(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 106797564 B
(45)授权公告日 2020.06.23

(21)申请号 201580051656.9

(22)申请日 2015.08.27

(65)同一申请的已公布的文献号
申请公布号 CN 106797564 A

(43)申请公布日 2017.05.31

(30)优先权数据
62/056,387 2014.09.26 US
14/675,676 2015.03.31 US

(85)PCT国际申请进入国家阶段日
2017.03.24

(86)PCT国际申请的申请数据
PCT/US2015/047297 2015.08.27

(87)PCT国际申请的公布数据
WO2016/048575 EN 2016.03.31

(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·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 12/06(2009.01)
H04L 29/06(2006.01)
H04W 12/12(2009.01)

(56)对比文件
WO 2013009508 A1,2013.01.17,
CN 1482549 A,2004.03.17,
CN 101183938 A,2008.05.21,
CN 101674304 A,2010.03.17,
GB 2424154 A,2006.09.13,
WO 2008074620 A3,2008.11.20,

审查员 赵琴

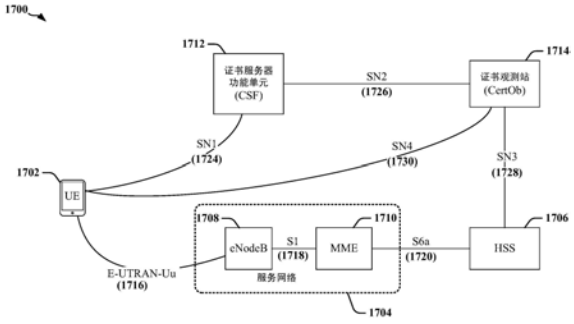
权利要求书4页 说明书21页 附图25页

(54)发明名称

请求式服务网络认证方法及装置

(57)摘要

提供了一种请求式服务网络认证方法及装置。一种方法包括:将具有随机数和签名请求的请求发送给服务网络,其被引导至服务网络的网络功能单元,从服务网络接收对请求的响应,以及基于网络功能单元的签名来认证服务网络。随机数可以提供重放保护。响应可以包括网络功能单元的签名。发送到服务网络的请求可以包括无线资源控制(RRC)消息或跟踪区域更新(TAU)请求。可以利用信任的第三方来认证服务网络以验证与服务网络相关联的证书。



CN 106797564 B

1.一种保护无线通信设备与服务网络之间的无线通信的方法,包括:

在所述服务网络已被认证之后,从所述无线通信设备将请求发送到所述服务网络中的网络功能单元,其中,所述请求包括随机数和签名请求;

由所述无线通信设备从所述网络功能单元接收对所述请求的响应,其中,所述响应包括所述网络功能单元的签名,所述签名是利用在所述网络功能单元中的在信任环境中维护的密钥生成的,所述信任环境是在所述网络功能单元之外的实体不可访问的;以及

基于所述网络功能单元的所述签名以及与在由所述无线通信设备维护的信任网络的列表中标识的信任网络相对应的证书,由所述无线通信设备验证所述服务网络的真实性。

2.根据权利要求1所述的方法,其中,所述签名是利用对应于所述网络功能单元的公共密钥证书来创建的,以及其中,所述公共密钥证书是利用由与所述服务网络相关联的网络运营商提供的所述服务网络的私有密钥来签名的。

3.根据权利要求2所述的方法,其中,验证所述服务网络的真实性包括:

利用信任的第三方来验证对应于所述网络功能单元的所述公共密钥证书。

4.根据权利要求1所述的方法,其中,所述签名是利用在所述无线通信设备和所述网络功能单元之间共享的密钥来创建的。

5.根据权利要求1所述的方法,其中:

由所述无线通信设备维护的所述信任网络的列表标识对应于信任网络的公共密钥或公共密钥证书;

其中,验证所述服务网络的真实性包括:验证所述网络功能单元的所述公共密钥和由所述网络功能单元生成的所述签名。

6.根据权利要求1所述的方法,其中,发送到所述服务网络的所述请求包括无线资源控制,RRC,消息。

7.根据权利要求6所述的方法,其中,所述RRC消息包括RRC连接请求、RRC连接重新建立请求、或RRC重新配置完成消息。

8.根据权利要求6所述的方法,其中,所述RRC消息是在从空闲模式转变期间发送的。

9.根据权利要求1所述的方法,其中,发送到所述服务网络的所述请求包括跟踪区域更新,TAU,请求。

10.根据权利要求1所述的方法,还包括:

将证书完整性信息请求发送到所述服务网络;以及

利用从归属用户服务器接收到的第二证书完整性信息来验证从所述服务网络接收到的第一证书完整性信息;

其中,所述证书完整性信息请求包括对应于所述第二证书完整性信息的证书观测站的标识符;以及

其中,所述证书观测站被配置为维护一个或多个网络的一组证书的完整性。

11.根据权利要求10所述的方法,其中,所述证书观测站的标识符包括互联网协议,IP,地址或通用资源定位符,URL。

12.根据权利要求10所述的方法,其中,验证第一证书完整性信息包括:

利用所述证书观测站的公共密钥来认证对所述证书完整性信息请求的响应。

13.根据权利要求10所述的方法,其中,验证第一证书完整性信息包括:

比较所述第一证书完整性信息与所述第二证书完整性信息；

当确定出所述第一证书完整性信息和所述第二证书完整性信息之间存在不同时，将证书状态请求发送给证书服务器功能单元，CSF；以及

基于来自所述CSF的响应，验证网络功能单元证书的状态；

其中，所述证书状态请求包括标识所述网络功能单元的第一标识信息，标识所述网络功能单元证书的第二标识信息，以及所述网络功能单元证书的版本号；以及

其中，来自所述CSF的响应包括证书状态响应，所述证书状态响应包括所述网络功能单元证书的状态、所述网络的公共密钥，以及利用所述网络的私有密钥由所述CSF创建的所述证书状态响应的签名，以及其中，所述证书状态响应的验证是利用所述网络的所述公共密钥来执行的。

14.一种用于无线通信的装置，包括：

无线收发机；以及

耦合到所述收发机的处理器，所述处理器被配置为：

在服务网络已经被认证之后，将请求发送到所述服务网络中的网络功能单元，其中，所述请求包括随机数和签名请求；

从所述网络功能单元接收对所述请求的响应，其中，所述响应包括所述网络功能单元的签名，所述签名是利用在所述网络功能单元中的在信任环境中维护的密钥生成的，所述信任环境是在所述网络功能单元之外的实体不可访问的；以及

基于所述网络功能单元的所述签名以及与在由所述装置维护的信任网络的列表中标识的信任网络相对应的证书，来验证所述服务网络的真实性。

15.根据权利要求14所述的装置，其中，所述请求包括无线资源控制连接请求或跟踪区域请求，以及其中，所述处理器被配置为：

在所述装置从空闲模式转变时，发送所述无线资源控制连接请求或跟踪区域请求到所述服务网络中的所述网络功能单元。

16.根据权利要求14所述的装置，其中，所述签名是利用在所述装置和所述网络功能单元之间共享的密钥，或是利用使用由与所述服务网络相关联的网络运营商提供的所述服务网络的私有密钥签名的公共密钥证书来创建的。

17.根据权利要求14所述的装置，其中，所述处理器被配置为：

将证书完整性信息请求发送给所述服务网络；

当确定出从所述服务网络接收到的第一证书完整性信息和从归属用户服务器接收到的第二证书完整性信息之间没有不同时，基于所述第二证书完整性信息，验证所述第一证书完整性信息；

当确定在所述第一证书完整性信息和所述第二证书完整性信息之间存在不同时，将证书状态请求发送到证书服务器功能单元，CSF；以及

基于来自所述CSF的响应，验证网络功能单元证书的状态；

其中，所述证书完整性信息请求包括对应于所述第二证书完整性信息的证书观测站的标识符；以及

其中，所述证书观测站被配置为维护一个或多个网络的一组证书的完整性；以及

其中，所述证书状态请求包括所述网络功能单元的标识符、所述网络功能单元证书的

标识符、以及所述网络功能单元证书的版本号。

18.一种证明服务网络的成员资格的方法,包括:

在无线通信设备已经通过与归属网络的安全连接验证了所述服务网络之后,从所述无线通信设备接收第一消息,其中,所述第一消息被引导至所述服务网络的网络功能单元,并且包括随机数和签名请求;

利用所述服务网络的所述网络功能单元中的在信任环境中维护的运营商签名的证书来生成签名,其中,所述信任环境是在所述网络功能单元之外的实体不可访问的;以及

将第二消息发送到所述无线通信设备,其中,所述签名被附加到所述第二消息,其中,所述无线通信设备被配置为使用所述签名基于由所述无线通信设备维护的信任网络的列表,来验证所述服务网络的真实性。

19.根据权利要求18所述的方法,其中,所述运营商签名的证书是由所述服务网络的运营商签名的公共密钥证书。

20.根据权利要求18所述的方法,其中,对应于所述运营商签名的证书的私有密钥是在安全存储设备或安全执行环境中维护的。

21.根据权利要求18所述的方法,其中,对应于所述运营商签名的证书的私有密钥是在信任环境中维护的。

22.根据权利要求18所述的方法,其中,所述签名包括利用在所述无线通信设备和所述网络功能单元之间共享的会话密钥创建的消息认证码,MAC,以及其中,对称密码用于对所述第二消息进行签名。

23.根据权利要求22所述的方法,其中,所述网络功能单元包括移动管理实体,MME,以及所述会话密钥包括访问安全管理实体密钥K_{ASME},以及还包括:

从归属用户服务器,HSS,在利用所述MME的公共密钥加密的消息中接收所述K_{ASME};

利用存储于信任环境中的私有密钥对所述K_{ASME}进行解密;以及

在所述信任环境中存储所述K_{ASME}。

24.根据权利要求22所述的方法,其中,所述网络功能单元包括eNodeB,以及所述会话密钥包括KeNB,以及还包括:

从MME在利用所述eNodeB的公共密钥加密的消息中接收所述KeNB;

利用存储于信任环境中的私有密钥对所述KeNB进行解密;以及

在所述信任环境中存储所述KeNB。

25.根据权利要求18所述的方法,其中,所述签名包括利用所述网络功能单元的私有密钥创建的数字签名,其中,非对称密码用于对所述第二消息签名,以及其中,所述网络功能单元的所述私有密钥存储于信任环境中并且所述签名是在所述信任环境中创建的。

26.根据权利要求18所述的方法,其中,所述网络功能单元包括eNodeB,以及其中,所述第一消息包括无线资源控制,RRC,消息,以及所述第二消息包括对所述RRC消息的响应。

27.根据权利要求26所述的方法,其中,所述RRC消息是RRC连接建立请求、RRC连接重新建立请求或RRC重新配置完成消息。

28.根据权利要求18所述的方法,其中,所述网络功能单元包括MME,以及其中,所述第一消息包括跟踪区域更新,TAU,请求。

29.一种用于无线通信的装置,包括:

用于在无线通信设备已经通过与归属网络的安全连接验证了所述服务网络之后从所述无线通信设备接收第一消息的单元,其中,所述第一消息被引导至服务网络的网络功能单元,并且包括随机数和签名请求;

用于利用所述服务网络的所述网络功能单元中的在信任环境中维护的运营商签名的证书来生成签名的单元,其中,所述信任环境是在所述网络功能单元之外的实体不可访问的;以及

用于将第二消息发送到所述无线通信设备的单元,其中,所述签名被附加到所述第二消息,其中,所述无线通信设备被配置为使用所述签名基于由所述无线通信设备维护的信任网络的列表,来验证所述服务网络的真实性。

30.根据权利要求29所述的装置,其中:

当所述网络功能单元包括eNodeB时,所述第一消息包括无线资源控制RRC消息,以及所述第二消息包括对所述RRC消息的响应;以及

当所述网络功能单元包括移动管理实体,MME,时,所述第一消息包括跟踪区域更新,TAU,请求。

请求式服务网络认证方法及装置

[0001] 相关申请的交叉引用

[0002] 本申请要求享受2014年9月26日提交到美国专利商标局的临时申请 No.62/056,387、以及2015年3月31日提交到美国专利商报局的非临时申请No.14/675,676的优先权和利益,这两个申请的整体内容以引用方式并入本文。

技术领域

[0003] 本公开内容一般涉及通信系统,更具体地涉及用于在无线通信系统中在用户设备和服务网络之间进行认证的系统。

背景技术

[0004] 无线通信系统被广泛部署以提供各种电信服务,例如,电话、视频、数据、消息传送和广播。典型的无线通信系统可以采用多址技术,其能够通过共享可用系统资源(例如,带宽、传输功率)而支持与多个用户的通信。这种多址技术的例子包括码分多址(CDMA)系统、时分多址(TDMA) 系统、频分多址(FDMA)系统、正交频分多址(OFDMA)系统、单载波频分多址(SC-FDMA)系统、以及时分同步码分多址(TD-SCDMA)系统。

[0005] 这些多址技术已经用于各种电信标准,以提供使得不同无线设备能够在城市、国家、区域以及甚至全球级别进行通信的常见协议。随着多址技术的改善和增加,出现了新的电信标准。出现的电信标准的例子是第四代长期演进(LTE)。LTE是对由第三代合作伙伴计划(3GPP)公布的通用移动电信系统(UMTS)移动标准的一组增强。其被设计为通过改善频谱效率、降低成本、改善服务、使用新频谱而更好地支持移动宽带互联网接入,以及使用在下行链路(DL)上的OFDMA、上行链路(UL)上的SC-FDMA 以及多输入多输出(MIMIO)天线技术来更好地集成其它开放式标准。然而,随着对移动宽带接入需求的持续增加,存在对LTE技术的进一步改善和/或具有改善能力的新一代的电信标准的需要。

[0006] 安全配置是建立LTE网络中的逻辑承载或信道(例如,在移动通信设备和网络实体或接入点之间的通信链路)的初始步骤。密钥导出和建立是该安全配置的一部分。大部分生成的密钥是用于非接入层(NAS)安全模式配置(NAS SMC)和接入层(AS)安全模式配置(AS SMC)的加密和完整性密钥。当新一代的通信技术被部署时,可能在安全配置过程中暴露易受攻击的漏洞(vulnerability)。因此,存在改善安全过程的需要。优选地,改善应该能应用于其它多址技术和采用这些技术的电信标准。

发明内容

[0007] 在本公开内容的一方面,提供了一种方法、一种计算机程序产品以及一种装置。

[0008] 根据本文公开的某些方面,一种保护用户设备(UE)和服务网络之间的无线通信的方法包括:在UE和服务网络之间已经建立了安全关联之后,通过UE向服务网络中的网络功能单元发送连接请求或跟踪区域请求,其中所述请求包括随机数(nonce)和签名请求;通过UE从网络功能单元接收对连接请求或跟踪区域请求的响应,其中所述响应包括网络功能单

元的签名;以及基于网络功能单元的签名以及对应于网络功能单元的公共密钥证书通过UE对服务网络进行认证,其中公共密钥证书是利用由与服务网络相关联的网络运营商提供的服务网络的私有密钥来签名的。

[0009] 根据本文公开的某些方面,一种装置包括:无线收发机;以及耦合到收发机的处理器。所述处理器可以被配置为:在UE和服务网络之间已经建立了安全关联之后,向服务网络中的网络功能单元发送连接请求或跟踪区域请求,其中所述请求包括随机数和签名请求;从网络功能单元接收对连接请求或跟踪区域请求的响应,其中所述响应包括网络功能单元的签名;以及基于网络功能单元的签名和对应于网络功能单元的公共密钥证书对服务网络进行认证,其中公共密钥证书是利用由与服务网络相关联的网络运营商提供的服务网络的私有密钥签名的。

[0010] 根据本文公开的某些方面,一种证明服务网络的成员资格的方法包括:在UE已经建立了与归属网络的安全连接之后,从UE接收第一消息,其中所述消息被引导至服务网络的网络功能单元,并且可以包括随机数和签名请求;利用由服务网络的网络功能单元维护的运营商签名的证书来生成签名;以及向UE发送第二消息,其中签名被附加到第二消息。

[0011] 根据本文公开的某些方面,一种装置包括:用于在UE已经建立了与归属网络的安全连接之后从UE接收第一消息的单元,其中所述消息被引导至服务网络的网络功能单元,并且包括随机数和签名请求;用于利用由服务网络的网络功能单元维护的运营商签名的证书来生成签名的单元;以及用于向UE发送第二消息的单元,其中签名被附加到第二消息。可以生成被附加到第二消息的签名以向UE证明所述装置是服务网络的成员。所述运营商签名的证书是由服务网络的运营商签名的公共密钥证书。

附图说明

[0012] 图1是示出网络架构的例子的图。

[0013] 图2是示出接入网络的例子的图。

[0014] 图3是示出用于用户和控制平面的无线协议架构的例子的图。

[0015] 图4是示出接入网络中的演进节点B和用户设备(UE)的例子的图。

[0016] 图5示出了可以在网络(例如LTE无线网络)中实现的E-UTRAN密钥层级的例子。

[0017] 图6示出了可以在操作在LTE分组交换网络中的通信设备中实现的协议栈。

[0018] 图7是示出LTE无线网络的例子中认证的消息流程图。

[0019] 图8示出了在其中UE与服务网络连接以便从归属网络获得服务的网络环境。

[0020] 图9是示出无线网络中的漏洞的第一例子的图。

[0021] 图10是根据本文公开的某些方面示出通过eNodeB用于服务网络的请求式认证的连接请求消息的第一例子的消息流程图。

[0022] 图11是根据本文公开的某些方面示出通过eNodeB用于服务网络的请求式认证的连接请求消息的第二例子的消息流程图。

[0023] 图12是根据本文公开的某些方面示出通过移动管理实体(MME)用于服务网络的请求式认证的跟踪区域更新(TAU)消息的第一例子的消息流程图。

[0024] 图13是根据本文公开的某些方面示出通过eNodeB用于服务网络的请求式认证的连接请求消息的第三例子的消息流程图。

[0025] 图14是根据本文公开的某些方面示出通过eNodeB用于服务网络的请求式认证的连接请求消息的第四例子的消息流程图。

[0026] 图15是根据本文公开的某些方面示出通过MME用于服务网络的请求式认证的TAU消息的第二例子的消息流程图。

[0027] 图16是示出无线网络中的漏洞的第二例子的图。

[0028] 图17是根据本文公开的某些方面示出被配置为克服图16中所示的漏洞的无线网络环境的图。

[0029] 图18是根据本文公开的某些方面示出通过eNodeB用于服务网络的请求式认证的连接请求消息的第五例子的消息流程图。

[0030] 图19是根据本文公开的某些方面示出通过eNodeB用于服务网络的请求式认证的连接请求消息的第六例子的消息流程图。

[0031] 图20是根据本文公开的某些方面示出通过MME用于服务网络的请求式认证的TAU消息的第三例子的消息流程图。

[0032] 图21是示出采用可以根据本文公开的某些方面适用的处理电路的装置的例子的框图。

[0033] 图22是根据本文公开的某些方面在UE处执行的无线通信方法的流程图。

[0034] 图23示出了根据本文公开的一个或多个方面适用的装置的硬件实现方式的第一例子。

[0035] 图24是根据本文公开的某些方面在网络节点处执行的无线通信方法的流程图。

[0036] 图25示出了根据本文公开的一个或多个方面适用的装置的硬件实现方式的第二例子。

具体实施方式

[0037] 结合附图在下文阐述的详细描述意图作为各种配置的描述，且不打算表示在其中可以实践本文描述的概念的仅有配置。为了提供对各个概念的透彻理解的目的，详细的描述包括特定细节。然而，本领域技术人员可以理解的是，可以在没有这些特定细节的情况下实践这些概念。在一些实例中，以框图形式示出已知的结构和部件，以避免模糊这种概念。

[0038] 现在将结合各种装置和方法呈现电信系统的若干方面。这些装置和方法可以在后续详细描述中进行描述并在附图中通过各种块、模块、部件、电路、步骤、过程、算法等(统称为“要素”)进行图示。可以使用电子硬件、计算机软件或其任意组合来实现这些要素。至于这些要素是实现为硬件还是软件取决于特定的应用和施加到整体系统上的设计约束。

[0039] 举例而言，可以通过计算机或包括一个或多个处理器的“处理系统”来实现要素、要素的任意部分或要素的任意组合。处理器的例子包括微处理器、微控制器、数字信号处理器(DSP)、现场可编程门阵列(FPGA)、可编程逻辑设备(PLD)、状态机、门控逻辑、离散硬件电路、以及被配置为执行遍及本公开内容描述的各种功能的其它适当的硬件。处理系统中的一个或多个处理器可以执行软件。不论被称作软件、固件、中间件、微码、硬件描述语言或其它，软件可以被广泛地解释以表示指令、指令集、代码、代码段、程序代码、程序、子程序、软件模块、应用、软件应用、软件封装、例程、子例程、对象、可执行文件、执行线程、进程、函数等。

[0040] 因此，在一个或多个示例性实施例中，所描述的功能可以实现在硬件、软件、固件或其任意组合中。如果实现在软件中，则功能可以存储于或编码为在计算机可读介质中的一个或多个指令或代码。计算机可读介质包括计算机存储介质。计算机可读介质可以包括瞬态和非瞬态存储介质，其可以由一个或多个处理器读取和/或操纵。存储介质可以是任意可用的介质，其可以由计算机访问。通过例子而非限制，这种计算机可读介质可以包括随机存取存储器(RAM)、只读存储器(ROM)、可编程ROM(PROM)、可擦除PROM(EPROM)、电可擦除PROM(EEPROM)、压缩盘只读存储器(CD-ROM)、或其它光盘存储、磁盘存储或其它磁存储设备、或可以用于以指令或数据结构形式携带或存储且被计算机访问的期望的程序代码的任意其它介质。如在本文使用的，磁盘或光盘包括压缩光盘(CD)、激光光盘、光盘、数字通用光盘(DVD)、以及软盘，其中磁盘通常磁性地复制数据，而光盘通过激光光学地复制数据。上述的组合也应该包含于计算机可读介质的范围内。

[0041] 本文公开的某些方面涉及系统和方法，通过其可以保护无线链路建立和/或承载建立过程。本公开内容的某些方面解决可能在较新一代无线接入技术(RAT)(包括第五代(5G)和后续的网络)以及在第四代(4G)和之前的网络中出现的安全问题。4G LTE网络架构的配置和操作在本文中通过例子描述，并且出于简化某些方案描述的目的，其可以应用于多个RAT。

[0042] 图1是示出LTE网络架构100的图。LTE网络架构100可以称作演进分组系统(EPS)。EPS可以包括一个或多个用户设备(UE)102、演进UMTS 陆地无线接入网络(E-UTRAN)104、演进分组核心(EPC)110、归属用户服务器(HSS)120、以及运营商的互联网协议(IP)服务122。EPS可以与其它接入网络互连，但是为了简单起见，没有示出那些实体/接口。如图所示，EPS提供分组交换服务，但是，如本领域技术人员可以理解的，遍及本公开内容呈现的各种概念可以延伸到提供电路交换服务的网络。

[0043] E-UTRAN包括演进节点B(eNodeB)106和其它eNodeB 108。eNodeB 106提供朝向UE 102的用户和控制平面协议终止。eNodeB 106可以经由回程(例如，X2接口)连接到其它eNodeB 108。eNodeB 106还可以称作基站、基站收发机、无线基站、无线收发机、收发机功能单元、基本服务集 (BSS)、扩展服务集(ESS)、eNB、或一些其它适当的术语。eNodeB 106 向UE 102提供到EPC 110的接入点。UE 102的例子包括蜂窝电话、智能电话、会话发起协议(SIP)电话、膝上型计算机、个人数字助理(PDA)、卫星无线电、全球定位系统、多媒体设备、视频设备、数字音频播放器(例如，MP3播放器)、摄像机、游戏控制台、虚拟现实设备、平板计算设备、媒体播放器、电器、游戏设备、可穿戴计算设备(例如，智能手表或光学头戴式显示器)、或任意其它类似功能设备。UE 102还可以被本领域技术人员称作移动站、用户站、移动单元、用户单元、无线单元、远程单元、移动设备、无线设备、无线通信设备、远程设备、移动用户站、接入终端、移动终端、无线终端、远程终端、手持设备、用户代理、移动客户端、客户端、或一些其它适当的术语。

[0044] eNodeB 106通过“S1”接口连接到EPC 110。EPC 110包括MME 112、其它MME 114、服务网关116、以及分组数据网络(PDN)网关118。MME 112是控制节点，其处理UE 102和EPC 110之间的信令。一般而言，MME 112提供承载和连接管理。所有的用户IP分组通过服务网关116转移，该网关自身连接到PDN网络118。PDN网关118提供UE IP地址分配以及其它功能。PDN网关118连接到运营商的IP服务122。运营商的IP服务122 可以包括互联网、内联网、IP

多媒体子系统(IMS)以及PS流传输服务(PSS)。

[0045] 图2是示出LTE网络架构中的接入网络200的例子的图。在该例子中，接入网络200被划分成多个蜂窝区域(小区)202。一个或多个较低功率类别的eNodeB 208可以具有与一个或多个小区202重叠的蜂窝区域210。较低功率类别的eNodeB 208可以是毫微微小区(例如，家庭eNodeB(HeNB))、微微小区、微小区、或远程无线电头端(RRH)。宏eNodeB 204均被分配给相应小区202，并被配置为向小区202内所有的UE 206提供到EPC 110 的接入点。在接入网络200的该例子中不存在集中式控制器，但是可以在替代配置中使用集中式控制器。eNodeB 204负责所有的无线电相关功能，包括无线电承载控制、准入控制、移动性控制、调度、安全以及到服务网关116的连接。

[0046] 接入网络200采用的调制和多址方案可能取决于所部署的特定电信标准而变化。在LTE应用中，在DL上使用OFDM且在UL上使用SC-FDMA，以支持频分双工(FDD)和时分双工(TDD)。如本领域技术人员可以根据后续详细描述理解到的，本文提出的各种概念非常适于LTE应用。然而，这些概念可以容易地扩展到采用其它调制和多址技术的其它电信标准。举例而言，这些概念可以扩展到演进数据优化(EV-DO)或超移动宽带(UMB)。EV-DO和UMB是由第三代合作伙伴计划2(3GPP2)公布的空中接口标准，其作为CDMA2000标准族的一部分，并采用CDMA来提供对移动站的宽带互联网接入。这些概念还可以扩展到通用陆地无线接入(UTRA)，其采用宽带CDMA(W-CDMA)和CDMA的其它变型，例如TD-SCDMA；采用TDMA的全球移动通信系统(GSM)；以及演进UTRA(E-UTRA)、IEEE 802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20、以及采用OFDMA 的闪速OFDMA。在来自3GPP组织的文档中描述了UTRA、E-UTRA、UMTS、LTE和GSM。在来自3GPP2组织的文档中描述了CDMA2000和 UMB。实际采用的无线通信标准和多址技术将取决于特定的应用和施加到系统上的整体设计约束。

[0047] eNodeB 204可以具有支持MIMO技术的多个天线。使用MIMO技术使得eNodeB 204能够利用空间域来支持空间复用、波束成型以及发射分集。空间复用可以用于在同一频率上同时发送不同的数据流。可以将数据流发送到单个UE 206以增加数据速率，或发送到多个UE 206以增加整体系统容量。这可以通过以下来实现：在空间上预编码每个数据流(即，应用振幅和相位的尺缩放)，然后通过DL上的多个发送天线来发送每个经空间预编码的流。经空间预编码的数据流到达具有不同的空间签名的UE 206，这使得每个UE 206能够恢复去往所述UE 206的一个或多个数据流。在UL 上，每个UE 206发送经空间预编码的数据流，这使得eNodeB 204能够识别每个经空间预编码的数据流的源。

[0048] 一般在信道状况良好时使用空间复用。当信道状况不是很好时，使用波束成型来将传输能量集中在一个或多个方向。这可以通过空间预编码数据以通过多个天线进行传输来实现。为了实现在小区边缘的良好覆盖，可以组合发射分集使用单个流波束成型传输。

[0049] 在后续详细描述中，将结合支持DL上的OFDM的MIMO系统描述接入网络的各方面。OFDM是扩频技术，其在OFDM符号内的多个子载波上调制数据。子载波以精确频率间隔开。间隔提供“正交性”，其使得接收机能够从子载波恢复数据。在时域中，保护间隔(例如，循环前缀)可以被添加到每个OFDM符号，以对抗OFDM符号间干扰。UL可以使用DFT扩展的OFDM信号形式的SC-FDMA，以补偿高的峰均功率比(PAPR)。

[0050] 图3是示出用于LTE中的用户和控制平面的无线协议架构的例子的图。用于UE和eNodeB的无线协议架构示出具有三层：层1、层2和层3。层1 (L1层)是最低层，并且实现各种

物理层信号处理功能。L1层在此将被称为物理层306。层2(L2层)308在物理层306之上,并负责在物理层306 之上在UE和eNodeB之间的链路。

[0051] 在用户平面中,L2层308包括介质访问控制子层(介质访问子层)310、无线链路控制(RLC)子层312、以及分组数据汇聚协议(PDCP)子层314,它们在网络侧终止于eNodeB处。虽然未示出,但是UE可以具有在L2层 308之上的若干上层,包括网络层(例如,IP层),其在网络侧终止于PDN 网关118,以及应用层,其在连接的另一端处(例如,远端UE、服务器等)终止。

[0052] PDCP子层314提供在不同无线承载和逻辑信道之间的复用。PDCP子层314还提供上层数据分组的头部压缩以减小无线传输开销,通过加密数据分组进行保护,以及针对UE在eNodeB之间的切换支持。RLC子层312 提供上层数据分组的分割和重组,重传丢失的数据分组,以及重新排序数据分组,以补偿由于混合自动重传请求(HARQ)引起的乱序接收。介质访问子层310提供在逻辑和传输信道之间的复用。介质访问子层310还负责在UE之间分配一个小区中的各种无线资源(例如,资源块)。介质访问子层310还负责HARQ操作。

[0053] 在控制平面中,用于UE和eNodeB的无线协议架构本质上与用于物理层306和L2层308的一样,除了对于控制平面不存在头部压缩功能。控制平面还包括在层3(L3层)内的无线资源控制(RRC)子层316。RRC子层316负责获得无线资源(即,无线电承载),并用于使用eNodeB和UE 之间的RRC信令配置较低层。

[0054] 图4是在接入网络中与UE 450通信的eNodeB 410的框图。在DL中,将来自核心网络的上层分组提供给控制器/处理器475。控制器/处理器475 实现L2层的功能。在DL中,控制器/处理器475提供头部压缩、加密、分组分段和重排序、在逻辑和传输信道之间的复用、以及基于各种优先度量针对UE 450的无线资源分配。控制器/处理器475还负责HARQ操作、丢失分组的重传、以及到UE 450的信号传输。

[0055] 发送(TX)处理器416实现用于L1层(即,物理层)的各种信号处理功能。信号处理功能包括编码和交织以促进在UE 450处的前向纠错 (FEC),以及基于各种调制方案(例如,二进制相移键控(BPSK)、正交相移键控(QPSK)、M相移相键控(M-PSK)、M阶正交幅度调制(M-QAM)) 映射到信号星座。然后将已编码和已调符号分割成并行的流。随后每个流被映射到OFDM子载波,在时域和/或频域中与参考信号(例如,导频)进行复用,然后使用逆傅里叶变换(IFFT)组合到一起以产生携带时域OFDM 符号流的物理信道。OFDM流被空间预编码以产生多个空间流。来自信道估计器474的信道估计可以用于确定编码和调制方案,以及用于空间处理。可以从参考信号和/或由UE 450发送的信道状况反馈来导出信道估计。然后将每个空间流经由单独的发射机418TX提供给不同的天线420。每个发射机418TX将RF载波调制有相应的空间流以供传输。

[0056] 在UE 450处,每个接收机454RX通过其各自的天线452接收信号。每个接收机454RX恢复被调制在RF载波上的信息并将该信息提供给接收 (RX)处理器456。RX处理器456实现L1层的各种信号处理功能。RX 处理器456执行对信息的空间处理以恢复去往UE 450的任意空间流。如果多个空间流去往UE 450,则它们可以被RX处理器456组合为单个OFDM 符号流。RX处理器456然后利用快速傅里叶变换(FFT)将OFDM符号流从时域转换到频域。频域信号包括用于OFDM信号的每个子载波的单独的 OFDM符号流。通过确定由eNodeB 410发送的最可能的信号星座点,来恢复和解调参考信号和每个子载波上的符号。这些软决策可以基于由

信道估计器458计算出的信道估计。然后对软决策进行解码和去交织来恢复最初在物理信道上由eNodeB 410发送的数据和控制信号。然后将所述数据和控制信号提供给控制器/处理器459。

[0057] 控制器/处理器459实现L2层。控制器/处理器可以与存储程序代码和数据的存储器460相关联。存储器460可以被称作计算机可读介质。在UL 中，控制器/处理器459提供在传输和逻辑信道之间的解复用、分组重组、解密、头部解压缩、控制信号处理，以恢复来自核心网络的上层分组。上层分组然后被提供给数据宿462，其表示在L2层之上的所有协议层。各种控制信号还可以被提供给数据宿462用于L3处理。控制器/处理器459还负责使用确认(ACK)和/或否定确认(NACK)协议进行误差检测以支持HARQ 操作。

[0058] 在UL中，数据源467用于向控制器/处理器459提供上层分组。数据源467表示在L2层之上所有的协议层。类似于结合通过eNodeB 410进行的DL传输描述的功能，控制器/处理器459通过基于eNodeB 410的无线资源分配提供头部压缩、加密、分组分段和重排序、以及在逻辑和传输信道之间的复用，来实现用于用户平面和控制平面的L2层。控制器/处理器459 还负责HARQ操作、丢失分组的重传以及到eNodeB 410的信号传输。

[0059] 由信道估计器458根据参考信号或eNodeB 410发送的反馈导出的信道估计可以由TX处理器468用于选择适当的编码和调制方案，并促进空间处理。将由TX处理器468生成的空间流经由单独的发射机454TX提供给不同的天线452。每个发射机454TX将RF载波调制有相应的空间流以供传输。

[0060] 在eNodeB 410处以类似于在UE 450处结合接收机功能描述的方式处理UL传输。每个接收机418RX通过其各自的天线420接收信号。每个接收机418RX恢复被调制在RF载波上的信息，并将所述信息提供给RX处理器470。RX处理器470可以实现L1层。

[0061] 控制器/处理器475实现L2层。控制器/处理器475可以与存储程序代码和数据的存储器476相关联。存储器476可以被称作计算机可读介质。在UL中，控制器/处理器475提供在传输和逻辑信道之间的解复用、分组重组、解密、头部解压缩、控制信号处理，以恢复来自UE 450的上层分组。可以将来自控制器/处理器475的上层分组提供给核心网络。控制器/处理器 475还负责使用ACK和/或NACK协议进行误差检测以支持HARQ操作。

[0062] LTE网络中的承载建立

[0063] 在LTE网络中的无线链路建立可以涉及在提供对网络的接入的接入点和通信设备之间建立一个或多个无线承载。无线链路建立通常包括安全激活交换。会话承载(其可以是逻辑承载或逻辑信道)然后可以建立在无线链路上，并且一个或多个服务和/或通信可以建立在会话承载上。会话承载、服务和/或通信可以由一个或多个安全密钥来保证安全。

[0064] 作为会话承载建立的一部分，可能发生认证请求和/或一个或多个密钥交换。在根据LTE兼容协议操作的网络中，可以通过通信设备基于由一个或多个网络实体提供的算法导出密钥。

[0065] E-UTRAN密钥层级的例子

[0066] 图5示出了可以实现在典型的LTE网络中的典型E-UTRAN密钥层级 500。在通信设备中，在网络侧的网络实体中的通用用户身份模块(USIM) 和认证中心(AuC)使用主密钥(K)502来生成密码密钥(CK)504和完整性密钥(IK)506。密码密钥(CK)504和完整性密钥(IK)506然后可以由网络实体中的通信设备和归属用户服务器(HSS)使用来生成接入安全

管理实体密钥(K_{ASME})508。在LTE网络中操作的通信设备的安全激活可以通过认证与密钥协商过程(AKA)、非接入层(NAS)安全模式配置(NAS SMC)和接入层(AS)安全模式配置(AS SMC)来完成。AKA用于导出 K_{ASME} 508,然后其用作用于计算NAS密钥510和512以及AS密钥514、516、518和520的基础密钥。通信设备和网络侧的MME随后可以使用K_{ASME} 508来生成一个或多个这些安全密钥。

[0067] LET分组交换网络可以构建于多个层级协议层中,其中较低协议层为上层提供服务,并且每层负责不同的任务。例如,图6示出了可以实现在 LTE分组交换网络中操作的通信设备中的协议栈600的例子。在该例子中, LTE协议栈600包括物理(PHY)层604、介质访问控制层606、无线链路控制(RLC)层608、分组数据汇聚协议(PDCP)层611、RRC层612、 NAS层614、以及应用(APP)层616。在NAS层614之下的层通常被称作接入层(AS)层602。

[0068] RLC层608可以包括一个或多个信道610。RRC层612可以实现用于 UE的各种监视模式,包括连接状态和空闲状态。NAS层614可以维护通信设备的移动管理上下文、分组数据上下文和/或其IP地址。注意,其它层可以存在于协议栈600中(例如,在图示层之上、之下和/或之间),但是为了图示目的进行了省略。无线电/会话承载613例如可以建立在RRC层612处和/或NAS层614处。因此,NAS层614可由通信设备和MME用于生成安全密钥$K_{NAS\ enc}$ 510和$K_{NAS-int}$ 512。类似地,RRC层612可以由通信设备和eNodeB用于生成安全密钥K_{UP-enc} 516、$K_{RRC-enc}$ 518以及$K_{RRC-int}$ 520。虽然安全密钥K_{UP-enc} 516、$K_{RRC-enc}$ 518以及$K_{RRC-int}$ 520可以在RRC层612 生成,这些密钥可以由PDCP层611用于保护信令和/或用户/数据通信的安全。例如,密钥K_{UP-enc} 516可以由PDCP层611用于保护用户/数据平面(UP) 通信的安全,而密钥$K_{RRC-enc}$ 518和$K_{RRC-int}$ 520可以用于保护在PDCP层611 处的信令(即,控制)通信的安全。

[0069] 在一个例子中,在建立这些安全密钥(密钥$K_{NAS\ enc}$ 510、$K_{NAS-int}$ 512、K_{UP-enc} 516、$K_{RRC-enc}$ 518和/或$K_{RRC-int}$ 520)之前,可以在不安全的公共控制信道(CCCH)上发送(未保护的或未加密的)到通信设备/来自通信设备的通信。在这些安全密钥建立之后,可以在专用控制信道(DCCH)上发送这些相同的用户数据和/或控制/信令通信。

[0070] 在LTE兼容的网络中在连接建立/会话承载建立过程期间,如果现有的本地NAS安全上下文已经从先前建立会话就存在,则AKA和NAS SMC 过程是可选的。在服务请求、附接请求和TAU请求时,可以重新使用现有的NAS上下文。TAU请求可以由UE周期性发送,或者在UE进入与UE 不关联的跟踪区域时发送,其中所述跟踪区域(或路由区域)可以是UE 在其中能够在无需首先更新网络的情况下移动的区域。

[0071] 可以使用作为输入之一提供的单独算法身份,导出在AS(用户平面和 RRC)和NAS二者处用于加密和完整性算法的安全密钥。在NAS级别处 (例如,NAS层614),这通过接入节点(eNodeB)在NAS安全模式命令中在NAS SMC过程期间提供给通信设备。在AS级别,待使用的算法由无线资源控制(RRC)安全模式命令提供。可以通过密钥导出函数(KDF),例如HMAC-SHA-256函数,进行密钥生成。在生成NAS安全密钥$K_{NAS\ enc}$ 510和完整性密钥$K_{NAS-int}$ 512和RRC安全密钥K_{UP-enc} 516、$K_{RRC-enc}$ 518和完整性密钥$K_{RRC-int}$ 520时,密钥导出函数KDF采用若干类型的输入,包括在安全激活交换期间由网络提供的输入算法身份。例如,输入算法身份可以标识高级加密标准(AES)或“SNOW-3G”。

[0072] 应该注意,在一些实现方式中,使用相同的密钥导出函数(KDF)(例如,HMAC-SHA-256)生成所有的安全密钥(例如,NAS加密和完整性密钥和RRC加密和完整性密钥),所述密

钥导出函数使用根/基础密钥(例如，K_{ASME})、一个或多个固定输入、以及多个可能的输入算法身份之一(即,安全密钥＝KDF(根/基础密钥,固定输入,算法身份))。

[0073] AKA过程的例子

[0074] 图7是示出在LTE无线网络中认证的例子的流程图700。UE 702可以通过服务网络704连接到网络,以便从网络运营商提供的归属网络706获得服务。在承载建立期间,UE 702可以建立与归属网络706的HSS 712的安全连接。UE 702可以信任HSS 712,而服务网络704的eNodeB 708可能不被信任。UE 702可以发送具有标识信息(例如,国际移动用户身份(IMSI)) 的NAS附接请求720。MME 710接收NAS附接请求720,并将请求720 在认证信息请求消息722中转发给HSS 712。认证信息请求消息722可以包括UE 702的IMSI和服务网络标识符(SN-id)。HSS 712可以用认证信息响应消息724来进行响应,其包括认证值(AUTN)、预期结果值(XRES)、随机数(RAND)以及K_{ASME}。AUTN由AuC生成,并与RAND一起向UE 702认证HSS 712。在MME 710和HSS 712之间的消息722、724在链路 740上被传送并受到认证、授权和计费协议(Diameter)的保护。

[0075] MME 710将NAS认证请求726发送到UE 702,UE 702用NAS认证响应消息728进行响应。NAS认证请求726包括AUTN、RAND和密钥集标识符(KSI_{ASME})。MME 710可以将非接入层(NAS)安全模式配置(NAS SMC)消息730发送到UE 702。UE 702随后将“NAS安全模式完成”消息732发送到MME 710,MME 710用信号通知eNodeB 708“S1AP初始上下文建立”消息734。eNodeB 708然后将RRC非接入层(NAS)安全模式配置(RRC SMC)消息736发送给UE 702,UE 702在就绪时用RRC安全模式完成消息738进行响应。

[0076] 在某些网络实现方式中,在已经完成认证之后一定时段内,服务网络 704受到信任。在一个例子中,可以在认证之后信任服务网络704,直到通过HSS 712执行另一认证过程(AKA)为止。可以通过网络运营商确定建立的信任续存的持续时间。网络运营商可以配置信任时段为持续数个小时、数天或数周。

[0077] 在演进网络技术中安全问题的例子

[0078] 由于4G、5G以及其它网络技术的开发,某些网络功能单元可以被推向网络边缘。在一些实例中,一个或多个网络功能单元的重新安置可能使对蜂窝核心网络的信任降低或无效。

[0079] 在一个例子中,毫微微小区或家庭eNodeB(HeNB)可以被部署为通过宽带连接提供局部无线服务。毫微微小区可以被特征化为小的、低功率的蜂窝基站,通常被设计用于家庭或小型商业环境。毫微微小区可以是任意的小型小区,通常具有有限范围和/或有限数量的活动附接UE,其通过广域网或连接而连接到网络运营商的网络上。毫微微小区可以在一个或多个网络中操作,包括WCDMA、GSM、CDMA2000、TD-SCDMA、WiMAX 和LTE网络。部署较新的技术和/或使用毫微微小区可能导致网络功能单元在更容易受到攻击的较少受到保护和/或隔离的位置中进行处理。对于这些和其它原因,由小型小区或中继节点提供的安全级别可能相对宏小区提供的安全显著降低。期望增加小型小区和中继器的部署以支持在网络中的多跳。

[0080] 在另一例子中,在某些较新的技术中的网络功能单元可以位于共享系统中,和/或在云环境中提供。在这种系统和环境中,网络和计算功能单元可以被虚拟化,并且通常被第三方提供商所管理。虽然网络运营商能够保护到云的接入路径,但是云内部的安全不能得

到保证。在一些实例中，在虚拟(云)环境的内部安全和虚拟化系统性能之间进行折衷。在一些实例中，网络运营商不需要拥有用于连接UE的网络设备，和/或网络中的网络设备的不同部件可以被不同运营商拥有。可能导致在运营商之间减少的隔离，并且一些网络运营商可能更容易访问其它网络运营商的证书。例如，当两个网络运营商共享公共的eNodeB或MME时，第一网络运营商的证书可能更容易被第二网络运营商侵占。

[0081] 当某些安全假设无效时，可以暗指网络是不安全的。在4G AKA中，例如，HSS是受信任的网络实体，并且HSS可以是信任根。在UE和服务网络之间相互认证可以取决于在HSS和服务网络之间的安全性。HSS代表 UE认证服务网络，并通过安全信道将用于UE的认证证书提供给服务网络。

[0082] 图8是示出UE 802在其中与服务网络804连接以便从归属网络812获得服务的网络环境的简化框图800。在描绘的例子中，UE 802可以通过在作为服务网络804的一部分操作的E-UTRAN中提供的eNodeB 808建立与 MME 810的无线连接814。MME 810通过链路818连接到归属网络812的 HSS 806。

[0083] 由于共享使用网络硬件、将网络功能单元重新布置到网络边缘和/或将 eNodeB 808和/或MME 810放置在公共或其它不安全的物理位置，可能损害服务网络的eNodeB 808和/或MME 810。

[0084] 图9是示出服务网络804的某些漏洞的简化框图900。攻击者902可能利用某些协议和/或软件漏洞来获得会话证书。攻击者902可以包括如下功能：能够使用会话证书来冒充(通过通信链路904)有效运营商的服务网络804并从试图建立与受到攻击者902损害的运营商网络804的连接的UE 802 捕获信息。

[0085] 在一个例子中，当攻击者902利用在原本良好的安全协议中的实现缺陷时，攻击可以表现为心脏流血(heart-bleed)攻击。攻击者902可以利用网络设备或网络功能单元共处一处来获取证书，例如，发送给MME 810的认证向量(AV)908和/或由eNodeB 808使用、维护或生成的加密密钥 (KeNB)906。可以从eNodeB 808、MME 810和/或从可用于提供共享网络设备或功能的并置硬件的互连814、816的一部分获取证书。

[0086] 会话证书很少从HSS 806获得，并且会话证书可以在以小时或天可测量的时段内保持有效。拦截到证书的攻击者902可以冒充服务网络804，直到通过HSS 806执行下一认证过程为止。

[0087] 在一个例子中，攻击者902可以在AKA过程之后拦截证书。攻击者 902可以是异常的公共陆地移动网络(PLMA)，其可以冒充由有效网络运营商提供的服务网络804。eNodeB 808、MME 810和/或互连814、816中的漏洞可能受到攻击者监视，以便捕获与UE 802相关联的IMSI、包括密钥906和其它证书的信息，例如与由UE 802或代表UE 802建立的连接相关的认证向量908。在一些实例中，攻击者902中的MME可能冒充有效服务网络804中的MME 810，并利用拦截的IMSI、认证向量908和密钥906 来建立与UE 802的通信链路904。攻击者902的网络实体然后可以存取UE 802上的信息，并可以监视起源于UE 802的通信。

[0088] 服务网络的增强认证

[0089] 根据本文公开的某些方面，可以通过在建立网络连接时对服务网络804 进行认证来增强网络的安全。UE 802可以适于或被配置为在必要时尽可能完全地对服务网络804进行认证。也就是说，UE 802可以被配置为当与服务网络的连接活跃时避免不必要的认证过

程并且基于先前认证可以信任服务网络。

[0090] 为了认证服务网络并避免基于获取会话秘密(例如,用于UE 802的认证向量)的攻击,可以在UE 802处维护信任网络的列表,其中所述列表标识公共或共享密钥、证书和/或对应于信任网络的其它证书。在一个例子中,UE 802可以配置有受信任的PLMN列表和对应的公共密钥证书。eNodeB 808和MME 810可以配置有由其各自的运营商签名的公共密钥证书,所述运营商可以是同一运营商,并且其可以包括服务网络804的运营商。在安全的存储设备或安全的执行环境(例如TrE)中维护对应于网络功能单元(包括eNodeB 808和MME 810)使用的公共密钥的私有密钥,并且攻击者通常不能获取保持在TrE内的私有密钥。

[0091] 图10、11和12是示出用于使用基于公共密钥的方法来认证服务网络 804的请求式过程的例子的消息流程图1000、1100、1200。运营商签名的公共密钥用于认证服务网络804。服务网络804可以配置有由信任的第三方 (TTP)(例如,Verisign或互联网号码分配局(IANA))签名的证书。在一些实例中,服务网络804可以采用自我签名的证书,其由归属网络812在信任认证机构(CA)的列表中提供给UE 802。信任CA的列表可以包括运营商及其对应公共密钥。信任CA的列表和公共密钥或证书可以通过安全信道分发给漫游合作伙伴。

[0092] 网络功能单元(包括MME 810和eNodeB 808)可以利用运营商签名的证书来证明其是服务网络804的成员。不具有对应于为网络功能单元发布的公共密钥的私有密钥的攻击者不能向UE 802认证其自己。

[0093] 根据本文公开的某些方面,UE 802发起的信令和/或消息可以被用于使能服务网络804的请求式认证。通过在这种信令上“捎带”认证服务网络 804,可以避免基线开销,并且可以消除空闲状态开销。

[0094] RRC消息可以用于认证eNodeB 808。这种RRC消息的例子包括RRC 连接请求以及RRC连接重新建立。UE 802可以请求对与eNodeB 808交换的连接消息进行签名。在一些实例中,UE 802可以请求eNodeB 808的公共密钥。

[0095] TAU或服务请求消息可以用于认证MME 810。在一个例子中,UE 802 可以请求对与MME 810交换的TAU或服务请求接受消息进行签名。在一些实例中,UE 802可以请求MME 810的公共密钥。

[0096] 图10是示出通过eNodeB 808用于服务网络804的请求式认证的RRC 消息1004的使用的第一例子的消息流程图1000。UE 802可以开始AKA过程1002。当成功完成AKA过程1002时,UE 802可以使用RRC消息1004 认证服务网络804。RRC连接请求(或连接建立请求)1010可以用作认证的一部分。在一个例子中,在从空闲模式转变期间,将RRC连接请求1010 发送到eNodeB 808。当UE 802进入空闲模式时,eNodeB 808可以由于省电原因丢弃UE 802的安全上下文。根据某些方面,UE 802可以发送包括额外字段的RRC连接请求1010。所述额外字段包括随机数,以及针对 eNodeB 808的签名的请求。在一些实例中,所述额外字段还可以包括针对 eNodeB 808的公共密钥的请求。随机数可以是任意的、随机的或伪随机的数,用于确保先前通信不会在重放攻击中被重新使用。eNodeB 808可以发送RRC连接建立响应1012,其使用私有密钥来签名,并且当验证eNodeB 808的真实性时,UE 802可以用信号通知RRC连接建立完成1014。

[0097] 图11是示出通过eNodeB 808用于服务网络804的请求式认证的RRC 消息1104的使用的第二例子的消息流程图1100。UE 802可以开始AKA过程1102。当成功完成AKA过程1102

时,UE 802可以使用RRC消息1104 来认证服务网络804。例如可以在连接故障恢复期间采用RRC连接重新建立请求1110。根据某些方面,UE 802可以发送包括额外字段的RRC连接重新建立请求1110。所述额外字段可以包括随机数,以及针对eNodeB 808 的签名的请求。在一些实例中,所述额外字段还可以包括针对eNodeB 808 的公共密钥的请求。eNodeB 808可以发送使用其私有密钥签名的连接重新建立响应1112,并且当验证eNodeB 808的真实性时,UE 802可以用信号通知RRC连接建立完成1114。通过图11的消息流程图1100的例子示出的过程可以防止引起断开连接以便在故障恢复过程期间拦截证书的攻击。

[0098] UE 802可以在需要时,如在要发送数据、接收数据时、或在切换到另一网络功能单元之前或之后,使用RRC消息来认证服务网络804。RRC连接、建立和/或重新建立请求由UE 802发起,并且这种请求要求来自eNodeB 808的响应。在一些实例中,UE 802可以确定没必要继续认证服务网络804。例如,当UE 802处于空闲状态和没有指示切换时,不需要执行认证。当按照请求提供签名时,可以最小化与基线协议相关联的开销。eNodeB 808通常仅在请求时提供网络功能单元证书。

[0099] 图12是示出通过MME 810用于服务网络的请求式认证的TAU消息 1204的第一例子的消息流程图1200。UE 802可以开始AKA过程1202。当成功完成AKA过程1202时,UE 802可以使用TAU消息来认证服务网络 804。可以例如在周期性登记期间或在切换之后采用TAU请求1210。根据某些方面,UE 802可以发送具有额外字段的TAU请求1210,所述额外字段包括随机数以及针对MME 810的签名的请求。在一些实例中,所述额外字段还包括针对MME 810的公共密钥的请求。MME 810可以发送使用其私有密钥签名的响应1212,并且在验证MME 810的真实性时,UE 802可以用信号通知RRC连接建立完成1214。

[0100] 图13、14和15是示出使用基于共享密钥的方法来阻止攻击的用于认证服务网络804的请求式过程的例子的消息流程图1300、1400、1500,在所述攻击中,攻击者可以损害和利用系统或协议漏洞来获取会话秘密,例如NAS密钥和AS密钥。诸如eNodeB 808和MME 810的网络功能单元可以配置有信任的执行环境,其可以用于维护网络功能单元的密钥导出密钥 (Key-Derivation-Keys)。攻击者通常不能获取存储于信任的执行环境中的密钥。在一个例子中,存储于MME 810的信任的执行环境中的密钥导出密钥是K_{ASME}密钥,而存储于eNodeB 808的信任的执行环境中的密钥导出密钥是K_{eNB}密钥。密钥导出密钥不直接用于加密和完整性保护,通常用于生成可用于加密和完整性保护的密钥。网络功能单元可以使用其各自的密钥导出密钥向服务网络804证明其是成员。不能访问存储于信任的执行环境中的密钥导出密钥的攻击者不能向服务网络804证明冒充的成员。

[0101] 使用共享密钥用于认证服务网络804的某些请求式过程可以利用由UE 802发起的消息。认证过程可以实现为请求式过程,以便限制基线协议开销和可能地消除空闲状态开销。

[0102] RRC消息可以用于认证eNodeB 808。这种RRC消息的例子包括RRC 连接请求以及RRC连接重新建立。UE 802可以请求对与eNodeB 808交换的连接消息进行签名。在一些实例中,当发送RRC连接建立消息时,eNodeB 808可能没有KeNB。因此,在安全模式控制过程之后将签名或消息认证码 (MAC)发送给UE 802。MAC码可以包括利用散列函数等产生的信息,其中MAC码可以认证和/或确保消息的完整性。

[0103] TAU消息可用于认证MME 810。在一个例子中,UE 802可以请求对与MME 810交换的

TAU接受消息进行签名。

[0104] 图13是示出通过eNodeB 808用于服务网络804的请求式认证的RRC 消息的第三例子的消息流程图1300。UE 802可以开始AKA过程1302。当成功完成AKA过程1302时，UE 802可以使用RRC消息1304来认证服务网络804。可以例如在从空闲模式转变期间采用RRC连接请求1310。根据某些方面，UE 802可以发送包括额外字段的RRC连接请求1310。所述额外字段可以包括随机数以及签名请求。eNodeB 808使用KeNB对其响应 1312进行签名，并且在验证eNodeB 808的真实性时，UE 802可以通过用信号通知RRC连接建立完成1314来确认完成过程。

[0105] 图14是示出通过eNodeB 808用于服务网络804的请求式认证的RRC 消息1404的第四例子的消息流程图1400。UE 802可以开始AKA过程1402，并且当成功完成AKA过程1402时，UE 802可以使用RRC消息1404来认证服务网络804。可以例如在连接故障恢复期间采用RRC连接重新建立请求1410。根据某些方面，UE 802可以发送包括额外字段的RRC连接重新建立请求1410。所述额外字段可以包括随机数以及签名请求。eNodeB 808 可以发送使用KeNB签名的响应1412，并且在验证eNodeB 808的真实性时， UE 802可以用信号通知RRC连接建立完成1414。

[0106] UE 802可以在需要时，如在要发送、接收数据时、或在切换到另一网络功能单元之前或之后，使用RRC消息来认证服务网络804。RRC连接建立、RRC连接和/或RRC重新建立请求由UE 802发起，并且这种请求要求来自eNodeB 808的响应。在一些实例中，UE 802可以确定没有必要继续认证服务网络804。例如，当UE 802处于空闲状态和没有指示切换时，不需要执行认证。当按照请求提供签名时，可以最小化与基线协议相关联的开销。eNodeB 808通常仅在请求时提供网络功能单元证书。

[0107] 图15是示出通过MME 810用于服务网络的请求式认证的TAU消息 1504的第二例子的消息流程图1500。UE 802可以开始AKA过程1502。当成功完成AKA过程1502时，UE 802可以使用TAU消息1504来认证服务网络804。可以例如在周期性登记期间或切换之后采用TAU请求1510。根据某些方面，UE 802可以发送具有额外字段的TAU请求1510，所述额外字段可以包括随机数以及签名请求。MME 810可以发送使用K_{ASME}密钥签名的响应1512，并且在验证MME 810的真实性时，UE 802可以用信号通知RRC连接建立完成1514。

[0108] 与物理可访问的网络功能单元相关的安全问题

[0109] 图16是示出在攻击者1602能物理访问提供服务网络804的某些网络功能单元(例如，eNodeB 808和/或MME 810)的网络设备时出现的服务网络804的某些漏洞的简化框图1600。在该形式的攻击下，攻击者1602可以获得对永久性证书的访问，其包括永久密钥1606、1608以及会话证书。例如，攻击者1602可以具有对永久密钥1606和/或1608的访问，例如，网络设备和/或网络功能单元(例如，eNodeB 808或MME 810)的私有密钥。私有密钥可以用于对消息进行签名。在该形式的攻击下，关于与UE 802的通信1604以及关于与HSS 806的通信1610，攻击者1602可以持续冒充服务网络804。

[0110] 可以物理访问网络设备的攻击者1602能够通过损害与网络功能单元相关联的网络设备而获取针对这些网络功能单元发布的所有证书。网络功能单元可以维护、提供或关联于证书，例如UE 802的认证向量和/或绑定到由网络运营商签名的证书的私有密钥。

[0111] 参考图17，当网络运营商利用公共密钥证书来配置网络功能单元(例如，eNode

1708和/或MME 1710)并采用证书观测站(CertOb)1714的服务时,可以增强网络的安全。CertOb 1714可以由不会被损害的信任第三方操作。CertOb 1714可以用于证明运营商发布的网络功能单元证书的完整性。可以使用证书观测站的标识符识别和/或访问CertOb 1714,所述证书观测站的标识符包括IP地址和/或通用资源定位符(URL)。可以使用基于公共密钥的认证过程来认证服务网络,其中验证网络功能单元(例如,eNodeB 1708 或MME 1710)的证书状态。

[0112] 证书服务器功能单元(CSF)1712管理网络功能单元证书,并基于请求将网络功能单元证书提供给UE 1702。CSF 1712将证书状态改变报告给 CertOb 1714。状态改变可以包括发布事件、取消事件等。CertOb 1714存储运营商的证书完整性信息,并将该信息提供给HSS 1706和UE 1702。可以将证书完整性信息提供作为服务网络1704的所有当前证书的散列。在一个例子中,所述散列可以被提供作为Merkel散列树,其提供对与对应于运营商网络的多个域相关联的证书的有效且安全的验证。

[0113] UE 1702可以初始通过比较由服务网络提供的证书完整性信息的第一副本与在UE 1702处从CertOb 1714接收到的证书完整性信息的第二副本来验证证书。如果证书完整性信息的第一和第二副本不匹配,则UE 1702可以请求CSF 1712提供服务网络1704的一个或多个证书,以便认证UE 1702 主动与其通信的网络功能单元。

[0114] 图18、19和20是示出使用基于用于认证服务网络1704的运营商签名的公共密钥的方法来用于认证服务网络1704的请求式过程的例子的消息流程图1800、1900、2000。服务网络1704可以被配置有由信任第三方(TTP) (例如,Verisign或互联网号码分配局(IANA))签名的证书。在一些实例中,服务网络1704可以采用自我签名的证书,其由归属网络在信任认证机构(CA)的列表中提供给UE 1702。信任CA列表可以包括运营商及其对应的公共密钥。CA列表和公共密钥或证书可以通过安全信道分发给漫游合作伙伴。

[0115] 图18是示出通过eNodeB 1708用于服务网络1704的请求式认证的 RRC消息1804的第五例子的消息流程图1800。UE 1702可以开始AKA过程1802。UE 1702可以在AKA过程1802期间或之后从HSS 1706接收服务网络1704的证书完整性信息。在成功完成AKA过程1802时,UE 1702可以使用RRC消息1804来认证服务网络1704。例如,可以在从空闲模式转变期间采用RRC连接请求1810。当UE 1702进入空闲模式时,eNodeB 1708 可以出于省电的原因丢弃UE 1702的安全上下文。根据某些方面,UE 1702 可以发送包括额外字段的RRC连接请求1810。所述额外字段可以包括随机数,以及针对eNodeB 1708的签名的请求。在一些实例中,所述额外字段还可以包括针对eNodeB 1708的公共密钥的请求。随机数可以是任意的、随机的或伪随机的数,用于确保先前通信不会在重放攻击中被重新使用。 eNodeB 1708可以发送用其私有密钥签名的响应1812,并且当验证eNodeB 1708的真实性时,UE 1702可以用信号通知RRC连接建立完成1814。

[0116] UE 1702可以从CertOb 1714获得1806服务网络1704的当前证书完整性信息。UE 1702然后可以验证当前证书完整性信息是否与由HSS 1706提供的当前证书完整性信息相同。如果服务网络的当前证书完整性信息不同于由HSS 1706在初始附接期间提供的当前证书完整性信息,则UE 1702通过例如查询1808CSF 1712来验证eNodeB 1708的网络功能单元证书。

[0117] 图19是示出通过eNodeB 1708用于服务网络1704的请求式认证的 RRC消息1904的

第六例子的消息流程图1900。UE 1702可以开始AKA过程1902。UE 1702可以在AKA过程1802期间或之后从HSS 1706接收服务网络1704的证书完整性信息。在成功完成AKA过程1902时，UE 1702可以使用RRC消息1904来认证服务网络1704。例如，可以在连接故障恢复期间采用RRC连接重新建立请求1910。根据某些方面，UE 1702可以发送包括额外字段的RRC连接重新建立请求1910。所述额外字段可以包括随机数，以及针对eNodeB 1708的签名的请求。在一些实例中，所述额外字段还可以包括针对eNodeB 1708的公共密钥的请求。eNodeB 1708可以发送用其私有密钥签名的响应1912，并且当验证eNodeB 1708的真实性时，UE 1702可以用信号通知RRC连接建立完成1914。

[0118] UE 1702可以从CertOb 1714获得1906服务网络1704的当前证书完整性信息。UE 1702然后可以验证当前证书完整性信息是否与由HSS 1706提供的当前证书完整性信息相同。如果服务网络的当前证书完整性信息不同于由HSS 1706在初始附接期间提供的当前证书完整性信息，则UE 1702通过例如查询1908CSF 1712来验证eNodeB 1708的网络功能单元证书。

[0119] UE 1702可以在需要时，如在要发送、接收数据时、或在切换到另一网络功能单元之前或之后，使用RRC消息来认证服务网络1704。RRC连接/ 重新建立请求由UE 1702发起，并且这种请求要求来自eNodeB 1708的响应。在一些实例中，UE 1702可以确定没有必要继续认证服务网络1704。例如，当UE 1702处于空闲状态和没有指示切换时，不需要执行认证。当按照请求提供签名时，可以最小化与基线协议相关联的开销。eNodeB 1708 通常仅在请求时提供网络功能单元证书。

[0120] 图20是示出通过MME 1710用于服务网络的请求式认证的TAU消息 2004的第三例子的消息流程图2000。UE 1702可以开始AKA过程2002。UE 1702可以在AKA过程2002期间或之后从HSS 1706接收服务网络1704 的证书完整性信息。在成功完成AKA过程2002时，UE 1702可以使用TAU 消息来认证服务网络1704。例如，可以在周期性登记期间或在切换之后采用TAU请求1210。根据某些方面，UE 1702可以发送具有额外字段的TAU 请求2010，所述额外字段可以包括随机数，以及针对MME 1710的签名的请求。在一些实例中，所述额外字段还可以包括针对MME 1710的公共密钥的请求。MME 1710可以发送用其私有密钥签名的响应2012，并且当验证MME 1710的真实性时，UE 1702可以用信号通知RRC连接建立完成 2014。

[0121] UE 1702可以从CertOb 1714获得2006服务网络1704的当前证书完整性信息。UE 1702然后可以验证当前证书完整性信息是否与由HSS 1706提供的当前证书完整性信息相同。如果服务网络的当前证书完整性信息不同于由HSS 1706在初始附接期间提供的当前证书完整性信息，则UE 1702通过例如查询2008CSF 1712来验证MME 1710的网络功能单元证书。

[0122] 某些方面的额外描述

[0123] 图21是示出采用可以被配置为执行本文公开的一个或多个功能的处理电路2102的装置的硬件实现方式的简化例子的概念图2100。根据本公开内容的各种方面，可以使用处理电路2102实现本文公开的元件、元件的任意部分或元件的任意组合。处理电路2102可以包括一个或多个处理器2104，其被硬件和软件模块的一些组合控制。处理器2104的例子包括微处理器、微控制器、数字信号处理器(DSP)、现场可编程门阵列(FPGA)、可编程逻辑设备(PLD)、状态机、定序器、门控逻辑、离散硬件电路、以及被配置为执行遍及本公开内容描

述的各种功能的其它适当的硬件。一个或多个处理器2104可以包括执行特定功能的专用处理器，并且其被软件模块2116 之一进行配置、增强或控制。可以通过组合在初始化期间加载的软件模块 2116来配置一个或多个处理器2104，还可以通过在操作期间加载或卸载一个或多个软件模块2116进行配置。

[0124] 在示出的例子中，处理电路2102可以实现有总线架构，其一般由总线 2110表示。取决于处理电路2102的特定应用和整体设计约束，总线2110 可以包括任意数量的互连总线和桥。总线2110将各种电路链接到一起，包括一个或多个处理器2104以及存储设备2106。存储设备2106可以包括存储器设备和大容量存储设备，并在此可以称作计算机可读介质和/或处理器可读介质。总线2110还可以链接各种其它电路，例如定时源、定时器、外围部件、电压调节器以及功率管理电路。总线接口2108可以提供在总线2110 和一个或多个收发机2112之间的接口。收发机2112可以被设置用于由处理电路支持的每种网络技术。在一些实例中，多个网络技术可以共享在收发机2112中发现的一些或所有电路或处理模块。每个收发机2112提供用于通过传输介质与各种其它装置进行通信的单元。取决于装置的本质，还可以提供用户接口2118(例如，键区、显示器、扬声器、麦克风、操纵杆)，并且其可以通信地直接地或通过总线接口2108耦合到总线2110。

[0125] 处理器2104可以负责管理总线2110并负责一般处理，所述处理包括执行存储于计算机可读介质(包括存储设备2106)中的软件。在该方面，处理电路2102(包括处理器2104)可以用于实现本文公开的任意方法、功能和技术。存储设备2106可以用于存储在执行软件时被处理器2104操纵的数据，并且软件可以被配置为实现本文公开的任一种方法。

[0126] 在处理电路2102中的一个或多个处理器2104可以执行软件。软件可以以计算机可读形式驻留在存储设备2106内或在外部计算机可读介质内。外部计算机可读介质和/或存储设备2106可以包括非瞬态计算机可读介质。例如，非瞬态计算机可读介质包括磁存储设备(例如，硬盘、软盘、磁条)、光盘(例如，CD或DVD)、智能卡、闪存设备(例如，“闪速驱动”、卡、棒、或键驱动)、RAM、ROM、PROM、EPROM、EEPROM、寄存器、可移除盘、以及用于存储可以被计算机访问和读取的软件和/或指令的任意其它适当的介质。计算机可读介质和/或存储设备2106还例如可以包括载波、传输线、以及用于发送被计算机访问和读取的软件和/或指令的任意其它适当介质。计算机可读介质和/或存储设备2106可以驻留在处理电路2102中、在处理器2104中、在处理电路2102外部、或跨包括处理电路2102的多个实体分布。计算机可读介质和/或存储设备2106可以实现在计算机程序产品中。举例而言，计算机程序产品可以包括封装材料中的计算机可读介质。本领域的技术人员可以认识到取决于特定应用和施加到整体系统上的整体设计约束如何最佳地实现遍及本公开内容呈现的所描述功能。

[0127] 存储设备2106可以维护在可加载代码段、模块、应用、程序等中维护和/或组织的软件，其在本文中可以称作软件模块2116。每个软件模块2116 可以包括指令和数据，当被安装或加载到处理电路2102上并被一个或多个处理器2104执行时，所述指令和数据贡献于控制一个或多个处理器2104 的操作的运行时图像2114。当被执行时，某些指令可以使得处理电路2102 根据本文描述的某些方法、算法和过程来执行功能。

[0128] 一些软件模块2116可以在初始化处理电路2102期间加载，并且这些软件模块2116可以配置处理电路2102以使得能够执行本文公开的各种功能。例如，一些软件模块2116可以配置处理器2104的内部设备和/或逻辑电路2122，并且可以管理对外部设备(例如，收发

机2112、总线接口2108、用户接口2118、定时器、算数协处理器等)的访问。软件模块2116可以包括与中断处理器和设备驱动器交互的控制程序和/或操作系统,并且控制程序和/或操作系统访问由处理电路2102提供的各种资源。所述资源可以包括存储器、处理时间、对收发机2112的访问、用户接口2118等。

[0129] 处理电路2102的一个或多个处理器2104可以是多功能的,由此一些软件模块2116被加载和配置为执行不同功能或相同功能的不同实例。一个或多个处理器2104可以额外地适应于管理响应于例如来自用户接口2118、收发机2112和设备驱动器的输入而开始的背景任务。为了支持执行多个功能,一个或多个处理器2104可以被配置为提供多任务环境,由此多个功能中的每个被实现为由一个或多个处理器2104按照需要或期望来服务的一组任务。在一个例子中,可以使用在不同任务之间传递对处理器2104的控制的时间共享程序2120来实现多任务环境,由此在完成任意未决操作时和/ 或响应于诸如中断的输入,每个任务将一个或多个处理器2104的控制返回到时间共享程序2120。当任务控制一个或多个处理器2104时,出于由与控制任务相关联的功能解决的目的而有效专门化处理电路。时间共享程序 2120可以包括操作系统,以循环为基础转移控制的主循环,根据功能的优先化来分配一个或多个处理器2104的控制的功能,和/或通过将一个或多个处理器2104的控制提供给处理功能单元以对外部事件进行响应的中断驱动主循环。

[0130] 后续流程图示出了在根据本文公开的某些方面适应或配置的网络元件上执行或操作的方法和过程的流程图。所述方法和过程可以实现于任意适当的网络技术中,包括3G、4G和5G技术等。因此,权利要求不被限制于单个网络技术。在该方面,提及“UE”可以理解为还指代移动站、用户站、移动单元、用户单元、无线单元、远程单元、移动设备、无线设备、无线通信设备、远程设备、移动用户站、接入终端、移动终端、无线终端、远程终端、手持设备、用户代理、移动客户端、客户端、或一些其它适当的术语。提及“eNodeB”可以理解为指代基站、基站收发机、无线基站、无线收发机、收发机功能单元、基本服务集、扩展服务集、或一些其它适当的术语。提及MME还可以指代用作服务网络中的认证器的实体和/或主要服务输送节点(例如,移动交换中心)。提及HSS还可以指代包含用户相关和订户相关信息的数据库,提供在移动管理中的支持功能、调用和会话建立、和/或用户认证和接入授权,例如包括归属位置寄存器(HLR)、认证中心(AuC)和/或认证、授权和计费(AAA)服务器。

[0131] 图22是保护在UE和服务网络之间的无线通信的方法的流程图2200。

[0132] 在框2202处,UE可以在UE和服务网络之间已经建立了安全关联之后向服务网络中的网络功能单元发送连接请求或跟踪区域请求。所述请求可以包括随机数和签名请求。发送到服务网络的请求可以在UE从空闲模式转变时或在这种从空闲模式的转变之后发送。在一些实例中,发送到服务网络的请求可以是RRC消息。RRC消息可以是RRC连接请求、RRC连接重新建立请求、和/或RRC重新配置完成消息。在一些实例中,发送到服务网络的请求可以是TAU请求。

[0133] 在框2204处,UE可以接收对来自网络功能单元的连接请求或跟踪区域请求的响应。所述响应可以包括网络功能单元的签名。

[0134] 在框2206处,UE可以基于网络功能单元的签名和对应于网络功能单元的公共密钥证书来认证服务网络。可以使用由与服务网络相关联的网络运营商提供的服务网络的私有密钥对公共密钥证书签名。UE可以维护标识与信任网络相对应的公共密钥或公共密钥证书

的信任网络的列表。UE可以通过使用信任网络的列表来验证网络功能单元的公共密钥和由网络功能单元生成的签名，而认证服务网络。可以使用信任的第三方来验证与网络功能单元相对应的公共密钥证书，而认证服务网络。

[0135] 在一些例子中，可以将证书完整性信息请求发送到网络，并且利用从归属用户服务器接收到的第二证书完整性信息来验证在来自网络的响应中接收到的第一证书完整性信息。证书完整性信息请求可以包括对应于第二证书完整性信息的证书观测站(例如，图17的CertOb 1714)的标识符。CertOb 1714可以被配置为维护网络的一组证书的完整性。CertOb 1714的标识符可以是IP地址或URL。可以通过利用CertOb 1714的公共密钥认证对证书完整性信息请求的响应来验证第一证书完整性信息。在一些实例中，可以通过比较第一证书完整性信息和第二证书完整性信息，在确定出第一证书完整性信息和第二证书完整性信息之间不同时发送证书状态请求到 CSF 1712，以及基于来自CSF 1712的响应来验证网络功能单元证书的状态，来验证第一证书完整性信息。证书状态请求可以包括标识网络功能单元的第一标识信息，标识网络功能单元证书的第二标识信息，以及网络功能单元证书的版本号。来自CSF 1712的响应可以包括证书状态响应，其包括网络功能单元证书的状态、网络的公共密钥、以及利用网络的私有密钥由CSF 1712创建的证书状态响应的签名。可以使用网络的公共密钥来执行证书状态响应的验证。

[0136] 图23是示出了采用处理电路2302的装置2300的硬件实现方式的简化例子的图。处理电路通常具有处理器2316，其可以包括微处理器、微控制器、数字信号处理器、定序器和状态机中的一个或多个。处理电路2302可以实现有总线架构，其一般由总线2320表示。取决于处理电路2302的特定应用和整体设计约束，总线2320可以包括任意数量的互连总线和桥。总线2320将各种电路链接到一起，包括一个或多个处理器和/或硬件模块，其由处理器2316、模块或电路2304、2306和2308、适于通过天线2314通信的无线收发机2312和计算机可读存储介质2318表示。总线2320还可以链接各种其它电路，例如定时源、外围部件、电压调节器以及功率管理电路，其在本领域中都是已知的，并因此不再进行描述。

[0137] 处理器2316负责一般处理，包括执行存储于计算机可读存储介质2318 上的软件。当被处理器2316执行时，所述软件使得处理电路2302执行上文针对任意特定装置描述的各种功能。计算机可读存储介质2318还用于存储由处理器2316在执行软件时操纵的数据，包括从通过天线2314发送的符号中解码的数据，其可以被配置作为数据通道和时钟通道。处理电路2302 还包括模块2304、2306和2308中的至少一个。模块2304、2306和2308 可以是在处理器2316中运行的、驻留/存储于计算机可读存储介质2318中的软件模块，与处理器2316耦合的一个或多个硬件模块、或其一些组合。模块2304、2306和/或2308可以包括微控制器指令、状态机配置参数、或其一些组合。

[0138] 在一个配置中，用于无线通信的装置2300包括：被配置为认证和/或保护与归属网络的连接的模块和/或电路2304，被配置为认证服务网络的模块和/或电路2306，以及被配置为向服务网络发送消息和接收消息的模块和/ 或电路2308。

[0139] 在一个例子中，无线收发机2312可以被配置为将消息发送到服务网络中的无线基站，并从无线基站接收消息。模块和/或电路2304可以包括用于在装置和归属网络之间建立安全连接的单元。可以响应于通过无线收发机发送到HSS的第一认证消息来建立经认证的连接。在建立安全连接之后并且在将第二认证请求发送到归属网络的HSS之前，模块和/或

电路2308、2312可以包括用于将请求发送到服务网络中的网络功能单元并且从网络功能单元接收针对请求的响应的单元，所述请求具有随机数和附加到其上的签名请求，其中所述响应包括网络功能单元的签名。模块和/或电路2306 可以包括用于基于网络功能单元的签名和对应于网络功能单元且由网络运营商签名的公共密钥证书来认证服务网络的单元。对应于网络功能单元的公共密钥证书可以包含于信任网络的列表中，并且其各个公共密钥证书由装置维护。

[0140] 模块和/或电路2308、2312可以包括用于将证书完整性信息请求发送到网络的单元，以及模块和/或电路2306可以包括用于使用从HSS接收到的第二证书完整性信息验证从网络接收到的第一证书完整性信息的单元。证书完整性信息请求包括对应于第二证书完整性信息的CertOb 1714的标识符。CertOb 1714可以被配置为维护网络的一组证书的完整性。

[0141] 模块和/或电路2306可以被配置为比较第一证书完整性信息和第二证书完整性信息，使得模块和/或电路2308、2312在确定出第一证书完整性信息和第二证书完整性信息之间存在不同时将证书状态请求发送到CSF 1712，并基于来自CSF 1712的响应来验证网络功能单元证书的状态。证书状态请求可以包括网络功能单元的标识符、网络功能单元证书的标识符、以及网络功能单元证书的版本号。

[0142] 图24是证明服务网络的成员资格的方法的流程图2400。该方法可以由服务网络的网络节点(或网络功能单元)执行。

[0143] 在框2202处，在UE已经建立了与归属网络的安全连接之后，网络节点可以从UE接收第一消息。所述消息可以被引导至服务网络的网络功能单元。所述消息可以包括随机数和签名请求。

[0144] 在框2204处，网络节点可以利用由服务网络的网络功能单元维护的运营商签名的证书来生成签名。运营商签名的证书可以是由服务网络的运营商签名的公共密钥证书。可以在安全存储设备或安全执行环境中和/或在信任环境中维护对应于运营商签名的证书的私有密钥。

[0145] 在框2206处，网络节点可以将第二消息发送给UE。签名可以附加到第二消息。

[0146] 在一些例子中，签名包括利用在UE和网络功能单元之间共享的会话密钥创建的MAC。对称密码可以用于对第二消息响应签名。

[0147] 在一些实例中，网络节点可以是MME，会话密钥可以是K_{ASME}。MME 可以从HSS在利用MME的公共密钥加密的消息中接收K_{ASME}，利用存储于信任环境中的私有密钥对K_{ASME}解密，并将解密后的K_{ASME}存储于信任环境中。可以在TAU请求中接收认证请求。

[0148] 在一些实例中，网络节点可以是eNodeB，会话密钥可以是KeNB。eNodeB可以从MME在利用eNodeB的公共密钥加密的消息中接收KeNB，利用存储于信任环境中的私有密钥对KeNB解密，并将解密后的KeNB存储于信任环境中。第一消息可以是无线资源控制(RRC)消息，而第二消息可以是对RRC消息的响应。例如，RRC消息可以是RRC连接建立请求、RRC连接重新建立请求或者RRC重新配置完成消息。

[0149] 在一些例子中，签名包括利用网络节点的私有密钥创建的数字签名。非对称密码可以用于对认证响应签名。网络节点的私有密钥可以存储于信任环境中，并且在信任环境中创建签名。

[0150] 图25是示出采用处理电路2502的装置2500的硬件实现方式的简化例子的图。处理电路通常具有处理器2516，其可以包括微处理器、微控制器、数字信号处理器、定序器和状态机中的一个或多个。处理电路2502可以实现有总线架构，其一般由总线2520表示。取决于处理电路2502的特定应用和整体设计约束，总线2520可以包括任意数量的互连总线和桥。总线2520 将各种电路链接到一起，包括一个或多个处理器和/或硬件模块，其由处理器2516、模块或电路2504、2506和2508、被配置为通过天线2514通信的无线收发机2512和计算机可读存储介质2518表示。总线2520还可以链接各种其它电路，例如定时源、外围部件、电压调节器以及功率管理电路，其在本领域中都是已知的，并因此不再进行描述。

[0151] 处理器2516负责一般处理，包括执行存储于计算机可读存储介质2518 上的软件。当被处理器2516执行时，所述软件使得处理电路2502执行上文针对任意特定装置描述的各种功能。计算机可读存储介质2518还用于存储由处理器2516在执行软件时操纵的数据，包括从通过天线2514发送的符号中解码的数据，其可以被配置为数据通道和时钟通道。处理电路2502 还包括模块2504、2506和2508中的至少一个。模块2504、2506和2508 可以是在处理器2516中运行的、驻留/存储于计算机可读存储介质2518中的软件模块，与处理器2516耦合的一个或多个硬件模块、或其一些组合。模块2504、2506和/或2508可以包括微控制器指令、状态机配置参数、或其一些组合。

[0152] 在一个配置中，用于无线通信的装置2500包括：被配置为生成认证签名的模块和/或电路2504，被配置为将消息发送到UE的模块和/或电路2506，以及被配置为从UE接收消息的模块和/或电路2508。

[0153] 在一个例子中，模块和/或电路2508可以提供用于在UE已经建立了与归属网络的安全连接之后从UE接收第一消息的单元。所述消息可以被引导至服务网络的网络功能单元，并包括随机数和签名请求，模块和/或电路 2504可以提供用于利用由服务网络的网络功能单元维护的运营商签名的证书来生成签名的单元，以及模块和/或电路2506可以提供用于发送第二消息到UE的单元，其中签名可以附加到第二消息。附加到第二消息的签名可以被生成以向UE证明装置2500是任务网络的成员。运营商签名的证书可以是由服务网络的运营商签名的公共密钥证书。

[0154] 在一些例子中，网络节点是eNodeB，第一消息是RRC消息，以及第二消息是对RRC消息的响应。

[0155] 在一些例子中，网络节点是MME，以及认证请求是在TAU请求中接收到的。

[0156] 可以理解的是，所公开的过程的步骤的特定次序或层级是示例性方法的图示。基于设计偏好，可以理解，可以重新安排过程中步骤的特定次序或层级。此外，可以组合或省略一些步骤。随附方法权利要求以样本次序呈现各种步骤的元素，并且并不表示限制于所呈现的特定次序或层级。

[0157] 提供了先前的描述以使得本领域任意技术人员可以实践本文描述的各个方面。本领域技术人员可以容易地理解对这些方面的各种修改，并且在本文中定义的通用原理可以应用于其它方面。因此，权利要求并不意图限制于本文所示的方面，而是被给予与语言权利要求一致的完全范围，其中提及单数形式的元件并不意图表示“一个且仅一个”(除非明确如此陈述)，否则是指“一个或多个”。除非另有明确陈述，否则术语“一些”指代一个或多个。本领域技术人员已知的或以后将知的贯穿该公开内容描述的各种方面的元件的所有结构

和功能等价可以通过引用被明确并入本文，并且意图被权利要求所涵盖。此外，本文中公开的任何事物都不意图致力于公众，而不管这种公开是否被明确记叙在权利要求中。没有权利要求被解释为单元加功能，除非明确利用短语“用于…的单元”来记叙要素。

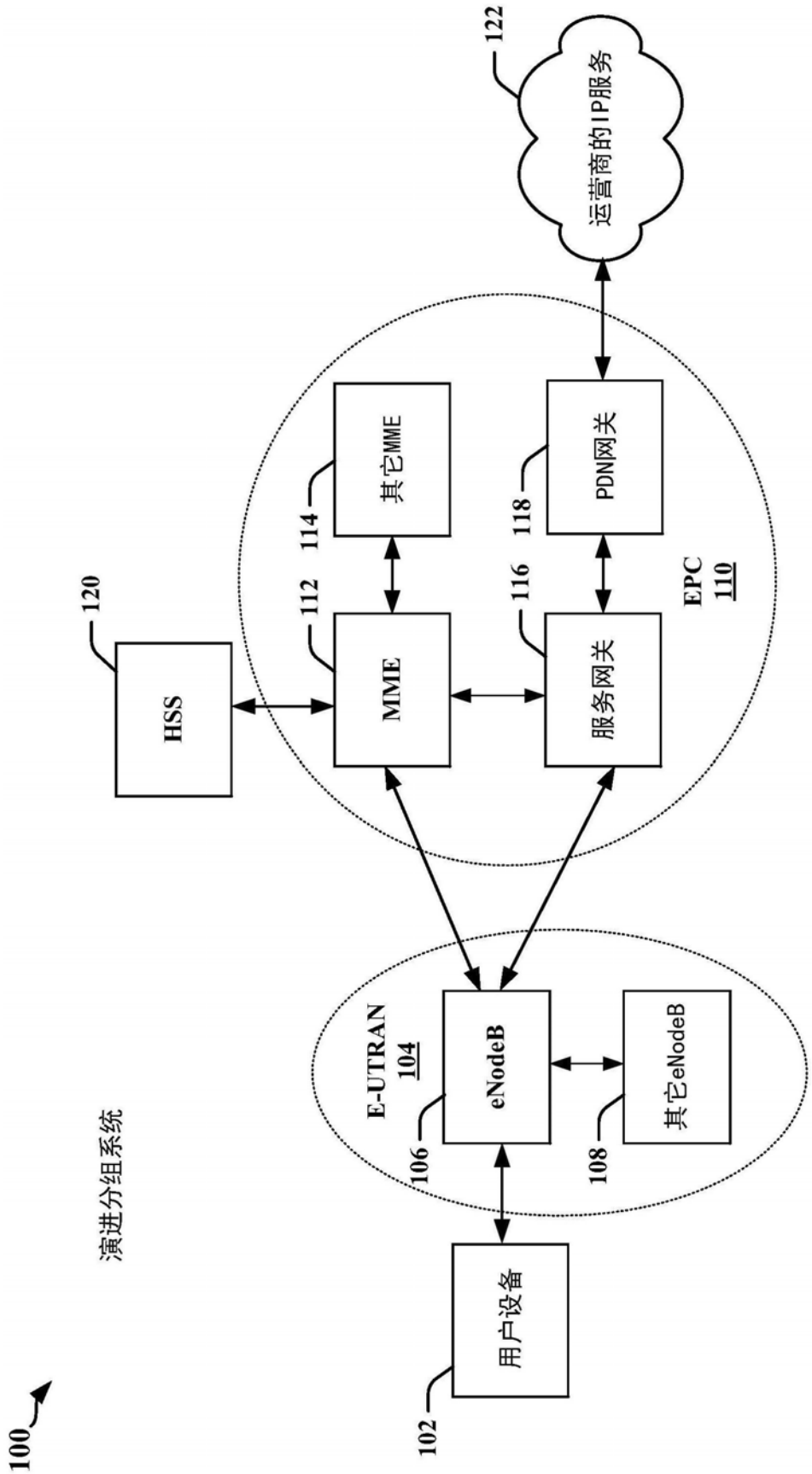

100
演进分组系统
用户设备
102
E-UTRAN
104
eNodeB
106
其它eNodeB
108
HSS
120
MME
112
服务网关
116
其它MME
114
PDN网关
118
EPC
110
运营商的IP服务
122

图1

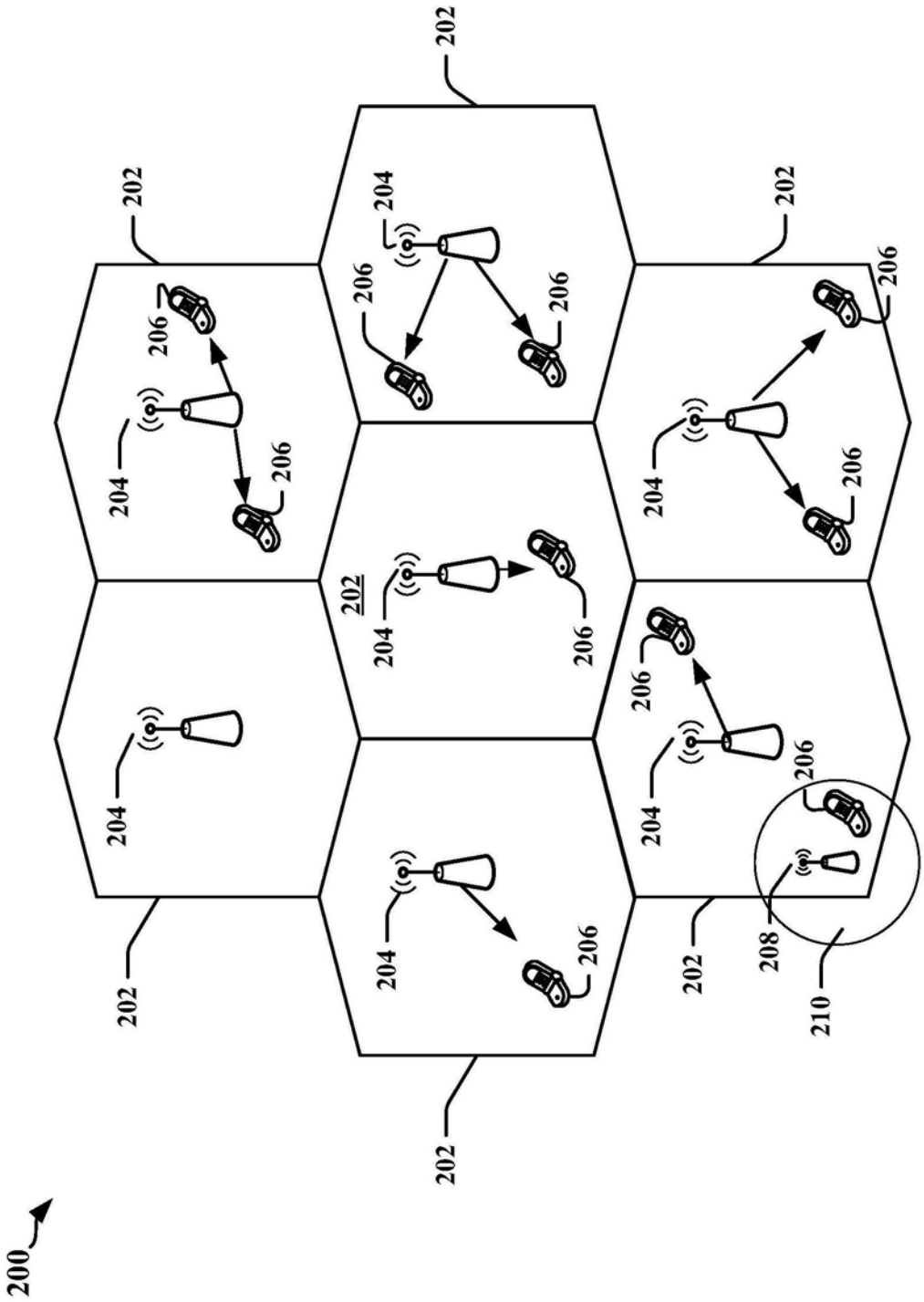


图2

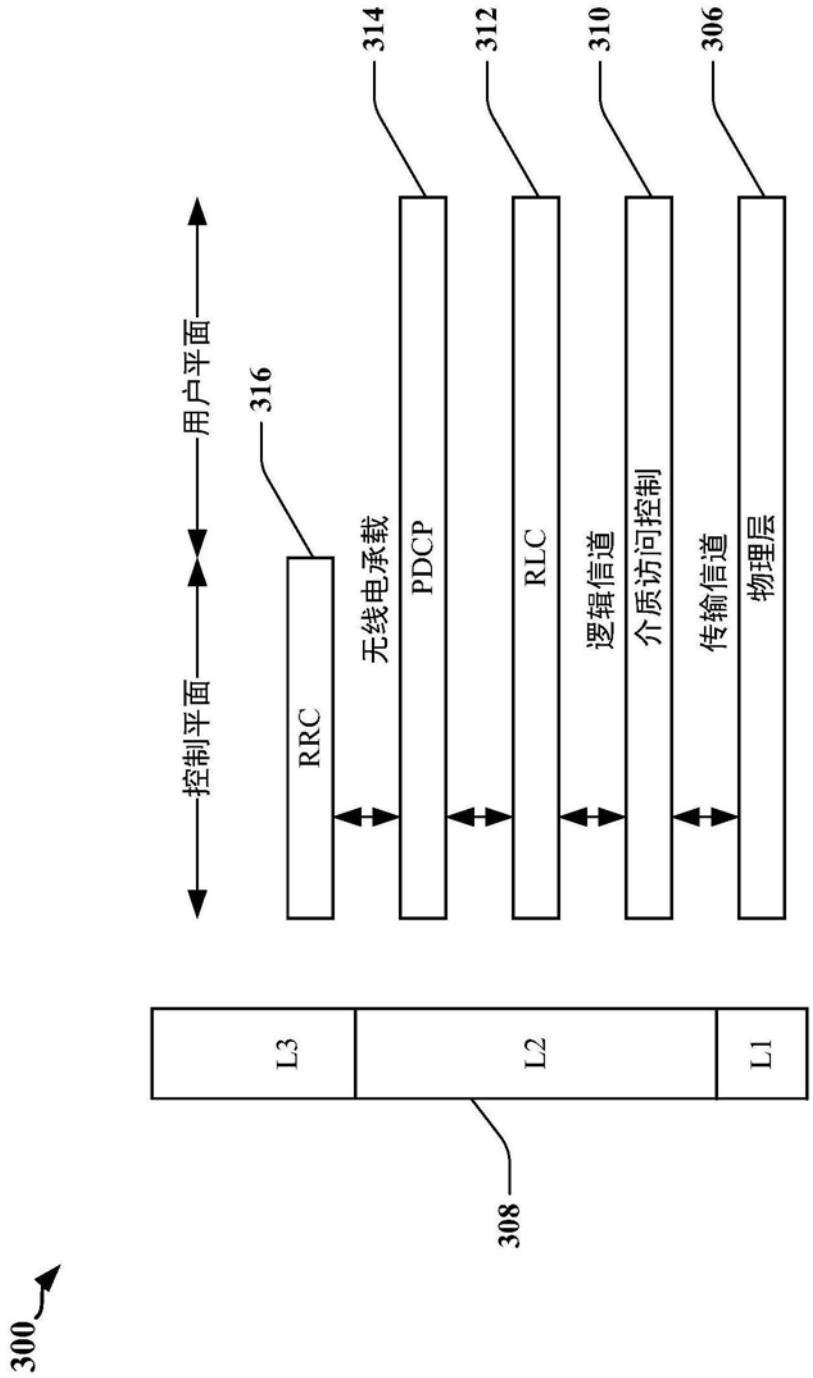

300
308
L3
L2
L1
316
RRC
无线电承载
PDCP
314
RLC
312
逻辑信道
介质访问控制
310
传输信道
物理层
306
控制平面
用户平面

图3

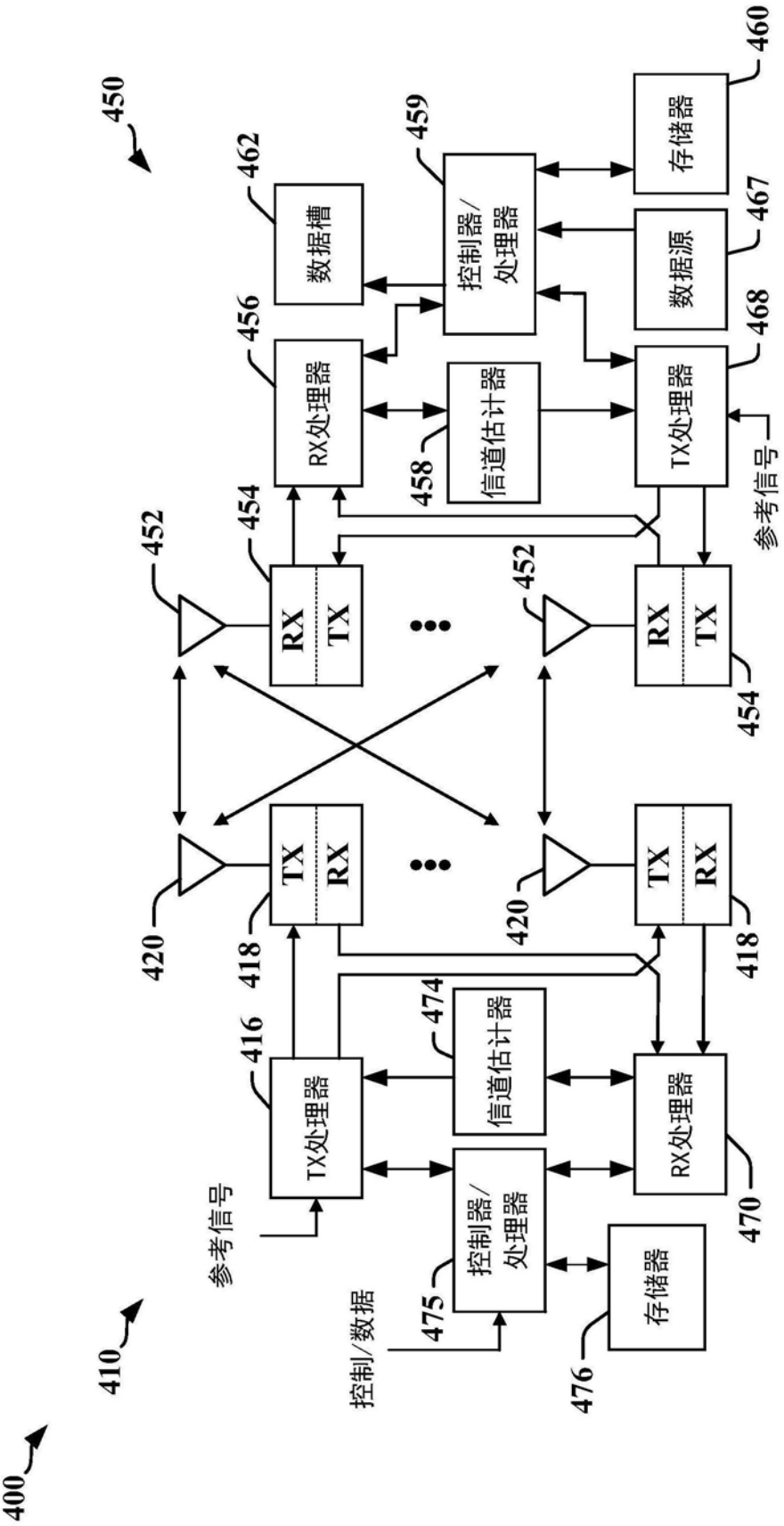

400
410
450
420
418
452
454
456
458
459
460
462
467
468
470
474
475
476
TX处理器
RX处理器
信道估计器
控制器/处理器
存储器
数据槽
数据源
参考信号
控制/数据
RX
TX

图4

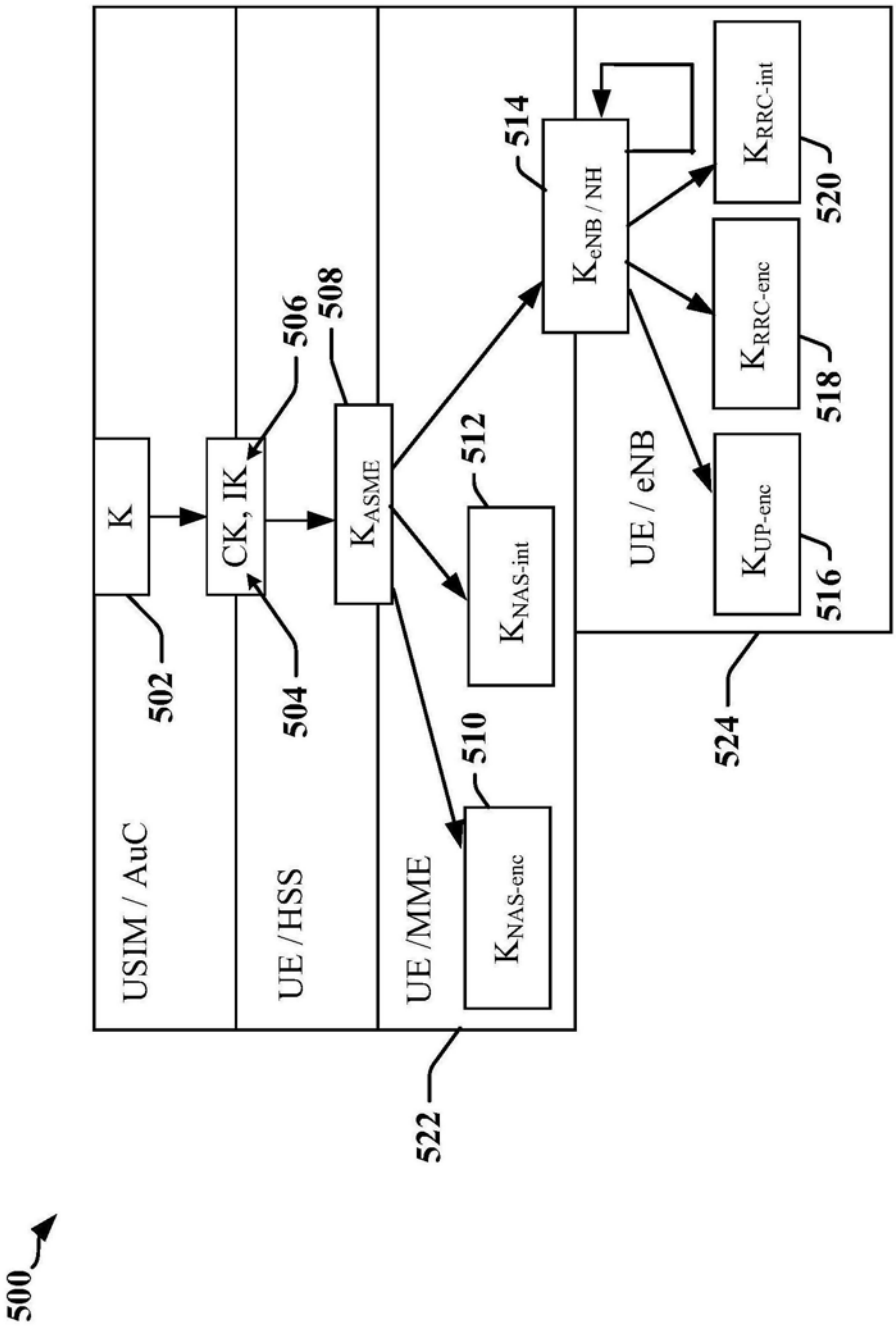

USIM / AuC
UE /HSS
UE /MME
UE / eNB
K
CK, IK
K_ASME
K_NAS-int
K_NAS-enc
K_eNB / NH
K_RRC-int
K_RRC-enc
K_UP-enc
500
502
504
506
508
510
512
514
516
518
520
522
524

图5

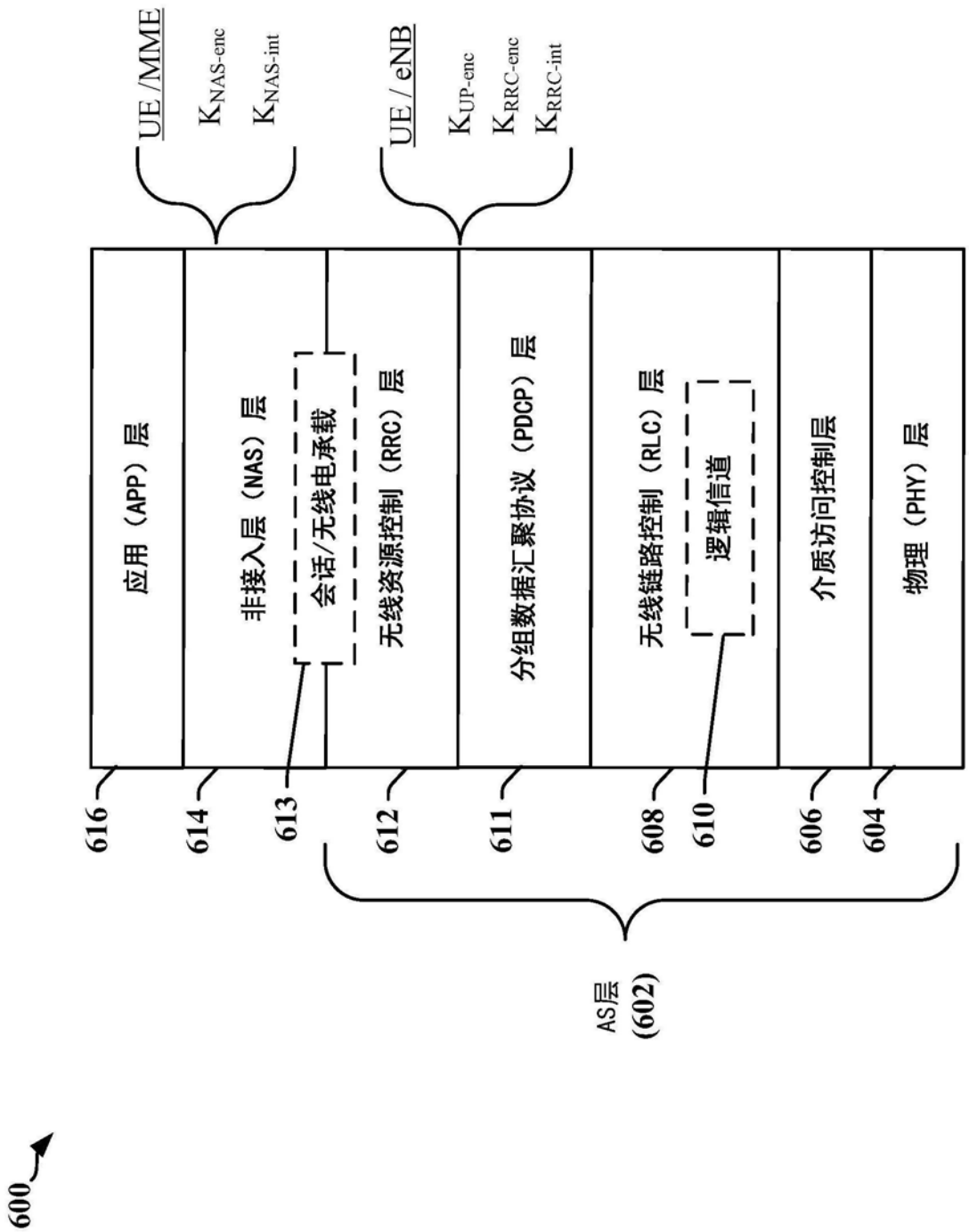

UE /MME
$K_{NAS-enc}$
$K_{NAS-int}$
UE / eNB
K_{UP-enc}
$K_{RRC-enc}$
$K_{RRC-int}$
应用（APP）层
非接入层（NAS）层
会话/无线电承载
无线资源控制（RRC）层
分组数据汇聚协议（PDCP）层
无线链路控制（RLC）层
逻辑信道
介质访问控制层
物理（PHY）层
616
614
613
612
611
608
610
606
604
AS层
(602)
600

图6

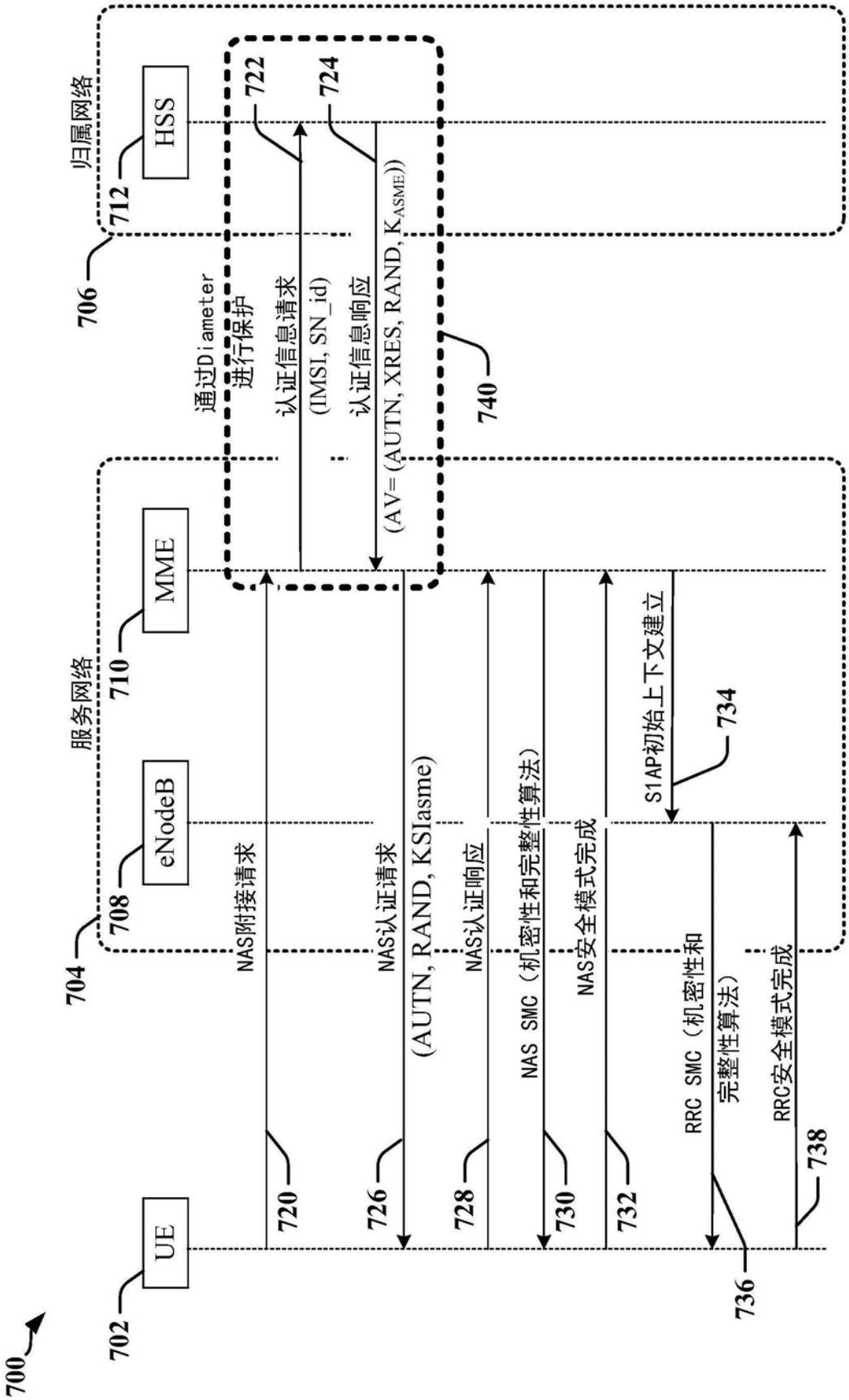

700
702
UE
704
服务网络
708
eNodeB
710
MME
706
归属网络
712
HSS
720
NAS附接请求
722
通过Diameter进行保护
724
认证信息请求
(IMSI, SN_id)
认证信息响应
(AV= (AUTN, XRES, RAND, KASME))
740
726
NAS认证请求
(AUTN, RAND, KSIasme)
728
NAS认证响应
730
NAS SMC（机密性和完整性算法）
732
NAS安全模式完成
734
S1AP初始上下文建立
736
RRC SMC（机密性和完整性算法）
738
RRC安全模式完成

图7

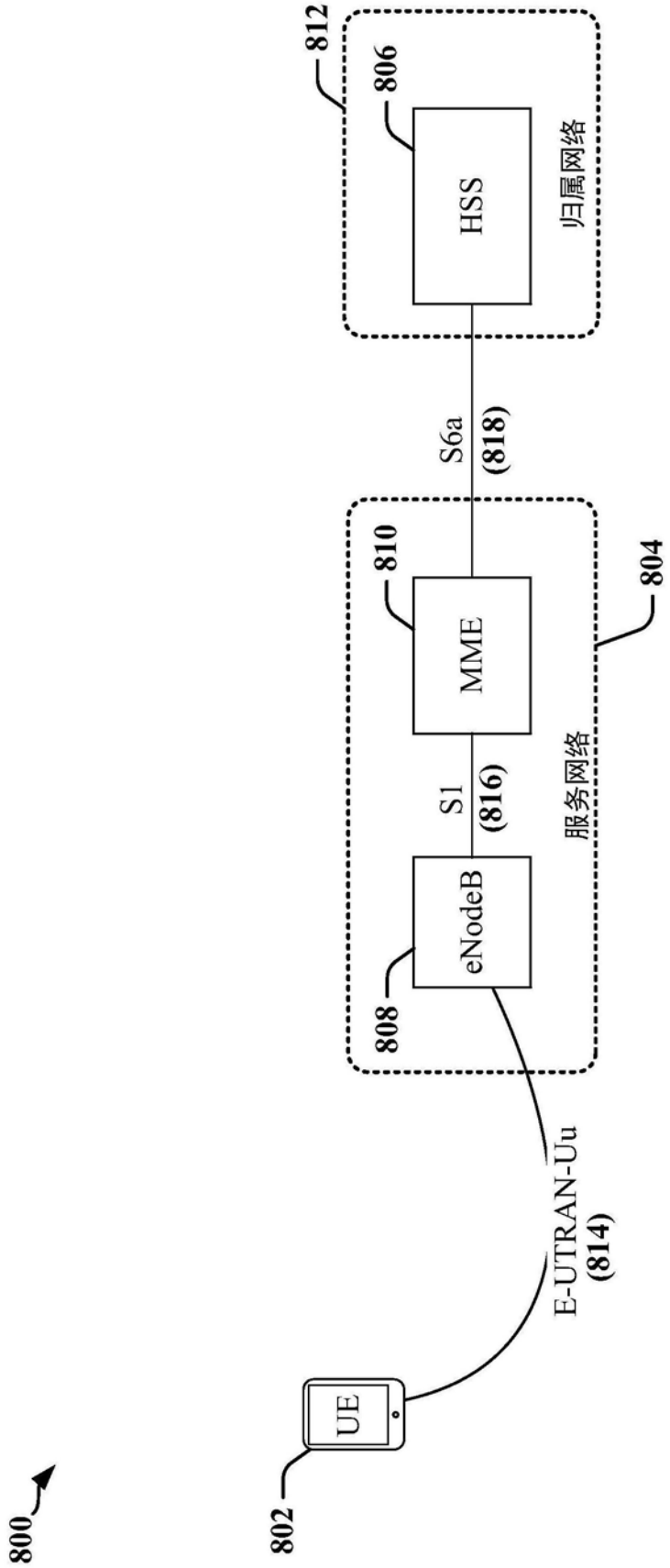

800
802
UE
E-UTRAN-Uu
(814)
808
eNodeB
S1
(816)
810
MME
804
服务网络
S6a
(818)
812
806
HSS
归属网络

图8

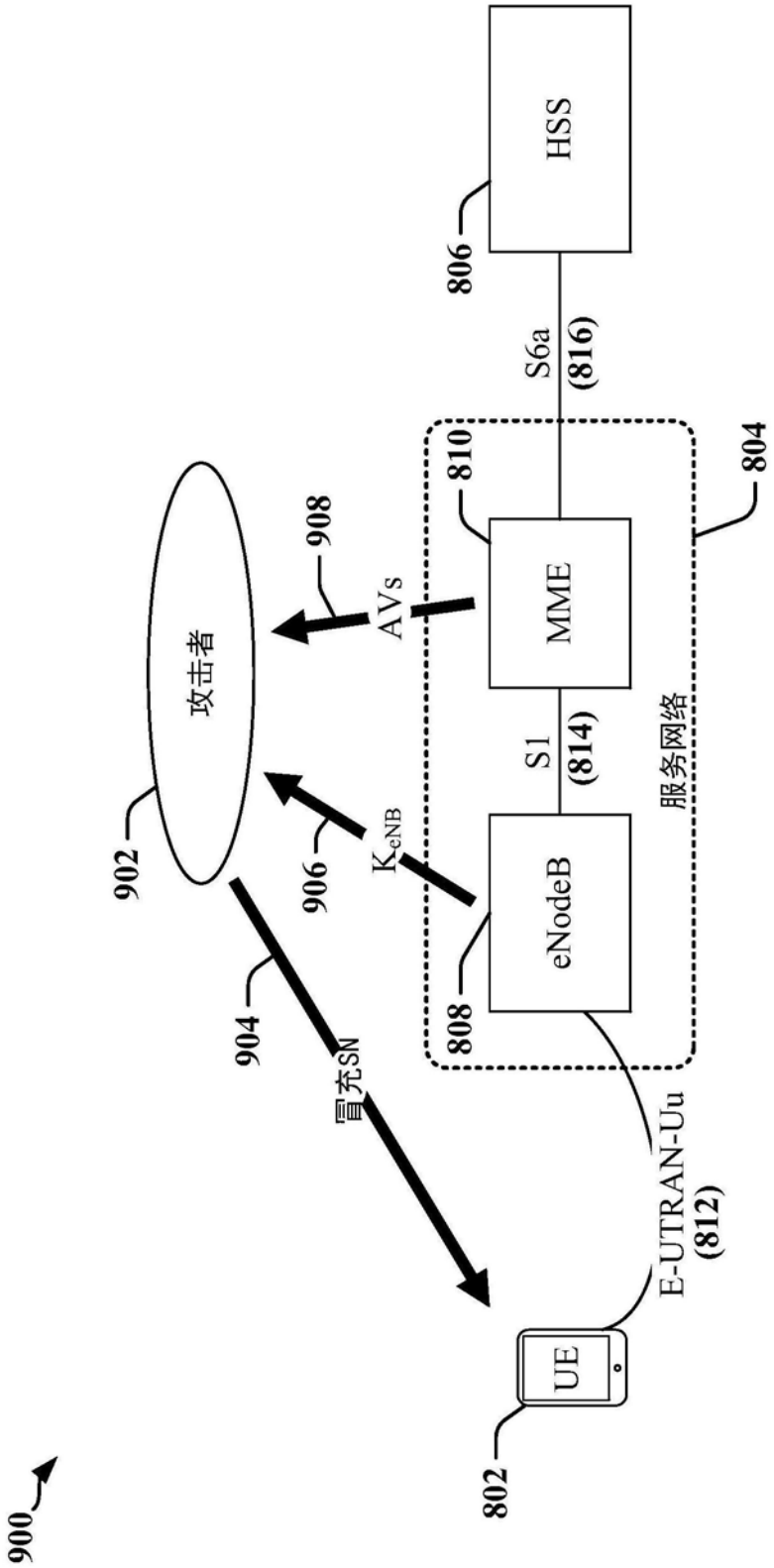

900
802
UE
808
eNodeB
804
服务网络
E-UTRAN-Uu
(812)
S1
(814)
MME
810
S6a
(816)
HSS
806
902
攻击者
904
冒充SN
906
K_{eNB}
908
AVs

图9

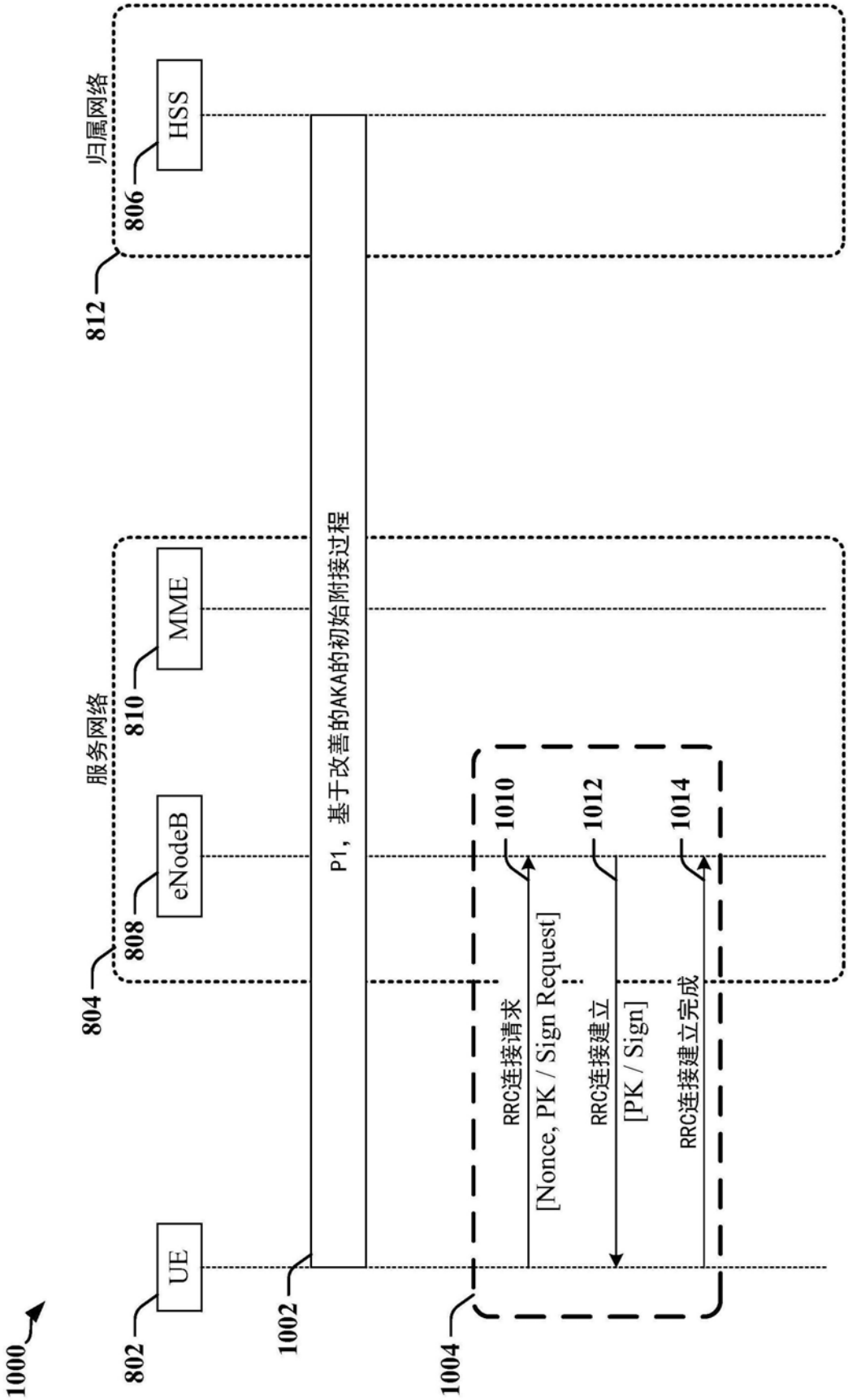

1000
802
UE
804
服务网络
808
eNodeB
810
MME
812
归属网络
806
HSS
1002
P1，基于改善的AKA的初始附接过程
1004
1010
RRC连接请求
[Nonce, PK / Sign Request]
1012
RRC连接建立
[PK / Sign]
1014
RRC连接建立完成

图10

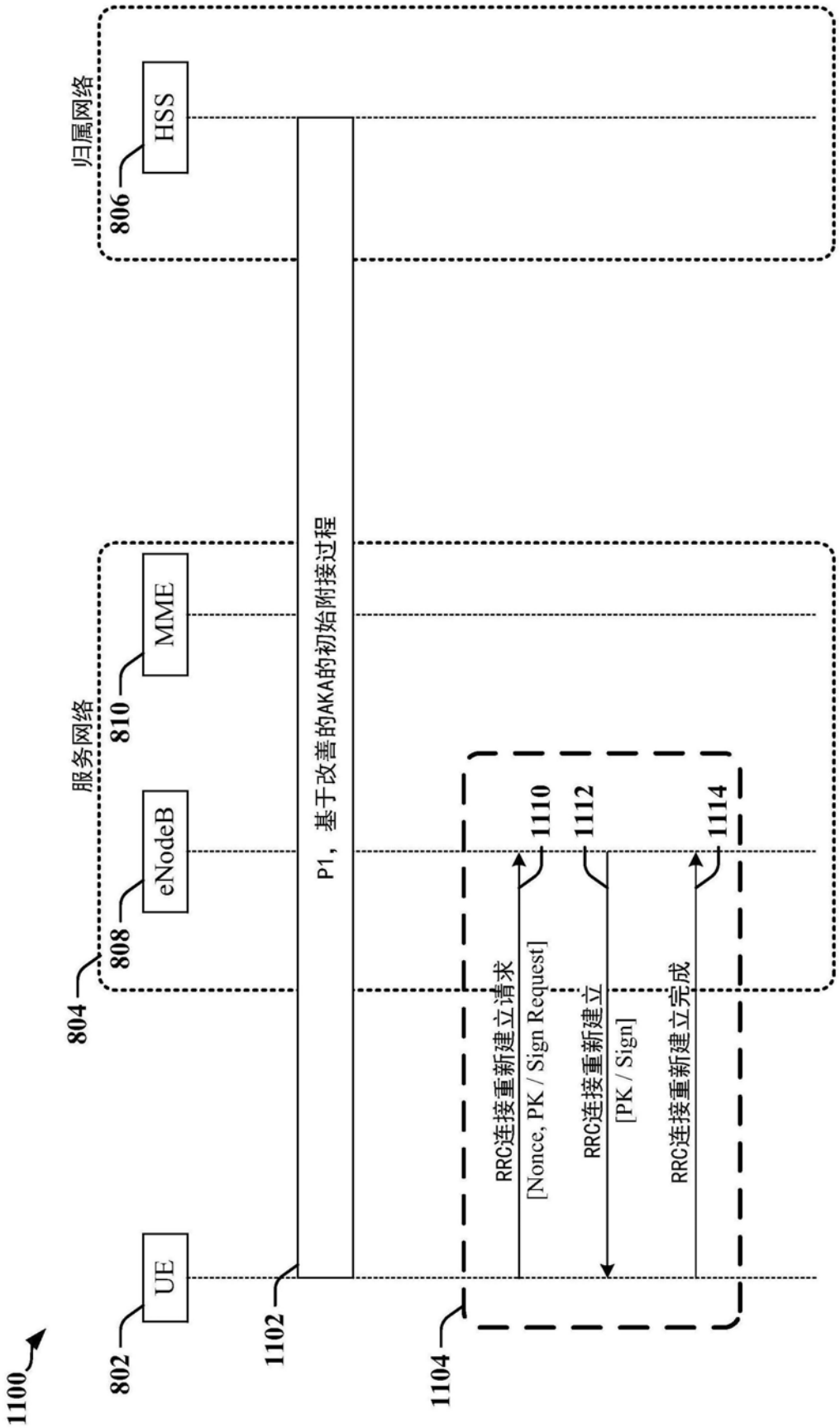

1100
802
UE
1102
804
服务网络
808
eNodeB
810
MME
806
归属网络
HSS
P1，基于改善的AKA的初始附接过程
1104
RRC连接重新建立请求
[Nonce, PK / Sign Request]
1110
RRC连接重新建立
[PK / Sign]
1112
RRC连接重新建立完成
1114

图11

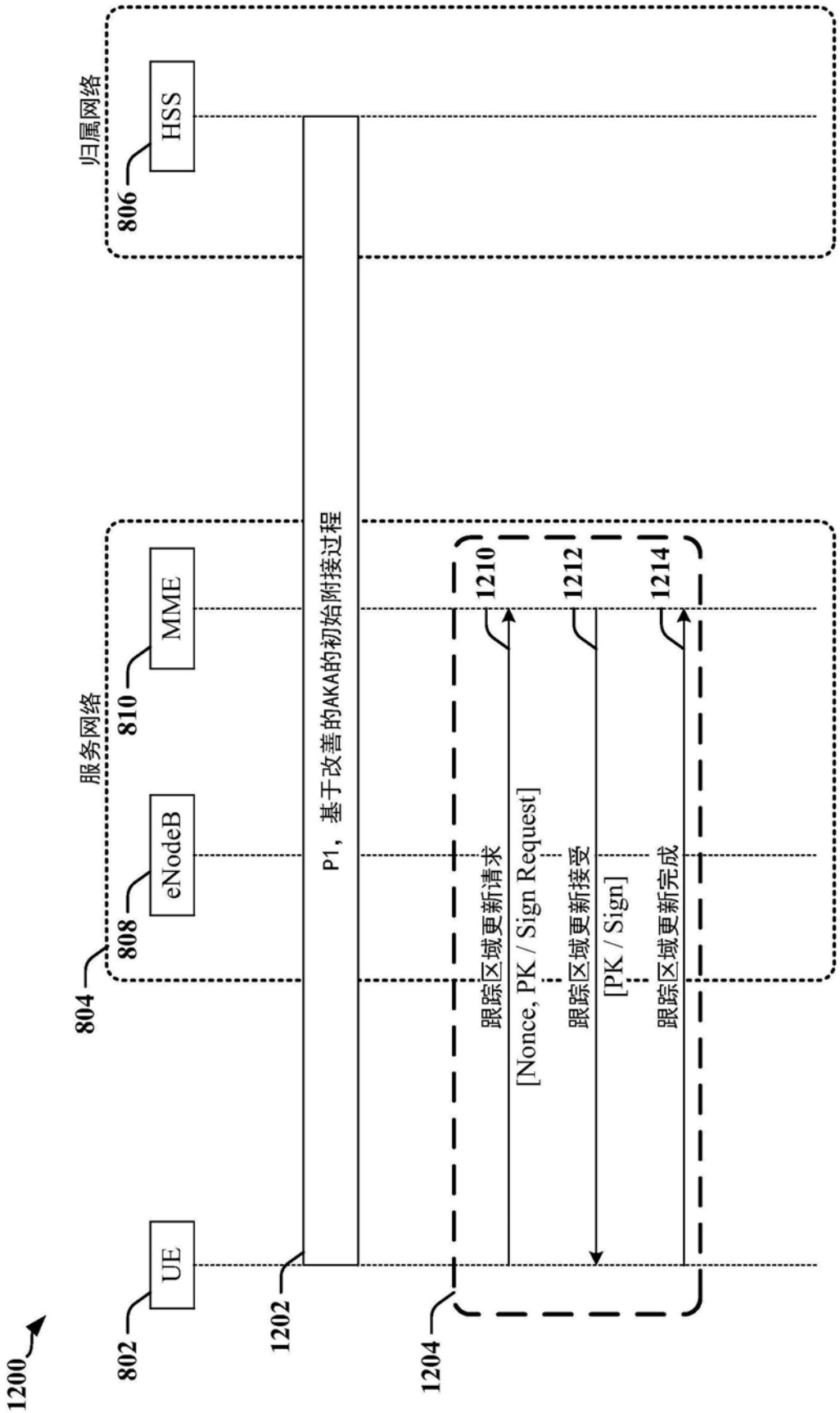

1200
802
UE
808
eNodeB
810
MME
806
HSS
804
服务网络
归属网络
1202
P1，基于改善的AKA的初始附接过程
1204
1210
跟踪区域更新请求
[Nonce, PK / Sign Request]
1212
跟踪区域更新接受
[PK / Sign]
1214
跟踪区域更新完成

图12

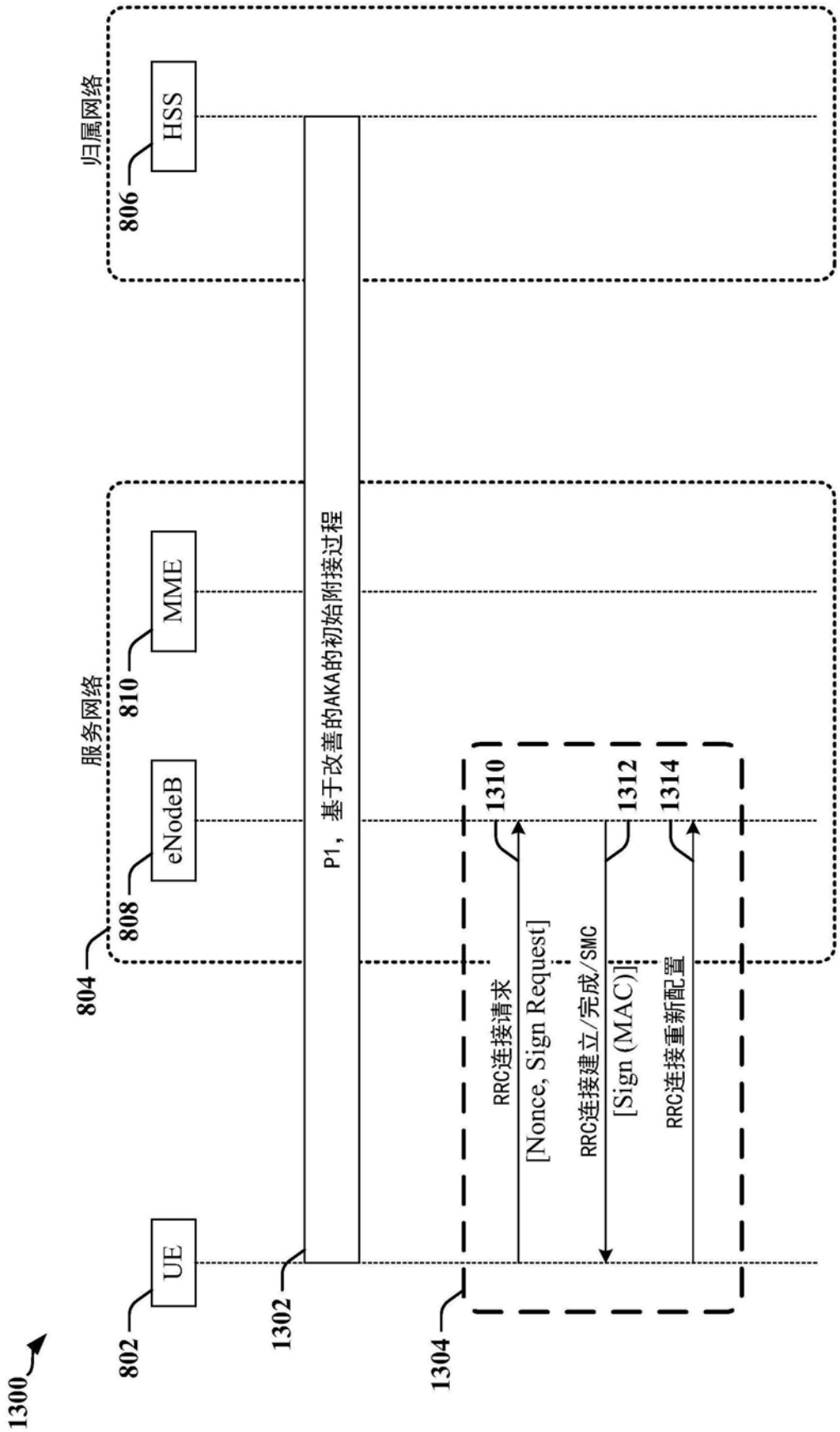

1300
802
UE
1302
1304
804
服务网络
808
eNodeB
810
MME
806
归属网络
HSS
P1，基于改善的AKA的初始附接过程
1310
RRC连接请求
[Nonce, Sign Request]
1312
RRC连接建立/完成/SMC
[Sign (MAC)]
1314
RRC连接重新配置

图13

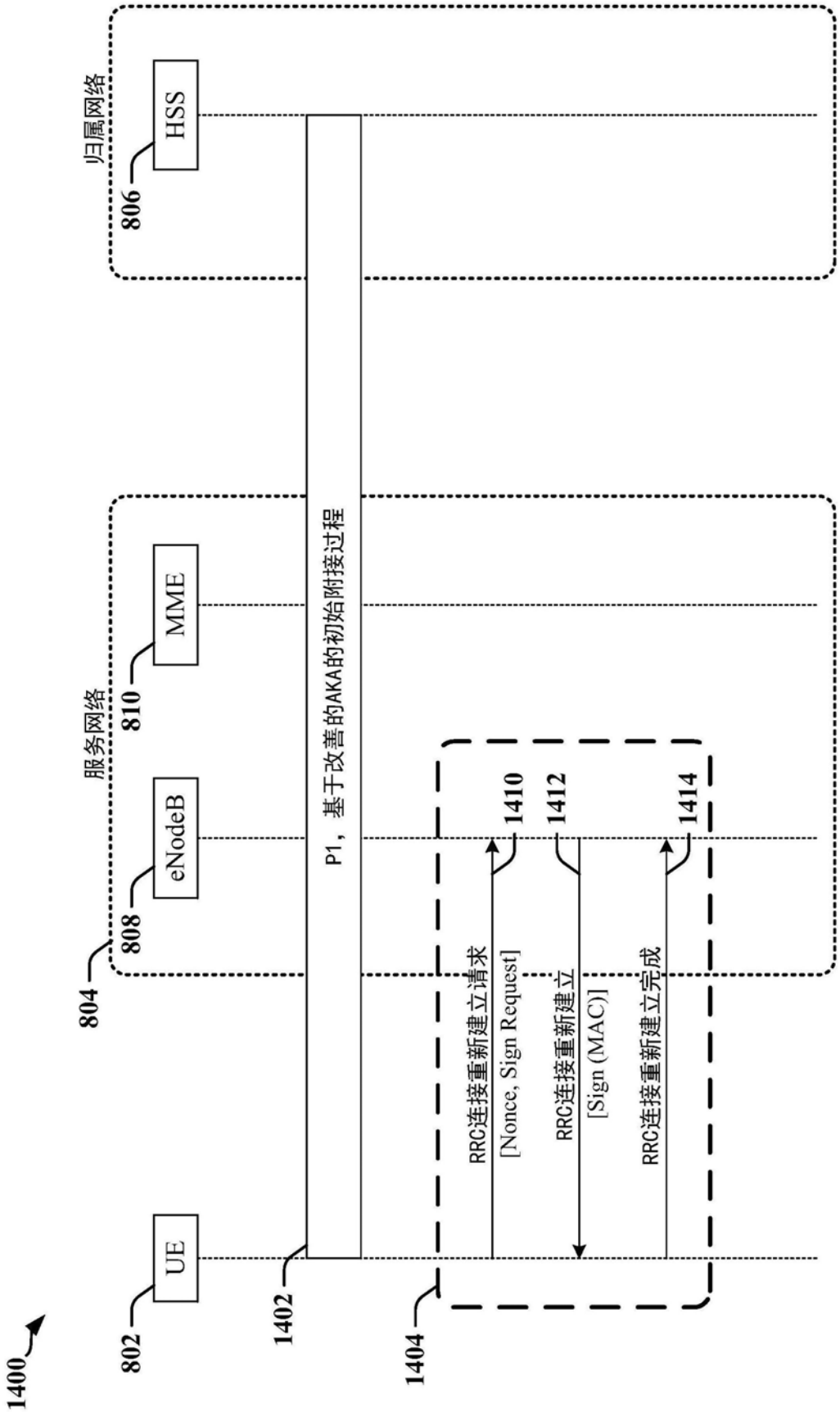

1400
802
UE
808
eNodeB
810
MME
806
HSS
归属网络
服务网络
804
1402
1404
P1，基于改善的AKA的初始附接过程
RRC连接重新建立请求
[Nonce, Sign Request]
RRC连接重新建立
[Sign (MAC)]
RRC连接重新建立完成
1410
1412
1414

图14

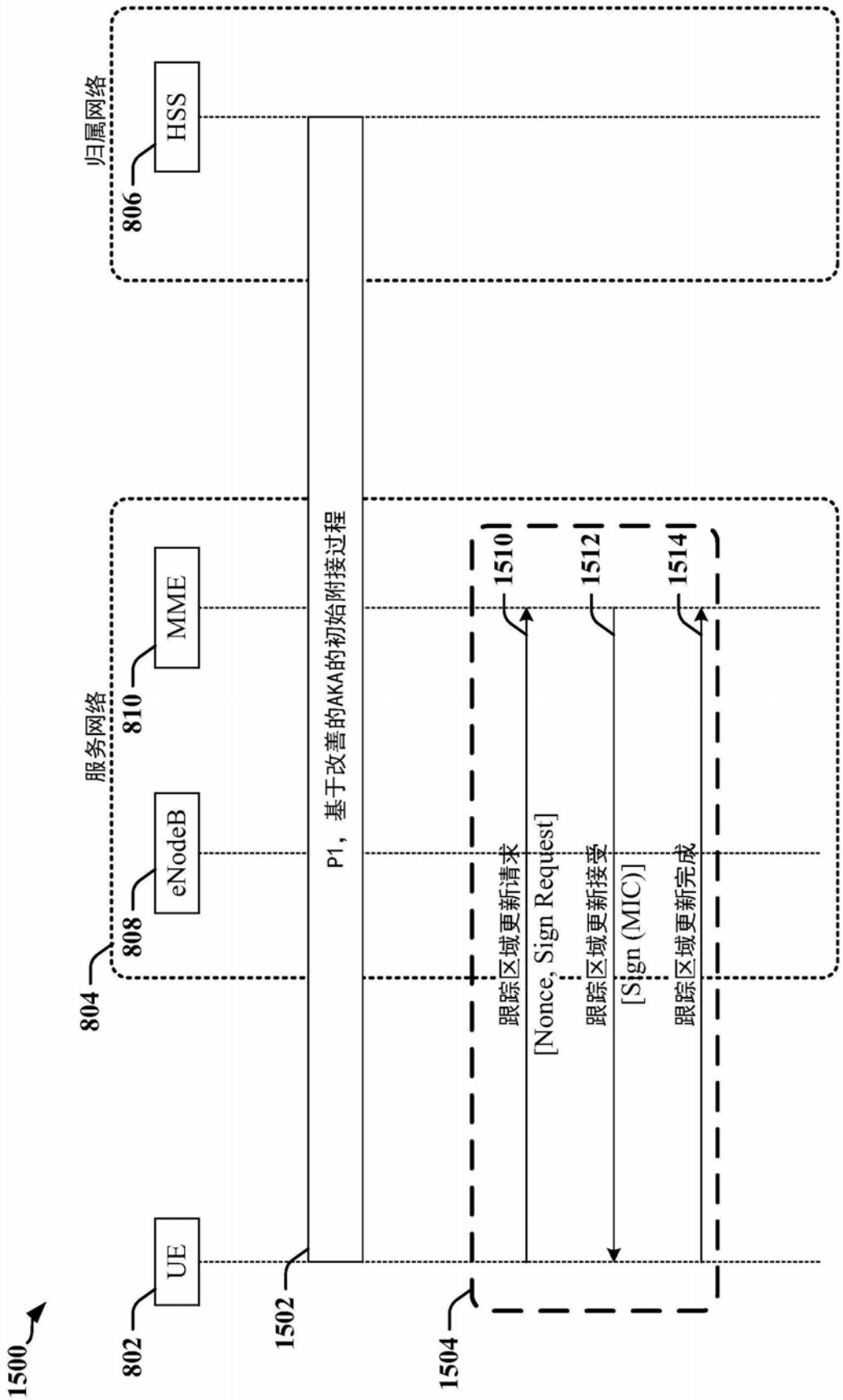

1500
802
UE
804
服务网络
808
eNodeB
810
MME
806
归属网络
HSS
1502
P1，基于改善的AKA的初始附接过程
1504
1510
跟踪区域更新请求
[Nonce, Sign Request]
1512
跟踪区域更新接受
[Sign (MIC)]
1514
跟踪区域更新完成

图15

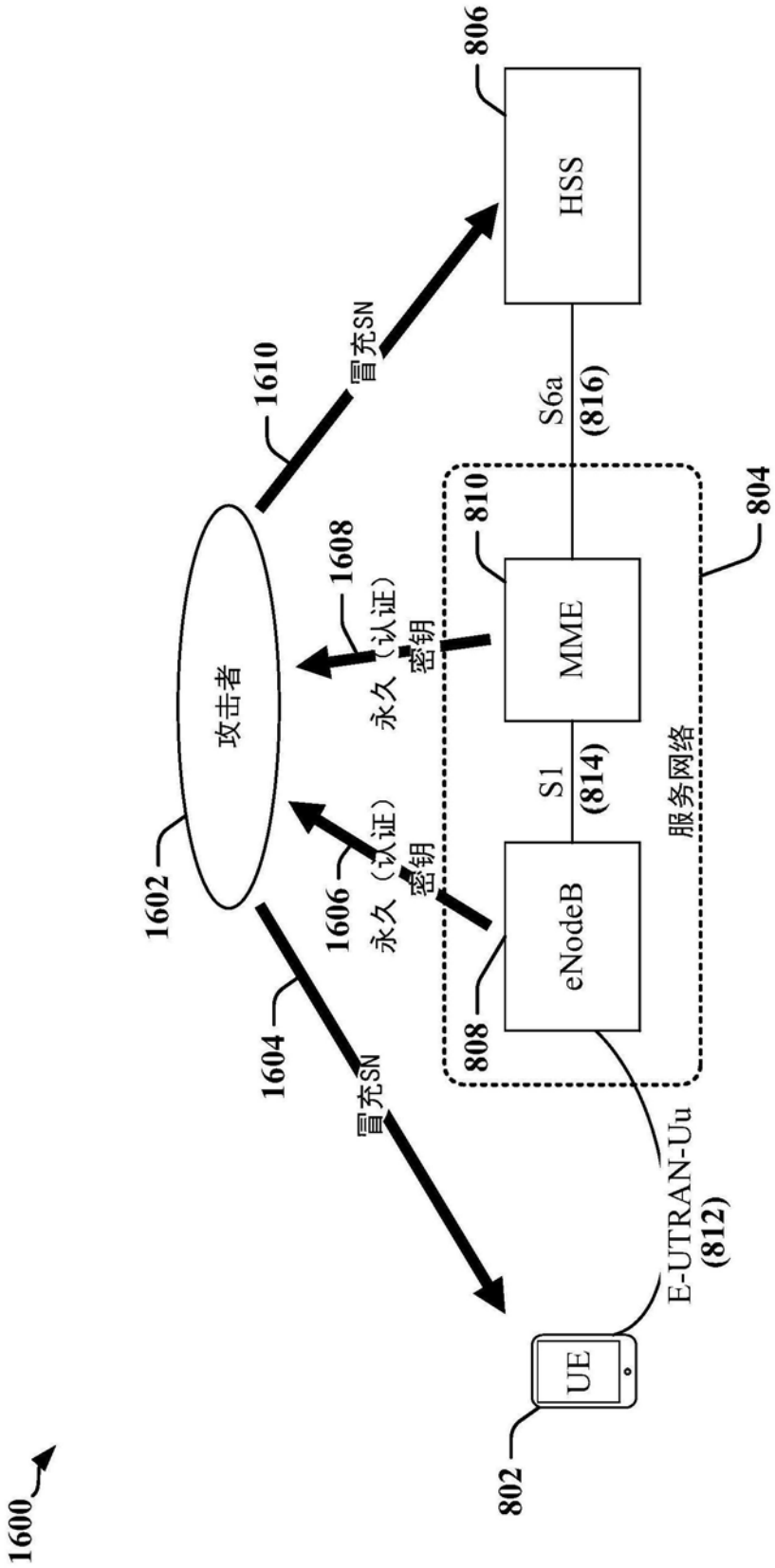

1600
802
UE
E-UTRAN-Uu
(812)
808
eNodeB
S1
(814)
MME
S6a
(816)
HSS
806
804
服务网络
810
1602
攻击者
1604
冒充SN
1606
永久（认证）密钥
1608
永久（认证）密钥
1610
冒充SN

图16

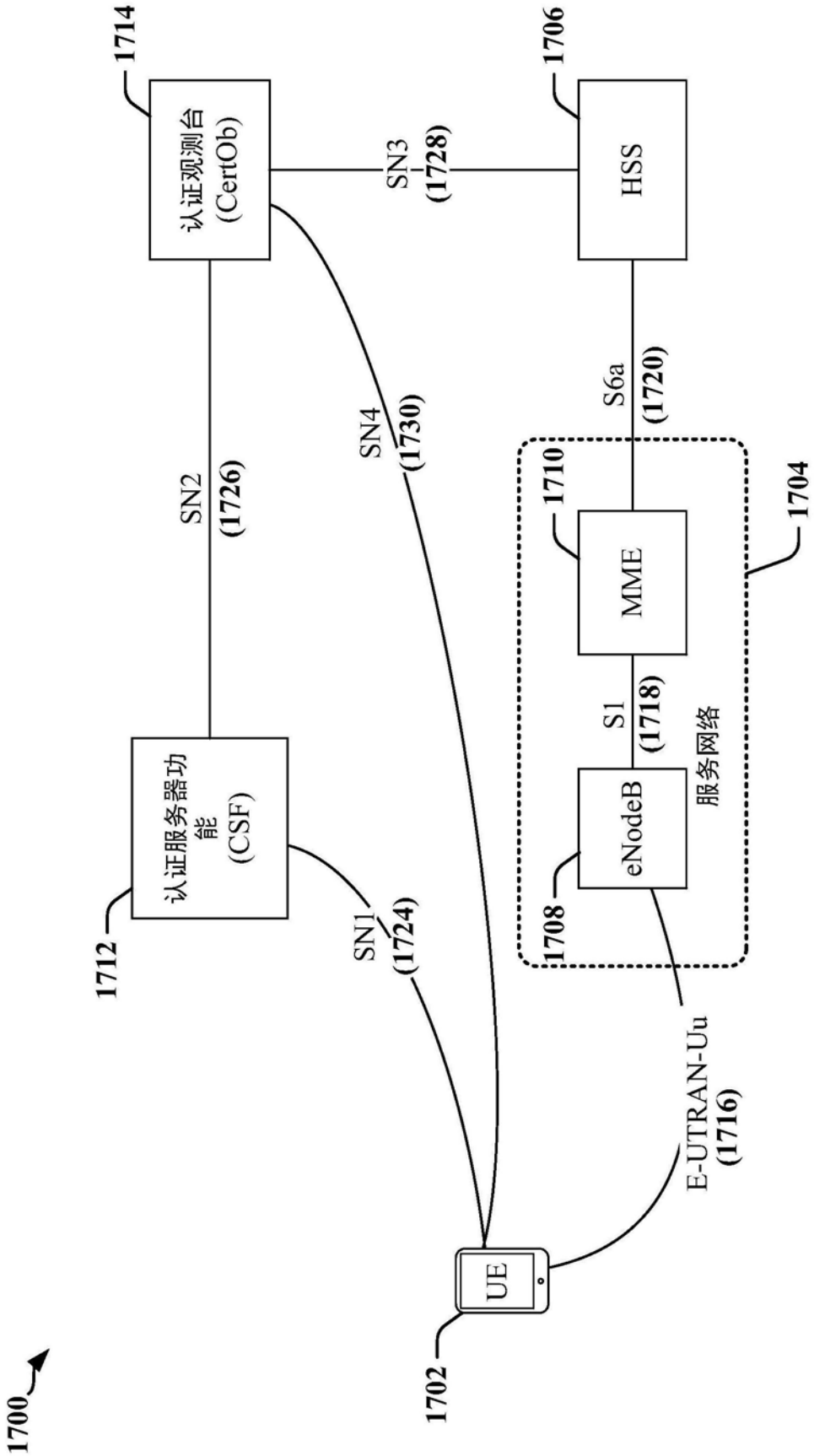

1700
1714
认证观测台
(CertOb)
1706
HSS
SN3
(1728)
SN2
(1726)
SN4
(1730)
S6a
(1720)
1710
MME
1704
S1
(1718)
服务网络
1712
认证服务器功能
(CSF)
SN1
(1724)
1708
eNodeB
E-UTRAN-Uu
(1716)
UE
1702

图17

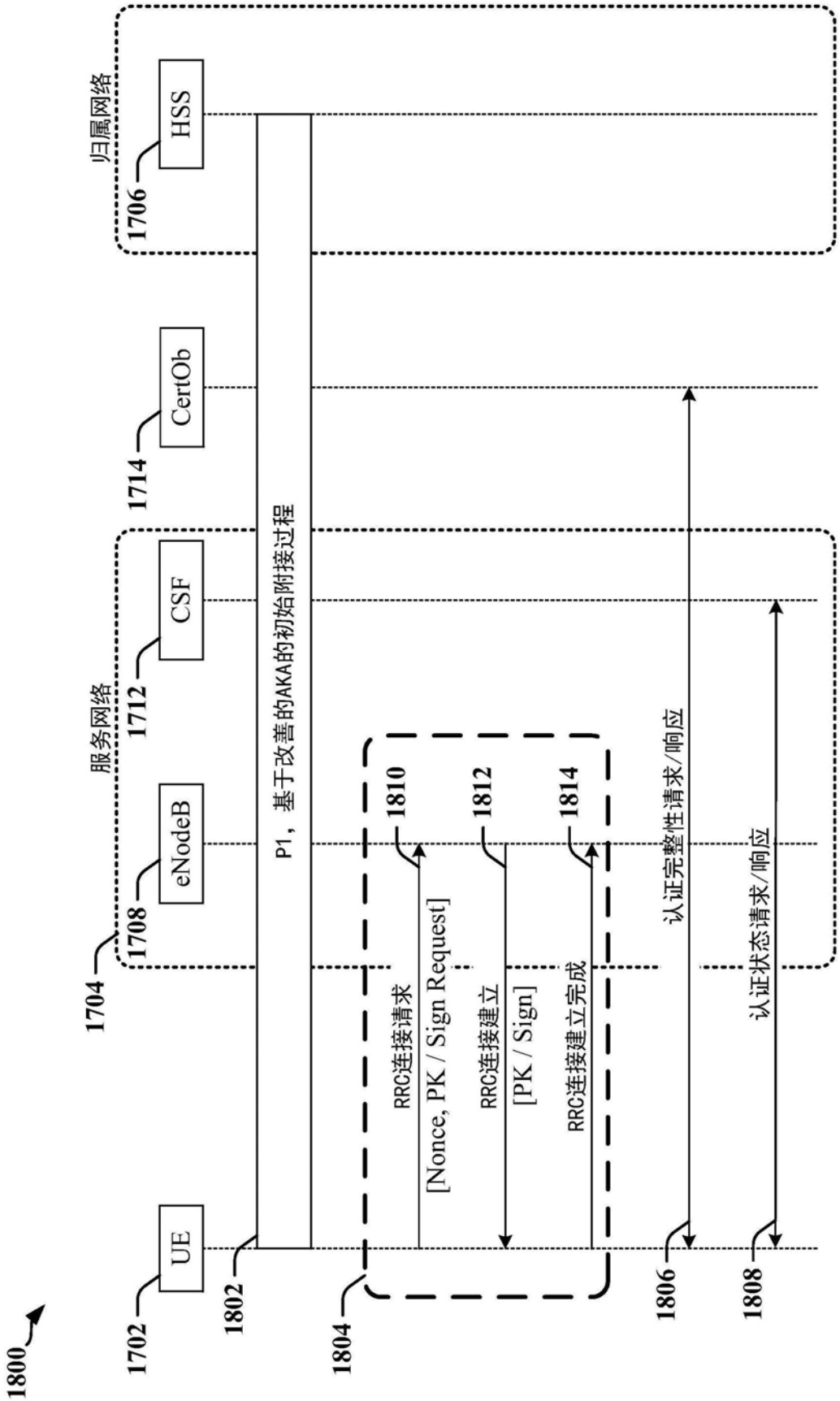

1800
1702
UE
1704
服务网络
1708
eNodeB
1712
CSF
1714
CertOb
归属网络
1706
HSS
1802
P1，基于改善的AKA的初始附接过程
1804
1810
RRC连接请求
[Nonce, PK / Sign Request]
1812
RRC连接建立
[PK / Sign]
1814
RRC连接建立完成
1806
认证完整性请求/响应
1808
认证状态请求/响应

图18

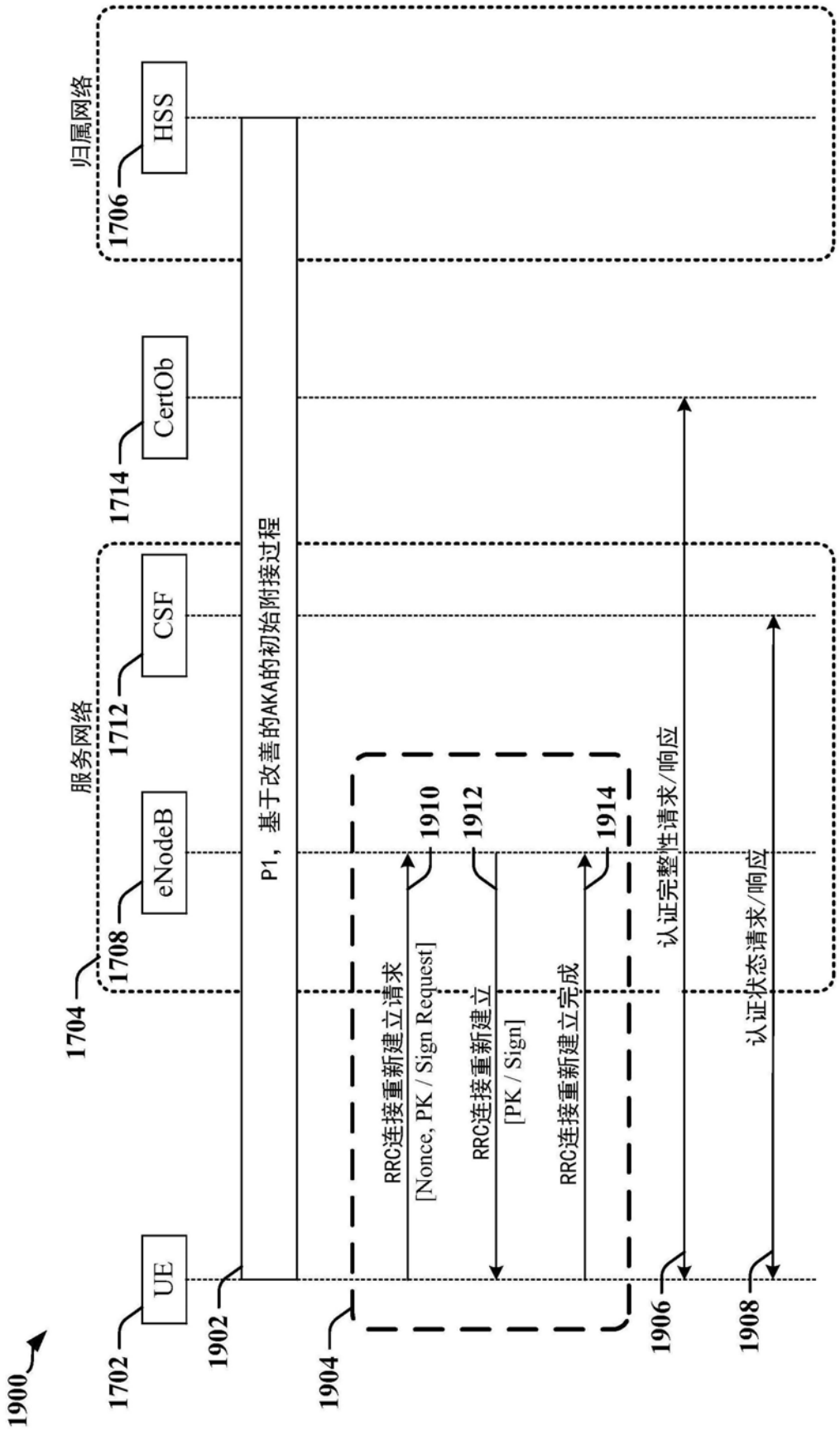

1900
1702
UE
1902
1704
服务网络
1708
eNodeB
1712
CSF
1714
CertOb
1706
归属网络
HSS
P1，基于改善的AKA的初始附接过程
1904
RRC连接重新建立请求
[Nonce, PK / Sign Request]
1910
RRC连接重新建立
[PK / Sign]
1912
RRC连接重新建立完成
1914
1906
认证完整性请求/响应
1908
认证状态请求/响应

图19

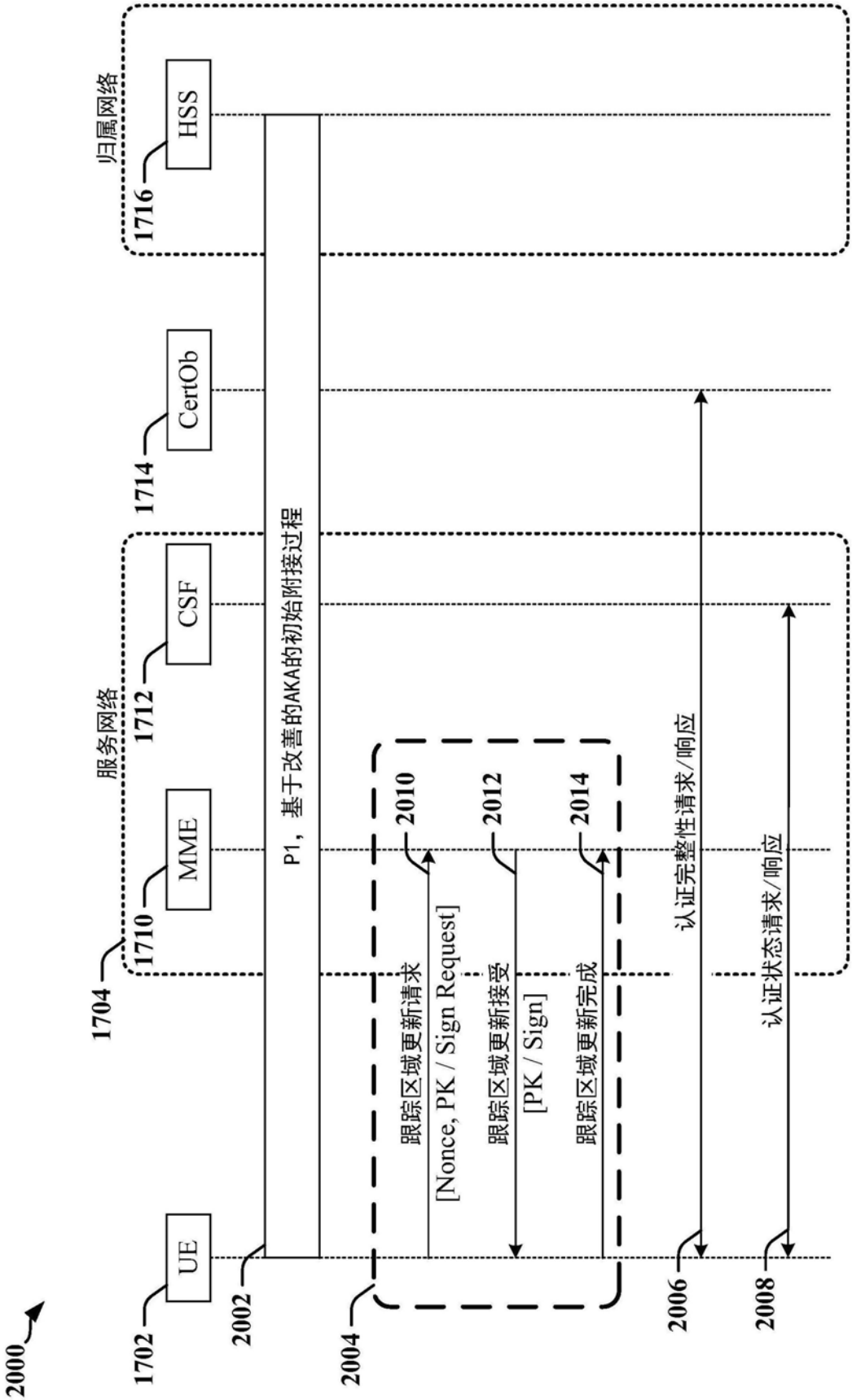

2000
1702
UE
2002
1704
服务网络
1710
MME
1712
CSF
1714
CertOb
1716
HSS
归属网络
P1，基于改善的AKA的初始附接过程
2004
跟踪区域更新请求
[Nonce, PK / Sign Request]
2010
跟踪区域更新接受
[PK / Sign]
2012
跟踪区域更新完成
2014
2006
认证完整性请求/响应
2008
认证状态请求/响应

图20

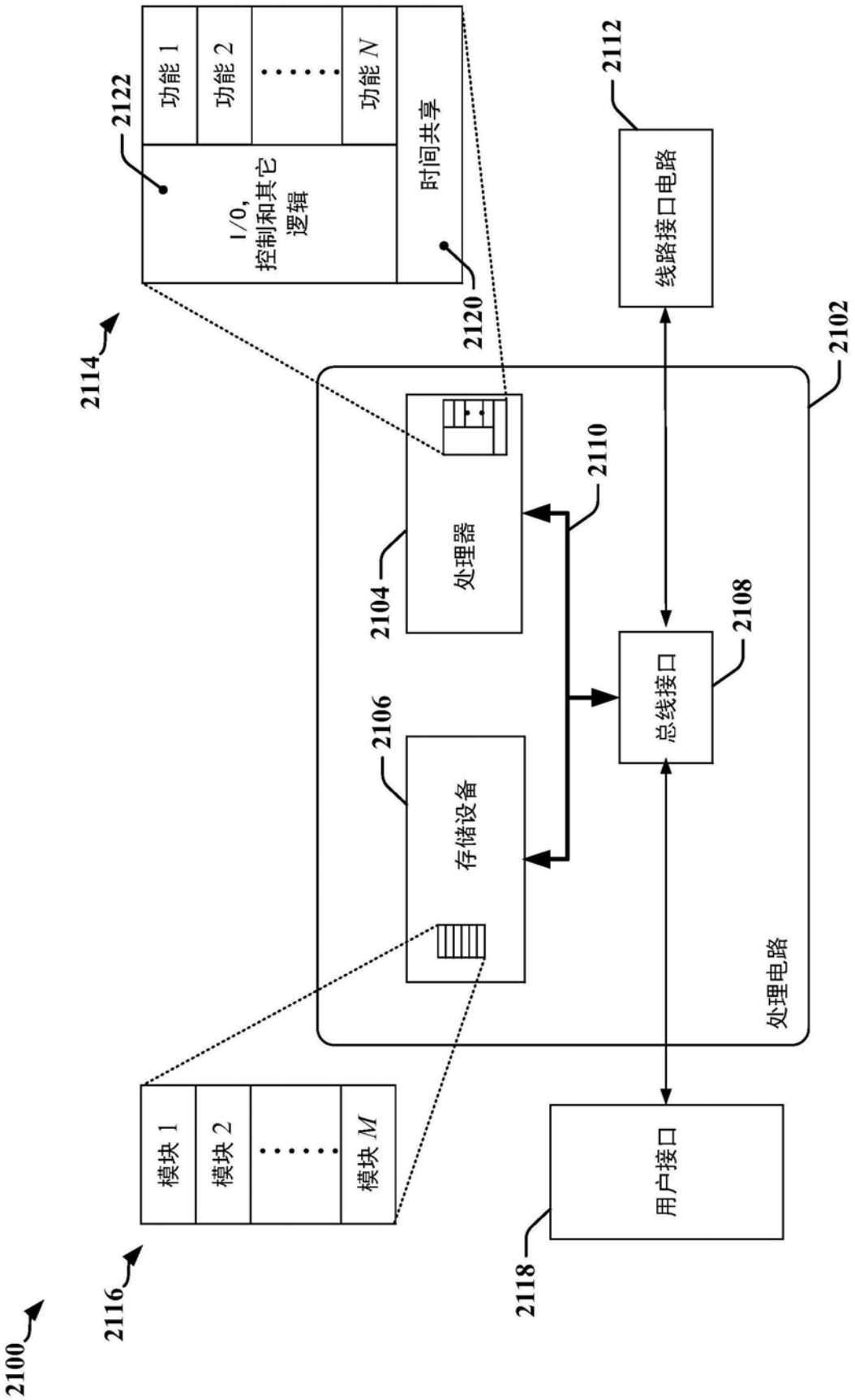

2100
2102
2104
处理器
2106
存储设备
2108
总线接口
2110
2112
线路接口电路
2114
2116
模块 1
模块 2
模块 M
2118
用户接口
2120
时间共享
2122
功能 1
功能 2
功能 N
I/O，
控制和其它
逻辑
处理电路

图21

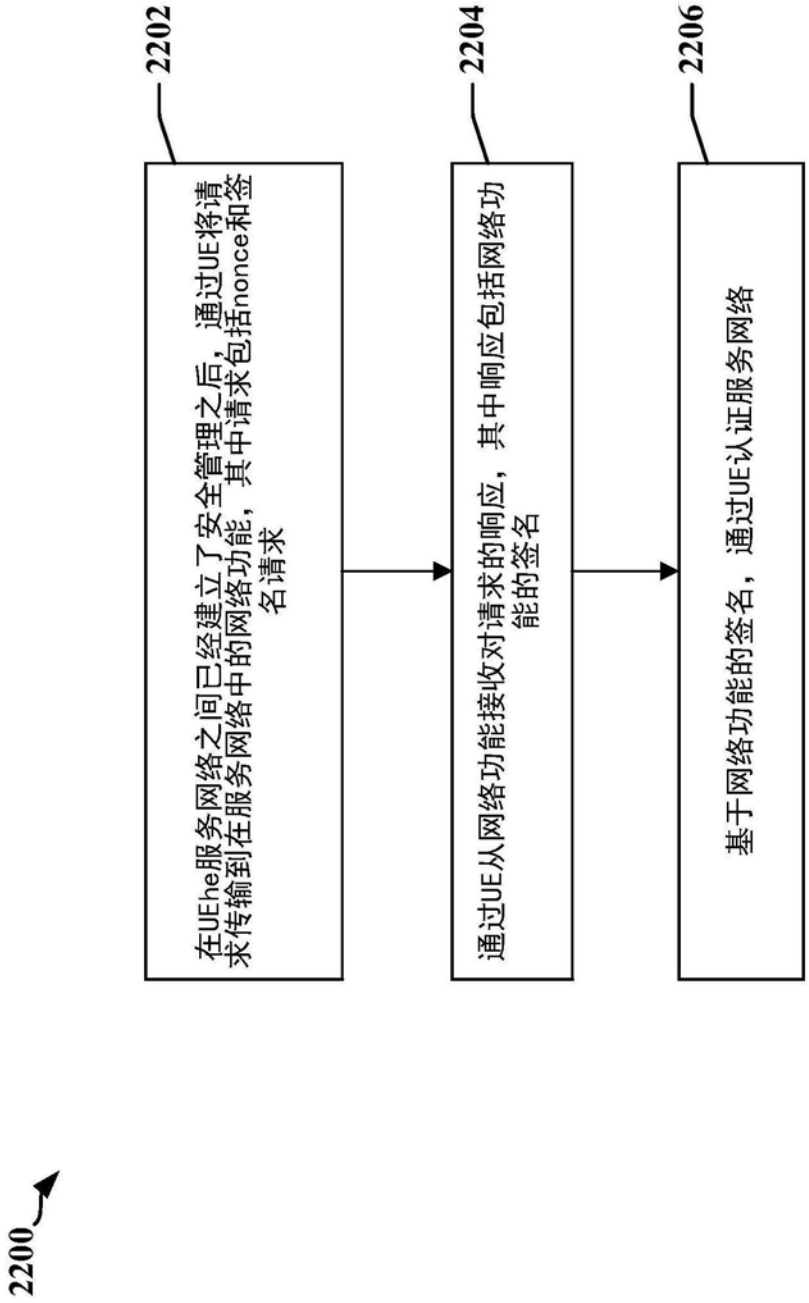

2200
2202
在UEhe服务网络之间已经建立了安全管理之后，通过UE将请求传输到在服务网络中的网络功能，其中请求包括nonce和签名请求
2204
通过UE从网络功能接收对请求的响应，其中响应包括网络功能的签名
2206
基于网络功能的签名，通过UE认证服务网络

图22

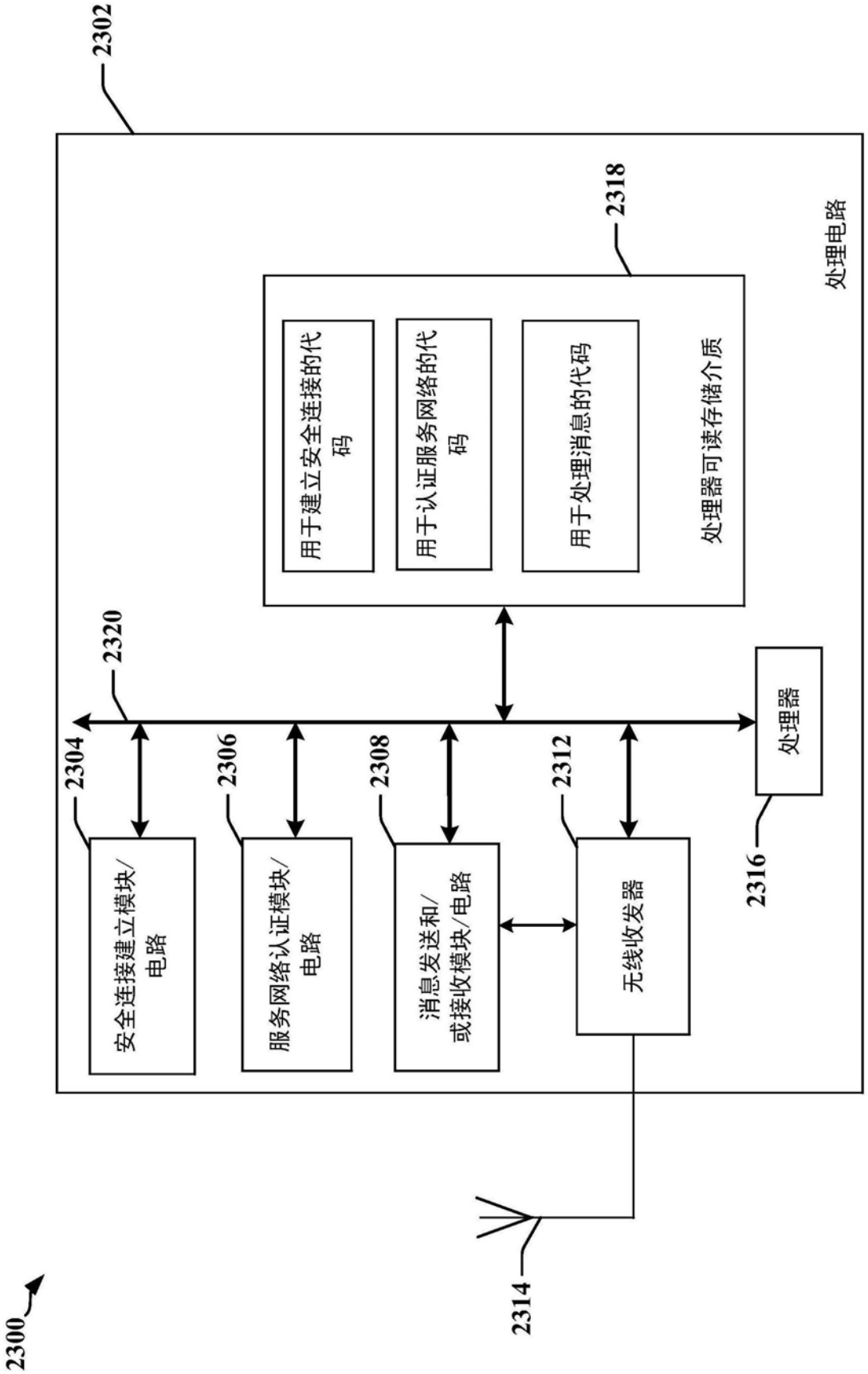

2300
2302
处理电路
2304
安全连接建立模块/电路
2306
服务网络认证模块/电路
2308
消息发送和/或接收模块/电路
2312
无线收发器
2314
2316
处理器
2318
处理器可读存储介质
用于处理消息的代码
用于认证服务网络的代码
用于建立安全连接的代码
2320

图23

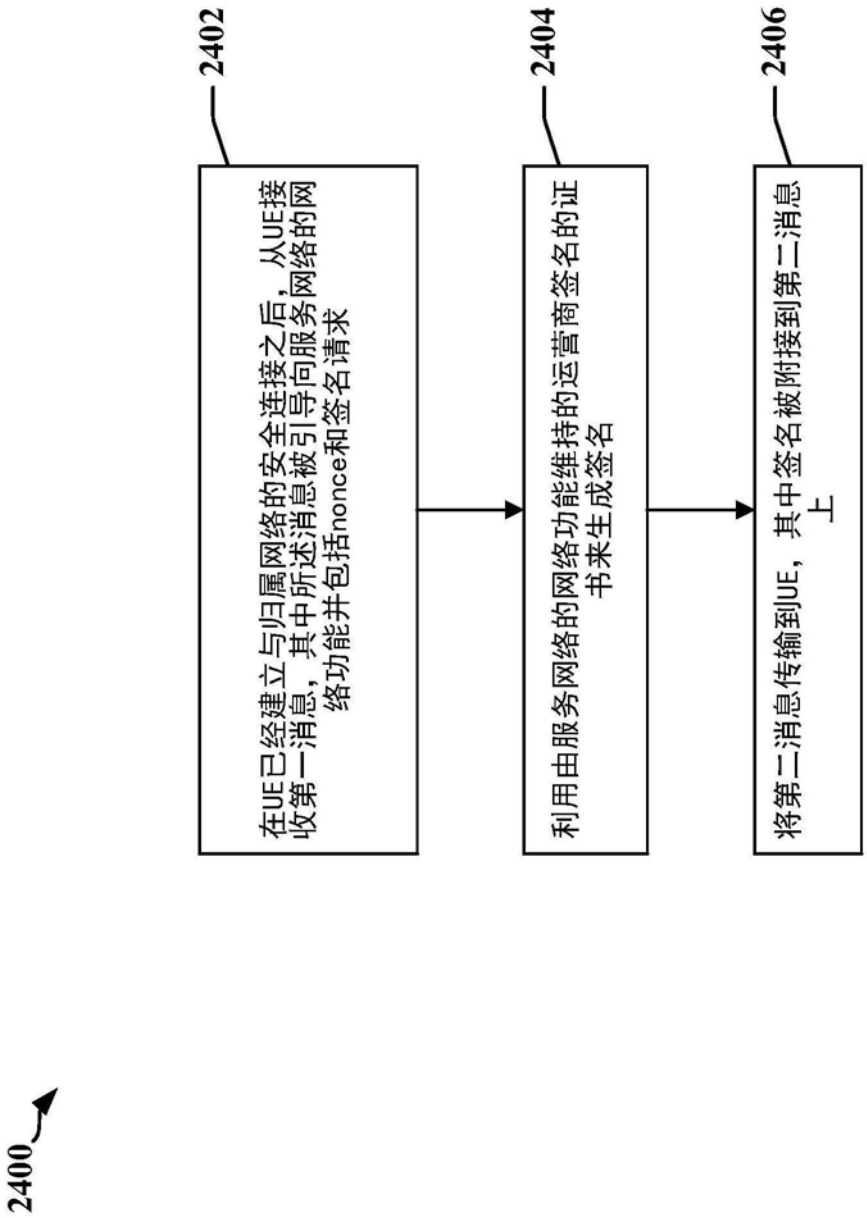

2400
2402
在UE已经建立与归属网络的安全连接之后，从UE接收第一消息，其中所述消息被引导向服务网络的网络功能并包括nonce和签名请求
2404
利用由服务网络的网络功能维持的运营商签名的证书来生成签名
2406
将第二消息传输到UE，其中签名被附接到第二消息上

图24

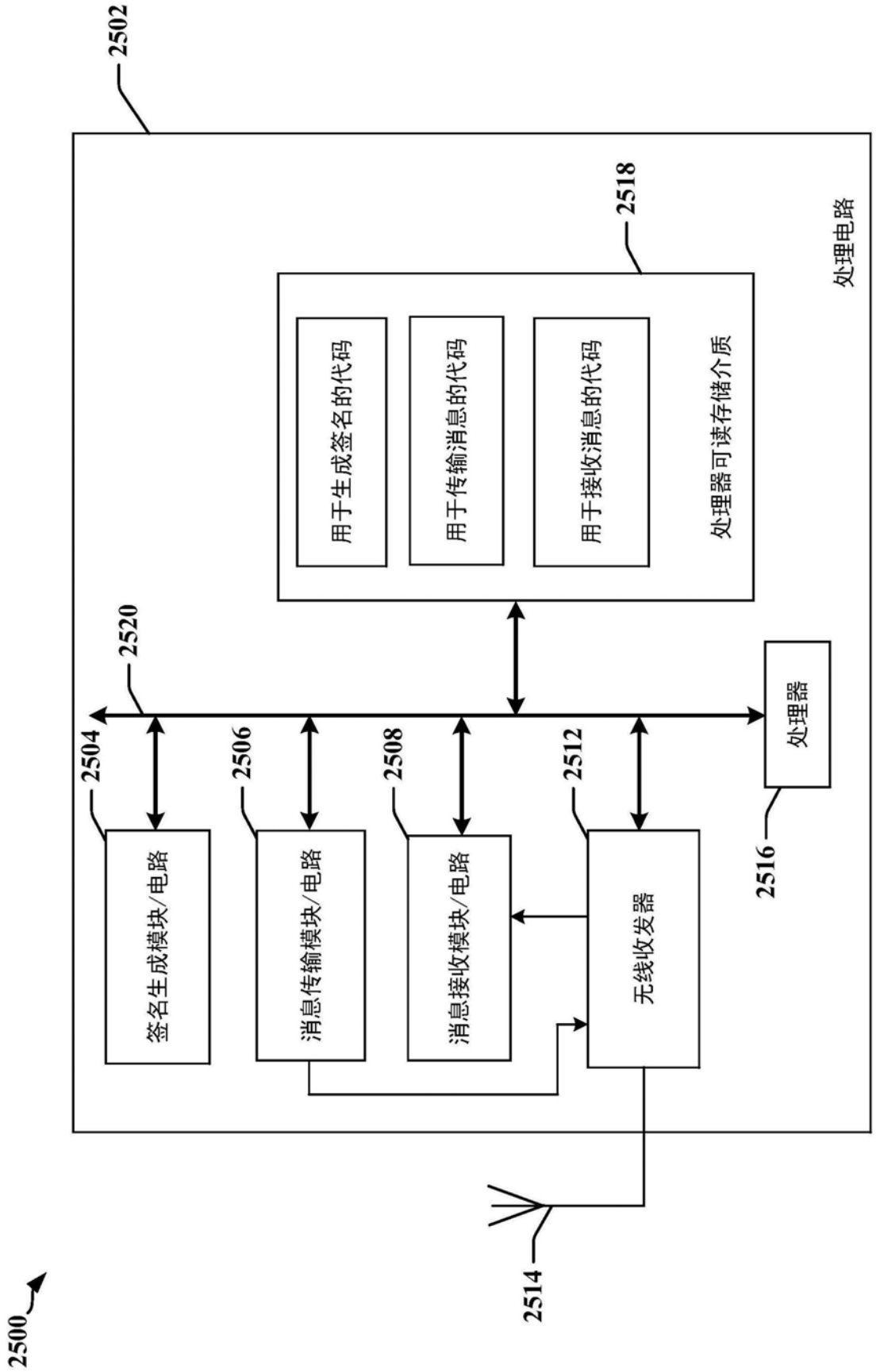

2500
2502
处理电路
2518
处理器可读存储介质
用于生成签名的代码
用于传输消息的代码
用于接收消息的代码
2520
2504
签名生成模块/电路
2506
消息传输模块/电路
2508
消息接收模块/电路
2512
无线收发器
2516
处理器
2514

图25