(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110999270 B
(45)授权公告日 2022.07.08

(21)申请号 201880050144.4
(22)申请日 2018.08.03
(65)同一申请的已公布的文献号
申请公布号 CN 110999270 A
(43)申请公布日 2020.04.10
(30)优先权数据
17184733.8 2017.08.03 EP
(85)PCT国际申请进入国家阶段日
2020.02.03
(86)PCT国际申请的申请数据
PCT/EP2018/071160 2018.08.03
(87)PCT国际申请的公布数据
WO2019/025603 EN 2019.02.07
(73)专利权人 IPCOM两合公司
地址 德国普拉赫
(72)发明人 A·卢夫特 M·汉斯
(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 郭毅
(51)Int.Cl.
H04W 4/24(2009.01)
H04W 12/0431(2021.01)
H04W 12/06(2021.01)
H04W 12/106(2021.01)
H04M 15/00(2006.01)
(56)对比文件
US 2002161723 A1,2002.10.31
US 2012100832 A1,2012.04.26
CN 1581183 A,2005.02.16
CN 101047978 A,2007.10.03
CN 101005359 A,2007.07.25
CN 101047505 A,2007.10.03
CN 101047505 A,2007.10.03
EP 1642437 B1,2011.08.31
审查员 马婷

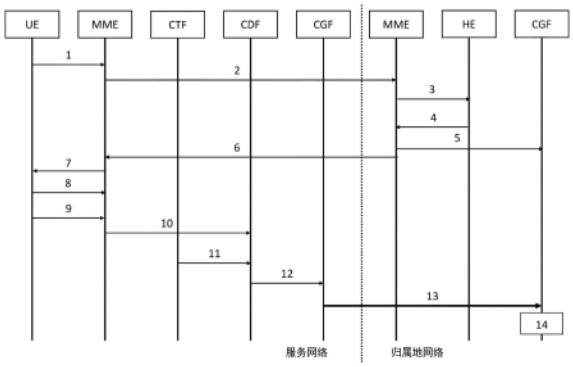
权利要求书1页 说明书6页 附图2页

(54)发明名称

适用于发送服务验证消息的用户设备

(57)摘要

本发明提供一种对由移动通信用户设备、UE装置执行的交易进行鉴权的方法，该方法在UE装置与受访网络的移动管理实体之间已经执行鉴权和密钥协商过程，以便在UE装置与受访网络之间建立安全上下文，该方法包括：将服务验证消息从UE装置发送给受访网络，该服务验证消息已经由UE装置在使用完整性保护密钥的情况下进行数字签名，所述完整性保护密钥在UE装置与归属网络之间所共享；将服务验证消息从受访网络传输给归属网络。



CN 110999270 B

1.一种对由移动通信用户设备、UE装置执行的交易进行鉴权的方法,所述方法在所述UE装置与受访网络的移动管理实体之间已经执行鉴权和密钥协商过程,以便在所述UE装置与所述受访网络之间建立安全上下文,所述方法包括:

将服务验证消息从所述UE装置发送给所述受访网络(9),所述服务验证消息是来自所述UE装置的用于验证所述受访网络对服务的建立或提供的消息,验证服务消息已经由所述UE装置在使用完整性保护密钥的情况下进行数字签名,所述完整性保护密钥仅在所述UE装置与归属网络之间所共享;

将所述服务验证消息从所述受访网络传递给所述归属网络(10)。

2.根据权利要求1所述的方法,其中,通过执行第二鉴权和密钥协商过程来获得所述完整性保护密钥(7),在所述第二鉴权和密钥协商过程中,所述归属网络提供鉴权向量,所述鉴权向量既不包含会话密钥层次结构的根也不包含用于完整性保护的会话密钥。

3.根据权利要求1所述的方法,其中,通过执行第二鉴权和密钥协商过程来获得所述完整性保护密钥,在所述第二鉴权和密钥协商过程中,所述归属网络仅向所述受访网络提供质询以及对所述质询的预期响应。

4.根据权利要求1所述的方法,其中,在使用从所述归属网络中的现有密钥导出的完整性保护密钥的情况下建立所述UE装置与所述受访网络之间的安全上下文。

5.根据以上权利要求中任一项所述的方法,其中,所述服务验证消息包括时间戳和消息序列号中的至少一个。

6.根据权利要求1至4中任一项所述的方法,其中,响应于请求来发送所述服务验证消息(6)。

7.根据权利要求6所述的方法,其中,所述请求作为非接入层消息的一部分进行发送。

8.根据权利要求1至4、7中一项所述的方法,其中,所述服务验证消息由所述UE装置自主地发送。

9.根据权利要求1至4、7中任一项所述的方法,其中,由所述受访网络将所述服务验证消息与计费数据记录相关联,并且将所关联的消息发送给所述归属网络的计费网关功能。

适用于发送服务验证消息的用户设备

技术领域

[0001] 本发明涉及在移动通信系统中由用户设备(UE)发送服务验证消息。

背景技术

[0002] GSM、UMTS和EPC(演进分组核心)网络提供在承载、子系统和服务级别上实现离线和/或在线计费机制的功能。为了支持这些计费机制,网络在上述三个级别上执行资源使用的实时监控,以便探测相关的可计费事件。

[0003] 在离线计费中,在资源使用已经发生之后,将资源使用从网络报告给计费域(BD)。在在线计费中,在授予使用所请求的网络资源的许可之前,查询位于在线计费系统(OCS)中的订户账户。

[0004] 网络资源使用的典型示例是确定持续时间的语音呼叫、确定数据量的传输或确定大小的多媒体消息的提交。网络资源使用请求可以由UE或由网络发起。

[0005] 离线计费是如下过程:在该过程中,在资源使用的同时收集关于网络资源使用的计费信息。然后,通过一系列逻辑计费功能传递计费信息。在该过程结束时,由网络生成计费数据记录(CDR)文件,然后将该文件传输给网络运营商的计费域,以便进行订户出账单和/或运营商间账户处理(或附加功能,例如由运营商自行决定的统计)。BD通常包括后处理系统——例如运营商的计费系统或计费中介设备。总之,离线计费是如下机制:在该机制中,计费信息不实时地影响所提供的服务。

[0006] 在线计费是如下过程:在该过程中,以与离线计费相同的方式,在资源使用的同时收集关于网络资源使用的计费信息。然而,必须在实际资源使用发生之前由网络获得网络资源使用的权限。OCS应网络的请求授予这种权限。

[0007] 当接收到网络资源使用请求时,网络收集相关的计费信息,并且实时地向OCS生成计费事件。然后,OCS返回适当的资源使用权限。资源使用权限可能在其范围(例如数据量或持续时间)方面受到限制,因此,只要用户的网络资源使用持续存在,就可能需要时不时地更新权限。

[0008] 在线计费是一种能够实时地影响所提供的服务的机制,因此需要计费机制与网络资源使用控制的直接交互。

[0009] 计费触发功能(CTF)基于对网络资源使用的观察生成计费事件。计费数据功能(CDF)通过所谓的Rf参考点从计费触发功能接收计费事件。然后,CTF使用计费事件中包含的信息建立CDR。由CTF产生的CDR通过所谓的Ga参考点被立即传输给计费网关功能(CGF)。CGF充当3GPP网络和BD之间的网关。该网关使用所谓的Bx参考点将CDR文件传输给BD。在线计费功能(OCF)由两个不同的模块组成——即基于会话的计费功能(SBCF)和基于事件的计费功能(EBCF)。

[0010] SBCF负责网络/用户会话的在线计费——例如话音呼叫、IP CAN承载、IP CAN会话或IMS会话。

[0011] EBCF结合任意应用服务器或服务NE(包括SIP应用服务器)来执行基于事件的在线

计费。

[0012] 批价功能(RF)代表OCF确定网络资源使用的值(在由OCF从网络接收的计费事件中描述)。

[0013] 离线计费系统(OFCS)是用于离线计费的计费功能的组。该离线计费系统收集并处理来自一个或多个CTF的计费事件,并且其为后续的离线下游计费过程生成CDR。

[0014] 在订户正在漫游并由受访网络提供服务的情况下,两个计费系统(在受访网络中和在归属网络中)都将分别对订户进行计费。漫游费用通常是每分钟语音呼叫(对于移动发起和移动终止的语音呼叫不同地收费)、每条SMS和每兆字节数据量的费用。出于计费原因,两个网络都通过传输账务过程(TAP)进行通信。TAP的传输机制是一种称为移动网络增强定制应用逻辑(CAMEL)的机制。

[0015] 对于受访网络所提供的通过归属网络路由的所有服务(例如语音呼叫、SMS、IMS),归属网络的运营商可以对从服务网络通过TAP传输的所有费用进行验证。目前已经存在一些不经由归属网络路由的服务——例如本地直接接入(local breakout internet access)或本地路由的IP语音(VoIP)呼叫。这些本地提供的服务可能变得更流行。归属运营商缺乏一种机制来验证从服务网络通过TAP传输的用于本地路由服务的费用。目前,运营商必须彼此信任:服务网络发送费用的服务实际上的确被提供给漫游订户。需要一种使归属运营商能够验证漫游费用的机制。

[0016] US 2002/0161723 A1描述一种技术,在该技术中,以传统方式使用存储在UE和鉴权中心中的密钥来验证UE的身份。当UE连接到并非其归属网络的本地网络时,由归属网络运营商和UE共享的共享密钥被用于UE与本地网络运营商的验证。如果UE的用户希望利用UE授权支付来进行购买,则使用不同的通信网络与卖方交换消息,其中UE对来自卖方的消息进行签名来指示接受交易。然后,使用网络签名验证服务来检查签名。该签名验证服务与归属网络和本地网络不同。如上所述,为UE和签名验证服务都提供签名密钥。

[0017] WO 2005/004456描述一种用于使用受访网络来对UE的用户进行计费的机制,在该机制中,归属网络发布计费证明,该计费证明被发送给UE,使得UE能够将该计费证明提供给受访网络的服务提供商。

发明内容

[0018] 本发明提供一种对由移动通信用户设备(UE装置)执行的交易进行鉴权(authenticate)的方法,该方法在UE装置与受访网络的移动管理实体之间已经执行鉴权和密钥协商过程,以便在UE装置与受访网络之间建立安全上下文,所述方法包括:将服务验证消息从UE装置发送给受访网络,该服务验证消息已经由UE装置在使用完整性保护密钥的情况下进行数字签名,该完整性保护密钥在UE装置与归属网络之间所共享;以及将服务验证消息从受访网络传递给归属网络。

[0019] 本发明提供如下机制:该机制给归属运营商提供对通过TAP传输的漫游费用的更多控制。用户同意可以是该机制的一部分。该机制的一方面是在UE与归属运营商之间建立共享秘密,并且使用该共享秘密来生成完整性保护的服务验证消息。共享秘密还可以用于从归属运营商网络向UE发送完整性保护消息;例如具有优选的或允许访问的网络的列表。关于如何将这些服务验证消息从UE传输给归属运营商,提供多种选择。最有利的选择是增

强受访网络中的CTF，由此将漫游UE中生成的服务验证消息添加到服务网络中生成的CDR，并通过TAP计费消息将其传递给归属运营商。还存在在UE与归属网络之间共享秘密的多种选择，该归属网络对于受访网络而言是未知的。一种选择是运行鉴权和密钥协商功能(AKA)两次，但是第二次运行时不与受访网络共享完整性保护密钥。这种方法的优点在于对于现有的SIM卡没有影响。在5G标准化的后期阶段中，将能够使用密钥导出函数(KDF)来导出从归属网络到受访网络的所有会话密钥，即受访网络不接收归属网络的密钥，而是接收从归属网络的密钥导出的专用于受访网络的密钥。在这种情况下，可以使用归属网络(其目前对于受访网络未知)的完整性保护密钥。

[0020] 本发明的特定方面可以为运营商提供对漫游费用的控制和/或建立更可靠的漫游费用业务协议。本发明的实现可以基于技术手段而不是信任，并且本发明使用户能够避免与漫游费用相关的欺诈。

附图说明

[0021] 现在参考附图仅通过示例的方式描述本发明的优选实施例，其中：

[0022] 图1示出移动管理实体的示意图，该移动管理实体向归属环境请求鉴权向量；

[0023] 图2示出鉴权和密钥协商过程的示意图；

[0024] 图3示出本发明的实施例的信息流程图。

具体实施方式

[0025] 在第一实施例中，为了生成两个不同的完整性密钥，运行两次已知的初始质询响应机制，该初始质询响应机制被称为“鉴权和密钥协商”(AKA)，在该初始质询机制中生成会话密钥。在传统的LTE漫游场景中，在UE与服务网络的移动管理实体(MME)之间执行一次AKA。MME向归属运营商请求鉴权向量，该鉴权向量包括质询、根会话密钥K_{ASME}和对质询的预期响应。MME将质询发送给UE;UE计算对该质询的响应以及相应的根会话密钥。UE将响应发送回MME。MME借助预期响应来验证该响应。所生成的会话密钥与标识符KSI_{ASME}一起存储在UE和MME中并且用于在UE中建立安全上下文。在3GPP TS 33.401v15.0.0中描述AKA过程。

[0026] 在该实施例中，执行两次AKA过程。第一次运行如上所述。在第二次运行中，仅将质询和预期响应从归属网络传输给服务网络，即会话根密钥$K_{ASME}2$被保留在归属网络中并且不提供给服务(受访)网络。服务网络与UE之间的安全上下文的会话密钥层次结构的根是$K_{ASME}1$，并且服务验证消息的完整性保护密钥是从$K_{ASME}2$导出的。由于服务网络不了解$K_{ASME}2$，因此完整性保护服务验证消息不能由服务网络生成，而只能由UE生成，该完整性保护服务验证消息仅由UE和归属运营商彼此共享并且借助完整性保护密钥进行签名。在服务网络改变服务验证消息的内容的情况下，归属网络中的完整性验证将失败。

[0027] 图1示出MME，该MME向归属运营商网络的归属环境(HE)中的订户数据库请求一个或多个鉴权向量。AKA过程在图2(现有技术)中示出。

[0028] 在以后的标准化版本中，归属网络中已知的当前会话密钥可能不会从归属运营商传递给服务网络。因此，在第二实施例中，归属运营商的会话密钥仅保留在归属运营商，并且服务网络中使用的会话密钥将由归属网络和UE中的现有密钥导出。在这种情况下，由于UE和归属运营商可以通过归属运营商的会话密钥来完整地保护它们的通信，所以上述第二

次AKA运行的过程已过时。

[0029] 如果服务验证消息是仅当归属网络正在请求时才由UE和服务网络执行的可选特征,则有必要将请求从归属运营商的网络发送给服务网络。响应于从HE到服务网络中的MME的鉴权请求而添加信息是有利的。在第三实施例中,归属运营商的网络以一个或多个专用消息来向服务网络请求服务验证消息。在第四实施例中,HE通过以下方式来隐式地向服务网络请求服务验证消息:HE比所请求的鉴权向量多一个地进行响应。

[0030] 此外,UE需要接收请求以生成服务验证消息。在鉴权过程中,该请求可以由归属运营商的网络或服务网络作为附加信息片段(例如以非接入层(NAS)安全模式命令消息)来发送。在另一实施例中,服务网络以一个或多个专用消息向UE请求服务验证消息。在一个实施例中,服务网络在连接过程期间(例如在鉴权过程或安全上下文建立期间)请求服务验证消息。在另一实施例中,服务网络在承载建立过程期间基于每个承载请求服务验证消息。对于服务网络来说有利的是,请求用于在UE中生成服务验证消息的相应周期。在另一实施例中,UE基于由归属运营商的网络提供的存储的策略信息来决定周期。

[0031] 归属运营商可以决定是否请求服务验证消息以及以哪个周期请求UE生成服务验证消息。这可以取决于每个订户的策略、或每个访问类策略、或者基于UE能力。在一个实施例中,服务验证消息策略被存储在归属运营商网络的HE中。在另一实施例中,服务验证消息策略是策略控制和计费功能(PCCF)的一部分。

[0032] 必须保护从UE通过受访网络发送到归属网络的服务验证消息免受重放攻击。这可以借助时间戳或消息序列或这二者来执行。第一服务验证消息可以是预先验证,即其验证(用于建立服务的)配置的建立或接收,而不验证重要的服务提供。该第一服务验证消息应包括时间戳或消息序列号1以及何时可以预期到第二验证消息(例如在一分钟内或在100KB的漫游数据流量之内或在通话结束时)。从第二服务验证消息开始,所述消息(对于每个服务)可以包括前一个服务周期的附加反馈信息——例如语音呼叫的前一分钟的语音呼叫质量或最后100KB漫游数据流量的数据速率。

[0033] 下面是这种服务验证消息的示例。

[0034]

ID	Ver	SEQ	TS	P	SID	FB	MAC

[0035] ID:订户ID;例如GUTI(全球唯一临时ID)

[0036] Ver:协议版本信息

[0037] SEQ:消息序列号;例如16位

[0038] TS:时间戳

[0039] P:用于该服务的服务验证消息的预期周期

[0040] SID:服务标识符(例如,本地直接接入数据业务、语音呼叫、承载或PDU

[0041] 会话ID)

[0042] FB:用于当前服务的反馈信息

[0043] MAC:消息鉴权码,作为具有共享会话密钥的完整性保护。

[0044] 图3中示出示例性的信息流程图。用户A在外国打开其UE。在注册过程期间(步骤1),UE找到如下服务网络:归属运营商与该服务网络具有漫游协议。由归属运营商控制的允许网络列表存储在SIM中。在步骤2中,服务网络向漫游用户的归属运营商请求鉴权向量。在步骤3中,服务网络的移动管理实体MME向归属网络的归属环境HE请求一个或多个鉴权向量

AV。在步骤4中，HE以所请求的鉴权向量和一个附加鉴权向量进行响应。在步骤5中，归属网络MME将由附加鉴权向量导出的用于完整性保护的会话密钥传输给计费网关功能。在步骤6中，服务网络接收两个鉴权向量AV。如现有技术中所已知的，一个AV是完整的，在根据本发明的第二个AV中，会话密钥层次结构的根(至少用于完整性保护的会话密钥)未被包括在内。接收到附加鉴权向量可以隐式地通知服务网络：归属运营商网络请求服务验证消息。根据3GPP TS 33.401，这种请求还可以在MME与HE之间的消息内与NAS服务验证请求一起显式地进行。在附图中未示出根据TS 33.401的作为现有技术中的鉴权过程的一部分运行的AKA。然后在步骤7中，服务网络执行第二次AKA(或潜在的后继AKA*)过程，其中，服务网络以NAS安全模式命令消息通知UE：应使用用于该附加AKA运行的完整性保护的会话密钥来对服务验证消息进行签名，并且请求这些服务验证消息。在步骤8中，UE以NAS安全模式完成消息向服务网络确认请求。将第二次AKA运行产生的完整性保护密钥存储在UE中，以便生成服务验证消息的MAC字段。

[0045] 用户现在发起本地路由的语音呼叫，因此在UE中生成第一服务验证消息，并且在步骤9中将NAS服务验证消息发送给服务网络的服务移动管理实体(MME)。该第一服务验证消息包含用户的GUTI、消息序列号“1”、当前时间戳、一分钟的预期周期、作为服务标识符“本地语音呼叫”、空的反馈信息字段和用于消息的前七个字段的有效消息鉴权码。

[0046] 在步骤10中，服务网络MME将确认消息传递给计费数据功能CDF。在步骤11中，CDF还从计费触发功能CTF接收计费事件消息并且生成CDR，并且根据本发明将服务验证消息关联到CDR。因为服务验证消息由UE自主生成、由归属或受访网络配置或影响。因此将服务验证消息与CDR同步是有利的，使得将对应的服务验证消息与每个CDR相关联，但是不同步的解决方案也是可能的。在这种情况下，取决于CDR中的消息的可用性，单个CDR可以包括零个、一个或多个验证消息。在单个CDR中包含多于一个服务验证消息的情况下，则一些服务验证消息可以验证之前不包含服务验证消息的CDR。

[0047] 在步骤12中，立即通过Ga参考点将由CDF产生的CDR(与服务验证消息相关联)传输给计费网关功能CGF。在步骤13中，CGF生成包括服务验证消息的TAP计费消息，该计费消息通过SS7上的CAMEL接口被传输给归属运营商的CGF。在步骤14中，在继续进行计费过程之前，归属运营商的CGF验证所请求的服务验证消息。

[0048] 上述情况的替代方案是基于来自受访网络的触发来生成服务验证消息。受访网络的计费系统的CDF或任何其他实体可以以新NAS消息中或以已知NAS消息中的新信息来触发UE，以便生成服务验证消息，从而确保每个TAP计费消息都包括一个用于验证计费服务的服务验证消息。在该替代方案中，由于UE不控制服务验证消息的生成时间，所以消息可能不包含关于预期的下一服务验证消息的任何信息，即不存在周期性信息。

[0049] 可以在UE中生成服务验证消息，以便验证受访(漫游到的)网络的服务的建立或提供。服务验证消息可以包括以下服务信息关于由受访网络建立或提供的服务的服务信息以及向归属网络验证服务信息的签名。

[0050] 在一方面，本发明提供向受访网络发送服务验证消息，以便向归属网络发送以下信息：该信息关于从受访网络到归属网络的计费信息(CDR)，该计费信息关于建立或提供的待计费服务。

[0051] 总之，本发明提供由受访网络向归属网络发送以下服务验证消息：该服务验证消

息关于从受访网络到归属网络的计费信息(CDR),该计费信息关于建立或提供的待计费服务。服务验证消息可以包括完整性保护(借助在UE与归属运营商之间共享的密钥)、借助时间戳或消息序列号或这二者的重放保护、预先的第一服务验证消息、第一消息或所有消息中的后续消息的预期周期、最后服务周期的反馈、每个服务的服务验证消息;例如数据流量和语音呼叫服务,以及由受访网络触发的服务验证消息(即应受访网络的要求而生成的消息)。在UE与归属运营商之间共享的完整性保护密钥要么通过第二次AKA运行产生、要么通过导出用于服务网络的专用会话密钥来实现。


MME
HE
鉴权数据请求
IMSI，SN识别码，网络类型
鉴权数据响应
EPS鉴权向量

图1


ME/USIM
MME
用户鉴权请求 (RAND, AUTN, KSIASME)
用户鉴权响应（RES）

图2

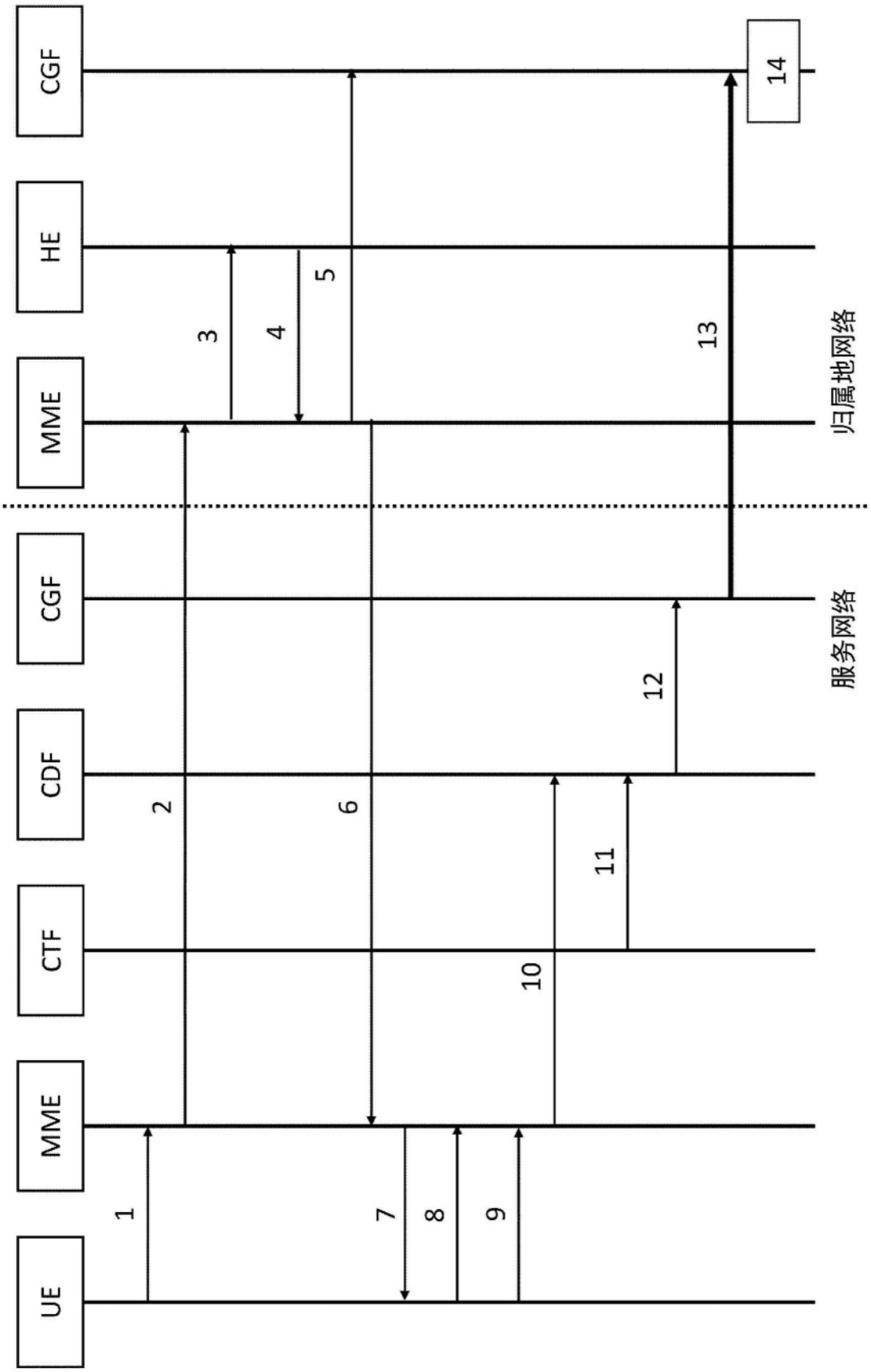

CGF
HE
MME
CGF
CDF
CTF
MME
UE
14
3
4
5
13
12
2
6
11
10
1
7
8
9
归属地网络
服务网络

图3