(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112566112 B
(45)授权公告日 2023.10.13

(21)申请号 202011263845.1

(22)申请日 2015.10.23

(65)同一申请的已公布的文献号
申请公布号 CN 112566112 A

(43)申请公布日 2021.03.26

(30)优先权数据
62/074,513 2014.11.03 US
14/919,397 2015.10.21 US

(62)分案原申请数据
201580059220.4 2015.10.23

(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 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
专利代理师 戴开良

(51)Int.Cl.
H04W 12/04(2021.01)
H04W 12/041(2021.01)
H04W 12/06(2021.01)

(56)对比文件
US 2011075675 A1,2011.03.31
US 2013305330 A1,2013.11.14
US 2014237559 A1,2014.08.21
V. Narayanan 等.EAP-Based Keying for IP Mobility Protocols draft-vidya-eap-usrk-ip-mobility-01;.IETF Network Working Group Internet-Draft.2007,全文.
Samsung.S2-081476 "23.401 CR0174: Authentication Vector update".3GPP tsg_sa\WG2_Arch.2008,(第TSGS2_63_Athens期),全文.
Samsung.S2-083478 "23.401 CR0342: P-GW Address and TEID in MME".3GPP tsg_sa\WG2_Arch.2008,(第TSGS2_65_Prague期),全文.

审查员 匡仁炳

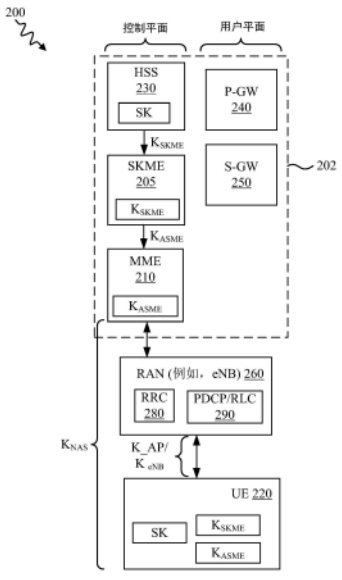
权利要求书2页 说明书15页 附图18页

(54)发明名称

用于无线通信的装置、方法和存储介质

(57)摘要

本公开内容涉及用于无线通信的装置、方法和存储介质。执行与设备的认证和密钥协商，并且获得与该设备相关联的认证信息，所述认证信息包括认证会话密钥。会话密钥管理实体(SKME)基于该认证会话密钥来生成移动性会话密钥，并且向对该设备进行服务的移动性管理实体(MME)发送该移动性会话密钥。



CN 112566112 B

1.一种在网络设备处可操作的方法,所述方法包括:

从设备接收非接入层(NAS)消息;

向核心网设备转发所述NAS消息连同标识所述网络设备的网络设备标识值;

从所述核心网设备接收移动性会话密钥,所述移动性会话密钥部分基于从在所述设备和无线通信网络之间共享的密钥导出的认证会话密钥;以及

向所述设备发送密钥导出数据,所述密钥导出数据使得所述设备能够导出所述移动性会话密钥。

2.根据权利要求1所述的方法,其中,从所述核心网设备接收的所述移动性会话密钥还是部分基于所述网络设备标识值的。

3.根据权利要求2所述的方法,其中,所述网络设备标识值是全球唯一的移动性管理实体标识符(GUMMEI)。

4.根据权利要求2所述的方法,其中,所述网络设备标识值是移动性管理实体组标识符(MMEGI)。

5.根据权利要求1所述的方法,其中,从所述核心网设备接收的所述移动性会话密钥还是部分基于在所述核心网设备处维持的计数器值Key Count的。

6.根据权利要求1所述的方法,其中,所述密钥导出数据是包括在向所述设备发送的NAS安全模式命令消息中的。

7.根据权利要求1所述的方法,其中,所述密钥导出数据包括所述网络设备标识值。

8.根据权利要求1所述的方法,其中,所述密钥导出数据包括在所述核心网设备处维持的计数器值Key Count。

9.根据权利要求1所述的方法,还包括:

确定第二网络设备需要对所述设备进行服务;

确定所述第二网络设备与所述网络设备共享公共组标识符;以及

向所述第二网络设备发送所述移动性会话密钥。

10.根据权利要求9所述的方法,其中,所述网络设备和所述第二网络设备是移动性管理实体(MME),并且所述公共组标识符是公共MME组标识符。

11.一种网络设备,包括:

适于发送和接收数据的通信接口;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:

从设备接收非接入层(NAS)消息;

向核心网设备转发所述NAS消息连同标识所述网络设备的网络设备标识值;

从所述核心网设备接收移动性会话密钥,所述移动性会话密钥部分基于从在所述设备和无线通信网络之间共享的密钥导出的认证会话密钥;以及

向所述设备发送密钥导出数据,所述密钥导出数据使得所述设备能够导出所述移动性会话密钥。

12.根据权利要求11所述的网络设备,其中,从所述核心网设备接收的所述移动性会话密钥还是部分基于所述网络设备标识值的。

13.根据权利要求12所述的网络设备,其中,所述网络设备标识值是全球唯一的移动性管理实体标识符(GUMMEI)。

14.根据权利要求11所述的网络设备,其中,从所述核心网设备接收的所述移动性会话密钥还是部分基于在所述核心网设备处维持的计数器值Key Count的。

15.根据权利要求11所述的网络设备,其中,所述密钥导出数据包括所述网络设备标识值。

16.根据权利要求11所述的网络设备,其中,所述处理电路还适于:

确定第二网络设备需要对所述设备进行服务;

确定所述第二网络设备与所述网络设备共享公共组标识符;以及

向所述第二网络设备发送所述移动性会话密钥。

17.一种网络设备,包括:

用于从设备接收非接入层(NAS)消息的单元;

用于向核心网设备转发所述NAS消息连同标识所述网络设备的网络设备标识值的单元;

用于从所述核心网设备接收移动性会话密钥的单元,所述移动性会话密钥部分基于从在所述设备和无线通信网络之间共享的密钥导出的认证会话密钥;以及

用于向所述设备发送密钥导出数据的单元,所述密钥导出数据使得所述设备能够导出所述移动性会话密钥。

18.根据权利要求17所述的网络设备,还包括:

用于确定第二网络设备需要对所述设备进行服务的单元;

用于确定所述第二网络设备与所述网络设备共享公共组标识符的单元;以及

用于向所述第二网络设备发送所述移动性会话密钥的单元。

用于无线通信的装置、方法和存储介质

[0001] 本申请是2017年04月28日提交的、申请号为201580059220.4的、发明名称为“用于无线通信的装置、方法和存储介质”的申请的分案申请。

[0002] 相关申请的交叉引用

[0003] 本申请要求以下申请的优先权和权益:于2014年11月3日向美国专利商标局提交的题为“Apparatus and Method Having an Improved Cellular Network Key Hierarchy”的临时申请No.62/074,513,以及于2015年10月21日向美国专利商标局提交的题为“Apparatuses and Methods for Wireless Communication”的非临时申请No.14/919,397,通过引用方式将上述申请的全部公开内容明确地并入本文。

技术领域

[0004] 概括地说,本公开内容涉及用于蜂窝网络的改进的密钥层次。

背景技术

[0005] 图1中所示的当前蜂窝网络架构100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,MME110作为核心网102元件由网络服务提供商(系统运营商)拥有和操作,并且位于由网络服务提供商控制的安全位置。核心网102具有包括归属订户服务器(HSS)130和MME 110的控制平面,以及包括分组数据网络(P-DN)网关(PGW)140和服务网关(S-GW)150的用户平面。MME 110连接到无线电接入节点160(例如,演进型节点B(eNB))。RAN 160提供与UE 120的无线电接口(例如,无线电资源控制(RRC)180和分组数据汇聚协议(PDCP)/无线电链路控制(RLC)190)。

[0006] 在未来的蜂窝网络架构中,可以想象到执行MME 110的功能中的许多功能的MME 110或网络组件将被朝网络边缘推出,在那里它们不太安全,因为它们在物理上更易于访问和/或不与其它网络运营商隔离。当网络功能被移动到例如云端(例如,互联网)时,可以不假设它们是安全的,因为它们可能具有较低级别的物理隔离或者没有物理隔离。此外,网络设备可能不由单个网络服务提供商拥有。作为示例,可以将多个MME实例托管在单个物理硬件设备内。结果,向MME发送的密钥可能需要较频繁地刷新,因此可能不建议向MME转发认证向量(AV)。

[0007] 需要改进的装置和方法,该装置和方法为靠近网络边缘执行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

[0008] 一个特征提供了一种在网络设备处可操作的方法,所述方法包括:执行与设备的认证和密钥协商;获得与所述设备相关联的认证信息,所述认证信息包括至少认证会话密钥;部分基于所述认证会话密钥来生成移动性会话密钥;以及向对所述设备进行服务的移动性管理实体(MME)发送所述移动性会话密钥。根据一个方面,所述方法还包括:基于所述认证会话密钥,针对不同的MME生成不同的移动性会话密钥。根据另一个方面,获得所述认

证信息包括:确定与所述设备相关联的认证信息没有存储在所述网络设备处;向归属订户服务器发送认证信息请求;以及响应于发送所述认证信息请求,从所述归属订户服务器接收与所述设备相关联的所述认证信息。

[0009] 根据一个方面,获得所述认证信息包括:确定与所述设备相关联的认证信息存储在所述网络设备处;以及从所述网络设备处的存储器电路取回(retrieve)所述认证信息。根据另一个方面,所述方法还包括:从所述设备接收密钥集标识符;以及基于接收到的所述密钥集标识符来确定与所述设备相关联的所述认证信息存储在所述网络设备处。根据又一个方面,所述方法还包括:在执行与所述设备的认证和密钥协商之前,从所述MME接收源自所述设备的非接入层(NAS)消息。

[0010] 根据一个方面,所述方法还包括:还部分基于标识所述MME的MME标识值来生成所述移动性会话密钥。根据另一个方面,所述MME标识值是全球唯一的MME标识符(GUMMEI)。根据又一个方面,所述MME标识值是MME组标识符(MMEGI)。

[0011] 根据一个方面,所述方法还包括:针对对所述设备进行服务的每个MME,生成不同的移动性管理密钥,所述不同的移动性管理密钥中的每个移动性管理密钥部分基于所述认证会话密钥和与每个MME相关联的不同的MME标识值。根据另一个方面,所述方法还包括:结合MME重定位(relocation)来确定第二MME正试图对所述设备进行服务;部分基于所述认证会话密钥和与所述第二MME相关联的MME标识值来生成第二移动性管理密钥;以及向所述第二MME发送所述第二移动性管理密钥以促进MME重定位。根据又一个方面,所述方法还包括:维持计数器值密钥计数(Key Count);以及还部分基于计数器值密钥计数来生成所述移动性会话密钥。根据另一个方面,生成所述移动性会话密钥包括:使用具有下列各项中的至少一项作为输入的密钥导出函数来导出所述移动性会话密钥:所述认证会话密钥、唯一地标识所述MME的MME标识值、和/或计数器值密钥计数。

[0012] 另一个特征提供了一种网络设备,其包括:适于发送和接收数据的通信接口;以及通信地耦合到所述通信接口的处理电路;所述处理电路适于:执行与设备的认证和密钥协商;获得与所述设备相关联的认证信息,所述认证信息包括至少认证会话密钥;部分基于所述认证会话密钥来生成移动性会话密钥,以及向对所述设备进行服务的移动性管理实体(MME)发送所述移动性会话密钥。根据一个方面,所述处理电路还适于:基于所述认证会话密钥,针对不同的MME生成不同的移动性会话密钥。根据另一个方面,所述处理电路适于获得所述认证信息包括:确定与所述设备相关联的认证信息没有存储在所述网络设备处;向归属订户服务器发送认证信息请求;以及响应于发送所述认证信息请求,从所述归属订户服务器接收与所述设备相关联的所述认证信息。

[0013] 根据一个方面,所述处理电路还适于:还部分基于标识所述MME的MME标识值来生成所述移动性会话密钥。根据另一个方面,所述处理电路还适于:在执行与所述设备的认证和密钥协商之前,从所述MME接收源自所述设备的非接入层(NAS)消息。根据又一个方面,接收到的所述NAS消息包括标识所述设备的设备标识符和标识所述MME的MME标识值。

[0014] 另一个特征提供了一种网络设备,其包括:用于执行与设备的认证和密钥协商的单元;用于获得与所述设备相关联的认证信息的单元,所述认证信息包括至少认证会话密钥;用于部分基于所述认证会话密钥来生成移动性会话密钥的单元;以及用于向对所述设备进行服务的移动性管理实体(MME)发送所述移动性会话密钥的单元。根据一个方面,所述

网络设备还包括:用于基于所述认证会话密钥,针对不同的MME生成不同的移动性会话密钥的单元。

[0015] 另一个特征提供了一种具有存储在其上、在网络设备处可操作的指令的非临时性计算机可读存储介质,所述指令在由至少一个处理器执行时使得所述处理器进行以下操作:执行与设备的认证和密钥协商;获得与所述设备相关联的认证信息,所述认证信息包括至少认证会话密钥;部分基于所述认证会话密钥来生成移动性会话密钥;以及向对所述设备进行服务的移动性管理实体(MME)发送所述移动性会话密钥。根据一个方面,所述指令在由所述处理器执行时还使得所述处理器进行以下操作:基于所述认证会话密钥,针对不同的MME生成不同的移动性会话密钥。

[0016] 另一个特征提供了一种在网络设备处可操作的方法,所述方法包括:从设备接收非接入层(NAS)消息;向会话密钥管理实体(SKME)设备转发所述NAS消息连同标识所述网络设备的网络设备标识值;从所述SKME设备接收移动性会话密钥,所述移动性会话密钥部分基于从在所述设备和无线通信网络之间共享的密钥导出的认证会话密钥;以及向所述设备发送密钥导出数据,所述密钥导出数据使得所述设备能够导出所述移动性会话密钥。根据一个方面,从所述SKME设备接收的所述移动性会话密钥还部分基于所述网络设备标识值。根据另一个方面,所述网络设备标识值是全球唯一的移动性管理实体标识符(GUMMEI)。

[0017] 根据一个方面,所述网络设备标识值是移动性管理实体组标识符(MMEGI)。根据另一个方面,从所述SKME设备接收的所述移动性会话密钥还部分基于在所述SKME设备处维持的计数器值密钥计数。根据又一个方面,所述密钥导出数据被包括在向所述设备发送的NAS安全模式命令消息中。

[0018] 根据一个方面,所述密钥导出数据包括所述网络设备标识值。根据另一个方面,所述密钥导出数据包括在所述SKME设备处维持的计数器值密钥计数。根据又一个方面,所述方法还包括:确定第二网络设备需要对所述设备进行服务;确定所述第二网络设备与所述网络设备共享公共组标识符;以及向所述第二网络设备发送所述移动性会话密钥。根据又一个方面,所述网络设备和所述第二网络设备是移动性管理实体(MME),并且所述公共组标识符是公共MME组标识符。

[0019] 另一个特征提供了一种网络设备,其包括:适于发送和接收数据的通信接口;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:从设备接收非接入层(NAS)消息;向会话密钥管理实体(SKME)设备转发所述NAS消息连同标识所述网络设备的网络设备标识值;从所述SKME设备接收移动性会话密钥,所述移动性会话密钥部分基于从在所述设备和无线通信网络之间共享的密钥导出的认证会话密钥;以及向所述设备发送密钥导出数据,所述密钥导出数据使得所述设备能够导出所述移动性会话密钥。根据一个方面,所述处理电路还适于:确定第二网络设备需要对所述设备进行服务;确定所述第二网络设备与所述网络设备共享公共组标识符;以及向所述第二网络设备发送所述移动性会话密钥。

[0020] 另一个特征提供了一种网络设备,其包括:用于从设备接收非接入层(NAS)消息的单元;用于向会话密钥管理实体(SKME)设备转发所述NAS消息连同标识所述网络设备的网络设备标识值的单元;用于从所述SKME设备接收移动性会话密钥的单元,所述移动性会话密钥部分基于从在所述设备和无线通信网络之间共享的密钥导出的认证会话密钥;以及用于向所述设备发送密钥导出数据的单元,所述密钥导出数据使得所述设备能够导出所述移

动性会话密钥。根据一个方面，所述网络设备还包括：用于确定第二网络设备需要对所述设备进行服务的单元；用于确定所述第二网络设备与所述网络设备共享公共组标识符的单元；以及用于向所述第二网络设备发送所述移动性会话密钥的单元。

[0021] 另一个特征提供了一种具有存储在其上、在网络设备处可操作的指令的非临时性计算机可读存储介质，所述指令在由至少一个处理器执行时使得所述处理器进行以下操作：从设备接收非接入层(NAS)消息；向会话密钥管理实体(SKME)设备转发所述NAS消息连同标识所述网络设备的网络设备标识值；从所述SKME设备接收移动性会话密钥，所述移动性会话密钥部分基于从在所述设备和无线通信网络之间共享的密钥导出的认证会话密钥；以及向所述设备发送密钥导出数据，所述密钥导出数据使得所述设备能够导出所述移动性会话密钥。根据一个方面，所述指令在由所述处理器执行时还使得所述处理器进行以下操作：确定第二网络设备需要对所述设备进行服务；确定所述第二网络设备与所述网络设备共享公共组标识符；以及向所述第二网络设备发送所述移动性会话密钥。

[0022] 另一个特征提供了一种在设备处可操作的方法，所述方法包括：执行与会话密钥管理实体(SKME)设备的认证和密钥协商；部分基于与归属订户服务器(HSS)共享的秘密密钥来生成认证会话密钥，所述认证会话密钥对于所述SKME设备是已知的；部分基于所述认证会话密钥来生成移动性会话密钥，所述移动性会话密钥对于对所述设备进行服务的移动性管理实体(MME)是已知的；以及使用所述移动性会话密钥来以密码方式保护从所述设备向无线通信网络发送的数据。根据一个方面，所述方法还包括：基于所述认证会话密钥，针对不同的MME生成不同的移动性会话密钥。根据另一个方面，所述方法还包括：在与所述SKME设备成功认证之后，从所述MME接收密钥导出数据，所述密钥导出数据使得所述设备能够导出所述移动性会话密钥。

[0023] 根据一个方面，所述密钥导出数据包括标识对所述设备进行服务的所述MME的MME标识值；并且所述方法还包括：还部分基于所述MME标识值来生成所述移动性会话密钥。根据另一个方面，所述密钥导出数据包括在所述SKME设备处维持的计数器值密钥计数。根据又一个方面，所述密钥导出数据被包括在从所述MME接收的安全模式命令消息中。

[0024] 根据一个方面，生成所述移动性会话密钥包括：使用具有下列各项中的至少一项作为输入的密钥导出函数来导出所述移动性会话密钥：所述认证会话密钥、唯一地标识所述MME的MME标识值、和/或计数器值密钥计数。根据另一个方面，所述方法还包括：接收包括唯一地标识试图对所述设备进行服务的第二MME的MME标识符的MME重定位的通知；部分基于所述认证会话密钥和唯一地标识所述第二MME的所述MME标识符来生成第二移动性会话密钥。根据又一个方面，所述方法还包括：部分基于所述移动性会话密钥来导出节点B密钥K_{eNB}；以及使用所述节点B密钥K_{eNB}来对发送到对所述设备进行服务的无线接入节点的数据进行加密。

[0025] 另一个特征提供了一种设备，其包括：适于向无线通信网络发送数据以及从无线通信网络接收数据的无线通信接口；以及通信地耦合到所述无线通信接口的处理电路，所述处理电路适于：执行与会话密钥管理实体(SKME)设备的认证和密钥协商；部分基于与归属订户服务器(HSS)共享的秘密密钥来生成认证会话密钥，所述认证会话密钥对于所述SKME设备是已知的；部分基于所述认证会话密钥来生成移动性会话密钥，所述移动性会话密钥对于对所述设备进行服务的移动性管理实体(MME)是已知的；以及使用所述移动性会

话密钥来以密码方式保护从所述设备向所述无线通信网络发送的数据。根据一个方面，所述处理电路还适于：基于所述认证会话密钥，针对不同的MME生成不同的移动性会话密钥。根据另一个方面，所述处理电路还适于：在与所述SKME设备成功认证之后，从所述MME接收密钥导出数据，所述密钥导出数据使得所述设备能够导出所述移动性会话密钥。根据又一个方面，所述密钥导出数据包括标识对所述设备进行服务的所述MME的MME标识值；并且所述处理电路还适于：还部分基于所述MME标识值来生成所述移动性会话密钥。

[0026] 根据一个方面，生成所述移动性会话密钥包括：使用具有下列各项中的至少一项作为输入的密钥导出函数来导出所述移动性会话密钥：所述认证会话密钥、唯一地标识所述MME的MME标识值、和/或计数器值密钥计数。根据另一个方面，所述处理电路还适于：接收包括唯一地标识试图对所述设备进行服务的第二MME的MME标识符的MME重定位的通知；部分基于所述认证会话密钥和唯一地标识所述第二MME的所述MME标识符来生成第二移动性会话密钥。

[0027] 另一个特征提供了一种设备，其包括：用于执行与会话密钥管理实体(SKME)设备的认证和密钥协商的单元；用于部分基于与归属订户服务器(HSS)共享的秘密密钥来生成认证会话密钥的单元，所述认证会话密钥对于所述SKME设备是已知的；用于部分基于所述认证密钥来生成移动性管理密钥的单元，所述移动性管理密钥对于对所述设备进行服务的移动性管理实体(MME)是已知的；以及用于使用所述移动性会话密钥来以密码方式保护从所述设备向无线通信网络发送的数据的单元。根据一个方面，所述设备还包括：用于基于所述认证会话密钥，针对不同的MME生成不同的移动性会话密钥的单元。

[0028] 另一个特征提供了一种具有存储在其上、在设备处可操作的指令的非临时性计算机可读存储介质，所述指令在由至少一个处理器执行时使得所述处理器进行以下操作：执行与会话密钥管理实体(SKME)设备的认证和密钥协商；部分基于与归属订户服务器(HSS)共享的秘密密钥来生成认证会话密钥，所述认证会话密钥对于所述SKME设备是已知的；部分基于所述认证会话密钥来生成移动性会话密钥，所述移动性会话密钥对于对所述设备进行服务的移动性管理实体(MME)是已知的；以及使用所述移动性会话密钥来以密码方式保护从所述设备向无线通信网络发送的数据。根据一个方面，所述指令在由所述处理器执行时还使得所述处理器进行以下操作：基于所述认证会话密钥，针对不同的MME生成不同的移动性会话密钥。

附图说明

[0029] 图1是现有技术中给出的无线通信系统的示例的框图。

[0030] 图2示出了一种无线通信网络。

[0031] 图3A和图3B示出了在无线通信网络上可操作的过程流程图。

[0032] 图4和图5示出了用户设备正在漫游并因此在归属网络之外的拜访网络中的场景。

[0033] 图6示出了无线通信网络的密钥层次的示意图。

[0034] 图7示出了连接到无线通信网络的UE的附着过程和初始数据传输的流程图。

[0035] 图8示出了S1切换过程的流程图。

[0036] 图9A和图9B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。

[0037] 图10示出了设备的示意性框图。

[0038] 图11示出了设备处理电路的示意性框图。

[0039] 图12示出了在设备处可操作的方法。

[0040] 图13示出了网络设备的示意性框图。

[0041] 图14示出了网络设备处理电路的第一示例性示意性框图。

[0042] 图15示出了网络设备处理电路的第二示例性示意性框图。

[0043] 图16示出了在网络设备处可操作的第一示例性方法。

[0044] 图17示出了在网络设备处可操作的第二示例性方法。

具体实施方式

[0045] 本文中使用的“示例性”一词意指“用作示例、实例或说明”。在本文中被描述为“示例性”的任何实施例不一定被解释为优选的或者比其它实施例更有优势。

[0046] 图2根据本公开内容的一个方面示出了无线通信网络200。无线通信网络200包括核心网202、无线电接入节点(例如,eNB)260和无线通信设备(例如,UE)220。除其它事项外,核心网包括会话密钥管理实体(SKME)设备205(在本文中可以称为“认证会话密钥锚功能设备”)、MME 210、HSS 230、P-GW 240和S-GW 250。SKME设备205、MME 210和HSS 230包括控制平面,而P-GW 240和S-GW 250包括用户平面。无线通信网络200的这种架构可以用于第五代(5G)蜂窝网络。

[0047] 例如,无线电接入节点260可以是演进型节点B(eNB),并且可以与MME 210和UE 220通信。RAN 260提供与UE 220的无线电接口(例如,无线电资源控制(RRC)280和分组数据汇聚协议(PDCP)/无线电链路控制(RLC)290)。

[0048] SKME 205可以是位于无线通信网络200内部深处的信任锚或密钥锚。SKME 205为其服务的每个MME 210导出移动性会话密钥(例如,密钥K_{ASME})。(尽管图2仅示出了一个(1个)MME 210,但SKME 205可以与多个MME进行通信和/或对多个MME进行服务)。因此,当执行MME的功能的MME 210和/或网络设备被推至网络的边缘(即,靠近RAN或与RAN共置),SKME 205保持在网络200内部的深处,在此处来自外部实体的物理访问被禁止。以这种方式,SKME 205充当MME 210和HSS 230之间的中介。

[0049] HSS 230基于在UE 220和无线通信网络的认证中心(AuC)(图2中未示出)之间共享的一个或多个秘密密钥(SK)来生成认证会话密钥(例如,密钥K_{SKME})。共享的一个或多个秘密密钥可以是例如根密钥和/或密码密钥(CK)以及从根密钥导出的完整性密钥(IK)。认证会话密钥K_{SKME}被发送到SKME 205,SKME 205转而部分基于认证会话密钥K_{SKME}来生成移动性会话密钥K_{AKME}。然后,SKME 205将移动性会话密钥K_{ASME}发送到生成该密钥所针对的MME 210。其它密钥(例如eNB密钥K_{eNB})可以从移动性会话密钥K_{ASME}导出,并且用于保护RAN 260与UE 220之间的通信。

[0050] 图3A和图3B根据本公开的一个方面示出了无线通信网络200的过程流程图300。为了清楚起见,已经从图3A和图3B中省略了网络200的一些组件(例如,RAN 260、P-GW 240、S-GW 250)。

[0051] 参照图3A,该过程可以开始于UE 220向MME 210发送302非接入层(NAS)消息(例如,经由图3A中未示出的RAN 260)。除其它事项外,NAS消息可以是例如附着请求、后续服务

请求或跟踪区域更新请求。在一些情况下,NAS消息可以包括与UE 220相关联的密钥集标识符(KSI)和/或标识UE 220的设备标识符(例如,国际移动用户身份(IMSI))。然后,MME 210可以将NAS消息和KSI(如果包括)转发304到SKME 205。接下来,SKME 205可以确定306UE 220的认证信息是否已经存储在SKME205处。如果是,则SKME 205使用所存储的针对UE 220的认证信息(例如,认证向量)来执行312与UE 220的认证和密钥协商(AKA)。如果不是,则SKME 205可以向HSS 230发送308认证信息请求,该认证信息请求请求与UE 220相关联的认证信息。作为响应,HSS 230可以向SKME 205提供310一个或多个认证向量(例如,认证信息)。所提供的认证向量中的至少一个与UE 220相关联,并且可以用于执行312与UE 200的AKA。认证向量可以包括预期响应(XRES)、认证值(AUTN)、随机数(RAND)以及认证会话密钥K_{SKME}在本文中可以被称为"第一认证会话密钥K_{SKME}"、"第二认证会话密钥K_{SKME}"等)。AUTN可以基于UE 220与HSS 230共享的序列号和密钥。

[0052] 部分基于UE和网络的AuC之间共享的一个或多个秘密密钥,可以在HSS处生成认证会话密钥K_{SKME}。这些秘密密钥可以包括根密钥和/或密码密钥(CK)以及从根密钥导出的完整性密钥(IK)。为了进一步执行AKA,SKME 205可以向请求认证响应(RES)的UE 220发送认证请求消息(例如,包括AUTN和RAND)。然后,SKME 205可以将RES与XRES进行比较寻求匹配,以确定与UE 220的认证是否成功。

[0053] 在AKA 312成功完成之后,SKME 205可以基于由UE 220提供的KSI(如果有的话)来识别314用于UE 220的适当的认证会话密钥K_{SKME}。如果SKME 205从HSS 230接收到具有多个认证会话密钥K_{SKME}的多个认证向量,则可以这样做。然后,SKME 205可以导出/生成移动性管理密钥K_{ASME}(例如,"第一移动性管理密钥K_{ASME}"、"第二移动性管理密钥K_{ASME}"、"第三移动性管理密钥K_{ASME}"等)。移动性管理密钥K_{ASME}可以基于认证会话密钥K_{ASME}、MME标识值(例如,全球唯一的MME标识符(GUMMEI)、MME标识符(MMEI)、MME组标识符(MMEGI)、公共陆地移动网络标识符(PLMN)ID)、MME代码(MMEC)等)和/或计数器值(例如,密钥计数)。因此,K_{ASME}可以被导出为K_{ASME}=KDF(K_{SKME},MME标识值|密钥计数),其中,KDF是密钥导出函数。计数器值密钥计数是可以由SKME205递增的计数器值,以便在每次回到MME 210的重定位发生时,使SKME205能够针对同一个MME 210导出新的K_{ASME}密钥。根据一个方面,可以使用一次使用的数字(随机数),而不是计数器值密钥计数。根据另一个方面,如果MME标识值(例如,GUMMEI、MMEGI、MMEI、MMEC、PLMN ID等)不用于授权特定的MME身份,则其可以省略。例如,如果SKME 205总是在与它向其提供K_{ASME}的MME 210相同的网络中,则在密钥导出中包括MME标识值可能是不必要的。因此,根据另一个示例,K_{ASME}可以导出为K_{ASME}=KDF(K_{SKME},nonce)或K_{ASME}=KDF(K_{SKME},密钥计数)。MME标识值可以是网络设备标识值的一个示例。

[0054] 接下来,SKME 205可以向其生成所针对的MME 210发送318移动性会话密钥K_{ASME}。MME 210可以向UE 220发送320密钥导出数据(KDD),以帮助UE 220生成移动性会话密钥K_{ASME}。根据一个示例,密钥导出数据可以被包括在非接入层(NAS)安全模式命令(SMC)中。密钥导出数据可以包括用于生成密钥K_{ASME}的MME标识值(例如,GUMMEI、MMEGI、MMEI、MMEC、PLMN ID等)、计数器值密钥计数和/或随机数。利用该数据,UE 220然后可以生成/导出322密钥K_{ASME},并使用它来保护其本身与无线通信网络/服务网络(例如,MME 210、SKME 205等)之间的通信(如数据业务)。MME 210和UE 220还可以基于移动性管理密钥K_{ASME}来生成/导出324随后的密钥(例如,K_{eNB}、K_{NASenc}、K_{NASint}、NK等),并使用它们来保护UE 220、MME 210、和/或

对UE 220进行服务的RAN(例如,eNB)260之间的通信。

[0055] 根据一个方面,可以使用具有秘密密钥(例如,CK、IK等)和服务网络身份(SN_id)作为输入的第一密钥导出函数来导出认证会话密钥K_{SKME}。可以使用第二密钥导出函数来导出移动性会话密钥K_{ASME}。第一和第二密钥导出函数可以基于例如密钥散列消息认证码(HMAC)HMAC-256、HMAC-SHA-256、HMAC-SHA-3等。可以使用可扩展认证协议(EAP)或特定NAS信令来执行认证和密钥协商。移动性会话密钥K_{ASME}可以在AKA过程(对于当前与UE附着的MME)期间或在涉及MME重定位的切换期间导出。可以由SKME 205为当前附着的MME定义会话。可以在共享MMEGI的一组MME内执行MME重定位。或者,MME重定位可以用具有不同MMEGI的另一个MME来执行。根据一个方面,GUMMEI可以基于MMEGI和MME代码的组合。

[0056] 根据本公开内容的一个方面,MME可以通过安全保护的通信信道从SKME 300接收移动性会话密钥K_{ASME}。根据另一方面,如果两个MME属于相同的MME组(例如,二者具有相同的MME组标识符(MMEGI)),则MME重定位期间的目标MME可以接收另一个MME使用的密钥K_{ASME}。

[0057] 图4和图5示出了图2所示的UE 220正在漫游并因此在归属网络202之外的拜访网络400中的场景。在这种情况下,拜访网络的SKME 405变为本地密钥锚,并且还与UE 220进行相互认证(例如,AKA),并且通常遵循上文针对图3A和图3B描述的过程。类似地,在拜访网络内的MME重定位(例如切换或跟踪区域更新)期间,拜访网络400的本地SKME 405导出新的K_{ASME}并将其提供给目标/新MME。密钥K_{eNB}可以从新的K_{ASME}导出。在图2、图4和图5中,密钥K_{NAS}用于保护UE 220和MME 210之间的控制消息。

[0058] 图6示出了上述无线通信网络200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)可以存储根密钥。从根密钥可以导出完整性密钥(IK)和密码密钥(CK),并将其提供给HSS。根密钥、CK和IK可以被认为是在UE和网络之间共享的共享秘密密钥。

[0059] HSS可以转而生成认证会话密钥K_{SKME}并将其提供给SKME。会话密钥K_{SKME}在整个认证会话期间有效。SKME可以利用K_{SKME}来生成移动性会话密钥K_{ASME},并向对UE进行服务的MME提供该密钥。在一个方面中,移动性会话密钥K_{ASME}可以仅对特定MME有效。在其它方面中,移动性会话密钥K_{ASME}可以在同一组的MME之间共享(例如具有相同的MMEGI)。对UE进行服务的MME可以转而基于K_{ASME}来生成其它密钥(K_{NASenc}、K_{NASint}、K_{eNB}/NH等)。

[0060] 附着、切换和跟踪区域更新(TAU)过程

[0061] 在初始附着到网络期间,UE执行与会话密钥管理实体(SKME)设备的认证和密钥协商(AKA)过程。一旦认证成功,SKME就针对UE所附着的MME导出密钥(例如,K_{ASME}),并向MME提供密钥。

[0062] 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从SKME接收新的密钥K_{ASME},并通过执行NAS SMC过程与UE建立安全关联。类似地,当涉及MME重定位的切换发生时,目标MME还从SKME获得新密钥K_{ASME},并与UE建立安全关联。

[0063] 支持两个跟踪区域的MME可以在UE在跟踪区域之间移动时发起移动性会话密钥K_{ASME}的改变。这将隐藏来自UE的网络配置。例如,UE可以仅看到跟踪区域而不是MME。这可能在响应于TAU或更改跟踪区域的切换二者时发生。

[0064] 图7根据本公开内容的一个方面示出了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 220向RAN 260发送附着请求702,RAN 260转而将该请求转发到MME 210,MME 210转而将该请求(连同可能的KSI信息)转发到SKME 205。然后,SKME 205可以向HSS 230发送认证信息请求704,并且作为响应,其从HSS 230接收可能包括预期响应(XRES)、认证值(AUTN)、随机数(RAND)和认证会话密钥K_{SKME}的一个或多个认证向量706。AUTN可以基于序列号以及UE 220与HSS 230共享的密钥。

[0065] 一旦SKME 205具有与UE 220相关联的认证向量,则UE 220和SKME205可以执行708AKA。一旦AKA成功,则SKME 205可以基于认证会话密钥K_{SKME}、MME标识值(例如,GUMMEI、MMEI、MMEGI等)和/或计数器值(例如,密钥计数)来导出移动性会话密钥K_{ASME})。因此,K_{ASME}可以导出为K_{ASME}=KDF(K_{SKME},MME标识值|密钥计数),其中,KDF是密钥导出函数。计数器值密钥计数是可以由SKME 205递增的计数器值,以便在每次回到MME 210的切换发生时,使SKME 205能够针对同一个MME 210导出新的K_{ASME}密钥。根据一个方面,可以使用一次使用的数字(随机数),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,则其可以省略。例如,如果SKME 205总是在与它向其提供K_{ASME}的MME相同的网络中,则在密钥导出中包括GUMMEI可能是不必要的。因此,根据另一个示例,K_{ASME}可以被导出为K_{ASME}=KDF(K_{SKME},nonce)。然后向MME 210发送710移动性会话密钥K_{ASME}。然后MME 210可以使用移动性会话密钥K_{ASME}来执行712与UE 220的NAS SMC过程。在NAS SMC过程期间,MME 210可以向UE 220提供其GUMMEI和/或密钥计数,从而UE 220也可以导出K_{ASME}。图7中所示的其余步骤714-728可以与4G LTE蜂窝通信协议中给出的步骤类似。

[0066] 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 260a(即,当前eNB)向源MME 210a(即,当前MME)发送切换(HO)所需消息802。接下来,源MME 210a基于HO所需消息向目标MME210b(即,新MME)发送/转发重定位请求804。目标MME 210b可以创建并向目标服务网关(S-GW)250b发送会话请求806,并从目标S-GW 250b接收会话响应808。目标MME 210b还可以向SKME 205发送针对移动性会话密钥K_{ASME}的密钥请求810。这样做,目标MME 210b可以向SKME 205提供其MME标识值(例如,GUMMEI)。SKME 205可以转而使用MME的GUMMEI、其先前从HSS 230接收的认证会话密钥K_{SKME}(如上所述)和密钥计数来生成移动性会话密钥K_{ASME}。根据一个方面,可以使用一次使用的数字(随机数)而不是密钥计数。根据另一个方面,如果不期望GUMMEI来授权特定的MME身份,则其可以省略。SKME 205向目标MME 210b发送K_{ASME} 812。根据一个方面,目标MME 210b可以向目标S-GW 250b发送会话请求806,并在大约相同的时间发送密钥请求810。因此,步骤806和810可以与步骤808和812同时执行。

[0067] 目标MME 210b然后可以向目标eNB 260b(即,潜在的新eNB)发送切换请求814,并且作为响应,目标eNB 260b发送回切换响应816。切换请求814可以包括由目标MME 210b使用K_{ASME}导出的密钥K_{eNB}。切换响应816指示目标eNB 260b是否同意接受切换。如果目标eNB 260b同意接受切换,则目标MME 210b向SKME 205发送密钥(即,K_{ASME})确认消息818。在接收到密钥确认消息时,SKME 205然后可以递增密钥计数计数器值。发送密钥确认消息818的步骤被延迟,直到接收到切换请求确认816,因为切换请求可能被目标eNB 260b拒绝。在这样的情况下,新的K_{ASME}不需要由UE 220导出,并且在该情况下,SKME 205可能不需要增加密钥计数。在目标MME 210b向源MME 210a发送重定位响应820之后,源MME210a向源eNB 260a发送切换命令822(其被转发到UE 220)。切换命令822、824可以包括目标MME 210b的GUMMEI和

密钥计数，使得UE 220可以针对目标eNB 260b导出新的K_{ASME}和新的K_{eNB}。UE 220利用切换确认消息826对目标eNB 260b进行响应。切换确认消息826可以被完整性保护和加密。

[0068] 图9A和图9B根据本公开内容的一个方面示出了在UE 220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。参照图9A，首先，UE 220生成并向RAN 260(例如，eNB)发送902跟踪区域更新请求。eNB 260转而向将与UE 220相关联和/或对UE 220进行服务的目标MME 210b(例如，“新MME”)转发904跟踪区域更新请求。eNB 260基于包括UE 220的位置的各个准则来确定哪个新的MME 210b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的临时标识符(GUTI)，其包括作为当前与UE 220相关联的MME的源MME 210a(例如，“旧MME”)的GUMMEI。目标MME 210b然后可以在其接收到的跟踪区域更新请求中使用GUMMEI来向源MME 210a发送906UE上下文请求消息。源MME210a然后在UE上下文响应消息中以UE上下文信息进行响应908。一旦接收到该响应，就可以从目标MME 210b向源MME 210a发送910确认。

[0069] 目标MME 210b然后可以向SKME 205发送912位置更新和密钥请求(即，K_{ASME})。位置更新被转发到HSS 230，HSS 230然后向源MME 210a发送914位置取消消息。作为响应，源MME 210a可以将位置取消确认消息发送916回HSS 230。SKME 205可以基于目标MME 210b的GUMMEI和/或如前所述的密钥计数计数器值来为目标MME 210b生成新的K_{ASME}。根据一个方面，可以使用一次使用的数字(随机数)而不是密钥计数。根据另一个方面，如果不期望GUMMEI来授权特定的MME身份，则其可以省略。向目标MME 210b发送918新的K_{ASME}。在从SKME 205接收到K_{ASME}时，目标MME 210b可以用密钥确认消息来对SKME 205进行回复920。根据一个方面，目标MME 210b可以在向SKME 205发送912MME位置更新和密钥请求的同时向源MME 210a发送906UE上下文请求消息。因此，步骤906、908和910可以与步骤912、914、916、918、920同时执行。

[0070] 参照图9B，一旦目标MME 210b已经从SKME 205接收到K_{ASME}，则目标MME 210b然后可以执行922、924与UE 220的非接入层安全模式命令过程。在安全模式命令过程中，UE 220导出目标MME 210b使用的密钥K_{ASME}，因为目标MME 210b向UE 220提供其GUMMEI。一旦UE 220也具有与目标MME 210b相同的K_{ASME}，则UE 220和目标MME 210b可以基于K_{ASME}密钥来参与安全通信。例如，目标MME 210b可以参与926、928与UE 220的跟踪区域更新交换，UE 220的通信由K_{ASME}或从K_{ASME}导出的其它密钥(例如，NAS加密和完整性保护密钥)加密。该交换可以包括基于目标MME的GUMMEI从目标MME 210b发送到UE 220的包括新GUTI的消息。这样的消息再次由K_{ASME}或从K_{ASME}导出的另一个密钥加密。

[0071] 如图9B所示并且如上所述，NAS SMC 922、924之后是跟踪区域更新过程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 210b发送到UE 220的NAS SMC消息922可以与跟踪区域更新消息926进行组合。在这样做时，只有组合消息的一部分(例如，与跟踪区域更新相关联的部分)可以是加密的，而帮助UE导出K_{ASME}的该消息的部分是未加密的。由MME分配的作为GUTI的一部分的新临时移动用户身份(TMSI)可以是加密的。

[0072] 密钥导出

[0073] 如上文所讨论的，AKA在UE和SKME之间运行。密钥K_{SKME}由HSS导出并发送到SKME。从HSS的角度来看，认证向量以与4G LTE相同的方式构建，并发送到SKME而不是MME。因此，HSS

可以连接到SKME而无需任何修改。

[0074] SKME针对给定MME导出移动性会话密钥K_{ASME}，因此MME的GUMMEI可以在K_{ASME}密钥导出过程中使用。针对新的K_{ASME}，NAS计数值可以初始化为零(0)。在一个示例中，如果跟踪区域更新未完成，则不会丢弃旧的NAS计数值。对于密钥K_{ASME}的新鲜度(freshness)，UE和SKME可以维持密钥计数计数器值并将其用于K_{ASME}导出。这样做可以避免在UE移动回到旧的MME的情况下导出相同的K_{ASME}。当成功执行初始AKA时，密钥计数计数器值可以被初始化为零(0)或某个其它预先确定的值。在某些方面中，可以使用随机数，而不是密钥计数计数器值。在另一个方面中，可以从密钥导出中省略GUMMEI。

[0075] 用于生成密钥K_{SKME}、K_{ASME}、K_{eNB}、下一跳(NH)等的密钥导出函数(KDF)可以利用HMAC-SHA-256、HMAC-SHA-3等。输入串S可以从n+1个输入参数构建。例如，S＝[FC||P_0||L_0||P_1||L_1||P_2||L_2||…||P_N||L_N]。字段代码FC可以是用于区分算法的不同实例的单个八位字节，并且可以使用范围0x50-0x5F中的值。输入参数P_0至P_N是n+1输入参数编码。P_0可以是静态ASCII编码字符串。值L_0至L_N是相应输入参数P_0至P_N的长度的两个八位字节表示。

[0076] K_{SKME}导出

[0077] K_{SKME}＝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，P_0＝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，AK是匿名密钥，XOR是异或运算。值SQN XOR AK作为认证令牌(AUTN)的一部分发送到UE。如果不使用AK，则可以根据TS 33.102(即，000…0)来对AK进行处理。输入密钥$K_{CK/IK}$是密码密钥(CK)和完整性密钥(IK)的串联，即$K_{CK/IK}$＝CK||IK。

[0078] K_{ASME}导出

[0079] K_{ASME}＝KDF(K_{SKME},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(即，L_1＝0x00 0x08)。这只是可以怎样导出K_{ASME}的一个示例。在另一个方面，可以省略GUMMEI，并且可以使用一次使用的随机数字(例如，随机数)，而不是使用密钥计数计数器值。

[0080] NH导出

[0081] NH＝KDF(K_{ASME},S)。输入S可以等于[FC||P_0||L_0]，其中，FC＝0x52，P_0＝同步输入，L_0＝同步输入的长度(即，L_0＝0x00 0x20)。同步输入参数可以是针对初始NH导出新导出的K_{eNB}，以及针对所有后续导出的之前NH。这导致NH链中的结果，其中，下一个NH总是新的并且是从之前NH导出的。

[0082] K_{eNB}导出

[0083] K'_{eNB}＝KDF(K_X,S)。当出于切换目的从当前的K_{eNB}或从新鲜的NH以及第7.2.8节中规定的UE和eNB中的目标物理小区标识符导出K'_{eNB}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比特的下一跳(NH)密钥，否则使用当前256比特的K_{eNB}。

[0084] 上面示出和描述的图7-图9A和图9B假设MME从源向目标MME改变。然而，当单个MME承担两个MME(源MME和目标MME)的角色并且这两个MME之间没有实际接口时，可以使用相同

的过程流程图。

[0085] 图10根据本公开的一个方面示出了设备1000(例如,“用户设备”、“用户装备”、“无线通信设备”)的示意性框图。设备1000可以是集成电路、多个集成电路或者包含一个或多个集成电路的电子设备。设备1000还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)、平板电脑、计算机、智能手表和头戴式可穿戴计算机(如Google眼镜®)。设备1000可以包括下列各项中的至少一个或多个: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/或可以通信地彼此耦合的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通信地彼此耦合。无线通信接口1002允许设备1000与无线通信网络104进行无线通信。因此,接口1002允许设备1000与无线广域网(WWAN)(如移动电信蜂窝网络)以及短距离无线局域网(例如,

WiFi®、Zigbee®、蓝牙®等)进行无线通信。

[0086] 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)、磁阻随机存取存储器(MRAM)、电可擦除可编程只读存储器(EEPROM)、闪存器等。存储器电路1004可以存储一个或多个密码密钥(cryptographic key)。存储电路1004还可以存储可由处理电路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、指纹扫描仪以及任何其它输入和/或输出设备。

[0087] 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)可以执行存储在存储器电路1006处的指令和/或存储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)处的指令。处理电路1008可以执行本文中描述的设备1000的步骤和/或过程(包括参考图3A、图3B、图6、图7、图8、图9A、图9B和/或图12讨论的那些)中的任何一个。根据一个方面,处理电路1008可以是通用处理器。根据另一个方面,处理电路可以是硬连线的(例如,其可以是专用集成电路(ASIC))来执行本文中描述的UE 220的步骤和/或过程(包括参考图3A、图3B、图6、图7、图8、图9A、图9B和/或图12讨论的那些)。

[0088] 图11根据一个方面示出了设备处理电路1008的示意性框图。处理电路1008可以包括授权和密钥协商(AKA)执行电路1102、认证会话密钥生成电路1104、移动性会话密钥生成电路1106和/或数据保护电路1108。根据一个方面,这些电路1102、1104、1106、1108可以是ASIC并且是硬接线的以便执行它们各自的过程。

[0089] AKA执行电路1102可以是用于执行与SKME设备的认证和密钥协商的单元的一个非限制性示例。认证会话密钥生成电路1104可以是用于部分基于与归属订户服务器共享的秘密密钥来生成认证会话密钥的单元的一个非限制性示例。移动性会话密钥生成电路1106可以是用于部分基于认证会话密钥来生成移动性会话密钥的单元的一个非限制性示例。数据保护电路1108可以是用于使用移动性会话密钥以密码方式来保护从设备向无线通信网络发送的数据的单元的一个非限制性示例。

[0090] 图12示出了在设备1000处可操作的方法1200。首先,执行1202与会话密钥管理实体(SKME)设备的认证和密钥协商。接下来,部分基于与归属订户服务器(HSS)共享的秘密密

钥来生成1204认证会话密钥，该认证会话密钥对于SKME设备是已知的。然后，部分基于认证会话密钥来生成1206移动性会话密钥，该移动性会话密钥对于对设备进行服务的移动性管理实体(MME)是已知的。接下来，使用移动性会话密钥来以密码方式保护1208从设备向无线通信网络发送的数据。

[0091] 图13根据本公开内容的一个方面示出了网络设备1300的示意性框图。网络设备可以是SKME、MME、RAN、S-GW和/或P-GW等其它网络组件。网络设备1300可以包括下列各项中的至少一个或多个：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/或可以通信地彼此耦合的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通信地彼此耦合。无线通信接口1302允许网络设备1300与用户设备102进行无线通信。因此，接口1302允许网络设备1300通过无线广域网(WWAN)(如移动电信蜂窝网络)和/或短距离无线局域网(例如，WiFi®、Zigbee®、蓝牙®等)进行无线通信。

[0092] 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、闪存器等。存储器电路1304可以存储一个或多个密码密钥。存储电路1304还可以存储可由处理电路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、指纹扫描仪以及任何其它输入和/或输出设备。

[0093] 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)可以执行存储在存储器电路1306处的指令和/或存储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)处的指令。处理电路1308可以执行本文中描述的网络设备的步骤和/或过程(包括参考图3A、图3B、图6、图7、图8、图9A、图9B、图16和/或图17讨论的那些)中的任何一个。根据一个方面，处理电路1308可以是通用处理器。根据另一个方面，处理电路1308可以是硬连线的(例如，其可以是专用集成电路(ASIC))来执行本文中描述的SKME 205和/或MME 210、210a、210b的步骤和/或过程(包括参考图3A、图3B、图6、图7、图8、图9A、图9B、图16和/或图17讨论的那些)。

[0094] 图14根据一个方面示出了网络设备处理电路1308的示意性框图。处理电路1308可以包括授权和密钥协商(AKA)执行电路1402、认证信息获取电路1404、移动性会话密钥生成电路1406和/或移动性会话密钥传输电路1408。根据一个方面，这些电路1402、1404、1406、1408可以是ASIC并且是硬接线的以便执行它们各自的过程。

[0095] AKA执行电路1402可以是用于执行与设备的认证和密钥协商的单元的一个非限制性示例。认证信息获取电路1404可以是用于获得与设备相关联的认证信息的单元的一个非限制性示例，该认证信息包括至少认证会话密钥。移动性会话密钥生成电路1406可以是用于部分基于认证会话密钥来生成移动性会话密钥的单元的一个非限制性示例。移动性会话密钥传输电路1408可以是用于向对设备进行服务的移动性管理实体(MME)发送移动性会话密钥的单元的一个非限制性示例。

[0096] 图15根据另一个方面示出了网络设备处理电路1308的示意性框图。处理电路1308可以包括NAS消息接收电路1502、NAS消息转发电路1504、移动性会话密钥接收电路1506和/或密钥导出数据传输电路1508。根据一个方面，这些电路1502、1504、1506、1508可以是ASIC并且是硬接线的以便执行它们各自的过程。

[0097] NAS消息接收电路1502可以是用于从设备接收非接入层(NAS)消息的单元的一个非限制性示例。NAS消息转发电路1504可以是用于向会话密钥管理实体(SKME)设备转发NAS消息连同标识网络设备的网络设备标识值的单元的一个非限制性示例。移动会话密钥接收电路1506可以是用于从SKME设备接收移动性会话密钥的单元的一个非限制性示例，该移动性会话密钥部分基于从设备和无线通信网络之间共享的密钥导出的认证会话密钥。密钥导出数据传输电路1508可以是用于向设备发送密钥导出数据的单元的一个非限制性示例，该密钥导出数据使得设备能够导出移动性会话密钥。

[0098] 图16示出了在网络设备1300处可操作的方法1600。首先，执行1602与设备的认证和密钥协商。接下来，获得1604与设备相关联的认证信息，该认证信息包括至少认证会话密钥。然后，部分基于认证会话密钥来生成1606移动性会话密钥。接下来，向对设备进行服务的移动性管理实体(MME)发送1608移动性会话密钥。

[0099] 图17示出了在网络设备1300处可操作的方法1700。首先，从设备接收1702非接入层(NAS)消息。接下来，向会话密钥管理实体(SKME)设备转发1704NAS消息连同标识网络设备的网络设备标识值。然后，从SKME设备接收1706移动性会话密钥，该移动性会话密钥部分基于从在设备和无线通信网络之间共享的密钥导出的认证会话密钥。接下来，向设备发送1708密钥导出数据，该密钥导出数据使得设备能够导出移动性会话密钥。

[0100] 可以将图2、图3A、图3B、图4、图5、图6、图7、图8、图9A、图9B、图10、图11、图12、图13、图14、图15、图16和/或图17中示出的组件、步骤、特征和/或功能中的一个或多个重新布置和/或组合成单个组件、步骤、特征或功能，或者体现在若干个组件、步骤、特征或功能中。在不脱离本发明的前提下，也可以添加额外的元素、组件、步骤和/或功能。图2、图3A、图3B、图4、图5、图7、图8、图9A、图9B、图10、图11、图13、图14和/或图15中示出的装置、设备和/或组件可以被配置为执行图2、图3A、图3B、图6、图7、图8、图9A、图9B、图12、图16和/或图17中描述的方法、特征或步骤中的一个或多个。本文中描述的算法还可以在软件中有效地实现和/或嵌入硬件中。

[0101] 此外，应该指出的是：本公开内容的一些方面可能描述成了被描绘为流程图、流图、结构图、或框图的过程。虽然流程图可以将操作描述为顺序过程，但操作中的许多操作可以并行或并发地执行。此外，可以对这些操作的顺序进行重新布置。当过程的操作完成时，该过程终止。过程可以与方法、函数、过程、子例程、子程序等相对应。当过程与函数相对应时，其终止与函数向调用函数或主函数的返回相对应。

[0102] 另外，存储介质可以表示用于存储数据的一个或多个设备，其包括：只读存储器(ROM)、随机存取存储器(RAM)、磁盘存储介质、光存储介质、闪存设备和/或其它机器可读介质和处理器可读介质、和/或用于存储信息的计算机可读介质。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存储设备、光存储设备的非临时性介质，以及能够存储或包含指令和/或数据的各种其它介质。因此，本文中描述的各种方法可以由存储在“机器可读介质”、“计算机可读介质”、和/或“处理器可读介质中”，并由一个或多个处理器、机器和/或设备执行的指令和/或数据完全或部分实现。

[0103] 另外，本公开内容的一些方面可由硬件、软件、固件、中间件、微代码或它们的任意组合来实现。当在软件、固件、中间件或微代码中实现时，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的机器可读介质中。处理器可以执行必要的任

务。代码段可以表示过程、功能、子程序、程序、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、参数或存储器内容来连接到另一个代码段或硬件电路。信息、自变量、参数数据等可经由包括存储器共享、消息传递、令牌传递、网络传输等的任何合适的手段来传递、转发或发送。

[0104] 利用被设计为执行本文所描述功能的通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件或者其任意组合,可以实现或执行结合本文公开的示例所描述的各个说明性的逻辑框、模块、电路、单元和/或组件。通用处理器可以是微处理器,或者,处理器可以是任何常规的处理器、控制器、微控制器或者状态机。处理器也可以实现为计算组件的组合,例如,DSP和微处理器的组合、多个微处理器、一个或多个微处理器与DSP内核的结合、或者任何其它这种配置。

[0105] 结合本文中公开的示例描述的方法或算法可以直接体现为处理单元、程序指令或其它指令的形式的硬件、处理器可执行的软件模块或这二者的组合,并且可以包含在单个设备中或跨越多个设备分布。软件模块可以位于RAM存储器、闪存、ROM存储器、EPROM存储器、EEPROM存储器、寄存器、硬盘、移动磁盘、CD-ROM、或者本领已知的任何其它形式的存储介质中。可以将存储介质耦合到处理器以使得处理器可以从该存储介质读取信息,并且向该存储介质写入信息。可替换地,存储介质可以是处理器的组成部分。

[0106] 本领域的技术人员还应当明白,结合本文公开的各个方面所描述的各个说明性的逻辑框、模块、电路和算法步骤均可以实现成电子硬件、计算机软件或二者的组合。为了清楚地表示硬件和软件之间的该可交换性,上文对各个说明性的组件、框、模块、电路和步骤均围绕其功能进行了总体描述。至于这种功能是实现为硬件还是实现为软件,取决于特定的应用和对整个系统所施加的设计约束。

[0107] 在不脱离本发明的前提下,本文中描述的本发明的各个特征可以在不同的系统中实现。应该指出的是:上述本公开内容的方面仅仅是示例,并且不应当被解释为对本发明的限制。本公开内容的方面的描述旨在是说明性的,而不是要限制权利要求的范围。因此,本发明的教导可以容易地应用于其它类型的装置,并且许多的替换、修改以及变型对本领域的技术人员来说将是显而易见的。

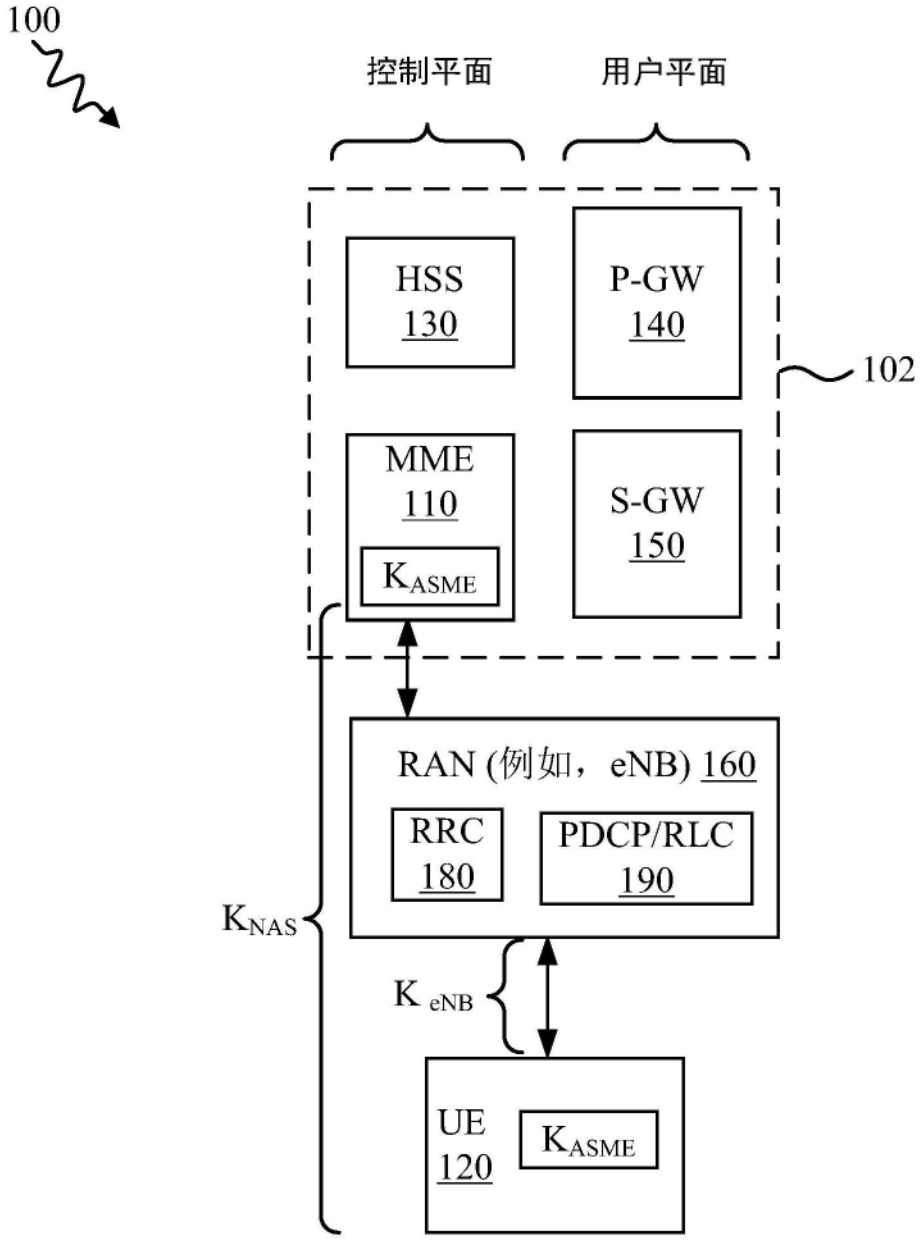

100
控制平面
用户平面
HSS
130
P-GW
140
102
MME
110
K_{ASME}
S-GW
150
RAN (例如，eNB) 160
RRC
180
PDCP/RLC
190
K_{NAS}
K_{eNB}
UE
120
K_{ASME}

图1(现有技术)

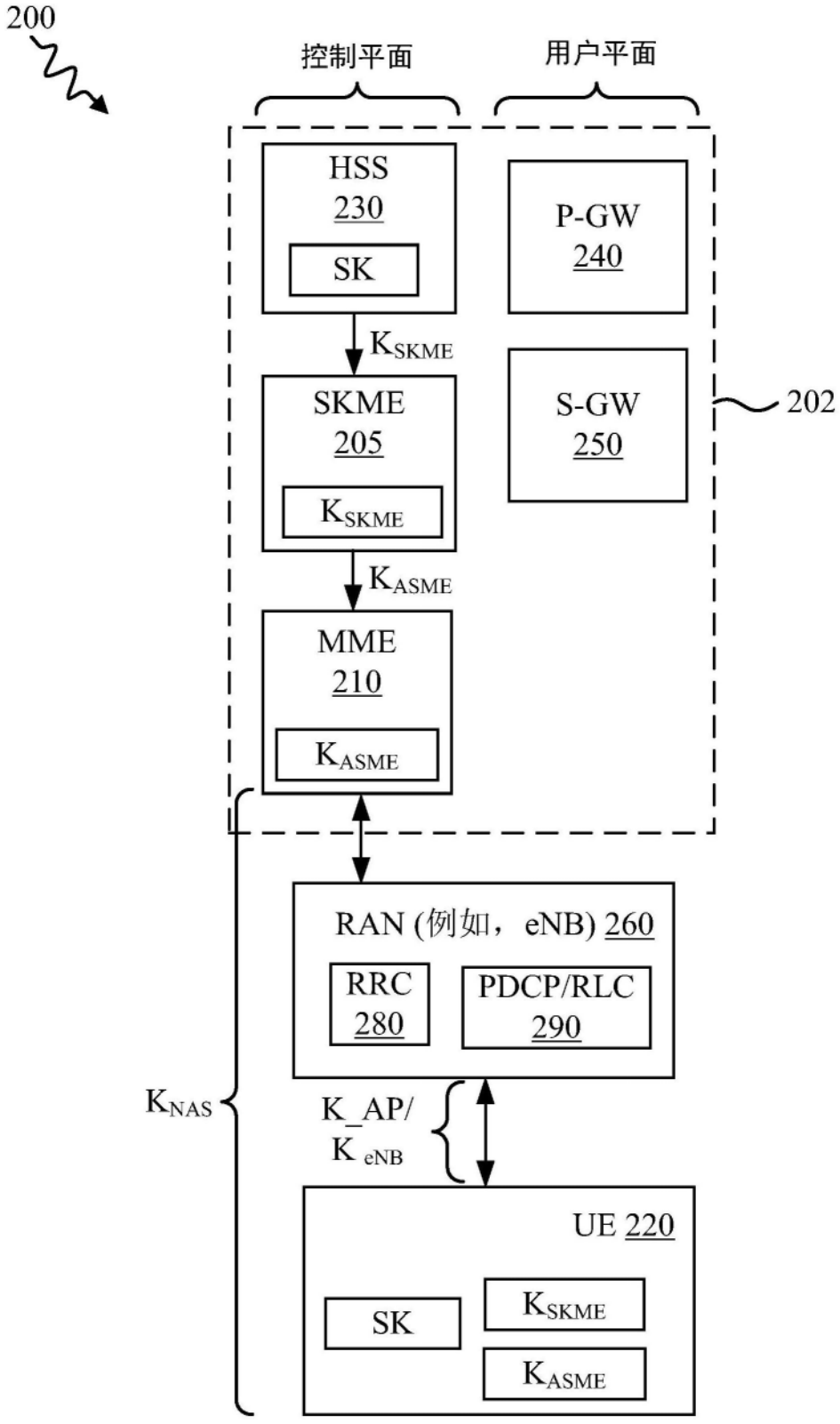

200
控制平面
用户平面
HSS
230
SK
P-GW
240
K_{SKME}
SKME
205
K_{SKME}
S-GW
250
202
K_{ASME}
MME
210
K_{ASME}
RAN (例如，eNB) 260
RRC
280
PDCP/RLC
290
K_{NAS}
K_AP/
K eNB
UE 220
SK
K_{SKME}
K_{ASME}

图2

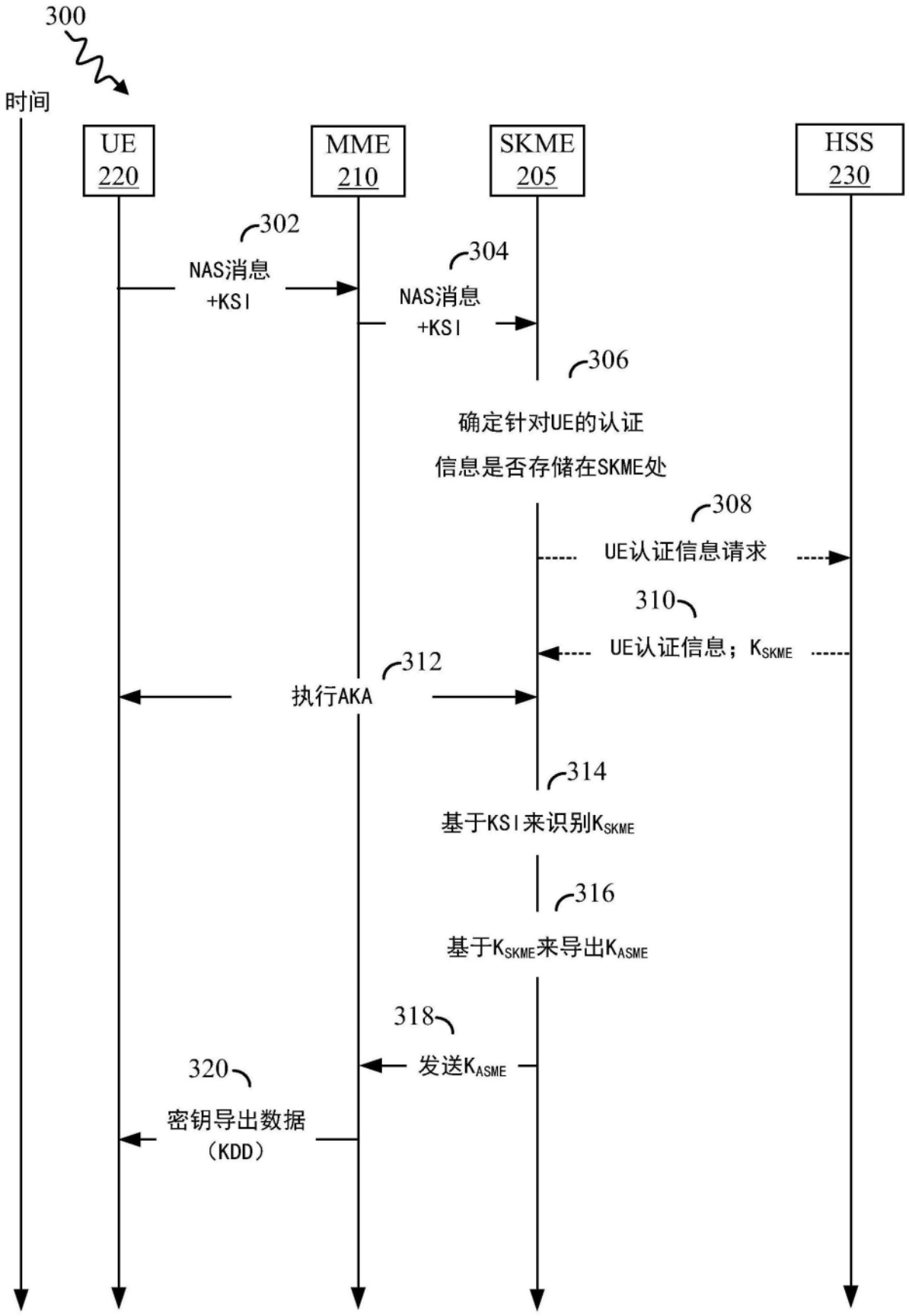

300
时间
UE
220
MME
210
SKME
205
HSS
230
302
NAS消息
+KSI
304
NAS消息
+KSI
306
确定针对UE的认证
信息是否存储在SKME处
308
UE认证信息请求
310
UE认证信息；KSKME
312
执行AKA
314
基于KSI来识别KSKME
316
基于KSKME来导出KASME
318
发送KASME
320
密钥导出数据
（KDD）

图3A

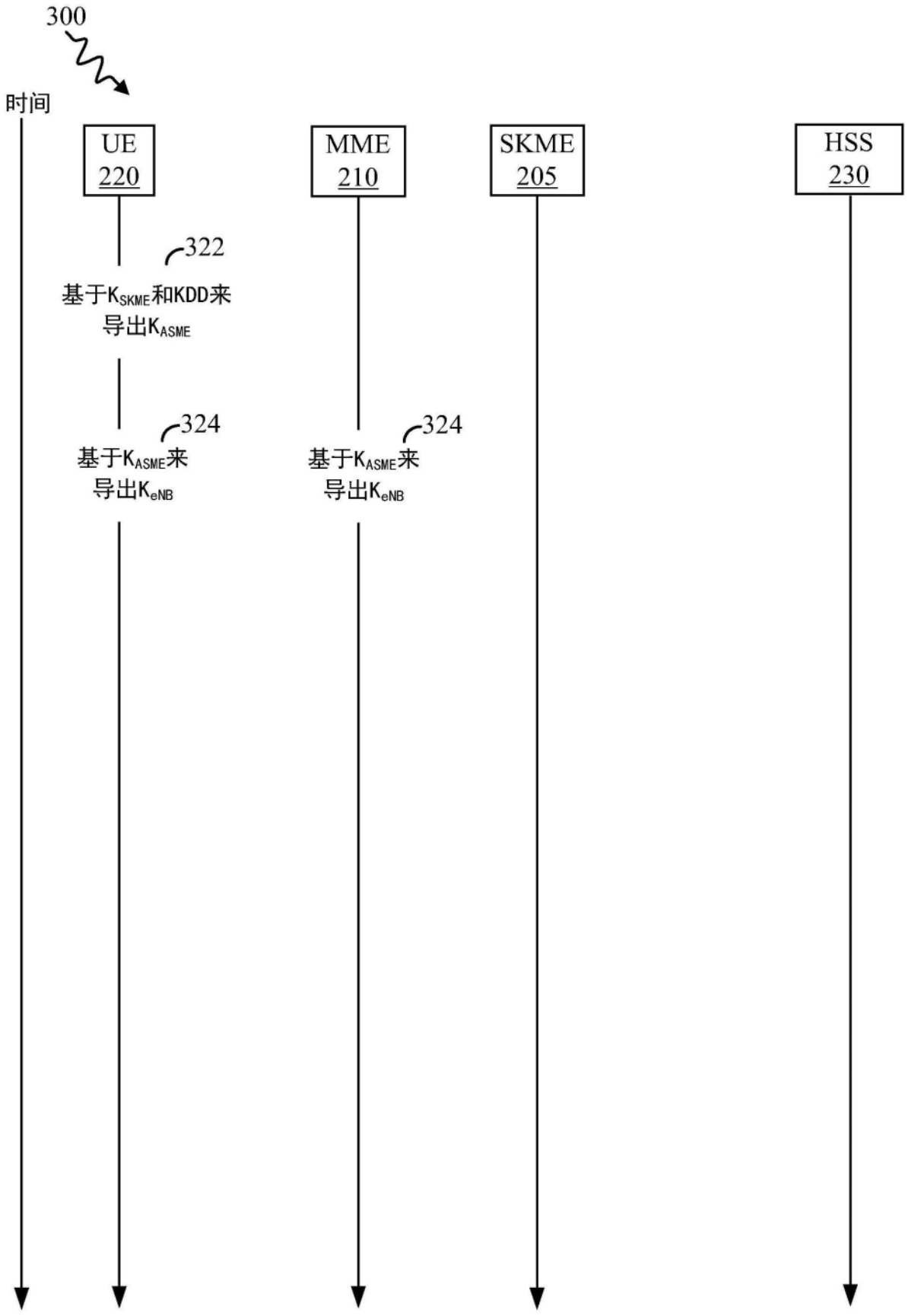

300
时间
UE
220
MME
210
SKME
205
HSS
230
322
基于K_{SKME}和KDD来
导出K_{ASME}
324
基于K_{ASME}来
导出K_{eNB}
324
基于K_{ASME}来
导出K_{eNB}

图3B

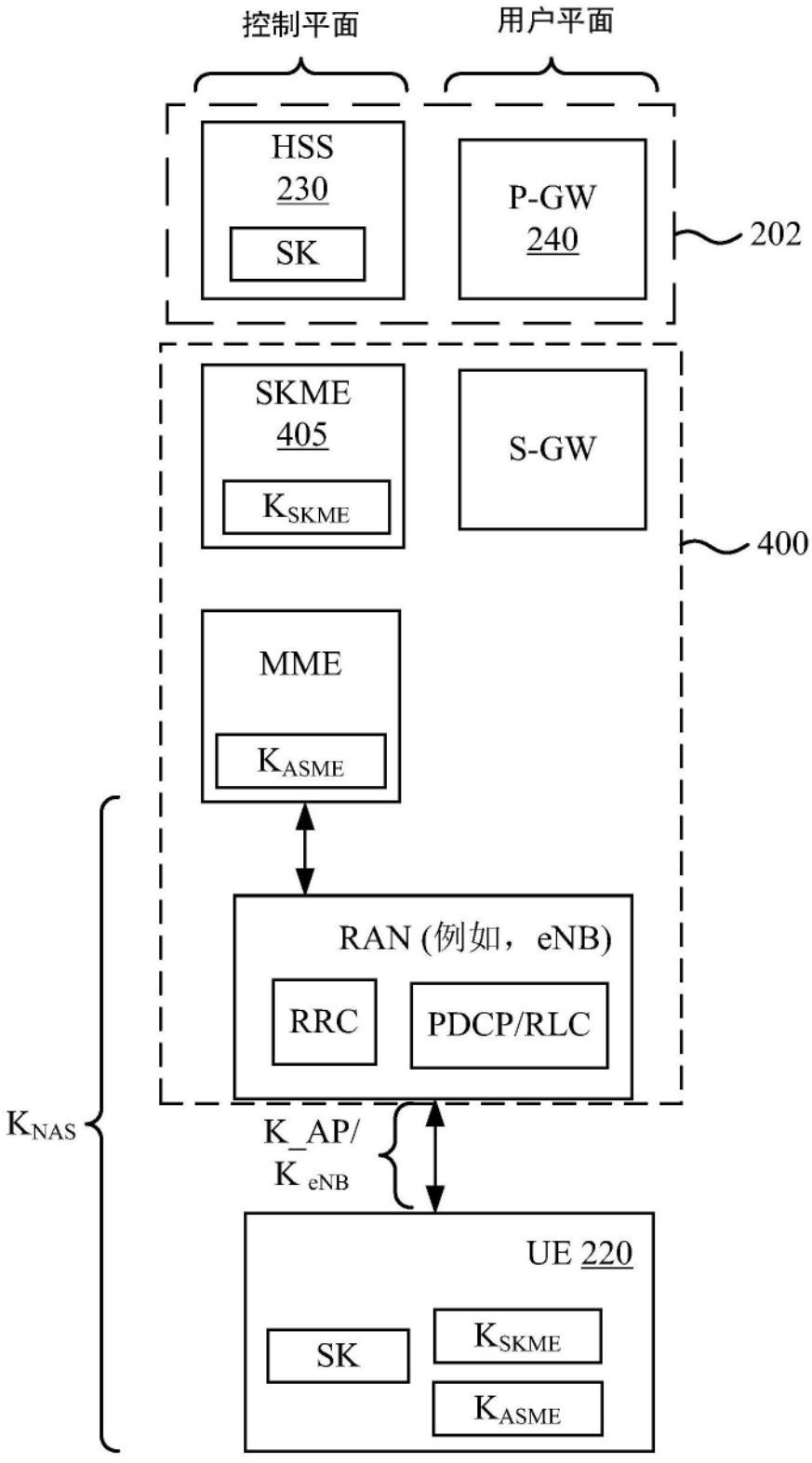

控制平面
用户平面
HSS
230
SK
P-GW
240
202
SKME
405
K_{SKME}
S-GW
400
MME
K_{ASME}
RAN (例如，eNB)
RRC
PDCP/RLC
K_{NAS}
K_AP/
K_{eNB}
UE 220
SK
K_{SKME}
K_{ASME}

图4

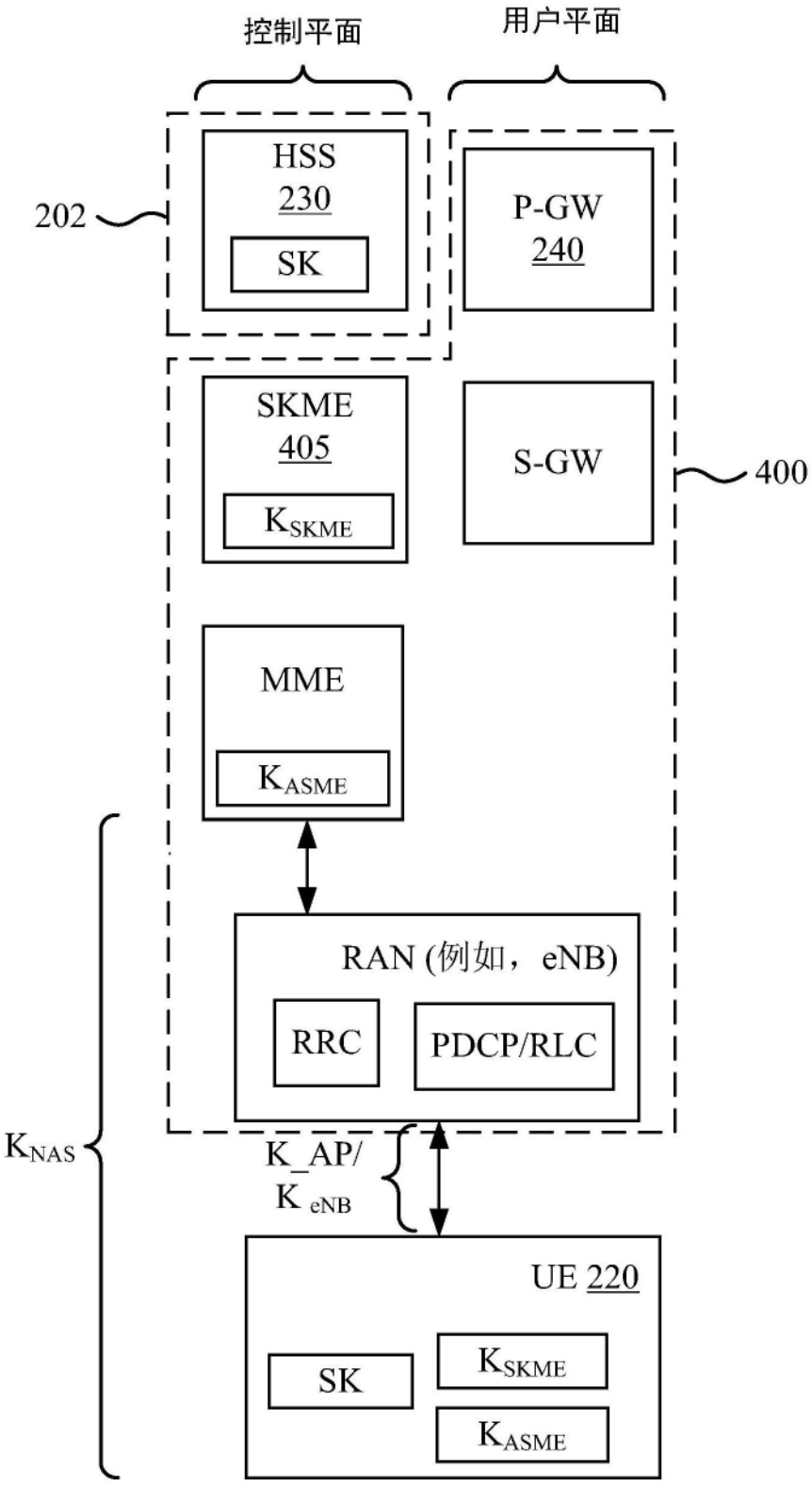

控制平面
用户平面
HSS
230
SK
202
P-GW
240
SKME
405
K_{SKME}
S-GW
400
MME
K_{ASME}
RAN (例如，eNB)
RRC
PDCP/RLC
K_{NAS}
K_AP/
K eNB
UE 220
SK
K_{SKME}
K_{ASME}

图5

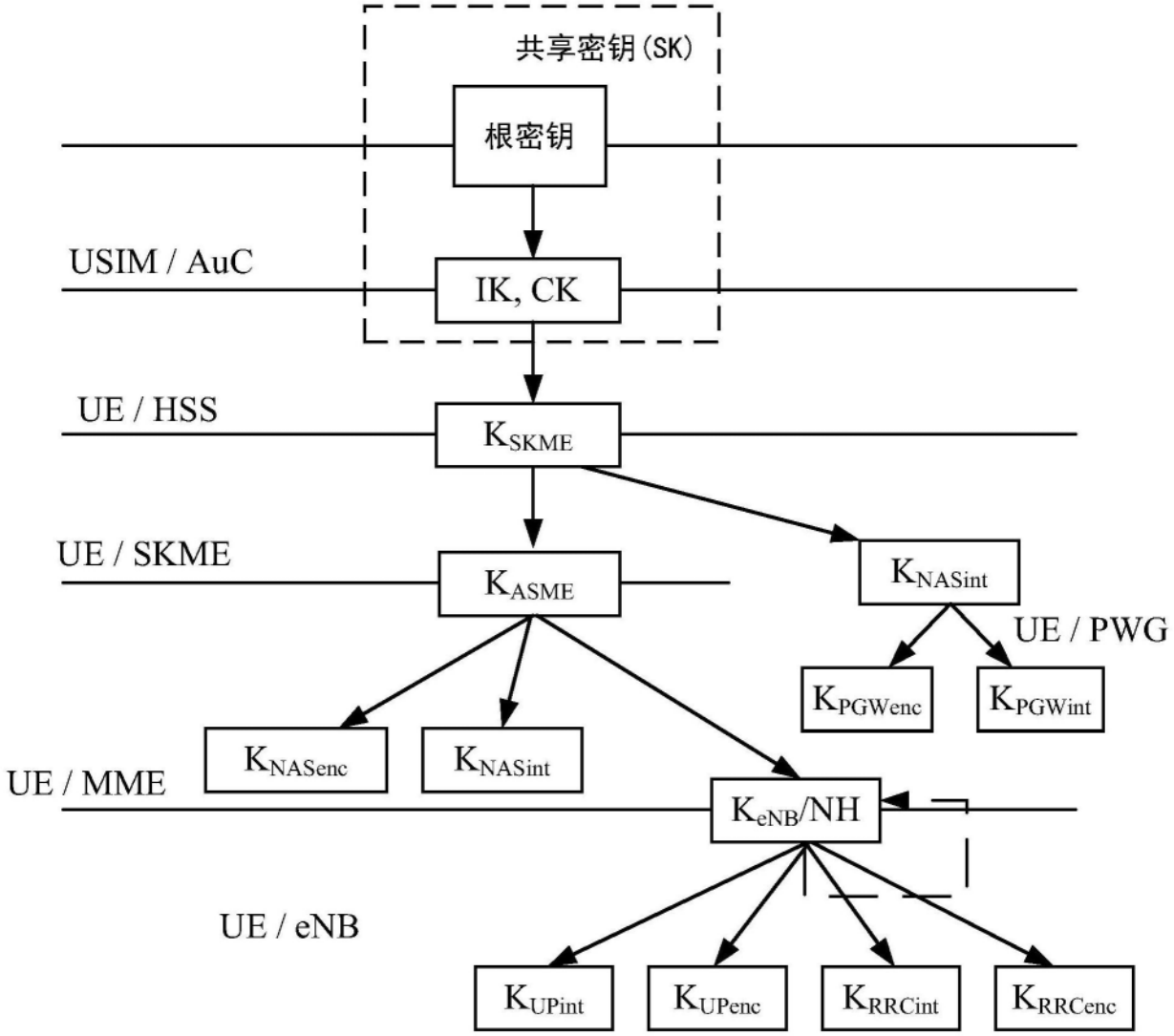

共享密钥(SK)
根密钥
USIM / AuC
IK, CK
UE / HSS
K_{SKME}
UE / SKME
K_{ASME}
K_{NASint}
UE / PWG
K_{PGWenc}
K_{PGWint}
K_{NASenc}
K_{NASint}
UE / MME
K_{eNB}/NH
UE / eNB
K_{UPint}
K_{UPenc}
K_{RRCint}
K_{RRCenc}

图6

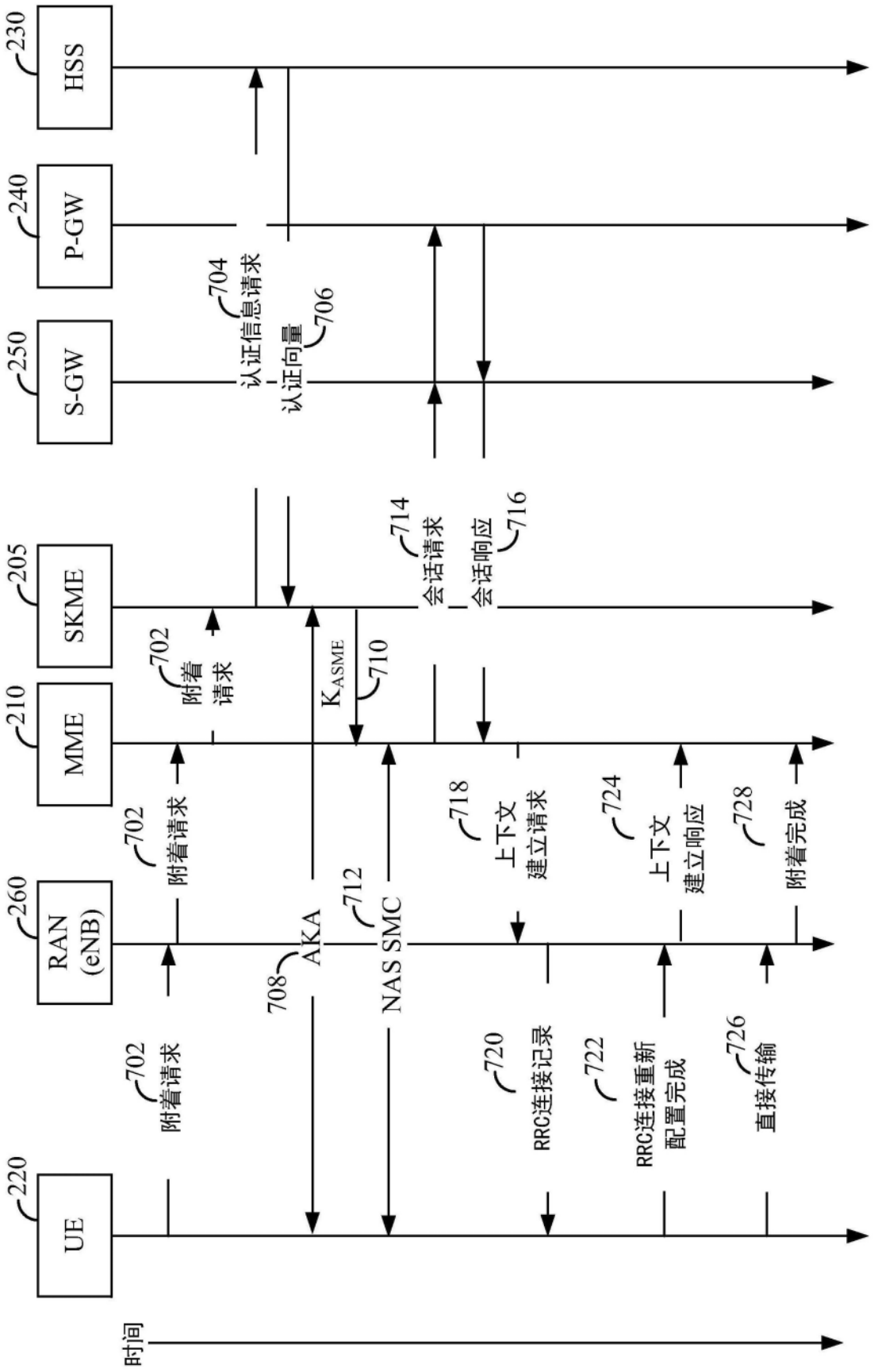

230
HSS
240
P-GW
250
S-GW
205
SKME
210
MME
260
RAN (eNB)
220
UE
704
认证信息请求
706
认证向量
702
附着请求
702
附着请求
702
附着请求
K_{ASME}
710
714
会话请求
716
会话响应
708
AKA
712
NAS SMC
718
上下文建立请求
720
RRC连接记录
724
上下文建立响应
722
RRC连接重新配置完成
728
附着完成
726
直接传输
时间

图7

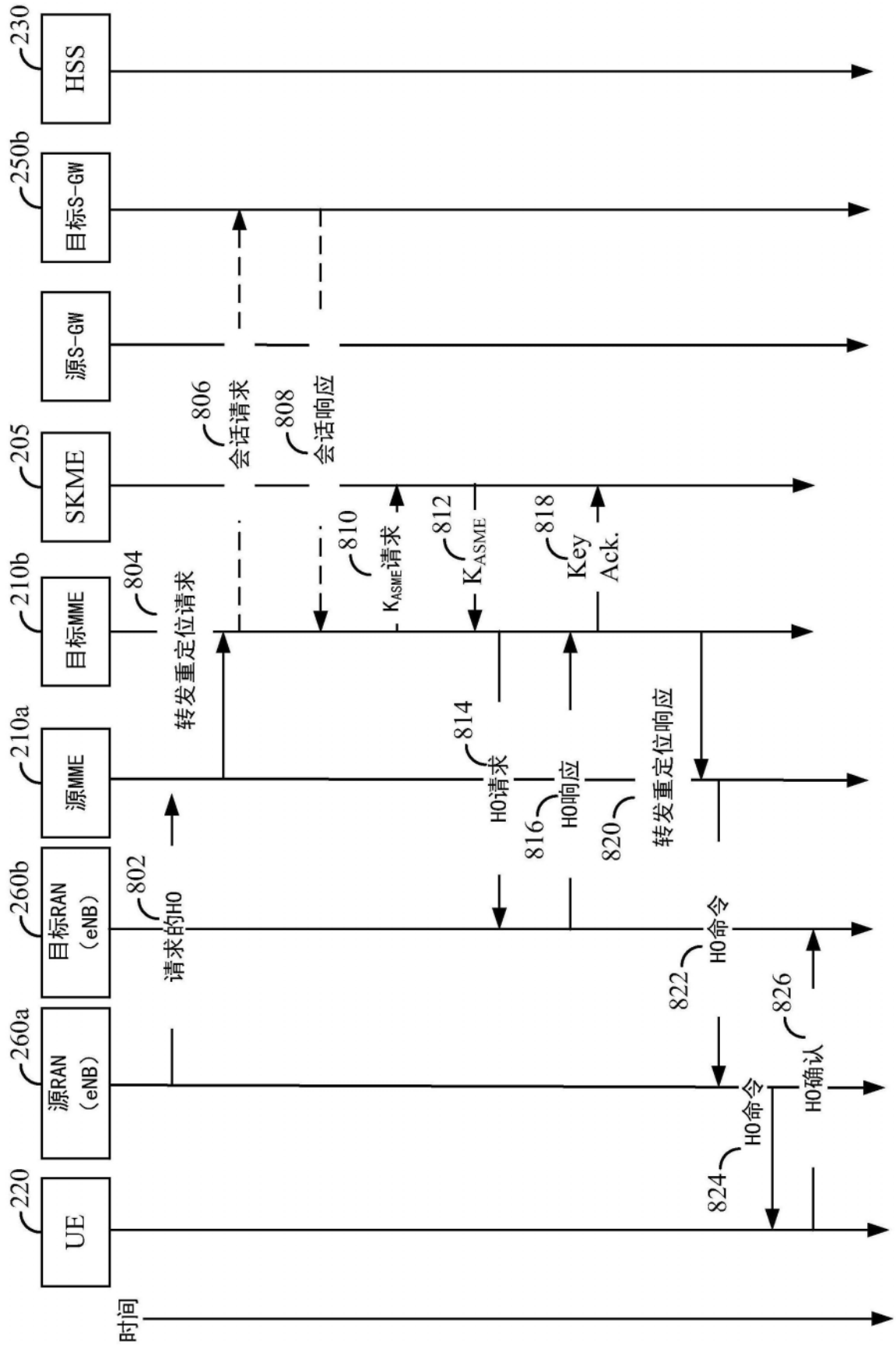

230
HSS
250b
目标S-GW
源S-GW
205
SKME
210b
目标MME
210a
源MME
260b
目标RAN（eNB）
260a
源RAN（eNB）
220
UE
时间
806
会话请求
808
会话响应
804
转发重定位请求
810
KASME请求
812
KASME
818
Key
Ack.
814
HO请求
816
HO响应
820
转发重定位响应
802
请求的HO
822
HO命令
826
HO确认
824
HO命令

图8

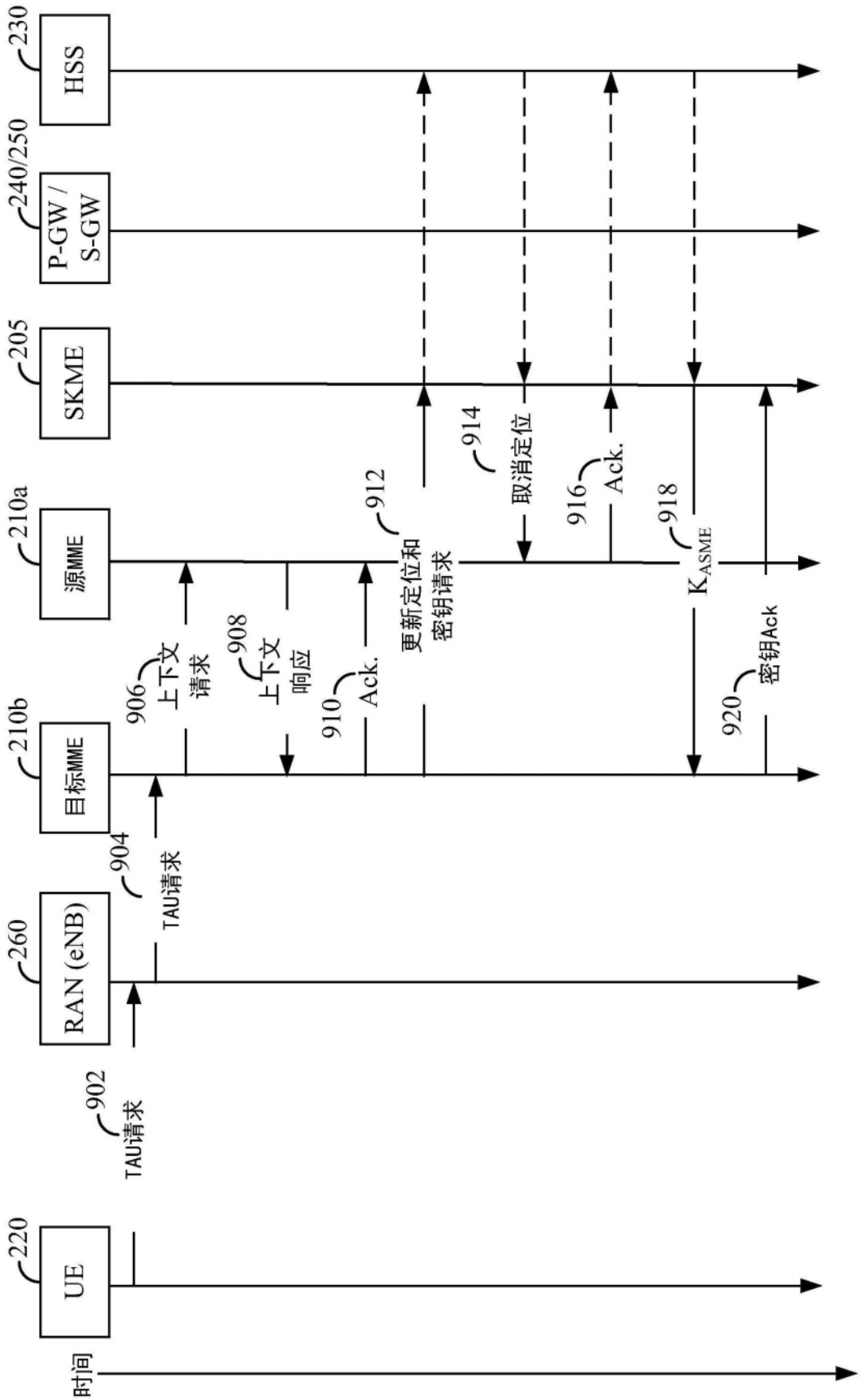

230
HSS
240/250
P-GW / S-GW
205
SKME
210a
源MME
210b
目标MME
260
RAN (eNB)
220
UE
时间
902
TAU请求
904
TAU请求
906
上下文请求
908
上下文响应
910
Ack.
912
更新定位和密钥请求
914
取消定位
916
Ack.
918
K_{ASME}
920
密钥Ack

图9A

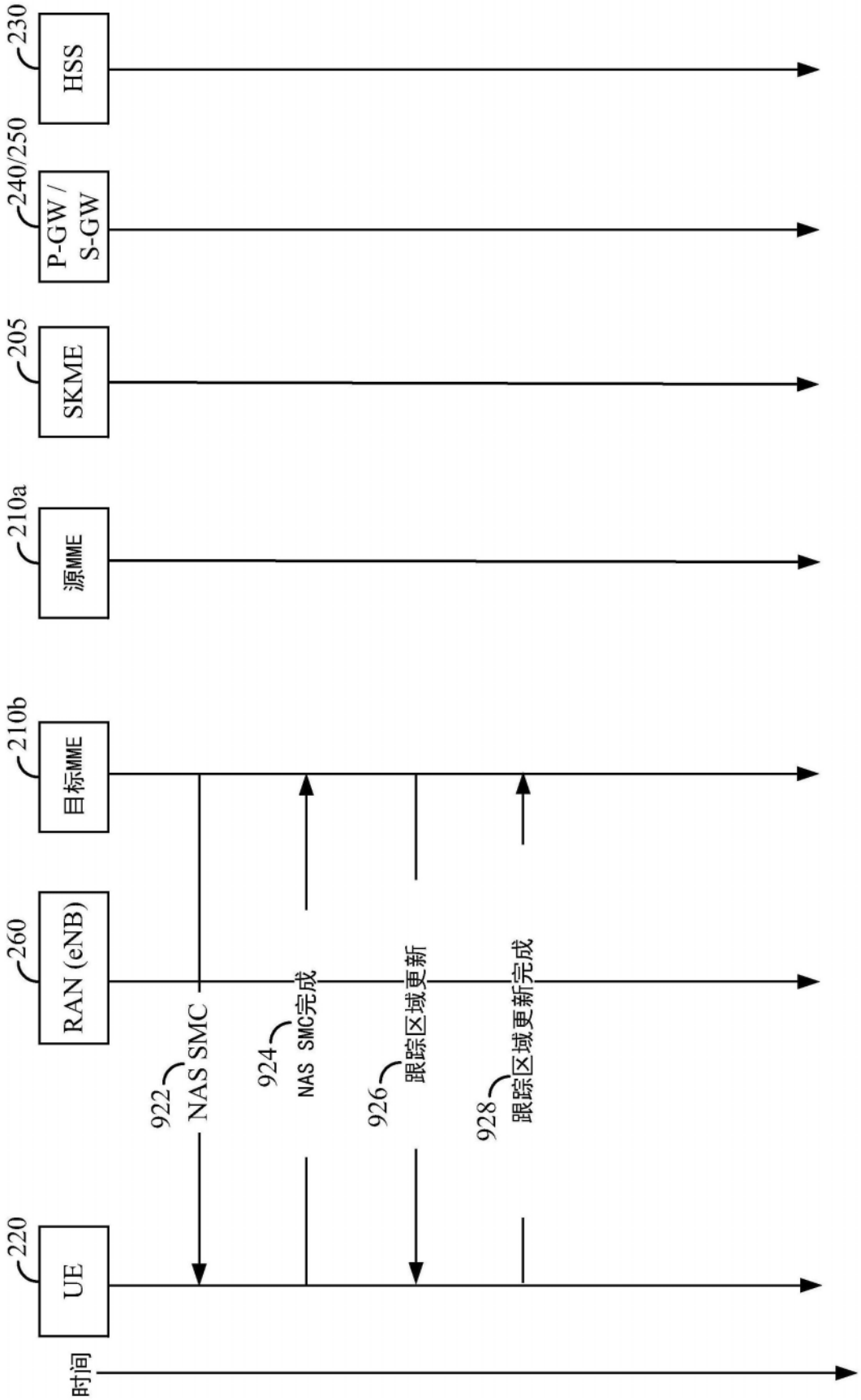

230
HSS
240/250
P-GW / S-GW
205
SKME
210a
源MME
210b
目标MME
260
RAN (eNB)
220
UE
922
NAS SMC
924
NAS SMC完成
926
跟踪区域更新
928
跟踪区域更新完成
时间

图9B

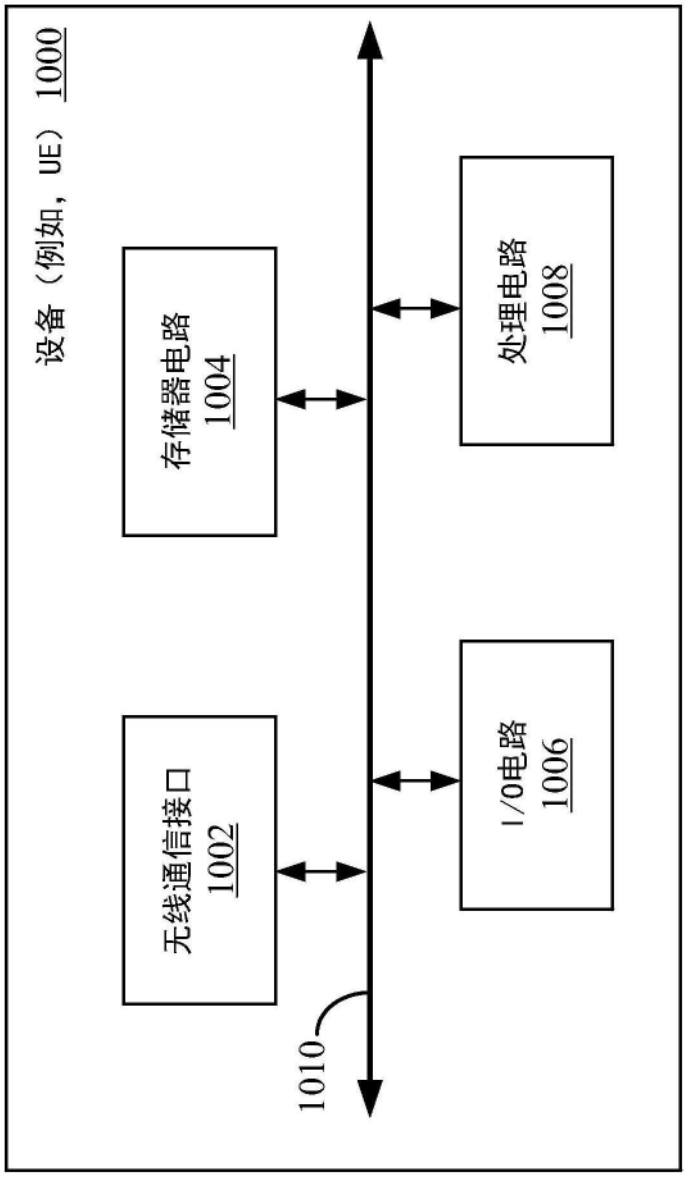


图10

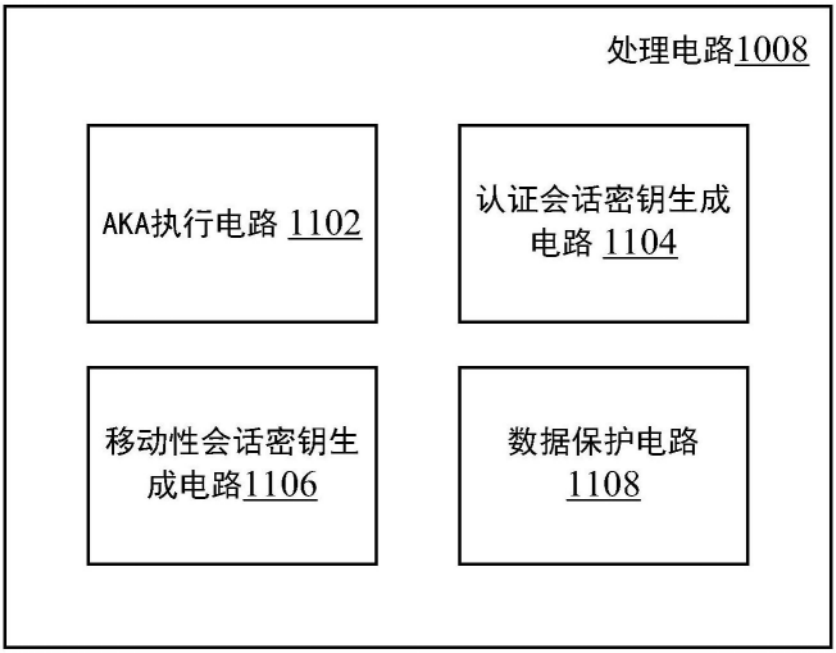

处理电路1008
AKA执行电路 1102
认证会话密钥生成电路 1104
移动性会话密钥生成电路1106
数据保护电路 1108

图11

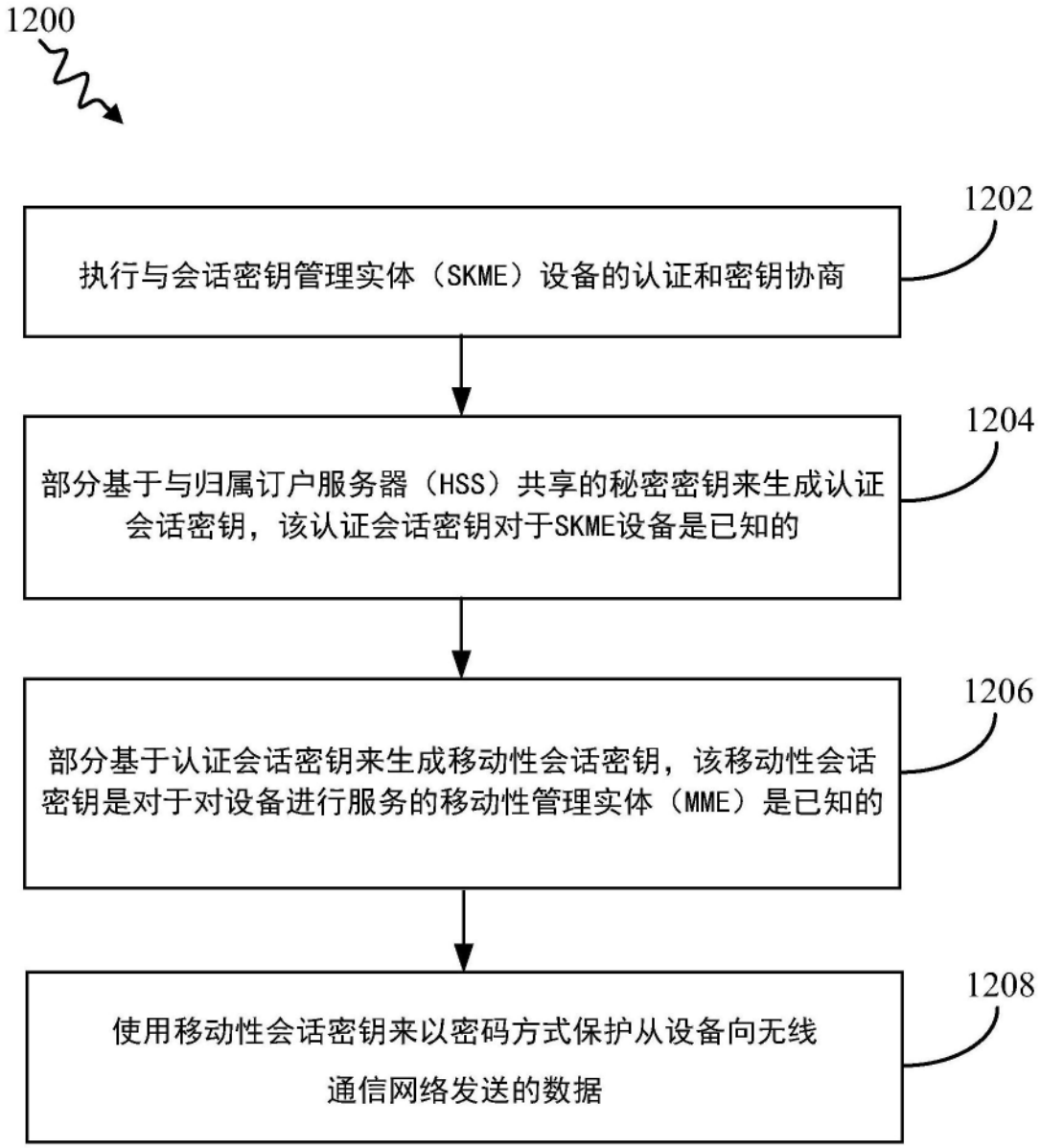

1200
1202
执行与会话密钥管理实体（SKME）设备的认证和密钥协商
1204
部分基于与归属订户服务器（HSS）共享的秘密密钥来生成认证会话密钥，该认证会话密钥对于SKME设备是已知的
1206
部分基于认证会话密钥来生成移动性会话密钥，该移动性会话密钥是对于对设备进行服务的移动性管理实体（MME）是已知的
1208
使用移动性会话密钥来以密码方式保护从设备向无线通信网络发送的数据

图12

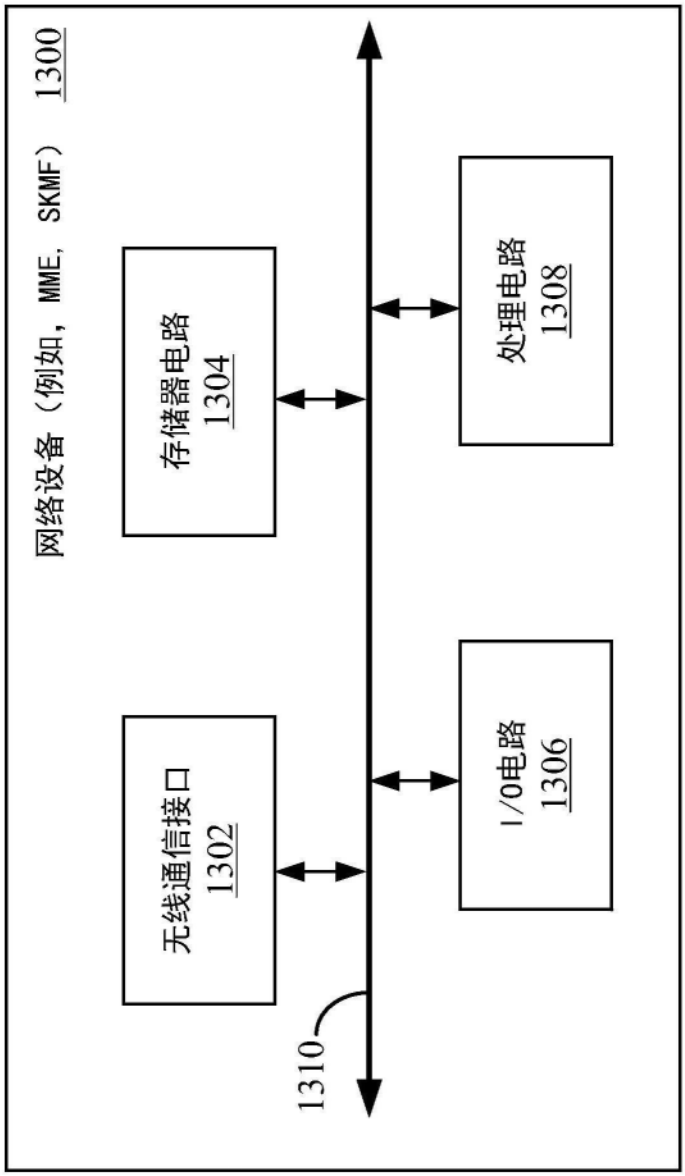

网络设备（例如，MME，SKMF） 1300
存储器电路 1304
处理电路 1308
无线通信接口 1302
I/O电路 1306
1310

图13

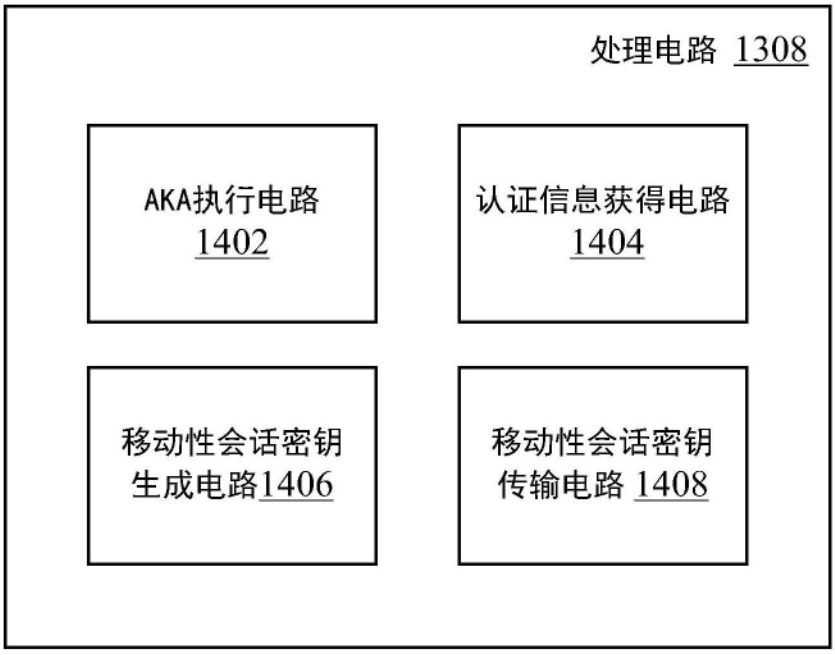

处理电路 1308
AKA执行电路 1402
认证信息获得电路 1404
移动性会话密钥生成电路1406
移动性会话密钥传输电路 1408

图14

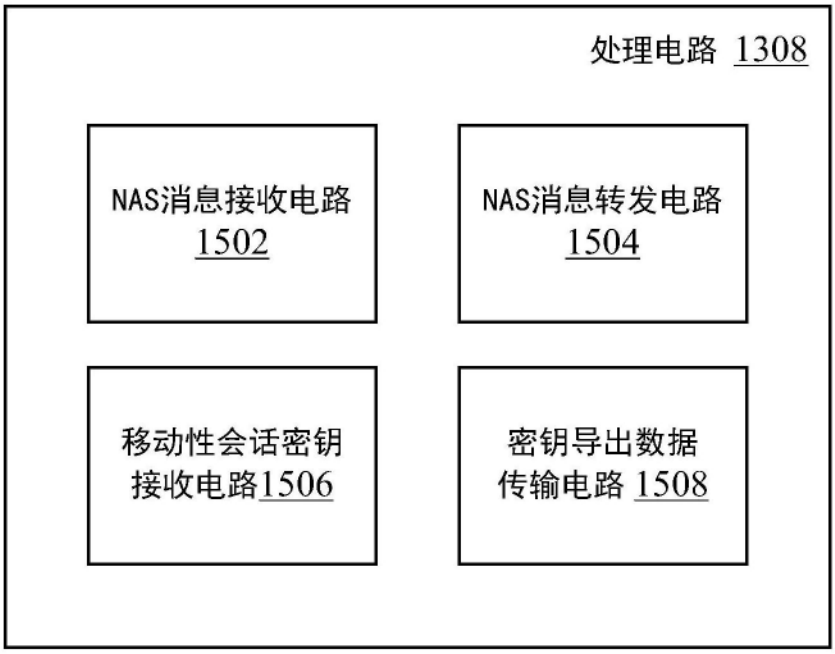

处理电路 1308
NAS消息接收电路 1502
NAS消息转发电路 1504
移动性会话密钥接收电路1506
密钥导出数据传输电路 1508

图15

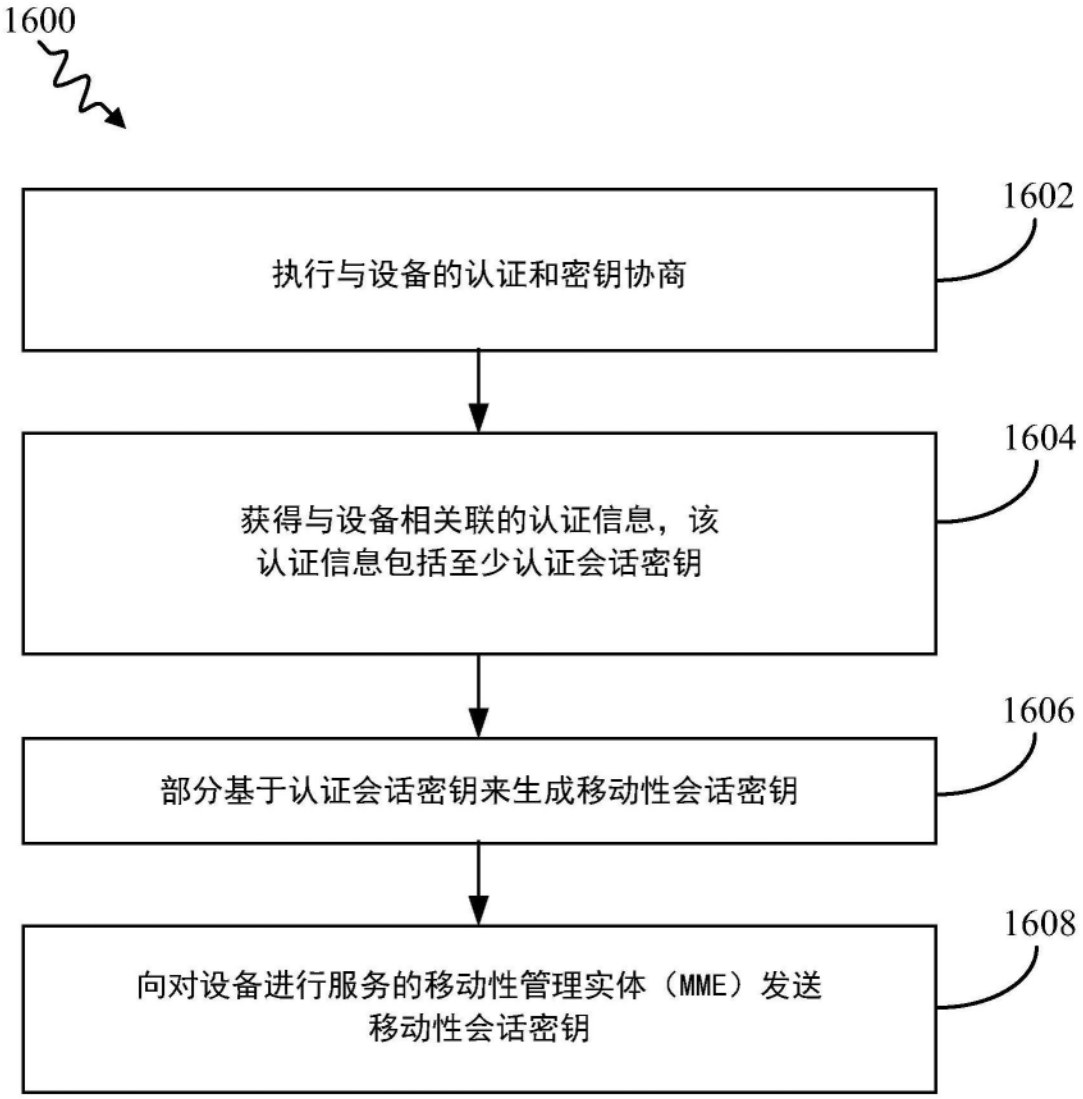

1600
1602
执行与设备的认证和密钥协商
1604
获得与设备相关联的认证信息，该
认证信息包括至少认证会话密钥
1606
部分基于认证会话密钥来生成移动性会话密钥
1608
向对设备进行服务的移动性管理实体（MME）发送
移动性会话密钥

图16

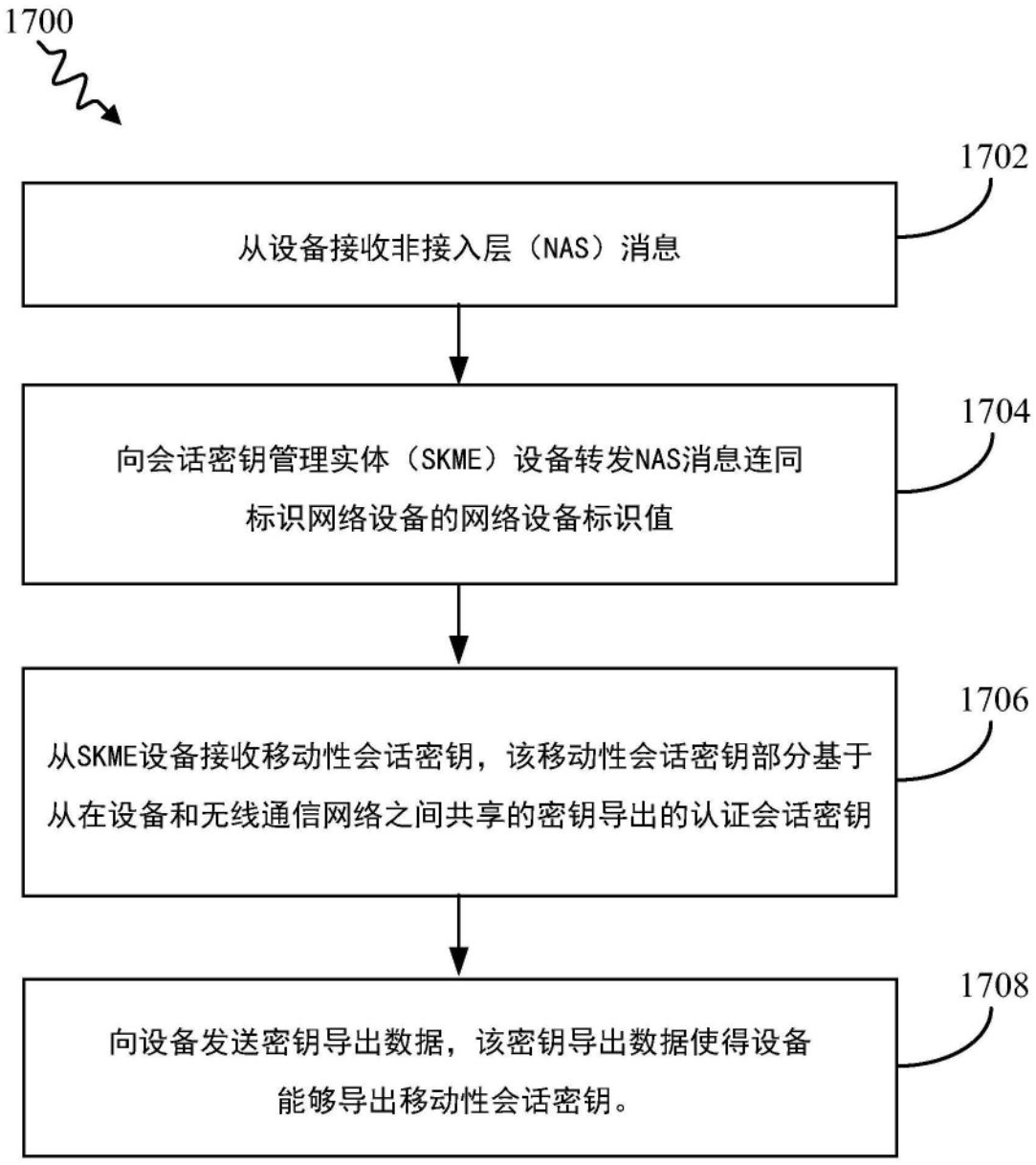

1700
1702
从设备接收非接入层（NAS）消息
1704
向会话密钥管理实体（SKME）设备转发NAS消息连同
标识网络设备的网络设备标识值
1706
从SKME设备接收移动性会话密钥，该移动性会话密钥部分基于
从在设备和无线通信网络之间共享的密钥导出的认证会话密钥
1708
向设备发送密钥导出数据，该密钥导出数据使得设备
能够导出移动性会话密钥。

图17