息完整性保护的配置信息,使得第一网络设备可以进行完整性保护验证;如此,就能够降低第一网络设备尤其是服务基站和锚基站之间进行信令交互所带来的数据传输,特别是能够避免系统中存在假UE攻击网络的场景。

[0109] 实施例三、

[0110] 本发明实施例提供了一种完整性验证方法,应用于UE,所述方法包括:

[0111] 向第一网络设备发送RRC恢复请求消息。

[0112] 本实施例中所述第一网络设备,可以为当前为UE提供服务的基站。

[0113] 所述UE会进行RRC恢复请求,在向目标发起RRC Resume request消息之前,UE根据当前SSB的ARFCN以及PCI信息,更新密钥并计算得到短MAC-I。

[0114] 相应的,所述第一网络设备侧基于所述完整性保护的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证。

[0115] 需要理解的是,本实施例提供的方案同样可以参见前述图4、5、6描述的场景,以及前述实施例描述的方案进行相应的处理,只是这里不再进行赘述。

[0116] 可见,通过采用上述方案,就能够通过预先配置RRC连接恢复请求消息完整性保护的配置信息,使得第一网络设备可以进行完整性保护验证;如此,就能够降低第一网络设备尤其是服务基站和锚基站之间进行信令交互所带来的数据传输,特别是能够避免系统中存在假UE攻击网络的场景。

[0117] 实施例四、

[0118] 本发明实施例提供了一种第一网络设备,如图7所示,包括:

[0119] 第一通信单元71,配置用于验证用户设备UE发起的RRC恢复请求消息的完整性保护验证配置信息;

[0120] 第一处理单元72,基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证。

[0121] 本实施例中所述第一网络设备,可以为当前为UE提供服务的基站。

[0122] 本实施例可以存在以下两种处理场景,分别说明如下:

[0123] 场景1、

[0124] 所述第一通信单元71,接收第二网络设备发来的关于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息;其中,所述第二网络设备为服务所述UE的原服务基站,且当所述第二网络设备在释放所述UE进入非激活态前,向所述第一网络设备发送用于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息。

[0125] 所述完整性保护验证配置信息,包括以下至少之一:至少一个短MAC-I、UE上下文标识I-RNTI。

[0126] 如果目标小区是一个频域范围包含多个SSBs的wideband carrier。则所述完整性保护验证配置信息包括每个SSB对应的ShortMAC-I以及对应的SSB标识信息。

[0127] 也就是说,当存在多个SSB的时候,所述完整性保护验证配置信息,还包括:所述第一网络设备管理的目标小区中频域范围包含的至少一个SSB所对应的SSB的标识信息;并且,所述至少一个短MAC-I,与所述至少一个SSB的标识信息相对应。

[0128] 前述网络侧完成配置处理,然后所述UE会进行RRC恢复请求,在向目标发起RRC Resume request消息之前,UE根据当前SSB的ARFCN和PCI信息更新密钥并计算ShortMAC-I。

[0129] 相应的,所述第一通信单元71,接收所述UE发来的RRC恢复请求消息;

[0130] 第一处理单元72,当存在所述UE对应的完整性保护验证配置信息时,基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证;当不存在所述UE对应的完整性保护验证配置信息时,寻址所述UE对应的锚基站,使得所述锚基站执行对RRC恢复请求消息进行完整性保护验证。

[0131] 也就是说,UE向某个基站发起RRC Resume request消息,如果该基站存在该UE对应的完整性保护验证配置信息,则执行RRC Resume request消息的完整性保护验证。否则寻址anchor gNB,让anchor gNB执行RRC Resume request消息的完整性保护验证。

[0132] 第一处理单元72,根据所述RRC恢复请求消息中所携带的UE标识信息,寻找存储的短MAC-I;基于所述短MAC-I进行完整性保护验证;当验证成功时,为所述UE寻址目标网络设备,进行所述UE上下文获取;当验证失败时,拒绝所述UE。

[0133] 也就是说,如果当前基站可以执行RRC Resume request消息的完整性保护验证,如果验证成功则寻址目标基站,进行UE上下文索取,否则直接拒绝UE。

[0134] 场景2、

[0135] 所述第一通信单元71,接收第二网络设备发来的关于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息;其中,所述第二网络设备为服务所述UE的原服务基站,且当所述第二网络设备在释放所述UE进入非激活态前,向所述第一网络设备发送用于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息。

[0136] 所述完整性保护验证配置信息,包括以下至少之一:至少一个密钥、UE上下文标识

I-RNTI、安全算法、原服务基站的PCI、原服务基站的C-RNTI。

[0137] 如果包括有多个SSB的时候,还可以包括:所述第一网络设备管理的目标小区中频域范围包含的至少一个SSB所对应的SSB的标识信息;并且,所述至少一个密钥,与所述至少一个SSB的标识信息相对应。

[0138] 所述完整性保护验证配置信息包括KgNB*,UE上下文标识I-RNTI,存储的安全算法,原侧的PCI和C-RNTI。如果目标小区是一个频域范围包含多个SSBs的wideband carrier。则所述完整性保护验证配置信息包括每个SSB对应的KgNB*以及对应的SSB标识信息。

[0139] 前述网络侧完成配置处理,然后所述UE会进行RRC恢复请求,在向目标发起RRC Resume request消息之前,UE根据当前SSB的ARFCN和PCI信息更新密钥并计算ShortMAC-I。

[0140] 相应的,所述第一通信单元71,接收所述UE发来的RRC恢复请求消息;

[0141] 第一处理单元72,当存在所述UE对应的完整性保护验证配置信息时,基于所述完整性保护验证的配置信息,对所述UE发来的RRC恢复请求消息进行完整性保护验证;当不存在所述UE对应的完整性保护验证配置信息时,寻址所述UE对应的锚基站,使得所述锚基站执行对RRC恢复请求消息进行完整性保护验证。

[0142] 也就是说,UE向某个基站发起RRC Resume request消息,如果该基站存在该UE对应的完整性保护验证配置信息,则执行RRC Resume request消息的完整性保护验证。否则寻址anchor gNB,让anchor gNB执行RRC Resume request消息的完整性保护验证。

[0143] 第一处理单元72,根据所述RRC恢复请求消息中所携带的标识信息,寻找存储的密钥;至少基于所述密钥和所述安全算法计算得到短MAC-I;基于计算得到的所述短MAC-I进行完整性保护验证;当验证成功时,为所述UE寻址目标网络设备,进行所述UE上下文获取;当验证失败时,拒绝所述UE。

[0144] 也就是说,目标基站根据RRC resume request消息所携带的信息,寻找存储的KgNB*,然后计算shortMAC-I。如果当前基站可以执行RRC Resume request消息的完整性保护验证,如果验证成功则寻址目标基站,进行UE上下文索取,否则直接拒绝UE。

[0145] 可见,通过采用上述方案,就能够通过预先配置RRC连接恢复请求消息完整性保护验证的配置信息,使得第一网络设备可以进行完整性保护验证;如此,就能够降低第一网络设备尤其是服务基站和锚基站之间进行信令交互所带来的数据传输,特别是能够避免系统中存在假UE攻击网络的场景。

[0146] 实施例五、

[0147] 本发明实施例提供了一种第二网络设备,如图8所示,包括:第二处理单元81,当作为UE的原服务基站、且保存所述UE的上下文时,在释放所述UE进入非激活状态之前,通过第二通信单元向第一网络设备发送关于验证UE发起的RRC恢复请求消息的完整性保护验证配置信息;

[0148] 第二通信单元82,向第一网络设备发送所述完整性保护验证配置信息。

[0149] 本实施例中所述第二网络设备,可以为当前为UE对应的原服务基站。其中,所述第一网络设备及小区,为RAN通知区域内的全部基站及其小区中的至少部分基站及小区中之一的基站及小区。或者可以理解为第一网络设备为UE的当前服务基站;该第一网络设备管理的某一个小区为UE的目标小区。

[0150] 本实施例也可以存在以下两种处理场景,分别说明如下:

[0151] 场景1、

[0152] 在发送配置信息之前(也就是说,向邻基站发送关于验证UE发起的RRC Resume request消息的完整性保护验证配置信息之前),第二处理单元,根据邻区的频域SSB配置信息计算对应的KgNB*(密钥),以及对应的shortMAC-I。

[0153] 所述完整性保护验证配置信息,包括以下至少之一:至少一个短MAC-I、UE上下文标识I-RNTI。

[0154] 如果目标小区是一个频域范围包含多个SSBs的wideband carrier。则所述完整性保护验证配置信息包括每个SSB对应的ShortMAC-I以及对应的SSB标识信息。

[0155] 也就是说,当存在多个SSB的时候,所述完整性保护验证配置信息,还包括:目标小区中频域范围包含的至少一个SSB所对应的SSB的标识信息;并且,所述至少一个短MAC-I,与所述至少一个SSB的标识信息相对应。

[0156] 前述网络侧完成配置处理,然后所述UE会进行RRC恢复请求,在向目标发起RRC Resume request消息之前,UE根据当前SSB的ARFCN和PCI信息更新密钥并计算ShortMAC-I。

[0157] 场景2、

[0158] 在第二网络设备侧还会进行以下处理:在发送配置信息之前(也就是说,向邻基站发送关于验证UE发起的RRC Resume request消息的完整性保护验证配置信息之前),所述第二处理单元,根据邻区的频域SSB配置信息计算至少一个SSB对应的密钥。

[0159] 所述完整性保护验证配置信息,包括以下至少之一:至少一个密钥、UE上下文标识I-RNTI、安全算法、原服务基站的PCI、原服务基站的C-RNTI。

[0160] 如果包括有多个SSB的时候,还可以包括:

[0161] 所述第一网络设备管理的目标小区中频域范围包含的至少一个SSB所对应的SSB的标识信息;并且,所述至少一个密钥,与所述至少一个SSB的标识信息相对应。

[0162] 所述完整性保护验证配置信息包括KgNB*,UE上下文标识I-RNTI,存储的安全算法,原侧的PCI和C-RNTI。如果目标小区是一个频域范围包含多个SSBs的wideband carrier。则所述完整性保护验证配置信息包括每个SSB对应的KgNB*以及对应的SSB标识信息。

[0163] 前述网络侧完成配置处理,然后所述UE会进行RRC恢复请求,在向目标发起RRC Resume request消息之前,UE根据当前SSB的ARFCN和PCI信息更新密钥并计算ShortMAC-I。

[0164] 可见,通过采用上述方案,就能够通过预先配置RRC连接恢复请求消息完整性保护的配置信息,使得第一网络设备可以进行完整性保护验证;如此,就能够降低第一网络设备尤其是服务基站和锚基站之间进行信令交互所带来的数据传输,特别是能够避免系统中存在假UE攻击网络的场景。

[0165] 实施例六、

[0166] 本发明实施例提供了一种UE,如图9所示包括:

[0167] 第三通信单元91,向第一网络设备发送RRC恢复请求消息。

[0168] 第三处理单元92,根据当前SSB的ARFCN以及PCI信息,更新密钥并计算得到短MAC-I。

[0169] 相应的,所述第一网络设备侧基于所述完整性保护的配置信息,对所述UE发

来的RRC恢复请求消息进行完整性保护验证。

[0170] 需要理解的是,本实施例提供的方案同样可以参见前述图4、5、6描述的场景,以及前述实施例描述的方案进行相应的处理,只是这里不再进行赘述。

[0171] 可见,通过采用上述方案,就能够通过预先配置RRC连接恢复请求消息完整性保护验证的配置信息,使得第一网络设备可以进行完整性保护验证;如此,就能够降低第一网络设备尤其是服务基站和锚基站之间进行信令交互所带来的数据传输,特别是能够避免系统中存在假UE攻击网络的场景。

[0172] 本发明实施例还提供了一种网络设备、或者UE的硬件组成架构,如图10所示,包括:至少一个处理器1001、存储器1002、至少一个网络接口1003。各个组件通过总线系统1004耦合在一起。可理解,总线系统1004用于实现这些组件之间的连接通信。总线系统1004除包括数据总线之外,还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见,在图100中将各种总线都标为总线系统1004。

[0173] 可以理解,本发明实施例中的存储器1002可以是易失性存储器或非易失性存储器,或可包括易失性和非易失性存储器两者。

[0174] 在一些实施方式中,存储器1002存储了如下的元素,可执行模块或者数据结构,或者他们的子集,或者他们的扩展集:

[0175] 操作系统10021和应用程序10022。

[0176] 其中,所述处理器1001配置为:能够处理前述实施例一至三任一实施例的方法步骤,这里不再进行赘述。

[0177] 本发明实施例提供一种计算机存储介质,所述计算机存储介质存储有计算机可执行指令,所述计算机可执行指令被执行时实施前述实施例一至三任一实施例的方法步骤。

[0178] 本发明实施例上述装置如果以软件功能模块的形式实现并作为独立的产品销售或使用,也可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机、服务器、或者网络设备等)执行本发明各个实施例所述方法的全部或部分。而前述的存储介质包括:U盘、移动硬盘、只读存储器(ROM,Read Only Memory)、磁碟或者光盘等各种可以存储程序代码的介质。这样,本发明实施例不限制于任何特定的硬件和软件结合。

[0179] 相应地,本发明实施例还提供一种计算机存储介质,其中存储有计算机程序,该计算机程序配置为执行本发明实施例的数据调度方法。

[0180] 尽管为示例目的,已经公开了本发明的优选实施例,本领域的技术人员将意识到各种改进、增加和取代也是可能的,因此,本发明的范围应当不限于上述实施例。

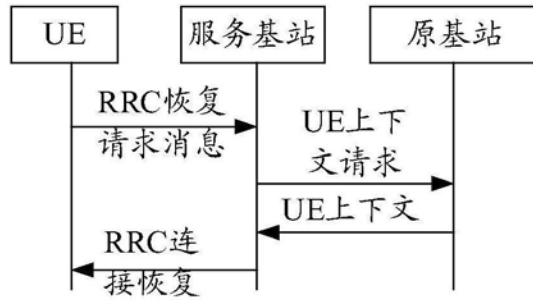


图1

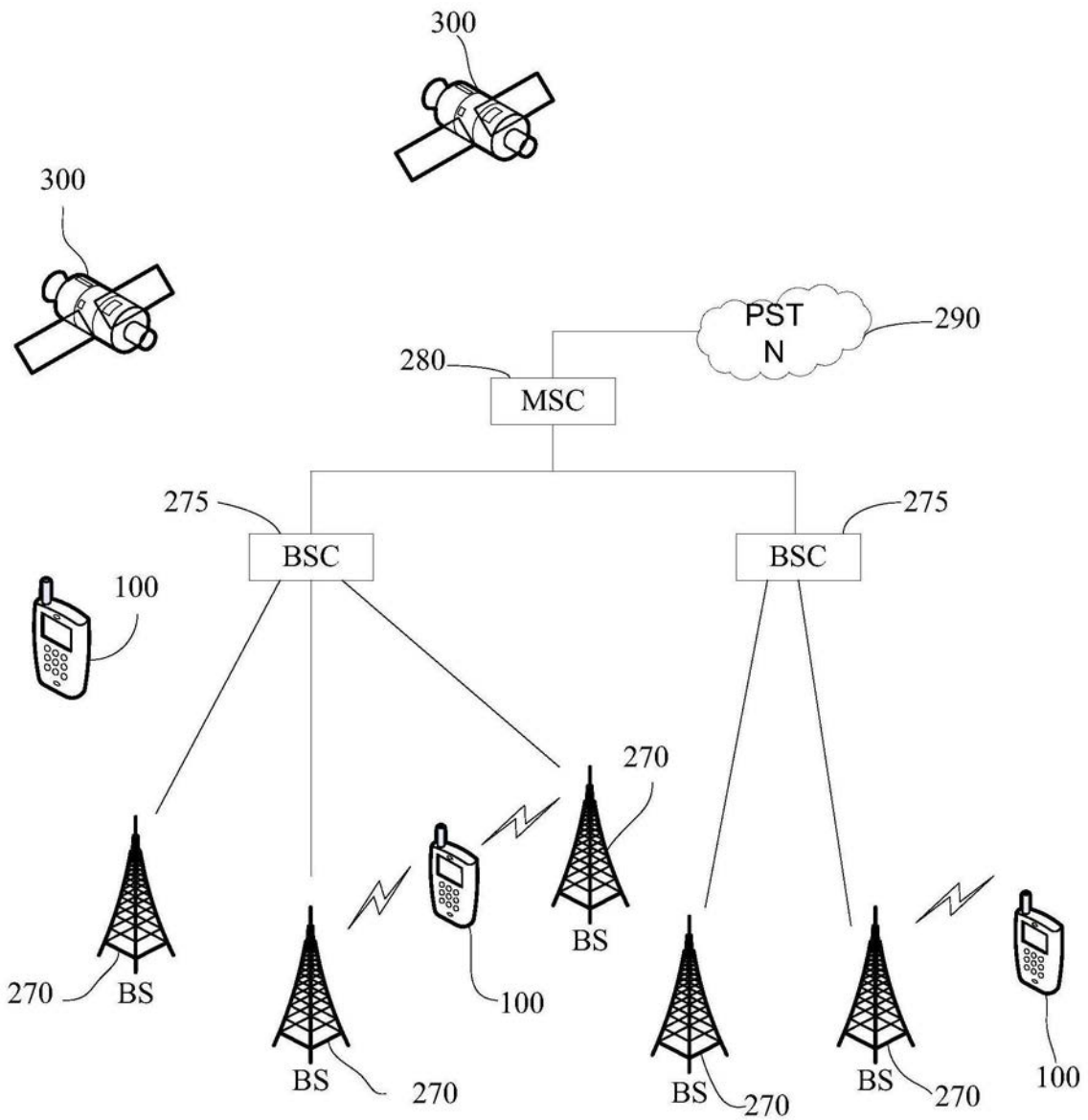


图2

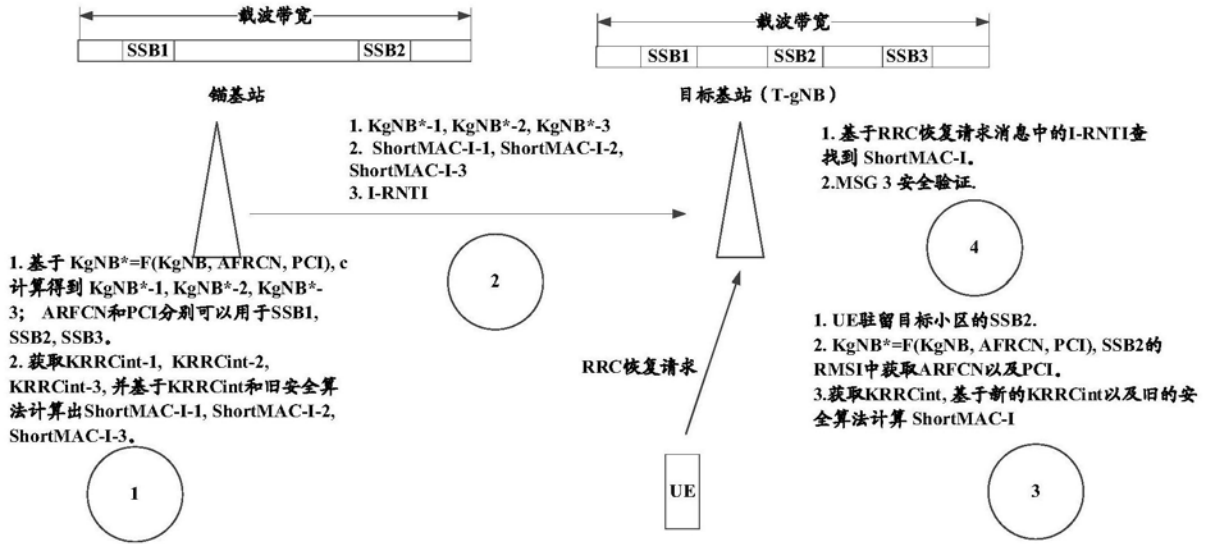


图5

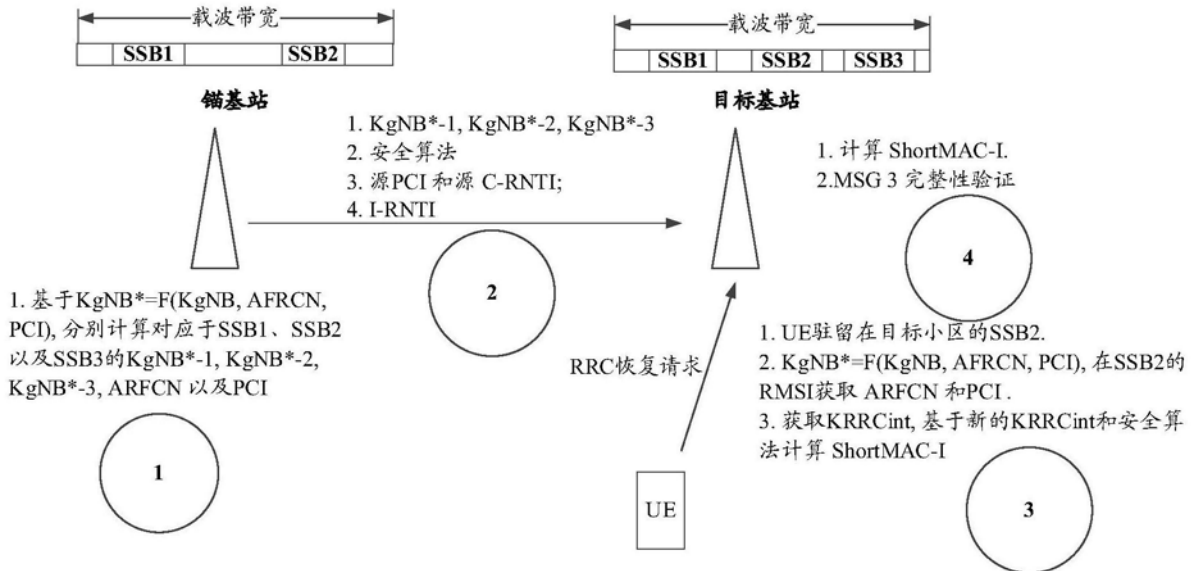


图6



图7

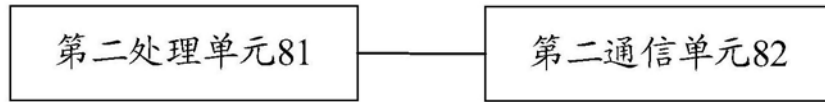


图8

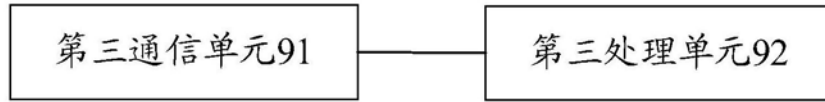


图9

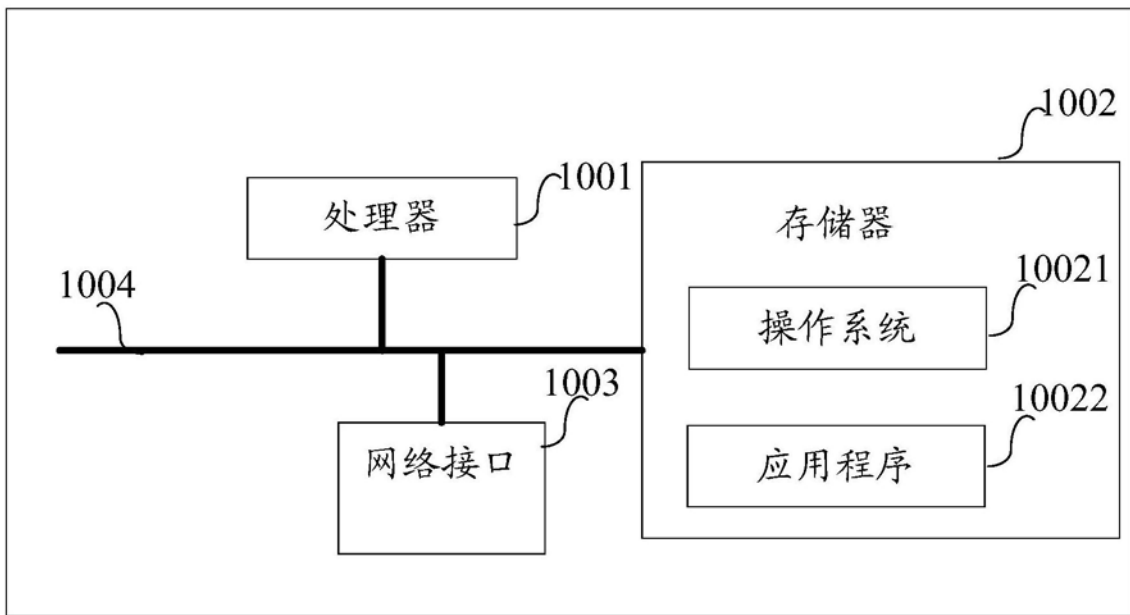


图10