



(12) 发明专利申请

(10) 申请公布号 CN 112105016 A

(43) 申请公布日 2020.12.18

(21) 申请号 202010813750.6

(22) 申请日 2015.07.02

(30) 优先权数据

62/020,593 2014.07.03 US

(62) 分案原申请数据

201580033491.2 2015.07.02

(71) 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72) 发明人 张航

(51) Int.Cl.

H04W 12/00 (2009.01)

H04W 12/04 (2009.01)

H04W 12/08 (2009.01)

H04W 76/10 (2018.01)

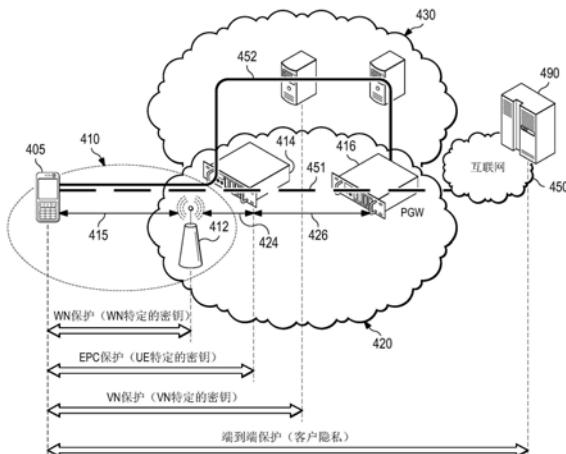
权利要求书2页 说明书10页 附图12页

(54) 发明名称

无线网络接入保护和安全架构的系统和方法

(57) 摘要

无线网络特定的(WN特定的)密钥可用于在无线接入链路上提供接入保护。WN特定的密钥可关联(或被分配给)无线网络，并被分发给无线网络的接入点，以及UE认证之后的用户设备(UE)。接着，WN特定的密钥用来加密/解密在无线接入链路上传输的数据。WN特定的密钥可与UE特定的密钥结合使用，以便提供多级接入保护。在一些实施例中，在相邻无线网络之间共享WN特定的密钥，以便在切换期间减少密钥交换的频率。业务特定的密钥可用来对机器对机器(M2M)业务提供接入保护。群组特定的密钥可用来对专用社交网络的成员之间通信的业务流提供接入保护。



1.一种密钥管理架构,包括:

无线网络(WN)保护控制器,适于获得用户设备(UE)特定的密钥,所述用户设备(UE)特定的密钥被分配给接入无线网络的所述UE,并且适于向所述无线网络中的服务网关(SGW)分发所述UE特定的密钥,其中所述UE特定的密钥适于提供在所述UE与所述SGW之间延伸的承载信道上的接入保护。

2.根据权利要求1所述的密钥管理架构,其中所述WN保护控制器从第三方密钥管理实体获得所述UE特定的密钥,所述第三方密钥管理实体由独立并区别于所述无线网络的运营商的第三方管理员运营。

3.根据权利要求1所述的密钥管理架构,进一步包括:

WN密钥控制器,适于生成被分配给所述无线网络的WN特定的密钥,并且向所述无线网络中的基站分发所述WN特定的密钥,其中所述WN特定的密钥独立并区别于所述UE特定的密钥,其中所述WN特定的密钥适于提供在所述基站与接入所述无线网络的用户设备(UE)之间建立的无线接入接口上的接入保护。

4.一种用于认证移动设备的方法,所述方法包括:

无线网络(WN)保护控制器接收UE特定的密钥,其中所述WN保护控制器被分配在整个无线网络中分发密钥;

所述WN保护控制器识别对应由所述UE特定的密钥指定的UE标识符的无线网络域;以及
所述WN保护控制器向所述无线网络域中的服务网关(SGW)分发所述UE特定的密钥,其中所述UE特定的密钥适于为所述UE与所述SGW之间延伸的承载信道上提供接入保护。

5.根据权利要求4所述的方法,其中所述WN保护控制器从第三方密钥管理实体接收所述UE特定的密钥,所述第三方密钥管理实体由区别于所述无线网络的运营商的第三方管理员运营。

6.根据权利要求4所述的方法,其中所述SGW为用户特定的SGW。

7.一种无线网络(WN)保护控制器,包括:

处理器;以及

计算机可读存储介质,存储用于所述处理器执行的程序,所述程序包括指令,用于:

从第三方密钥管理实体接收UE特定的密钥,其中所述WN保护控制器被分配在整个无线网络中分发密钥,并且所述第三方密钥管理实体由区别于所述无线网络的运营商的第三方管理员运营;

识别对应由所述UE特定的密钥指定的UE标识符的无线网络域;以及

向所述无线网络域中的服务网关(SGW)分发所述UE特定的密钥,其中UE特定的密钥适于为所述UE与所述SGW之间延伸的承载信道提供接入保护。

8.一种业务特定的接入保护的方法,所述方法包括:

服务网关(SGW)识别与机器对机器(M2M)客户相关联的M2M业务;

所述SGW接收分配给所述M2M业务的业务特定的密钥;

所述SGW从网络设备接收与所述M2M业务相关的分组;

使用所述业务特定的密钥尝试解密所述分组;以及

当解密所述分组的尝试不成功时,丢弃所述分组。

9.根据权利要求8所述的方法,其中所述SGW为业务特定的SGW。

10. 根据权利要求8所述的方法,进一步包括:

当解密所述分组的尝试成功时,向所述M2M客户转发所述解密的分组。

11. 根据权利要求8所述的方法,其中所述业务特定的密钥被分配给所述M2M业务,并且所述业务特定的密钥并不特定于所述网络设备。

12. 根据权利要求8所述的方法,其中在所述M2M客户认证所述网络设备之后,向所述网络设备提供所述业务特定的密钥。

13. 一种服务网关(SGW),包括:

处理器;以及

计算机可读存储介质,存储用于所述处理器执行的程序,所述程序包括指令,用于:

识别与机器对机器(M2M)客户相关联的M2M业务;

接收分配给所述M2M业务的业务特定的密钥;

从网络设备接收与所述M2M业务相关的分组;

使用所述业务特定的密钥尝试解密所述分组;以及

当解密所述分组的尝试不成功时,丢弃所述分组。

14. 一种群组特定的接入保护的方法,所述方法包括:

服务网关(SGW)识别专用网络;

所述SGW接收分配给所述专用网络的群组特定的密钥;

所述SGW接收寻址到属于所述专用网络的网络设备的分组;

使用所述群组特定的密钥尝试解密所述分组;以及

当解密所述分组的尝试不成功时,丢弃所述分组。

15. 根据权利要求14所述的方法,其中所述SGW为业务特定的SGW。

16. 根据权利要求14所述的方法,其中公共群组包括专用社交网络。

17. 根据权利要求14所述的方法,其中所述密钥被分配给所述专用网络,并且所述密钥并不特定于任何一个单独的网络设备。

18. 一种服务网关(SGW),包括:

处理器;以及

计算机可读存储介质,存储用于所述处理器执行的程序,所述程序包括指令,用于:

识别专用网络;

接收分配给所述专用网络的群组特定的密钥;

接收寻址到属于所述专用网络的网络设备的分组;

使用所述群组特定的密钥尝试解密所述分组;以及

当解密所述分组的尝试不成功时,丢弃所述分组。

无线网络接入保护和安全架构的系统和方法

技术领域

[0001] 本发明涉及一种用于无线通信的系统和方法，并且在具体实施例中，涉及一种用于无线网络接入保护和安全架构的系统和方法。

背景技术

[0002] 无线网络经常使用接入密钥，以确保只有有效用户才允许接入该无线网络。在传统的3G/4G无线网络中，在UE认证/授权之后，移动性管理实体(MME)向演进的分组核心(EPC)中的分组数据网(PDN)网关(PGW)和用户设备(UE)分发用户设备(UE)特定的密钥材料，所述用户设备特定的密钥材料用来加密在UE和PGW之间延伸的承载信道上的数据通信。特别地，在切换期间无线网络之间传送UE特定的密钥材料，或UE特定的密钥(简称)。在切换更加频繁的密集部署环境中传送UE特定的密钥可能会有问题，这是因为在无线网络之间反复地传送密钥材料会显著增加与UE移动性相关的延迟和开销。因此，需要在密集部署环境中能够快速、有效认证UE的技术。

发明内容

[0003] 技术优点一般通过本公开描述“无线网络接入保护和安全架构”的实施例来实现。

[0004] 根据一实施例，提供了一种无线网络接入保护的方法。在本实例中，该方法包括基站获得无线网络(WN)特定的密钥，所述无线网络(WN)特定的密钥被分配给无线网络。该基站属于该无线网络。该方法进一步包括：建立基站和用户设备(UE)之间的无线连接，以及在无线连接上从UE接收加密的数据。加密的数据具有第一层加密和第二层加密。该方法进一步包括：使用WN特定的密钥解密第一层加密，以获得部分解密的数据；以及向所述WN中的网关转发该部分解密的数据。还提供了一种执行该方法的装置。

[0005] 根据另一个实施例，提供了一种在无线网络中分发密钥的方法。在本实例中，该方法包括在WN密钥控制器生成无线网络(WN)特定的密钥。所述WN特定的密钥被分配给第一无线网络。该方法进一步包括：向所述第一无线网络中的基站分发WN特定的密钥，用于提供所述基站与接入所述无线网络的用户设备(UE)之间建立的无线接入接口上的接入保护。还提供了一种执行该方法的装置。

[0006] 根据再一个实施例，提供了一种密钥管理架构。在本实例中，所述密钥管理架构包括：无线网络(WN)保护控制器，适于获得用户设备(UE)特定的密钥，所述用户设备(UE)特定的密钥被分配给接入无线网络的UE，并且适于向无线网络中的服务网关(SGW)分发UE特定的密钥。UE特定的密钥适于提供在UE与SGW之间延伸的承载信道上的接入保护。

[0007] 根据再一个实施例，提供了一种用于认证移动设备的方法。在本实例中，该方法包括：在WN保护控制器接收UE特定的密钥，该WN保护控制器被分配在整个无线网络中分发密钥。该方法进一步包括：识别对应由UE特定的密钥指定的UE标识符的无线网络域；以及向无线网络域中的服务网关(SGW)分发UE特定的密钥。所述UE特定的密钥适于为UE与SGW之间延伸的承载信道上提供接入保护。还提供了一种执行该方法的装置。

[0008] 根据再一个实施例,提供了一种提供业务特定的接入保护的方法。在本实例中,该方法包括:识别与机器对机器(M2M)客户相关联的M2M业务;在SGW接收分配给M2M业务的业务特定的密钥;以及从网络设备接收分组。所述分组与M2M业务相关。该方法进一步包括:使用业务特定的密钥尝试解密所述分组;以及当解密所述分组的尝试不成功时,丢弃所述分组。也提供了一种执行该方法的装置。

[0009] 根据再一个实施例,提供了一种群组(group)特定的接入保护的方法。在本实例中,该方法包括:识别专用网络,在SGW接收分配给所述专用网络的群组特定的密钥,接收寻址到属于所述专用网络的网络设备的分组;以及使用群组特定的密钥尝试解密分组。该方法进一步包括:当解密所述分组的尝试不成功时,丢弃所述分组。还提供了一种执行该方法的装置。

附图说明

[0010] 为了更全面地理解本公开及其优点,现在参考下面结合附图的说明,附图中:

[0011] 图1示出了无线网络实施例的示意图;

[0012] 图2示出了传统无线网络安全架构的示意图;

[0013] 图3示出了无线网络安全架构实施例的示意图;

[0014] 图4示出了用于提供多级接入保护的无线网络架构实施例的示意图;

[0015] 图5示出了用于管理网络接入密钥的无线网络安全架构实施例的示意图;

[0016] 图6示出了用于管理网络接入密钥的无线网络安全架构另一个实施例的示意图;

[0017] 图7示出了用于管理UE特定的密钥材料的无线网络架构实施例的示意图;

[0018] 图8示出了用于向M2M业务提供接入保护的网络架构实施例的示意图;

[0019] 图9示出了用于管理业务特定的密钥材料的无线网络架构实施例的示意图;

[0020] 图10示出了用于为公共群组的成员之间的通信提供接入保护的网络架构实施例的示意图;

[0021] 图11示出了用于管理群组特定的密钥材料的无线网络架构实施例的示意图;

[0022] 图12示出了计算平台实施例的示意图;以及

[0023] 图13示出了通信设备实施例的示意图。

[0024] 除非另外指明,不同附图中对应编号和符号一般表示对应部件。附图的绘制清楚地示出了实施例的相关方面,并不必是按比例绘制。

具体实施方式

[0025] 下面将更详细地讨论本公开的实施例的实现和运用。然而,应理解,本文公开的构思可以体现在多种特定语境中,并且所讨论的具体实施例仅仅是说明性的,并不用来限制权利要求书的范围。应进一步理解,可以在不偏离所附权利要求限定的本公开的精神和范围的情况下,做出各种改变、替换和变更。

[0026] 3G/4G无线网络使用UE特定的密钥向从UE向演进的分组核心(EPC)网络的分组数据网(PDN)网关(PGW)之间延伸的承载信道提供接入保护。然而,不会为UE和RAN之间延伸的无线连接提供单独等级的接入保护。在未来的网络架构中,无线接入网可具有第一实体提供的基础设施以及另一实体在该基础设施之上提供的电信服务。为了适应对带宽日益增长

的需求,很可能未来的网络部署将包括作为整个网络一部分的密集和超密集网络片段。因此,需要适合密集部署的无线网络的多级接入网络安全框架。

[0027] 本公开的各个方面提供了利用无线网络特定的(WN特定的)密钥材料,或WN特定的密钥(简称)的技术,以便提供在无线接入链路上的接入保护。更具体地,WN特定的密钥关联(或被分配给)无线网络,并被分发给无线网络的接入点,以及UE认证之后的UE。接着,WN特定的密钥用来加密/解密在无线接入链路上传输的数据。WN特定的密钥可与UE特定的密钥结合使用,以便提供多级接入保护。在一些实施例中,在相邻无线网络之间分享WN特定的密钥,以便减少在切换期间密钥交换的频率。例如,公共WN特定的密钥可预分发给相邻无线网络中的接入点,以便在这些相邻无线网络之间发生切换,而在切换期间不交换WN特定的密钥。本公开的多个方面还提供了用于向机器对机器(M2M)业务提供接入保护的业务特定的密钥,以及用于向例如专用社交网络等公共群组的成员之间通信的业务流提供接入保护的群组特定的密钥。也提供了用于分发UE特定的、WN特定的、业务特定的以及群组特定的密钥的网络安全架构。下文将更详细地描述这些及其他细节。

[0028] 图1示出了用于通信数据的网络100。网络100包括具有覆盖区域101的接入点(AP)110,多个移动设备120和回程网络130。AP 110可包括能够提供无线接入的,特别是通过与移动设备120建立上行链路(短划线)和/或下行链路(点划线)连接的任何组件,例如基站、增强的基站(eNB)、毫微微蜂窝基站以及其他无线启用的设备。移动设备120可包括能够与AP 110建立无线连接的任何组件,例如用户设备(UE)、移动站(STA)或其他无线启用的设备。回程网络130可以是能够使数据在AP 110和远程端(未示出)之间进行交换的任何组件或组件集合。在一些实施例中,网络100可包括各种其他无线设备,例如继电器、低功率节点等。

[0029] 传统的3G/4G无线网络使用UE特定的密钥向从UE向EPC网络的PGW之间延伸的承载信道提供接入保护,但不会为UE和RAN之间延伸的无线连接提供单独等级的接入保护。图2示出了提供单层接入保护的传统的无线网络安全架构200。如图所示,传统的无线网络安全架构200包括向UE 205提供无线接入的无线网络域210。所述无线网络域210包括基站212、SGW 214、PGW 216、移动性管理实体(MME)218以及家庭安全服务器(HHS)220。通过BS 212和SGW 214在UE 205和PGW 216之间建立承载信道。PGW 216充当无线网络域210和互联网240之间的网关。

[0030] 当建立承载信道时,MME 218认证UE 205。具体地,认证中心230在UE认证期间使用加密密钥(CK)和完整性密钥(IK)生成共享密钥(例如,公共私密密钥接入安全管理实体(KASME))。接着,认证中心230使用共享密钥和随机数生成一组密钥和校验和,并向MME 218发送生成的密钥、校验和以及随机数。MME 218向UE 205分发生成的校验和以及随机数。UE 205中的通用用户标识模块(USIM)使用MME 218提供的随机数和共享密钥独立地计算一组相同的密钥。通过验证在UE 205和EPC 218中计算的校验和执行双向认证。其后,MME 218向UE 205和PGW 216两者分发UE特定的密钥。UE特定的密钥用于加密/解密在承载信道上通信的数据。例如,UE 205可使用UE特定的密钥来加密在承载信道上上行链路传输中承载的数据,并且PGW 216可使用该UE特定的密钥,尝试解密在该承载信道上接收的数据。一旦数据被解密,PGW 216可通过互联网240向远程目的地转发该数据。在一些实施例中,MME 218向UE 205和PGW 216发送公开-私有密钥对。UE 205和PGW 216可使用该公开-私有密钥对生成

UE特定的密钥。例如,UE 205可单侧生成UE特定的密钥,使用公开-私有密钥对加密该UE特定的密钥,然后向PGW 216通信该加密的UE特定的密钥。又如另一实例,PGW 216可单侧生成UE特定的密钥,使用该公开-私有密钥对加密该UE特定的密钥,然后向UE 205通信该加密的UE特定的密钥。再如又一实例,例如通过密钥交换协议,PGW 216和UE 205可双侧生成UE特定的密钥,并且可使用公开-私有密钥加密在密钥交换协议期间交换的消息。

[0031] 然而,UE特定的密钥可向UE和PGW之间延伸的承载信道提供接入保护,但不会为UE和BS之间延伸的无线连接提供保护。因此,需要适合密集部署的无线网络的多级接入网络安全框架。

[0032] 本公开的各个方面提供了一种多层接入保护方案,该方案除了使用UE特定的密钥向承载信道提供接入保护之外,使用WN特定的密钥向无线接入链路提供接入保护。图3示出了用于提供多级接入保护的无线网络安全架构300的实施例。如图所示,实施例的无线网络安全架构300包括向UE 305提供无线接入的无线网络域310。无线网络域310包括基站312(也称为接入点312)、服务网关314、分组网关316、WN密钥控制器322、WN保护控制器324以及密钥管理实体326。

[0033] UE特定的密钥用来加密/解密在UE 305和服务网关314之间延伸的承载信道上通信的数据。服务网关314可为虚拟服务网关,例如虚拟用户特定的服务网关或虚拟业务特定的服务网关。UE特定的密钥可经由WN保护控制器324向服务网关314分发,WN保护控制器324可从密钥管理实体326获得UE特定的密钥。在一实施例中,密钥管理实体326为由独立并区别于无线网络的运营商的第三方管理员运营的第三方管理实体。密钥管理实体326可使用认证中心330提供的信息导出UE特定的密钥。WN保护控制器324可具有多种职责。例如,WN保护控制器324可维护例如UE特定的密钥、业务特定的密钥、群组特定的密钥、回程(BH)密钥等密钥材料。WN保护控制器324还可以管理网络-节点/设备认证,并且协调与其他无线网络域中的其他控制器的密钥同步。

[0034] WN特定的密钥用来加密/解密在UE 305和接入点312之间延伸的无线连接上通信的数据。在UE 305建立无线链路连接之前,WN特定的密钥可分发给接入点312。WN特定的密钥可在UE认证之后发送给UE 305。WN特定的密钥可专属地被分配给无线网络域310。可替代地,WN特定的密钥可被分配给无线网络域310所属的无线网络域的群组或集群。

[0035] 图4示出了用于提供多级接入保护的无线网络架构400的实施例。如图所示,实施例的无线网络架构400包括无线接入网络410、演进的分组核心(EPC) 420以及虚拟网络430。RAN 410包括适于向UE 405提供无线接入的接入点412。EPC 420特别地包括适于充当在EPC 420和RAN 410之间的网关的网关,例如服务网关(SGW) 414,以及适于充当EPC 420与互联网450之间的网关的分组数据网(PDN)网关(PGW) 416。EPC 420可包括其他组件(图4中未示出),例如移动性管理实体(MME)、演进的分组数据网关以及归属用户服务器(HSS)。在下一代网络中,EPC 420可划分为多个分布式EPC,这种情况下,一些组件(例如SGW)可置于分布式EPC中。

[0036] 特别地,RAN 410和EPC 420共同形成提供UE 405和互联网450之间的承载路径451的无线网络。承载路径451可承载UE 405和远程端490之间通信的业务流,并且可以包括多个接口和/或片段。在该实例中,承载路径451包括UE 405和接入点412之间延伸的无线连接415(例如,“UU接口”)、接入点412和SGW 414之间延伸的承载信道424(例如,“S1-U接口”)、

以及SGW 414和PGW 416之间延伸的承载信道426(例如,“S5接口”)。在一些实施例中,RAN 410和EPC 420形成的无线网络的物理拓扑可使用虚拟网络430映射到虚拟拓扑。在这些实施例中,承载路径451可对应于通过虚拟网络430延伸的虚拟路径452。

[0037] 如图所示,实施例的无线网络架构400沿着承载路径451提供多级接入保护。具体地,WN特定的密钥适于提供在无线连接415上的接入保护,而UE特定的密钥适于提供在承载信道424和/或承载信道426上的接入保护。在一些实施例中,还可以使用客户隐私信息提供端到端保护。另外,可以使用虚拟网络特定的(VN特定的)密钥材料或VN特定的密钥(简称)提供虚拟网络保护。尽管无线网络架构400描述为提供多级接入保护,本公开的方面并不仅限于此。例如,无线网络400可适于提供单级接入保护,例如不用使用UE特定的密钥信息,通过使用WN特定的密钥来加密/解密在无线连接415上通信的数据。这提供了更有效的切换,因为不用交换任何密钥就可以发生切换。

[0038] 图5示出了用于管理无线网络域510中网络接入密钥的无线网络安全架构500的实施例。如图所示,无线网络域510包括多个无线节点515以及无线网络接入链路保护密钥控制器509或WN密钥控制器509(简称)。WN密钥控制器509向本地无线节点515发送WN特定的密钥。无线节点515在UE认证之后向UE 505分发该WN特定的密钥,此后,该WN特定的密钥用于加密/解密无线接入链路上通信的数据。在一实施例中,WN特定的密钥在所述多个无线节点515上被同步,使得UE 505可在所述多个无线节点515之间被切换,而在切换期间不用传送WN特定的密钥。所述多个无线节点515可由相同网络运营商管理。

[0039] 图6示出了用于管理多个无线网络域610、620上的网络接入密钥的无线网络安全架构600的实施例。无线网络域610、620可由相同或不同运营商管理,并可包括适于向UE 605、606提供无线接入的无线节点615、625。在无线连接建立之前,密钥控制器609向无线节点615、625分发WN特定的密钥。UE认证之后,无线节点615、625向UE 605、606分发WN特定的密钥。在无线网络域610、620之间共享WN特定的密钥,使得在切换期间不用传送WN特定的密钥就可以进行域间切换。

[0040] 本公开的各个方面提供了用于管理UE特定的密钥的安全架构。图7示出了用于管理无线网络域710、720之间UE特定的密钥材料的无线网络架构700的实施例。如图所示,网络架构700包括位于各自无线网络域710、720的UE特定的SGW 714、SGW 724,与各自无线网络域710、720相关联的WN保护控制器718、728,密钥管理实体736以及认证中心740。

[0041] 对无线网络架构700中UE特定的密钥材料的管理以八个步骤的顺序进行描述,当UE 705启动链路建立过程时,可触发这些步骤。在第一步骤(1)中,UE 705由认证中心740授权和认证。在一些实施例中,认证中心740包括负责例如UE特定的名称、认证、授权和/或计费中心等各种UE特定的任务的全局实体。在其他实施例中,认证中心740包括UE 705的归属网络的控制中心。

[0042] 在第二步骤(2)期间,认证中心740向密钥管理实体736提供UE特定的密钥或用于导出UE特定的密钥的材料。接着,密钥管理实体在第三步骤(3)期间向WN保护控制器718提供UE特定的密钥。WN保护控制器718在第四步骤(4)期间向UE特定的SGW 714分发UE特定的密钥,以及在第五步骤(5)期间向UE 705分发UE特定的密钥。

[0043] 在第六步骤期间,UE 705从无线网络域710移动到无线网络域720,从而触发切换。切换的结果是,在第七步骤(7)期间,从WN保护控制器718向WN保护控制器728传送UE特定的

密钥。WN保护控制器728负责第二无线域720中的密钥分发，并且在第八步骤(8)期间向UE特定的SGW分发UE特定的密钥。

[0044] 本公开的各个方面提供适于为机器对机器(M2M)业务相关的业务流提供接入保护的业务特定的密钥。图8示出了为在多个网络域801、802、803上传输的M2M业务相关的业务流提供接入保护的网络架构800的实施例。在本实例中，第一M2M业务注册到M2M客户810，并且第二M2M业务注册到M2M客户820。可使用业务特定的密钥信息加密/解密M2M相关的业务流。例如，在将业务流通信到M2M业务客户810之前，机器811、812可使用第一业务特定的密钥加密数据，而在将业务流通信到M2M业务客户820之前，机器821、822可使用第二业务特定的密钥加密数据。

[0045] 可以在不同网络位置过滤M2M业务相关的业务流。例如，具有相对稳定拓扑(例如，不频繁增加/去除机器)的网络可在网络边缘，例如在各自的机器和M2M客户上执行业务流过滤。其他网络可在网络域801-803中的网关831-833的其中一个上过滤M2M业务相关的业务流。例如，可在例如虚拟业务特定的SGW等业务特定的网关处执行过滤。也可以由PGW或虚拟网络域中的网关执行过滤。对M2M相关的业务流进行过滤的实体可尝试使用相应的业务特定的密钥解密在业务流流量中的分组，接着丢弃实体不能成功解密的任何分组。

[0046] 本公开的各个方面提供了用于管理业务特定的密钥材料的架构。图9示出了用于管理网络域910中业务特定的密钥材料的无线网络架构900的实施例。如图所示，网络架构900包括位于网络域910中业务特定的SGW 914，与网络域910相关联的保护控制器918、密钥管理实体936、认证中心940和M2M客户950。

[0047] 对无线网络架构900中业务特定的密钥材料的管理以八个步骤的顺序进行描述，当M2M客户950启动M2M业务注册时，可触发这些步骤。在第一步骤(1)中，M2M客户950由认证中心940授权和认证，认证中心可以是负责多种M2M业务特定的任务的全局实体或M2M客户950的归属网络中的控制中心。

[0048] 在第二步骤(2)期间，认证中心940向密钥管理实体936提供业务特定的密钥或用于导出业务特定的密钥的材料。接着在第三步骤(3)期间，密钥管理实体向保护控制器918提供业务特定的密钥，并且在第四步骤(4)期间，保护控制器918向业务特定的SGW914分发业务特定的密钥。在第五步骤(5)期间，机器905尝试注册为M2M业务的参与者，其可包括向业务特定的SGW 914发送指定业务名称的请求。当机器905通电或以其他方式被用户配置时，可触发该注册尝试。在第六步骤(6)期间，从业务特定的SGW 914向M2M客户950转发业务请求，M2M客户950可维护用于认证允许参与M2M业务的设备/机器的安全信息。在第七步骤(7)期间，M2M客户950向保护控制器918通知机器905已经被认证，提示保护控制器918在第八步骤(8)期间向机器905分发业务特定的密钥。

[0049] 本公开的各个方面使用群组特定的密钥向专用社交网络的成员之间通信的业务流提供接入保护。图10示出了用于向例如专用社交网络的公共群组的成员之间通信的业务流提供接入保护的网络架构1000的实施例。如图所示，实施例的网络架构1000包括用于向注册到公共网络或群组，例如专用社交网络/群组的无线设备1005、1006、1007提供无线接入的无线网络域1010、1020。如图所示，无线网络域1010、1020包括适于向无线设备1005、1006、1007提供无线接入的接入点1012、1022，以及服务网关1014、1024，和分组网关1016、1026。在一些实施例中，经由互联网1030向远程端1036(例如应用服务器等)传输群组相关

的业务流。也可在群组成员1005、1006、1007之间通信群组相关的业务流。成员1005、1006、1007以及远程端1036可使用群组特定的密钥加密/解密群组相关的业务流。

[0050] 图11示出了用于管理网络域1110中群组特定的密钥材料的无线网络架构1100的实施例。如图所示，网络架构1100包括位于网络域1110中的群组特定的SGW 1114、与网络域1110相关联的保护控制器1118、密钥管理实体1136、以及认证中心1150。对无线网络架构1100中群组特定的密钥材料的管理以八个步骤的顺序进行描述，当群组头设备1105启动专用群组/网络注册时，可触发这些步骤。

[0051] 在第一步骤(1)中，头设备1105由认证中心1150授权和认证。认证中心1150可以是负责多种群组特定的任务的全局实体，或头设备1105的归属网络的控制中心。在第二步骤(2)中，密钥管理实体1136创建群组特定的密钥。接着在第三步骤(3)中，密钥管理实体1136向WN保护控制器1118提供群组特定的密钥，并且在第四步骤(4)期间，WN保护控制器1118向群组特定的SGW 1114发送群组特定的密钥。在第五步骤(5)期间，群组成员1106通过向认证中心1150发送注册请求尝试注册为专用网络的参与者。在第六步骤中，认证中心1150向头设备1105转发该请求，在第七步骤中向WN保护控制器1118发送认证确认。在第八步骤(8)中，WN保护控制器1118向群组成员1106发送群组特定的密钥，在此之后，群组特定的密钥用来加密/解密群组相关的业务流。

[0052] 本公开的各个方面提供了几个益处。例如，实施例的技术可以为无线网络接入提供灵活的保护方案，并减少切换期间传送的链路保护材料的量。实施例也可提供统一的安全控制并提供虚拟用户特定的SGW、虚拟业务特定的SGW和/或群组特定的SGW处的安全控制收敛(convergence)。本公开的各个方面可以向无线回程链路提供接入保护，以及防止恶意节点攻击客户业务流。在一实施例中，无线网络域中的节点可使用回程(BH)密钥，来加密/解密无线回程接口上的通信。对不同类型的密钥的管理可彼此独立进行。

[0053] 可以在相应链路、接口或信道上以任一方向使用各种密钥(例如UE特定的密钥、WN特定的密钥等)进行加密/解密。例如，WN特定的密钥可用来执行无线接入链路上通信的上行链路数据的加密/解密，以及执行无线接入链路上通信的下行链路数据的加密/解密。

[0054] 本公开的各个方面提供了一种无线网络接入保护的方法。该方法包括：获得分配给无线网络的无线网络(WN)特定的密钥，建立基站和用户设备(UE)之间的无线接口，以及在无线接口上从UE接收加密的数据。加密的数据至少具有第一层加密和第二层加密。该方法进一步包括：使用WN特定的密钥部分地解密该加密的数据，以便从加密的数据除去第一层加密，从而获得包括第二层加密的部分解密的数据，并且向WN中的网关转发该部分解密的数据。在一些实施例中，网关包括用户特定的服务网关(SGW)。在一些实施例中，用户特定的SGW适于使用UE特定的密钥进一步解密该部分解密的数据，以便从解密的数据中除去第二层加密。UE特定的密钥可以不同于WN特定的密钥。在一些实施例中，用户特定的SGW和基站共同处于相同的网络侧设备上。在另一些实施例中，用户特定的SGW和基站处于不同的网络侧设备上。在一些实施例中，该方法进一步包括：在无线接口上接收分组，使用WN特定的密钥尝试部分解密该分组；以及当部分解密该分组的尝试不成功时，丢弃该分组。该方法可进一步包括：当部分地解密该分组的尝试成功时，向用户特定的SGW转发该分组。用户特定的SGW适于使用UE特定的密钥尝试进一步解密该分组，并且适于当使用UE特定的密钥进一步解密该分组的尝试失败时，丢弃该分组。在一些实施例中，第一层加密为无线接口提供接

入保护，并且第二层加密为UE和用户特定的SGW之间延伸的承载信道提供接入保护。在一些实施例中，向无线网络中的一组基站分发WN特定的密钥，使得该组基站中的基站之间发生切换，而在切换期间，不用交换WN特定的密钥。向一群组无线网络分配WN特定的密钥，使得该群组无线网络中的无线网络之间发生切换，而在切换期间，不用交换WN特定的密钥。还提供了一种执行该方法的装置。

[0055] 本公开的各个方面提供了一种在无线网络中分发密钥的方法。在本实例中，该方法包括：在WN密钥控制器上生成无线网络(WN)特定的密钥。向第一无线网络分配WN特定的密钥。该方法进一步包括：向在第一无线网络中的基站分发WN特定的密钥，以便在基站和接入该无线网络的用户设备(UE)之间建立的无线接入接口上提供接入保护。在一些实施例中，向至少包括第一无线网络和第二无线网络的一群组无线网络分配WN特定的密钥。在这些实施例中，该方法进一步包括：向第二无线网络中的基站分发WN特定的密钥。在一些实施例中，该方法进一步包括：在第一时间段结束时，更新WN特定的密钥，以及在第二时间段开始时，向第一无线网络中的基站分发更新的WN特定的密钥。在第一时间段期间，WN特定的密钥向无线接入接口提供接入保护，并且在第二时间段期间，更新的WN特定的密钥向无线接入接口提供接入保护。还提供了一种执行该方法的装置。WN特定的密钥可被分发到UE没有连接的接入点，减轻了在基站到基站切换过程中包括密钥信息的需求。同时，如果使用不同的密钥(例如，UE特定的密钥)加密到网关的UE业务流时，UE业务流在其被网关接收前仍被保护免于入侵。

[0056] 本公开的各个方面提供了一种密钥管理架构。在本实例中，该密钥管理架构包括：无线网络(WN)保护控制器，适于获得分配给接入无线网络的UE的用户设备(UE)特定的密钥，并且向该无线网络中的服务网关(SGW)分发该UE特定的密钥。该UE特定的密钥适于对在UE和SGW之间延伸的承载信道提供接入保护。在一些实施例中，该WN保护控制器从第三方密钥管理实体获得UE特定的密钥。该第三方密钥管理实体由独立并区别于所述无线网络的运营商的第三方管理员运营。在一些实施例中，密钥管理架构还包括WN密钥控制器，适于生成向无线网络分配的WN特定的密钥，以及向无线网络中的基站分发WN特定的密钥。该WN特定的密钥可独立并区别于UE特定的密钥。该WN特定的密钥适于对在基站和接入该无线网络的用户设备(UE)之间建立的无线接入接口提供接入保护。

[0057] 本公开的各个方面提供了一种用于认证移动设备的方法。在本实例中，该方法包括：在WN保护控制器处，从第三方密钥管理实体接收UE特定的密钥，该WN保护控制器被指派在整个无线网络中分发密钥。该第三方密钥管理实体由不同于无线网络的运营商的第三方管理员运营。该方法进一步包括：识别对应由UE特定的密钥指定的UE标识符的无线网络域；以及向无线网络域中的服务网关(SGW)分发UE特定的密钥。UE特定的密钥适于对在UE和SGW之间延伸的承载信道提供接入保护。在一些实施例中，SGW为用户特定的SGW。还提供了一种执行该方法的装置。

[0058] 本公开的各个方面提供了一种提供业务特定的接入保护的方法。在本实例中，该方法包括：识别与机器对机器(M2M)客户相关联的M2M业务；在SGW处接收分配给该M2M业务的业务特定的密钥；以及从网络设备接收分组。该分组与M2M业务相关。该方法进一步包括：使用业务特定的密钥尝试解密该分组；以及当解密该分组的尝试不成功时，丢弃该分组。在一些实施例中，SGW为业务特定的SGW。在一些实施例中，该方法进一步包括：当解密该分组

的尝试成功时,向M2M客户转发解密的分组。在一些实施例中,向M2M业务分配业务特定的密钥,并且该业务特定的密钥并不特定于该网络设备。在一些实施例中,在M2M客户认证网络设备之后,向网络设备提供业务特定的密钥。还提供了一种执行该方法的装置。

[0059] 本公开的各个方面提供了一种群组特定的接入保护的方法。在本实例中,该方法包括:识别专用网络,在SGW处接收分配给该专用网络的群组特定的密钥,接收寻址到属于该专用网络的网络设备的分组,以及使用该群组特定的密钥尝试解密该分组。该方法进一步包括:当解密该分组的尝试不成功时,丢弃该分组。在一些实施例中,该SGW为业务特定的SGW。在一些实施例中,公共群组包括专用社交网络。在一些实施例中,向专用网络分配密钥,并且该密钥并不特定于任何一个单独的网络设备。还提供了一种执行该方法的装置。

[0060] 图12为可用于实现此处公开的设备和方法的处理系统的框图。特定设备可使用示出的所有组件,或组件的仅仅一个子集,并且集成水平可随不同设备而变化。此外,设备可含有组件的多个实例,例如,多个处理单元、处理器、存储器、发送器、接收器等。处理系统可包括处理单元,该处理单元配备有一个或多个输入/输出设备、例如,扬声器、麦克风、鼠标、触摸屏、小键盘、键盘、打印机、显示器等。处理单元可包括连接到总线的中央处理单元(CPU)、存储器、大容量存储设备、视频适配器,以及I/O接口。

[0061] 总线可为一个或多个任何类型的几个总线架构,包括存储器总线或存储器控制器,外围总线、视频总线等。CPU可包括任何类型的电子数据处理器。存储器可包括任何类型的非瞬态系统存储器,诸如静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、同步DRAM(SDRAM)、只读存储器(ROM)或其组合等。在一实施例中,存储器可包括启动时使用的ROM,执行程序时使用的用于程序和数据存储的DRAM。

[0062] 大容量存储设备可包括用于存储数据、程序及其它信息并用于通过总线使数据、程序及其它信息可访问的任何类型的非瞬态存储设备。大容量存储设备可包括,例如,一个或多个固态驱动器、硬盘驱动器、磁盘驱动器、光盘驱动器等。

[0063] 视频适配器以及I/O接口提供将外部输入和输出设备耦合到处理单元的接口。如图所示,输入和输出设备的实例包括耦合至视频适配器的显示器,以及耦合至I/O接口的鼠标/键盘/打印机。其他设备可耦合至处理单元,并且可使用附加的或更少的接口卡。例如,可使用诸如通用串行总线(USB)(未示出)的串行接口为打印机提供接口。

[0064] 处理单元还包括一个或多个网络接口,这些网络接口可包括诸如以太网线缆之类的有线连接,和/或接入节点或不同网络的无线连接。网络接口使得处理单元经由网络与远程单元进行通信。例如,网络接口可经由一个或多个发送器/发送天线和一个或多个接收器/接收天线提供无线通信。在一实施例中,处理单元耦合至局域网或广域网以便与远程设备进行数据处理和通信,远程设备例如其他处理单元、互联网、远程存储设施等。

[0065] 图13示出了通信设备1300的实施例的框图,通信设备1300相当于如上所述的一个或多个设备(例如,UE、eNB、控制器等)。通信设备1300可包括可以(或不是)按照图13所示排列的处理器1304、存储器1306以及多个接口1310、1312、1314。处理器1304可以是能够进行计算和/或其他处理相关任务的任何组件,并且存储器1306可以是能够存储用于处理器1304的程序和/或指令的任何组件。接口1310、1312、1314可以是使得通信设备1300与其他设备进行通信的任何组件或组件集合。

[0066] 尽管已经详细描述了本发明,但应理解,可以在不偏离所附权利要求限定的本公

开的精神和范围的情况下,做出各种改变、替换和变更。此外,本公开的范围并不意图受限于此处描述的具体实施例,正如本领域普通技术人员可以轻易地从本公开意识到一样,目前存在的或以后待开发的过程、机器、制造、物质组成、手段、方法或步骤可与此处描述的相应实施例实现基本相同的功能或达到基本相同的结果。因此,所附权利要求旨在其范围内包括这些过程、机器、制造、物质组成、手段、方法或步骤。

[0067] 虽然已结合示例性实施例对本发明进行了描述,但是本发明并不旨在被解释为限于此。参照这些描述,对示例性实施例和本发明的其它实施例进行各种修改和组合对本领域技术人来讲是显而易见的。因此,所附权利要求涵盖任何这些修改或实施例。

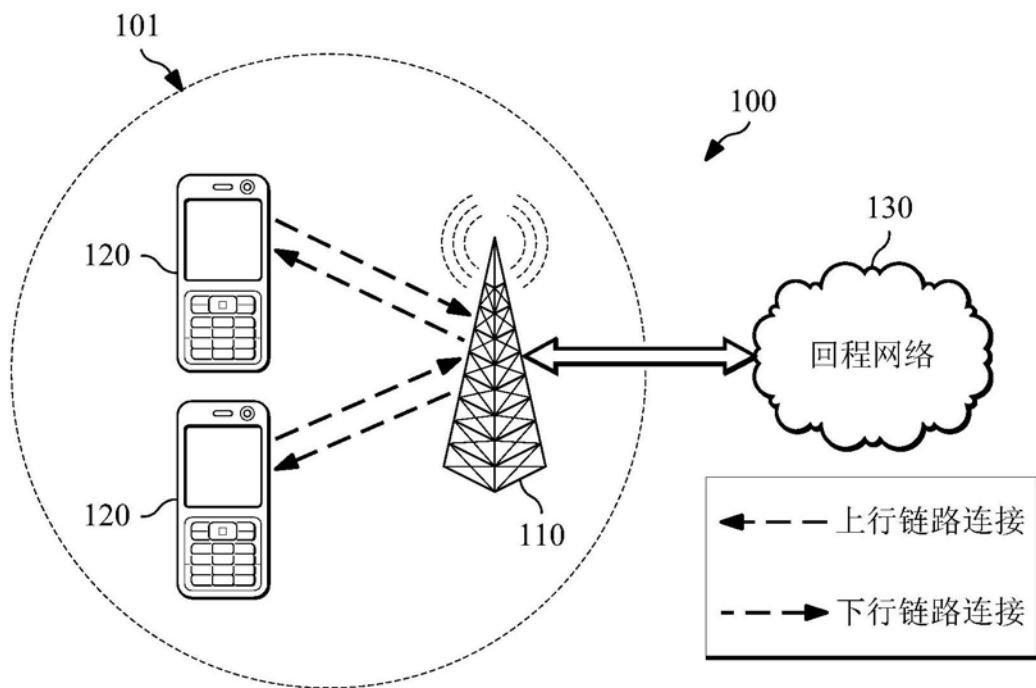


图1

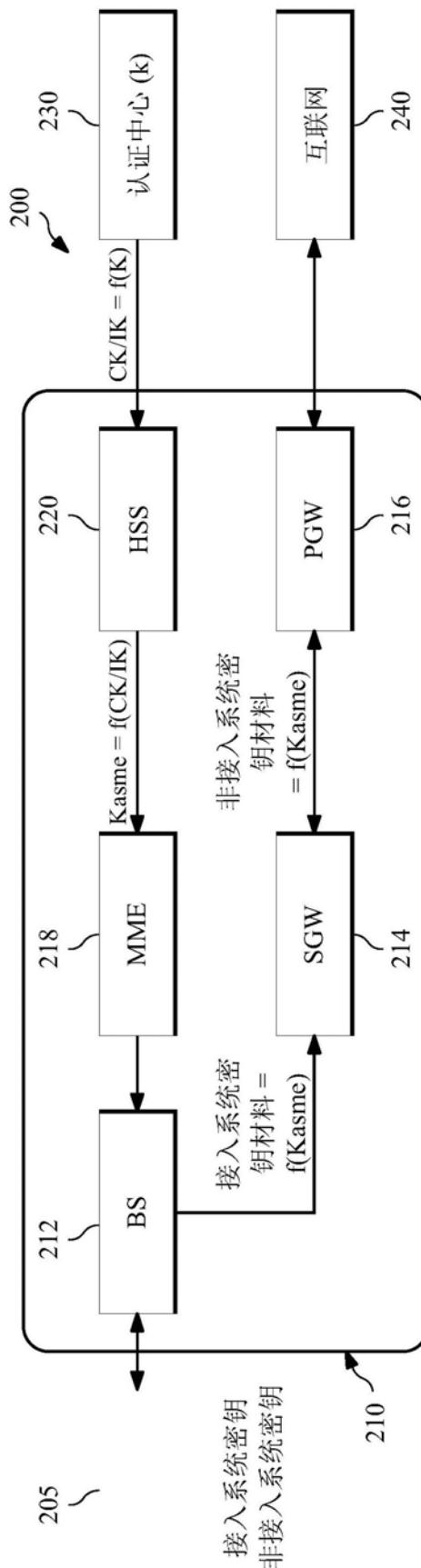


图2

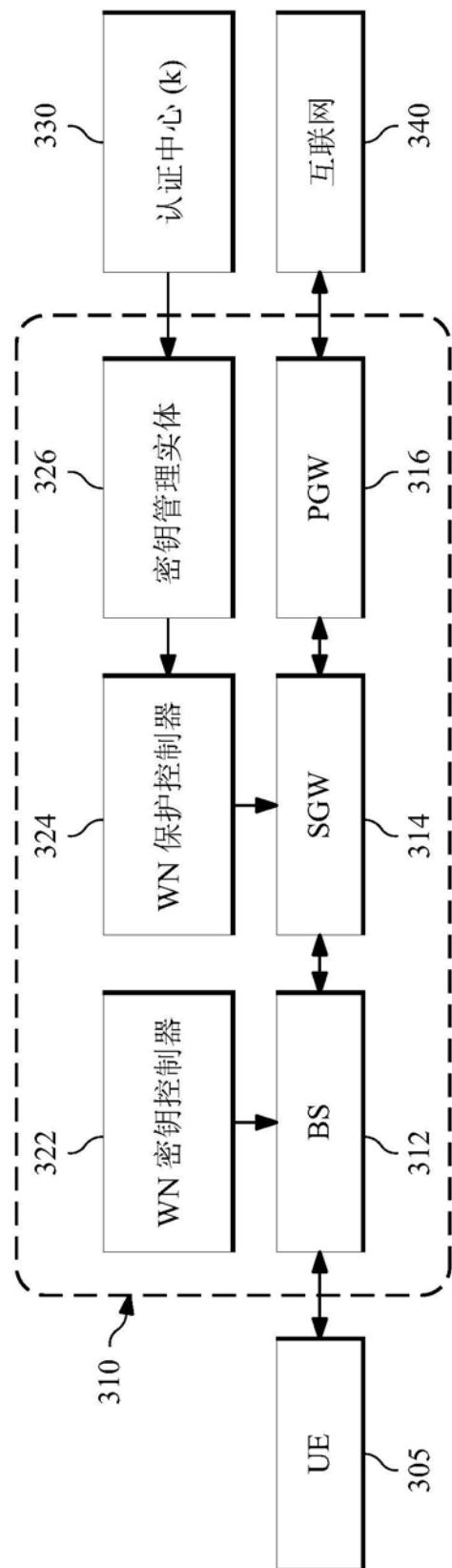


图3

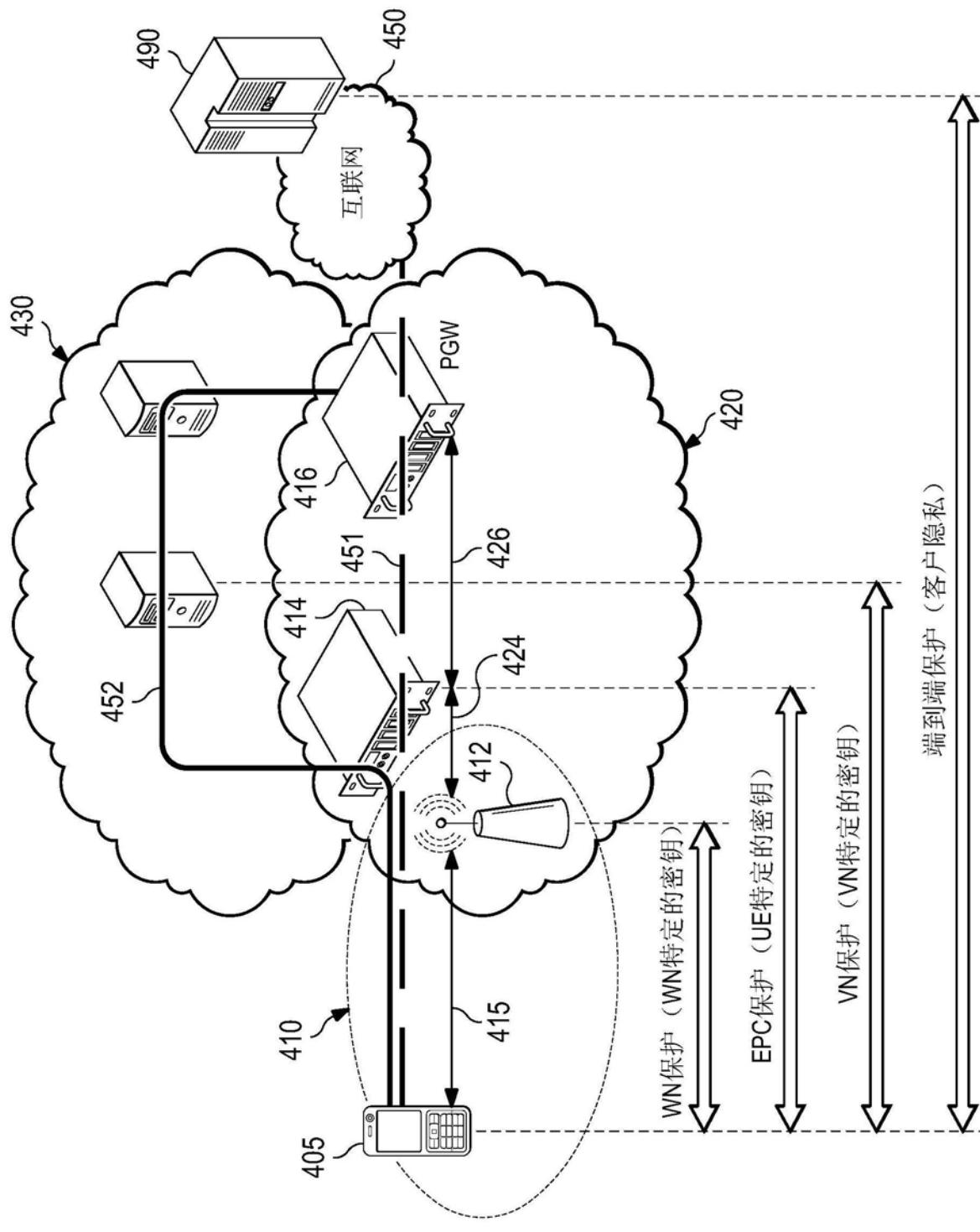


图4

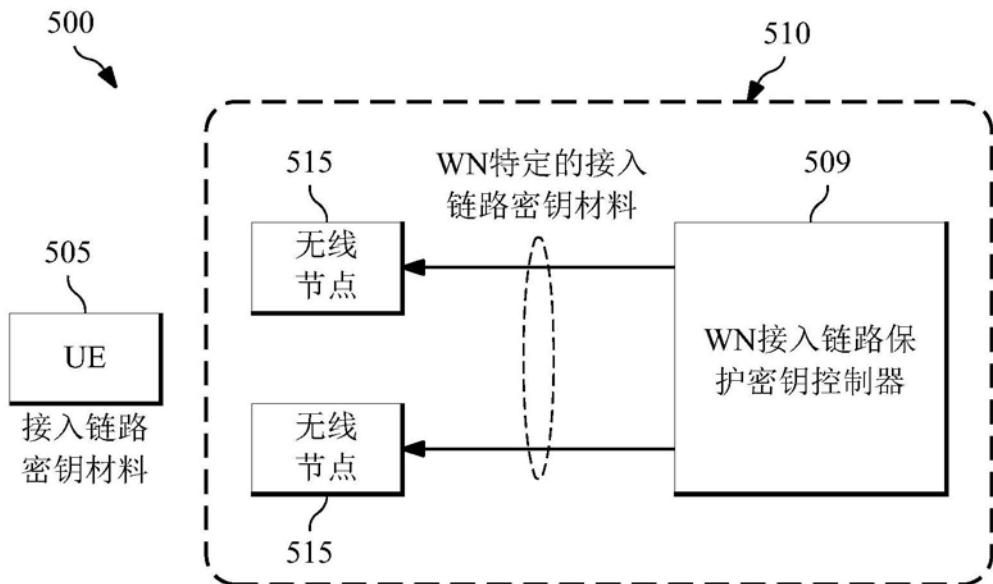


图5

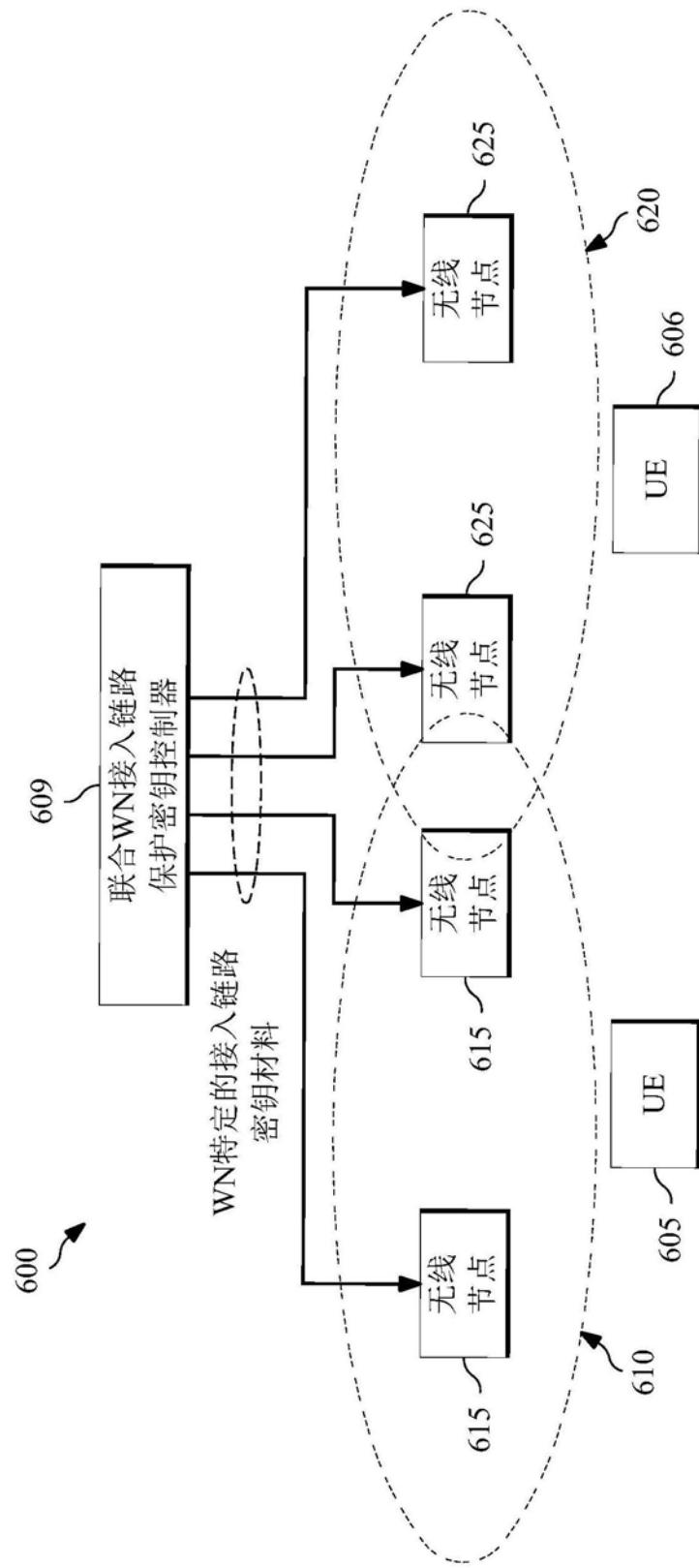


图6

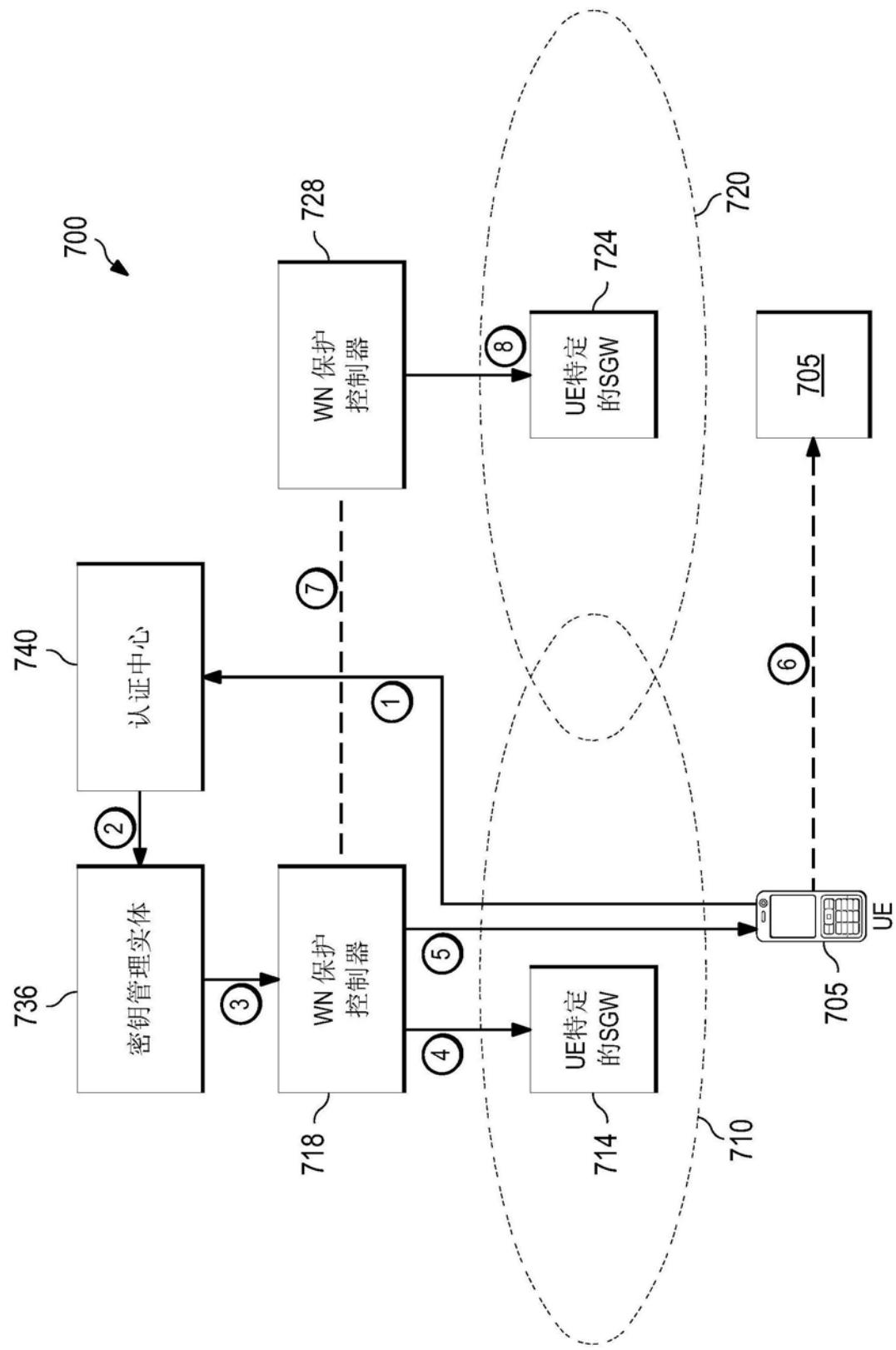


图7

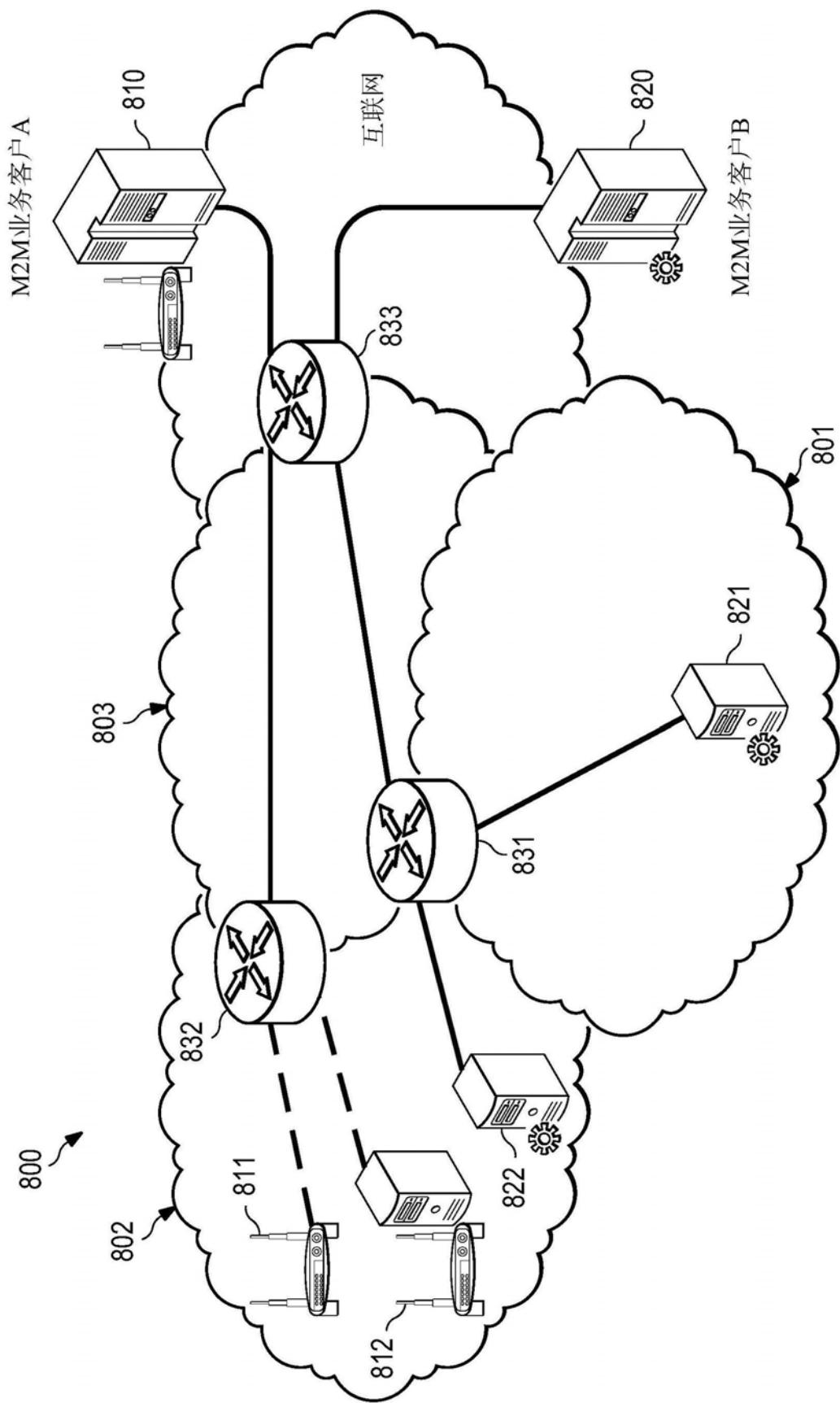


图8

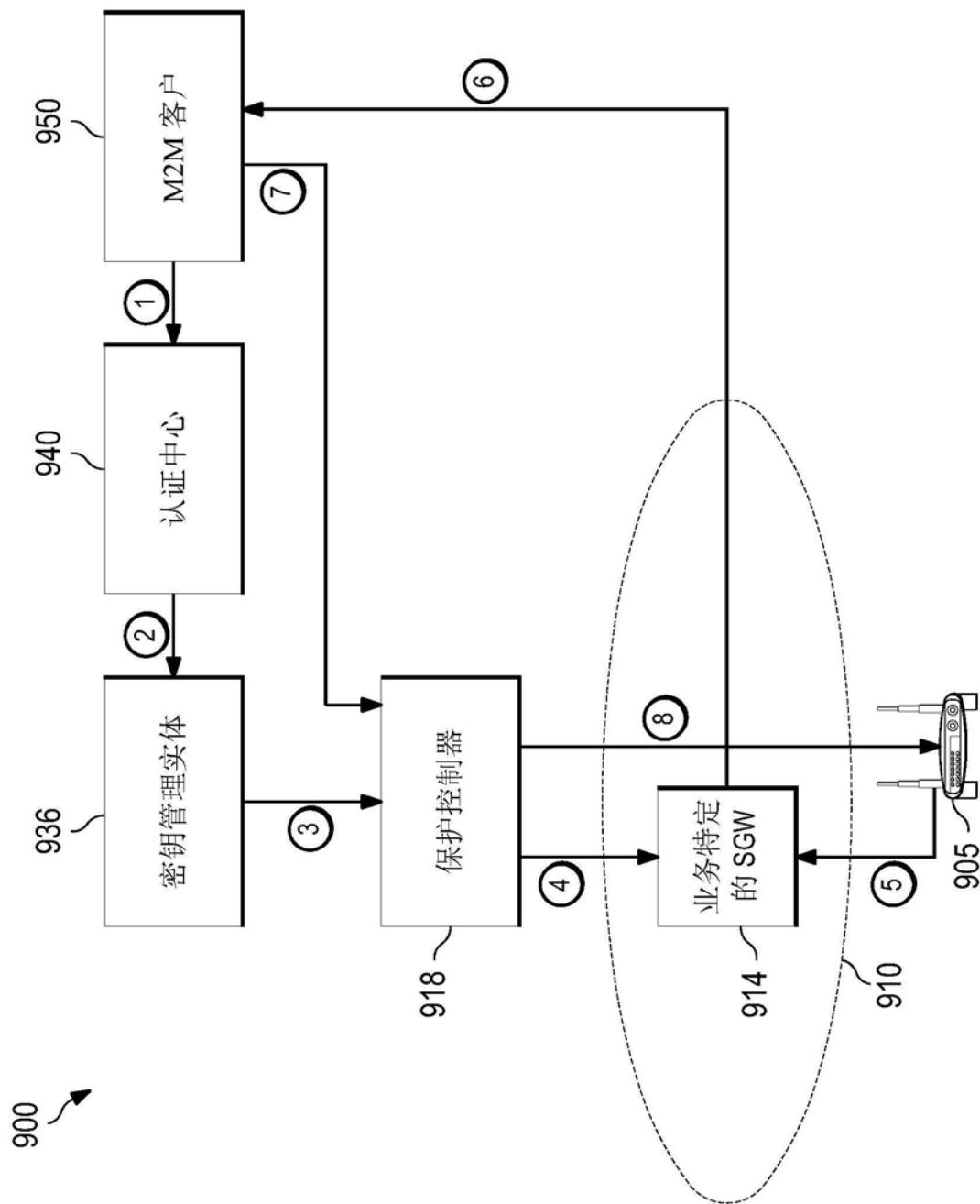


图9

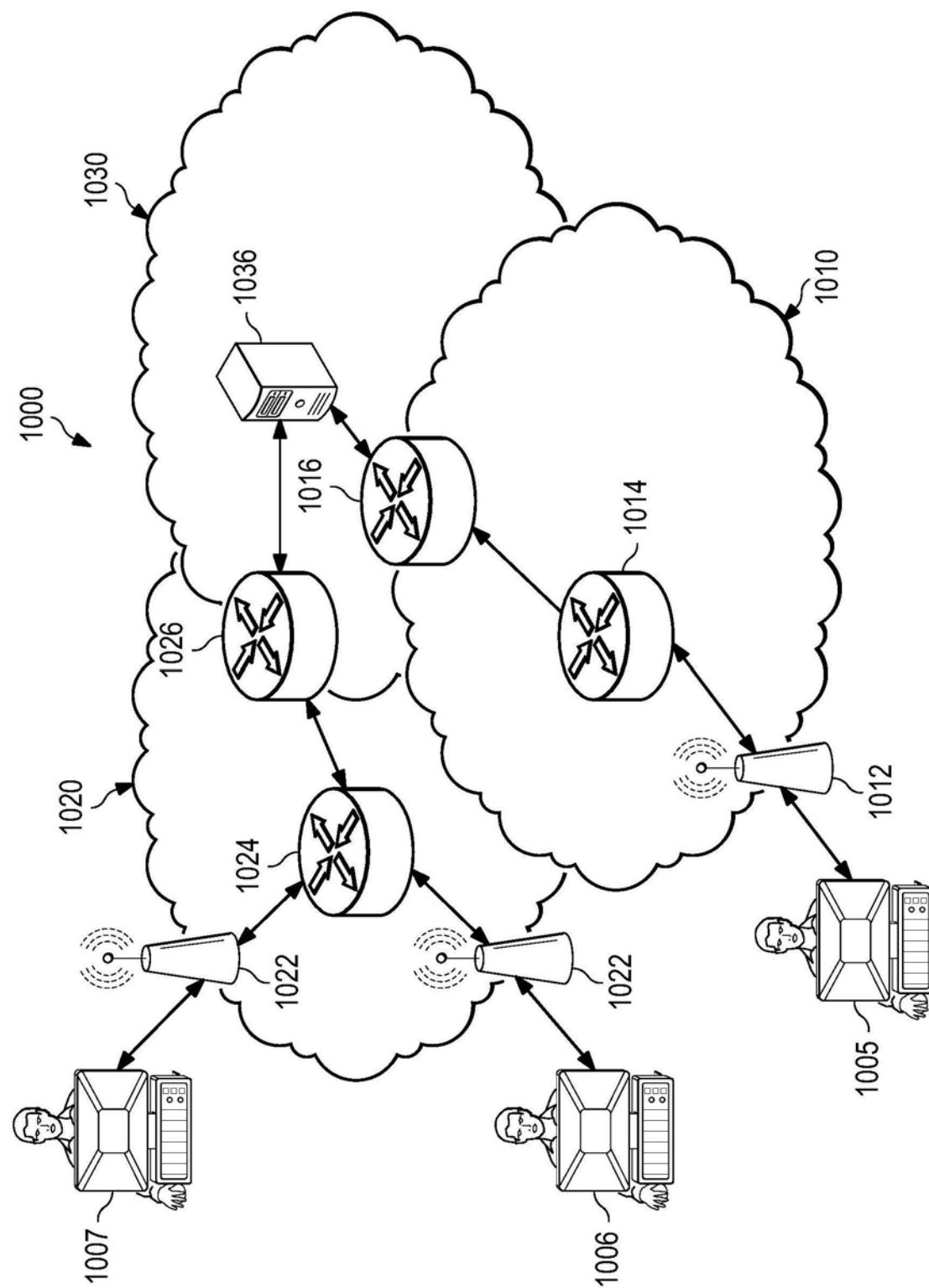


图10

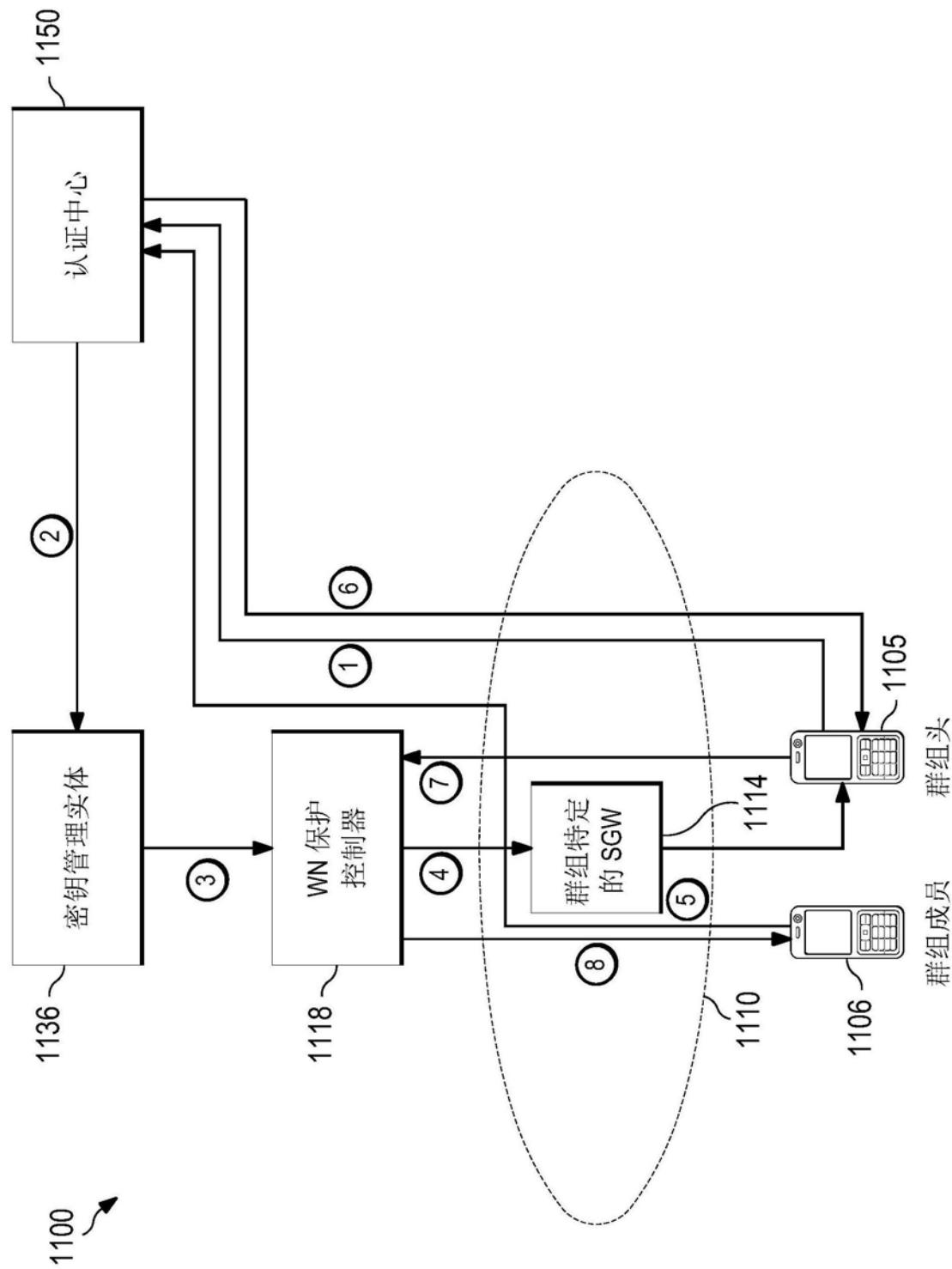


图11

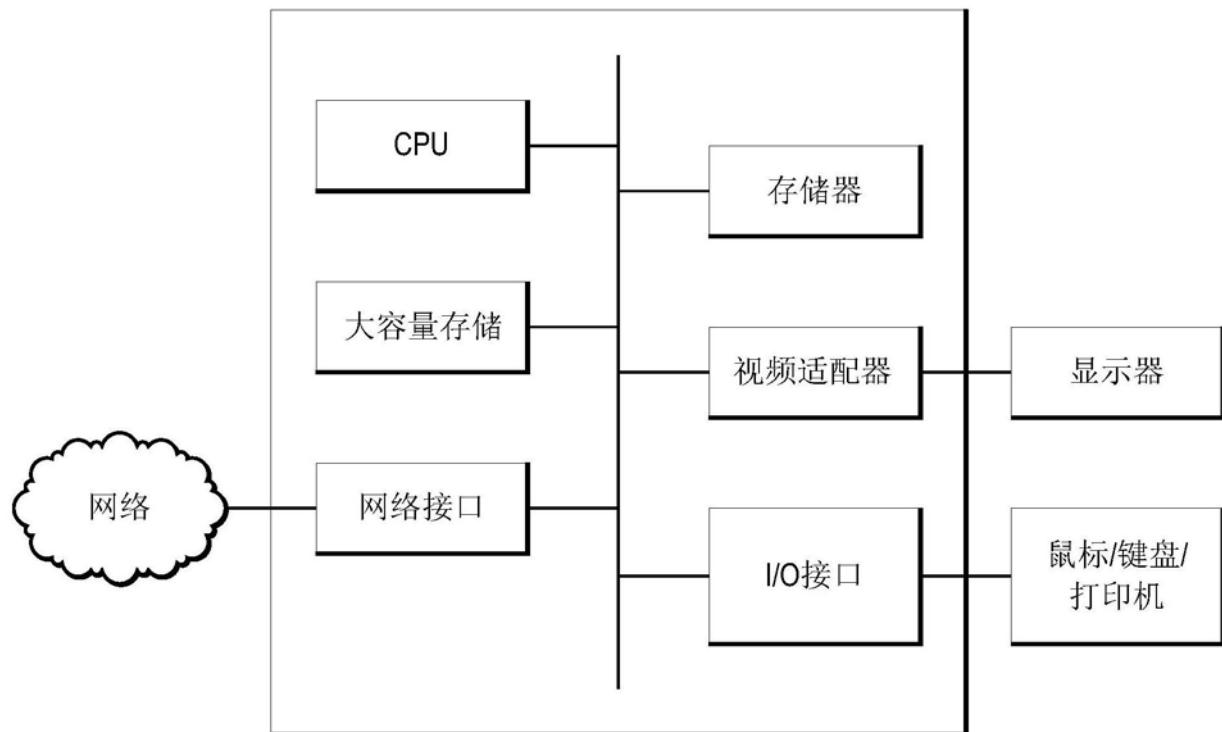


图12

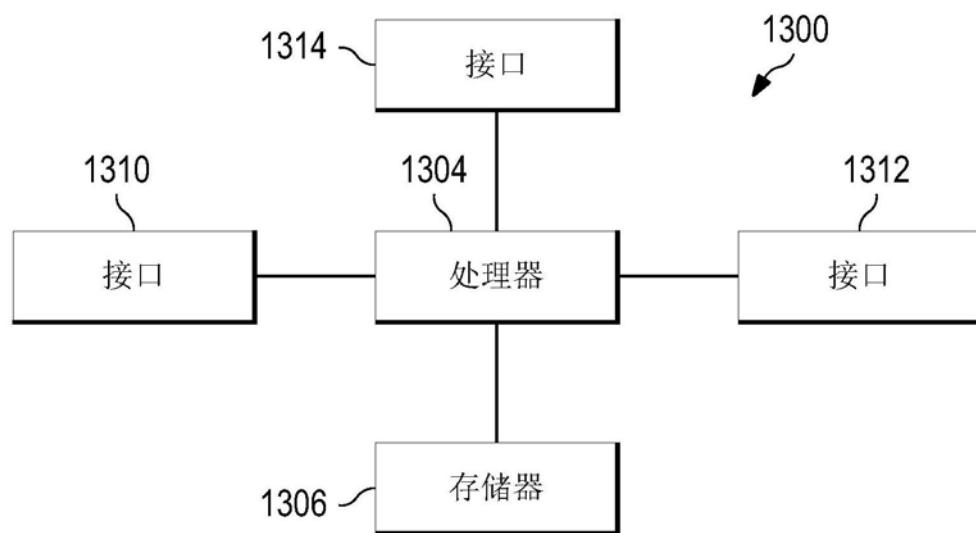


图13