(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108141754 B
(45)授权公告日 2021.12.28

(21)申请号 201680052920.5
(22)申请日 2016.08.15
(65)同一申请的已公布的文献号
申请公布号 CN 108141754 A
(43)申请公布日 2018.06.08
(30)优先权数据
62/218,863 2015.09.15 US
15/089,396 2016.04.01 US
(85)PCT国际申请进入国家阶段日
2018.03.13
(86)PCT国际申请的申请数据
PCT/US2016/047101 2016.08.15
(87)PCT国际申请的公布数据
WO2017/048434 EN 2017.03.23
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚
(72)发明人 S·B·李 A·E·埃斯科特 G·B·霍恩 A·帕拉尼恭德尔
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张扬 王英
(51)Int.Cl.
H04W 12/04(2021.01)
H04W 12/037(2021.01)
H04W 12/02(2009.01)
H04W 36/00(2009.01)
H04W 12/043(2021.01)
(56)对比文件
CN 102948183 A,2013.02.27
CN 101523797 A,2009.09.02
CN 102484817 A,2012.05.30
US 2011021216 A1,2011.01.27
US 2008181411 A1,2008.07.31
审查员 谭菲菲

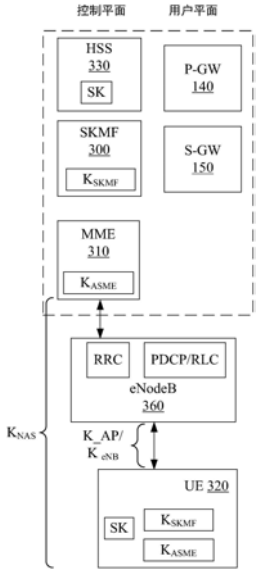
权利要求书4页 说明书17页 附图18页

(54)发明名称

用于涉及移动性管理实体重定位的移动性过程的装置和方法

(57)摘要

一种设备，其识别进入新服务区域，向与网络相关联的网络设备发送服务区域更新请求，从所述网络接收控制平面消息，所述控制平面消息指示由于响应于发送所述服务区域更新请求的服务区域变化而引起的控制平面设备重定位或密钥刷新，以及部分地基于在所述控制平面消息中包括的数据以及在所述设备与密钥管理设备之间共享的第二密钥来推导第一密钥。另一种设备，其从与网络相关联的网络设备接收切换命令，所述切换命令指示新服务区域，基于在所述切换命令中包括的数据以及在所述设备与密钥管理设备之间共享的第二密钥来推导第一密钥，以及发送基于所述第一密钥来保护的切换确认消息。



CN 108141754 B

1.一种无线设备,包括:

无线通信接口,其适于向网络无线地发送数据以及从网络无线地接收数据,其中,所述网络包括密钥管理设备、源移动性管理实体MME和目标MME;以及

处理电路,其通信地耦合到所述无线通信接口,所述处理电路适于:

识别所述无线设备进入新服务区域;

向所述目标MME发送服务区域更新请求;

接收来自所述网络的控制平面消息,所述控制平面消息指示由于服务区域变化而引起的控制平面设备重定位或密钥刷新,所述控制平面消息是响应于发送所述服务区域更新请求而接收的;以及

部分地基于在接收到的所述控制平面消息中包括的数据以及在所述无线设备与所述密钥管理设备之间共享的第二密钥来推导用于在所述无线设备和所述目标MME之间执行安全模式命令SMC过程的第一密钥,其中,所述目标MME是与所述密钥管理设备分离的。

2.根据权利要求1所述的无线设备,其中,所述目标MME不同于当前对所述无线设备进行服务的所述源MME。

3.根据权利要求1所述的无线设备,其中,推导所述第一密钥还部分地基于被保持在所述密钥管理设备处并被包括在所述控制平面消息中的计数器值密钥计数。

4.根据权利要求1所述的无线设备,其中,所述处理电路还适于:

基于所述第一密钥来推导演进型节点B(eNB)密钥K_{eNB}、非接入层密钥K_{NAS}、和/或下一跳跃(NH)密钥中的至少一者,以保护所述无线设备与所述网络之间的通信。

5.根据权利要求1所述的无线设备,其中,所述新服务区域是新跟踪区域和/或新路由区域中的至少一者,并且所述服务区域更新请求与跟踪区域更新和/或路由区域更新中的至少一者相关联。

6.根据权利要求1所述的无线设备,其中,所述控制平面消息是安全模式命令,所述密钥管理设备是会话密钥管理功能(SKMF)设备,并且所述第二密钥是用于认证会话的会话根密钥。

7.根据权利要求1所述的无线设备,其中,至少一个MME保持针对所述无线设备的移动性管理上下文和会话管理上下文。

8.一种无线设备,包括:

无线通信接口,其适于向网络无线地发送数据以及从网络无线地接收数据,其中,所述网络包括密钥管理设备、源移动性管理实体MME和目标MME;以及

处理电路,其通信地耦合到所述无线通信接口,所述处理电路适于:

从所述源MME接收切换命令,所述切换命令指示新服务区域,其中,所述切换命令包括与对目标无线接入节点进行服务的所述目标MME相关联的目标MME标识符,所述目标无线接入节点正在和/或将对所述无线设备进行服务;

基于在所述切换命令中包括的数据以及在所述无线设备与所述密钥管理设备之间共享的第二密钥来推导第一密钥,其中,所述目标MME是与所述密钥管理设备分离的;以及

发送基于所述第一密钥来保护的切换确认消息。

9.根据权利要求8所述的无线设备,其中,所述密钥管理设备是会话密钥管理功能(SKMF)设备,并且所述数据是与所述目标MME相关联的MME标识符。

10.根据权利要求8所述的无线设备，其中，推导所述第一密钥还部分地基于被保持在所述密钥管理设备处的计数器值密钥计数。

11.根据权利要求8所述的无线设备，其中，所述第二密钥是用于认证会话的会话根密钥。

12.一种在无线设备处可操作的方法，所述方法包括：

识别所述无线设备进入网络的新服务区域，其中，所述网络包括密钥管理设备、源移动性管理实体MME和目标MME；

向所述目标MME发送服务区域更新请求；

接收来自所述网络的控制平面消息，所述控制平面消息指示由于服务区域变化而引起的控制平面设备重定位或密钥刷新，所述控制平面消息是响应于发送所述服务区域更新请求而接收的；以及

部分地基于在接收到的所述控制平面消息中包括的数据以及在所述无线设备与所述密钥管理设备之间共享的第二密钥来推导用于在所述无线设备和所述目标MME之间执行安全模式命令SMC过程的第一密钥，其中，所述目标MME是与所述密钥管理设备分离的。

13.根据权利要求12所述的方法，其中，所述目标MME不同于当前对所述无线设备进行服务的所述源MME。

14.根据权利要求12所述的方法，其中，推导所述第一密钥还部分地基于被保持在所述密钥管理设备处并被包括在所述控制平面消息中的计数器值密钥计数。

15.根据权利要求12所述的方法，还包括：

基于所述第一密钥来推导演进型节点B(eNB)密钥K_{eNB}、非接入层密钥K_{NAS}、和/或下一跳跃(NH)密钥中的至少一者，以保护所述无线设备与所述网络之间的通信。

16.根据权利要求12所述的方法，其中，所述新服务区域是新跟踪区域和/或新路由区域中的至少一者，并且所述服务区域更新请求与跟踪区域更新和/或路由区域更新中的至少一者相关联。

17.根据权利要求12所述的方法，其中，所述控制平面消息是安全模式命令，所述密钥管理设备是会话密钥管理功能(SKMF)设备，并且所述第二密钥是用于认证会话的会话根密钥。

18.根据权利要求12所述的方法，其中，至少一个MME保持针对所述无线设备的移动性管理上下文和会话管理上下文。

19.一种无线设备，包括：

用于识别所述无线设备进入网络的新服务区域的单元，其中，所述网络包括密钥管理设备、源移动性管理实体MME和目标MME；

用于向所述目标MME发送服务区域更新请求的单元；

用于接收来自所述网络的控制平面消息的单元，所述控制平面消息指示由于服务区域变化而引起的控制平面设备重定位或密钥刷新，所述控制平面消息是响应于发送所述服务区域更新请求而接收的；以及

用于部分地基于在接收到的所述控制平面消息中包括的数据以及在所述无线设备与所述密钥管理设备之间共享的第二密钥来推导用于在所述无线设备和所述目标MME之间执行安全模式命令SMC过程的第一密钥的单元，其中，所述目标MME是与所述密钥管理设备分

离的。

20.根据权利要求19所述的无线设备,其中,所述目标MME不同于当前对所述无线设备进行服务的所述源MME。

21.根据权利要求19所述的无线设备,其中,推导所述第一密钥还部分地基于被保持在所述密钥管理设备处并被包括在所述控制平面消息中的计数器值密钥计数。

22.根据权利要求19所述的无线设备,还包括:

用于基于所述第一密钥来推导演进型节点B(eNB)密钥K_{eNB}、非接入层密钥K_{NAS}、和/或下一跳跃(NH)密钥中的至少一者,以保护所述无线设备与所述网络之间的通信的单元。

23.根据权利要求19所述的无线设备,其中,所述新服务区域是新跟踪区域和/或新路由区域中的至少一者,并且所述服务区域更新请求与跟踪区域更新和/或路由区域更新中的至少一者相关联。

24.根据权利要求19所述的无线设备,其中,所述控制平面消息是安全模式命令,所述密钥管理设备是会话密钥管理功能(SKMF)设备,并且所述第二密钥是用于认证会话的会话根密钥。

25.根据权利要求19所述的无线设备,其中,至少一个MME保持针对所述无线设备的移动性管理上下文和会话管理上下文。

26.一种具有存储在其上的指令的非临时性计算机可读存储介质,所述指令当由至少一个处理器执行时,使得所述处理器进行以下操作:

识别无线设备进入网络的新服务区域,其中,所述网络包括密钥管理设备、源移动性管理实体MME和目标MME;

向所述目标MME发送服务区域更新请求;

接收来自所述网络的控制平面消息,所述控制平面消息指示由于服务区域变化而引起的控制平面设备重定位或密钥刷新,所述控制平面消息是响应于发送所述服务区域更新请求而接收的;以及

部分地基于在接收到的所述控制平面消息中包括的数据以及在所述无线设备与所述密钥管理设备之间共享的第二密钥来推导用于在所述无线设备和所述目标MME之间执行安全模式命令SMC过程的第一密钥,其中,所述目标MME是与所述密钥管理设备分离的。

27.根据权利要求26所述的非临时性计算机可读存储介质,其中,推导所述第一密钥还部分地基于被保持在所述密钥管理设备处并被包括在所述控制平面消息中的计数器值密钥计数。

28.根据权利要求26所述的非临时性计算机可读存储介质,其中,所述新服务区域是新跟踪区域和/或新路由区域中的至少一者,并且所述服务区域更新请求与跟踪区域更新和/或路由区域更新中的至少一者相关联。

29.根据权利要求26所述的非临时性计算机可读存储介质,其中,所述控制平面消息是安全模式命令,所述密钥管理设备是会话密钥管理功能(SKMF)设备,并且所述第二密钥是用于认证会话的会话根密钥。

30.根据权利要求26所述的非临时性计算机可读存储介质,其中,至少一个MME保持针对所述无线设备的移动性管理上下文和会话管理上下文。

31.根据权利要求26所述的非临时性计算机可读存储介质,其中,所述目标MME不同于

当前对所述无线设备进行服务的所述源MME。

用于涉及移动性管理实体重定位的移动性过程的装置和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求于2015年9月15日在美国专利商标局递交的临时申请No.62/218,863以及于2016年4月1日在美国专利商标局递交的非临时申请No.15/089,396的优先权和权益,通过引用的方式将上述申请的全部内容并入本文。

技术领域

[0003] 本公开内容总体上涉及用于改进的涉及移动性管理实体(MME)重定位的移动性过程的装置和方法。

背景技术

[0004] 图1中示出的当前的蜂窝网络架构使用移动性管理实体(MME)110来实现用于控制用户设备(UE)120对蜂窝网络的接入的过程。通常,MME由网络服务提供商(系统运营商)所拥有并由网络服务提供商操作作为核心网络元素,并且位于由网络服务提供商控制的安全位置。核心网100具有控制平面和用户平面,控制平面包括归属用户服务器(HSS)130和MME,用户平面包括分组数据网络(PDN)网关(PGW)140和服务网关(SGW)150。MME连接到演进型节点B(eNodeB)160。eNodeB向UE提供无线接口、RRC 180和PDCP/RLC 190。

[0005] 在未来的蜂窝网络架构中,可以预见的是,MME 110或执行MME 110的功能中的许多功能的网络组件将被朝着网络边缘推出,其中在网络边缘,它们不那么安全,这是因为它们在物理上更可访问和/或没有与其它网络运营商隔离。随着将网络功能移动至例如云端(例如,互联网),可能不假定它们是安全的,这是因为它们可以具有较低等级的物理隔离,或者没有物理隔离。此外,网络设备可以不是由单个网络服务提供商所拥有。举例而言,可以利用单个物理硬件设备来托管多个MME实例。结果,发送至MME的密钥可能需要更频繁地刷新,并且因此向MME转发认证向量(AV)可能是不可取的。

[0006] 存在针对改进的装置和方法的需求,该改进的装置和方法为其中靠近网络边缘来执行MME功能的未来的蜂窝网络架构提供额外的安全性。

发明内容

[0007] 一个特征提供了一种设备(例如,用户设备),所述设备包括:无线通信接口,其适于向网络无线地发送数据以及从网络无线地接收数据;以及处理电路,其通信地耦合到所述无线通信接口。所述处理电路可以适于:识别进入新服务区域;向与所述网络相关联的网络设备发送服务区域更新请求;从所述网络接收控制平面消息,所述控制平面消息指示由于响应于发送所述服务区域更新请求的服务区域变化而引起的控制平面设备重定位或密钥刷新;以及部分地基于在接收到的所述控制平面消息中包括的数据以及在所述设备与密钥管理设备之间共享的第二密钥来推导第一密钥,所述密钥管理设备与所述网络相关联。根据一个方面,所述控制平面消息是由于所述服务区域变化而从目标控制平面设备接收的,所述目标控制平面设备是与当前对所述设备进行服务的控制平面设备不同的控制平面

设备。根据另一个方面，在所述控制平面消息中包括的所述数据包括控制平面设备标识符，所述控制平面设备标识符标识正在和/或将对所述设备进行服务的控制平面设备。

[0008] 根据一个方面，推导所述第一密钥还部分地基于被保持在所述密钥管理设备处并被包括在所述控制平面消息中的计数器值密钥计数。根据另一个方面，所述处理电路还适于：基于所述第一密钥来推导演进型节点B(eNB)密钥K_{eNB}、非接入层密钥K_{NAS}、和/或下一跳跃(NH)密钥中的至少一者以保护所述设备与所述网络之间的通信。根据另一个方面，所述新服务区域是新跟踪区域和/或新路由区域中的至少一者，并且所述服务区域更新请求与跟踪区域更新和/或路由区域更新中的至少一者相关联。

[0009] 根据一个方面，所述控制平面消息是安全模式命令，所述目标控制平面设备是目标移动性管理实体(MME)，所述密钥管理设备是会话密钥管理功能(SKMF)设备，并且所述第二密钥是用于认证会话的会话根密钥。根据另一个方面，控制平面设备保持针对所述设备的移动性管理上下文和会话管理上下文，并且所述密钥管理设备保持所述第二密钥。

[0010] 另一个特征提供了一种设备，所述设备包括：无线通信接口，其适于向网络无线地发送数据以及从网络无线地接收数据；以及处理电路，其通信地耦合到所述无线通信接口。所述处理电路适于：从与所述网络相关联的网络设备接收切换命令，所述切换命令指示新服务区域；基于在所述切换命令中包括的数据以及在所述设备与密钥管理设备之间共享的第二密钥来推导第一密钥，所述密钥管理设备与所述网络相关联；以及发送基于所述第一密钥来保护的切换确认消息。根据一个方面，所述切换命令包括与对目标无线接入节点进行服务的目标控制平面设备相关联的目标控制平面设备标识符，所述目标无线接入节点正在和/或将对所述设备进行服务。根据另一个方面，推导所述第一密钥部分地基于所述目标控制平面设备标识符。

[0011] 根据一个方面，所述目标控制平面设备是目标移动性管理实体(MME)，所述密钥管理设备是会话密钥管理功能(SKMF)设备，并且所述目标控制平面设备标识符是与所述目标MME相关联的MME标识符。根据另一个方面，推导所述第一密钥还部分地基于被保持在所述密钥管理设备处的计数器值密钥计数。根据再一个方面，所述第二密钥是用于认证会话的会话根密钥。

[0012] 另一个特征提供了一种与网络相关联的网络设备，所述网络设备包括：通信接口，其适于发送和接收信息；以及处理电路，其通信地耦合到所述通信接口。所述处理电路适于：从设备接收服务区域更新请求，其中针对所述设备，所述网络设备不具有设备上下文或者所述设备已改变服务区域；向密钥管理设备发送针对第一密钥的请求；从所述密钥管理设备接收所述第一密钥，所述第一密钥部分地基于在所述密钥管理设备与所述设备之间共享的第二密钥；以及向所述设备发送控制平面消息，所述控制平面消息包括允许所述设备推导所述第一密钥的数据。根据一个方面，所述网络设备是移动性管理实体(MME)，并且所述第一密钥还基于标识所述MME的MME标识符。根据另一个方面，所述处理电路还适于：如果所述网络设备不具有所述设备上下文，则向先前对所述设备进行服务的在先控制平面设备发送设备上下文请求；以及响应于发送所述设备上下文请求，从所述在先控制平面设备接收所述设备上下文。

[0013] 根据一个方面，所述数据包括标识所述网络设备的控制平面设备标识符。根据另一个方面，所述处理电路还适于：从所述密钥管理设备接收计数器值密钥计数连同所述第

一密钥;以及将所述计数器值密钥计数包括在发送给所述设备的所述数据中。根据再一个方面,所述处理电路还适于:在从所述设备接收关于所述控制平面消息被成功地接收的通知之后,向所述设备发送服务区域更新。

[0014] 根据一个方面,所述服务区域更新请求与跟踪区域更新和/或路由区域更新中的至少一者相关联,并且改变服务区域包括改变跟踪区域和/或改变路由区域中的至少一者。根据另一个方面,所述控制平面消息是非接入层安全模式命令,所述密钥管理设备是会话密钥管理功能(SKMF)设备,所述设备是用户设备,所述设备上下文是与所述用户设备相关联的用户设备上下文,并且所述第二密钥是用于认证会话的会话根密钥。

[0015] 另一个特征提供了一种与网络相关联的网络设备,所述网络设备包括:通信接口,其适于发送和接收信息;以及处理电路,其通信地耦合到所述通信接口。所述处理电路适于:在所述网络设备处从源控制平面设备接收前向重定位请求;向密钥管理设备发送针对第一密钥的请求;从所述密钥管理设备接收所述第一密钥,所述第一密钥部分地基于在所述密钥管理设备与设备之间共享的第二密钥;以及利用根据所述第一密钥推导出的无线接入节点(RAN)会话密钥向目标RAN发送切换请求。根据一个方面,所述处理电路还适于:从所述目标RAN接收切换请求确认消息,所述切换请求确认消息指示所述目标RAN将对所述设备进行服务。根据另一个方面,所述处理电路还适于:仅在从所述目标RAN接收所述切换请求确认消息之后,向所述密钥管理设备发送指示接收到所述第一密钥的确认消息。

[0016] 根据一个方面,所述处理电路还适于:向所述源控制平面设备发送前向重定位响应,所述前向重定位响应包括被所述设备用于推导所述第一密钥的数据。根据另一个方面,所述网络设备是将对所述设备进行服务的目标控制平面设备,并且所述数据包括标识所述目标控制平面设备的目标控制平面设备标识符。根据再一个方面,所述目标控制平面设备是目标移动性管理实体(MME),所述源控制平面设备是源MME,所述目标控制平面设备标识符是全球唯一MME标识符(GUMMEI),所述密钥管理设备是会话密钥管理功能(SKMF)设备,并且所述设备是用户设备。

[0017] 根据一个方面,所述数据包括被保持在所述密钥管理设备处的计数器值密钥计数。根据另一个方面,适于从所述密钥管理设备接收所述第一密钥的所述处理电路还适于:接收计数器值密钥计数连同所述第一密钥。

[0018] 另一个特征提供了一种在设备处操作的、用于执行涉及移动性管理实体(MME)重定位或改变跟踪区域的跟踪区域更新的方法,所述方法包括:识别进入新跟踪区域;向与无线通信网络相关联的网络设备发送跟踪区域更新(TAU)请求;从所述网络设备接收安全模式命令,所述安全模式命令指示由于响应于发送所述TAU请求而改变跟踪区域所引起的MME重定位或密钥刷新;以及部分地基于在接收到的所述安全模式命令中包括的数据来推导第一密钥K_{ASME}。根据一个方面,由MME发送所述安全模式命令以刷新所述第一密钥K_{ASME}。根据另一个方面,由于跟踪区域变化,由目标MME发送所述安全模式命令。

[0019] 根据一个方面,在所述安全模式命令中包括的所述数据包括MME标识符。根据另一个方面,所述MME标识符是全球唯一MME标识符(GUMMEI)。根据再一个方面,推导所述第一密钥K_{ASME}部分地基于所述GUMMEI。

[0020] 根据一个方面,推导所述第一密钥K_{ASME}还部分地基于在所述设备与会话密钥管理功能(SKMF)设备之间共享的第二密钥K_{SKMF}。根据另一个方面,推导所述第一K_{ASME}还部分地基

于被保持在所述SKMF设备处的计数器值密钥计数。根据再一个方面，在所述安全模式命令中包括的所述数据还包括所述计数器值密钥计数。

[0021] 根据一个方面，所述方法还包括：从所述网络设备接收跟踪区域更新消息。根据另一个方面，所述方法还包括：使用根据所述第一密钥K_{ASME}推导出的一个或多个密钥来解密跟踪区域更新消息。根据再一个方面，所述跟踪区域更新消息包括新的全球唯一临时标识符(GUTI)。

[0022] 另一个特征提供了一种设备，所述设备包括：无线通信接口，其适于与关联于无线通信网络的网络设备无线地发送和接收数据；以及处理电路，其通信地耦合到所述无线通信接口，所述处理电路适于：识别进入新跟踪区域；向与所述无线通信网络相关联的所述网络设备发送跟踪区域更新(TAU)请求；从所述网络设备接收安全模式命令，所述安全模式命令指示由于响应于发送所述TAU请求而改变跟踪区域所引起的移动性管理实体(MME)重定位或密钥刷新；以及部分地基于在接收到的所述安全模式命令中包括的数据来推导第一密钥K_{ASME}。

[0023] 另一个特征提供了一种设备，所述设备包括：用于识别进入新跟踪区域的单元；用于向与无线通信网络相关联的网络设备发送跟踪区域更新(TAU)请求的单元；用于从所述网络设备接收安全模式命令的单元，所述安全模式命令指示由于响应于发送所述TAU请求而改变跟踪区域所引起的移动性管理实体(MME)重定位或密钥刷新；以及用于部分地基于在接收到的所述安全模式命令中包括的数据来推导第一密钥K_{ASME}的单元。

[0024] 另一个特征提供了一种具有存储在其上的指令的非暂时性计算机可读存储介质，所述指令用于执行涉及移动性管理实体(MME)重定位或改变跟踪区域的跟踪区域更新，当所述指令被至少一个处理器执行时，使得所述处理器执行以下操作：识别进入新跟踪区域；向与无线通信网络相关联的网络设备发送跟踪区域更新(TAU)请求；从所述网络设备接收安全模式命令，所述安全模式命令指示由于响应于发送所述TAU请求而改变跟踪区域所引起的MME重定位或密钥刷新；以及部分地基于在接收到的所述安全模式命令中包括的数据来推导第一密钥K_{ASME}。

[0025] 另一个特征提供了一种在设备处操作的、用于执行涉及移动性管理实体(MME)重定位或改变跟踪区域的切换的方法，所述方法包括：从网络设备接收切换命令，所述切换命令指示新跟踪区域；基于在所述切换命令中包括的数据来推导第一密钥K_{ASME}；以及发送基于所述第一密钥K_{ASME}来保护的切换确认消息。根据一个方面，所述方法还包括：在推导所述第一密钥K_{ASME}之前，验证所述切换命令。根据另一个方面，所述切换命令包括：与对所述网络设备进行服务的目标MME相关联的目标MME标识符。

[0026] 根据一个方面，推导所述第一密钥K_{ASME}部分地基于所述目标MME标识符。根据另一个方面，所述目标MME标识符是与对所述网络设备进行服务的所述目标MME相关联的全球唯一MME标识符(GUMMEI)。根据再一个方面，推导所述第一密钥K_{ASME}还部分地基于在所述设备与对所述目标MME进行服务的会话密钥管理功能(SKMF)设备之间共享的第二密钥K_{SKMF}。

[0027] 根据一个方面，推导所述第一密钥K_{ASME}还部分地基于被保持在所述SKMF设备处的计数器值密钥计数。根据另一个方面，在所述切换命令中包括的所述数据还包括所述计数器值密钥计数。

[0028] 另一个特征提供了一种设备，所述设备包括：无线通信接口，其适于与关联于无线

通信网络的网络设备无线地发送和接收数据;以及处理电路,其通信地耦合到所述无线通信接口,所述处理电路适于:从所述网络设备接收切换命令,所述切换命令指示新跟踪区域;基于在所述切换命令中包括的数据来推导第一密钥K_{ASME};以及发送基于所述第一密钥K_{ASME}来保护的切换确认消息。

[0029] 另一个特征提供了一种设备,所述设备包括:用于从网络设备接收切换命令的单元,所述切换命令指示新跟踪区域;用于基于在所述切换命令中包括的数据来推导第一密钥K_{ASME}的单元;以及用于发送基于所述第一密钥K_{ASME}来保护的切换确认消息的单元。

[0030] 另一个特征提供了一种具有存储在其上的指令的非暂时性计算机可读存储介质,所述指令用于执行涉及移动性管理实体(MME)重定位或改变跟踪区域的切换,当所述指令被至少一个处理器执行时,使得所述处理器执行以下操作:从网络设备接收切换命令,所述切换命令指示新跟踪区域;基于在所述切换命令中包括的数据来推导第一密钥K_{ASME};以及发送基于所述第一密钥K_{ASME}来保护的切换确认消息。

[0031] 另一个特征提供了一种用于在移动性管理实体(MME)处执行涉及MME重定位或改变跟踪区域的跟踪区域更新的方法,所述方法包括:从用户设备(UE)接收跟踪区域更新(TAU)请求,其中针对所述UE,所述MME不具有与所述UE相关联的UE上下文或者所述UE已改变跟踪区域;向会话密钥管理功能(SKMF)设备发送针对第一密钥K_{ASME}的请求;从所述SKMF设备接收所述第一密钥K_{ASME};以及向所述UE发送非接入层(NAS)安全模式命令(SMC),所述NAS SMC包括允许所述UE推导所述第一密钥K_{ASME}的数据。根据一个方面,所述方法还包括:如果所述MME不具有所述UE上下文,则向先前对所述UE进行服务的源MME发送UE上下文请求。根据另一个方面,所述方法还包括:响应于发送所述UE上下文请求,从所述源MME接收所述UE上下文。根据再一个方面,所述方法还包括:在接收所述第一密钥K_{ASME}之后,向所述SKMF设备发送密钥确认。

[0032] 根据一个方面,所述数据包括标识所述MME的MME标识符。根据另一个方面,所述MME标识符是全球唯一MME标识符(GUMMEI)。根据再一个方面,所述数据包括被保持在所述SKMF设备处的计数器值密钥计数。

[0033] 根据一个方面,从所述SKMF设备接收所述第一密钥K_{ASME}还包括:从所述SKMF设备接收计数器值密钥计数。根据另一个方面,所述方法还包括:在从所述UE接收关于NAS SMC被成功地完成的通知之后,向所述UE发送跟踪区域更新。根据另一个方面,所述方法还包括:向所述UE同时发送经加密的跟踪区域更新和所述NAS SMC。根据另一个方面,发送针对所述第一密钥K_{ASME}的所述请求包括:发送UE位置更新。

[0034] 另一个特征提供了一种与无线通信网络相关联的网络设备,所述网络设备包括:通信接口,其适于发送和接收信息;以及处理电路,其通信地耦合到所述通信接口,所述处理电路适于:从用户设备(UE)接收跟踪区域更新(TAU)请求,其中针对所述UE,所述网络设备不具有与所述UE相关联的UE上下文或者所述UE已改变跟踪区域;向会话密钥管理功能(SKMF)设备发送针对第一密钥K_{ASME}的请求;从所述SKMF设备接收所述第一密钥K_{ASME};以及向所述UE发送非接入层(NAS)安全模式命令(SMC),所述NAS MSC包括允许所述UE推导所述第一密钥K_{ASME}的数据。

[0035] 另一个特征提供了一种与无线通信网络相关联的网络设备,所述网络设备包括:用于从用户设备(UE)接收跟踪区域更新(TAU)请求的单元,其中针对所述UE,所述网络设备

不具有与所述UE相关联的UE上下文或者所述UE已改变跟踪区域;用于向会话密钥管理功能(SKMF)设备发送针对第一密钥K_{ASME}的请求的单元;用于从所述SKMF设备接收所述第一密钥K_{ASME}的单元;以及用于向所述UE发送非接入层(NAS)安全模式命令(SMC)的单元,所述NAS SMC包括允许所述UE推导所述第一密钥K_{ASME}的数据。

[0036] 另一个特征提供了一种具有存储在其上的指令的非暂时性计算机可读存储介质,所述指令用于在移动性管理实体(MME)处执行涉及所述MME重定位或改变跟踪区域的跟踪区域更新,当所述指令被至少一个处理器执行时,使得所述处理器执行以下操作:从用户设备(UE)接收跟踪区域更新(TAU)请求,其中针对所述UE,所述网络设备不具有与所述UE相关联的UE上下文或者所述UE已改变跟踪区域;向会话密钥管理功能(SKMF)设备发送针对第一密钥K_{ASME}的请求;从所述SKMF设备接收所述第一密钥K_{ASME};以及向所述UE发送非接入层(NAS)安全模式命令(SMC),所述NAS SMC包括允许所述UE推导所述第一密钥K_{ASME}的数据。

[0037] 另一个特征提供了一种用于在移动性管理实体(MME)处执行涉及所述MME重定位或改变跟踪区域的切换的方法,所述方法包括:在目标MME处从源MME接收前向重定位请求;向会话密钥管理功能(SKMF)设备发送针对第一密钥K_{ASME}的请求;从所述SKMF设备接收所述第一密钥K_{ASME};以及利用根据所述第一密钥K_{ASME}推导出的密钥K_{eNB}向目标无线接入节点(RAN)发送切换请求。根据一个方面,所述方法还包括:从所述目标RAN接收切换请求确认消息,所述切换请求确认消息指示所述目标RAN将对所述用户设备(UE)进行服务。根据另一个方面,所述方法还包括:仅在从所述目标RAN接收所述切换请求确认消息之后,向所述SKMF发送指示接收到所述第一密钥K_{ASME}的确认消息。

[0038] 根据一个方面,所述方法还包括:向所述源MME发送前向重定位响应,所述前向重定位响应包括被UE用于推导所述第一密钥K_{ASME}的数据。根据另一个方面,所述数据包括标识所述目标MME的MME标识符。根据再一个方面,所述MME标识符是全球唯一MME标识符(GUMMEI)。

[0039] 根据一个方面,所述数据包括被保持在所述SKMF设备处的计数器值密钥计数。根据另一个方面,从所述SKMF设备接收所述第一密钥K_{ASME}还包括:从所述SKMF设备接收计数器值密钥计数。

[0040] 另一个特征提供了一种网络设备,所述网络设备包括:通信接口,其适于发送和接收信息;以及处理电路,其通信地耦合到所述通信接口,所述处理电路适于:在所述网络设备处从源移动性管理实体(MME)接收前向重定位请求;向会话密钥管理功能(SKMF)设备发送针对第一密钥K_{ASME}的请求;从所述SKMF设备接收所述第一密钥K_{ASME};以及利用根据所述第一密钥K_{ASME}推导出的密钥K_{eNB}向目标无线接入节点(RAN)发送切换请求。

[0041] 另一个特征提供了一种与无线通信网络相关联的网络设备,所述网络设备包括:用于在所述网络设备处从源移动性管理实体(MME)接收前向重定位请求的单元;用于向会话密钥管理功能(SKMF)设备发送针对第一密钥K_{ASME}的请求的单元;用于从所述SKMF设备接收所述第一密钥K_{ASME}的单元;以及用于利用根据所述第一密钥K_{ASME}推导出的密钥K_{eNB}向目标无线接入节点(RAN)发送切换请求的单元。

[0042] 另一个特征提供了一种具有存储在其上的指令的非暂时性计算机可读存储介质,所述指令用于在移动性管理实体(MME)处执行涉及所述MME重定位或改变跟踪区域的切换,当所述指令被至少一个处理器执行时,使得所述处理器执行以下操作:在所述网络设备处

从源MME接收前向重定位请求;向会话密钥管理功能(SKMF)设备发送针对第一密钥K_{ASME}的请求;从所述SKMF设备接收所述第一密钥K_{ASME};以及利用根据所述第一密钥K_{ASME}推导出的密钥K_{eNB}向目标无线接入节点(RAN)发送切换请求。

附图说明

[0043] 图1是在现有技术中找到的无线通信系统的示例的框图。

[0044] 图2是用于推导用于蜂窝网络安全的数字密钥的方法的流程图。

[0045] 图3是具有改进的网络密钥层次的无线通信系统的第一实施例的框图。

[0046] 图4是具有改进的网络密钥层次的无线通信系统的第二实施例的框图。

[0047] 图5是具有改进的网络密钥层次的无线通信系统的第三实施例的框图

[0048] 图6是用于蜂窝网络的改进的密钥层次的示意图。

[0049] 图7示出了用于连接到无线通信网络(例如,无线蜂窝网络)的UE的附着过程和初始数据传输的流程图。

[0050] 图8示出了S1-切换过程的流程图。

[0051] 图9示出了在UE移动到需要MME重定位的新位置之后的跟踪区域更新过程的流程图。

[0052] 图10示出了诸如用户设备/装置之类的设备的第一示例性示意框图。

[0053] 图11示出了在设备处操作的、用于执行涉及控制平面设备重定位或改变服务区域的服务区域更新的第一示例性方法。

[0054] 图12示出了在设备处操作的、用于执行涉及控制平面设备重定位或改变服务区域的切换的第二示例性方法。

[0055] 图13示出了诸如MME之类的网络设备的第一示例性示意框图。

[0056] 图14示出了在网络设备处操作的、用于在控制平面设备处执行涉及控制平面设备重定位或改变服务区域的服务区域更新的第一示例性方法。

[0057] 图15示出了在网络设备处操作的、用于在控制平面设备处执行涉及控制平面设备重定位或改变服务区域的切换的第二示例性方法。

[0058] 图16示出了诸如用户设备/装置之类的设备的第二示例性示意框图。

[0059] 图17示出了诸如用户设备/装置之类的设备的第三示例性示意框图。

[0060] 图18示出了诸如MME之类的网络设备的第二示例性示意框图。

[0061] 图19示出了诸如MME之类的网络设备的第三示例性示意框图。

具体实施方式

[0062] 本文使用词语“示例性”来意指“作为示例、实例或说明”。本文描述为“示例性”的任何实施例并不必然地被解释为比其它实施例优选或有利。

[0063] 参照图2和图3,本公开内容的方面可以位于用于推导用于蜂窝网络安全的数字密钥的方法200中。在该方法中,用户设备(UE)320与会话密钥管理功能设备300(以下称为“SKMF”)互相认证。用户设备使用与归属用户服务器(HSS)330共享的秘密密钥(SK)来推导与SKMF 300共享的第一会话密钥(例如,K_{SKMF})。用户设备随后使用第一会话密钥来推导与移动性管理实体(MME)310共享的第二会话密钥(例如,K_{ASME})。

[0064] 在本公开内容的更详细的方面中,SKMF(认证器)可以是位于电信网络内部深处的信任锚(或密钥锚),其推导用于每个MME的密钥(例如,K_{ASME})。因此,当执行其功能的MME和/或网络设备被推到网络的边缘时,SKMF留在网络内部深处并且非常安全。可以使用具有秘密密钥和服务网络标识(SN_id)作为输入的第一密钥推导函数来推导第一会话密钥。第一密钥推导函数可以基于例如HMAC-256。可以使用可扩展的认证协议(EAP)或特定的NAS信令来执行互相认证。可以在认证和密钥协定(AKA)过程(针对与UE当前附着的MME)期间或在涉及MME重定位的切换期间推导第二会话密钥。可以由AAA服务器针对当前附着的MME来定义会话。可以在共享MME群组标识(MMEGI)的MME群组内执行MME重定位。替代地,可以与具有不同MMEGI的另一个MME执行MME重定位。

[0065] 在本公开内容的其它更详细的方面中,可以使用具有第一会话密钥和唯一的全球唯一MME标识符(GUMMEI)作为输入的第二密钥推导函数来推导第二会话密钥。GUMMEI可以基于MMEGI和MME码的组合。第二密钥推导函数可以基于HMAC-256。替代地,可以使用具有第一会话密钥和MMEGI作为输入的第二密钥推导函数来推导第二会话密钥。

[0066] 本公开内容的另一个方面可以位于用于推导用于用户设备320的密钥的方法中。在该方法中,网络实体从SKMF 300接收用于用户设备的会话密钥(例如,K_{ASME})。用于接收会话密钥的通信信道可以是安全性受保护的。网络实体可以是eNB 360、MME、GW等。替代地,本公开内容的一个方面可以位于其中网络实体可以从相同群组中的另一个网络实体接收用于用户设备的会话密钥的方法中。在本公开内容的更详细的方面中,当源MME在不传输会话密钥的情况下请求切换时,网络实体可以从SKMF请求会话密钥(例如,K_{ASME})。

[0067] 本公开内容的另一个方面,SKMF 300可以与用户设备320互相认证。SKMF 300可以推导会话密钥(例如,K_{ASME}),以供在与连接到MME 310的UE 320进行通信时使用。SKMF 300可以向MME 10发送用于UE 320的会话密钥。与UE 320互相认证可以包括:SKMF 300向HSS 330转发针对UE 320的认证信息的请求。认证信息可以包括用于UE 320的认证向量(AV)。与UE 320互相认证还可以包括:SKMF 300从UE 320接收认证响应。认证向量可以包括期望响应(XRES)、认证值(AUTN)、随机数(RAND)和第一会话密钥(例如,K_{SKMF})。AUTN可以基于UE 320与HSS 330共享的序列号和秘密密钥(SK)。

[0068] 本公开内容允许将网络功能(例如,MME 310)移动到远离网络核心的网络边缘。SKMF 300可以被放置在MME 310与HSS 330之间。SKMF 300可以充当本地密钥锚。因此,可以减少MME 310所要求的信任。结果,在MME重定位期间将不会传输用于UE 320的MME 310。

[0069] UE可以执行与SKMF的认证密钥协定(AKA)。HHS可以向SKMF发送AV。AV可以包括XRES、AUTN、RAND和K_{SKMF}。可以根据在UE与HSS之间共享的秘密密钥SK来推导K_{SKMF}。因此,可以在UE与SKMF之间执行相互认证。该架构可以用于第五代(5G)蜂窝网络中。

[0070] 如果AKA是成功的,则SKMF向MME发送MME密钥(例如,K_{ASME})。可以根据下文进一步提供的细节来推导MME密钥(以及根据其推导出的其它密钥)。

[0071] 在漫游场景中(即,UE处于拜访网络中),拜访网络中的SKMF可以变成本地密钥锚。类似地,可以通过SKMF来执行AKA。如图4和图5中所示出,SKMF 300(其处于拜访网络中并且不处于归属网络406中)是本地密钥锚。在本地网络内的MME重定位(例如,切换或跟踪区域更新)期间,SKMF推导新的K_{ASME}并将其提供给目标/新MME。可以根据新K_{ASME}来推导无线接入节点(RAN)会话密钥(例如,K_{eNB})。

[0072] 图6示出了用于蜂窝网络的改进的密钥层次的示意图。UE的通用用户身份模块(USIM)和网络的认证中心(AuC)存储共享的秘密密钥(SK)。根据SK推导出完整性密钥(IK)和加密密钥(CK)并且将其提供给HSS。HSS可以继而生成第一会话密钥(K_{SKMF})并将其提供给SKMF。第一会话密钥K_{SKMF}在整个认证会话期间是有效的。SKMF可以使用K_{SKMF}来生成第二会话密钥(K_{ASME})并将该密钥提供给MME。K_{ASME}可以对于仅特定的MME是有效的。MME可以继而基于K_{ASME}来生成其它密钥(K_{NASenc}、K_{NASint}、K_{eNB}/NH等)。

[0073] 示例性附着、切换和跟踪区域更新(TAU)过程

[0074] 下文参照4G长期演进系统组件在一些部分中描述了本公开内容的方面。这仅是示例性的。本公开内容不受诸如4G LTE之类的任何一个特定网络系统限制,而是可以应用于其它类型的通信系统,包括但不限于5G系统。

[0075] 在至网络的初始附着期间,UE执行与会话密钥管理功能(SKMF)设备的认证和密钥协定(AKA)过程。一旦认证是成功的,SKMF就推导用于UE所附着到的MME的密钥(例如,K_{ASME})并且将密钥提供给MME。

[0076] 当UE请求涉及MME重定位的跟踪区域更新(TAU)时,接收TAU请求的新MME(例如,目标MME)从SKMF接收新密钥K_{ASME}并且通过执行非接入层(NAS)安全模式命令(SMC)过程来与UE建立安全关联。类似地,当发生涉及MME重定位的切换时,目标MME还从SKMF得到新密钥K_{ASME}并与UE建立安全关联。

[0077] 当UE在跟踪区域之间移动时,支持两个跟踪区域的MME可以发起对K_{ASME}的改变。这隐藏了网络配置不让UE看到。例如,UE仅看到跟踪区域而不是MME。这可以响应于TAU和改变跟踪区域的切换两者发生。

[0078] 图7根据本公开内容的一个方面,示出了用于连接到无线通信网络(例如,无线蜂窝网络)的UE的附着过程和初始数据传输的流程图。首先,UE向eNB发送附着请求702,eNB继而向MME发送初始UE消息704。接着,UE和SKMF执行认证和密钥协定(AKA)706。为了执行AKA,SKMF向HSS发送认证信息请求707,并且作为响应,其可以从HSS接收认证向量708,认证向量708可以包括期望响应(XRES)、认证值(AUTN)、随机数(RAND)和特定于MME的密钥K_{SKMF}。AUTN可以基于UE与HSS共享的序列号和秘密密钥(SK)。

[0079] 一旦AKA是成功的,SKMF就可以基于K_{SKMF}(例如,“第二密钥”)、MME标识符(例如,GUMMEI)和/或计数器值(例如,密钥计数)来推导会话密钥K_{ASME}(例如,“第一密钥”)。因此,K_{ASME}可以等于KDF(K_{SKMF},GUMMEI|密钥计数),其中KDF是密钥推导函数。计数器值密钥计数是可以由SKMF递增的计数器值,以使得SKMF能够在每当发生切换回MME时推导用于相同MME的新鲜的K_{ASME}密钥。根据一个方面,可以使用仅用一次的数(nonce)而不是计数器值。根据另一个方面,如果GUMMEI不用于授权特定的MME身份,则可以省略GUMMEI。例如,如果SKMF总是与为其提供K_{ASME}的MME在相同的网络中,则在密钥推导中包括GUMMEI可能是不必要的。因此,根据另一个示例,K_{ASME}可以等于KDF(K_{SKMF},nonce)。随后向MME 710发送特定于MME的密钥K_{ASME}。MME可以随后使用密钥K_{ASME}来执行与UE的非接入层(NAS)安全模式命令(SMC)过程712。在NAS SMC过程712期间,MME可以将其GUMMEI和/或密钥计数提供给UE,因此UE也可以推导K_{ASME}。图7中剩余的714-728类似于在4G LTE蜂窝通信协议中找到的那些过程。

[0080] 图8根据本公开内容的一个方面,示出了S1-切换过程的流程图。首先,源eNB(即,当前eNB)向源MME(即,当前MME)发送需要切换(HO)消息802。接着,源MME向目标MME(例如,

新MME)发送/转发重定位请求804。目标MME可以创建会话请求806并将其发送给目标服务网关(S-GW),以及从目标S-GW接收会话响应808。目标MME还可以向SKMF发送针对特定于MME的密钥K_{ASME}的密钥请求810。这样做,目标MME可以向SKMF提供其GUMMEI。SKMF可以继而使用MME的GUMMEI、其先前从HSS接收的K_{SKMF}密钥(上文所描述的)以及密钥计数来生成K_{ASME}。根据一个方面,可以使用仅用一次的数(nonce)而不是密钥计数。根据另一个方面,如果不期望授权特定的MME身份,则可以省略GUMMEI。SKMF向目标MME发送K_{ASME} 812。根据一个方面,目标MME可以向目标S-GW发送会话请求806并且在大约同时发送密钥请求810。因此,步骤806和810可以与步骤808和812同时地执行。

[0081] 目标MME可以随后向目标eNB(即,潜在的新eNB)发送切换请求814,并且作为响应,目标eNB发送回切换响应816。切换请求814可以包括由目标MME使用K_{ASME}推导的密钥K_{eNB}。切换响应816指示目标eNB是否同意接受切换。如果目标eNB的确同意接受切换,则目标MME向SKMF发送密钥(即,K_{ASME})确认消息818。在接收到密钥确认消息时,SKMF可以随后递增密钥计数计数器值。对发送密钥确认消息818的步骤进行延迟,直到接收到切换请求确认816为止,这是因为切换请求可能被目标eNB拒绝。在这种情况下,不需要由UE推导新K_{ASME},并且SKMF可以不需要增加密钥计数。在目标MME向源MME发送重定位响应820之后,源MME向源eNB发送切换命令822,其中切换命令822被转发824给UE。切换命令822、824可以包括目标MME的GUMMEI和密钥计数,使得UE可以推导新K_{ASME}和用于目标eNB的K_{eNB}。UE利用切换确认消息826来对目标eNB进行响应。切换确认消息826是完整性受保护和加密的。

[0082] 图9根据本公开内容的一个方面,示出了在UE移动到需要MME重定位的新位置之后的跟踪区域更新过程的流程图。首先,UE生成跟踪区域更新请求902并将其发送给eNB。eNB继而将跟踪区域更新请求904转发给将与UE相关联的目标MME。eNB基于包括UE的位置的各种标准来确定向哪个新/目标MME发送跟踪区域更新请求。跟踪区域更新请求可以包括全球唯一临时标识符(GUTI),GUTI继而包括源MME(即,当前与UE相关联的MME)的GUMMEI。目标MME可以随后使用在其接收的跟踪区域更新请求中的GUMMEI来向源MME发送UE上下文请求消息906。源MME随后利用UE上下文响应消息908中的UE上下文信息来进行响应。一旦接收到该响应,就可以从目标MME向源MME发送确认910。

[0083] 目标MME可以随后向SKMF 912发送位置更新和密钥请求(即,K_{ASME}密钥请求)。位置更新被转发给HSS,HSS随后向旧MME发送位置取消消息914(旧MME可以将位置取消确认消息916发送回给HSS)。SKMF 912可以基于如先前所描述的目标MME的GUMMEI和/或密钥计数计数器值来生成用于目标MME的新K_{ASME}。根据一个方面,可以使用仅用一次的数(nonce)而不是密钥计数。根据另一个方面,如果不期望授权特定的MME身份,则可以省略GUMMEI。向目标MME发送新K_{ASME} 918连同位置更新确认。在从SKMF接收到K_{ASME}时,目标MME可以利用密钥确认消息920来向SKMF进行回应。根据一个方面,目标MME可以大约在其向SKMF发送位置更新和密钥请求912的同时向源MME发送UE上下文请求消息906。因此,步骤906、908和910可以与步骤914、916、918、920同时地执行。

[0084] 一旦目标MME已经从SKMF接收了K_{ASME},目标MME就可以随后执行与UE的非接入层安全模式命令过程922、924。在安全模式命令过程期间,由于目标MME向UE提供其GUMMEI,因此UE推导目标MME所使用的密钥K_{ASME}。一旦UE也具有与目标MME相同的K_{ASME},UE和目标MME就可以基于K_{ASME}密钥来参与安全通信。例如,目标MME可以参与与UE的跟踪区域更新交换926、

928,UE的通信通过K_{ASME}或根据K_{ASME}推导出的其它密钥(例如,NAS加密和完整性保护密钥)来加密。该交换可以包括从目标MME向UE发送的消息,其中该消息包括基于目标MME的GUMMEI的新GUTI。这种消息再次通过K_{ASME}或根据K_{ASME}推导出的另一个密钥来加密。

[0085] 如图9所示和上文所描述的,NAS SMC 922、924后面跟有跟踪区域更新过程926、928。在本公开内容的一些方面中,可以对NAS SMC 922、924和跟踪区域更新过程926、928进行组合。例如,从目标MME向UE发送的NAS SMC消息922可以与跟踪区域更新消息926进行组合。这样做,可以对组合的消息的仅部分(例如,与跟踪区域更新相关联的部分)进行加密,而消息中的帮助UE推导K_{ASME}的部分保持未加密。可以对MME所分配的新临时移动用户身份(TMSI)(其是GUTI的部分)进行加密。

[0086] 密钥推导

[0087] 如上所述,在UE与SKMF之间运行AKA。密钥K_{SKMF}由HSS推导并且被发送给SKMF。从HSS的角度看,认证向量以与4G LTE相同的方式来构造并且被发送给SKMF而不是MME。因此,HSS可以连接到SKMF而无需任何修改。

[0088] SKMF推导用于给定MME的特定于MME的密钥K_{ASME},并且因此MME的GUMMEI可以用于K_{ASME}密钥推导过程中。对于新K_{ASME},可以将NAS计数值初始化为零(0)。在一个示例中,如果跟踪区域更新没有完成,则不丢弃旧NAS计数值。为了密钥K_{ASME}的新鲜度,UE和SKMF可以保持密钥计数计数器值并且将其用于K_{ASME}推导。这可以被完成以避免在UE移动回到旧MME(例如,源MME)的情况中推导相同的K_{ASME}。当成功地执行初始AKA时,可以将密钥计数计数器值初始化为零(0)或某个其它预先确定的值。在一些方面中,可以使用nonce而不是密钥计数计数器值。在另一个方面中,可以从密钥推导中省略GUMMEI。

[0089] 用于生成密钥K_{SKMF}、K_{ASME}、K_{eNB}、下一跳跃(NH)等的密钥推导函数(KDF)可以使用HMAC-SHA-256、HMAC-SHA-3等。输入字符串S可以是构造自n+1个输入参数。例如,$S=[FC||P_0||L_0||P_1||L_1||P_2||L_2||\cdots||P_N||L_N]$。字段码FC可以是用于在算法的不同实例之间进行区分的单个八位字节并且可以使用在范围0x50-0x5F中的值。输入参数P_0至P_N是n+1个输入参数编码。P_0可以是静态的ASCII编码字符串。值L_0至L_N是对应的输入参数P_0至P_N的长度的两个八位字节表示。

[0090] K_{SKMF}推导。

[0091] $K_{SKMF}=KDF(K_{CK/IK},S)$。输入S可以等于$[FC||P_0||L_0||P_1||L_1]$,其中FC=0x50,P0=SN id,$L_0$=SN id的长度(即,$L_0$=0x00 0x03),$P_1$=SQN XOR AK,并且$L_1=P_1$的长度(即,$L_1$=0x00 0x06)。SQN是序列号并且AK是匿名密钥,并且XOR是异或运算。将值SQN XOR AK发送给UE作为认证令牌(AUTN)的部分。如果不使用AK,则可以根据TS 33.102来处理AK(即,000…0)。输入密钥$K_{CK/IK}$是加密密钥(CK)和完整性密钥(IK)的级联,即$K_{CK/IK}=CK||IK$。

[0092] K_{ASME}推导。

[0093] $K_{ASME}=KDF(K_{SKMF},S)$。输入S可以等于$[FC||P_0||L_0||P_1||L_1]$,其中FC=0x51,P_0=GUMMEI,L_0=48比特GUMMEI的长度(即,L_0=0x000x06),P_1=密钥计数,并且L_1可以等于P_1的长度(例如,L_1=0x00 0x08)。这仅是可以如何推导K_{ASME}的一个示例。在另一些方面中,可以省略GUMMEI,并且可以使用仅用一次的随机数(例如,nonce)而不是密钥计数计数器值。

[0094] NH推导。

[0095] $NH=KDF(K_{ASME},S)$。输入S可以等于$[FC||P_0||L_0]$,其中FC=0x52,P_0=Sync-Input,

L_0＝Sync-Input的长度(即,L0＝0x00 0x20)。对于初始的NH推导,Sync-Input参数可以是新推导的K_{eNB},而对于所有后续的推导,其可以是先前的NH。这产生了NH链,其中下一个NH总是新鲜的并且是根据先前的NH推导的。

[0096] K_{eNB}推导。

[0097] K'_{eNB}＝KDF(K_X,S)。当出于切换目的在UE和eNB中根据当前K_{eNB}或根据新鲜的NH和目标物理小区标识符推导K'_{eNB}(如条款7.2.8所规定的)时,输入S可以等于[FC||P_0||L_0||P_1||L_1],其中FC＝0x53,P_0＝目标物理小区标识符(PCI),L_0＝PCI的长度(例如,L_0＝0x00 0x02),P_1＝EARFCN-DL(目标物理小区下行链路频率),并且L_1＝P_1的长度(例如,L_1＝0x00 0x02)。当切换中的索引增加时,输入密钥K_X可以是256比特下一跳跃(NH)密钥,否则使用当前的256比特K_{eNB}。

[0098] 上文所示出和描述的图7-图9假定MME从源改变到目标MME。然而,当单个MME承担两个MME(源MME和目标MME)的角色并且在这两个MME之间不存在实际接口时,可以使用相同的过程流程图。

[0099] 在上文关于图7-图9和密钥推导的描述中,使用网络组件和相关术语的特定非排他性、非限制性示例来展示本申请的公开内容的方面。例如,“用户设备”可以仅是设备的一个示例。MME可以仅是控制平面设备的一个示例。SMKF可以仅是密钥管理设备的一个示例。MME标识符(例如,GUMMEI)可以仅是控制平面设备标识符的一个示例。跟踪区域可以仅是服务区域的一个示例,并且类似地,跟踪区域更新可以仅是服务区域更新的一个示例。SMC和NAS SMC可以仅是控制平面消息的一些示例。eNB可以仅是无线接入节点的一个示例。

[0100] 图10根据本公开内容的一个方面,示出了设备1000(例如,“用户设备”、“用户装置”、“无线设备”等)的示意框图。用户设备1000可以是任何无线通信设备,诸如但不限于移动电话、智能电话、膝上型计算机、个人数字助理(PDA)、平板计算机、计算机、智能手表和头戴式可穿戴计算机(例如,谷歌眼镜®)。用户设备1000可以包括可以彼此通信地耦合的至少一个或多个无线通信接口1002、一个或多个存储器电路1004、一个或多个输入和/或输出(I/O)设备/电路1006、和/或一个或多个处理电路1008。例如,接口1002、存储器电路1004、I/O设备1006和处理电路1008可以通过总线1010来彼此通信地耦合。无线通信接口1002允许用户设备1000与无线通信网络104无线地通信。因此,接口1002允许用户设备1000与诸如移动电信蜂窝网络之类的无线广域网(WWAN)以及短距离无线局域网(例如,WiFi®、紫蜂(Zigbee)®、蓝牙®等)无线地通信。

[0101] 存储器电路1004可以包括一个或多个易失性存储器电路和/或非易失性存储器电路。因此,存储器电路1004可以包括动态随机存取存储器(DRAM)、静态随机存取存储器(SRAM)、磁阻式随机存取存储器(MRAM)、电可擦除可编程只读存储器(EEPROM)、闪存等。存储器电路1004可以存储一个或多个密码密钥。存储器电路1004还可以存储可由处理器电路1008执行的指令。I/O设备/电路1006可以包括一个或多个键盘、鼠标、显示器、触摸屏显示器、打印机、指纹扫描器、以及任何其它输入和/或输出设备。

[0102] 处理电路1008(例如,处理器、中央处理单元(CPU)、应用处理单元(APU)等)可以执行在存储器电路1006处存储的指令和/或在通信地耦合到用户设备1000的另一个计算机可读存储介质(例如,硬盘驱动器、光盘驱动器、固态驱动器等)处存储的指令。处理电路1008

可以执行本文所描述的用户设备1000的步骤和/或过程中的任何一个步骤和/或过程，包括参照图2、图3、图4、图5、图6、图7、图8、图9、图11和图12论述的那些步骤和/或过程。

[0103] 图11示出了在设备处操作的方法1100。设备可以是集成电路、多个集成电路、或并入一个或多个集成电路的电子设备。该方法可以用于执行涉及控制平面设备重定位或改变服务区域的服务区域更新。首先，在设备处识别1102进入新服务区域(例如，新跟踪区域、新路由区域等)。接着，向与网络相关联的网络设备发送1104服务区域更新请求。随后，从网络接收1106控制平面消息(一个非限制性的、非排他性的示例包括安全模式命令)，该控制平面消息指示由于响应于发送服务区域更新请求的服务区域变化而引起的控制平面设备重定位或密钥刷新。接着，部分地基于在接收到的控制平面消息中包括的数据以及在设备与密钥管理设备(例如，SKMF)之间共享的第二密钥(例如，K_{SKMF})来推导1108第一密钥(例如，K_{ASME})，其中密钥管理设备与网络相关联。根据一个方面，控制平面消息是由于服务区域变化而从目标控制平面设备(例如，目标MME)接收的，目标控制平面设备是与当前对设备进行服务的控制平面设备不同的控制平面设备(例如，源MME)。根据另一个方面，在控制平面消息中包括的数据包括控制平面设备标识符(例如，MME标识符，诸如但不限于GUMMEI)，该控制平面设备标识符标识正在和/或将对设备进行服务的控制平面设备。

[0104] 根据一个方面，推导第一密钥还部分地基于被保持在密钥管理设备处并被包括在控制平面消息中的计数器值密钥计数。根据另一个方面，基于第一密钥来推导演进型节点B(eNB)密钥K_{eNB}、非接入层密钥K_{NAS}、和/或下一跳跃(NH)密钥中的至少一者以保护设备与网络之间的通信。根据再一个方面，新服务区域是新跟踪区域和/或新路由区域中的至少一者，并且服务区域更新请求与跟踪区域更新和/或路由区域更新中的至少一者相关联。

[0105] 根据一个方面，控制平面消息是安全模式命令，目标控制平面设备是目标MME，密钥管理设备是SKMF设备，并且第二密钥是用于认证会话的会话根密钥。根据另一个方面，控制平面设备保持针对设备的移动性管理上下文和会话管理上下文，并且密钥管理设备保持第二密钥。

[0106] 图12示出了在设备处操作的、用于执行涉及控制平面设备重定位或改变服务区域的切换的方法1200。首先，从与网络相关联的网络设备(例如，源eNB)接收1202切换命令，其中切换命令指示新服务区域(例如，新跟踪区域、新路由区域等)。接着，基于在切换命令中包括的数据以及基于在设备与密钥管理设备(例如，SKMF)之间共享的第二密钥(例如，K_{SKMF})来推导1204第一密钥(例如，K_{ASME})，其中密钥管理设备与网络相关联。随后，向网络设备发送1206基于第一密钥来保护的切换确认消息。

[0107] 根据一个方面，切换命令包括与对目标无线接入节点(例如，目标eNB)进行服务的目标控制平面设备(例如，目标MME)相关联的目标控制平面设备标识符(例如，可以包括GUMMEI的目标MME标识符)，该目标无线接入节点正在和/或将对设备进行服务。根据另一个方面，推导第一密钥部分地基于目标控制平面设备标识符。根据再一个方面，目标控制平面设备是目标移动性管理实体(MME)，密钥管理设备是会话密钥管理功能(SKMF)设备，并且目标控制平面设备标识符是与目标MME相关联的MME标识符。

[0108] 图13根据本公开内容的一个方面，示出了网络设备1300的示意框图。网络设备1300可以是MME、RAN、S-GW和/或P-GW。网络设备1300可以包括可以彼此通信地耦合的至少一个或多个无线通信接口1302、一个或多个存储器电路1304、一个或多个输入和/或输出

(I/O)设备/电路1306、和/或一个或多个处理电路1308。例如，接口1302、存储器电路1304、I/O设备1306和处理电路1308可以通过总线1310来彼此通信地耦合。无线通信接口1302允许网络设备1300与用户设备102无线地通信。因此，接口1302允许网络设备1300与诸如移动电信蜂窝网络之类的无线广域网(WWAN)和/或短距离无线局域网(例如，WiFi®、紫蜂(Zigbee)®、蓝牙®等)无线地通信。

[0109] 存储器电路1304可以包括一个或多个易失性存储器电路和/或非易失性存储器电路。因此，存储器电路1304可以包括DRAM、SRAM、MRAM、EEPROM、闪存等。存储器电路1304可以存储一个或多个密码密钥。存储器电路1304还可以存储可由处理器电路1308执行的指令。I/O设备/电路1306可以包括一个或多个键盘、鼠标、显示器、触摸屏显示器、打印机、指纹扫描器、以及任何其它输入和/或输出设备。

[0110] 处理电路1308(例如，处理器、中央处理单元(CPU)、应用处理单元(APU)等)可以执行在存储器电路1306处存储的指令和/或在通信地耦合到网络设备1300的另一个计算机可读存储介质(例如，硬盘驱动器、光盘驱动器、固态驱动器等)处存储的指令。处理电路1308可以执行本文所描述的网络设备的步骤和/或过程中的任何一个步骤和/或过程，包括参照图2、图3、图4、图5、图6、图7、图8、图9、图14和图15论述的那些步骤和/或过程。

[0111] 图14示出了在网络设备处操作的、用于在控制平面设备处执行涉及控制平面设备重定位或改变服务区域的跟踪区域更新的方法1400。首先，从设备(例如，用户设备)接收1402服务区域更新请求，针对该设备，网络设备不具有设备上下文(例如，UE上下文)或者该设备已改变服务区域(例如，跟踪区域或路由区域)。接着，向密钥管理设备(例如，SKMF)发送1404针对第一密钥(例如，K_{ASME})的请求。随后，从密钥管理设备接收1406第一密钥，其中第一密钥部分地基于在密钥管理设备与设备之间共享的第二密钥(例如，K_{SKMF})。接着，向设备发送1408控制平面消息，该控制平面消息包括允许该设备推导第一密钥的数据。根据一个方面，网络设备是移动性管理实体(MME)，并且第一密钥还基于标识MME的MME标识符。根据另一个方面，如果网络设备不具有设备上下文，则向先前对设备进行服务的在先控制平面设备发送设备上下文请求。

[0112] 根据一个方面，响应于发送设备上下文请求，从在先控制平面设备接收设备上下文。根据另一个方面，数据包括标识网络设备的控制平面设备标识符。根据再一个方面，从密钥管理设备接收计数器值密钥计数连同第一密钥。

[0113] 根据一个方面，计数器值密钥计数被包括在发送给设备的数据中。根据另一个方面，在从设备接收关于控制平面消息被成功地接收的通知之后，向该备发送服务区域更新。根据再一个方面，服务区域更新请求与跟踪区域更新和/或路由区域更新中的至少一者相关联，并且改变服务区域包括改变跟踪区域和/或改变路由区域中的至少一者。根据另一个方面，控制平面消息是非接入层安全模式命令，密钥管理设备是会话密钥管理功能(SKMF)设备，设备是用户设备，设备上下文是与用户设备相关联的用户设备上下文，并且第二密钥是用于认证会话的会话根密钥。

[0114] 图15示出了在网络设备处操作的、用于在控制平面设备处执行涉及控制平面设备重定位或改变服务区域的切换的方法1500。首先，在网络设备处从源控制平面设备接收1502前向重定位请求。接着，向会密钥管理(SKMF)设备发送1504针对第一密钥的请求。随后，从密钥管理设备接收1506第一密钥，其中第一密钥部分地基于在密钥管理设备与设备

之间共享的第二密钥。接着，利用根据第一密钥推导出的无线接入节点(RAN)会话密钥向目标RAN发送切换请求。根据一个方面，从目标RAN接收切换请求确认消息，该切换请求确认消息指示目标RAN将对设备进行服务。根据另一个方面，仅在从目标RAN接收切换请求确认消息之后，向密钥管理设备发送指示接收到第一密钥的确认消息。

[0115] 根据一个方面，向源控制平面设备发送前向重定位响应，该前向重定位响应包括被设备用于推导第一密钥的数据。根据另一个方面，网络设备是将对设备进行服务的目标控制平面设备，并且数据包括标识目标控制平面设备的目标控制平面设备标识符。根据再一个方面，目标控制平面设备是目标移动性管理实体(MME)，源控制平面设备是源MME，目标控制平面设备标识符是全球唯一MME标识符(GUMMEI)，密钥管理设备是会话密钥管理功能(SKMF)设备，并且设备是用户设备。根据再一个方面，接收计数器值密钥计数连同第一密钥。

[0116] 图16根据本公开内容的一个方面，示出了设备1600(例如，用户设备/装置)的框图。设备1600可以包括服务区域识别电路1602、服务区域更新请求发送电路1604、控制平面消息接收电路1606、和/或第一密钥推导电路1608，这些电路都可以经由通信总线1610来通信地耦合。设备1600的电路1602、1604、1606、1608中的每一个电路可以是专用电路(例如，专用集成电路(ASIC)、现场可编程门阵列(FPGA)等)，其被专门地连线以执行其相应的特定功能。

[0117] 服务区域识别电路1602可以是用于识别进入新服务区域的单元的一个示例。服务区域更新请求发送电路1604可以是用于向与网络相关联的网络设备发送服务区域更新请求的单元的一个示例。控制平面消息接收电路1606可以是用于从网络接收控制平面消息的单元的一个示例，该控制平面消息指示由于响应于发送服务区域更新请求的服务区域变化而引起的控制平面设备重定位或密钥刷新。第一密钥推导电路1608可以是用于部分地基于在接收到的控制平面消息中包括的数据以及在设备与密钥管理设备之间共享的第二密钥来推导第一密钥的单元的一个示例。

[0118] 图17根据本公开内容的一个方面，示出了设备1700(例如，用户设备/装置)的框图。设备1700可以包括切换命令接收电路1702、第一密钥推导电路1704、和/或切换确认发送电路1706，这些电路都可以经由通信总线1708来通信地耦合。设备1700的电路1702、1704、1706中的每一个电路可以是专用电路(例如，ASIC、FPGA等)，其被专门地连线以执行其相应的特定功能。

[0119] 切换命令接收电路1702可以是用于从与网络相关联的网络设备接收切换命令的单元的一个示例，该切换命令指示新服务区域。第一密钥推导电路1704可以是用于基于在切换命令中包括的数据以及在设备与密钥管理设备之间共享的第二密钥来推导第一密钥的单元的一个示例。切换确认发送电路1706可以是用于发送基于第一密钥来保护的切换确认消息的单元的一个示例。

[0120] 图18根据本公开内容的一个方面，示出了网络设备1800(例如，MME)的框图。设备1800可以包括第一密钥请求发送电路1802、服务区域更新请求接收电路1804、第一密钥接收电路1806、和/或控制平面消息发送电路1808，这些电路都可以经由通信总线1810来通信地耦合。网络设备1800的电路1802、1804、1806、1808中的每一个电路可以是专用电路(例如，ASIC、FPGA等)，其被专门地连线以执行其相应的特定功能。

[0121] 第一密钥请求发送电路1802可以是用于向密钥管理设备发送针对第一密钥的请求的单元的一个示例。服务区域更新请求接收电路1804可以是用于从设备接收服务区域更新请求的单元的一个示例，针对该设备，网络设备不具有设备上下文或该设备已改变服务区域。第一密钥接收电路1806可以是用于从密钥管理设备接收第一密钥的单元的一个示例，第一密钥部分地基于在密钥管理设备与设备之间共享的第二密钥。控制平面消息发送电路1808可以是用于向设备发送控制平面消息的单元的一个示例，该控制平面消息包括允许设备推导第一密钥的数据。

[0122] 图19根据本公开内容的一个方面，示出了网络设备1900(例如，MME)的框图。设备1900可以包括前向重定位请求接收电路1902、第一密钥请求发送电路1904、第一密钥接收电路1906、和/或切换请求发送电路1908，这些电路都可以经由通信总线1910来通信地耦合。网络设备1900的电路1902、1904、1906、1908中的每一个可以是专用电路(例如，ASIC、FPGA等)，其被专门地连线以执行其相应的特定功能。

[0123] 前向重定位请求接收电路1902可以是用于在网络设备处从源控制平面设备接收前向重定位请求的单元的一个示例。第一密钥请求发送电路1904可以是用于向密钥管理设备发送针对第一密钥的请求的单元的一个示例。第一密钥接收电路1906可以是用于从密钥管理设备接收第一密钥的单元的一个示例，第一密钥部分地基于在密钥管理设备与设备之间共享的第二密钥。切换请求发送电路1908可以是用于利用根据第一密钥推导出的无线接入节点(RAN)会话密钥向目标RAN发送切换请求的单元的一个示例。

[0124] 图2、图3、图4、图5、图6、图7、图8、图9、图10、图11、图12、图13、图14、图15、图16、图17、图18和/或图19中所示出的组件、步骤、特征和/或功能中的一个或多个可以被重新排列和/或组合成单个组件、步骤、特征、或功能，或可以体现在若干组件、步骤或功能中。在不脱离本发明的情况下还可以添加额外的元件、组件、步骤、和/或功能。图1、图3、图4、图5、图7、图8、图9、图10、图13、图16、图17、图18、和/或图19中所示出的装置、设备和/或组件可以被配置为执行在图2、图6、图7、图8、图9、图11、图12、图14和/或图15中所描述的方法、特征或步骤中的一个或多个。本文所描述的算法还可以高效地实现在软件中和/或嵌入在硬件中。

[0125] 此外，应当注意，本公开内容的方面可能是作为被描绘为流程图、流图、结构图、或框图的过程来描述的。尽管流程图可能会把操作描述为顺序过程，但是这些操作中的许多操作能够并行或并发地执行。此外，这些操作的次序可以被重新排列。过程在其操作完成时终止。过程可以对应于方法、函数、规程、子例程、子程序等。当过程对应于函数时，其终止对应于该函数返回至调用函数或主函数。

[0126] 此外，存储介质可以表示用于存储数据的一个或多个设备，包括只读存储器(ROM)、随机存取存储器(RAM)、磁盘存储介质、光学存储介质、闪存设备、和/或用于存储信息的其它机器可读介质和处理器可读介质、和/或计算机可读介质。术语“机器可读介质”、“计算机可读介质”和/或“处理器可读介质”可以包括但不限于诸如便携式或固定的存储设备、光学存储设备之类的非暂时性介质以及能够存储或包含指令和/或数据的各种其它介质。因此，本文所描述的各种方法可以完全或部分地由可存储在“机器可读介质”、“计算机可读介质”和/或“处理器可读介质”中并由一或多个处理器、机器和/或设备执行的指令及/或数据来实现。

[0127] 此外，本公开内容的方面可以由硬件、软件、固件、中间件、微代码、或其任意组合

来实现。当用软件、固件、中间件或微代码来实现时，用于执行必要任务的程序代码或代码段可以存储在诸如存储介质或其它存储装置之类的机器可读介质中。处理器可以执行必要任务。代码段可以表示过程、函数、子程序、程序、例程、子例程、模块、软件包、类、或者指令、数据结构或程序语句的任意组合。代码段可以通过传递和/或接收信息、数据、自变量、参数或存储器内容而耦合到另一代码段或硬件电路。信息、自变量、参数、数据等可以经由包括存储器共享、消息传递、令牌传递、网络传输等任何合适的方式来传递、转发或发送。

[0128] 结合本文公开的示例所描述的各种说明性的逻辑框、模块、电路、元件和/或组件可以利用被设计为执行本文所描述的功能的通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑组件、分立门或晶体管逻辑、分立硬件组件、或者其任意组合来实现或执行。通用处理器可以是微处理器，但在替代方案中，处理器可以是任何常规的处理器、控制器、微控制器或状态机。处理器还可以实现为计算组件的组合，例如，DSP与微处理器的组合、多个微处理器、一个或多个微处理器结合DSP内核，或者任何其它此种配置。

[0129] 结合本文公开的示例所描述的方法或算法可以以处理单元、编程指令或其它指示的形式直接体现在硬件中、可由处理器执行的软件模块中、或两者的组合中，并且可以包含在单个设备中或跨越多个设备分布。软件模块可以驻留在RAM存储器、闪存、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、可移动盘、CD-ROM、或者本领域已知的任何其它形式的存储介质中。存储介质可以耦合到处理器，以使得处理器能够从存储介质读取信息以及向存储介质写入信息。在替代方案中，存储介质可以集成到处理器。

[0130] 本领域技术人员还将明白，结合本文公开的方面所描述的各个说明性的逻辑框、模块、电路和算法步骤可以实现为电子硬件、计算机软件或两者的组合。为了清楚地说明硬件和软件的这种可互换性，上文已经围绕说明性的组件、框、模块、电路和步骤的功能性对它们进行了一般地描述。至于这种功能是实现为硬件还是软件，取决于特定应用和施加在整体系统上的设计约束。

[0131] 在不脱离本发明的情况下，可以在不同系统中实现本文所描述的本发明的各种特征。应当注意，本公开内容的前述方面仅是示例，并不应解释为限制本发明。本公开内容的方面的描述旨在是说明性的，并不旨在限制权利要求书的范围。因此，本教导可以容易应用于其它类型的装置，并且许多替代方案、修改及变型对于本领域技术人员来说将是显而易见的。

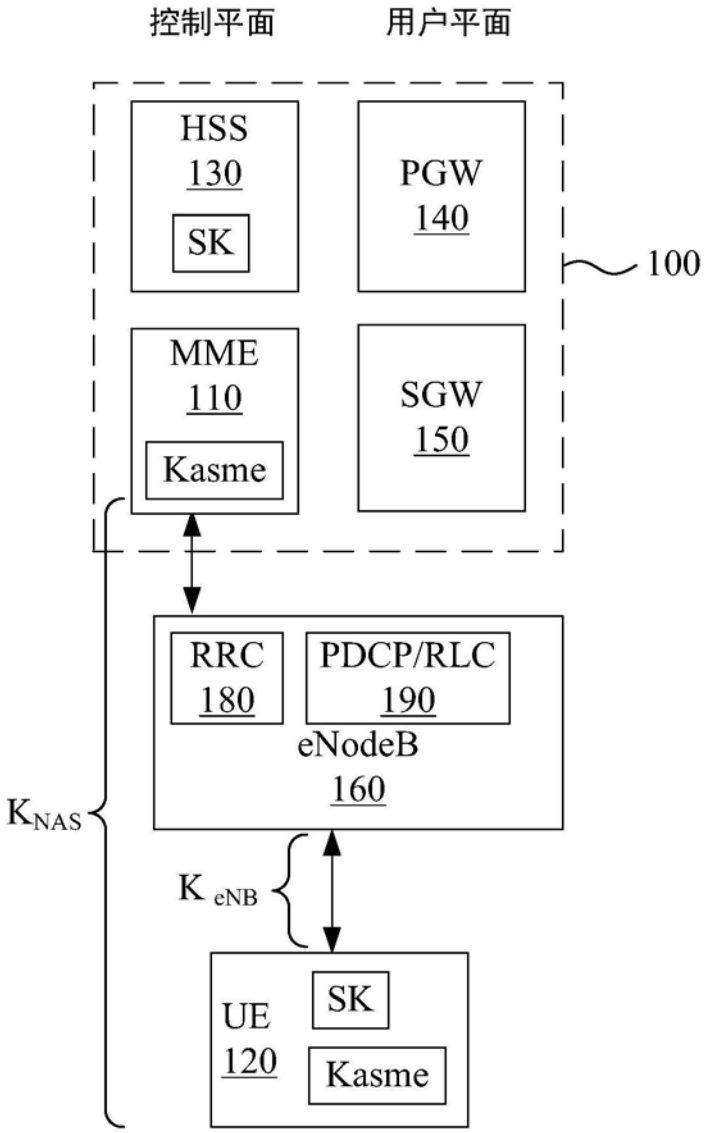

控制平面
用户平面
HSS
130
SK
PGW
140
100
MME
110
Kasme
SGW
150
RRC
180
PDCP/RLC
190
eNodeB
160
K_{NAS}
K_{eNB}
UE
120
SK
Kasme

图1现有技术

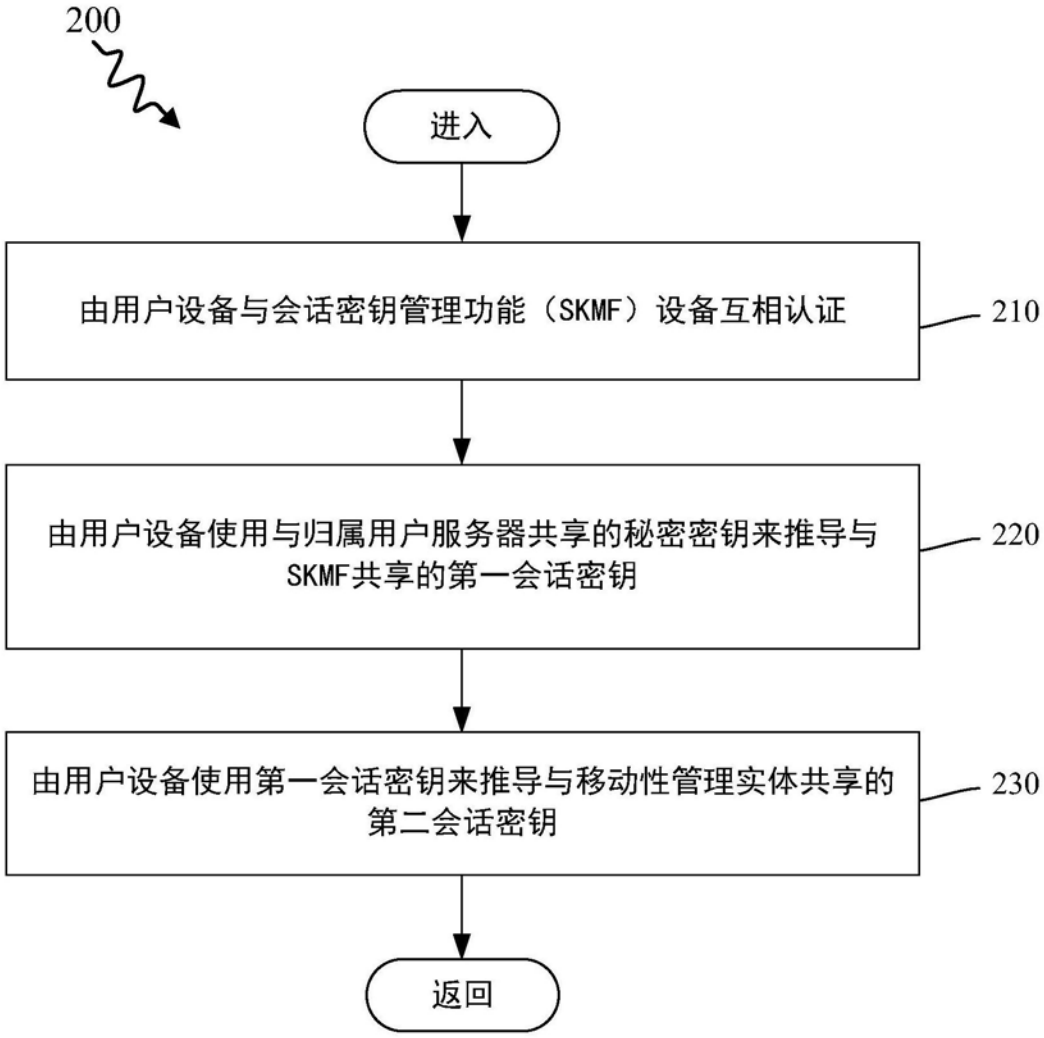

200
进入
由用户设备与会话密钥管理功能（SKMF）设备互相认证
210
由用户设备使用与归属用户服务器共享的秘密密钥来推导与SKMF共享的第一会话密钥
220
由用户设备使用第一会话密钥来推导与移动性管理实体共享的第二会话密钥
230
返回

图2

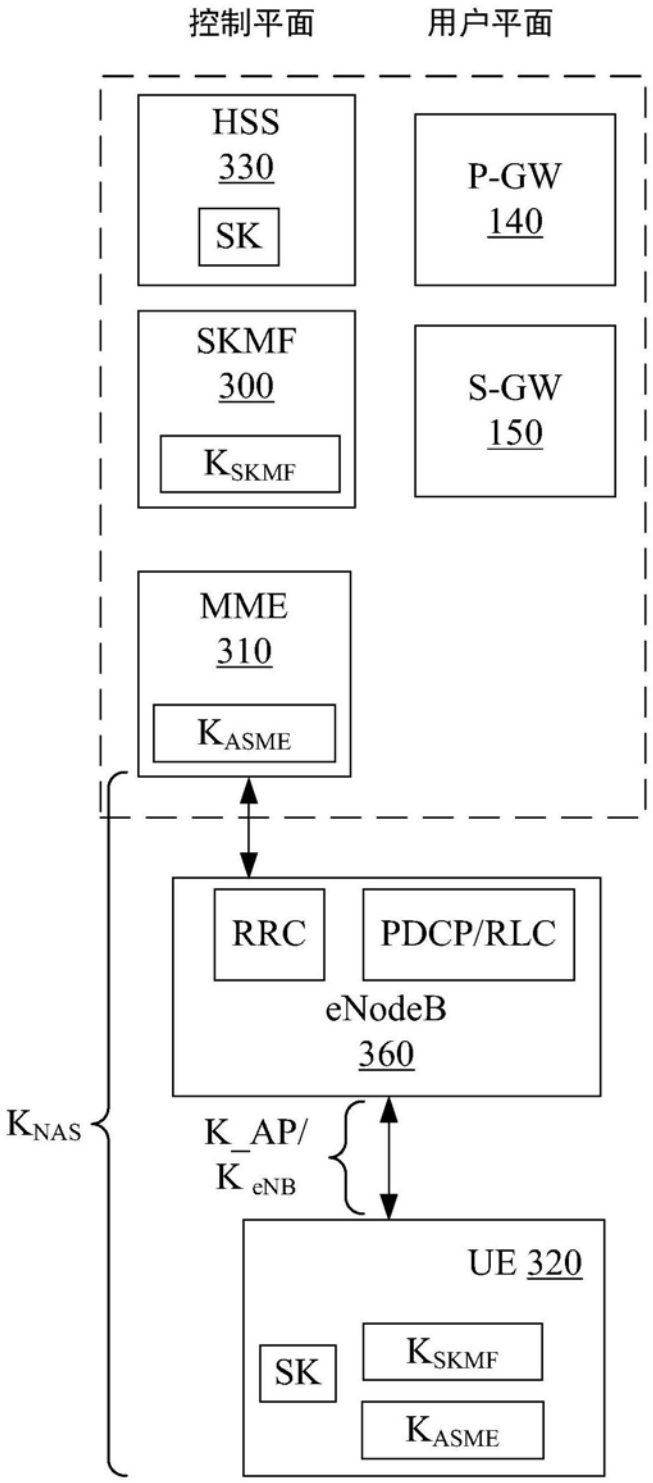

控制平面
用户平面
HSS
330
SK
P-GW
140
SKMF
300
K_{SKMF}
S-GW
150
MME
310
K_{ASME}
RRC
PDCP/RLC
eNodeB
360
K_{NAS}
K_AP/
K_{eNB}
UE 320
SK
K_{SKMF}
K_{ASME}

图3

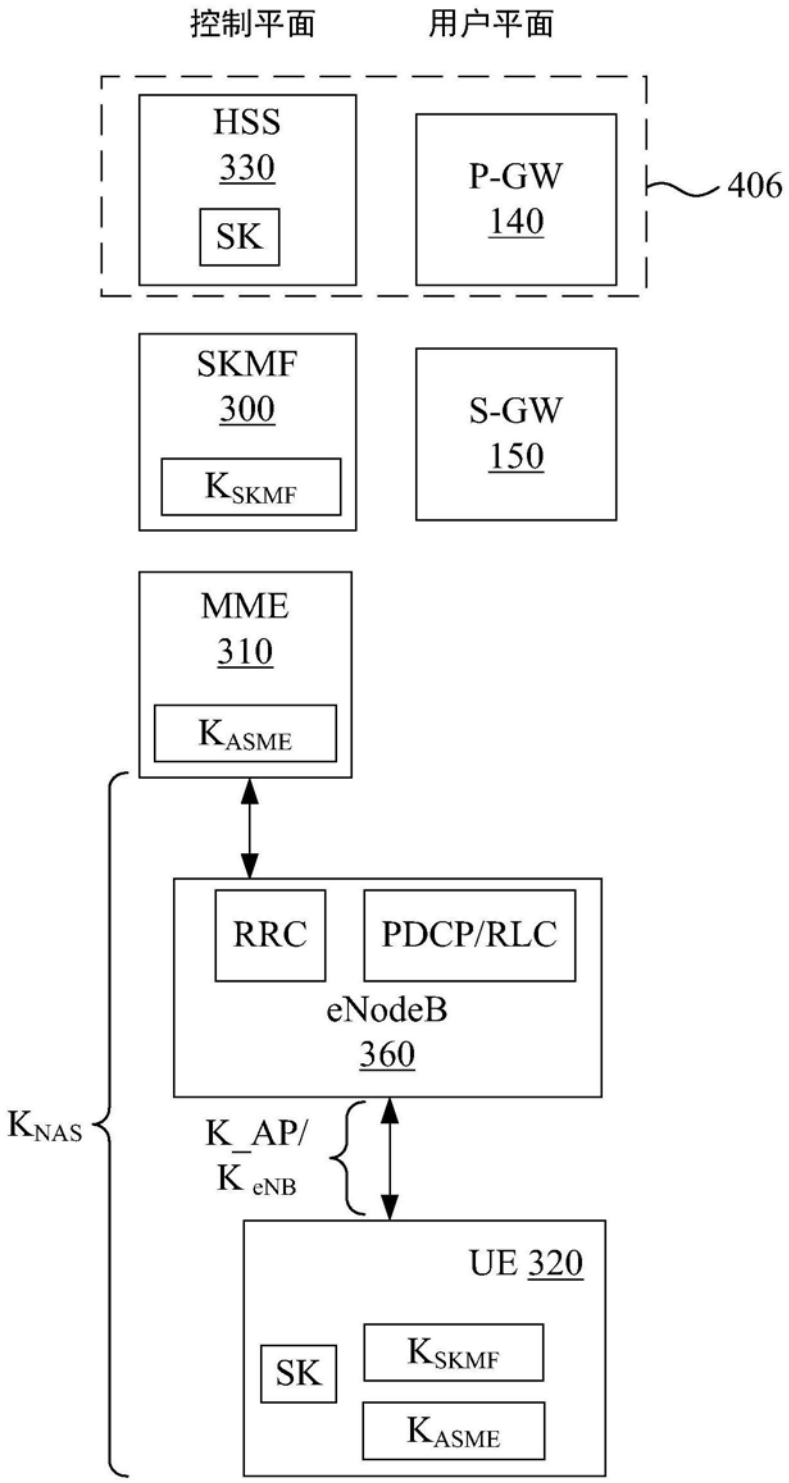

控制平面
用户平面
HSS
330
SK
P-GW
140
406
SKMF
300
K_{SKMF}
S-GW
150
MME
310
K_{ASME}
RRC
PDCP/RLC
eNodeB
360
K_{NAS}
K_AP/
K eNB
UE 320
SK
K_{SKMF}
K_{ASME}

图4

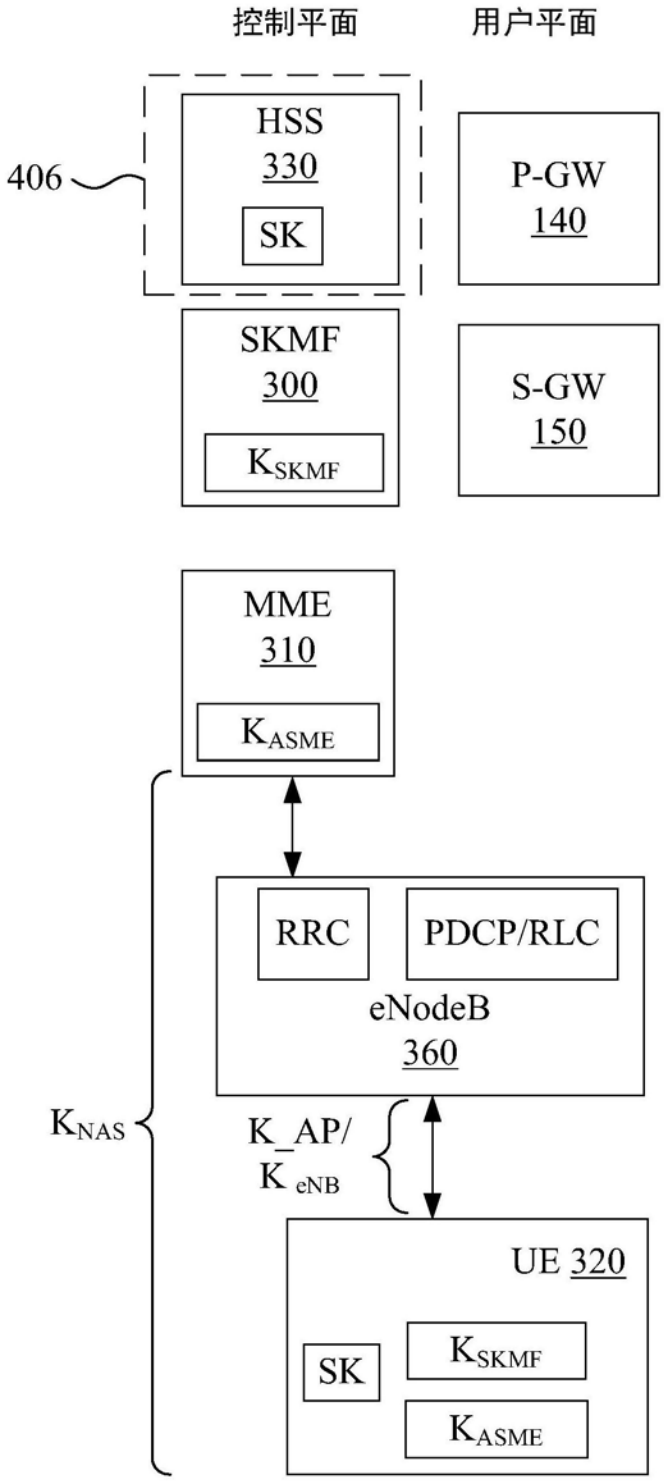

控制平面
用户平面
406
HSS
330
SK
P-GW
140
SKMF
300
K_{SKMF}
S-GW
150
MME
310
K_{ASME}
RRC
PDCP/RLC
eNodeB
360
K_{NAS}
K_AP/
K_{eNB}
UE 320
SK
K_{SKMF}
K_{ASME}

图5

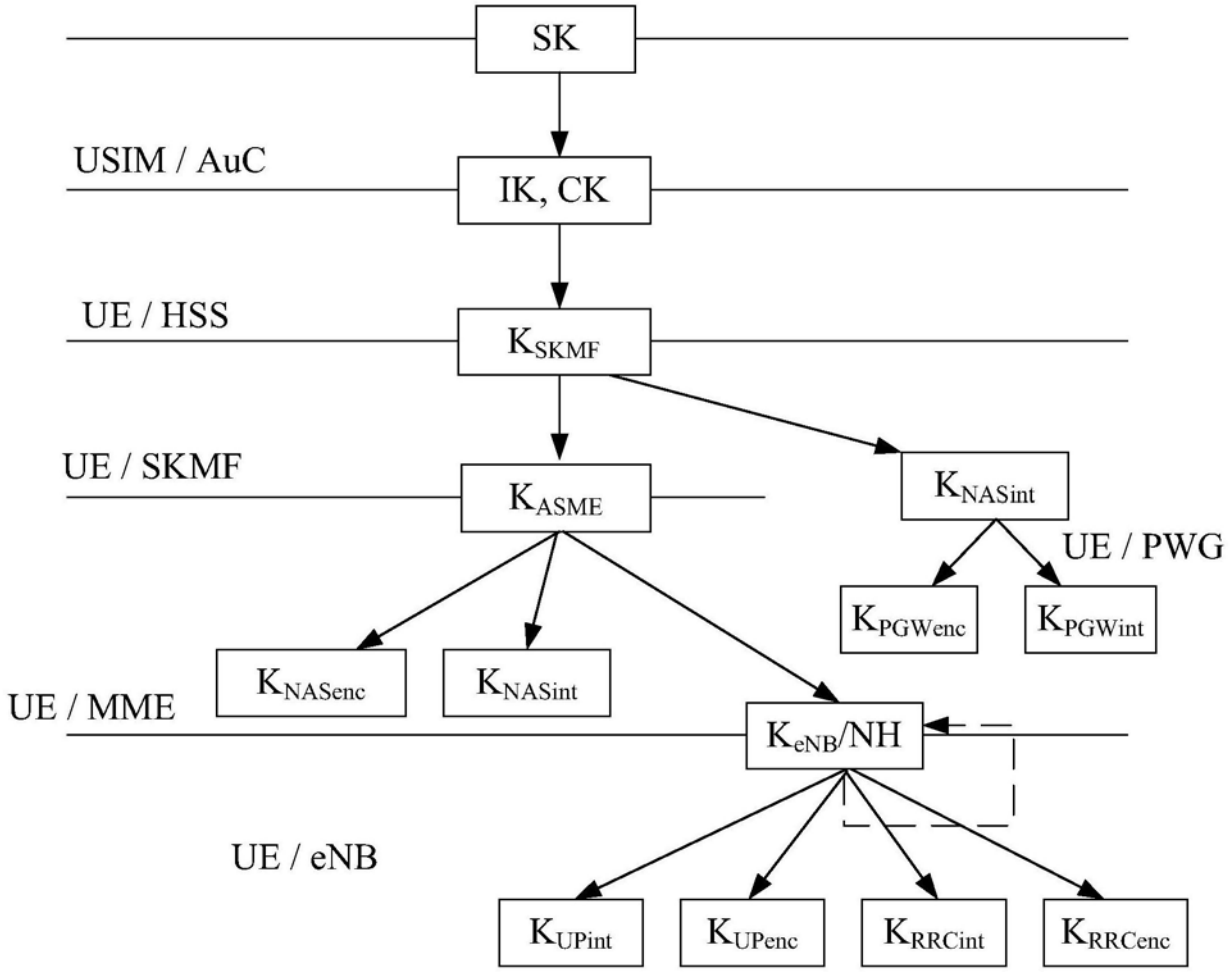

SK
USIM / AuC
IK, CK
UE / HSS
K_{SKMF}
UE / SKMF
K_{ASME}
K_{NASint}
UE / PWG
K_{PGWenc}
K_{PGWint}
K_{NASenc}
K_{NASint}
UE / MME
K_{eNB}/NH
UE / eNB
K_{UPint}
K_{UPenc}
K_{RRCint}
K_{RRCenc}

图6

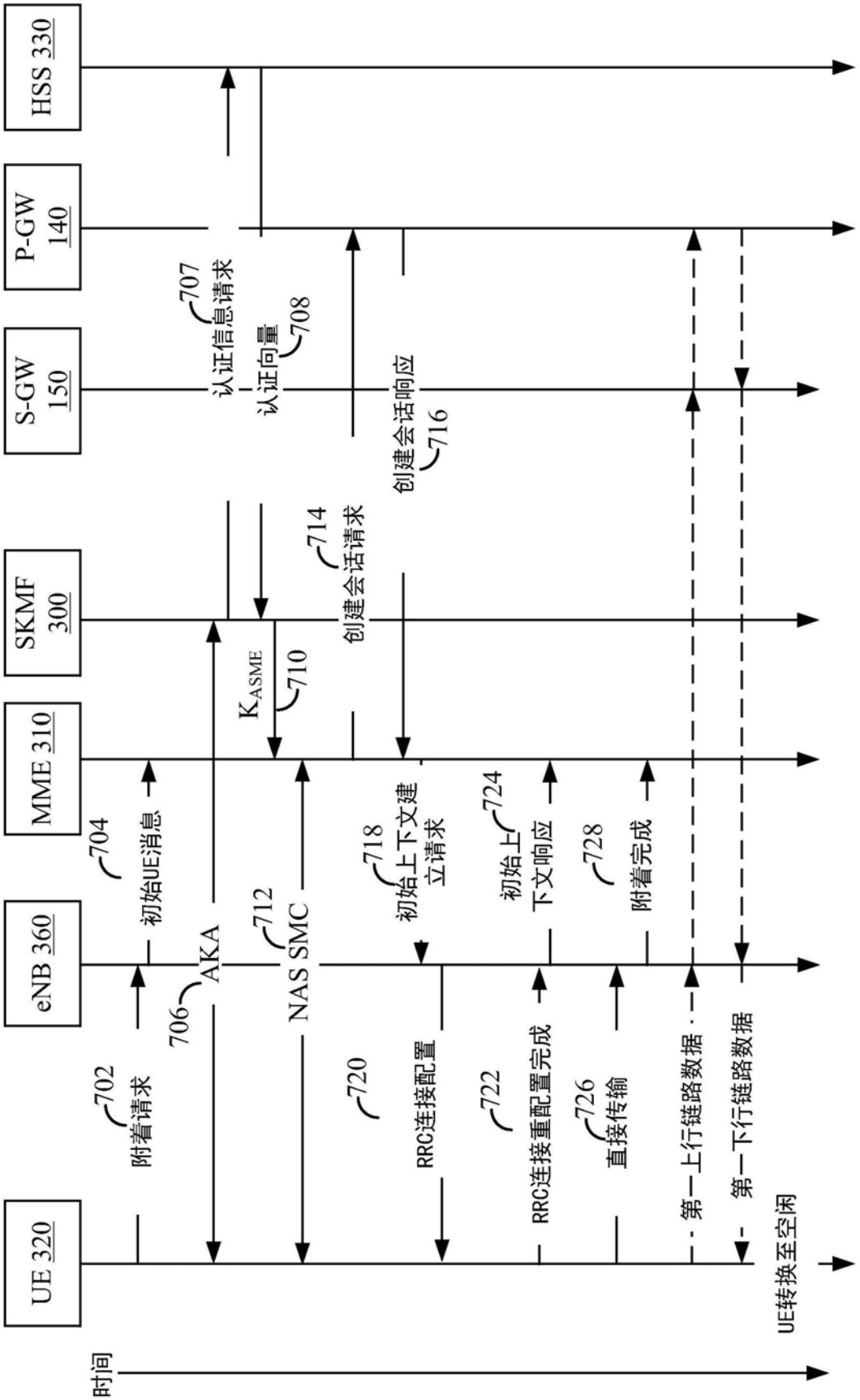

UE 320
eNB 360
MME 310
SKMF 300
S-GW 150
P-GW 140
HSS 330
时间
702 附着请求
704 初始UE消息
706 AKA
707 认证信息请求
708 认证向量
710 K_{ASME}
712 NAS SMC
714 创建会话请求
716 创建会话响应
718 初始上下文建立请求
720 RRC连接配置
722 RRC连接重配置完成
724 初始上下文响应
726 直接传输
728 附着完成
第一上行链路数据
第一下行链路数据
UE转换至空闲

图7

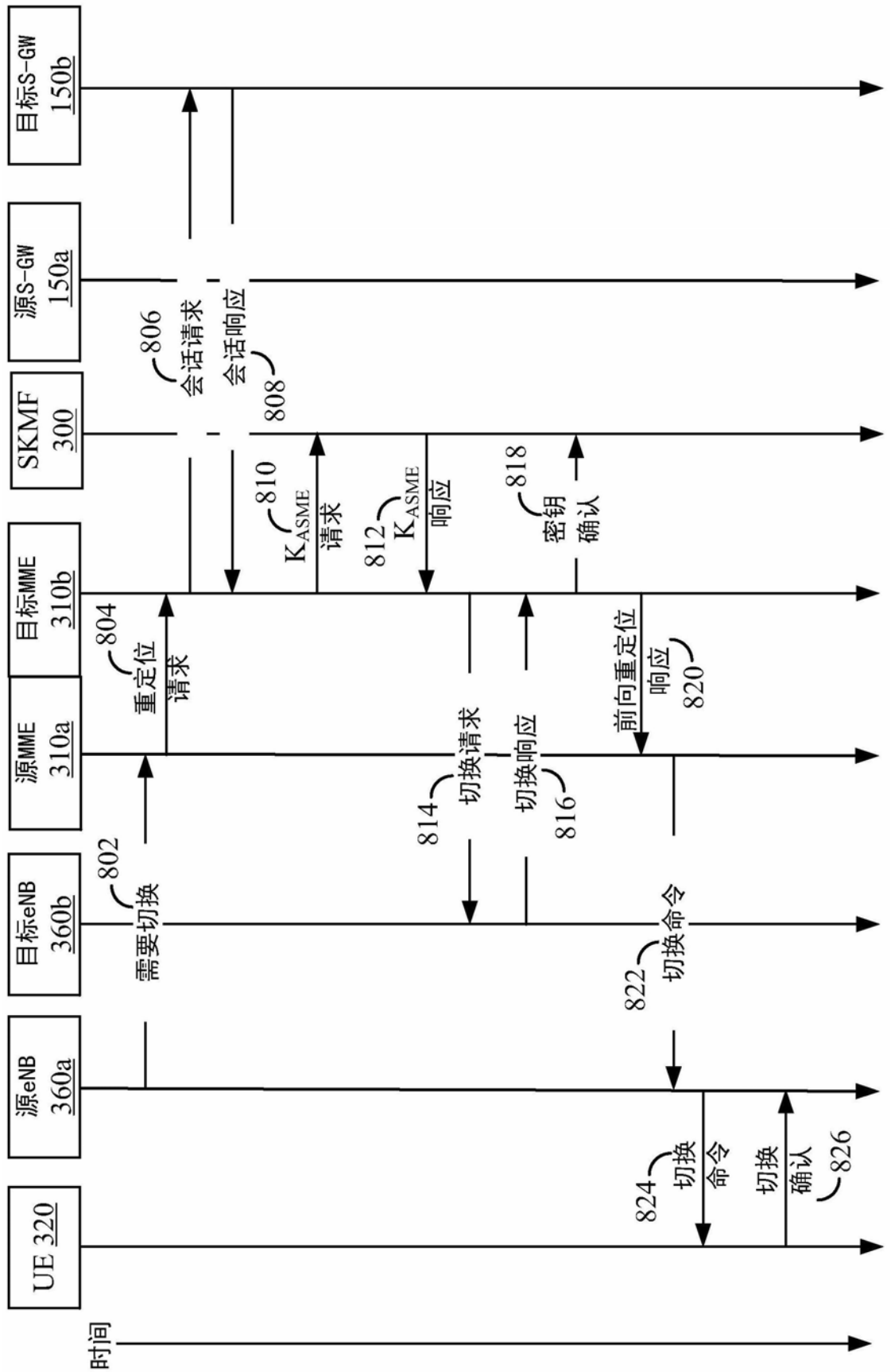

UE 320
源eNB 360a
目标eNB 360b
源MME 310a
目标MME 310b
SKMF 300
源S-GW 150a
目标S-GW 150b
时间
802 需要切换
804 重定位请求
806 会话请求
808 会话响应
810 K_{ASME} 请求
812 K_{ASME} 响应
814 切换请求
816 切换响应
818 密钥确认
820 前向重定位响应
822 切换命令
824 切换命令
826 切换确认

图8

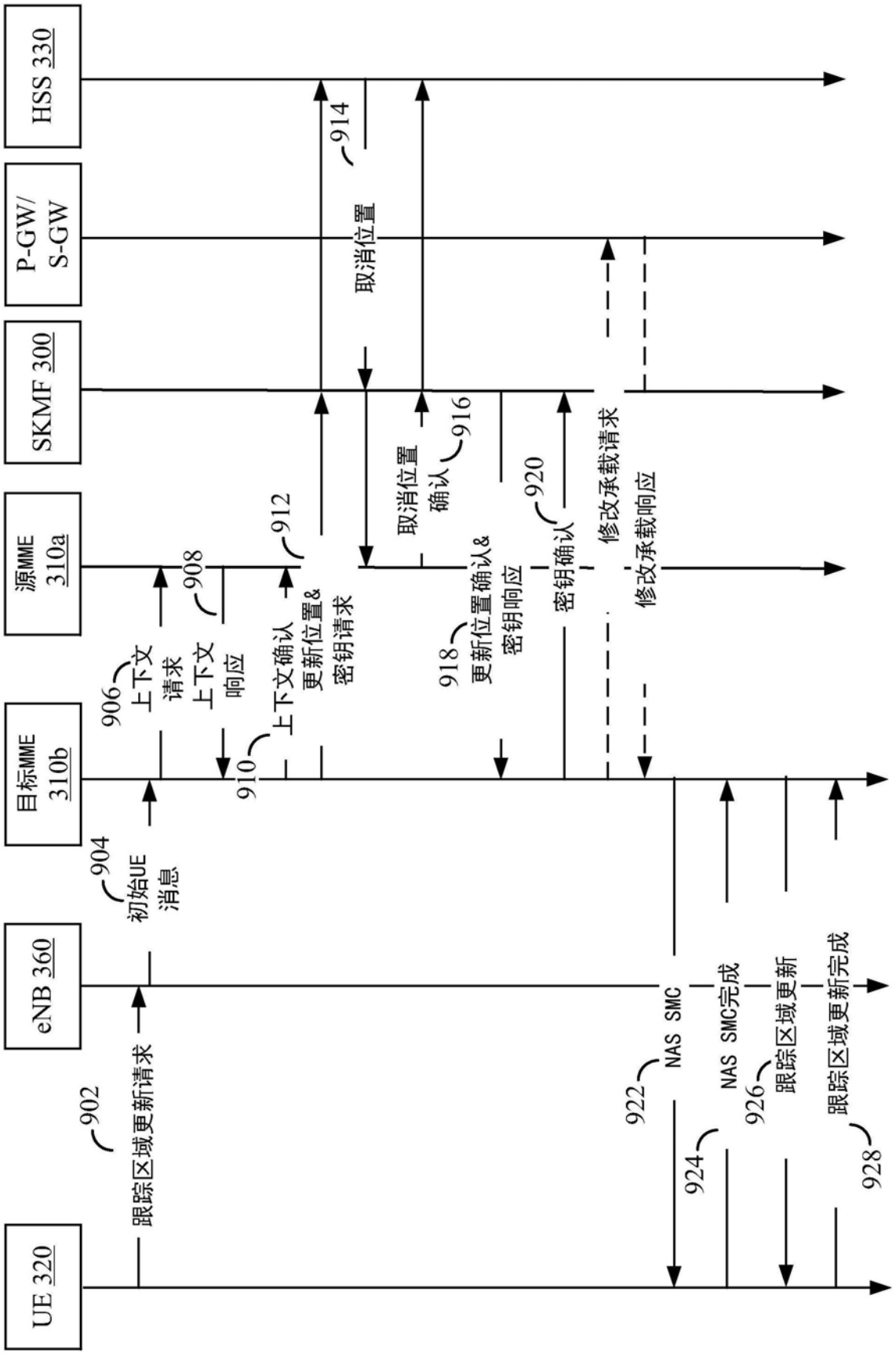

UE 320
eNB 360
目标MME 310b
源MME 310a
SKMF 300
P-GW/ S-GW
HSS 330
902 跟踪区域更新请求
904 初始UE 消息
906 上下文请求
908 上下文响应
910 上下文确认
912 更新位置& 密钥请求
914 取消位置
916 取消位置确认
918 更新位置确认& 密钥响应
920 密钥确认
修改承载请求
修改承载响应
922 NAS SMC
924
926 NAS SMC完成
跟踪区域更新
928 跟踪区域更新完成

图9

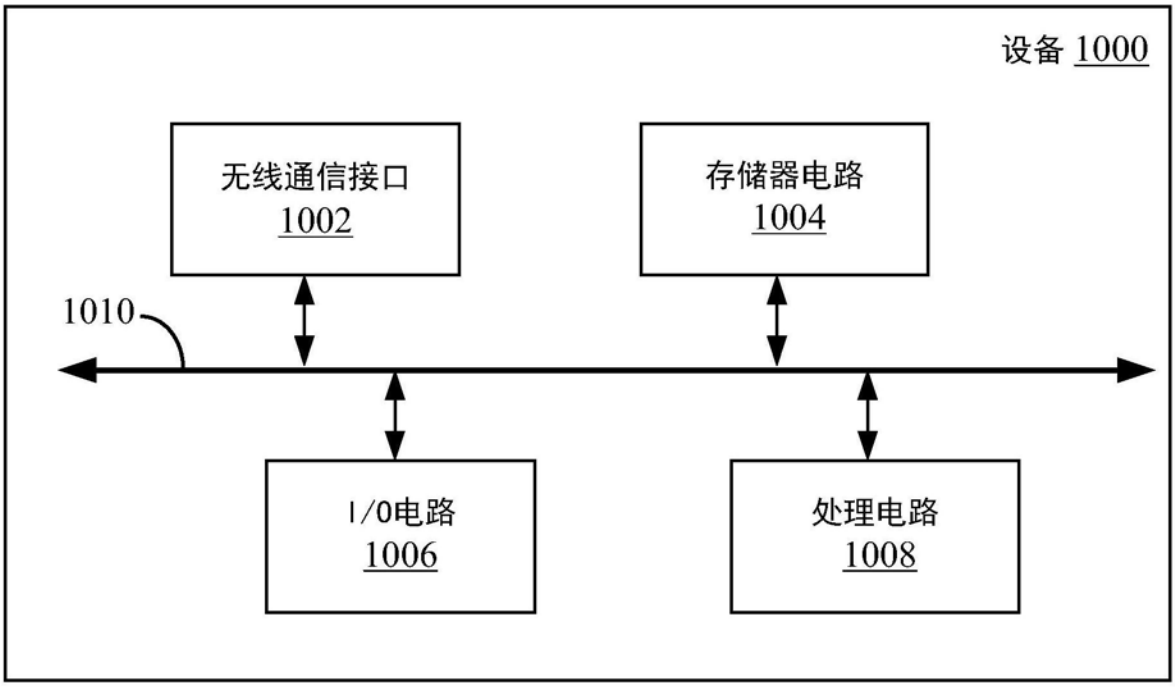


图10

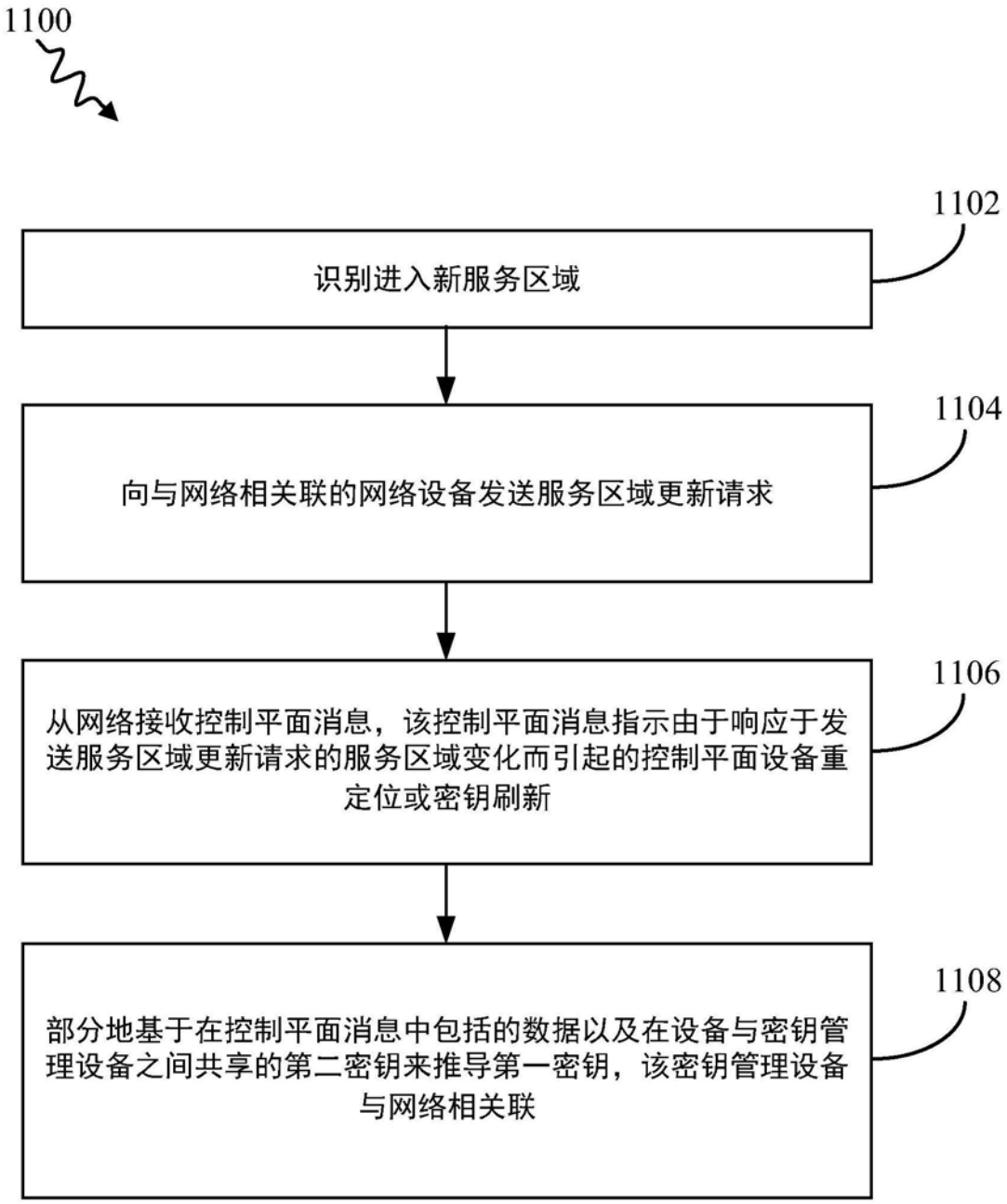

1100
1102
识别进入新服务区域
1104
向与网络相关联的网络设备发送服务区域更新请求
1106
从网络接收控制平面消息，该控制平面消息指示由于响应于发送服务区域更新请求的服务区域变化而引起的控制平面设备重定位或密钥刷新
1108
部分地基于在控制平面消息中包括的数据以及在设备与密钥管理设备之间共享的第二密钥来推导第一密钥，该密钥管理设备与网络相关联

图11

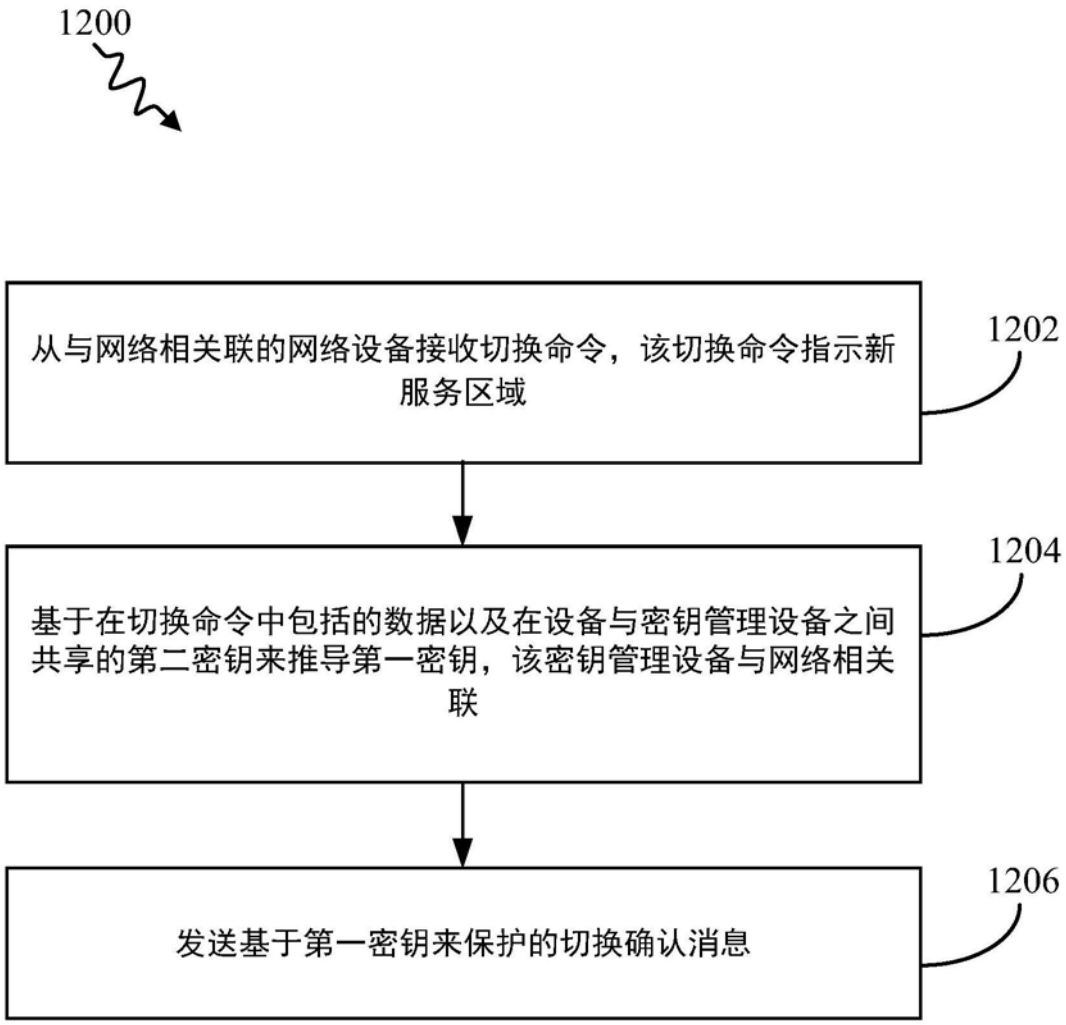

1200
从与网络相关联的网络设备接收切换命令，该切换命令指示新服务区域
1202
基于在切换命令中包括的数据以及在设备与密钥管理设备之间共享的第二密钥来推导第一密钥，该密钥管理设备与网络相关联
1204
发送基于第一密钥来保护的切换确认消息
1206

图12

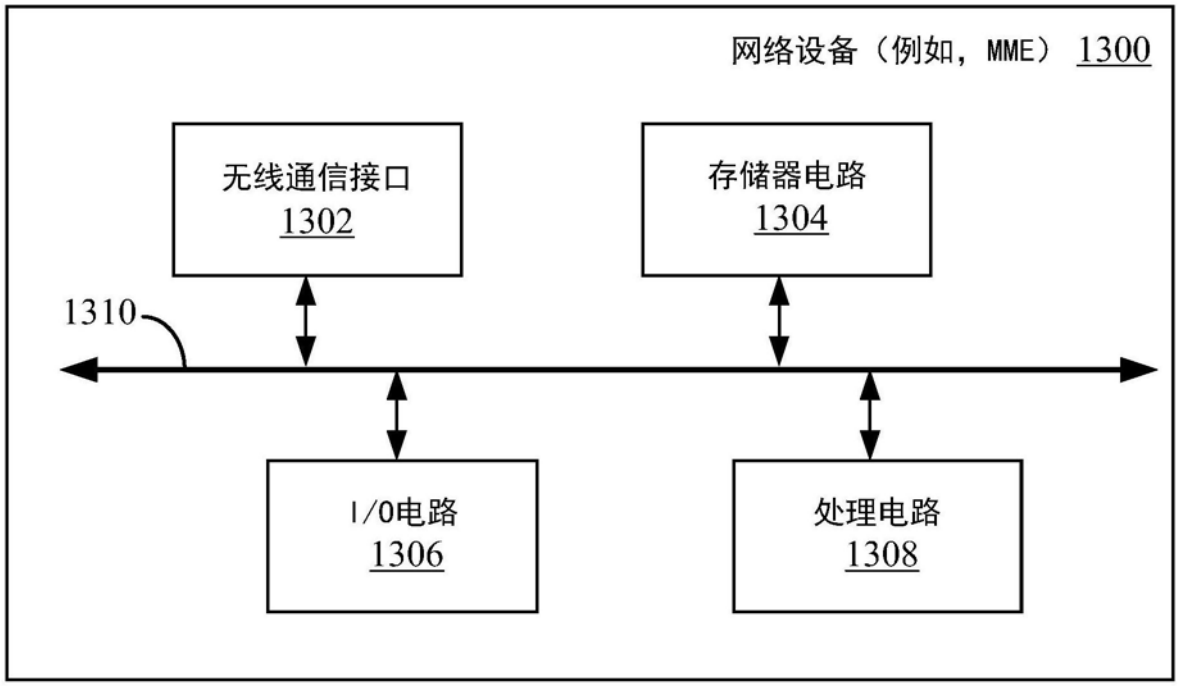

网络设备（例如，MME） 1300
无线通信接口
1302
存储器电路
1304
1310
I/O电路
1306
处理电路
1308

图13

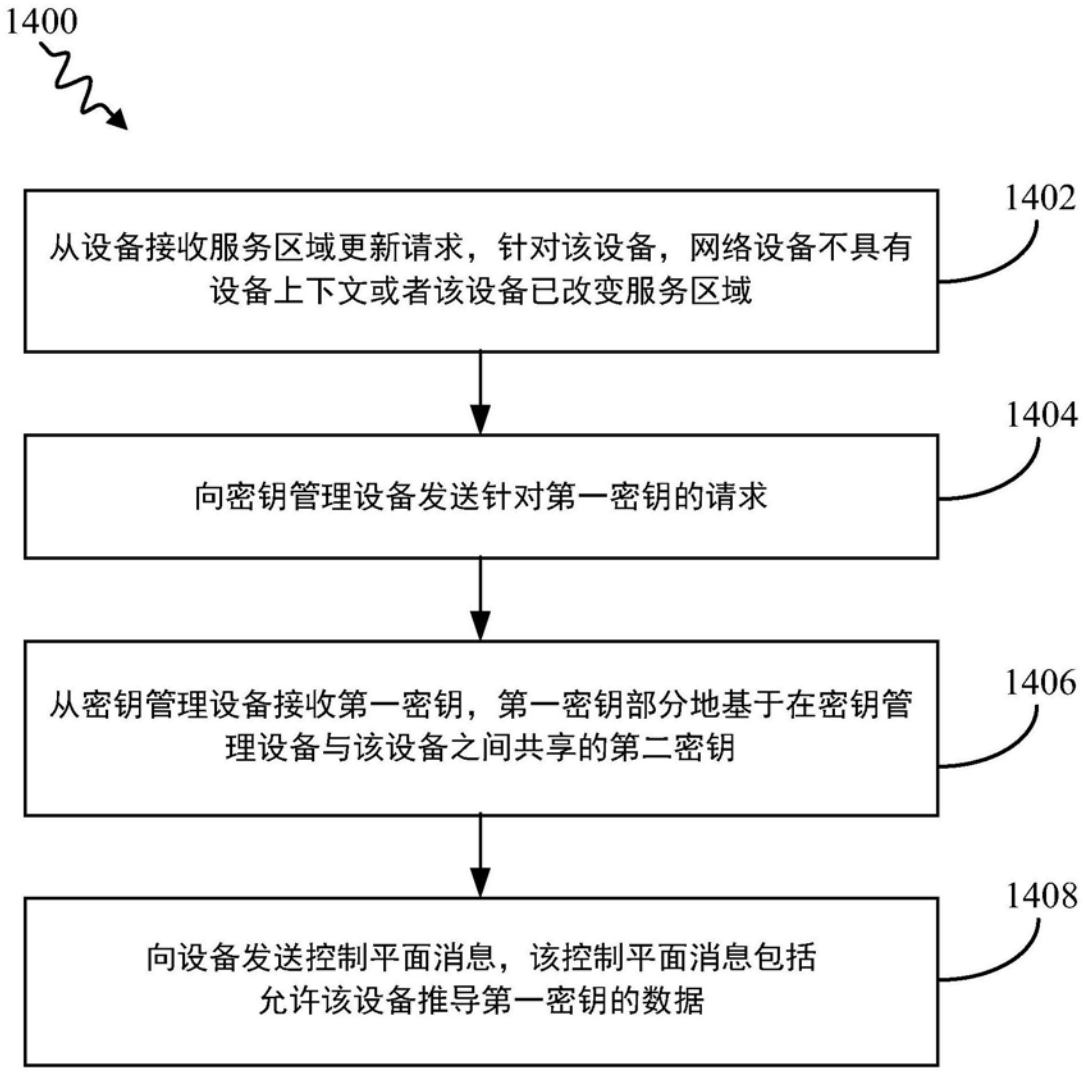

1400
从设备接收服务区域更新请求，针对该设备，网络设备不具有设备上下文或者该设备已改变服务区域
1402
向密钥管理设备发送针对第一密钥的请求
1404
从密钥管理设备接收第一密钥，第一密钥部分地基于在密钥管理设备与该设备之间共享的第二密钥
1406
向设备发送控制平面消息，该控制平面消息包括允许该设备推导第一密钥的数据
1408

图14

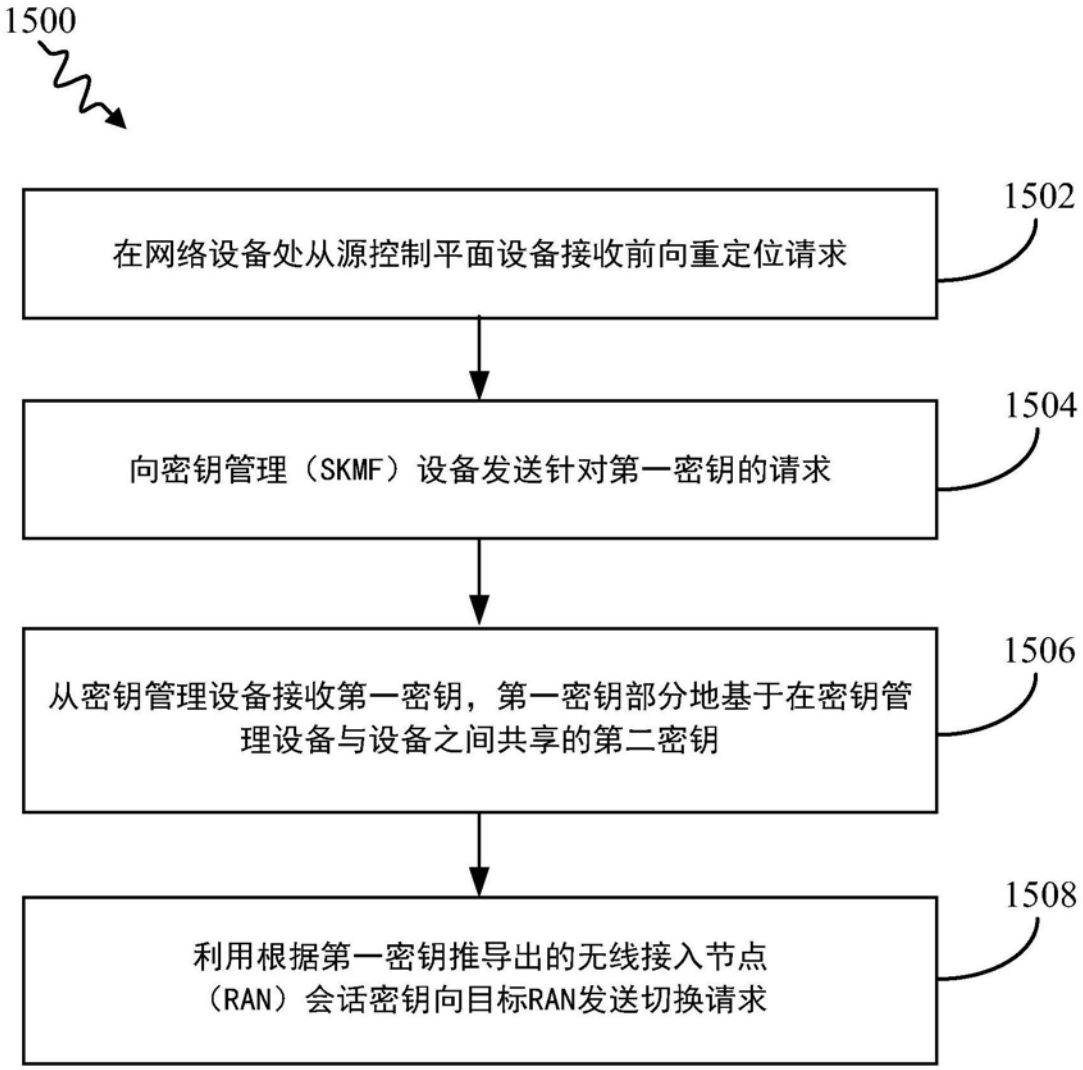

1500
在网络设备处从源控制平面设备接收前向重定位请求
1502
向密钥管理（SKMF）设备发送针对第一密钥的请求
1504
从密钥管理设备接收第一密钥，第一密钥部分地基于在密钥管理设备与设备之间共享的第二密钥
1506
利用根据第一密钥推导出的无线接入节点（RAN）会话密钥向目标RAN发送切换请求
1508

图15

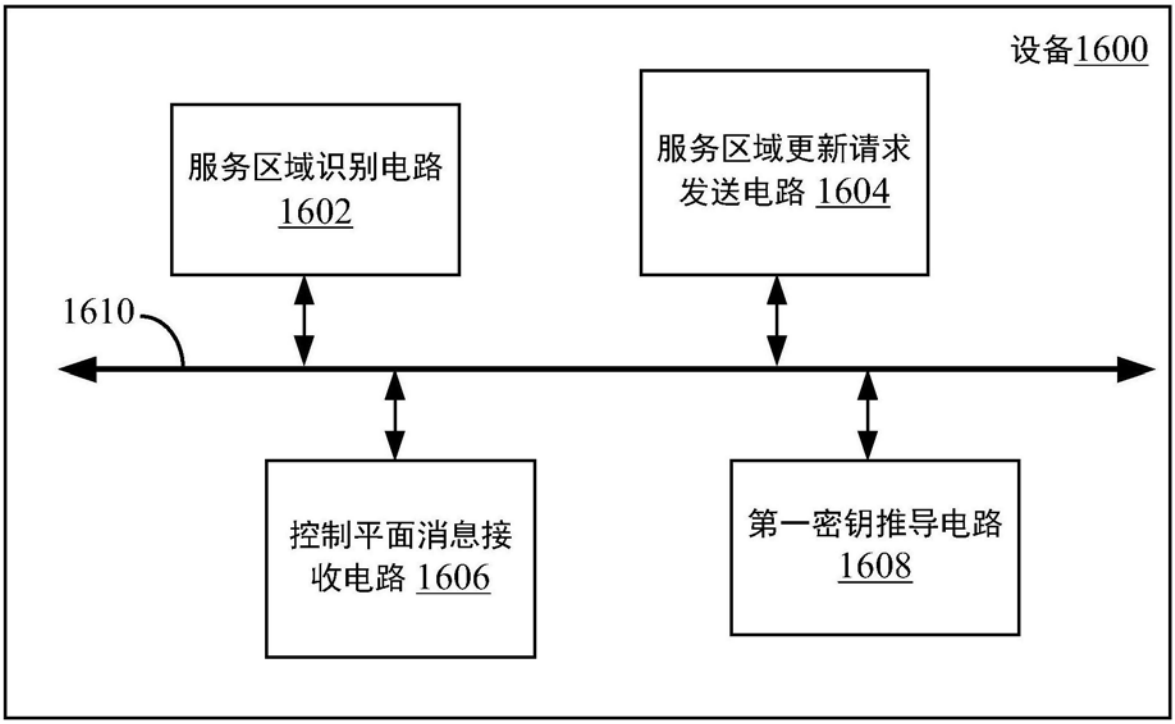

设备1600
服务区域识别电路 1602
服务区域更新请求发送电路 1604
1610
控制平面消息接收电路 1606
第一密钥推导电路 1608

图16

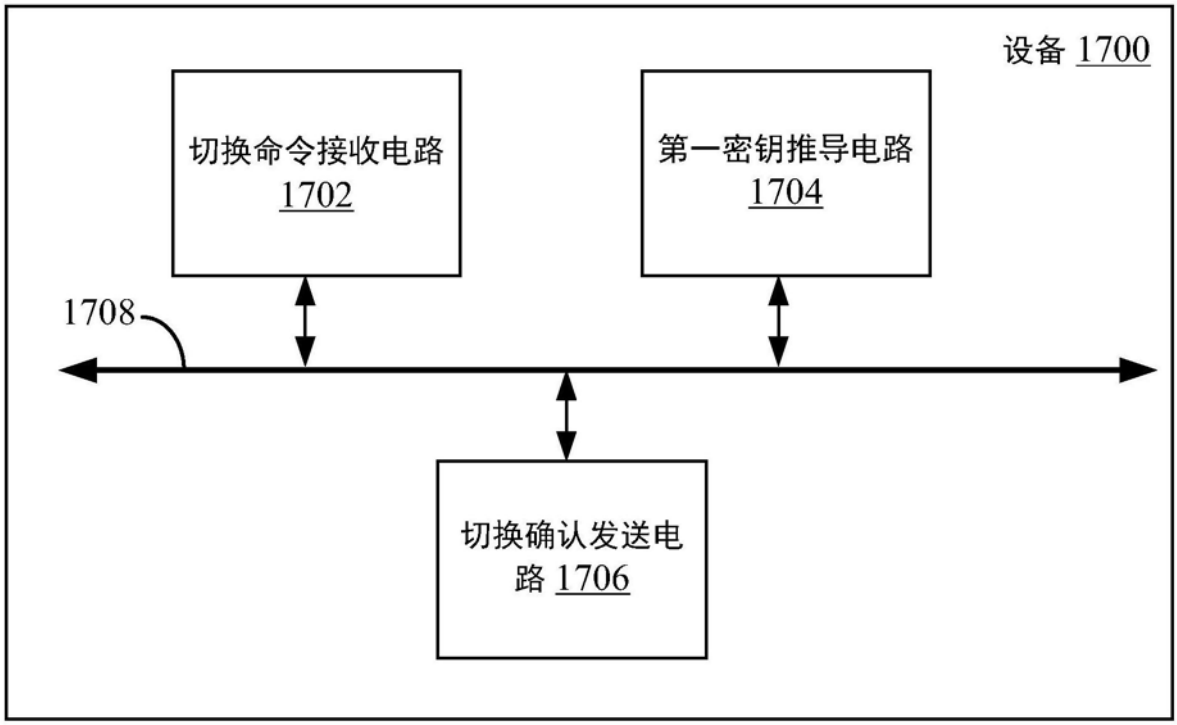

设备 1700
切换命令接收电路 1702
第一密钥推导电路 1704
1708
切换确认发送电路 1706

图17

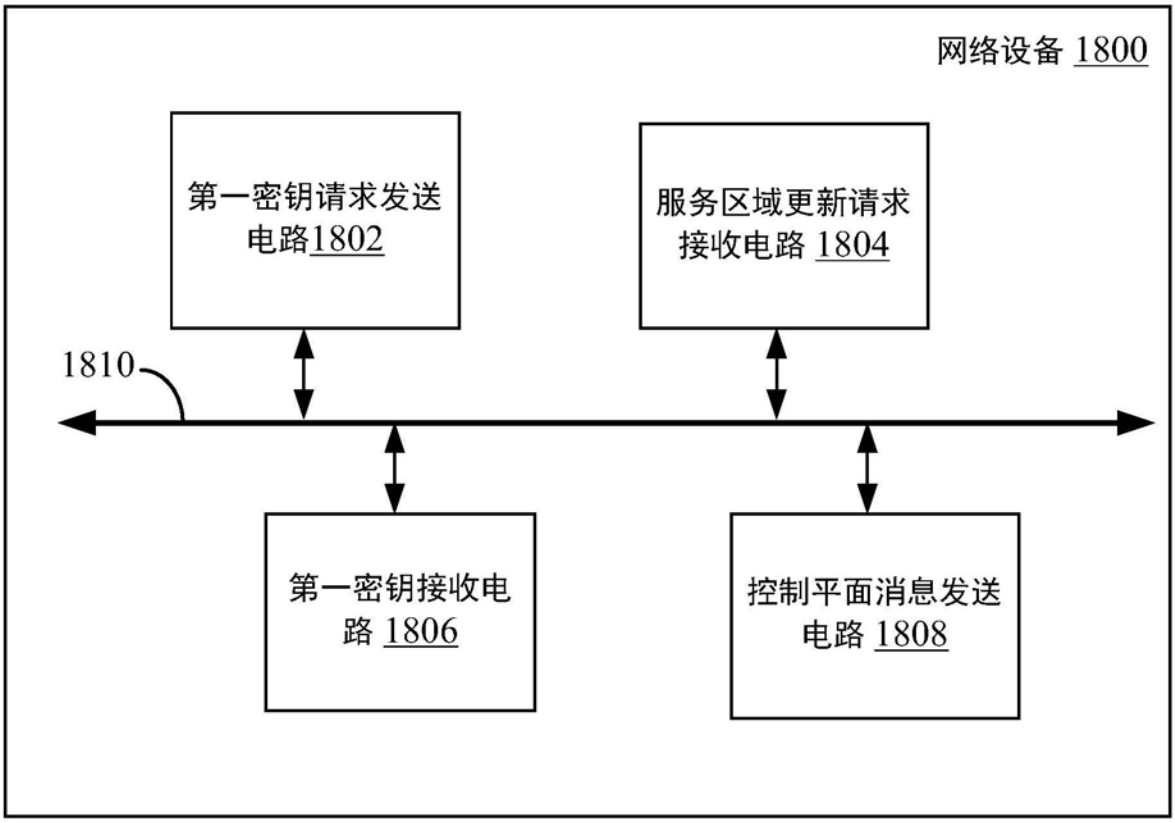

网络设备 1800
第一密钥请求发送电路1802
服务区域更新请求接收电路 1804
1810
第一密钥接收电路 1806
控制平面消息发送电路 1808

图18

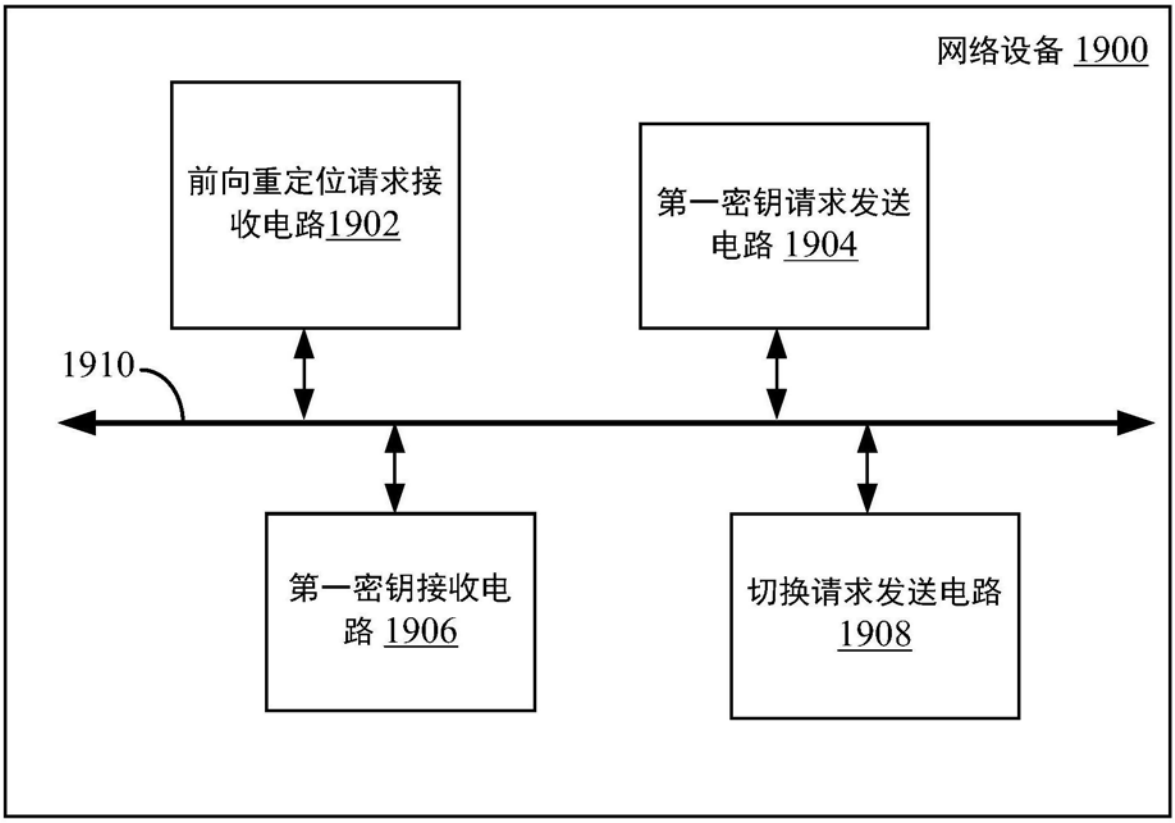

网络设备 1900
前向重定位请求接收电路1902
第一密钥请求发送电路 1904
1910
第一密钥接收电路 1906
切换请求发送电路 1908

图19