



(12) 发明专利申请

(10) 申请公布号 CN 112243232 A

(43) 申请公布日 2021.01.19

(21) 申请号 202011099901.2

(51) Int.Cl.

(22) 申请日 2018.01.29

H04W 12/06 (2021.01)

(30) 优先权数据

H04W 76/18 (2018.01)

62/451866 2017.01.30 US

H04W 76/19 (2018.01)

H04W 76/27 (2018.01)

(62) 分案原申请数据

201880009288.5 2018.01.29

(71) 申请人 瑞典爱立信有限公司

地址 瑞典斯德哥尔摩

(72) 发明人 韦萨·勒托威尔塔

莫尼卡·威弗森

普拉耶沃·库马·纳卡米

(74) 专利代理机构 中科专利商标代理有限责任
公司 11021

代理人 余婧娜

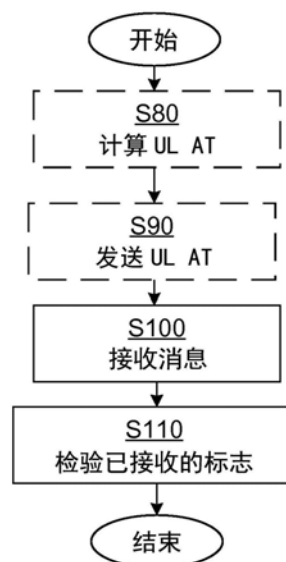
权利要求书3页 说明书16页 附图14页

(54) 发明名称

用于重新建立无线电资源控制(RRC)连接的
方法及装置

(57) 摘要

一种用于在用户设备(UE)(1)与目标演进NodeB(目标eNB)(3)之间重新建立无线电资源控制(RRC)连接的方法,所述方法由UE(1)执行且包括:从所述目标eNB(3)接收(S100)RRC连接重新建立消息,所述RRC连接重新建立消息包括下行链路(DL)认证标志,所述DL认证标志由移动性管理实体(4)生成且已将非接入层完整性密钥和新鲜度参数作为输入;以及认证(S110)所接收的DL认证标志。还公开了UE、目标eNB、源eNB和移动性管理实体、以及与其相关的方法、计算机程序和计算机程序产品。



1. 一种用于在用户设备UE (1) 与目标演进NodeB ‘目标eNB’ (3) 之间重新建立无线电资源控制RRC连接的方法,所述方法由所述UE (1) 执行且包括:

从所述目标eNB (3) 接收 (S100) RRC连接重新建立消息,所述RRC连接重新建立消息包括下行链路DL认证标志,所述DL认证标志由移动性管理实体 (4) 生成且将非接入层完整性密钥和新鲜度参数作为输入;以及

认证 (S110) 所接收的DL认证标志。

2. 根据权利要求1所述的方法,包括:利用所述非接入层完整性密钥作为输入来计算上行链路UL认证标志,并且向所述目标eNB (3) 发送包括所述UL认证标志的RRC连接重新建立请求。

3. 根据权利要求2所述的方法,其中,所述UL认证标志利用目标小区的标识作为输入来计算。

4. 根据权利要求3所述的方法,在所述RRC连接重新建立请求中包括所述目标小区的标识。

5. 根据权利要求1所述的方法,其中,所述DL认证标志由所述移动性管理实体 (4) 利用目标小区的标识作为输入来计算。

6. 一种用于在用户设备UE (1) 与目标演进NodeB ‘目标eNB’ (3) 之间重新建立无线电资源控制RRC连接的方法,所述方法由所述目标eNB (3) 执行且包括:

从移动性管理实体MME (4) 接收 (S300) 包括下行链路DL认证标志的消息,所述DL认证标志由所述MME (4) 生成,其中,所述DL认证标志利用非接入层完整性密钥和新鲜度参数作为输入而生成;以及

向所述UE (1) 发送 (S310) RRC连接重新建立消息,所述RRC连接重新建立消息包括所述DL认证标志,使得所述UE (1) 能够认证所述DL认证标志。

7. 根据权利要求6所述的方法,包括:从所述UE (1) 接收包括上行链路UL认证标志的RRC连接重新建立请求,其中,所述UL认证标志由所述UE (1) 利用所述非接入层完整性密钥作为输入来计算。

8. 根据权利要求7所述的方法,其中,所述UL认证标志由所述UE (1) 利用目标小区的标识作为输入来计算。

9. 根据权利要求6所述的方法,其中,所述DL认证标志由所述MME (4) 利用目标小区的标识作为输入来计算。

10. 一种用于在用户设备UE (1) 与目标演进NodeB ‘目标eNB’ (3) 之间重新建立无线电资源控制RRC连接的方法,所述方法由移动性管理实体MME (4) 执行且包括:

利用非接入层完整性密钥和新鲜度参数作为输入生成 (S400) 下行链路DL认证标志;以及

向所述目标eNB (3) 发送 (S410) 包括已生成的DL认证标志的消息,使得所述目标eNB (3) 能够向所述UE (1) 发送RRC连接重新建立消息,所述RRC连接重新建立消息包括所述DL认证标志,进而使得所述UE (1) 能够认证所述DL认证标志。

11. 根据权利要求10所述的方法,包括利用目标小区的标识作为输入生成所述DL认证标志。

12. 根据权利要求10所述的方法,包括:

从所述目标eNB接收上行链路UL认证标志,所述UL认证标志由所述UE (1) 利用所述非接入层完整性密钥作为输入而生成,以及
验证所述UL认证标志。

13. 根据权利要求12所述的方法,其中,所述UL认证标志由所述UE (1) 利用目标小区的标识作为输入而生成。

14. 一种用户设备UE (1),用于在所述UE (1) 与目标演进NodeB ‘目标eNB’ (3) 之间重新建立无线电资源控制RRC连接,所述UE (1) 包括:

处理器 (10); 以及

存储器,存储有计算机程序,所述计算机程序在被所述处理器执行时使所述UE:

从所述目标eNB (3) 接收RRC连接重新建立消息,所述RRC连接重新建立消息包括下行链路DL认证标志,所述DL认证标志由移动性管理实体 (4) 生成且将非接入层完整性密钥和新鲜度参数作为输入; 以及

认证所接收的DL认证标志。

15. 根据权利要求14所述的UE,其中,所述DL认证标志由所述移动性管理实体 (4) 利用目标小区的标识作为输入来计算。

16. 一种目标演进NodeB ‘目标eNB’ (3),用于在用户设备UE (1) 与所述目标eNB (3) 之间重新建立无线电资源控制RRC连接,所述目标eNB (3) 包括:

处理器 (30); 以及

存储器,存储有计算机程序,所述计算机程序在被所述处理器执行时使所述目标eNB:

从移动性管理实体MME (4) 接收包括下行链路DL认证标志的消息,所述DL认证标志由所述MME (4) 生成,其中,所述DL认证标志利用非接入层完整性密钥和新鲜度参数作为输入而生成; 以及

向所述UE (1) 发送RRC连接重新建立消息,所述RRC连接重新建立消息包括所述DL认证标志,使得所述UE (1) 能够认证所述DL认证标志。

17. 根据权利要求16所述的目标eNB (3),其中,所述DL认证标志由所述MME (4) 利用目标小区的标识作为输入来计算。

18. 一种源演进NodeB ‘源eNB’ (2),用于在用户设备UE (1) 与目标eNB (3) 之间重新建立无线电资源控制RRC连接,所述源eNB (2) 包括:

处理器 (20); 以及

存储器,存储有计算机程序,所述计算机程序在被所述处理器执行时使所述源eNB:

获得下行链路DL认证标志,所述DL认证标志是利用非接入层完整性密钥和新鲜度参数作为输入而生成的; 以及

向所述目标eNB (3) 发送响应消息,所述响应消息包括已获得的DL认证标志,使得所述目标eNB (3) 能够向所述UE (1) 发送RRC连接重新建立消息,所述RRC连接重新建立消息包括所述DL认证标志,进而使得所述UE (1) 能够认证所述DL认证标志。

19. 一种移动性管理实体MME (4),用于在用户设备UE (1) 与目标演进NodeB ‘目标eNB’ (3) 之间重新建立无线电资源控制RRC连接,所述MME (4) 包括:

处理器 (40); 以及

存储器,存储有计算机程序,所述计算机程序在被所述处理器执行时使所述MME:

利用非接入层完整性密钥和新鲜度参数作为输入生成下行链路DL认证标志;以及

向所述目标eNB (3) 发送包括已生成的DL认证标志的消息,使得所述目标eNB (3) 能够向所述UE (1) 发送RRC连接重新建立消息,所述RRC连接重新建立消息包括所述DL认证标志,进而使得所述UE (1) 能够认证所述DL认证标志。

20. 一种计算机可读介质,存储有用于在用户设备UE (1) 与目标演进NodeB ‘目标eNB’ (3) 之间重新建立无线电资源控制RRC连接的计算机程序 (14,15),所述计算机程序在被处理器执行时,使所述UE:

从所述目标eNB (3) 接收 (S100) RRC连接重新建立消息,所述RRC连接重新建立消息包括下行链路DL认证标志,所述DL认证标志由移动性管理实体 (4) 生成且将非接入层完整性密钥和新鲜度参数作为输入;以及

认证 (S110) 所接收的DL认证标志。

21. 一种计算机可读介质,存储有用于在用户设备UE (1) 与目标演进NodeB ‘目标eNB’ (3) 之间重新建立无线电资源控制RRC连接的计算机程序 (34,35),所述计算机程序在被处理器运行时,使所述目标eNB:

从移动性管理实体MME (4) 接收包括由所述MME (4) 生成的下行链路DL认证标志的消息,其中,所述DL认证标志利用非接入层完整性密钥和新鲜度参数作为输入而生成;以及

向所述UE (1) 发送RRC连接重新建立消息,所述RRC连接重新建立消息包括所述DL认证标志,使得所述UE (1) 能够认证所述DL认证标志。

22. 一种计算机可读介质,存储有用于在用户设备UE (1) 与目标演进NodeB ‘目标eNB’ (3) 之间重新建立无线电资源控制RRC连接的计算机程序 (44,45),所述计算机程序在被处理器运行时,使移动性管理实体MME (4):

利用非接入层完整性密钥和新鲜度参数作为输入生成下行链路DL认证标志;以及

向所述目标eNB (3) 发送包括已生成的DL认证标志的消息,使得所述目标eNB (3) 能够向所述UE (1) 发送RRC连接重新建立消息,所述RRC连接重新建立消息包括所述DL认证标志,进而使得所述UE (1) 能够认证所述DL认证标志。

用于重新建立无线电资源控制(RRC)连接的方法及装置

[0001] 本申请是2018年1月29日提交的中国专利申请No.2018800092885的发明名称为“用于重新建立无线电资源控制(RRC)连接的方法及装置”的分案申请。

技术领域

[0002] 本发明涉及用于重新建立无线电资源控制连接的方法、用户设备、源NodeB、目标NodeB、移动性管理实体、计算机程序和计算机程序产品。

背景技术

[0003] 控制平面(CP)蜂窝物联网(CIoT)优化(也被称为非接入层上的数据(NAS)(DoNAS))是用于根据第3代合作伙伴计划(3GPP)的技术规范TS 23.401 V14.2.0的第5.3.4B条(以及诸如TS 24.301V14.2.0的其它规范)的规定在NAS上传输数据的方案。在TS 33.401V14.1.0的第8.2条中规定了安全特征。基本方案的安全作用非常有限。DoNAS特征的目的是在NAS信令上发送数据而无需建立数据无线电承载(DRB)且无需建立接入层(AS)安全。目的是为了节省信令。对应于TS 23.401 V14.2.0的图5.3.4B.2-1的图1说明了DoNAS原理。

[0004] 3GPP文档R3-161324中的工作项目关注对于CP CIoT的移动性增强。针对CP CIoT不支持切换,但是用户设备(UE)可能无论如何都要移动,使UE处于已连接模式(即,与演进NodeB(eNB)具有无线电资源控制(RRC)连接)时无线电链路失败(RLF)。这提出了在这种情况下做什么的问题。因为针对CP CIoT特征不支持AS安全,所以用于RLF的已有的机制实际上不能安全地使用。换言之,在CP CIoT中使用现有的RLF处理机制在安全方面是不可接受的。

[0005] 参见3GPP TS 36.331 V14.1.0,在当前的LTE(长期演进)系统中,RRC层被规定为包括被称为ShortMAC-I的信息元素(IE),ShortMAC-I例如在RRC连接重新建立步骤期间被用于UE的识别。ShortMAC-I的计算包括以下作为输入:

[0006] -RRC完整性密钥:比特串(大小(128))

[0007] -目标小区的标识:比特串(大小(28))

[0008] -源小区的物理小区标识:整数(0...503)

[0009] -源小区处的UE的C-RNTI(小区无线网络临时标识符):比特串(大小(16))

[0010] 在TS 33.401 V14.1.0中规定了所使用的函数。

[0011] RRC层在LTE系统中被规定为包括被称为ShortResumeMAC-I的信息元素(IE),ShortResumeMAC-I例如在RRC连接恢复步骤期间被用于UE的识别。ShortResumeMAC-I的计算包括以下作为输入:

[0012] -RRC完整性密钥:比特串(大小(128))

[0013] -目标小区的标识:比特串(大小(28))

[0014] -源小区的物理小区标识:整数(0...503)

[0015] -源小区处的UE的C-RNTI:比特串(大小(16))

[0016] -恢复常数

[0017] 注意, ShortResumeMAC-I的计算附加地包括恢复常数, 这允许ShortMAC-I与ShortResumeMAC的区分。在TS 33.401 V14.1.0中规定了所使用的函数=。

发明内容

[0018] 本发明的目的是实现无线电资源控制连接的重新建立期间的减少的信令。

[0019] 本发明的另一个目的是实现RRC连接重新建立期间UE对目标eNB的认证。

[0020] 根据本发明的第一方面, 提出了用于在用户设备 (UE) 与目标演进NodeB (目标eNB) 之间重新建立无线电资源控制 (RRC) 连接的方法。所述方法是由UE执行的且包括:

[0021] 从目标eNB接收RRC连接重新建立消息, 所述RRC连接重新建立消息包括下行链路 (DL) 认证标志, 所述DL认证标志由移动性管理实体 (MME) 生成且将非接入层 (NAS) 完整性密钥作为输入; 以及

[0022] 认证所接收的DL认证标志。

[0023] 由此特别地实现了, UE能够借助于NAS完整性密钥在RRC连接重新建立 (例如, 用于EPS CP IoT优化的RRC连接重新建立) 期间认证eNB。因此, 无需创建接入层 (AS) 密钥, 这是非常有益的 (例如, 因为无论如何都要生成NAS密钥, 但是只在用于RRC连接重新建立时才会必须生成AS密钥)。

[0024] 所述方法还包括, 利用NAS完整性密钥作为输入计算上行链路 (UL) 认证标志、以及向目标eNB发送包括UL认证标志的RRC连接重新建立请求的步骤。在这种情况下可以利用目标小区的标识作为输入来计算UL认证标志。在后一种情况下可以将目标小区的标识包括在RRC连接重新建立请求中。

[0025] 在所述方法的实施例中, DL认证标志是由MME利用目标小区的标识作为输入来计算的。

[0026] RRC连接重新建立消息可以包括输入 (Input) MAC C-IoT DL。认证所接收的DL认证标志可以通过使用Input-MAC C-IoT DL和所述非接入层完整性密钥完成。Input-MAC C-IoT DL可以包括目标小区的标识。

[0027] 第二方面涉及用于在UE与目标eNB之间重新建立RRC连接的方法, 且由目标eNB执行。所述方法包括:

[0028] 从MME接收包括由所述MME生成的DL认证标志的消息, 其中, 所述DL认证标志利用NAS完整性密钥作为输入而生成; 以及

[0029] 向UE发送RRC连接重新建立消息, 所述RRC连接重新建立消息包括DL认证标志。

[0030] 在第二方面的实施例中, 所述方法包括, 从UE接收包括UL认证标志的RRC连接重新建立请求, 其中, 所述UL认证标志由UE使用NAS完整性密钥作为输入来计算。UL认证标志可以由UE利用目标小区的标识作为输入来计算。

[0031] 在第二方面的实施例中, DL认证标志由MME利用目标小区的标识作为输入来计算。

[0032] 在第二方面的实施例中, RRC连接重新建立消息包括Input MAC C-IoT DL。

[0033] 所接收的消息可以是临时性线路 (PATCH) 切换请求确认消息且包括Input-MAC C-IoT DL。备选地, 所接收的消息可以是检验 (check) MAC确认消息且包括Input-MAC C-IoT DL。

[0034] 第三方面涉及用于在UE与目标eNB之间重新建立RRC连接的方法,且在源eNB中执行。所述方法包括:

[0035] 获得利用NAS完整性密钥作为输入而生成的DL认证标志;以及

[0036] 向目标eNB发送响应消息,所述响应消息包括已获得的DL认证标志。

[0037] 在第三方面的实施例中执行的所述获得包括:生成认证标志,或从MME接收S1检验响应消息,所接收的S1检验响应消息包括DL认证标志和/或Input-MAC C IoT DL。

[0038] 在第三方面的实施例中的响应消息是X2 UE上下文响应消息。

[0039] 第四方面涉及用于在UE与目标eNB之间重新建立RRC连接的方法,且由MME执行。所述方法包括:

[0040] 利用NAS完整性密钥作为输入生成DL认证标志;以及

[0041] 向目标eNB发送包括已生成的DL认证标志的消息。

[0042] 在第四方面的实施例中,DL认证标志的生成利用目标小区的标识作为输入(除了NAS完整性密钥之外)完成。

[0043] 根据第四方面的方法可以包括:

[0044] 从目标eNB接收UL认证标志,所述UL认证标志由所述UE利用NAS完整性密钥作为输入而生成,以及

[0045] 验证所述UL认证标志。

[0046] UL认证标志可以由UE利用目标小区的标识作为输入而生成。

[0047] 所述消息可以是路径切换请求确认消息且包括Input-MAC C IoT DL。在另一实施例中,所述方法可以是检验MAC确认消息且包括Input-MAC C IoT DL。

[0048] 本发明的第五方面涉及用于在UE与目标eNB之间重新建立RRC连接的UE。所述UE包括:

[0049] 处理器;以及存储有指令的计算机程序产品,所述指令在被所述处理器执行时使所述UE:

[0050] 从目标eNB接收RRC连接重新建立消息,所述RRC连接重新建立消息包括DL认证标志,所述DL认证标志由MME生成且将NAS完整性密钥作为输入;以及

[0051] 认证所接收的DL认证标志。

[0052] 在UE的实施例中,RRC连接重新建立消息包括Input-MAC C IoT DL,且所接收的DL认证标志通过使用所述Input-MAC C IoT DL和所述非接入层完整性密钥进行认证。

[0053] 在UE的实施例中,DL认证标志由MME利用目标小区的标识作为输入来计算。

[0054] 第六方面涉及用于在UE与目标eNB之间重新建立RRC连接的目标eNB。所述目标eNB包括:

[0055] 处理器;以及

[0056] 存储有指令的计算机程序产品,所述指令在被所述处理器执行时使所述目标eNB:

[0057] 从MME接收包括由所述MME生成的DL认证标志的消息,其中,所述DL认证标志利用NAS完整性密钥作为输入而生成;以及

[0058] 向UE发送RRC连接重新建立消息,所述RRC连接重新建立消息包括DL认证标志。

[0059] 在目标eNB的实施例中,DL认证标志由MME利用目标小区的标识作为输入来计算。

[0060] 在目标eNB的实施例中,RRC连接重新建立消息包括Input MAC C IoT DL(即,用于

DL认证标志的生成的输入)。

[0061] 在目标eNB的实施例中,所接收的消息是临时性线路切换请求确认消息且包括Input-MAC CIoT DL。

[0062] 在目标eNB的另一实施例中,所接收的消息是检验MAC确认消息且包括Input-MAC CIoT DL。

[0063] 第七方面涉及用于在UE与目标eNB之间重新建立RRC连接的源eNB。所述源eNB包括:

[0064] 处理器;以及

[0065] 存储有指令的计算机程序产品,所述指令在被所述处理器执行时使所述源eNB:

[0066] 获得DL认证标志,所述DL认证标志是利用非接入层完整性密钥作为输入而生成的;以及

[0067] 向目标eNB发送响应消息,所述响应消息包括已获得的DL认证标志。

[0068] 在源eNB的实施例中,响应消息是X2 UE上下文响应消息。

[0069] 第八方面涉及用于在UE与目标eNB之间重新建立RRC连接的MME。所述MME包括:

[0070] 处理器;以及

[0071] 存储有指令的计算机程序产品,所述指令在被所述处理器执行时使所述MME:

[0072] 利用NAS完整性密钥作为输入生成DL认证标志;以及

[0073] 向目标eNB发送包括已生成的DL认证标志的消息。

[0074] 在MME的实施例中,所述消息是路径切换请求确认消息且在该实施例中,所述消息包括Input-MAC CIoT DL。

[0075] 在MME的另一实施例中,所述消息是检验MAC确认消息。在这种情况下,所述消息包括Input-MAC CIoT DL。

[0076] 第九方面涉及用于在UE与目标eNB之间重新建立RRC连接的UE。所述UE包括:

[0077] 通信管理器,用于从目标eNB接收RRC连接重新建立消息,所述RRC连接重新建立消息包括DL认证标志,所述DL认证标志由MME生成且将NAS完整性密钥作为输入;以及

[0078] 确定管理器,用于认证所接收的DL认证标志。

[0079] 第十方面涉及用于在UE与目标eNB之间重新建立RRC连接的目标eNB。所述目标eNB包括:

[0080] 通信管理器,用于从MME接收包括由MME生成的DL认证标志的消息,其中,所述DL认证标志利用NAS完整性密钥作为输入而生成;且用于向UE发送RRC连接重新建立消息,所述RRC连接重新建立消息包括所述DL认证标志。

[0081] 第十一方面涉及用于在UE与目标eNB之间重新建立RRC连接的源eNB。所述源eNB包括:

[0082] 确定管理器,用于获得利用NAS完整性密钥作为输入而生成的DL认证标志;以及

[0083] 通信管理器,用于向目标eNB发送响应消息,所述响应消息包括已获得的DL认证标志。

[0084] 第十二方面涉及用于在UE与目标eNB之间重新建立RRC连接的MME。所述MME包括:

[0085] 确定管理器,用于利用NAS完整性密钥作为输入生成DL认证标志;以及

[0086] 通信管理器,用于向目标eNB发送包括已生成的DL认证标志的消息。

[0087] 第十三方面涉及用于在UE与目标eNB之间重新建立RRC连接的计算机程序。所述计算机程序包括计算机程序代码,所述计算机程序代码在UE上运行时,使UE:

[0088] 从目标eNB接收RRC连接重新建立消息,所述RRC连接重新建立消息包括DL认证标志,所述DL认证标志由MME生成且将NAS层完整性密钥作为输入;以及

[0089] 认证所接收的DL认证标志。

[0090] 第十四方面涉及用于在UE与目标eNB之间重新建立RRC连接的计算机程序。所述计算机程序包括计算机程序代码,所述计算机程序代码在目标eNB上运行时,使目标eNB:

[0091] 从MME接收包括由所述MME生成的DL认证标志的消息,其中,所述DL认证标志利用NAS完整性密钥作为输入而生成;以及

[0092] 向UE发送RRC连接重新建立消息,所述RRC连接重新建立消息包括DL认证标志。

[0093] 第十五方面涉及用于在UE与目标eNB之间重新建立RRC连接的计算机程序。所述计算机程序包括计算机程序代码,所述计算机程序代码在源eNB上运行时,使源eNB:

[0094] 获得利用NAS完整性密钥作为输入而生成的DL认证标志;以及

[0095] 向目标eNB发送响应消息,所述响应消息包括已获得的DL认证标志。

[0096] 第十六方面涉及用于在UE与目标eNB之间重新建立RRC连接的计算机程序。所述计算机程序包括计算机程序代码,所述计算机程序代码在MME上运行时,使MME:

[0097] 利用NAS完整性密钥作为输入生成DL认证标志;以及

[0098] 向目标eNB发送包括已生成的DL认证标志的消息。

[0099] 第十七方面涉及计算机程序产品,所述计算机程序产品包括根据第十三方面至第十六方面的计算机程序中的至少一种和在其上存储有所述至少一种计算机可读存储装置。

[0100] 在上述所有的十七个方面中,RRC连接的重新建立可以用于控制平面物联网优化。

[0101] 通常,除非本文另有明确定义,否则实施例的项目列表中使用的所有术语根据其技术领域中的普通含义来解释。除非另有明确说明,否则对“一/一个/元件、设备、组件、装置、步骤等”的所有引用应被开放地解释为指代元件、设备、组件、装置、步骤等中的至少一个实例。除非明确说明,否则本文公开的任何方法的步骤不必严格以所公开的确切顺序来执行。

附图说明

[0102] 现在通过举例的方式参考附图描述本发明,在附图中:

[0103] 图1示意性地示出了DoNAS原理信令;

[0104] 图2示意性地示出了可以应用本文提出的实施例的环境;

[0105] 图3A示意性地示出了根据本文提出的实施例的一部分的信令;

[0106] 图3B示意性地示出了根据本文提出的实施例的一部分的且接续图3A的信令;

[0107] 图4A示意性地示出了根据本文提出的实施例的一部分的信令;

[0108] 图4B示意性地示出了根据本文提出的实施例的一部分的且接续图4A的信令;

[0109] 图5示意性地示出了根据本文提出的实施例的信令;

[0110] 图6示意性地示出了根据本文提出的实施例的信令;

[0111] 图7A-7D是示出了根据本文提出的实施例的方法的流程图;

[0112] 图8-图11是示出了本文提出的实体的一些组件的示意图;以及

[0113] 图12-图15是示出了本文提出的实施例的功能模块的示意图。

具体实施方式

[0114] 现在将在下文参考其中示出本发明的特定实施例的附图来更全面地描述本发明。然而,本发明可以按多种不同形式来实现,并且不应当被解释为受到本文阐述的实施例的限制;相反,通过示例的方式给出这些实施例,使得本公开将是透彻和完整的,并且向本领域技术人员充分地传达本发明的范围。在说明书全文中,相似的标记指代相似的要素。

[0115] 无线电资源控制(RRC)连接重新建立和RRC连接挂起/恢复步骤是已有的方案,在控制平面(CP)蜂窝物联网(CIoT)优化的情况下,它们可能是用于处理无线电链路失败的候选。所有这些已有的方案都使用如背景技术中描述的用户设备的(UE的)认证标志,以向演进的NodeB(eNB)显示真正的UE 1想要重新建立或恢复RRC连接。另外,下行链路(DL)方向中的受完整性保护的RRC消息用于向UE 1显示UE 1连接到了真正的eNB。然而,这些方案依赖于接入层(AS)安全(特别是RRC安全)的存在,但是AS安全和RRC安全并不存在或者没有被用于CP CIoT优化。因此,原样的RRC连接重新建立和RRC连接挂起/恢复步骤用于处理CP CIoT中的移动性在安全性方面是不可接受的。

[0116] 在3GPP的贡献S3-161717中描述的方案提出了认证标志将基于新的RRC完整性密钥(被称为KeNB-RRC),该新的RRC完整性密钥能够由UE 1和移动性管理实体(MME) 4二者导出,而无需经由AS安全模式命令(SMC)步骤在UE 1与源eNB 2之间建立AS安全(包括RRC安全),并且该标志将在UE 1和目标eNB 3之间使用。然而,3GPP的贡献S3-161717中描述的方案试图解决如何向eNB显示真正的UE 1想要重新建立RRC连接的问题。未考虑如何向UE 1显示UE 1连接到了真正的eNB的问题。

[0117] 在缺少安全、以及因此缺少从eNB至UE的DL RRC消息的完整性保护时,在CP CIoT移动性的上下文中,当前没有办法向UE显示UE连接到了真正的eNB。为了减轻这一问题,提出了在从网络至UE的DL方向上使用认证标志。能够由MME、源eNB或目标eNB生成并发送该认证标志。根据在哪个实体上发送DL认证标志,可以使用NAS或AS密钥(但是后者不在本申请的权利要求的范围之内)计算该DL认证标志。识别以下情况:

[0118] 总是经由目标eNB向UE发送DL认证标志。

[0119] 以下四种变化的方案示出了如何实现这一目的。

[0120] 1a:DL认证标志从源eNB经由目标eNB发送至UE且由UE利用AS密钥进行检验。备选地,目标eNB利用从源eNB接收的Krrc_int密钥计算标志。这种变化不在本申请的权利要求的范围之内。

[0121] 1b:DL认证标志从MME经由源eNB和目标eNB发送至UE且由UE利用NAS密钥进行检验。

[0122] 2a:DL认证标志在路径切换确认消息中从MME经由目标eNB发送至UE且UE利用NAS密钥检验该DL认证标志。

[0123] 2b:DL认证标志在新消息中从MME经由目标eNB发送至UE且UE利用NAS密钥检验该标志。

[0124] 当UE基于DL认证标志做出UE连接到了真正的eNB的检验时,根本无需建立AS密钥。因此,能够避免AS密钥的生成,这是有益的,因为否则将只能必须生成用于RRC连接的重新

建立且不能用作它用的AS密钥。然而,NAS密钥还能够用于除仅认证eNB之外的其它安全问题。更准确地,无论如何NAS密钥都被创建了,因为存在用于在NAS上发送数据的UE的NAS安全上下文。

[0125] 参见图2,当UE在CP CIoT (DoNAS) 连接期间经历无线电链路失败 (RLF) 时,UE试图与另一个eNB重新建立RRC连接。

[0126] CP CIoT中使用的网络的认证标志(表示为MAC CIoT DL)是将用于网络的认证的标志,即,用于向UE 1显示UE 1连接到了真正的目标eNB 3。

[0127] 根据要求保护的发明的各方面,可以利用以下作为输入来计算MAC CIoT DL:

[0128] -NAS完整性密钥(NAS-int,例如, K_{NASint})。在其它变化中,虽然在本申请中没有声明,但也可以是AS完整性密钥或根据NAS-int或AS完整性密钥(K_{rrc_int}) 导出的密钥或根据这些密钥的任一个导出的密钥。NAS-int在以下文字的许多实例中被表示为Key-MAC CIoT DL。NAS或AS密钥的使用取决于MAC CIoT DL是由MME 4还是由eNB计算的。在本申请的权利要求的范围之外的其它备选的密钥是,用于NAS-int的根密钥(root key) (例如,LTE中的KASME,以及新无线电系统中的KAUSF、KSEAF和KAMF)。

[0129] -目标小区的标识(cell-ID)。

[0130] -源小区的物理小区标识。

[0131] -源小区处的UE的C-RNTI。

[0132] -常数(该常数允许MAC CIoT与ShortResumeMAC-I和ShortMAC-I或以其它方法定义的MAC的区分)。

[0133] -MAC CIoT DL计算的可能的输入是上行链路UL认证标志,本文中称为MAC CIoT UL(上行链路)。

[0134] -新鲜度(freshness) 参数。

[0135] 用于MAC CIoT DL的计算的输入将被表示为Input-MAC CIoT DL。目标小区的标识因此可以是Input-MAC CIoT DL的一部分,但是NAS完整性密钥与由UE接收的Input-MAC CIoT DL可以是分离的,这是因为通常它已经有了NAS完整性密钥且将其用于了MAC CIoT UL的计算。

[0136] 用于MAC CIoT DL的计算的函数(表示为Fun-MAC CIoT DL)可以与用于RRC重新建立和RRC恢复的TS 33.401的附录B.2中使用的(即,NAS 128比特完整性算法(可以是128-EIA1、128-EIA2和128-EIA3)形式的完整性算法)相同。

[0137] 在图3A和图3B中示出了变化1a,其中,MAC CIoT DL从源eNB发送且由UE利用AS密钥(不在本申请的权利要求的范围之内)或NAS密钥进行检验。

[0138] 这种变化基于经由NAS协议的AS算法的协商和后续对源eNB中的被称为MAC CIoT UL的上行链路标志的检验。该变化包括:源eNB在检验了MAC CIoT UL之后生成被称为MAC CIoT DL的下行链路标志的机制。源eNB在X2 UE上下文响应消息中向目标eNB发送MAC CIoT DL。目标eNB在用于认证检验的RRC消息中进一步向UE发送MAC CIoT DL。如果MAC CIoT DL的检验是成功的,则UE知道其连接到了可信的(authentic) eNB,而不是假的eNB。

[0139] 在当前的3GPP规范中定义了步骤1至步骤15。UE建立RRC连接且在NAS上发送数据,数据从MME转发至服务网关(S-GW)/分组数据网络网关(P-GW)。在步骤15中发生RLF。RLF也能够在UE接收到DL数据之前发生。

- [0140] 步骤16:UE通过向目标eNB发送随机接入消息发起RRC连接。
- [0141] 步骤17:目标eNB利用随机接入响应向UE响应。
- [0142] 步骤18:UE生成认证标志MAC CIoT UL。可以用以下方式计算该标志:标志=f(源PCI,源C-RNTI,目标Cell-ID,NAS密钥,重放输入),其中NAS密钥是当前的NAS完整性密钥(例如, K_{NASint} 、或其导出物),f=函数。然而,对于这种特定的变化1a,可以通过AS密钥代替NAS密钥导出该标志。AS密钥可以是AS完整性密钥(例如, K_{RRCint})。
- [0143] 步骤19:UE向目标eNB发送RRC连接重新建立消息,例如,用于CP IoT EPS(演进的分组系统)优化。该消息包括MAC CIoT UL。
- [0144] 步骤20:目标eNB向源eNB发送X2 UE上下文请求消息。该消息包括MAC CIoT UL。
- [0145] 步骤21:源eNB检验MAC CIoT UL是否是可信的。
- [0146] 步骤22:如果认证是成功的,则如上文所述,源eNB使用Input-MAC CIoT DL和Key-MAC CIoT DL生成MAC CIoT DL且继续步骤23中的处理。如果认证失败,则源eNB发送指示失败的X2 UE上下文响应。该失败将触发目标eNB释放RRC连接(未示出)。
- [0147] 步骤23:源eNB向目标eNB发送X2 UE上下文响应。该消息包括MAC CIoT DL。该消息可以还包括Input-MAC CIoT DL。
- [0148] 步骤24:目标eNB向UE发送RRC连接重新建立消息。该消息包括MAC CIoT DL。该消息可以还包括Input-MAC CIoT DL。
- [0149] 步骤25:在接收RRC连接重新建立消息之后,如上文所述,UE使用Input-MAC CIoT DL和Key-MAC CIoT DL认证MAC CIoT DL。
- [0150] 步骤26A:如果MAC CIoT DL认证是成功的。
- [0151] 26A.1:UE向目标eNB发送RRC连接重新建立完成消息(可选地,包含NAS数据PDU)。
- [0152] 步骤26A.2-步骤26A.5:这些步骤是正常的路径切换和承载修改步骤。
- [0153] 26A.6:目标eNB现在通过发送被称为UE上下文释放的X2消息告知源eNB释放UE上下文。
- [0154] 如果步骤25中的MAC CIoT DL的认证失败,则UE可以执行动作,如,不发送另外的消息、或转变至RRC_CONNECTED模式以认证网络等。
- [0155] 在图4A-图4B中示出了变化1b,其中,MAC CIoT DL从MME向源eNB、并从源eNB向目标eNB、并从目标eNB向UE发送,并且随后由UE利用NAS密钥进行检验。
- [0156] 例如,这个示例适用于RLF发生在用于CP IoT优化的NAS数据的发送期间的情形。
- [0157] 在当前的3GPP规范中定义了步骤1至步骤18。
- [0158] 步骤19:UE向目标eNB发送包括MAC CIoT UL的RRC消息。所述RRC消息可以是RRC连接重新建立请求、RRC恢复请求、或一些其它的RRC消息。
- [0159] 步骤20:目标eNB向源eNB发送包括MAC CIoT UL的X2消息。所述X2消息可以是X2上下文获取消息。
- [0160] 步骤21:源eNB向MME发送包括MAC CIoT UL和Input-MAC CIoT UL的S1消息。
- [0161] 步骤22:在接收MAC CIoT UL和Input-MAC CIoT UL之后,MME通过执行与UE执行的相同的计算并将它与接收到的MAC CIoT UL进行比较来验证MAC CIoT UL。如果验证是成功的,则如上文所述,MME使用Input-MAC CIoT DL和Key-MAC CIoT DL生成MAC CIoT DL,且继续步骤23中的处理,其中,MME向源eNB发送指示成功且包括MAC CIoT DL的S1消息。如果验

证是不成功的,则MME向源eNB发送指示错误的S1消息。源eNB随后发送指示失败的X2 UE上下文响应。该失败将触发目标eNB释放RRC连接(未示出)。

[0162] 步骤23:MME向源eNB发送指示成功的S1检验响应消息。该消息包括MAC CIoT DL。该消息可以还包括Input-MAC CIoT DL。

[0163] 步骤24:源eNB向目标eNB发送UE上下文响应。该消息包括MAC CIoT DL。该消息可以还包括Input-MAC CIoT DL。

[0164] 步骤25:目标eNB向UE发送RRC连接重新建立消息。该消息包括MAC CIoT DL。该消息可以还包括Input-MAC CIoT DL。

[0165] 步骤26:在接收RRC连接重新建立消息之后,如上文所述,UE使用Input-MAC CIoT DL和Key-MAC CIoT DL认证MAC CIoT DL。

[0166] 步骤27A:如果MAC CIoT DL认证是成功的,

[0167] 27A.1:UE向目标eNB发送RRC连接重新建立完成消息(可选地,包含NAS数据PDU)。

[0168] 步骤27A.2-27A.5:这些步骤是正常的路径切换和承载修改步骤。

[0169] 27A.6:目标eNB现在通过发送被称为UE上下文释放的X2消息告知源eNB释放UE上下文。

[0170] 如果步骤25中的MAC CIoT DL的认证失败,则UE可以执行动作,如,不发送另外的消息、或转变至RRC_CONNECTED模式以认证网络等。

[0171] 在图5中示出了变化2a,其中,在S1AP路径切换请求确认消息中从MME向目标eNB发送MAC CIoT DL。从目标eNB向UE发送MAC CIoT DL。

[0172] 这种变化基于从MME向目标eNB发送的被称为路径切换请求确认的已有的S1AP消息。路径切换请求确认被修改成能够承载MAC CIoT DL和Input-MAC CIoT DL。对于本领域技术人员将明显的是,这些步骤、消息和字段的次序可以改变;消息可以被组合;字段可以放在不同的消息中等;以实现相同的效果。

[0173] 步骤1-步骤17与如上结合图3A所述的相同。

[0174] 步骤18-步骤19也与如上结合图3A所述的相同,但是为了RRC连接重新建立步骤的完整在图5中也示出了这些步骤。

[0175] 步骤20:目标eNB请求源eNB发送UE的上下文。被称为获取UE上下文请求的已有的X2消息可以根据需要修改(例如,使用ReestabUE-Identity代替ResumeIdentity)。

[0176] 步骤21:源eNB向目标eNB发送UE的上下文。被称为获取UE上下文响应的已有的X2消息可以根据需要修改。

[0177] 步骤22:目标eNB向UE发送RRC连接重新建立消息。

[0178] 步骤23:UE向目标eNB发送RRC连接重新建立完成消息(可选地,包含NAS数据PDU(协议数据单元))。

[0179] 步骤24:目标eNB向MME发送路径切换请求。目标eNB在路径切换请求中包括了MAC CIoT UL和Input-MAC CIoT UL。如上所述,Input-MAC CIoT UL可以包括目标小区的标识。目标eNB在步骤19中接收MAC CIoT UL。Input-MAC CIoT UL可以包括在步骤19和/或步骤21中接收目标eNB的信息、和/或目标eNB自己的信息。路径切换请求可以包含使MME能够在MME中识别UE的上下文的UE的信息。该UE的信息现在被称为目标eNB能够根据其在步骤23中接收的信息提供的“源MME UE S1AP ID”。

[0180] 步骤25:例如,通过使用Input-MAC CIoT UL和Key-MAC CIoT UL作为对Fun-MAC CIoT UL的输入,MME认证MAC CIoT UL。在一实施例中的Key-MAC CIoT UL与Key-MAC CIoT DL(即,可以由MME和UE分别基于KASME独立地导出的NAS完整性密钥)相同,这是本领域技术人员已知的。

[0181] 在下文中,为了简单,仅进一步描述了与本方案相关的步骤,即,如果在步骤25中的认证成功,则这些步骤是:

[0182] 步骤26:如上文所述,MME使用Input-MAC CIoT DL和Key-MAC CIoT DL生成MAC CIoT DL。Input-MAC CIoT DL中的一些元素(像目标小区的标识(cell-ID))可以从Input-MAC CIoT UL中获得。

[0183] 步骤27:MME向目标eNB发送S1消息-指示成功的路径切换请求确认消息,且该路径切换请求确认消息被调整为包括MAC CIoT DL和Input-MAC CIoT DL。

[0184] 步骤28:目标eNB现在知道了由UE发送且在之前的步骤中提及的MAC CIoT UL是可信的。目标eNB在RRC消息中向UE发送MAC CIoT DL和Input-MAC CIoT DL(例如,通过将它们放在RRC DL信息传递步骤的DLInformationTransfer消息的DedicatedInfoNAS字段中)。为了向UE传送MAC CIoT DL的该特定目的,引入了一种新的RRC步骤(例如,RRC重新建立确认)。

[0185] 步骤29:UE使用Input-MAC CIoT DL和Key-MAC CIoT DL作为对Fun-MAC CIoT DL的输入,认证MAC CIoT DL。

[0186] 如果步骤27中的MAC CIoT DL的认证失败,则UE可以执行动作,如,不发送另外的消息、或转变至RRC_CONNECTED模式以认证网络等。

[0187] 在图6中示出了变化2b,其中,在新的S1AP消息中从MME向目标eNB发送、并从目标eNB向UE发送MAC CIoT DL。

[0188] 这种变化基于从目标eNB向MME发送的新的S1AP消息(表示为检验MAC请求)。检验MAC请求消息能够承载MAC CIoT UL和Input-MAC CIoT UL。类似地,从目标eNB向MME发送的新的S1AP消息(表示为检验MAC确认和检验MAC失败)被用于分别指示MAC CIoT UL是可信的或是不可信的。新的S1AP消息“检验MAC确认”承载从MME至目标eNB的MAC CIoT DL和Input-MAC CIoT DL。目标eNB在RRC连接重新建立消息中包括去往UE的MAC CIoT DL和Input-MAC CIoT DL。本领域技术人员将明显注意到的是,这些步骤、消息和字段的次序可以改变;消息可以被组合;字段放在不同的消息中等,以实现相同的效果。

[0189] 步骤1-步骤17与如上结合图3A所讨论的相同。

[0190] 步骤18-步骤19与上文讨论的相同,只是为了RRC连接重新建立步骤的完整而示出。

[0191] 步骤20:目标eNB请求源eNB发送UE的上下文。被称为获取UE上下文请求的已有的X2消息可以根据需要修改(例如,使用ReestabUE-Identity代替ResumeIdentity)。

[0192] 步骤21:源eNB向目标eNB发送UE的上下文。被称为获取UE上下文响应的已有的X2消息可以根据需要修改。UE的上下文告知目标eNB该UE所注册到的对应MME。

[0193] 步骤22:目标eNB以检验MAC请求的形式向MME发送在步骤21中识别的消息。目标eNB在检验MAC请求中包括MAC CIoT UL和Input-MAC CIoT UL。目标eNB在步骤19中接收MAC CIoT UL。Input-MAC CIoT UL可以包括目标eNB在步骤19和/或步骤21中接收的信息、和/或

目标eNB自己的信息, Input-MAC CIoT UL中包括的这些信息可以是目标小区的标识, 这些信息因此已经与至少NAS完整性密钥一起作为输入使用, 以生成UL认证标志MAC CIoT UL。检验MAC请求可以包含使MME能够在MME中识别UE的上下文的UE的信息。例如, 该UE的信息可以是目标eNB在步骤21中从源eNB接收的MME UE S1AP ID。

[0194] 步骤23: MME使用Input-MAC CIoT UL和Key-MAC CIoT UL (例如, 相同的NAS完整性密钥用作Key-MAC CIoT DL) 作为对Fun-MAC CIoT UL的输入, 认证MAC CIoT UL。换言之, Fun-MAC CIoT UL的结果与所接收的MAC CIoT UL比较, 以验证所接收的MAC CIoT UL。

[0195] 在下文中, 为了简单, 仅进一步描述了关于本方案的步骤, 即, 如果在步骤23中的认证成功, 则这些步骤是:

[0196] 步骤24: 如上文所述, MME使用Input-MAC CIoT DL和Key-MAC CIoT DL生成MAC CIoT DL。Input-MAC CIoT DL中的一些元素 (像目标小区的标识) 可以从Input-MAC CIoT UL中获得。MME向目标eNB发送指示成功且包括CIoT DL和Input-MAC CIoT DL的S1消息 (检验MAC确认消息)。

[0197] 步骤25: MME向目标eNB发送检验MAC请求确认消息。该消息包括MAC CIoT DL且可选地还包括Input-MAC CIoT DL。目标eNB现在知道了在之前的步骤中提及的MAC CIoT UL是可信的。

[0198] 步骤26: 目标eNB向UE发送RRC连接重新建立消息。该消息包括MAC CIoT DL且可以包括Input-MAC CIoT DL。

[0199] 步骤27: UE使用Input-MAC CIoT DL和Key-MAC CIoT DL作为对Fun-MAC CIoT DL的输入, 认证MAC CIoT DL。

[0200] 步骤28: 如果步骤27中的MAC CIoT DL的认证是成功的, 则UE向目标eNB发送RRC连接重新建立完成消息 (可选地, 包含NAS数据PDU)。

[0201] 如果步骤27中的MAC CIoT DL的认证失败, 则UE可以执行一些动作, 如, 不发送另外的消息、或转变至RRC_CONNECTED模式以认证网络等。

[0202] 参考图7A提出了根据实施例的用于在UE与目标eNB之间重新建立RRC连接的方法。所述方法由UE 1执行且包括: 从目标eNB 3接收S100RRC连接重新建立消息 (例如, 用于CP IoT优化), 该RRC连接重新建立消息包括DL认证标志, 该DL认证标志由MME 4生成且将NAS完整性密钥作为输入; 以及认证S110所接收的DL认证标志。

[0203] 包括DL认证标志的RRC连接重新建立消息可以可选地还包括Input-MAC CIoT DL, 且所接收的DL认证标志可以通过使用所接收的Input-MAC CIoT DL和NAS完整性密钥进行认证。

[0204] 所述RRC消息可以是包括MAC CIoT DL和 (可选的) Input-MAC CIoT DL的RRC DL信息传递消息, 且所接收的MAC CIoT DL可以通过使用Input-MAC CIoT DL和Key-MAC CIoT DL进行认证。

[0205] 在S100之前的可选步骤S80中, UE利用NAS完整性密钥作为输入计算UL认证标志 (在图7A中被称为ULAT), 并且在可选步骤S90中向目标eNB 3发送包括UL认证标志的RRC连接重新建立请求。UL认证标志可以利用目标小区的标识作为输入计算, 并且目标小区的标识可以包括在RRC连接重新建立请求中 (例如, 作为Input-MAC UL的一部分)。

[0206] 参考图7B提出了根据实施例的 (例如, 用于CP IoT优化的) 用于在UE与目标eNB之

间重新建立RRC连接的方法。所述方法由目标eNB 3执行且包括：从MME 4接收S300包括由MME生成的DL认证标志的消息，其中，该DL认证标志利用非接入层完整性密钥作为输入生成；以及向UE 1发送S310包括该DL认证标志的RRC连接重新建立消息。

[0207] 在S300之前的可选步骤S280中，目标eNB从UE 1接收包括UL认证标志的RRC连接重新建立请求，其中，该UL认证标志由UE1利用NAS完整性密钥作为输入来计算。在一个实施例中，UL认证标志连同Input-MAC CIoT UL一起包括目标小区的标识。在S300之前的可选步骤S290中，目标eNB可选地利用包括目标小区的标识的Input-MAC CIoT UL，向MME 4发送/转发UL认证标志。

[0208] 已发送的RRC连接重新建立消息可以包括Input-MAC CIoT DL。

[0209] 所接收的消息可以是包括Input-MAC CIoT DL的临时性线路切换请求确认消息。

[0210] 所接收的消息可以是包括Input-MAC CIoTDL的检验MAC确认消息。

[0211] 参考图7C提出了根据实施例的（例如，用于CP IoT优化的）用于在UE与目标eNB之间重新建立RRC连接的方法。所述方法在源eNB 2中执行且包括：获得S200利用NAS完整性密钥作为输入生成的DL认证标志；以及向目标eNB 3发送S210响应消息，该响应消息包括已获得的DL认证标志。

[0212] 所述获得S200可以包括生成DL认证标志、或从MME 4接收S1检验响应消息，所接收的S1检验响应包括DL认证标志且可选地还包括Input-MAC CIoT DL。

[0213] 该响应消息可以是X2 UE上下文响应消息。

[0214] 参考图7D提出了根据实施例的（例如，用于CP IoT优化的）用于在UE与目标eNB之间重新建立RRC连接的方法。所述方法由MME4执行且包括：利用NAS完整性密钥作为输入生成S400 DL认证标志；以及向目标eNB 3发送S410包括已生成的DL认证标志的消息。DL认证标志还可以利用目标小区的标识作为输入而生成。

[0215] 在S400之前的可选步骤S380中，MME从目标eNB 3接收UL认证标志，所述UL认证标志由UE 1利用NAS完整性密钥作为输入而生成，且在可选步骤S390中，MME例如通过以与UE所采用的相同的方式计算第二UL认证标志（例如，利用NAS完整性密钥和目标小区的标识作为输入）并且随后比较第二UL认证标志与从目标eNB所接收的UL认证标志来验证UL认证标志。

[0216] 所述消息可以是路径切换请求确认消息且包括Input-MAC CIoT DL。

[0217] 所述消息可以是包括Input-MAC CIoT DL的检验MAC确认消息。

[0218] 参考图8提出了根据实施例的用于在UE 1与目标eNB 3之间重新建立RRC连接的UE 1。UE 1包括处理器10和计算机程序产品。计算机程序产品存储有指令，所述指令在由处理器执行时使UE：从目标eNB 3接收RRC连接重新建立消息，该RRC连接重新建立消息包括DL认证标志，该DL认证标志由MME 4生成且将NAS完整性密钥作为输入；以及认证所接收的DL认证标志。

[0219] RRC连接重新建立消息可以可选地包括Input-MAC CIoT DL，且所接收的DL认证标志可以通过使用Input-MAC CIoT DL和NAS完整性密钥进行认证。

[0220] 参考图9提出了根据实施例的用于在UE 1与目标eNB 3之间重新建立RRC连接的源eNB。源eNB 2包括处理器20和计算机程序产品。计算机程序产品存储有指令，所述指令在由处理器执行时使源eNB：获得利用NAS完整性密钥作为输入生成的DL认证标志；以及向目标

eNB 3发送响应消息,该响应消息包括已获得的DL认证标志。

[0221] 该响应消息可以是X2 UE上下文响应消息。

[0222] 参考图10提出了根据实施例的用于在UE 1与目标eNB 3之间重新建立RRC连接的目标eNB。目标eNB 3包括处理器30和计算机程序产品。计算机程序产品存储有指令,所述指令在由处理器执行时使目标eNB:从MME 4接收包括由MME 4生成的DL认证标志的消息,其中,所述DL认证标志利用NAS完整性密钥作为输入而生成;以及向UE 1发送RRC连接重新建立消息,所述RRC连接重新建立消息包括所述DL认证标志。在一个实施例中,DL认证标志由MME 4利用目标小区的标识作为输入来计算。

[0223] 已发送的RRC连接重新建立消息可选地包括Input-MAC CIoT DL,Input-MAC CIoT DL可以包括目标小区的标识。

[0224] 所接收的消息可以是包括Input-MAC CIoT DL的临时性线路切换请求确认消息。

[0225] 所接收的消息可以是包括Input-MAC CIoT DL的检验MAC确认消息。

[0226] 参考图11提出了根据实施例的用于在UE 1与目标eNB 3之间重新建立RRC连接的MME。MME 4包括处理器40和计算机程序产品。计算机程序产品存储有指令,所述指令在由处理器执行时使MME:利用NAS完整性密钥作为输入生成DL认证标志;以及向目标eNB 3发送包括已生成的DL认证标志的消息。

[0227] 所述消息可以是路径切换请求确认消息,所述消息包括Input-MAC CIoT DL。

[0228] 所述消息可以是检验MAC确认消息,所述消息包括Input-MAC CIoT DL。

[0229] 图8是示出了UE 1的一些组件的示意图。可以使用能够执行存储在存储器中的计算机程序14的软件指令的合适的中央处理单元(CPU)、多处理器、微控制器、数字信号处理器(DSP)、专用集成电路等中的一个或多个的任何组合来提供处理器10。存储器因此可以被认为是计算机程序产品12的一部分或形成计算机程序产品12的一部分。处理器10可以被配置为执行本文参考图7A描述的方法。

[0230] 存储器可以是读写存储器(RAM)和只读存储器(ROM)的任意组合。存储器还可以包括持久存储设备,其例如可以是磁存储器、光存储器、固态存储器或甚至远程安装存储器中的任意单独一个或组合。

[0231] 还可以提供数据存储器形式的第二计算机程序产品13,例如,用于在处理器10中执行软件指令期间读取和/或存储数据。数据存储器可以是读写存储器(RAM)和只读存储器(ROM)的任何组合,并且还可以包括持久存储设备,其例如可以是磁存储器、光存储器、固态存储器或甚至远程安装存储器中的任意单独一个或组合。数据存储器可以例如保存其它软件指令15,以改进UE 1的功能。

[0232] UE 1还可以包括输入/输出(I/O)接口11,输入/输出(I/O)接口11包括例如用户接口。UE 1可以还包括被配置为从其它节点接收信令的接收机、以及被配置为向其它节点传输信令的发射机(未示出)。UE 1的其它组件被省略,以便不会模糊本文提出的构思。

[0233] 图12是示出了UE 1的功能块的示意图。模块可以仅被实现为诸如在高速缓存服务器中执行的计算机程序之类的软件指令或者仅被实现为诸如专用集成电路、现场可编程门阵列、离散逻辑组件、收发机等之类的硬件,或者实现为其组合。在备选实施例中,一些功能块可以由软件实现,而另一些功能块可以由硬件实现。这些模块对应于图7A中示出的方法中的步骤,包括确定管理器单元60和通信管理器单元61。应该理解的是,在一个或多个模块

由计算机程序实现的实施例，这些模块不一定对应于处理模块，而是可以根据其将被实现的编程语言编写为指令，因为一些编程语言通常不包含处理模块。

[0234] 确定管理器60用于实现在UE与目标eNB之间重新建立RRC连接。该模块与图7A的步骤S110(即，对所接收的DL认证标志的认证)对应。该模块可以例如在运行计算机程序时由图8的处理器10实现。

[0235] 通信管理器61用于实现在UE与目标eNB之间重新建立RRC连接。该模块与图7A的接收步骤S100对应。该模块可以例如在运行计算机程序时由图12的处理器10实现。

[0236] 图9是示出了源eNB2的一些组件的示意图。可以使用能够执行存储在存储器中的计算机程序24的软件指令的合适的中央处理单元(CPU)、多处理器、微控制器、数字信号处理器(DSP)、专用集成电路等中的一个或多个的任何组合来提供处理器20。存储器因此可以被认为是计算机程序产品22的一部分或形成计算机程序产品22的一部分。处理器20可以被配置为执行本文参考图7B描述的方法。

[0237] 存储器可以是读写存储器(RAM)和只读存储器(ROM)的任意组合。存储器还可以包括持久存储设备，其例如可以是磁存储器、光存储器、固态存储器或甚至远程安装存储器中的任意单独一个或组合。

[0238] 还可以提供数据存储器形式的第二计算机程序产品23，例如，用于在处理器20中执行软件指令期间读取和/或存储数据。数据存储器可以是读写存储器(RAM)和只读存储器(ROM)的任何组合，并且还可以包括持久存储设备，其例如可以是磁存储器、光存储器、固态存储器或甚至远程安装存储器中的任意单独一个或组合。数据存储器可以例如保存其它软件指令25，以改进源eNB 2的功能。

[0239] 源eNB 2还可以包括输入/输出(I/O)接口21，输入/输出(I/O)接口21包括例如用户接口。源eNB 2可以还包括被配置为从其它节点接收信令的接收机、以及被配置为向其它节点传输信令的发射机(未示出)。源eNB 2的其它组件被省略，以便不模糊本文提出的构思。

[0240] 图13是示出了源eNB 2的功能块的示意图。模块可以仅被实现为诸如在高速缓存服务器中执行的计算机程序之类的软件指令或者仅被实现为诸如专用集成电路、现场可编程门阵列、离散逻辑组件、收发机等之类的硬件，或者实现为其组合。在备选实施例中，一些功能块可以由软件实现，而另一些功能块可以由硬件实现。这些模块对应于图7C中示出的方法中的步骤，包括确定管理器单元70和通信管理器单元71。应该理解的是，在一个或多个模块由计算机程序实现的实施例中，这些模块不一定对应于处理模块，而是可以根据其将被实现的编程语言编写为指令，因为一些编程语言通常不包含处理模块。

[0241] 确定管理器70用于实现在UE与目标eNB之间重新建立RRC连接。该模块与图7C的获得步骤S200对应。该模块可以例如在运行计算机程序时由图9的处理器20实现。

[0242] 通信管理器71用于实现在UE与目标eNB之间重新建立RRC连接。该模块与图7C的发送步骤S210对应。该模块可以例如在运行计算机程序时由图13的处理器20实现。

[0243] 图10是示出了目标eNB 3的一些组件的示意图。可以使用能够执行存储在存储器中的计算机程序34的软件指令的合适的中央处理单元(CPU)、多处理器、微控制器、数字信号处理器(DSP)、专用集成电路等中的一个或多个的任何组合来提供处理器30。存储器因此可以被认为是计算机程序产品32的一部分或形成计算机程序产品32的一部分。处理器30可

以被配置为执行本文参考图7C描述的方法。

[0244] 存储器可以是读写存储器 (RAM) 和只读存储器 (ROM) 的任意组合。存储器还可以包括持久存储设备,其例如可以是磁存储器、光存储器、固态存储器或甚至远程安装存储器中的任意单独一个或组合。

[0245] 还可以提供数据存储器形式的第二计算机程序产品33,例如,用于在处理器30中执行软件指令期间读取和/或存储数据。数据存储器可以是读写存储器 (RAM) 和只读存储器 (ROM) 的任何组合,并且还可以包括持久存储设备,其例如可以是磁存储器、光存储器、固态存储器或甚至远程安装存储器中的任意单独一个或组合。数据存储器可以例如保存其它软件指令35,以改进目标eNB 3的功能。

[0246] 目标eNB 3还可以包括输入/输出 (I/O) 接口31,输入/输出 (I/O) 接口31包括例如用户接口。目标eNB 3可以还包括被配置为从其它节点接收信令的接收机、以及被配置为向其它节点传输信令的发射机(未示出)。目标eNB 3的其它组件被省略,以便不模糊本文提出的构思。

[0247] 图14是示出了目标eNB 3的功能块的示意图。模块可以仅被实现为诸如在高速缓存服务器中执行的计算机程序之类的软件指令或者仅被实现为诸如专用集成电路、现场可编程门阵列、离散逻辑组件、收发机等之类的硬件,或者实现为其组合。在备选实施例中,一些功能块可以由软件实现,而另一些功能块可以由硬件实现。这些模块对应于图7B中示出的方法中的步骤,包括确定管理器单元80和通信管理器单元81。应该理解的是,在一个或多个模块由计算机程序实现的实施例中,这些模块不一定对应于处理模块,而是可以根据其将被实现的编程语言编写为指令,因为一些编程语言通常不包含处理模块。

[0248] 通信管理器81用于实现在UE与目标eNB之间重新建立RRC连接。该模块与图7B的接收步骤S300和发送步骤310对应。该模块可以例如在运行计算机程序时由图10的处理器30实现。

[0249] 图11是示出了MME 4的一些组件的示意图。可以使用能够执行存储在存储器中的计算机程序44的软件指令的合适的中央处理单元 (CPU)、多处理器、微控制器、数字信号处理器 (DSP)、专用集成电路等中的一个或多个的任何组合来提供处理器40。存储器因此可以被认为是计算机程序产品42的一部分或形成计算机程序产品42的一部分。处理器40可以被配置为执行本文参考图7D描述的方法。

[0250] 存储器可以是读写存储器 (RAM) 和只读存储器 (ROM) 的任意组合。存储器还可以包括持久存储设备,其例如可以是磁存储器、光存储器、固态存储器或甚至远程安装存储器中的任意单独一个或组合。

[0251] 还可以提供数据存储器形式的第二计算机程序产品43,例如,用于在处理器40中执行软件指令期间读取和/或存储数据。数据存储器可以是读写存储器 (RAM) 和只读存储器 (ROM) 的任何组合,并且还可以包括持久存储设备,其例如可以是磁存储器、光存储器、固态存储器或甚至远程安装存储器中的任意单独一个或组合。数据存储器可以例如保存其它软件指令45,以改进MME 4的功能。

[0252] MME 4还可以包括输入/输出 (I/O) 接口41,输入/输出 (I/O) 接口41包括例如用户接口。MME 4可以还包括被配置为从其它节点接收信令的接收机、以及被配置为向其它节点传输信令的发射机(未示出)。MME 4的其它部件被省略,以便不模糊本文提出的构思。

[0253] 图15是示出了MME 4的功能模块的示意图。模块可以仅被实现为诸如在高速缓存服务器中执行的计算机程序之类的软件指令或者仅被实现为诸如专用集成电路、现场可编程门阵列、离散逻辑组件、收发机等之类的硬件,或者实现为其组合。在备选实施例中,一些功能块可以由软件实现,而另一些功能块可以由硬件实现。这些模块对应于图7D中示出的方法中的步骤,包括确定管理器单元90和通信管理器单元91。应该理解的是,在一个或多个模块由计算机程序实现的实施例中,这些模块不一定对应于处理模块,而是可以根据其将被实现的编程语言编写为指令,因为一些编程语言通常不包含处理模块。

[0254] 确定管理器90用于实现在UE与目标eNB之间重新建立RRC连接。该模块与图7D的生成步骤400对应。该模块可以例如在运行计算机程序时由图11的处理器40实现。

[0255] 通信管理器91用于实现在UE与目标eNB之间重新建立RRC连接。该模块与图7D的发送步骤410对应。该模块可以例如在运行计算机程序时由图11的处理器40实现。

[0256] 已经参考一些实施例在上文中主要地描述了本发明。然而,如本领域技术人员容易理解的,除了上文所公开的实施例之外的其它实施例同样可能在由所附实施例的项目列表定义的本发明的范围内。

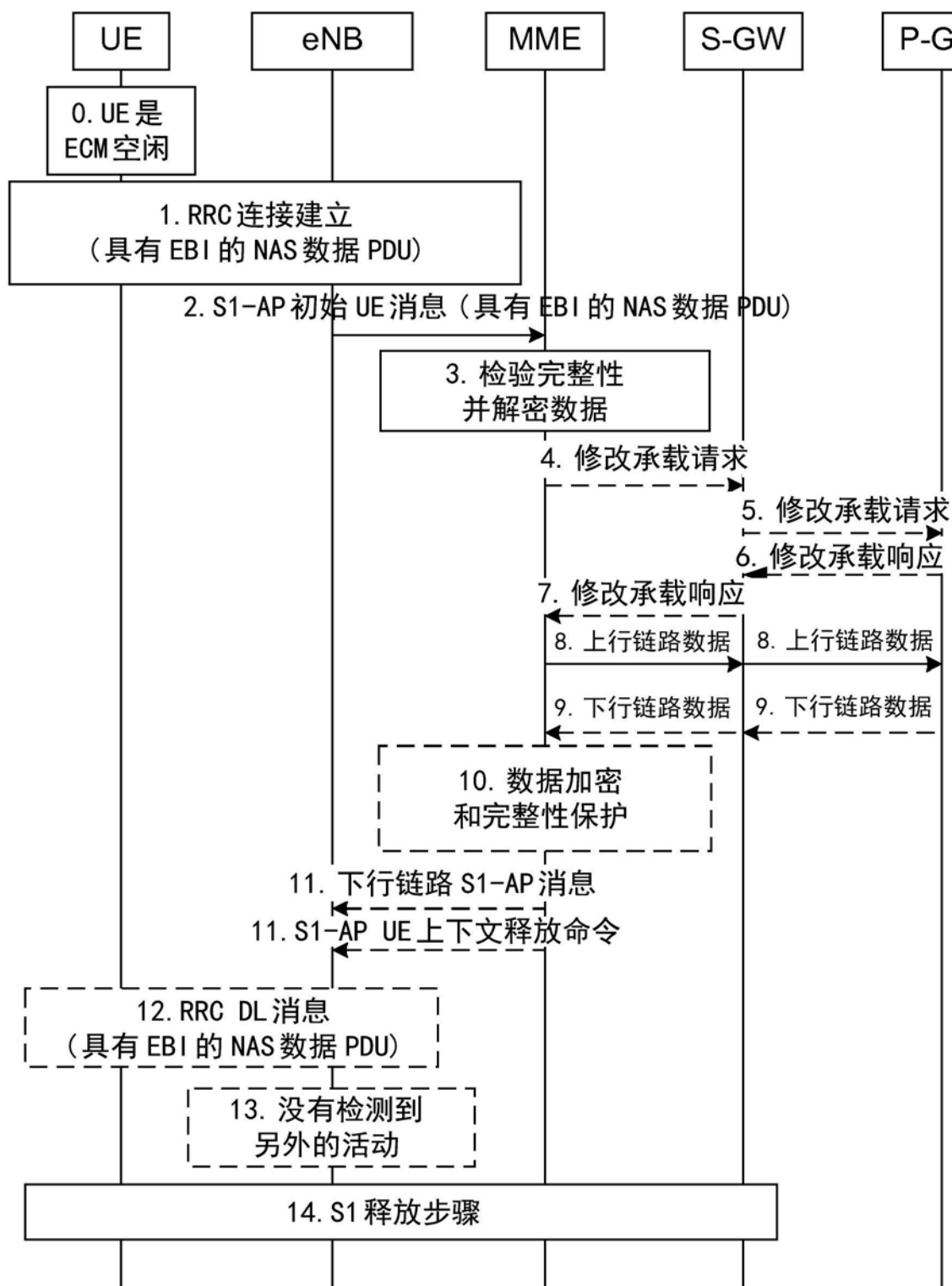


图1

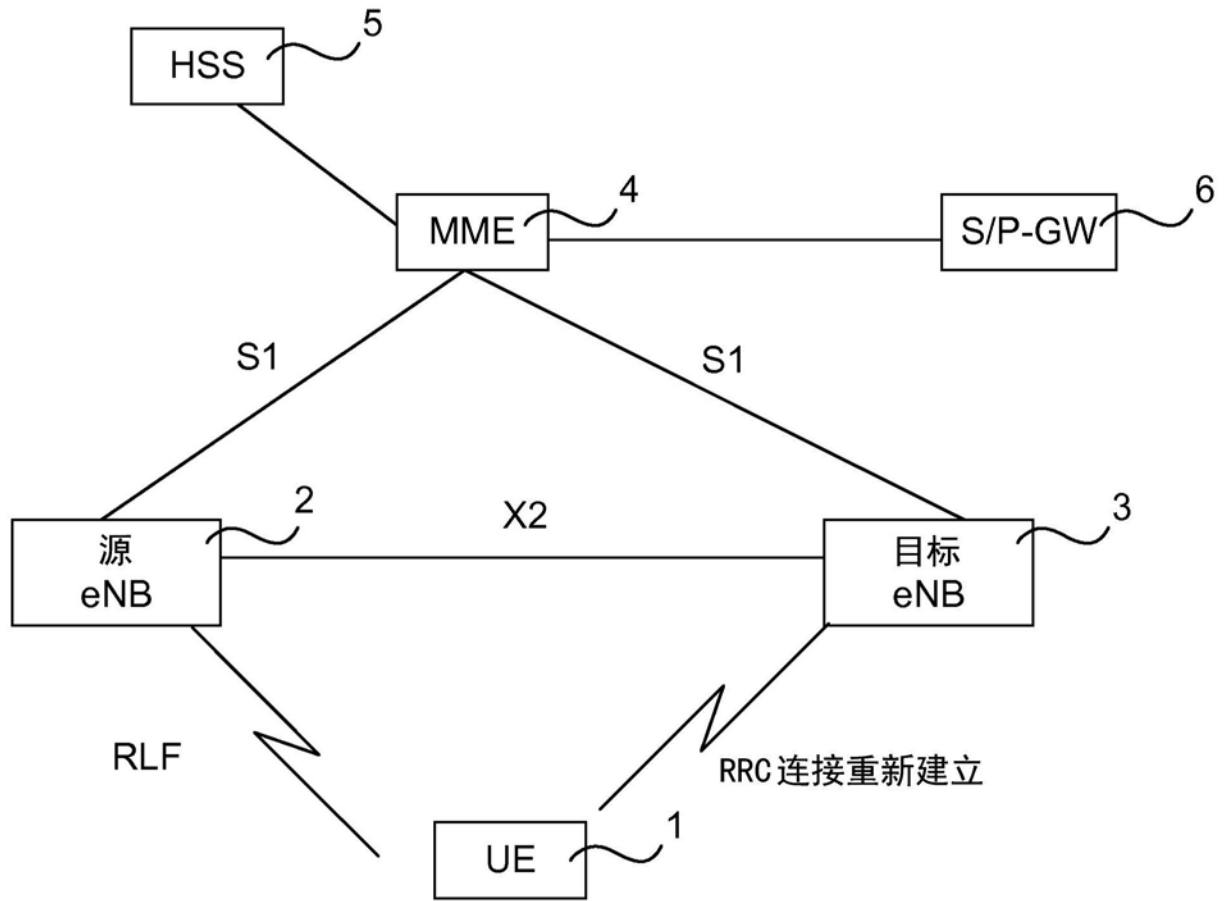


图2

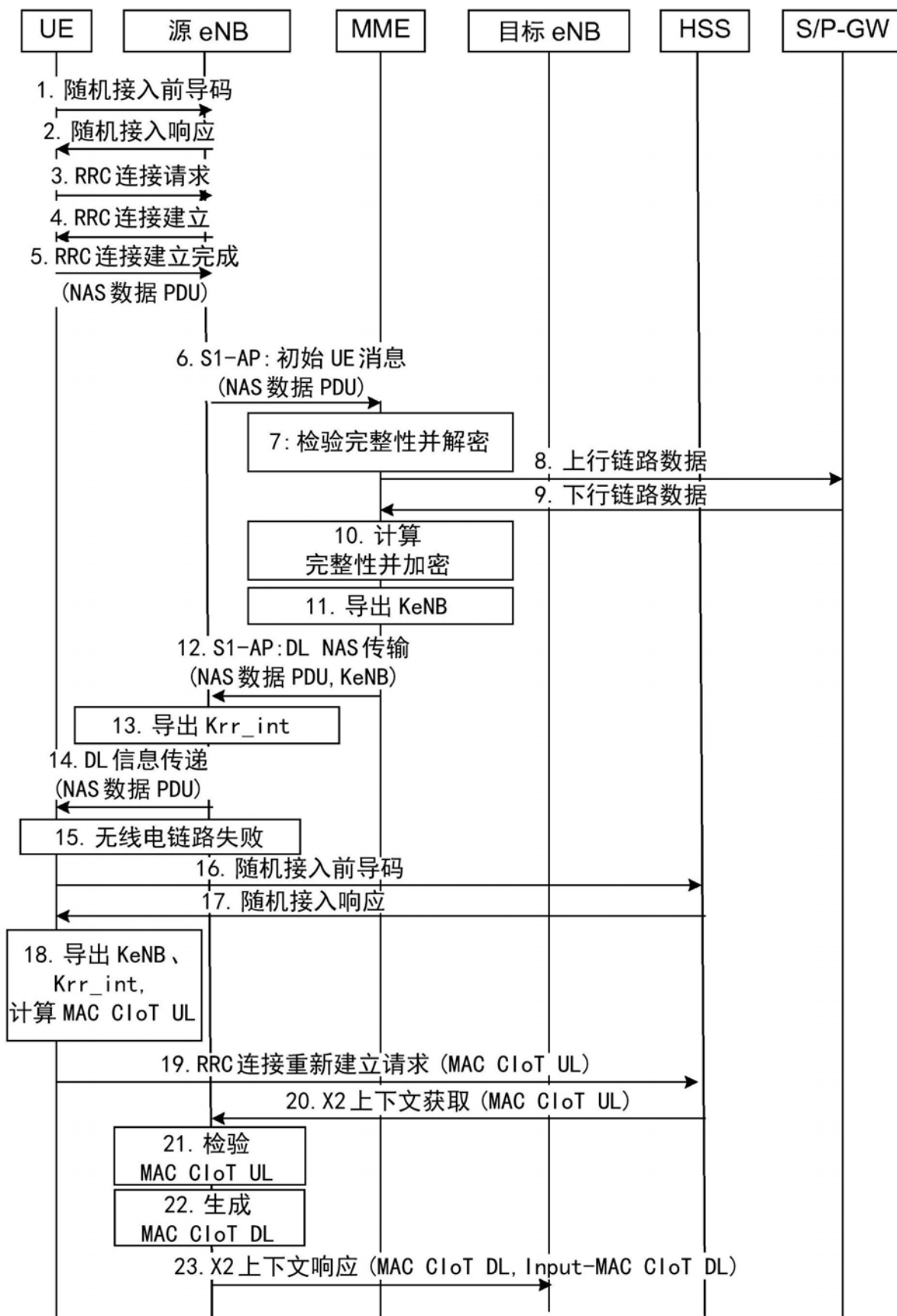


图3A

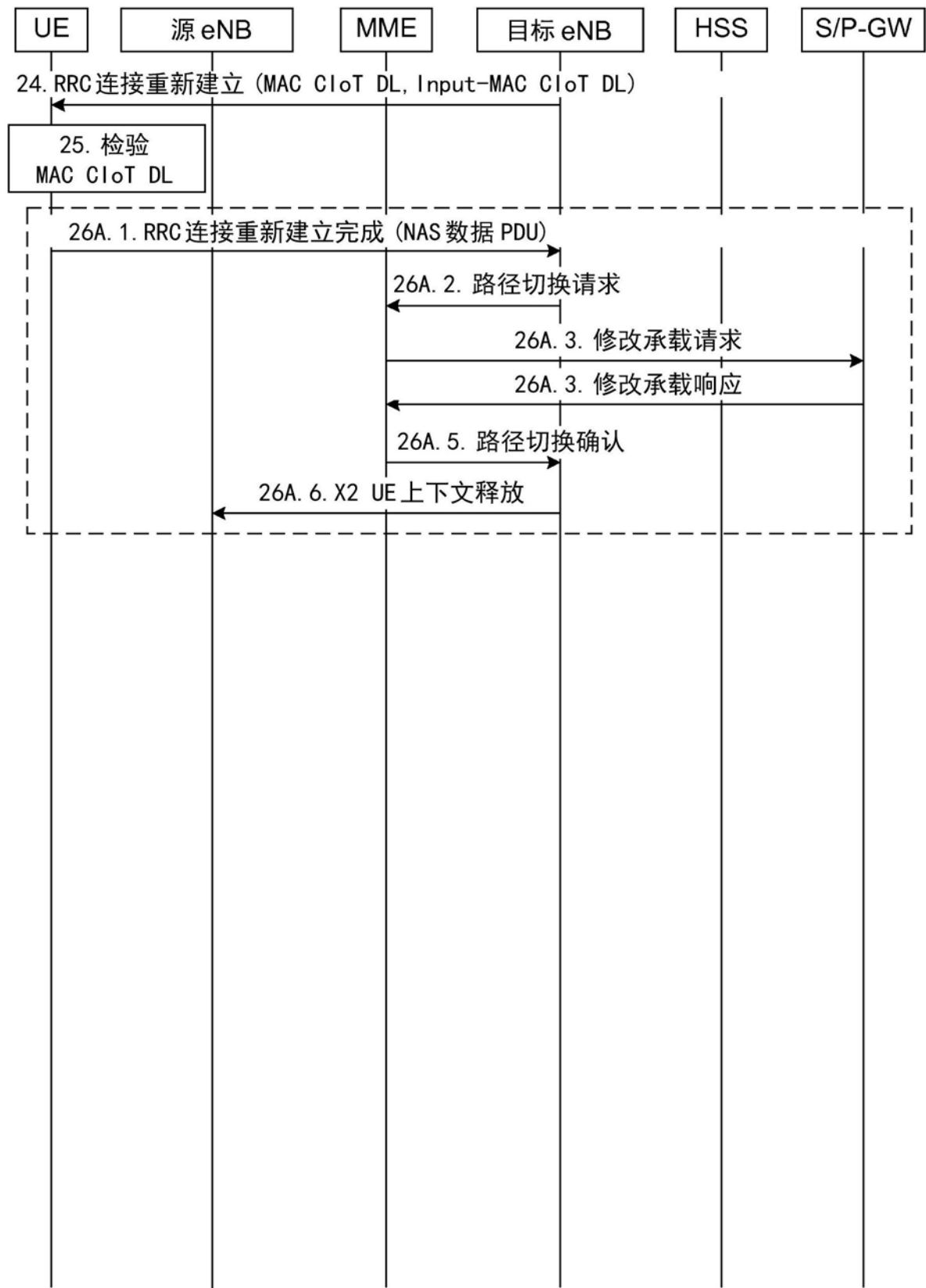


图3B

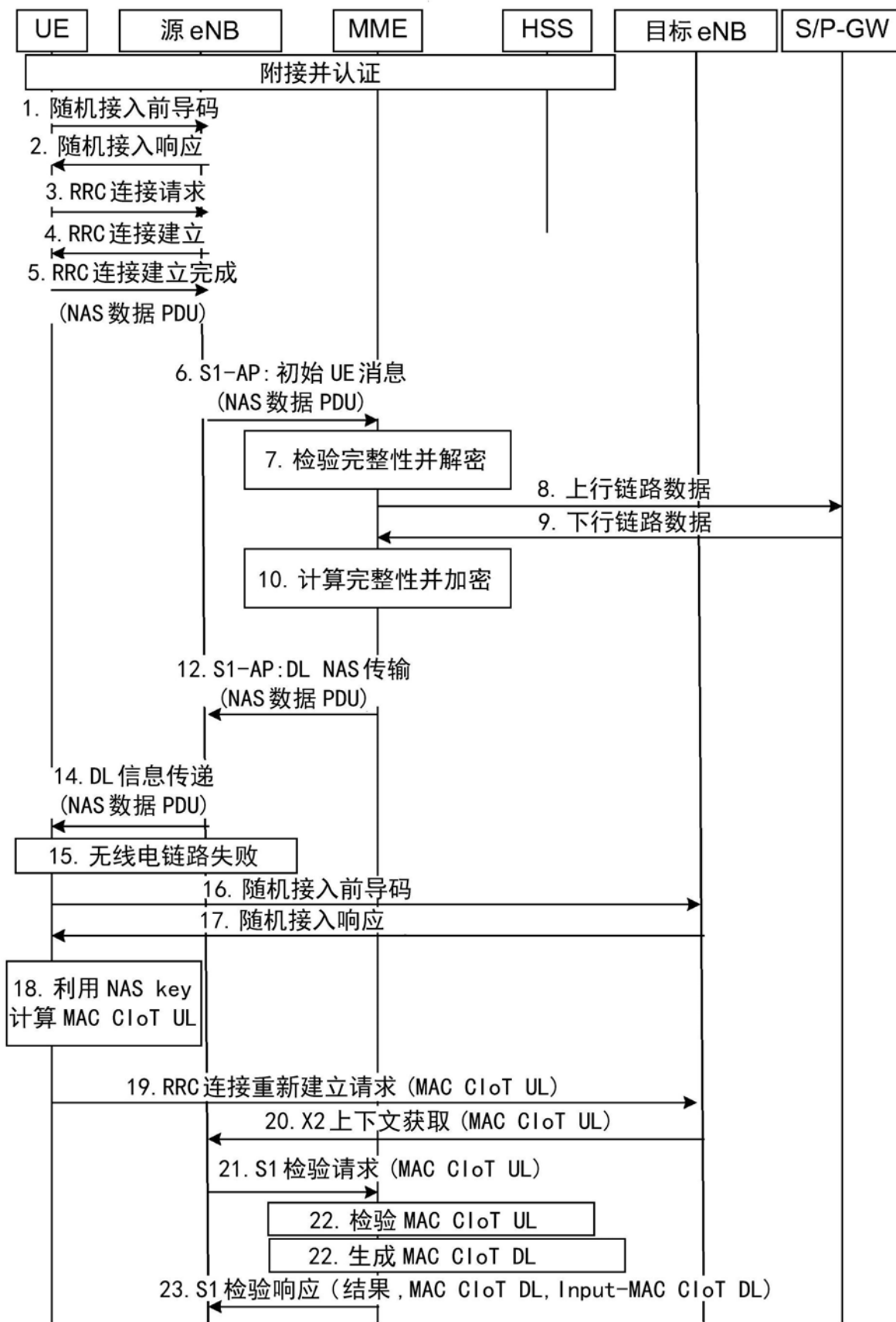


图4A

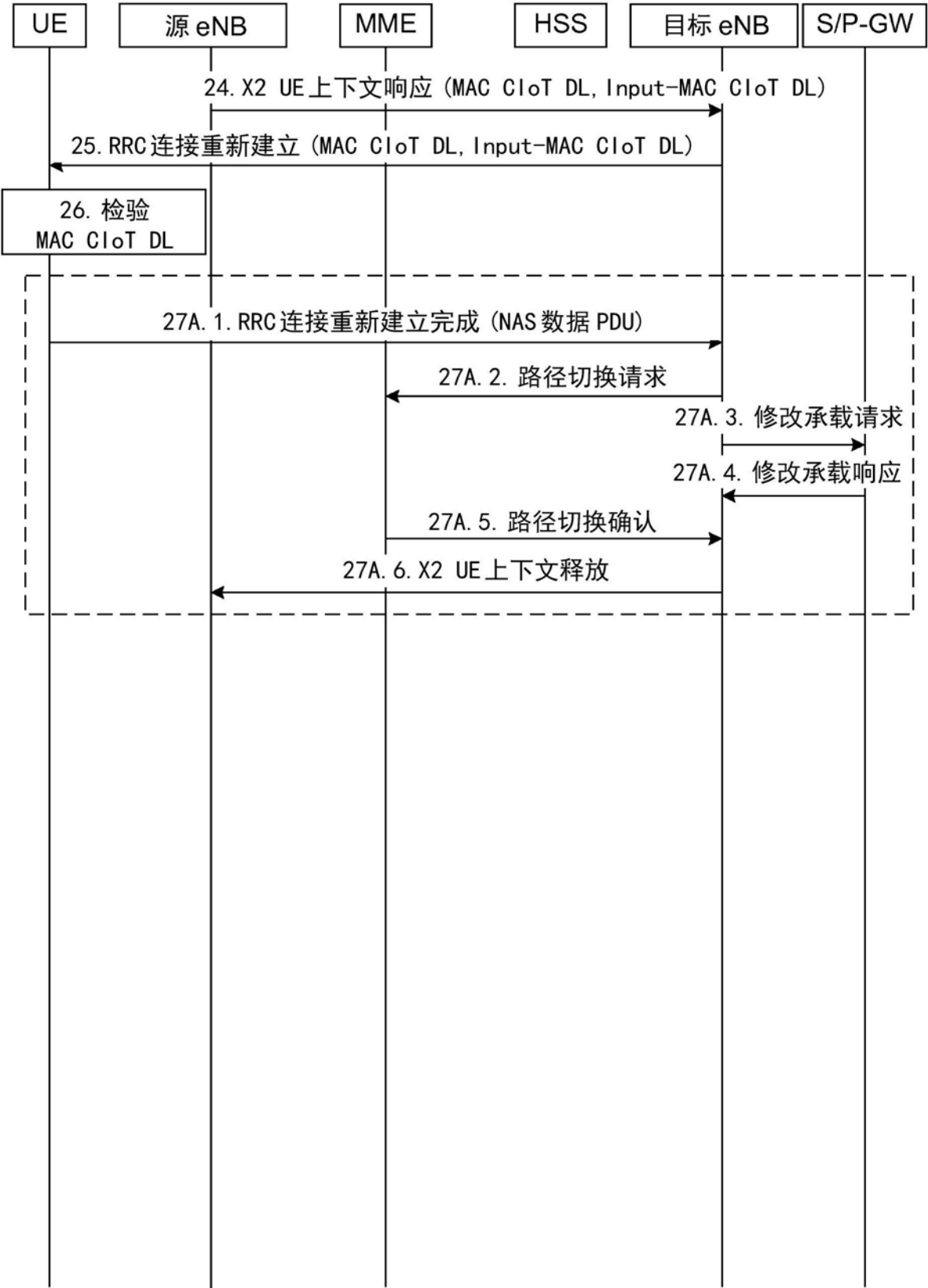


图4B

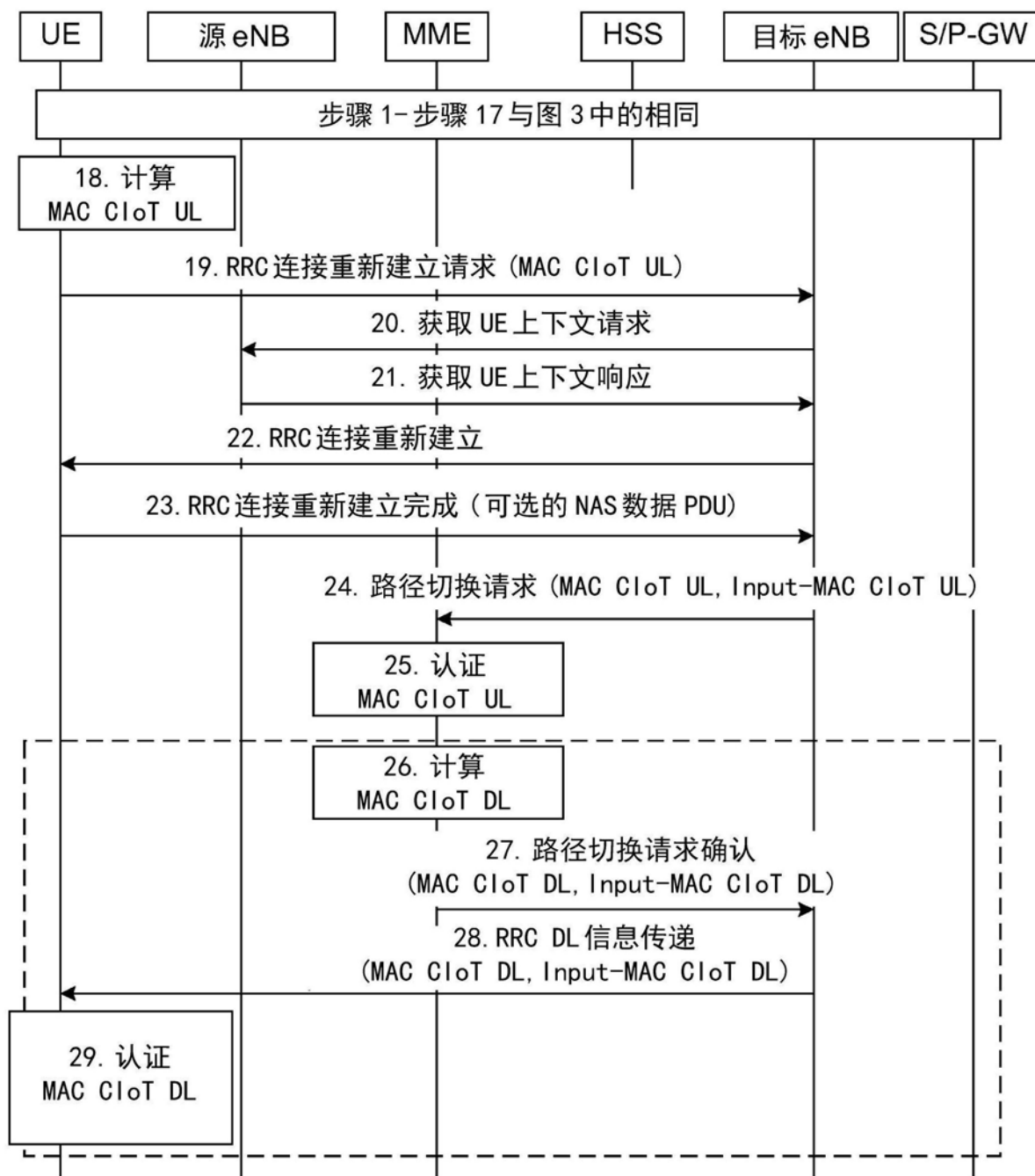


图5

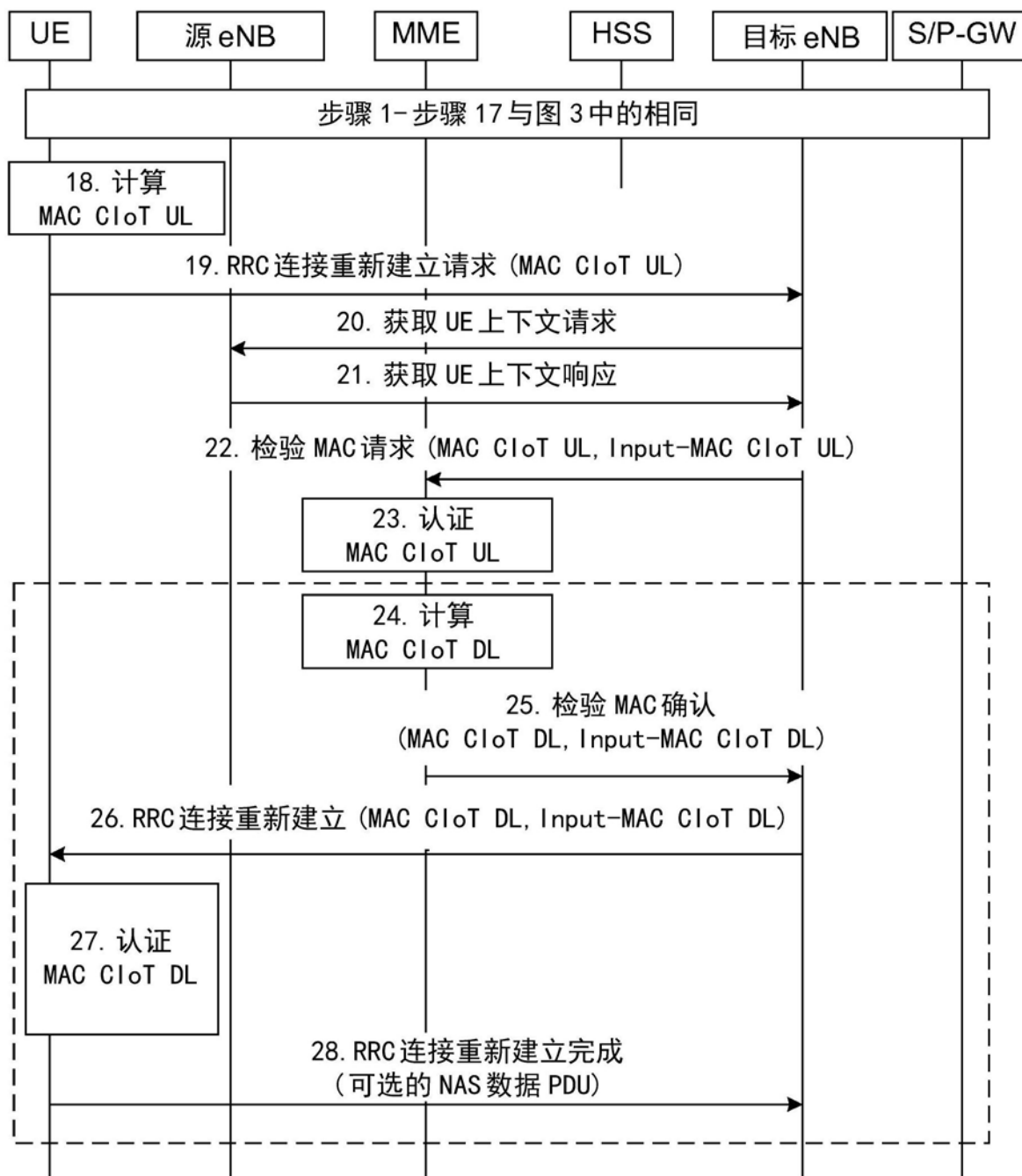


图6

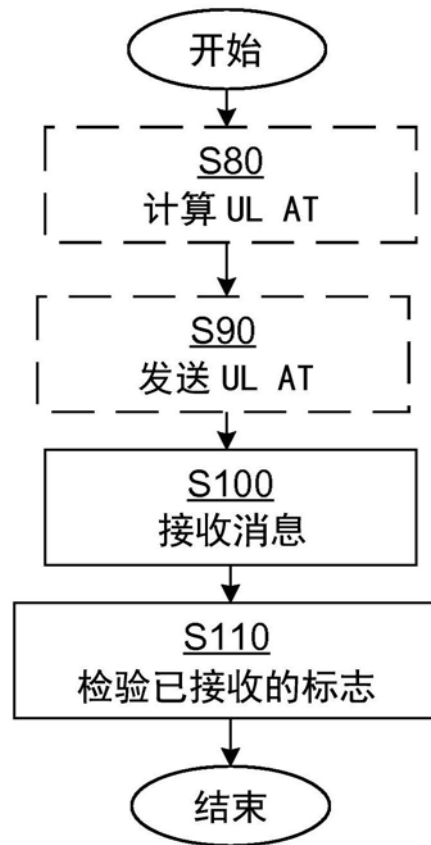


图7A

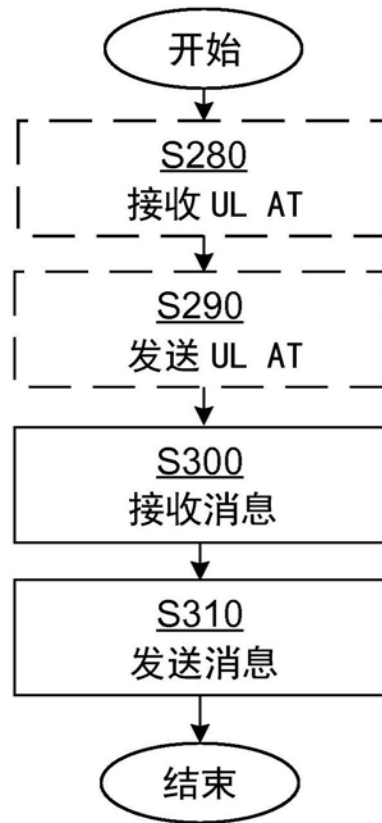


图7B

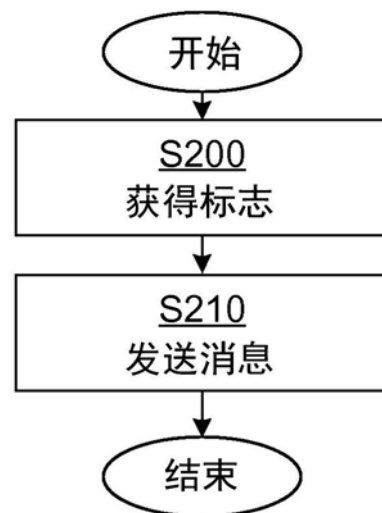


图7C

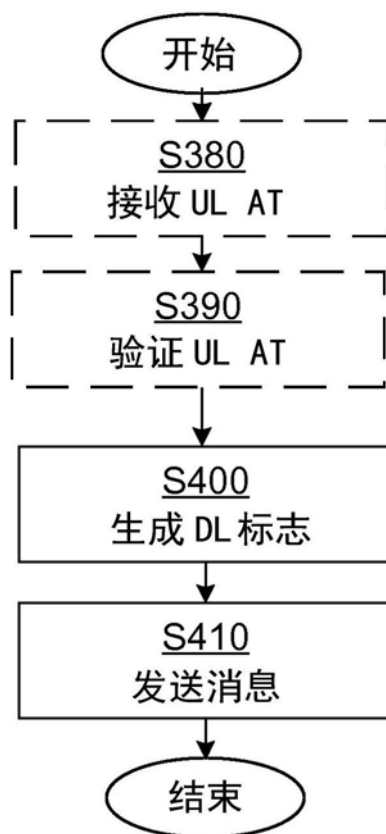


图7D

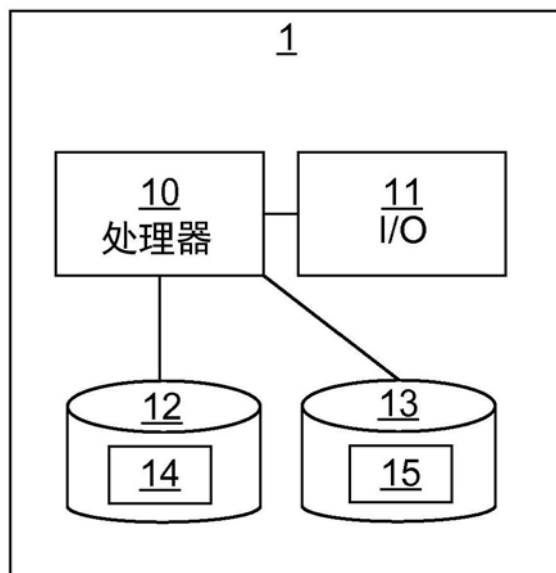


图8

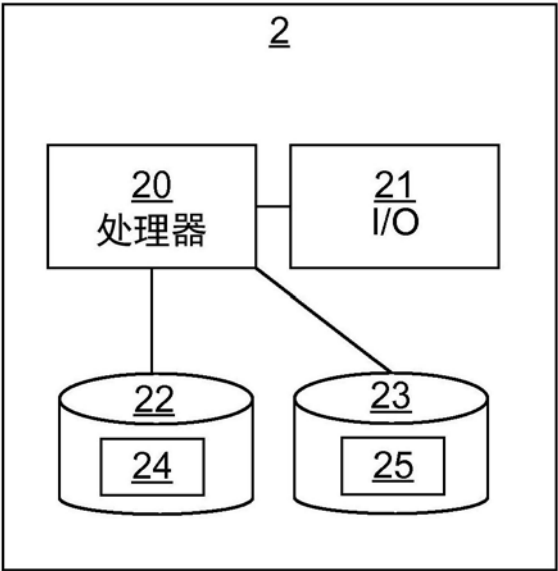


图9

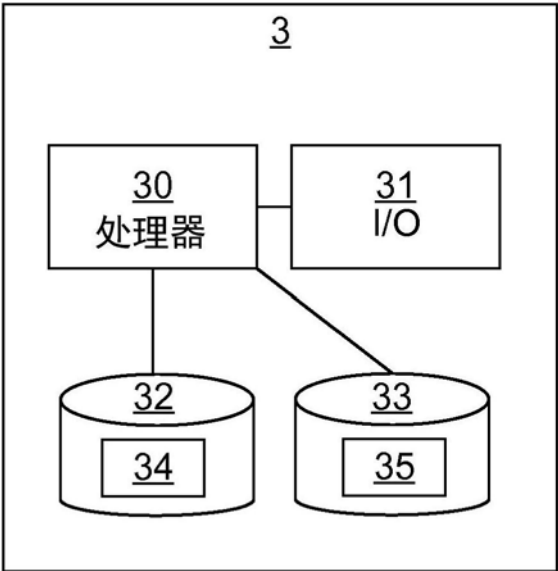


图10

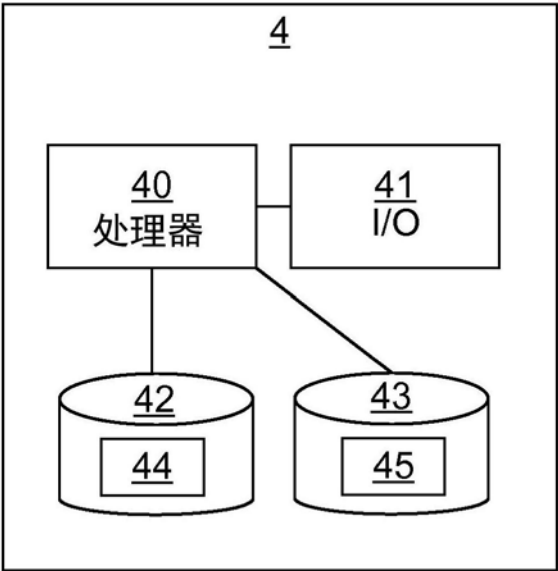


图11

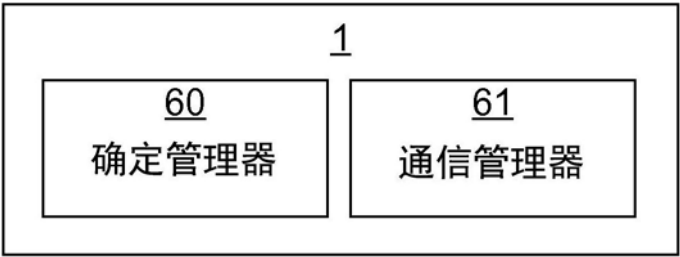


图12

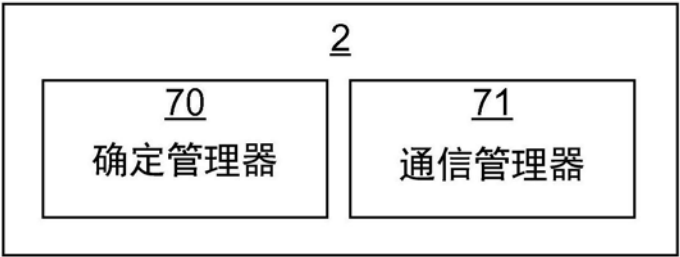


图13

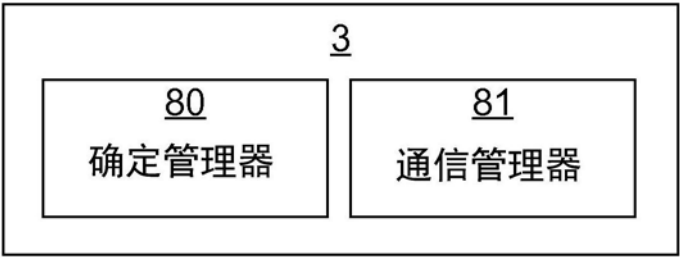


图14

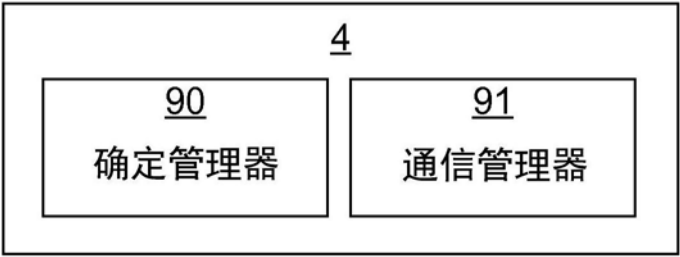


图15