(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 109889509 B
(45)授权公告日 2021.06.01

(21)申请号 201910079015.4

(22)申请日 2014.05.22

(65)同一申请的已公布的文献号
申请公布号 CN 109889509 A

(43)申请公布日 2019.06.14

(30)优先权数据
61/826,176 2013.05.22 US

(62)分案原申请数据
201480037441.7 2014.05.22

(73)专利权人 康维达无线有限责任公司
地址 美国特拉华州

(72)发明人 迈克尔·F·斯塔西尼克
光·X·卢 苏雷什·帕拉尼萨米
李晴 黛尔·N·希德

(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
代理人 张鑫

(51)Int.Cl.
H04L 29/06(2006.01)
H04W 4/70(2018.01)
H04W 12/06(2021.01)

(56)对比文件
US 2012284785 A1,2012.11.08
CN 1848994 A,2006.10.18
US 2007022476 A1,2007.01.25
US 2013003972 A1,2013.01.03
CN 101426190 A,2009.05.06
CN 101272297 A,2008.09.24
3GPP."TR 33.922 V1.0.0".《3GPP》.2008,1-30页.
史永贺,刘焕淋."基于3G/WLAN交互网络的认证方法改进".《信息网络安全》.2008,(第8期),43-45、70页.

审查员 王务鹏

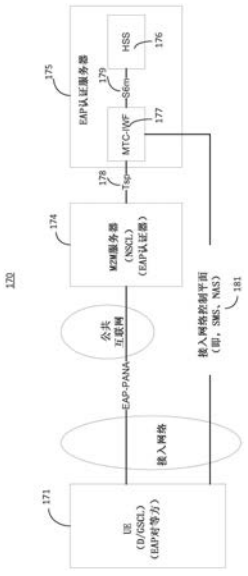
权利要求书2页 说明书16页 附图12页

(54)发明名称

用于机器对机器通信的网络辅助引导自举

(57)摘要

本发明公开用于机器对机器通信的网络辅助引导自举。服务层可以利用接入网络基础设施,使得设备上的应用可以与机器对机器服务器进行引导自举而不需要超越接入网络所已经要求的而提供。



CN 109889509 B

1.一种网络节点(243,224),包括:

存储器,所述存储器与处理器耦合,所述存储器具有存储在其上的可执行指令,当所述可执行指令在由所述处理器执行时使所述处理器实现操作,所述操作包括:

从设备(241,221)接收第一可扩展认证协议消息,所述第一可扩展认证协议消息与所述设备(241,221)相关联,所述第一可扩展认证协议消息包括机器到机器服务提供者标识符,所述机器到机器服务提供者标识符包括用于标识应授权所述设备(241,221)的服务层的第一服务层标识符;以及

向所述设备(241,221)提供来自所述网络节点(243,224)的第二可扩展认证协议消息,所述第二可扩展认证协议消息包括用于标识所述设备应连接到的服务层的第二服务层标识符。

2.根据权利要求1所述的网络节点,其中,所述第二可扩展认证协议消息包括随机挑战。

3.根据前述权利要求中的任一项所述的网络节点,其中,所述第二可扩展认证协议消息包括网络认证矢量。

4.根据权利要求1或2中的任一项所述的网络节点,其中,所述第二可扩展认证协议消息包括消息认证代码。

5.根据权利要求1或2中的任一项所述的网络节点,其中,所述网络节点是受信任的非3gpp接入点。

6.根据权利要求1或2中的任一项所述的网络节点,其中,所述存储器进一步包括可执行指令,所述可执行指令在由所述处理器执行时使得所述处理器实现包括基于来自主订阅服务器的订阅信息验证允许所述设备向所述网络节点注册的操作。

7.根据权利要求1或2中的任一项所述的网络节点,其中,所述第二可扩展认证协议消息进一步包括设备上的应用的标识符、由机器到机器服务器指配给所述应用的应用的标识符。

8.根据权利要求1或2中的任一项所述的网络节点,其中,所述第一可扩展认证协议消息进一步包括将特定应用标识符指配给所述设备的请求。

9.一种引导自举方法,包括:

由网络节点从设备(241,221)接收与所述设备(241,221)相关联的第一可扩展认证协议消息,所述第一可扩展认证协议消息包括机器到机器服务提供者标识符,所述机器到机器服务提供者标识符包括用于标识应授权所述设备(241,221)的服务层的第一服务层标识符;以及

向所述设备(241,221)提供来自所述网络节点(243,224)的第二可扩展认证协议消息,所述第二可扩展认证协议消息包括用于标识所述设备应连接到的服务层的第二服务层标识符。

10.根据权利要求9所述的方法,其中,所述第二可扩展认证协议消息包含消息认证代码。

11.根据权利要求9或10中的任一项所述的方法,其中,所述第一可扩展认证协议消息进一步包括将特定应用标识符指配给所述设备的请求。

12.根据权利要求9或10中的任一项所述的方法,其中,所述第二可扩展认证协议消息

进一步包括在所述设备上的应用的标识符、由机器到机器服务器指配给所述应用的所述应用的标识符。

13.根据权利要求9或10中的任一项所述的方法，其中，所述第一可扩展认证协议消息进一步包括所述设备的访问网络标识符。

14.根据权利要求9或10中的任一项所述的方法，其中，所述第二可扩展认证协议消息包括网络认证矢量。

15.一种计算机可读存储介质，所述计算机可读存储介质上记录有包括程序指令的计算机程序，当所述计算机程序由数据处理单元运行时，所述计算机程序被加载到所述数据处理单元中并适于使所述数据处理单元执行根据权利要求9到14中的任一项所述的方法步骤。

用于机器对机器通信的网络辅助引导自举

[0001] 本申请是2015年12月29日提交的国际申请日为2014年5月22日的申请号为201480037441.7(PCT/US2014/039205)的,发明名称为“用于机器对机器通信的网络辅助引导自举”专利申请的分案申请。

[0002] 相关申请交叉引用

[0003] 本申请要求于2013年5月22日提交的题为“ACCESS NETWORK ASSISTED BOOTSTRAPPING”的美国临时专利申请No.61/826176的权益,其内容在此通过引用合并于此。

背景技术

[0004] 机器对机器(M2M)技术允许设备使用有线或无线通信系统更直接地互相通信。M2M技术使得能够进一步实现物联网(IoT)——彼此通信以及通过诸如互联网的网络进行通信的唯一可识别对象和这样的对象的虚拟表现的系统。IoT可以便于甚至与诸如杂货店中的产品或家中家电的普通日常对象进行通信,并且从而通过改进这样的对象的知识来降低成本和浪费。例如,商店通过能够与可能在存货中的对象或可能已经售出的对象通信或者从它们获得数据而可以保持非常精确的存货数据。

[0005] 已经做出了若干努力来发展用于机器对机器通信的标准化架构。这些架构包括第三代伙伴计划(3GPP)机器类型通信(MTC)架构、ETSIM2M架构、以及oneM2M架构。这些架构被简单总结如下。

[0006] 3GPP演进分组核心(EPC)网络一开始并非按照用于为处理机器对机器(M2M)通信、也被称为机器类型通信(MTC)的优化而设计,其中,机器或设备通过网络彼此通信,诸如涉及智能计量、家庭自动化、电子健康(eHealth)、消费者产品、车队管理等等。因此,在3GPP规范的版本11(R11)中,3GPP加权了UMTS核心网络的互联能力以用于机器类型通信/机器对机器通信。互联指的是服务器或应用与核心网络相接以便交换信息、控制设备、或监视设备、或与设备通信。图1示出了由3GPP在TS 23.682V11.5.0中呈现的部分MTC架构。

[0007] 如图1中所示,用户设备314可以通过可包括E-UTRAN(LTE接入网络)的无线电接入网络(RAN)319连接到EPC。演进节点B(eNodeB)3是用于LTE无线电的基站。在此图中,EPC包括包含服务网关(服务GW)310、分组数据网络网关(PDN GW或P-GW)353、移动性管理实体(MME)312和归属订户服务器(HSS)357的多个网络元件。

[0008] HSS 357是包含用户相关以及订户相关的信息的数据库。其还提供移动性管理中的支持功能、呼叫与会话建立、用户认证、和接入授权。

[0009] 网关(S-GW 310和P-GW 352)处理用户平面。所述网关在用户设备(UE)314和外部网络之间传输IP数据流量。S-GW 310是在无线电侧和EPC之间的互连的点。如其名称指示,该网关通过路由传入和传出的IP分组来服务UE。其是用于LTE内移动性(即,在RAN 319的eNodeB之间切换的情况)以及在LTE和其他3GPP接入之间的锚点。其逻辑上连接到其他网关P-GW 353。

[0010] P-GW 353是在EPC和诸如互联网的外部IP网络之间互连的点。这些网络被称为PDN

(分组数据网络),由此得名。P-GW 353路由去往和来自PDN的分组。P-GW 353还执行诸如IP地址/IP前缀分配或策略控制和计费的各种功能。3GPP指定了这些网关独立操作但实际上它们可以被网络提供者组合在一个“盒子”中。

[0011] MME 312处理控制平面。其处理与E-UTRAN接入的移动性和安全性相关的信令。MME 312负责追踪和寻呼空闲模式的UE。其还是非接入层(NAS)的终止点。

[0012] 如上所提及的,UE 314可以使用E-UTRAN到达EPC,但是这并不是所支持的唯一接入技术。3GPP指定了支持多种接入技术并且还指定了这些接入之间的切换。想法是使用通过多种接入技术提供各种基于IP的服务的独特核心网络带来汇聚。支持现有的3GPP无线电接入网络。3GPP规范限定如何在E-UTRAN(LTE和LTE高级)、GREAN(GSM/GPRS的无线电接入网络)和UTRAN(基于UMTS的技术WCDMA和HSPA的无线电接入网络)之间网络互连。

[0013] 该架构还允许非3GPP技术互连UE和EPC。非3GPP意味着这些接入并非在3GPP中指定。这些技术包括例如WiMAX、cdma2000®、WLAN或者固定网络。非3GPP接入可以被分成两个类别:“受信任的”和“不受信任的”。信任的非3GPP接入可以直接与EPC交互。不受信任的非3GPP接入经由被称为ePDG(用于演进分组数据网关)的网络实体(未示出)与EPC互联互通。ePDG的主要作用在于提供安全机制,诸如通过不受信任的非3GPP访问与UE连接的IPsec隧道。3GPP不指定哪些非3GPP技术应该被认为是受信任的还是不受信任的。这个决定由运营商作出。

[0014] 如图1中进一步所图示,服务能力服务器(SCS)361可以向核心网络、设备、和应用提供服务。SCS还可以被称为M2M服务器、MTC服务器、服务能力层(SCL)、或公共服务实体(CSE)。SCS 361可以由归属公共陆地移动网(HPLMN)的运营商或由MTC服务提供者所控制。SCS可以被部署在运营商域内或外。如果SCS被部署在运营商域内,则SCS可以是内部网络功能并且可以由运营商控制。如果SCS被部署在运营商域外,则SCS可以由MTC服务提供者控制。

[0015] 在图1的MTC架构中,SCS 361可以经由Tsp参考点(即接口)308与机器类型通信(MTC)网络互连功能(MTC-IWF)359通信。Tsp参考点是用于与核心网络进行网络互连的接口的示例。

[0016] UE可以通过包括无线电接入网络(RAN)319的公共陆地移动网(PLMN)与SCS和/或其他MTC UE通信。MTC UE 214可以托管一个或多个MTC应用316。MTC应用还可以被托管在一个或多个应用服务器(AS)(例如AS 320)上。MTC应用316可以是MTC可以与SCS 361、AS MTC应用或其他UE MTC应用交互的通信端点。

[0017] 应用服务器(AS)(例如AS 320)还可以托管一个或多个MTC应用。AS 320可以与SCS 161相接口,并且SCS 361可以向运行在AS 320上的应用提供服务。AS上的MTC应用可以与SCS、UE MTC应用、或其他MTC应用交互。

[0018] MTC网络互连功能(MTC-IWF)359向SCS 361隐藏内部PLMN拓扑。MTC-IWF可以中继和/或转化其自身与SCS之间所使用的信令协议(例如,通过Tsp参考点308)以支持PLMN中的MTC功能(例如MTC UE触发)。例如,SCS可以请求MTC-IWF发送触发到MTC设备。例如,MTC-IWF可以经由SMS(未示出)递送MTC触发到MTC设备314。基于该触发,MTC设备316可以对SCS 312作出响应。例如,MTC设备314可以利用传感器读取来作出响应。当MTC设备214对SCS 312作出响应时,MTC设备可以使用分组数据网络(PDN)/分组数据协议(PDP)连接经由P-GW 353以

与SCS 361通信。MTC设备可以使用IP连接与SCS连接。

[0019] 在SCS可以建立与3GPP网络的通信之前,MTC-IWF 359可以授权SCS 361。例如,当SCS 359在Tsp参考点上进行触发请求时,MTC-IWF 359可以检查SCS是否被授权来发送触发请求以及SCS尚未超过其触发提交的配额或比率。

[0020] ETSI M2M架构在图2中图示。在ETSI M2M架构中,服务能力层(SCL)通过暴露的接口集合来使用核心网络功能以向网络提供服务能力。SCL可以与一个或若干不同核心网络相接口。

[0021] 在ETSI M2M架构中,网络包括M2M设备(例如设备145)、M2M网关(例如网关140)、和M2M服务器(例如M2M服务器125)。设备应用(DA)可以正在M2M设备上执行,网关应用(GA)可以正在M2M网关上执行,并且网络应用(NA)可以正在M2M服务器上执行。如进一步所示,设备(例如设备145)可以使用设备服务能力层(DSCL)(例如DSCL 146)实现M2M服务性能,网关可以实现网关SCL(GSCL 141),并且服务器可以实现网络SCL(NSCL)(例如NSCL 126)。

[0022] mIa参考点允许网络应用访问M2M服务器中的M2M服务能力。

[0023] dIa参考点允许驻留在M2M设备中的设备应用访问相同的M2M设备中或M2M网关中的不同的M2M服务能力;并且允许驻留在M2M网关中的网关应用访问相同的M2M网关中的不同的M2M服务能力。

[0024] mId参考点允许驻留在M2M设备或M2M网关中的M2M服务能力层与网络中的M2M服务能力层通信。mId参考点使用核心网络连接性功能作为底层。

[0025] 进一步根据ETSI M2M架构,M2M实体(例如,诸如可以由硬件和/或软件的组合来实现的设备、网关、或服务器/平台的M2M功能实体)可以提供应用或服务。例如,光传感器可以提供指示所检测到的光照水平的数据或者恒温器可以提供温度数据以及调整空调控制的能力。该数据可以作为可用资源,其可由其他M2M实体访问并且实际上充当M2M实体之间交换数据的手段。资源可以是数据唯一可寻址的表示,其可以使用统一资源指示符(URI)或统一资源定位符(URL)来寻址。这样的资源的可用性可以经由M2M服务能力层(SCL)而在M2M实体之间传递。

[0026] M2M SCL也是功能实体,其可以使用硬件和软件的组合来实现,并且提供在上述的参考点(即M2M实体之间的功能接口)上暴露的功能。例如,M2M SCL可以提供公共(服务)功能,所述公共服务功能由不同M2M应用和/或服务所共享地或公共地使用。M2M服务能力可以通过暴露的接口(例如,由3GPP、3GPP2、ETSI TISPAN等所指定的现有接口)集合来使用3GPP核心网络架构的功能和能力并且还可以接口到一个或多个其他核心网络。M2M设备和实体通常被组织进M2M网络域。在许多实施方式中,配置有网络SCL实体(NSCL)的M2M服务器(例如M2M服务器125)可以保持资源和资源数据以供相同的M2M网络域中的其他设备(例如,其他M2M设备和M2M网关)使用。

[0027] 仍参看图2,NSCL 126可以在网络域122中并且在M2M服务器平台125处配置有网络应用(NA)127。NA 127和NSCL 126可以经由参考点mIa 128通信。mIa参考点可以允许NA访问从M2M域中的NSCL可用的M2M服务能力。同样在网络域122内的可以是GSCL 141和网关应用(GA)142,GSCL 141和网关应用(GA)142可以在M2M网关设备140处被配置。GSCL 141和GA 142可以使用参考点dIa 143来通信。同样在网络域122内的可以是DSCL 146和设备应用(DA)147,DSCL 146和设备应用(DA)147可以在M2M设备145处被配置。DSCL 146和DA 147可

以使用参考点dIa 148来通信。GSCL 141和DSCL 146中每个可以使用参考点mId 124来与NSCL 126通信。通常,dIa参考点允许设备和网关应用与它们各自的本地服务能力(即,分别在DSCL和GSCL处可用的服务能力)通信。mId参考点允许驻留在M2M设备(例如DSCL 146)或M2M网关(例如GSCL 141)中的M2M SCL与网络域中的M2M服务能力通信,反之亦然(例如NSCL 126)。

[0028] 典型地,设备145、网关140、和M2M服务器平台125包括计算设备,诸如图8C和图8D中所图示以及下面所述的设备。NSCL、DSCL、GSCL、NA、GA、和DA实体通常是以软件形式实现的在下层设备或平台上执行的逻辑实体,以在系统120中执行它们各自的功能。ETSI M2M架构的M2M服务器125可以是3GPP MTC架构中的SCS(例如,图1的SCS 361)。

[0029] 进一步如图2中所示,NSCL 131可以与NA 132在域130中。NA 132和NSCL 131可以经由mIa参考点133来通信。网络域135中可以存在NSCL 136,以及网络域138中可以存在NSCL 139。mIm参考点123可以是域间参考点,其允许不同网络域中的M2M网络节点(诸如网络域122中的NSCL 126、网络域130中的NSCL 131、网络域135中的NSCL 136、或网络域138中的NSCL 139)相互通信。在这里为了简便,术语"M2M服务器"可以用来指示服务能力服务器(SCS)、NSCL、应用服务器、NA、或MTC服务器。此外,如这里所讨论的术语用户设备(UE),可以应用于GA、GSCL、DA或DSCL。UE可以包括能够在3GPP或其他无线网络中通信的任何无线设备,诸如M2M或MTC设备或网关,并且包括例如机器、传感器、电器等、移动站、固定或移动订户单元、寻呼机、个人数字助理(PDA)、计算机、移动电话或智能电话、或者能够在有线或无线环境中操作的任何其他类型的设备。

[0030] 尽管这里通过背景技术的方式描述了3GPP MTC和ETSI M2M架构并且可用其来图示下文所述的各种实施例,应该理解,下文所述实施例的实施方式可以变化而同时保持在本公开的范围内。本领域技术人员还将认识到,所公开的实施例不限于使用上面讨论的3GPP或ETS M2M架构的实施方式,而是可以以诸如oneM2M、MQ遥测传输(MQTT)以及其他相关M2M系统和架构的其他架构和系统来实现。

[0031] 经常在M2M系统中执行的一种处理被称为引导自举。引导自举是实体(例如,终端用户设备和服务器)通过其执行相互认证和密钥协商以建立使得能够在它们之间安全通信的关系的处理。相互认证是每一方向其他方证明其身份的过程。认证帮助防止欺诈设备通过假装自己是合法终端用户设备而向服务器注册。认证还帮助防止欺骗性服务器执行中间人攻击,其可由通过假装自己是合法服务器与终端用户设备建立连接的欺骗性服务器组成。

[0032] 密钥协商是通信实体导出安全密钥的过程,通信实体可接着使用该安全密钥以在通信实体之间安全通信,例如,通过使用安全密钥的加密处理。密钥协商机制的特征在于密钥不被传送。密钥导出功能可以基于共享的秘密值,其中共享的秘密值意味着例如仅终端用户设备和服务器知晓。这个共享的秘密也不被传送。该密钥导出功能被设计成使得其对于不知晓共享秘密的偷听者来讲,通过观察在密钥协商过程期间所传送的消息来计算密钥在计算上相当复杂。这里讨论一些认证和密钥协商机制的概述。下面讨论诸如可扩展认证协议(EAP)和网络接入认证信息承载协议(PANA)的一些认证和密钥协商机制的概述,以对所公开的实施例给出进一步的上下文。

[0033] 可扩展认证协议(EAP)其自身不是认证方法,而是可以用来实现特定认证方法的

常见认证框架。换句话说，EAP是允许对等方、认证器、以及认证服务器协商将使用什么认证方法的协议。所选择的认证方法随后在EAP协议内运行。EAP是在RFC 3748中定义的。RFC 3748描述了EAP分组格式、过程、以及基本功能，诸如所需认证机制的协商。

[0034] 图4图示了基本EAP架构。如图4中所示，并且在RFC 3748中所述的，存在EAP对等方161，其可以经由EAP认证器163(例如接入点)联系认证服务器162。EAP可以使用半径或直径协议。存在许多由IETF定义的EAP方法。这里讨论的是被称为EAP认证和密钥协商(AKA)的EAP方法，其基于通用移动电信系统(UMTS)-AKA并且在RFC 4187中定义。而且，可以使用这里所呈现的许多想法而不用管所选择的EAP认证方法。EAP被设计为链路层(层2)协议。PANA是可用于在IP网络上承载EAP消息的协议。换句话说，PANA是EAP的运输工具。PANA在网络(IP)层之上运行。PANA在RFC 5191中定义。PANA允许动态服务提供商选择、支持各种认证方法、适合于漫游用户、并且独立于链路层机制。

发明内容

[0035] 引导自举会是昂贵的处理，因为其经常需要在设备中提供秘密密钥或证书以便获取所需的安全级别。这在机器对机器领域中是个尤其重要的问题，因为大量设备需要与SCS或M2M服务器进行引导自举。这里所公开的是方法、设备、和用于至少两种引导自举方法的系统。在一个实施例中，服务层可以利用接入网络基础设施来使得D/GSCL可以与M2M服务器进行引导自举而不需要供应超越接入网络已经要求的。在这个方法中，MTC-IWF可以提供到接入网络的AAA服务器的安全连接。当UE附接于接入网络时，可以由接入网络的AAA服务器将服务层密钥材料提供给M2M服务器。在另一实施例中，定义过程使得M2M服务器使用核心网络的基础设施以对设备进行认证和授权。例如，基于EAP-PANA的方法可以使用HSS作为EAP认证服务器，使得UE和M2M服务器能够执行EAP-AKA-PANA认证。

[0036] 提供该发明内容以用简化的形式引入概念的选择，在下面的具体实施方式中进一步描述。该发明内容不旨在识别所要求保护的主题的关键特征或必要特征，而且也不旨在被用来限制所要求保护的主题的范围。此外，所要求保护的主题不被限制为解决在本公开内容的任何部分中提及的任何或所有缺点的限定特征。

附图说明

[0037] 可以通过示例的方式结合附图，从下面的描述得到更详细的理解，所述附图中：

[0038] 图1是图示3GPP机器类型通信(MTC)架构的框图；

[0039] 图2是图示ETSI M2M架构的框图；

[0040] 图3图示通用EAP架构；

[0041] 图4图示用于M2M的EAP-PANA-AKA架构；

[0042] 图5图示EAP-PANA D/GSCL引导自举的流程图；

[0043] 图6图示用于M2M的基于EAP接入网络的服务层引导自举；

[0044] 图7A图示基于接入网络EAP的D/GSCL引导自举的流程图；

[0045] 图7B图示继续图7A的基于接入网络EAP的D/GSCL引导自举的流程图；

[0046] 图8A是在其中可以实现一个或多个所公开的实施例的、示例机器对机器(M2M)或物联网(IoT)通信系统的系统图；

[0047] 图8B是可以在图8A中所图示的M2M/IoT通信系统内使用的示例架构的系统图；

[0048] 图8C是可以在图8A中所图示的通信系统内使用的示例M2M/IoT终端或网关设备的系统图；以及

[0049] 图8D是在其中可以实现图8A的通信系统的方面的示例计算系统的框图。

具体实施方式

[0050] 在进行之前，应该注意到，这里所描述的实施例可以依据表述性状态转移(REST)架构来描述，其中所述的组件和实体符合REST架构(REST性架构)的限制。REST性架构是依据应用于用在该架构中的组件、实体、连接器、和数据元件的限制而非依据所使用的物理组件实施方式或通信协议而描述的。因此，将描述所述组件、实体、连接器、和数据元件的作用和功能。

[0051] 在REST性架构中，唯一可寻址的资源的表示是在实体之间转移的。ETSI M2M规范(例如，这里所讨论的TS 102 921和TS 102 690)已经将驻留在SCL上的资源结构标准化。当处理REST性架构中的资源时，存在可应用于资源的基本方法，诸如创建(创建子资源)、检索(读取资源的内容)、更新(写入资源的内容)或删除(删除资源)。本领域技术人员将认识到示例实施例的实施方式可以变化，而同时落入本公开的范围内。本领域技术人员还将认识到，所公开的实施例不限于使用这里所述的用来描述示例性实施例的ETSI M2M架构的实施方式。所公开的实施例可以实现在诸如oneM2M和其他M2M系统和架构的其他架构和系统中。

[0052] 这里所讨论的EAP-PANA方法和基于EAP接入网络的方法可以允许服务层更加轻量级。在EAP-PANA和基于EAP接入网络的方法中，从M2M服务器的NSCL到接入网络提供接口，但该接口并未由ETSI M2M规范完整定义。包括ETSI M2M架构规范的第8.3.2节以及ETMS M2M mIa、dIa、mId规范的第6.2节的ETSI M2M规范，提供对于接入网络辅助的引导自举方法的支持，如这里所讨论的。这里所公开的密钥协商示例包括导出M2M服务层根密钥(Kmr)的D/GSCL和M2M服务器。

[0053] 这里所公开的引导自举方法与ETSI M2M架构规范的第8.3.2节、ETSI TS 102 690、和ETSI TS 102 921中概述的接入网络辅助的M2M引导自举过程相类似。如下面进一步详细讨论的，ETSI M2M架构被用作基线并且扩展为使得过程更加有效率并且更好地利用接入网络的能力。接入网络通常可以被认为是将订户连接到其即时应用服务提供者的电信网络的一部分。

[0054] 这里所公开的每个引导自举方法可以(i)利用核心网络基础设施以允许UE的D/GSCL(下文称为UE D/GSCL)使用M2M服务器的NSCL(下文称为M2M服务器)来执行相互认证，(ii)利用核心网络基础设施(例如，归属公共陆地移动网络)以导出服务层根密钥Kmr作为引导自举处理的一部分；以及(iii)将注册处理进行集成，由此当引导自举处理完成时，UE D/GSCL将向M2M服务器注册。

[0055] 这里所公开的引导自举方法中的一个是基于EAP-PANA的方法。概括地讲，基于EAP-PANA的方法可以使用归属订户服务器(HSS)作为EAP认证服务器(例如，认证服务器162)，使得UE D/GSCL和M2M服务器可以执行EAP-AKA-PANA认证。在此方法中，UE D/GSCL被认为是EAP对等方(例如，EAP对等方161)并且M2M服务器被认为是EAP认证器(例如，EAP认证器163)。M2M服务器经由机器类型通信网络互连功能(MTC-IWF)联系EAP认证服务器(例如

HSS)。

[0056] 图4显示了用于与蜂窝接入网络进行网络互连的EAP-PANA-AKA架构170(EAP-PANA方法)。UE D/GSCL 171使用EAP-PANA与M2M服务器174通信地连接。M2M服务器174经由Tsp参考点178通信地连接到EAP认证服务器175。EAP认证服务器175包括MTC-IWF 177和HSS 176，MTC-IWF 177和HSS 176经由S6m参考点179连接。EAP认证服务器175经由诸如非接入层(NAS)和短消息传递服务(SMS)的接入网络控制平面181而通信连接到UE 171。在这个架构中，UE D/GSCL 171是EAP对等方，M2M服务器174是EAP认证器并且MTC-IWF 177连同HSS 176一起被认为集成在EAP认证服务器175内。

[0057] MTC-IWF 177向M2M服务器174隐藏核心网络拓扑。因此，EAP认证服务器175可包括除HSS 176以外的实体，诸如认证、授权、和计费(AAA)服务器(未示出)。在ETSI术语中，MTC-IWF 177是M2M认证服务器(MAS)或到MAS的接口。M2M服务引导自举功能(MSBF)是M2M服务器174的一部分。

[0058] 参考如图4中所示的基于EAP-PANA的架构，如果使用AKA，则HSS 176被用作认证服务器，因为认证密钥Ki在通用集成电路卡(UICC)(未示出)和HSS 176中提供。如果认证密钥存储在UE D/GSCL171上的一些其他介质中以及在诸如AAA服务器的另一网络节点中供应，则相同的架构也适用。

[0059] 在图5中图示并在下面讨论EAP-PANA-AKA引导自举过程的呼叫流。图5图示了UE D/GSCL 191使用EAP-PANA-AKA与M2M服务器192进行引导自举并且向其注册的流190。在步骤195处，PANA-客户端-发起(PCI)消息被UE D/GSCL 191发送到M2M服务器192。PCI消息在PANA规范IETF RFC 5191中定义。在步骤195处发送的PCI消息是注册请求。PCI消息的目的地IP地址是M2M服务器192的IP地址并且目的地端口号可以是PANA端口号(例如，端口716)。M2M服务器192使用消息的源IP地址和端口号来确定用于PANA消息的IP地址和UE D/GSCL 191侦听的端口号。在一个实施例中，如果M2M服务器192知道UE D/GSCL 191的IP地址并且其知道其所侦听的PANA消息的端口号，则M2M服务器192可以发起引导自举。例如，如果M2M服务器192在UE 191上发现其需要的一些服务，这可能是所期望的。PANA规范在PCI消息中没有定义属性值对(AVP)。然而，ETSI规范ETSI TS 102 921定义了可用于PCI消息的AVP。表1显示了可以使用的一些AVP的示例。MSM-MSBF-ID、M2M-NSCL-ID、M2M-D/GSCL-ID和M2M-SP-ID是可选的AVP，如果D/GSCL想要限制到某MSBF、NSCL、或服务提供者的目标注册，则可以使用这些可选AVP。

[0060] 表1.用于PCI消息的AVP

[0061]

AVP	描述
M2M-使用-类型	当引导自举时，其可以被设为“M2M引导自举”。
M2M-节点-ID	M2M-节点-ID 承载设备标识符。具有3GPP 能力的设备可以将该值设为其M2M-节点-ID 外部标识符。
MSM-MSBF-ID	MSM-MSBF-ID 承载 M2M 服务引导自举功能(MSBF)标识符。 MSM-MSBF-ID AVP 将认证服务器的身份通知给 NSCL。该字段在 3GPP 设备引导自举时并不需要。在 3GPP 设备中，认证服务器是 MTC-IWF/HSS。MTC-IWF 的身份将经由在 M2M-节点-ID 上的域名服务(DNS)查找而被导出。
M2M-NSCL-ID	M2M-NSCL-ID 识别 NSCL。

[0062]

M2M-D/GSCL-ID	M2M-D/GSCL-ID 识别 D/GSCL。 M2M-D/GSCL-ID 是所请求的 D/GSCL 标识符。
M2M_SP-ID	M2M_SP-ID 识别服务提供者。

[0063] 在步骤196处，PANA-认证-请求(PAR)消息被发送到UE D/GSCL 191。PANA-认证-请求(PAR)消息在IETF RFC 5191(PANA规范)中定义。当M2M服务器192不知道UE D/GSCL 191的IP地址时，则PAR消息可以被广播、组播、或者任意播到UE D/GSCL 191可到达的地址。在步骤197处，在PANA规范中定义的PANA-认证-请求(PAR)消息被发送到M2M服务器192。PAN消息具有被设置为“M2M引导自举”的M2M-使用-类型AVP。

[0064] 在步骤198处，M2M服务器192对MTC-IWF 193进行设备认证请求。设备认证请求包括设备的3GPP外部设备标识符。对于这个例子，如这里更详细讨论的，设备-信息-请求(DIR)命令可以是所执行的命令。DIR命令可以包括EAP_负荷AVP，其承载IETF RFC 4187(EAP-AKA规范)中所定义的EAP-响应/AKA-身份消息。EAP负荷等于EAP-响应消息或AKA-身份消息。DIR命令还可包括外部ID、M2M服务器ID(SCS ID)以及所请求的参数(Requested Param)，上述所有都是EAP AKA密钥材料(EAP_AKA_密钥_材料)。

[0065] 在步骤199处，MTC-IWF 193发送与步骤198相关联的设备认证请求到HSS 194。在接收到设备认证请求之后，HSS 194在步骤200处运行AKA算法以生成认证令牌(AUTN)、随机询问(RAND)、所期望的认证响应(XRES)、消息认证代码(MAC)、和M2M根密钥。在步骤201处，HSS 194发送EAP-AKA引导自举信息到MTC-IWF 193。这里更详细讨论，设备-信息-应答

(DIA)命令可以是所执行的命令。DIA命令可以包括外部ID、M2M服务器ID、和所请求的参数(Requested Param)，上述所有都是EAP AKA密钥材料(EAP_AKA_密钥_材料)。DIA命令还可以包括密钥-材料，其等于RAND、XRES、AUTN、MAC、和M2M根密钥。

[0066] 在步骤202处，MTC-IWF 193发送EAP-AKA引导自举信息到M2M服务器192。DIA命令可以包括EAP_负荷AVP。如所讨论的，EAP_负荷AVP承载EAP-请求/AKA-询问消息，其在EAP-AKA规范中定义。在步骤202处的消息承载随机询问(AT_RAND)AUTN和MAC。MTC-IWF 193保留XRES和M2M根密钥(Kmr)。XRES不被传递到M2M服务器192。

[0067] 在步骤203处，UE D/GSCL 191接收PAR消息。这个PAR消息的EAP_负荷承载来自步骤202的EAP-请求/AKA-询问消息。在步骤204处，UE D/GSCL 191运行AKA算法并且生成对随机询问(RAND)的响应(RES)并且其使用AUTN来对M2M服务器192进行认证。UE D/GSCL 191还导出M2M根密钥Kmr，如ETSI TS 102 921所定义。在步骤205处，M2M服务器192接收承载在EAP-AKA规范中所定义的EAP-响应/AKA-询问消息的PAN消息。在步骤206处，M2M服务器192对MTC-IWF 193进行另一个设备认证请求以检查来自UE D/GSCL 191的RES是正确的。在步骤206处的请求包括UE D/GSCL 191的3GPP外部设备标识符。在步骤206处，DIR命令可以被发送并且包括外部ID、M2M服务器ID、EAP_负荷、以及所请求的参数AVP的。所请求的参数可以被设置为EAP_AKA_密钥_材料，其包括外部ID、M2M服务器ID、和所请求的参数。EAP_负荷AVP可以等于EAP响应消息或AKA询问消息。

[0068] 在MTC-IWF 193接收到步骤206的请求之后，MTC-IWF 193在步骤207处比较RES与XRES。在步骤208处，M2M服务器192接收包括EAP_AKA_密钥_材料(＝外部ID,SCS ID和所请求的参数)和EAP_负荷(＝EAP-成功或EAP-失败,作为Kmr的密钥-材料)的响应。EAP-成功消息和EAP-失败消息是在EAP规范IETF RFC 3748中定义的。在步骤208处，假定EAP成功消息被接收。

[0069] 在步骤209处，UE D/GSCL 191接收承载与步骤208相关联的EAP-成功消息(或EAP-失败消息)的PAR消息。步骤209的PAR消息可以包括诸如M2M-引导自举-结果、M2M-节点-ID(承载服务提供者指派的节点-ID)、M2M-D/GSCL-ID和M2M-NSCL-ID的附加信息。在步骤210处，PAN消息承载信息(例如，一组完成的或“C”比特)，该信息指示通过PANA使用EAP-AKA协议与M2M服务器192引导自举并且向其注册是成功的。

[0070] 现在将描述第二引导自举方法。该第二引导自举方法利用用于服务层引导自举和注册的基于EAP的接入网注册(下文中的基于EAP接入网的方法)。概括地讲，基于EAP接入网络的方法可以被用在UE D/GSCL使用EAP方法来与接入网络进行认证的情况下。在该方法中，MTC-IWF提供到接入网络认证服务器的安全连接。当UE D/GSCL附接到接入网络时，服务器密钥材料可以被接入网络的AAA服务器提供给M2M服务器。通过使用该方法来交换安全密钥，避免了M2M服务器和UE D/GSCL在尚不安全的接口上协商安全密钥的需要。该方法可以使得将设备连接到M2M服务器的处理流线型化。

[0071] 在3GPP TS 33.402中定义了经由受信任的无线局域网(WLAN)的授权和认证。图6图示了根据本实施例的用于利用用于服务层引导自举和注册的基于EAP的接入网络注册的架构。服务层根密钥是由AAA服务器/HSS 224在关于接入网络222的密钥被生成时生成的。MTC-IWF 255将被用于将密钥材料传递到M2M服务器229。呼叫流在图7A和图7B中示出，在下面更详细讨论。

[0072] 当EAP或类似的认证方法被用于利用接入网络引导自举D/GSCL时,M2M服务器的服务层可以利用该处理以与设备引导自举。一些接入网络使用EAP方法以用于接入网络注册。例如,参考图6,当UE D/GSCL 221经由受信任的WLAN 223连接到演进分组系统(EPS)时,UE D/GSCL 221使用EAP-AKA'通过核心网络来认证。AKA'(AKA-主要)在RFC 5488中定义。AKA'是AKA的变形,其中,导出的密钥(即,M2M根密钥)基于接入网络名称。对于基于EAP接入网络的方法,图3中的EAP角色将如下分别被映射到图6中所示的角色。EAP对等方161可以通过UE D/GSCL 221来映射,EAP认证器163可以通过WLAN接入点223来映射,且认证服务器162可以映射到HSS 224。

[0073] 图7A到图7B基于3GPP TS 33.402的图6.2-1。3GPP TS 33.402的图6.2-1示出了UE在经由受信任的非3GPP接入点连接时如何认证以及执行与3GPP接入网络的密钥协商。图7A到图7B连同下面的讨论一起示出了该处理可以如何被扩展以使得UE D/GSCL 221可以同时地与M2M服务器229引导自举、与其执行密钥协商、并向其注册。

[0074] 下面的消息描述示出了呼叫流如何被扩展以支持服务层引导自举。对于现有步骤的更详细描述,参考3GPP TS 33.402的图6.2-1。注意,尽管图7A到图7B基于经由受信任的非3GPP网络(例如包括直径连接-SWm)的UE D/GSCL认证,可以将服务层引导自举的增强应用于允许设备经由基于EAP的方法或其他类似手段认证的任何接入网络。

[0075] 参看图7A,在步骤247处,UE D/GSCL 241与接入点242相连接,接入点242是受信任的非3GPP接入点。在步骤248处,接入点242请求UE D/GSCL 241的身份。在步骤249处,UE D/GSCL 241发送对步骤248的身份请求的EAP响应。UE D/GSCL 241的身份可以是其网络接入标识(NAI)。步骤249的响应还可以包括AVP,该AVP承载包括接入网络公共ID(例如,3GPP外部标识符)、服务提供者标识符、或UE D/GSCL 241上的应用的应用ID的参数。服务提供者标识符可以是提供设备想要与其连接的服务层的公司的名称或者其可以命名设备想要与其连接的特定服务层(例如,NSCL ID)。应用ID(例如用于3GPP的D/GSCL ID;用于oneM2M的DA或NA)可以是请求应用(GA、DA、DSCL或GSCL)正在请求其被指派的名称。

[0076] 在步骤250处,接入点242将来自步骤249的信息发送到接入网络AAA服务器243,其也可以是HSS。步骤251到步骤254通常是在使用AKA'时完成的,尤其在UE D/GSCL 241和AAA服务器243之间的节点已经改变了步骤249中的原始EAP身份响应消息中的用户身份的情况下。在步骤251处,AAA服务器243请求UE D/GSCL 241的AKA'身份。在步骤252处,步骤251的请求被发送到UE D/GSCL 241。在步骤253处,UE D/GSCL 241用其标识来响应(类似于步骤249)。在步骤254处,接入点242将来自步骤253的信息发送到接入网络AAA服务器243。

[0077] 在步骤255处,基于来自HSS的订户信息,AAA服务器243验证UE D/GSCL 241被许可接入EPC并且验证UE D/GSCL 241被许可向在之前步骤中命名的M2M服务器246注册。为了进一步澄清,通常HSS可以被认为是保持订户信息的数据库。这里AAA服务器243是被允许接入HSS并且基于HSS中的信息进行AAA决策的服务器。在步骤256处,如果UE D/GSCL 241被许可接入所述接入网络,则AKA算法将被运行。而且,如果启用了"附接块启用"标志或者如果在步骤253中提供了NSCL ID,则AAA服务器243将发送消息到MTC-IWF 245的地址,MTC-IWF 245的地址在订户数据中提供。这里更详细讨论的,设备-许可-请求(DPR)命令可以利用行动-类型=设备附接请求、外部-ID、SCS-标识符来执行。步骤256处的消息在S6m参考点上被发送。该消息的目的是查看UE D/GSCL 241是否应该被允许附接或者M2M服务器246是否希

望附接请求被拒绝。如果在步骤253中提供了UE D/GSCL 241的名称，则该消息还用于向M2M服务器246提议UE D/GSCL 241的名称，使得UE D/GSCL 241可以被注册。

[0078] 在步骤257处，MTC-IWF 245发送消息到M2M服务器246以确定UE D/GSCL 241是否应该被允许附接。该消息在Tsp参考点上被发送。DPR命令可以利用行为-类型＝设备附接请求、外部-ID来执行。在步骤258处，M2M服务器246用UE D/GSCL 241是否应该被允许附接的指示来进行响应。如果M2M服务器246指示UE D/GSCL 241不应该被允许附接，则M2M服务器246向MTC-IWF 245提供原因并且M2M服务器246可以向MTC-IWF 245提供补偿时间。如果提供(例如，在步骤257处经由DPR)了UE D/GSCL 241的名称，则来自M2M服务器246的响应包括UE D/GSCL 241的名称。如果M2M服务器246接受提议的名称，则相同名称被提供回MTC-IWF。设备-许可-应答(DPA)命令可以针对步骤258而执行。

[0079] 在步骤259处，MTC-IWF 245向AAA服务器243发送M2M服务器246是否想要UE D/GSCL 241被允许附接的指示。如果M2M服务器246指示UE D/GSCL 241此时不需要被附接，则MTC-IWF 245向AAA服务器243提供原因和补偿时间。该消息在S6m参考点上发送，其可以使用DPA命令来执行。在步骤260处，EAP MSK和EMSK被生成。EAP MSK和EMSK是脱离EAP算法的标准密钥。服务层根密钥(Kmr)可以由AAA服务器生成，如ETSI M2M架构规范ETSI TS 102 690的第8.3.2.3节所述。Kmr等于(EMSK,“ETSI M2M设备-网络根密钥”|M2M-节点-ID|M2M-SP-ID)的散列。

[0080] 在步骤261处，AAA服务器243向UE D/GSCL 241发送EAP-请求。如果EAP方法是AKA’，则该消息包括随机询问(RAND)、网络认证矢量(AUTN)、以及消息认证代码(MAC)。该身份响应可以包括AVP，所述AVP承载诸如接入网络公共ID、NSCL ID、或所指派的应用ID(例如D/GSCL ID)的参数。接入网络公共ID可以被用作用于生成Kmr的M2M-节点_ID。NSCL ID表示UE应用(DA、GA、DSCL或GSCL)应该连接到的特定服务层，并且其是用于生成Kmr的M2M-SP-IN。所指派的应用ID表示已经被NSCL指派给应用的特定标识符。该值可以被用作用于生成Kmr的M2M-节点_ID。在步骤262处，接入点242向UE D/GSCL 241发送步骤261的消息。

[0081] 如图7B中所示，其是图7A的流的继续，在步骤263处，UE D/GSCL 241运行AKA算法并且验证AUTN是正确的以对网络进行认证。在该网络被验证之后，UE D/GSCL 214生成对RES的响应。服务层根密钥(例如Kmr)可以由UE D/GSCL 241来生成，如ETSI M2M架构规范的第8.3.2.3节中所述。Kmr等于(EMSK,“ETSI M2M设备-网络根密钥”|M2M-节点-ID|M2M-SP-ID)的散列。在步骤264处，UE D/GSCL 241发送对随机询问的RES。在步骤265处，AAA服务器243接收步骤264的RES。在步骤266处，AAA服务器243验证RES等于XRES。

[0082] 进一步参看图7B，在步骤267处，如果启用了“可达指标启用”标志或者如果在步骤253中提供了NSCL ID，则AAA服务器243向用于UE D/GSCL 241的订户数据中所提供的MTC-IWF 245的地址发送消息。如这里更详细讨论的，设备-通知-请求(DNR)命令可以利用行为-类型＝设备附接事件、外部-ID、M2M-标识符、密钥-材料、UE服务层ID来执行。步骤267处的消息在S6m参考点上被发送并且将最终通知M2M服务器246UE D/GSCL 241已经附接。

[0083] 在步骤268处，M2M服务器246在Tsp参考点上接收附接通知。DNR命令可以利用行为-类型＝设备附接事件、密钥-材料、外部-ID来执行。在步骤269处，M2M服务器246肯定步骤268的所接收的通知。这里更详细讨论的DNA命令，可以在步骤269处执行。在步骤270处，MTC-IWF 245在S6m参考点上向AAA服务器243发送步骤269的肯定。

[0084] 与步骤251到步骤254相类似，块271中的步骤通常仅仅在AKA’被使用时完成。在步骤272处，如果AAA服务器243和UE D/GSCL 241正在使用受保护的成功结果指示，则AAA服务器243在发送EAP-成功消息之前向UE D/GSCL 241发送EAP-请求/AKA’-通知消息。在步骤273处，接入点242向UE D/GSCL 241发送步骤272的响应。在步骤275处，UE D/GSCL 241发送EAP-响应/AKA’-通知消息，其在步骤274处被转发到AAA服务器243。在步骤276处，AAA服务器243发送EAP-成功消息，其在步骤277处被转发到UE D/GSCL 241。在步骤278处，UE D/GSCL 241被注册，但M2M服务器可能不知道UE D/GSCL 241的IP地址。UE D/GSCL 241可以开始mId上的通信或者M2M服务器246可以通过发送设备触发来开始通信。

[0085] 由于接入网络辅助引导自举，附加信息可以保留在允许使用该特征的设备的预订信息中。新的接入网络预订信息被添加到HSS中以支持服务层引导自举的授权。

[0086] 图8A是示例机器对机器(M2M)、物联网(IoT)或物的网络(WoT)通信系统10，其中一个或多个所公开的实施例可以被实现。通常，M2M技术提供用于IoT/WoT的建筑块，且任何M2M设备、网关或服务平台可以是IoT/WoT的组件以及IoT/WoT服务层等等。

[0087] 如图8A中所示，M2M/IoT/WoT通信系统10包括通信网络12。通信网络12可以是固定网络(例如，以太网、光纤、ISDN、PLC等)或无线网络(例如，WLAN、蜂窝等)或者异构网络的网络。例如，通信网络12可以包括多个接入网络，所述接入网络将诸如语音、数据、视频、消息传递、广播等的内容提供给多个用户。例如，通信网络12可采用一个或多个信道接入方法，诸如码分多址(CDMA)、时分多址(TDMA)、频分多址(FDMA)、正交FDMA(OFDMA)、单载波FDMA(SC-FDMA)等。此外，通信网络12可以包括其他网络，诸如核心网络、互联网、传感器网络、工业控制网络、个域网、融合的个人网络、卫星网络、家庭网络或企业网络等。

[0088] 如图8A中所示，M2M/IoT/WoT通信系统10可以包括基础设施域和现场域。基础设施域指的是端到端M2M部署的网络侧，且现场域指的是区域网络，通常在M2M网关之后。现场域包括M2M网关14和终端设备18。将认识到，任何数量的M2M网关设备14和M2M终端设备18可以如所需被包括在M2M/IoT/WoT通信系统10中。M2M网关设备14和M2M终端设备18中的每一个被配置成经由通信网络12或直接无线电链路发射和接收信号。M2M网关设备14允许无线M2M设备(例如蜂窝式和非蜂窝式)以及固定网络M2M设备(例如PLC)通过诸如通信网络12的运营商网络或直接无线电链路来通信。例如，M2M设备18可以收集数据，并且经由通信网络12或直接无线电链路而将数据发送到M2M应用20或M2M设备18。M2M设备18也可以从M2M应用20或M2M设备18接收数据。进一步，如下所述，数据和信号可以如下所述经由M2M服务层22被发送到M2M应用20以及从其接收。M2M设备18和网关14可以经由包括例如蜂窝、WLAN、WPAN(例如，Zigbee、6LoWPAN、蓝牙)、直接无线电链路和有线线路的各种网络来通信。

[0089] 参看图8B，图示的现场域中的M2M服务层22(例如，这里所述的网络服务能力层(NSCL))提供用于M2M应用20、M2M网关设备14和M2M终端设备18以及通信网络12的服务。应理解，视需要，M2M服务层22可以与任何数量的M2M应用、M2M网关设备14、M2M终端设备18和通信网络12通信。M2M服务层22可以由一个或多个服务器、计算机等来实现。M2M服务层22提供应用于M2M终端设备18、M2M网关设备14和M2M应用20的服务能力。M2M服务层22的功能可以用多种方式来实现，例如实现为Web服务器、实现在蜂窝核心网络中、实现在云中等等。

[0090] 类似于所图示的M2M服务层22，在基础设施域中存在M2M服务层22’。M2M服务层22’提供用于在基础设施域中的M2M应用20’以及下层通信网络12’的服务。M2M服务层22’还提

供用于现场域中的M2M网关设备14和M2M终端设备18的服务。将理解，M2M服务层22’可以与任何数量的M2M应用、M2M网关设备和M2M终端设备通信。M2M服务层22’可以通过不同服务提供者与服务层交互。M2M服务层22’可以由一个或多个服务器、计算机、虚拟机(例如云/计算机/存储库等等)等来实现。

[0091] 还是参看图8B，M2M服务层22和22’提供各种应用和纵向产品可利用的服务交付能力的核心集合。这些服务能力使得M2M应用20和20’能够与设备交互，且执行诸如数据收集、数据分析、设备管理、安全性、计费、服务/设备发现等功能。基本上，这些服务能力使应用摆脱实现这些功能性的负担，由此简化了应用开发并降低成本并缩短上市时间。服务层22和22’还使得M2M应用20和20’结合服务层22和22’提供的服务通过各种网络12和12’而通信。

[0092] 在一些实施例中，M2M应用20和20’可以包括如这里所讨论的使用EAP的通信的所需的应用。M2M应用20和20’可以包括各种行业的应用，诸如(但不限于)运输、健康和保健、家庭联网、能源管理、资产追踪、以及安全和监控。如上所述，横跨系统的设备、网关和其他服务器运行的M2M服务层支持诸如例如数据收集、设备管理、安全性、计费、位置追踪/地理围栏、设备/服务发现、和遗留系统集成等功能，并且将这些功能作为服务提供到M2M应用20和20’。

[0093] 在本申请中使用的EAP相关方法(例如，基于EA-PANA或EAP接入网络的方法)可以被实现为服务层的一部分。服务层(例如，UE D/GSCL 191)是软件中间件层，其通过应用编程接口(API)集合和下层网络互连接口而支持增值服务能力。M2M实体(例如，诸如设备、网关或可以由硬件和软件组合实现的服务/平台的M2M功能实体)可以提供应用或服务。ETSI M2M和oneM2M都使用可包含本发明的EAP相关方法的服务层。ETSI M2M的服务层被称为服务能力层(SCL)。SCL可以在M2M设备内实现(被称为设备SCL(DSCL))、在网关内实现(被称为网关SCL(GSCL))和/或在网络节点内实现(被称为网络SCL(NSCL))。oneM2M服务层支持公共服务功能(CSF)(即服务能力)集合。一个或多个特定类型的CSF的集合的实例被称为公共服务实体(CSE)，其可以被托管在不同类型的网络节点上(例如，基础设施节点、中间节点、专用节点)。进一步，本申请的EAP相关方法可以被实现为使用面向服务架构(SOA)和/或面向资源架构(ROA)的M2M网络的一部分以访问诸如本申请的EAP相关方法的服务。

[0094] 图8C是示例M2M设备30，诸如例如M2M终端设备18或M2M网关设备14的系统图。如图8C中所示，M2M设备30可以包括处理器32、收发器34、发射/接收元件36、扬声器/麦克风38、键盘40、显示器/触摸板42、不可移除存储器44、可移除存储器46、电源48、全球定位系统(GPS)芯片组50、以及其他外围设备52。应了解，M2M设备30可以包括前述元件的任何子组合，同时仍保持与实施例一致。该设备可以是使用所公开的用于使用EAP-PANA来引导自举的系统和方法的设备。

[0095] 处理器32可以是通用处理器、专用处理器、常规处理器、数字信号处理器(DSP)、多个微处理器、与DSP核心相关联的一个或多个微处理器、控制器、微控制器、专用集成电路(ASIC)、现场可编程门阵列(FPGA)电路、任何其他类型的集成电路(IC)、状态机等。处理器32可以执行信号编码、数据处理、功率控制、输入/输出处理、和/或使得M2M设备30能够在无线环境中操作的任何其他功能。处理器32可以耦合到收发器34，收发器34可以耦合到发射/接收元件36。虽然图8C将处理器32和收发器34描绘为独立组件，将认识到，处理器32和收发器34可以被一起集成到电子封装或芯片中。处理器32可以执行应用层程序(例如浏览器)

和/或无线电接入层(RAN)程序和/或通信。处理器32可以诸如在接入层和/或应用层执行诸如认证认证、安全密钥协商、和/或加密操作的安全操作。

[0096] 发射/接收元件36可以被配置为发射信号到M2M服务平台22或者从M2M服务平台22接收信号。例如,在实施例中,发射/接收元件36可以是被配置成发射和/或接收RF信号的天线。发射/接收元件36可以支持各种网络和无线接口,诸如WLAN、WPAN、蜂窝等。在实施例中,发射/接收元件36可以是被配置成发射和/或接收例如IR、UV或可见光信号的发射器/检测器。在另一实施例中,发射/接收元件36可以被配置成发射和接收RF和光信号二者。将认识到,发射/接收元件36可以被配置为发射和/或接收无线或有线信号的任何组合。

[0097] 此外,尽管发射/接收元件36在图8C中被描绘为单一元件,但M2M设备30可以包括任何数量的发射/接收元件36。更具体地,M2M设备30可以使用MIMO技术。因此,在实施例中,M2M设备30可以包括用于发射和接收无线信号的两个或更多发射/接收元件36(例如,多个天线)。

[0098] 收发器34可以被配置为调制将由发射/接收元件36发射的信号,并且解调由发射/接收元件36接收的信号。如上所述,M2M设备30可以具有多模式能力。因此,例如,收发器34可以包括用于使M2M设备30能够经由多个RAT诸如UTRA和IEEE 802.11通信的多个收发器。

[0099] 处理器32可以从任何类型的适当存储器,诸如不可移除存储器44和/或可移除存储器46,访问信息,并将数据存储在其中。不可移除存储器44可以包括随机存取存储器(RAM)、只读存储器(ROM)、硬盘、或任何其他类型存储器存储设备。可移除储器46可以包括用户身份模块(SIM)卡、存储棒、安全数字(SD)存储卡等。在其它实施例中,处理器32设备可从未物理地位于M2M设备30上(诸如位于服务器上或家用计算机上)的存储器访问信息,并将数据存储在其中。处理器32可以被配置成控制显示器或指示器42上的发光模式、图像、或颜色,以响应在这里所述的一些实施例中的引导自举(例如,使用EAP的引导自举)成功或不成功,或者指示资源传播过程的状态。经由显示器42观看的用户接口可以向用户给出使用EAP-PANA、基于EAP接入网络的方法、GBA等用于认证的选项。

[0100] 处理器32可以从电源48接收电力,并且可以被配置为分配和/或控制电力到M2M设备30中的其它组件。电源48可以是用于向M2M设备30供电的任何适当的设备。例如,电源48可以包括一个或多个干电池(例如,镍镉(NiCd)、镍锌(NiZn)、镍金属氢化物(NiMH)、锂离子(Li离子)等)、太阳能电池、燃料电池等。

[0101] 处理器32还可以耦合到GPS芯片组50,GPS芯片组50被配置为提供关于M2M设备30的当前位置的位置信息(例如经纬度)。将认识到,M2M设备30可以通过任何适当位置确定方法来获取位置信息,同时保持与实施例一致。

[0102] 处理器32可以进一步被耦合到其他外围设备52,外围设备52可以包括提供额外特征、功能和/或有线或无线连通性的一个或多个软件和/或硬件模块。例如,外围设备52可以包括加速度计、电子罗盘、卫星收发器、传感器、数码相机(用于照片或视频)、通用串行总线(USB)端口、振动设备、电视收发器、免提耳机、蓝牙®模块、调频(FM)无线电单元、数字音乐播放器、媒体播放器、视频游戏播放器模块、互联网浏览器等。

[0103] 图8D是可以例如实现图8A和图8B的M2M服务平台22的示例性计算系统90的框图。计算系统90可以包括计算机或服务器,并且可以主要由计算机可读指令控制,计算机可读指令可以是软件的形式,而不管该软件是在何处或通过何种方式来存储或访问。这些计算

机可读指令可以在中央处理单元(CPU)91内执行,以使得计算系统90工作。在许多已知工作站、服务器和个人计算机中,中央处理单元91是由被称为微处理器的单芯片CPU实现的。在其他机器中,中央处理单元91可以包括多个处理器。协同处理器81是与主CPU 91不同的可选处理器,其用于执行额外功能或辅助CPU 91。CPU 91和/或协同处理器81可以接收、生成、和处理与所公开的系统和用于EAP的方法相关的数据,诸如交换设备认证消息。

[0104] 操作中,CPU 91取得、解码和执行指令,并且经由计算机的主数据转移路径系统总线80,将信息转移到其他资源以及从其他资源转移信息。这样的系统总线将计算系统90中的组件相连并且限定数据交换的媒介。系统总线80通常包括用于发送数据的数据线路、用于发送地址的地址线路、以及用于发送中断和用于操作系统总线的控制线路。这样的系统总线80的示例是PCI(外围组件互连)总线。

[0105] 耦合到系统总线80的存储器设备包括随机存取存储器(RAM)82和只读存储器(ROM)93。这些存储器包括允许存储和检索信息的电路。ROM 93通常包含不能轻易被修改的所存储数据。在RAM 82中存储的数据可以被CPU 91或其他硬件设备读取或改变。对RAM 82和/或ROM 93的存取可以由存储器控制器92来控制。存储器控制器92可以提供地址转换功能,随着指令被执行,地址转换功能将虚拟地址转换为物理地址。存储器控制器92还可以提供存储器保护功能,所述存储器保护功能隔离系统内的进程,并且将系统进程与用户进程隔离。这样,运行在第一模式下的程序可以只能访问由其自身的进程虚拟地址空间所映射的存储器;该程序不能访问另一进程的虚拟地址空间内的存储器,除非已经设置了进程之间的存储器共享。

[0106] 此外,计算系统90可以包含外围设备控制器83,外围设备控制器83负责将指令从CPU 91传送到诸如打印机94、键盘84、鼠标95和磁盘驱动器85的外围设备。

[0107] 由显示器控制器96控制的显示器86被用于显示由计算系统90生成的视觉输出。这样的视觉输出可以包括文本、图形、动画图形、和视频。显示器86可以利用基于CRT的视频显示器、基于LCD的平板显示器、基于气体等离子的平板显示器、或触摸板来实现。显示器控制器96包括产生被发送到显示器86的视频信号所需的电子组件。

[0108] 进一步,计算系统90可以包含网络适配器97,网络适配器97可以用于将计算系统90连接到外部通信网络,诸如图8A和图8B的网络12。

[0109] 应该理解,上文所述的任何或所有系统、方法和处理可以以存储在计算机可读存储介质上的计算机可执行指令的方式来实现,所述指令当由诸如计算机、服务器、M2M终端设备、M2M网关设备等的机器执行时,执行和/或实现这里所述的系统、方法和处理。具体地,上述的步骤、操作或功能中的任何一个可以以这样的计算机可执行指令的形式来实现。计算机可读存储介质包括易失性和非易失性、可移动和不可移动介质,以用于信息存储的任何方法或技术来实现,但这样的计算机可读存储介质不包括信号。计算机可读存储介质包括,但不限于,RAM、ROM、EEPROM、闪速存储器或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光盘存储、磁带盒、磁条、磁盘存储或其他磁性存储设备、或者能够用于存储所期望的信息且由计算机存取的任何其他物理介质。

[0110] 在描述本公开的主题的优选实施例时,如图所图示,为了清楚起见而使用了特定术语。然而,所要求的主题不旨在限于所选择的特定术语,且应该理解,每个特定元件包括以类似方式操作以实现类似目的的所有技术等同物。

[0111] 本书面描述使用示例来公开本发明(包括最佳模式)还使得本领域的任何技术人员能够实践本发明,包括做出和使用任何设备或系统并执行任何所并入的方法。本发明的可取得专利的范围由权利要求限定,并且可以包括本领域技术人员想到的其他示例。如果这些其他示例具有不与权利要求文字表述不同的结构元件或者如果这些其他示例包括具有与权利要求的文字表述的非实质性不同的等同结构元件,则这些其他示例旨在处于权利要求的范围之内。

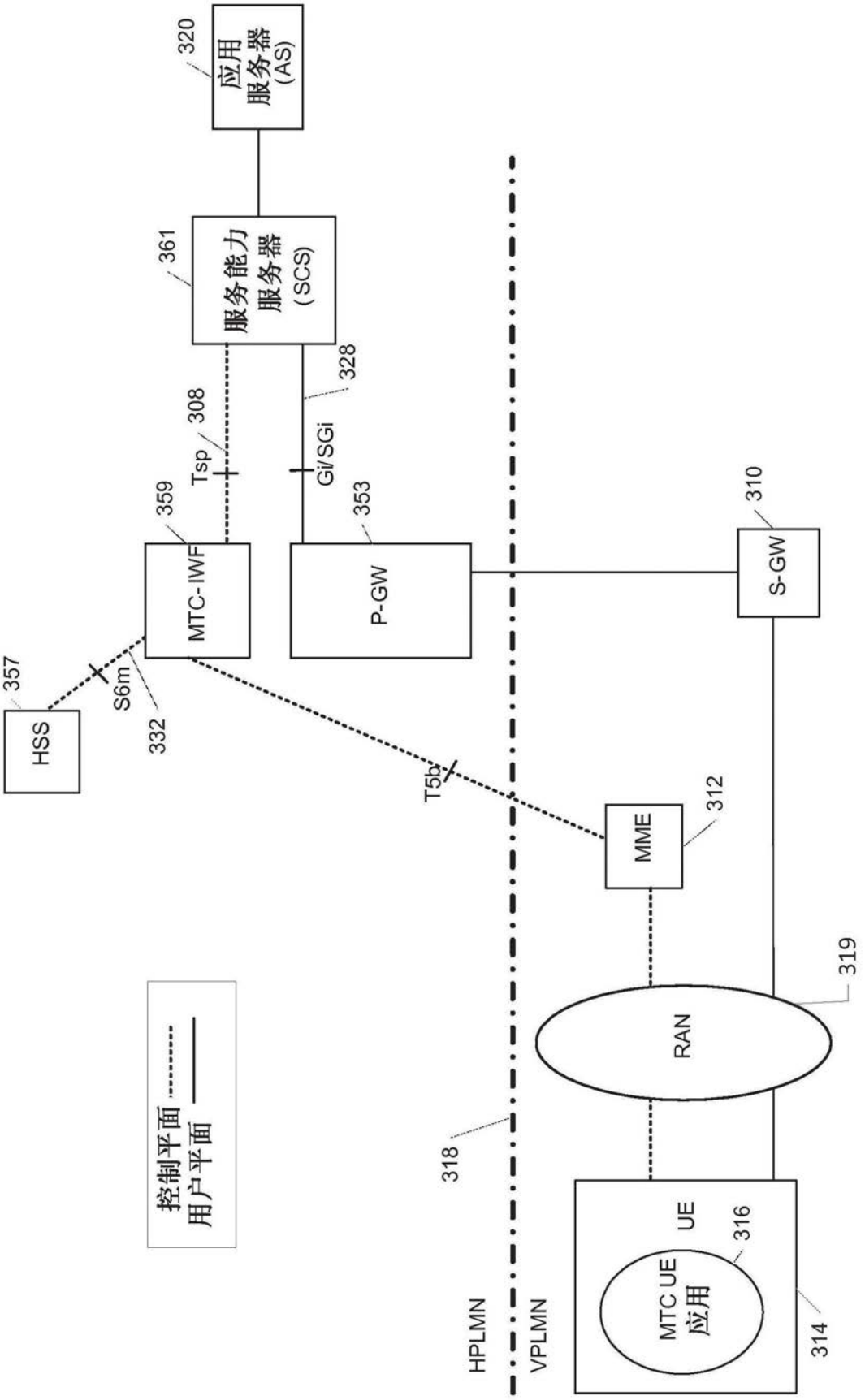

320
应用服务器(AS)
361
服务能力服务器(SCS)
328
308
Tsp
Gi/SGi
359
353
310
MTC-IWF
P-GW
S-GW
357
HSS
S6m
332
T5b
312
MME
319
RAN
318
UE
316
MTC UE应用
314
HPLMN
VPLMN
控制平面
用户平面

图1

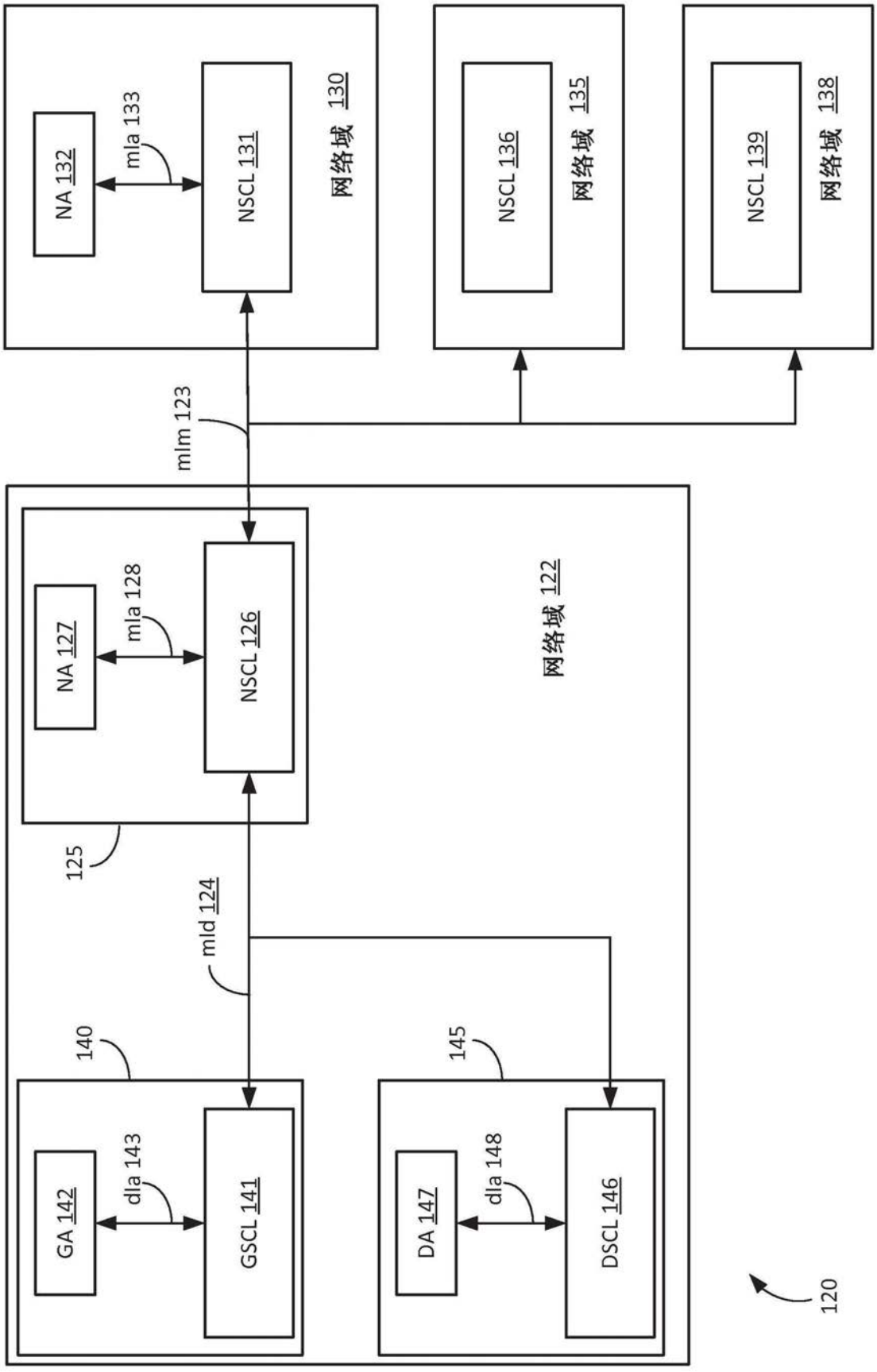

网络域 130
NA 132
mla 133
NSCL 131
网络域 135
NSCL 136
网络域 138
NSCL 139
mlm 123
网络域 122
NA 127
mla 128
NSCL 126
125
mld 124
140
GA 142
dla 143
GSCL 141
145
DA 147
dla 148
DSCL 146
120

图2

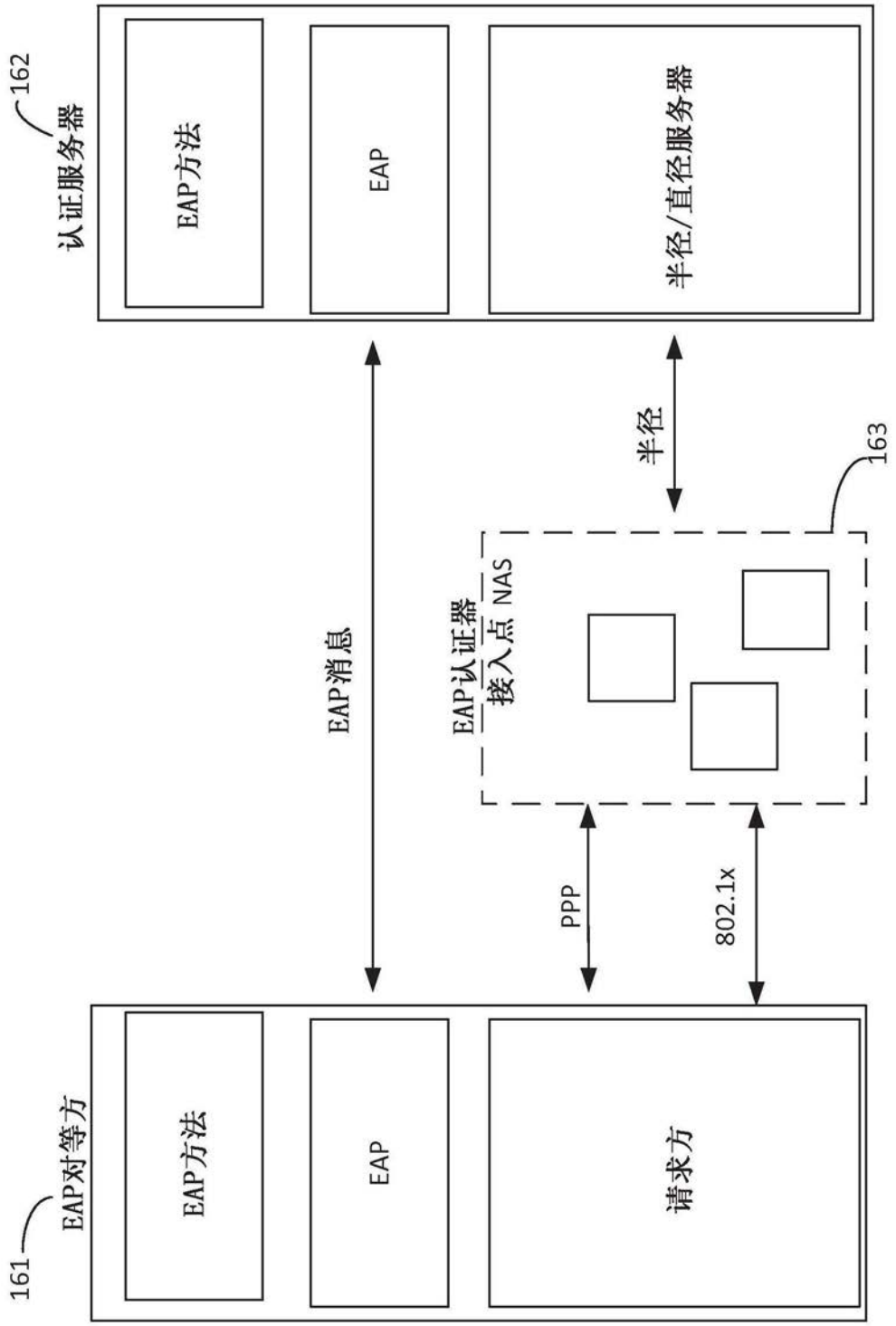

162
认证服务器
EAP方法
EAP
半径/直径服务器
半径
163
EAP消息
EAP认证器
接入点 NAS
PPP
802.1x
161
EAP对等方
EAP方法
EAP
请求方

图3

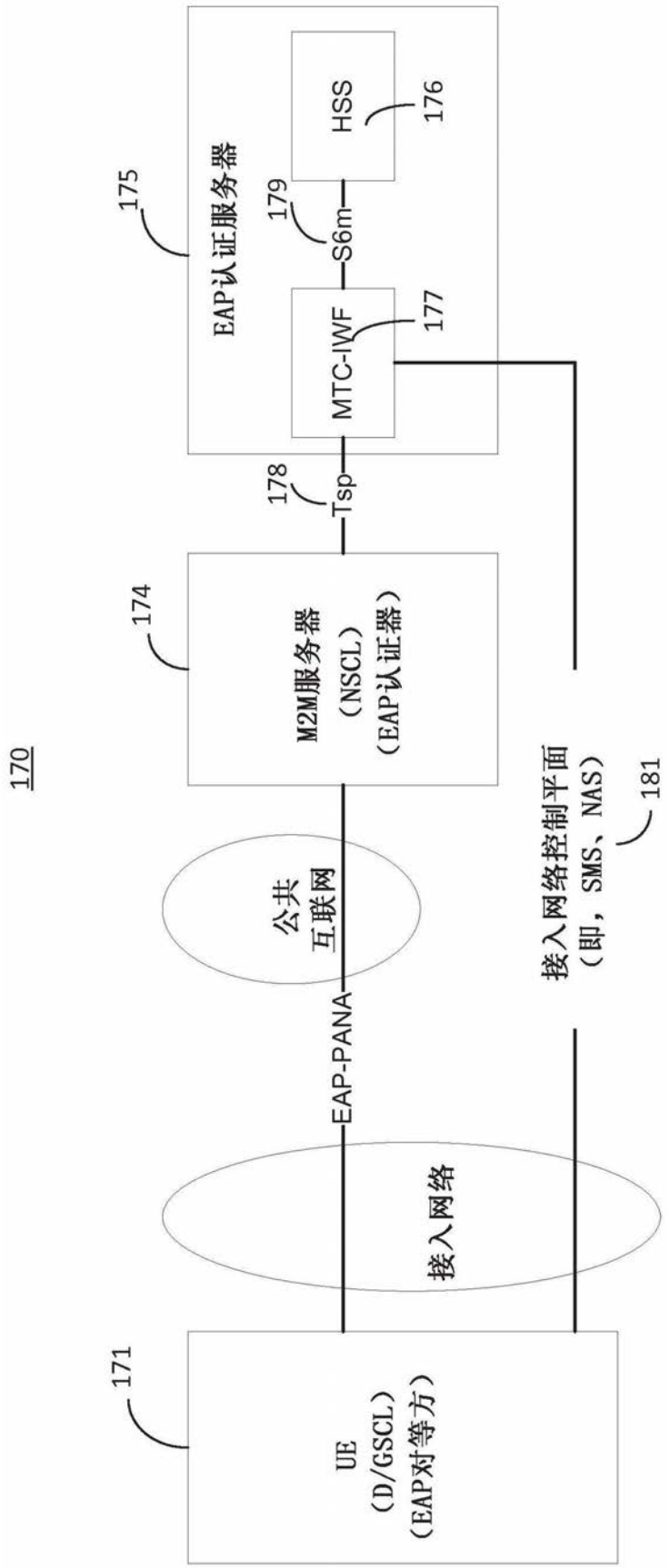

170
171
UE
(D/GSCL)
(EAP对等方)
接入网络
EAP-PANA
公共
互联网
174
M2M服务器
(NSCL)
(EAP认证器)
178
Tsp
175
EAP认证服务器
179
S6m
HSS
176
MTC-IWF
177
接入网络控制平面
(即，SMS、NAS)
181

图4

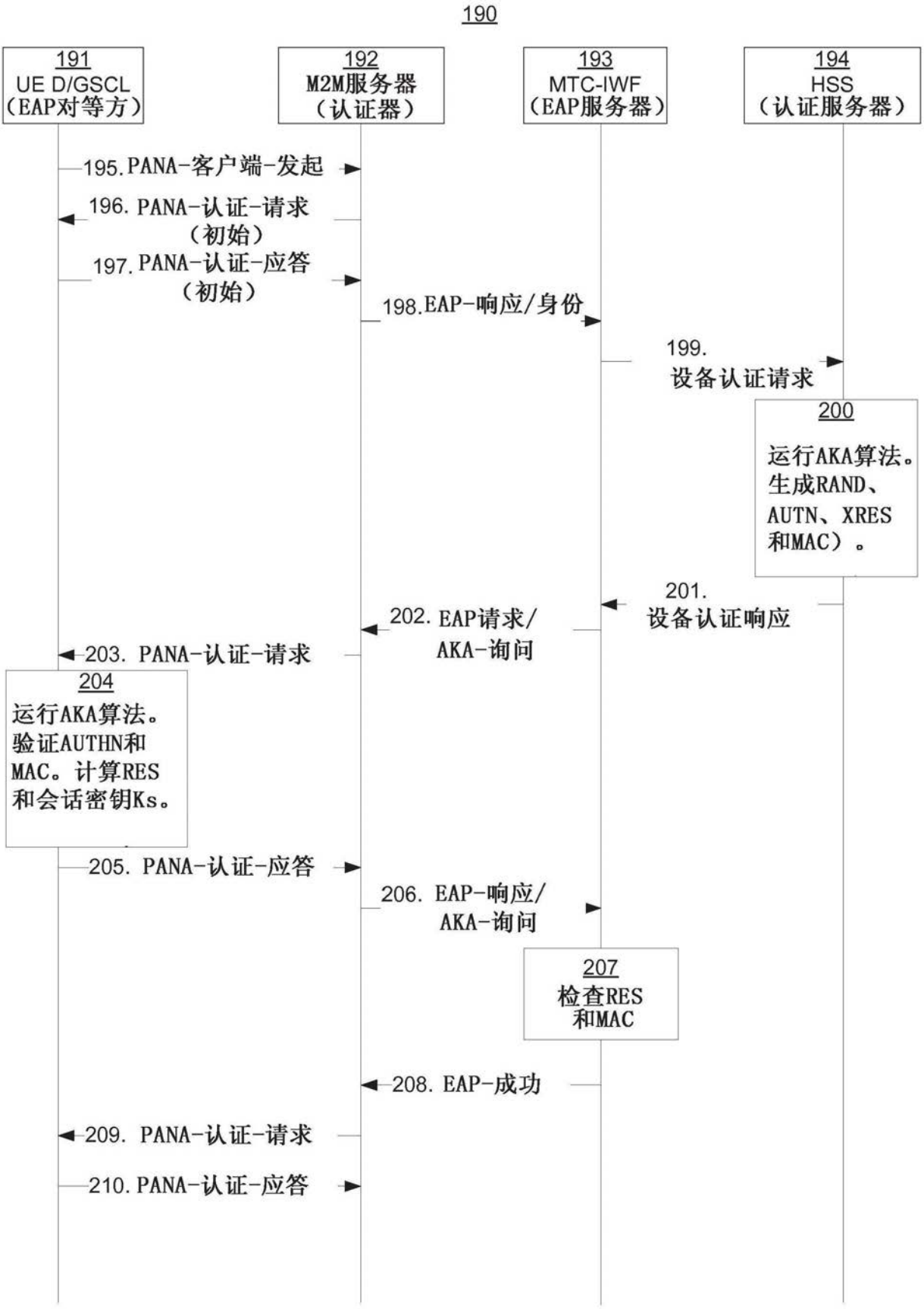

190
191
UE D/GSCL
(EAP对等方)
192
M2M服务器
(认证器)
193
MTC-IWF
(EAP服务器)
194
HSS
(认证服务器)
195.PANA-客户端-发起
196. PANA-认证-请求
(初始)
197. PANA-认证-应答
(初始)
198.EAP-响应/身份
199.
设备认证请求
200
运行AKA算法。
生成RAND、
AUTN、XRES
和MAC)。
201.
设备认证响应
202. EAP请求/
AKA-询问
203. PANA-认证-请求
204
运行AKA算法。
验证AUTHN和
MAC。计算RES
和会话密钥Ks。
205. PANA-认证-应答
206. EAP-响应/
AKA-询问
207
检查RES
和MAC
208. EAP-成功
209. PANA-认证-请求
210. PANA-认证-应答

图5

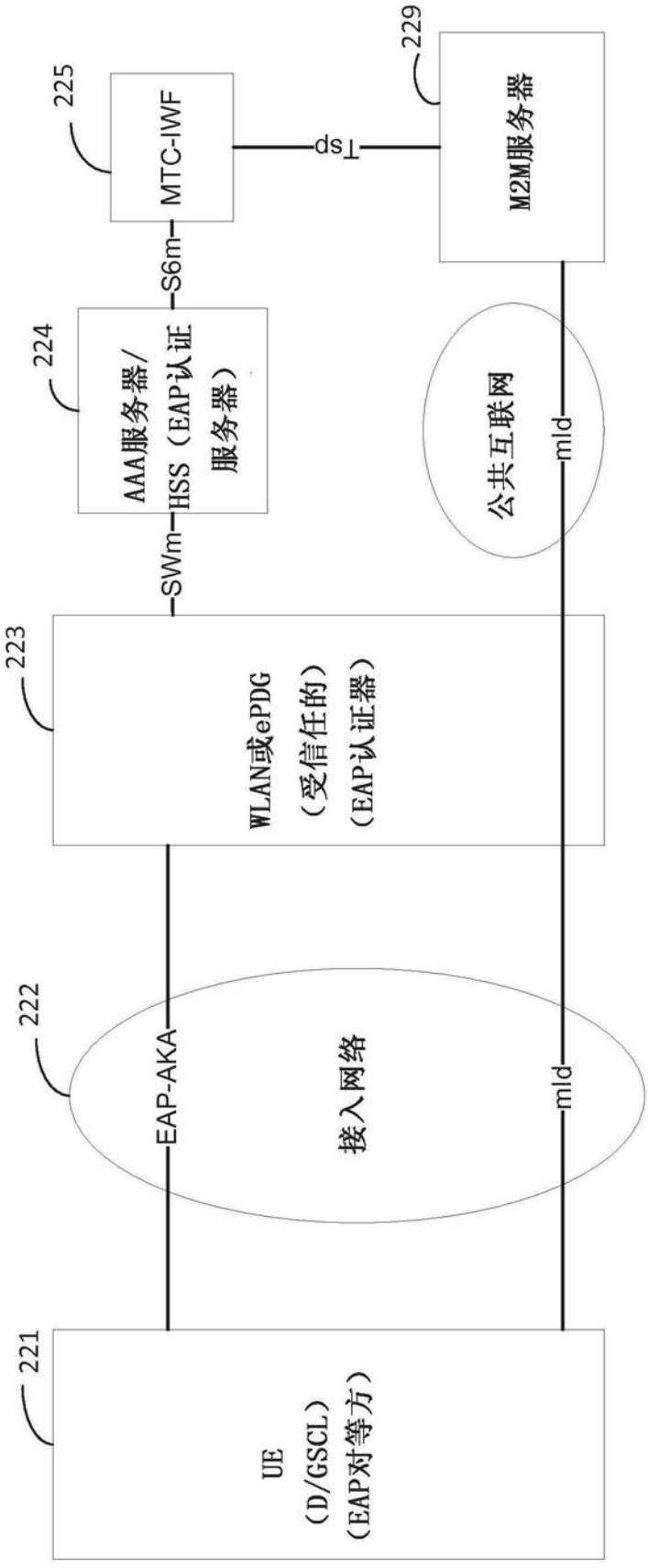

221
UE
（D/GSCL）
（EAP对等方）
222
接入网络
EAP-AKA
mld
223
WLAN或ePDG
（受信任的）
（EAP认证器）
SWm
224
AAA服务器/
HSS（EAP认证
服务器）
S6m
225
MTC-IWF
Tsp
229
M2M服务器
公共互联网
mld

图6

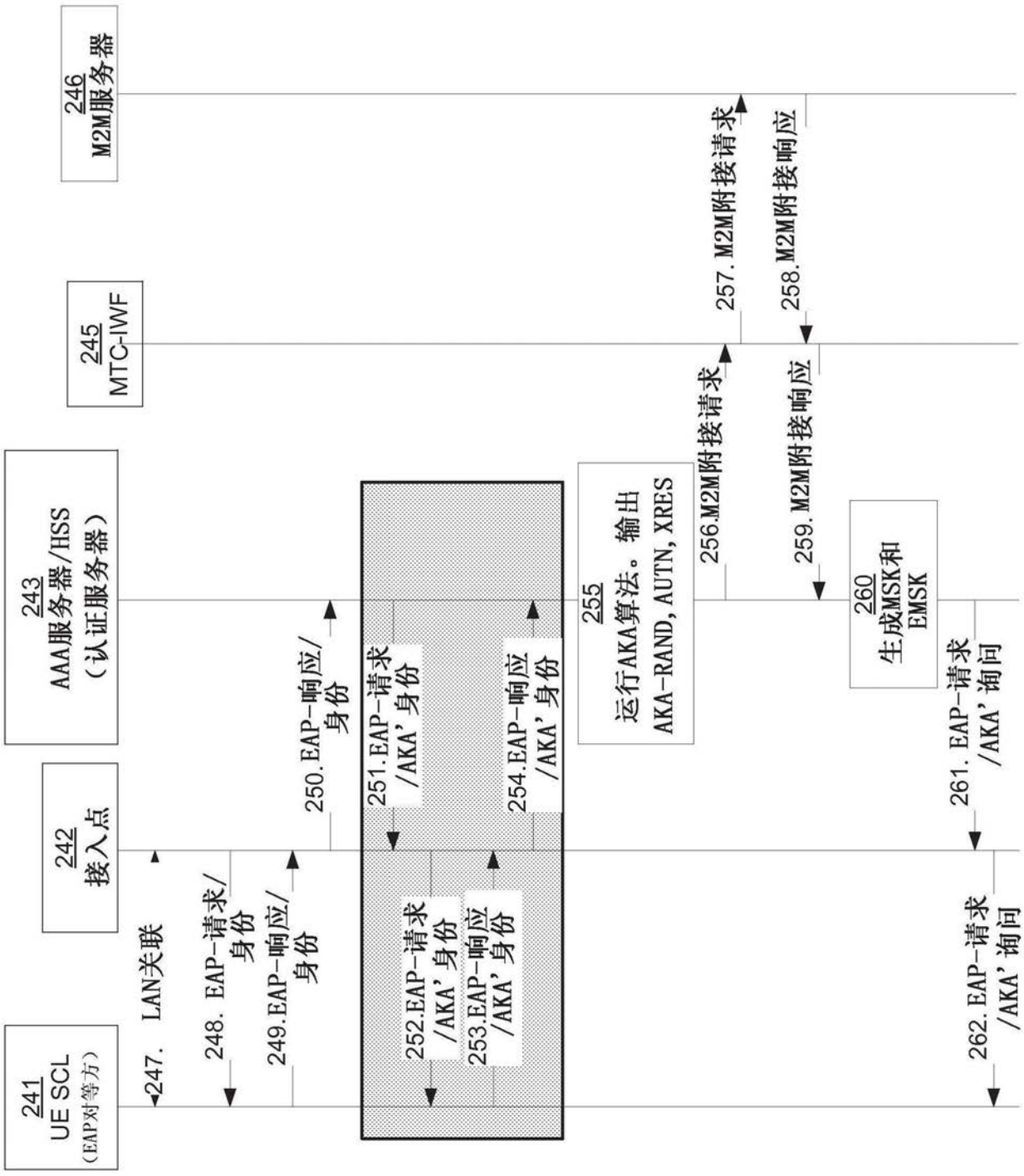

241
UE SCL
(EAP对等方)
242
接入点
243
AAA服务器/HSS
(认证服务器)
245
MTC-IWF
246
M2M服务器
247. LAN关联
248. EAP-请求/
身份
249.EAP-响应/
身份
250. EAP-响应/
身份
251.EAP-请求
/AKA'身份
252.EAP-请求
/AKA'身份
253.EAP-响应
/AKA'身份
254.EAP-响应
/AKA'身份
255
运行AKA算法。输出
AKA-RAND, AUTN, XRES
256.M2M附接请求
257. M2M附接请求
258.M2M附接响应
259. M2M附接响应
260
生成MSK和
EMSK
261. EAP-请求
/AKA'询问
262. EAP-请求
/AKA'询问

图7A

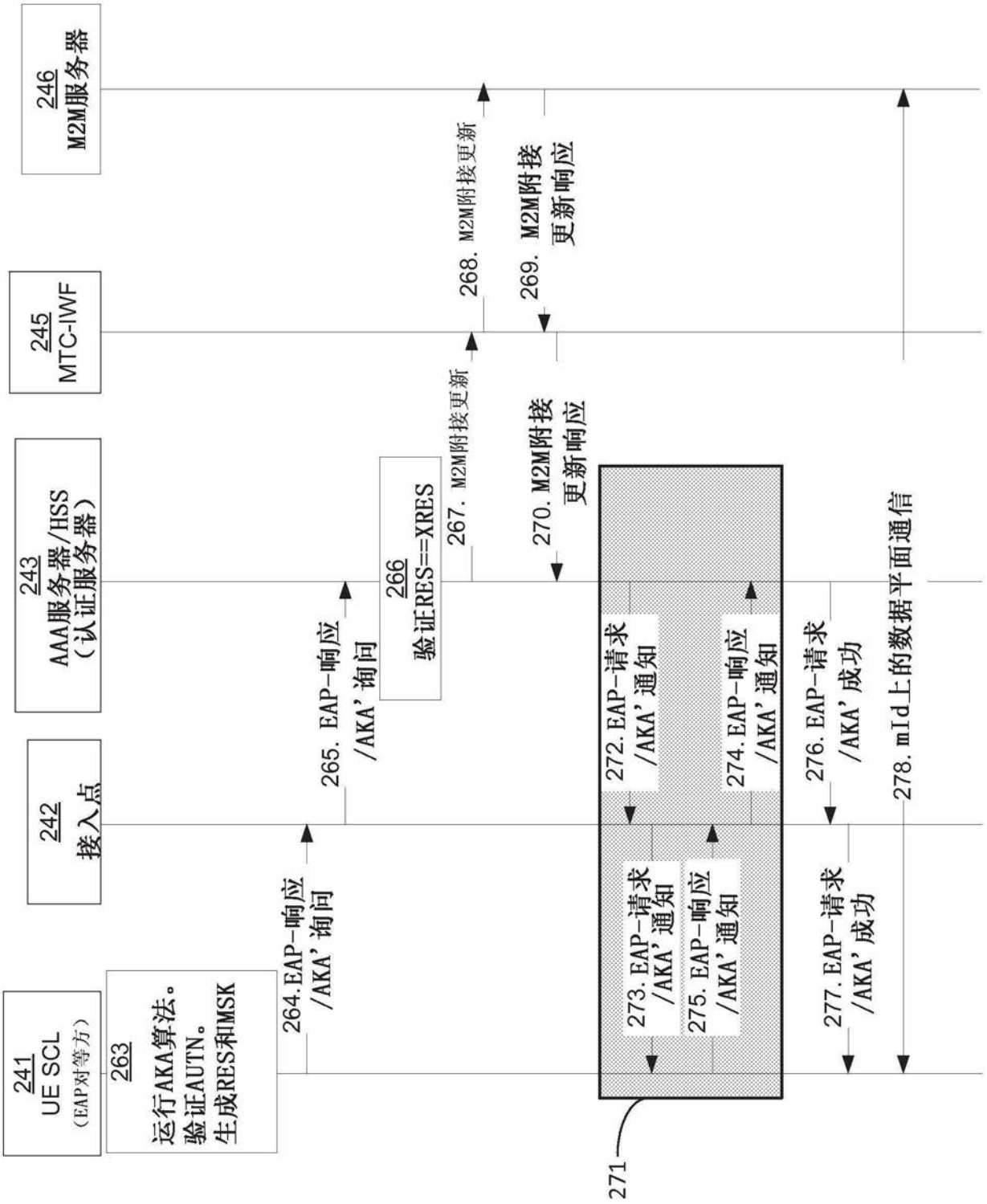

241
UE SCL
(EAP对等方)
263
运行AKA算法。
验证AUTN。
生成RES和MSK
242
接入点
243
AAA服务器/HSS
(认证服务器)
245
MTC-IWF
246
M2M服务器
264.EAP-响应
/AKA'询问
265. EAP-响应
/AKA'询问
266
验证RES==XRES
267. M2M附接更新
268. M2M附接更新
269. M2M附接
更新响应
270. M2M附接
更新响应
271
272. EAP-请求
/AKA'通知
273. EAP-请求
/AKA'通知
274. EAP-响应
/AKA'通知
275. EAP-响应
/AKA'通知
276. EAP-请求
/AKA'成功
277. EAP-请求
/AKA'成功
278. mId上的数据平面通信

图7B

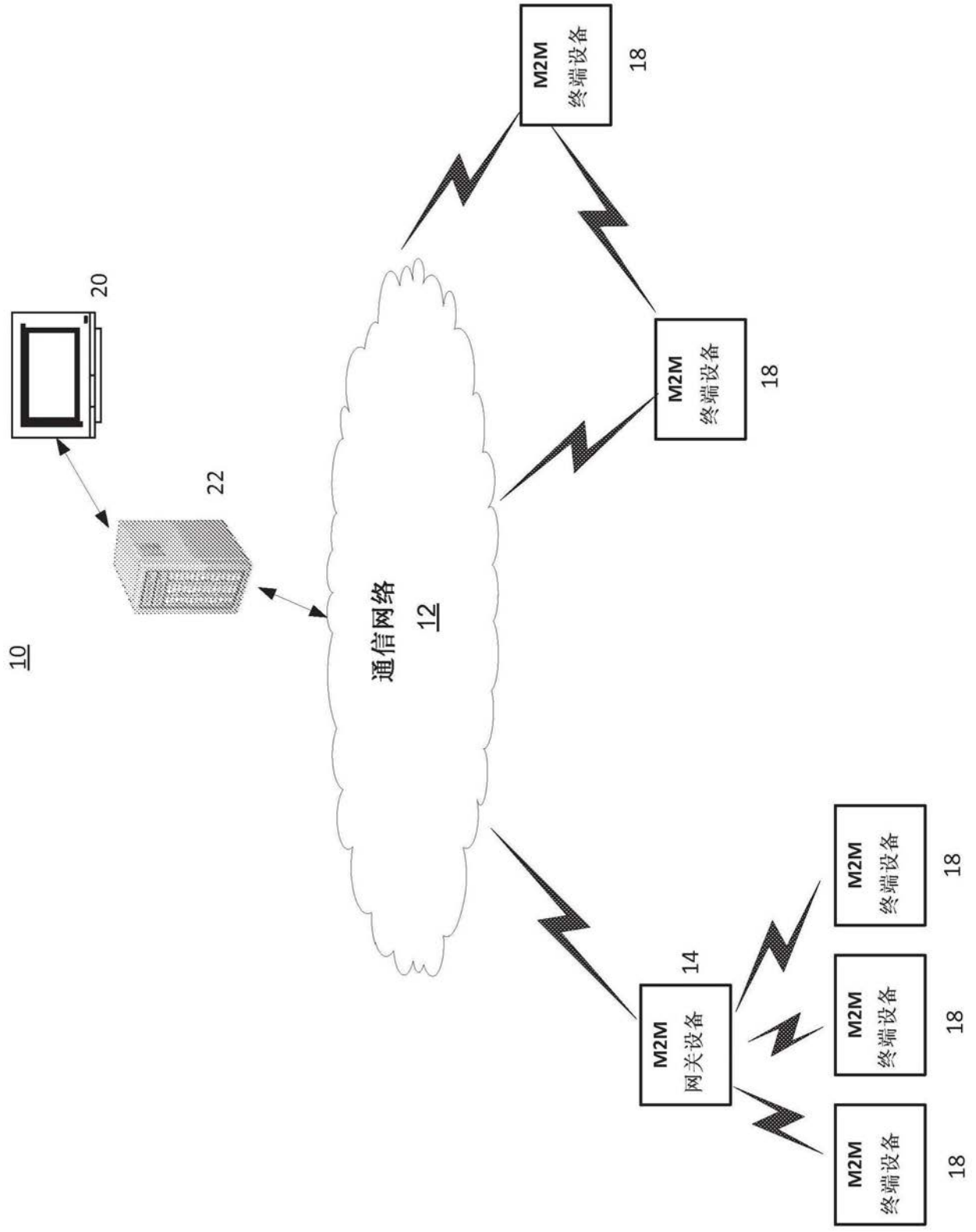

M2M
终端设备
18
M2M
终端设备
18
20
22
通信网络
12
10
M2M
网关设备
14
M2M
终端设备
18
M2M
终端设备
18
M2M
终端设备
18

图8A

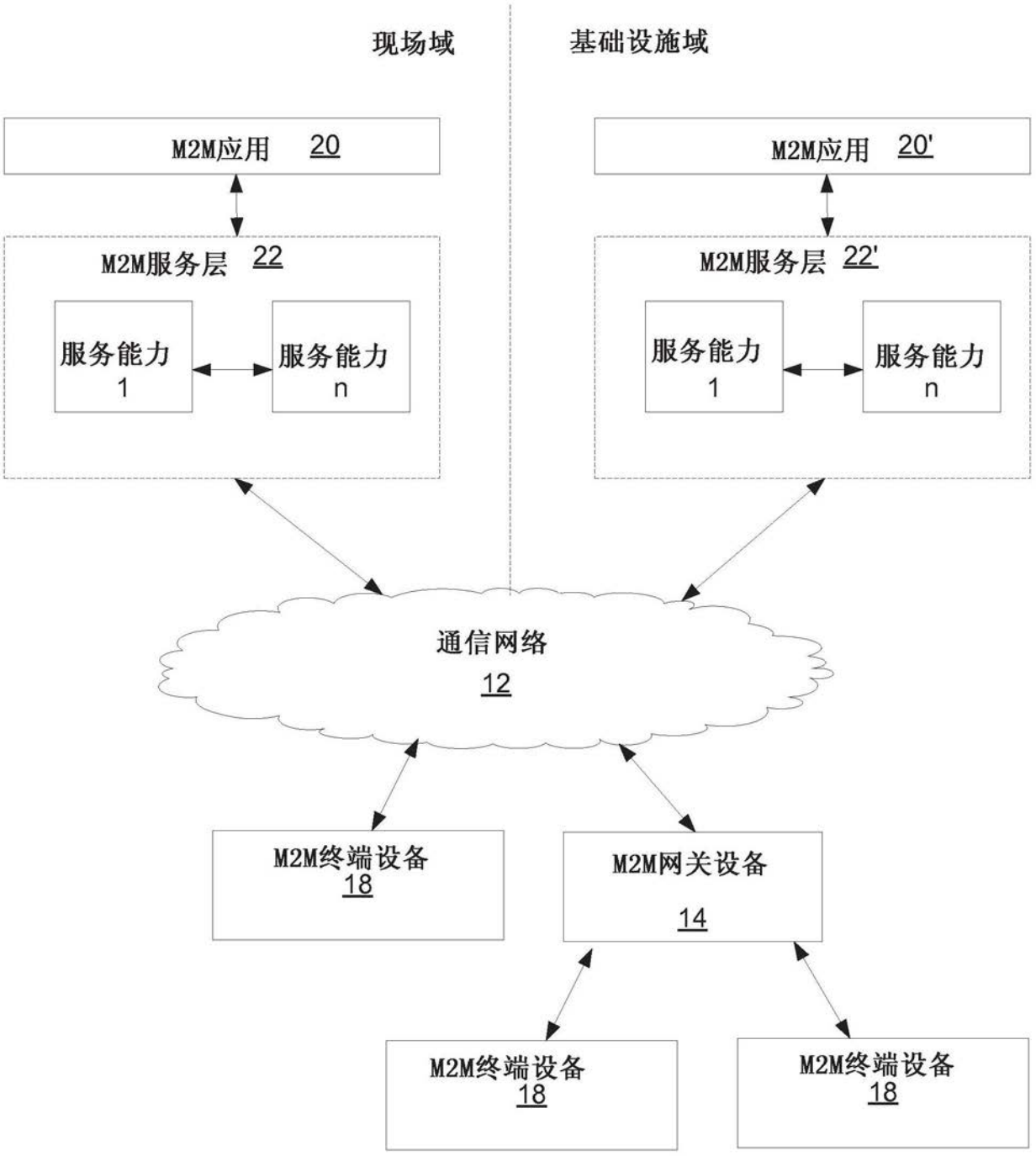

现场域
基础设施域
M2M应用 20
M2M应用 20'
M2M服务层 22
M2M服务层 22'
服务能力 1
服务能力 n
服务能力 1
服务能力 n
通信网络 12
M2M终端设备 18
M2M网关设备 14
M2M终端设备 18
M2M终端设备 18

图8B

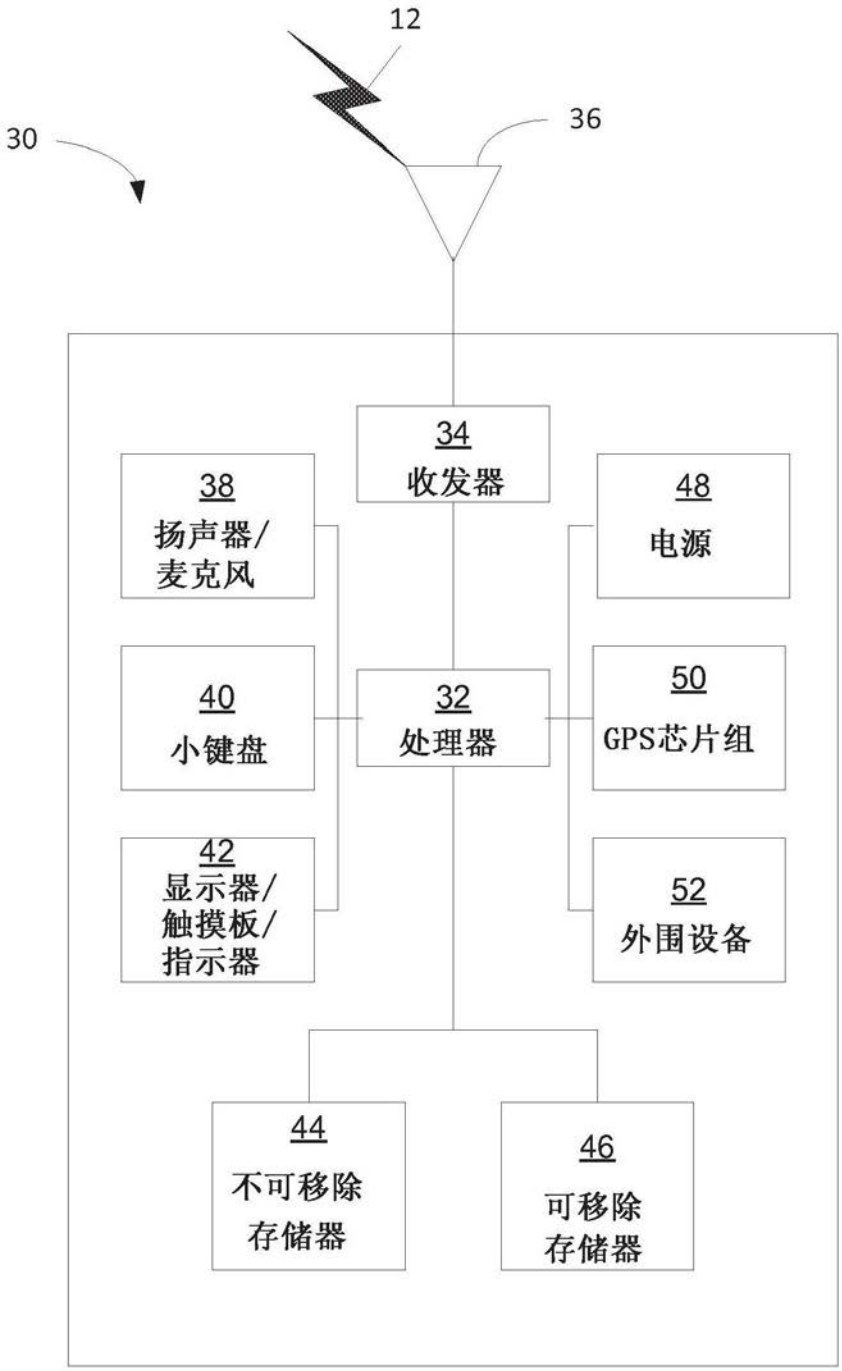

12
36
30
34
收发器
38
扬声器/
麦克风
48
电源
40
小键盘
32
处理器
50
GPS芯片组
42
显示器/
触摸板/
指示器
52
外围设备
44
不可移除
存储器
46
可移除
存储器

图8C

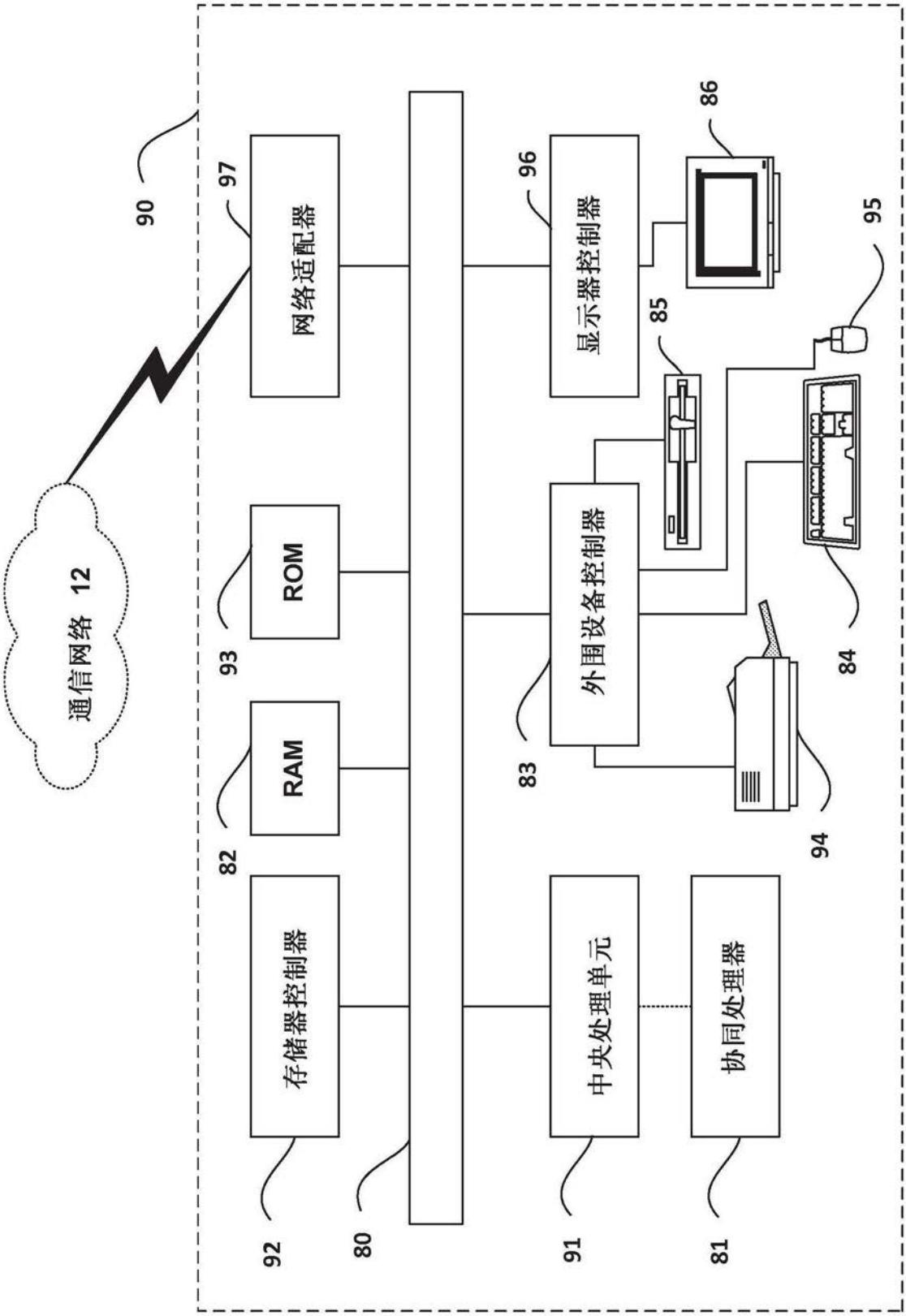

通信网络 12
90
网络适配器
97
ROM
93
RAM
82
存储器控制器
92
80
显示器控制器
96
外围设备控制器
83
中央处理单元
91
协同处理器
81
86
85
95
84
94

图8D