(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 103597774 B
(45)授权公告日 2017.11.07

(21)申请号 201280029345.9

(22)申请日 2012.04.16

(65)同一申请的已公布的文献号
申请公布号 CN 103597774 A

(43)申请公布日 2014.02.19

(30)优先权数据
61/475,972 2011.04.15 US
61/485,275 2011.05.12 US
61/544,577 2011.10.07 US

(85)PCT国际申请进入国家阶段日
2013.12.13

(86)PCT国际申请的申请数据
PCT/KR2012/002874 2012.04.16

(87)PCT国际申请的公布数据
WO2012/141555 EN 2012.10.18

(73)专利权人 三星电子株式会社
地址 韩国京畿道

(72)发明人 A.耶金 白令教

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 邵亚丽

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 101299666 A,2008.11.05,全文.
US 2003/0179885 A1,2003.09.25,全文.
CN 101039311 A,2007.09.19,全文.
US 2009/0191857 A1,2009.07.30,全文.

审查员 王田园

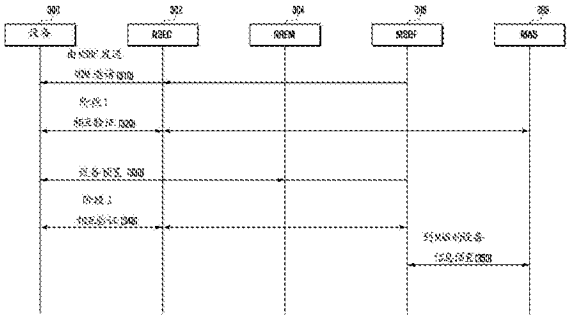
权利要求书2页 说明书11页 附图10页

(54)发明名称

提供机器到机器服务的方法和装置

(57)摘要

提供了用于提供服务的方法和装置。由机器到机器(M2M)设备提供服务的方法包括:向网络安全能力(NESC)发送对于第一验证的请求,所述对于第一验证的请求包括M2M设备的标识符;与NESC执行可扩展验证协议(EAP)验证;以及如果第一验证成功,则使用主会话密钥(MSK)和M2M设备的标识符中的至少一个生成秘密钥。



CN 103597774 B

1.一种用于机器到机器(M2M)设备的M2M服务自举的方法,该方法包括:

在M2M设备处从网络M2M节点接收第一消息,所述第一消息包括服务提供者(SP)标识符(ID)以及使用类型,M2M服务自举功能(MSBF)ID、网络安全能力(NESC)ID、以及目标设备ID中的至少一个;

在从网络M2M节点接收第一消息之后在M2M设备处从网络M2M节点接收第二消息;

识别第二消息是否包括网络分配的设备ID;以及

如果基于所述识别来自网络M2M节点的第二消息包括网络分配的设备ID,则由M2M设备基于SP ID和网络分配的设备ID生成M2M根密钥。

2.如权利要求1所述的方法,其中所述M2M根密钥的生成包括:

基于扩展的主会话密钥(EMSK)、预定字符串、SP ID以及网络分配的设备ID来生成M2M根密钥。

3.如权利要求1所述的方法,还包括:如果目标设备ID不匹配M2M设备自己的ID,则丢弃第一消息。

4.如权利要求1所述的方法,其中所述M2M根密钥和所述网络分配的设备ID中的至少一个被发送给M2M验证服务器(MAS),

其中所述M2M根密钥被用于M2M设备和相应于SP ID的服务提供者之间的相互验证,

其中所述M2M根密钥的生成包括:

如果所述网络分配的设备ID未由网络分配,则基于扩展的主会话密钥(EMSK)、预定字符串、SP ID以及M2M设备自己的ID来生成M2M根密钥。

5.一种用于机器到机器(M2M)服务自举的M2M设备的装置,该装置包括:

收发器,被配置为与网络M2M节点通信;以及

控制器,被配置为:

从网络M2M节点接收第一消息,所述第一消息包括服务提供者(SP)标识符(ID)、以及使用类型、M2M服务自举功能(MSBF)ID、网络安全 能力(NESC)ID、和目标设备ID中的至少一个;

在从网络M2M节点接收第一消息之后从网络M2M节点接收第二消息;

识别第二消息是否包括网络分配的设备ID;以及

如果基于所述识别来自网络M2M节点的第二消息包括网络分配的设备ID,则基于SP ID和网络分配的设备ID生成M2M根密钥。

6.如权利要求5所述的装置,其中所述控制器还被配置为基于扩展的主会话密钥(EMSK)、预定字符串、SP ID以及网络分配的设备ID来生成M2M根密钥。

7.如权利要求5所述的装置,其中,所述控制器还被配置为如果目标设备ID不匹配M2M设备自己的ID,则丢弃第一消息。

8.如权利要求5所述的装置,其中,所述M2M根密钥和所述网络分配的设备ID中的至少一个被发送给M2M验证服务器(MAS),

其中所述M2M根密钥被用于M2M设备和相应于SP ID的服务提供者之间的相互验证,以及

其中所述控制器还被配置为如果所述网络分配的设备ID未由网络分配,则基于扩展的主会话密钥(EMSK)、预定字符串、SP ID以及M2M设备自己的ID来生成M2M根密钥。

9.一种用于机器到机器(M2M)网络节点服务器的M2M服务自举的方法,该方法包括:

由M2M网络节点服务器向M2M设备发送第一消息,所述第一消息包括服务提供者(SP)标识符(ID)、以及使用类型、M2M服务自举功能(MSBF)ID、网络安全能力(NESC)ID和目标设备ID中的至少一个;

由M2M网络节点服务器识别M2M设备是否被分配了网络分配的设备ID;

在向M2M设备发送第一消息之后,由M2M网络节点服务器向M2M设备发送第二消息;以及

如果基于所述识别来自网络M2M节点的第二消息包括网络分配的设备ID,则由M2M网络节点服务器基于SP ID和网络分配的设备ID生成M2M根密钥。

10.如权利要求9所述的方法,其中所述M2M根密钥的生成包括:

基于扩展的主会话密钥(EMSK)、预定字符串、SP ID以及网络分配的 设备ID来生成M2M根密钥,

其中如果目标设备ID不匹配M2M设备自己的ID,则丢弃第一消息。

11.如权利要求9所述的方法,还包括将所述M2M根密钥和所述网络分配的设备ID中的至少一个发送给M2M验证服务器(MAS),

其中所述M2M根密钥被用于M2M设备和相应于SP ID的服务提供者之间的相互验证,

其中所述M2M根密钥的生成包括:

如果所述网络分配的设备ID未由网络分配,则基于扩展的主会话密钥(EMSK)、预定字符串、SP ID以及M2M设备自己的ID来生成M2M根密钥。

12.一种用于在机器到机器(M2M)服务自举的M2M网络节点服务器的装置,该装置包括:

收发器,被配置为与M2M设备和M2M验证服务器(MAS)中的至少一个通信;以及

控制器,被配置为:

向M2M设备发送第一消息,所述第一消息包括服务提供者(SP)标识符(ID)、以及使用类型、M2M服务自举功能(MSBF)ID、网络安全能力(NESC)ID和目标设备ID中的至少一个;

识别M2M设备是否被分配了网络分配的设备ID;

在向M2M设备发送第一消息之后,向M2M设备发送第二消息;以及

如果基于所述识别来自网络M2M节点的第二消息包括网络分配的设备ID,则基于SP ID和网络分配的设备ID生成M2M根密钥。

13.如权利要求12所述的装置,其中所述控制器还被配置为基于扩展的主会话密钥(EMSK)、预定字符串、SP ID以及网络分配的设备ID来生成M2M根密钥,以及

其中如果目标设备ID不匹配M2M设备自己的ID,则丢弃第一消息。

14.如权利要求12所述的装置,所述控制器还被配置为向MAS发送M2M根密钥和网络分配的设备ID中的至少一个,

其中所述M2M根密钥被用于M2M设备和相应于SP ID的服务提供者之间的相互验证,以及

其中所述控制器还被配置为如果所述网络分配的设备ID未由网络分配, 则基于扩展的主会话密钥(EMSK)、预定字符串、SP ID以及M2M设备自己的ID来生成M2M根密钥。

提供机器到机器服务的方法和装置

技术领域

[0001] 本发明涉及用于通信系统的方法和装置。更具体地，本发明涉及用于提供机器到机器(M2M)服务的方法和装置。

背景技术

[0002] M2M技术正在被研究，而且是正在被开发和定义的技术，该技术允许M2M设备加入M2M网络并与M2M网络通信以使得在M2M设备上运行的应用能够与在因特网中的各种控制节点(即，服务器其他类似设备)上运行的应用通信。为了便于这种通信，M2M核心网络被指定的角色是具有便于向设备动态提供服务参数以及注册M2M设备以使其能够进行应用层访问。

发明内容

[0003] 技术问题

[0004] M2M自动自举是在M2M设备和M2M网络之间运行的程序，以执行设备的动态预置(provisioning)。因此，需要一种系统和方法，用于执行设备的自诊断而没有当从计算机或用户界面手动选择自诊断项目时造成的不方便的。

[0005] 技术方案

[0006] 本发明的各方面解决上述问题和/或缺点并且至少提供下述优点。因此，本发明的一方面提供了一种由机器到机器(M2M)设备提供服务的方法，该方法包括：向网络安全能力(NESC)发送对于第一验证的请求，所述对于第一验证的请求包括M2M设备的标识符；与NESC执行可扩展验证协议(EAP)验证；以及如果第一验证成功，则使用主会话密钥(MSK)和M2M设备的标识符中的至少一个生成秘密钥(secret key)。

[0007] 根据本发明的一方面，提供了一种用于提供服务的机器到机器(M2M)设备。M2M设备包括：发送器，用于向网络安全能力(NESC)发送对于第一验证的请求，所述对于第一验证的请求包括M2M设备的标识符；控制器，用于与NESC执行可扩展验证协议(EAP)验证；以及密钥生成器，用于如果第一验证成功，则使用主会话密钥(MSK)和M2M设备的标识符中的至少一个生成秘密钥。

[0008] 根据本发明的另一方面，提供了一种在机器到机器(M2M)系统中由网络安全能力(NESC)提供服务的方法。该方法包括：确定是否从M2M设备接收到对于第一验证的请求，所述对于第一验证的请求包括M2M设备的标识符；如果接收到对于第一验证的请求，则与M2M设备执行可扩展验证协议(EAP)验证；以及如果第一验证成功，则使用主会话密钥(MSK)和M2M设备的标识符中的至少一个生成秘密钥。

[0009] 根据本发明的另一方面，提供了一种用于在机器到机器(M2M)系统中提供服务的网络安全能力(NESC)。该NESC包括：控制器，用于确定是否从M2M设备接收到对于第一验证的请求，所述对于第一验证的请求包括M2M设备的标识符，而且用于如果接收到对于第一验证的请求，则与M2M设备执行可扩展验证协议(EAP)验证；以及密钥生成器，用于如果第一验

证成功，则使用主会话密钥(MSK)和M2M设备的标识符中的至少一个生成秘密钥。

[0010] 技术效果

[0011] 根据本发明的一方面，存在多个益处：

[0012] 代码重用：EAP被广泛用于“网络访问验证”，诸如用于WiFi网络、WiMAX、紫蜂(ZigBee)、以太网。PANA被用于紫蜂设备中的“网络访问验证”。重用相同的组件的另一目的是，降低M2M设备的开发和生产的成本。

[0013] 可扩展性：EAP和PANA二者都是可扩展的协议。它们允许使用任何验证方法，不像TLS只允许使用PSK和基于证书的验证。以可以通过定义新的AVP(Attribute-Value-Pair，属性值对)容易地携带新的有效载荷的方式，PANA是可扩展的。

[0014] 轻便(Lightweight)：这个解决方案支持基于UDP的栈和基于TCP的栈二者。TLS需要基于TCP的协议栈，所以它需要更多的代码和处理。

[0015] 模型拟合：EAP和PANA的三方验证模型更适合于设备-核心-MSBF系统。TLS基于两方设计，而且基于TLS的解决方案无法自然融入M2M架构。

附图说明

[0016] 通过以下结合附图的描述，本发明特定示例性实施例的上述和其它方面、特征和优点将变得明显。

[0017] 图1描绘了根据本发明的实施例的M2M自动自举程序(M2M Automated Bootstrap Procedure)中涉及的网络元素；

[0018] 图2描绘了根据本发明的实施例的在M2M网络上发生的事件的高层流程图；

[0019] 图3描绘了涉及根据本发明的示例性实施例的自举程序的呼叫流；

[0020] 图4A描绘了根据本发明的示例性实施例的设备的自举程序的流程图；

[0021] 图4B描绘了根据本发明的示例性实施例的网络安全能力(NESC)的自举程序的流程图；

[0022] 图4C描绘了根据本发明的示例性实施例的网络远程实体管理能力(NREM)的自举程序的流程图；

[0023] 图4D描绘了根据本发明的示例性实施例的M2M服务自举功能(MSBF)的自举程序的流程图；

[0024] 图4E描绘了根据本发明的示例性实施例的M2M服务层AAA服务器(MAS)的自举程序的流程图；

[0025] 图5描绘了根据本发明的示例性实施例的设备功能模型；

[0026] 图6描绘了根据本发明的示例性实施例的分离的网络访问验证和M2M自举程序；

[0027] 图7描绘了根据本发明的示例性实施例的通过协议实施网络访问验证(Protocol for carrying Authentication for Network Access，PANA)使用可扩展验证协议(Extensible Authentication Protocol，EAP)的网络和使用EAP的任何网络二者的呼叫流；以及

[0028] 图8描绘了根据本发明的示例性实施例的设备功能模型。

[0029] 贯穿附图，应该注意，相同的参考标记用于描绘相同的或相似的元素、特征和结构。

具体实施方式

[0030] 提供下列参考附图的描述以有助于对通过权利要求及其等效物定义的本发明的示例性实施例的全面理解。本描述包括各种具体细节以有助于理解但是仅应当被认为是示例性的。因此，本领域普通技术人员将认识到，能够对 这里描述的实施例进行各种改变和修改而不脱离本发明的范围与精神。此外，为了清楚和简明起见，略去了对公知功能与结构的描述。

[0031] 在下面说明书和权利要求书中使用的术语和措词不局限于它们的词典意义，而是仅仅由发明人用于使得能够对于本发明清楚和一致的理解。因此，对本领域技术人员来说应当明显的是，提供以下对本发明的示例性实施例的描述仅用于图示的目的而非限制如所附权利要求及其等效物所定义的本发明的目的。

[0032] 应当理解，单数形式的“一”、“该”和“所述”包括复数指代，除非上下文清楚地指示不是如此。因此，例如，对“部件表面”的指代包括指代一个或多个这样的表面。

[0033] 图1描绘了根据本发明的实施例的M2M自动自举程序中涉及的网络元素。

[0034] 参照图1，连接网络元素的线对应网络元素当中使用的通信接口。设备110是自举以便开始使用由M2M核心网络120提供的M2M设施(facility)的实体。设备110经由M2M核心网络120利用M2M服务自举功能(M2M Service Bootstrapping Function)从事自举程序。在自举程序结束时，生成根秘密钥(KR)，其用于密码保护M2M网络上的应用通信。KR存储在网络上的M2M服务层AAA服务器(MAS)140中。

[0035] 欧洲电信标准协会(ETSI)M2M技术委员会(TC)正在设计M2M标准，而且已经确定要求自动的M2M自举程序并且已经确定对此的需要。

[0036] 图2描绘了根据本发明的实施例的在M2M网络上发生的事件的高层流。

[0037] 参照图2，包括网络访问验证的网络注册是由设备使用以获取对互联网协议(IP)网络的访问的程序。更高层程序，诸如M2M相关程序，可以在成功运行网络注册程序之后使用。M2M程序，诸如M2M服务自举和M2M服务连接，用于获取对M2M网络和IP网络之上的覆盖网络的访问。在图2中，M2M设备包含设备服务能力层(DSCL)，M2M网关包含网关服务能力层(GSCL)，并且网络域包含网络服务能力层(NSCL)。NSCL指的是网络域中的M2M服务能力。GSCL指的是M2M网关中的M2M服务能力。DSCL指的是M2M设备中的M2M服务能力。DSCL具有标识DSCL的DSCL标识符(ID)，而且GSCL具有标识GSCL的GSCL标识符(ID)。

[0038] ETSI M2M架构支持设备和网关式装置二者到核心网络的连接。为简单 起见，贯穿本文档仅使用术语“设备”来指代电子设备和网关式装置，并因此，相对于M2M设备列举的特征、元素和操作也适用于M2M网关和网关式装置。此处可以使用词“设备”来指代DSCL和/或GSCL。

[0039] 本示例性实施例提供了使用协议实施网络访问验证(PANA)和可扩展验证协议(EAP)的自动的M2M服务层自举程序。在这种方法中，网络注册和M2M服务自举是两个独立程序，如图2中所描绘的。PANA是用于在设备和核心网络之间携带EAP数据的协议。然而，本发明不限于此，而且其他合适的协议可以替代PANA，只要替代协议可以携带EAP和所需的有效载荷，而且此处相对于示例性实施例所介绍的操作遵循该替代协议。

[0040] 在本发明的示例性实施例，以基于身份的验证密钥交换(Identity-Based

Authenticated Key Exchange,IBAKE)为基础的EAP验证被用作运行的EAP验证方法。然而，本发明的各方面的不特定于使用的EAP验证方法。换句话说，本发明不限于EAP-IBAKE和任何EAP验证方法，可以使用诸如EAP-TLS、EAP-AKA、EAP-TTLS、EAP-GPSK、或其它类似的协议。

[0041] 传输层安全性(TLS)已经被提出以用于设备和网络的相互验证，并且用于将自举参数作为有效载荷传送到超文本传输协议(HTTPS)层。然而，TLS的使用引入了若干个问题，对于这些问题，EAP和PANA通过若干个关键特征提供了解决方案，包括代码重用、可扩展性、轻便(lightweight)以及提供改进的模型拟合(model fit)。例如，相对于代码重用，EAP被广泛用于“网络访问验证”，诸如用于无线保真(WiFi)网络、无线互通微波存取(WiMAX)网络、紫蜂(ZigBee)网络和以太网网络。PANA被用于紫蜂设备中的“网络访问验证”。因此，重用相似或相同的组件的另一目的是，降低M2M设备的开发和生产的成本。相对于可扩展性，EAP和PANA二者是可扩展的协议，并且允许使用任何验证方法，不像TLS只允许使用预共享密钥(Pre-Shared Key,PSK)和基于证书的验证。PANA是可扩展的，以使得可以容易地通过定义新的属性值对(Attribute-Value-Pair,AVP)携带新的有效载荷。相对于轻便，EAP和PANA的使用支持基于用户数据报协议(UDP)的栈和基于传输控制协议(TCP)的栈二者。另一方面，TLS需要基于TCP的栈，并因此与使用EAP和PANA相比，它需要增加的代码和处理。相对于更好的模型拟合，EAP和PANA的三方验证模型对应M2M设备-核心-M2M服务自举功能(MSBF)系统架构。相比之下，TLS基于两方设计，而且基于TLS 的解决方案无法自然融入M2M系统架构。

[0042] 图3描绘了涉及根据本发明的示例性实施例的自举程序的呼叫流。

[0043] 参照图3，网络安全能力(NESC)302和网络远程实体管理能力(NREM)304驻留在M2M核心网络中。NESC302是验证器，而且NREM304是设备300的配置服务器。虽然在本发明的所有实施例中没有要求，但是在步骤310中，由M2M服务自举功能(MSBF)306发送M2M邀请。在由设备300发起自举程序的情况下，可以跳过步骤310，因为步骤310允许网络发起自举程序。因此，步骤310可以由NESC302或MSBF306发起。在由NESC302发起步骤310的情况下，在MSBF306和NESC302之间不存在相应的消息。然而，因为MSBF306或NESC302应该知道设备300的网络位置，所以在这样的情况下，步骤310中所涉及的消息在因特网协议(IP)层和/或链路层单播。可替换地，在MSBF306或NESC302不知道设备300的确切位置的情况下，那么消息在IP层和/或链路层任播、多播或广播。

[0044] 在NESC302和MSBF306之间使用验证、授权和计费(AAA)协议。AAA协议的两个例子是远程验证拨入用户服务(RADIUS)和基于Diameter的协议(Diameter)。根据本示例性实施例，在NESC302和设备300之间使用的AAA协议是PANA。在步骤310中使用的PANA消息是PANA验证请求(PAR)消息，并且，除了PANA标准中定义的标准AVP，PANA消息可以包括PAR消息中的以下AVP：MSBF标识符(ID)，用于将MSBF306的标识符传送到设备300；AVP的值字段，其包括数据元素，诸如指示标识符的类型的ID-Type(ID类型)、标识符的ID-value(ID值)和NESC-ID，其中ID-Type诸如完全合格的域名(FQDN)、网络访问标识符(NAI)、统一资源标识符、以及其他类似的标识符，而且NESC-ID用于将NESC标识符传送到设备300。此外，AVP的值字段包括以下数据元素：指示标识符的类型的ID-Type，诸如FQDN、NAI和URI；以及ID-value，它是标识符的值。

[0045] 由于NESC302相对于PANA协议用作PANA验证代理(PAA)，因此NESC-ID和PAA标识符

彼此相等。此外，Network-ID(网络ID)用于将由MSBF306服务的(多个)M2M网络的标识符传送到设备300。零个、一个或多个这样的AVP可以被包括在同一消息中，而且单一MSBF306可以为多个网络服务。此外，除了其他数据元素，AVP的值字段还可以包括如上所述的ID-Tpye和ID-value。

[0046] 此外，如上所述，也可以由传统的PAA，即，不在M2M网络中的PAA使用相同的AVP，以便通知PPA为其服务的各个网络。因此，Network-ID可以用于代表服务提供者和服务提供者所拥有的网络二者。此外，Device-ID(设备ID)也可以用于将目标设备的标识符传送到接收设备。由于包括AVP的消息可以被选播、多播或广播，并因此除了被目标设备接收之外还被多个节点接收，Device-ID使接收设备或节点能够确定请求是否打算供各接收设备或者其他一些设备使用。只有当Device-ID中的一个或多个匹配设备300的标识符时设备300才消费传入消息，否则设备300将丢弃该消息。除了其他数据元素，AVP的值字段还包括以下数据元素：指示标识符的类型的ID-Type，诸如FQDN、NAI、URI和MAC地址；以及ID-value，它是标识符的值。上面所讨论的AVP将ID类型和ID值一起呈现。在使用AVP的网络的架构不需要支持多种不同类型的ID的灵活性的情况下，可以使用这些AVP的变体，其中ID类型被省略。

[0047] 此外，定义用于指示PANA运行的目的的Usage-Type(用途类型)AVP，即，PANA运行用于M2M自举、用于网络访问(即，PANA运行是PANA的传统使用)、还是用于其他类型的PANA运行。Usage-Type AVP可以被包括在首次、任何或所有的PANA消息交换中。Usage-Type AVP在值字段中包括以下数据元素：Tpye(类型)，它携带指示用途类型的枚举值，例如，0用于网络访问，1用于M2M自举，2用于M2M服务注册，或用于其他类型的用途的其他值。

[0048] 接着，在步骤320中，运行阶段1相互验证，以便设备300和网络彼此相互验证。根据本发明的示例性实施例，阶段1的相互验证可以只是验证的一个阶段(例如，利用EAP-TLS)，或者可以是两个或更多个阶段。例如，EAP-IBAKE有两个阶段：使用临时ID和密码的第一阶段，随后是使用基于身份的加密(IBE)的第二阶段(见步骤340)。在使用两个阶段的情况下，每个阶段运行完整验证方法。例如，利用IBAKE方法，第一阶段运行一种方法，诸如EAP-广义PSK(GPSK)，而且第二阶段运行另一种EAP方法，诸如EAP-IBAKE。在使用一个阶段的情况下，根据步骤340运行该阶段。换句话说，如果使用一个阶段则跳过步骤320。

[0049] 在步骤320中运行完整EAP验证方法。EAP验证方法经由EAP通过PANA在设备300和NESC302之间通信，并且经由EAP通过AAA协议在NESC302和M2M服务层AAA服务器(MAS)308之间通信。因此，在这个阶段建立完整PANA会话。然而，如果验证失败，则步骤320中断。如果在步骤320中的验证成功，则将采取动作以使能步骤330。因此，步骤320完成设备300和网络之间的相互验证，并且还使能发现、识别和安全性以便为步骤330做准备。

[0050] 为了使能步骤330，携带验证结果的最后的PANA消息携带附加的AVP。附加的AVP包括DM-server-ID(DM服务器ID)，其用于将设备管理服务器的标识符传送到设备300，其中，零个、一个或多个这样的AVP可以被包括在同一消息中。DM-server-ID AVP的值字段可以包括以下两个数据元素：指示标识符的类型的ID-Type，诸如FQDN、IPv4地址、URI或其他类似的标识符；以及ID-value，它是标识符的值。

[0051] 另一附加的AVP是Assigned-Device-ID(分配的设备ID)，其用于传送由网络分配给设备300的设备标识符，而且将是用于随后在设备300和M2M核心网络之间发送信令的设备300的标识符，其中，零个、一个或多个这样的AVP可以被包括在同一消息中。Assigned-

Device-ID AVP的值字段可以包括以下数据元素:指示标识符的类型的ID-Type,诸如FQDN、NAI、URI、和MAC地址;以及ID-value,它是标识符的值(例如,“light-switch-1001”(“灯-开关-1001”))。

[0052] DM-server-ID AVP和Assigned-Device-ID AVP将ID类型和ID值一起给出。在网络架构不需要支持多种不同类型的ID的情况下(即,只使用一种类型),可以使用这些AVP的变体,其中ID类型被省略。

[0053] 此外,在步骤320的这个阶段,还建立设备300和设备管理服务器之间的加密安全关联。当Assigned-Device-ID和DM-server-ID作为终端点标识符时,根据以下共享秘密钥(shared secret key,KD-DM)公式基于主会话密钥(Master Session Key,MSK)来计算设备300和设备管理服务器之间的共享秘密钥:

[0054] KD-DM=Hash(MSK,constant_string|DM-server-ID|Assigned-Device-ID|other_parameters)

[0055] 其中,Hash(哈希)是单向密钥哈希函数,诸如基于哈希的消息验证码(HMAC)安全哈希算法1(SHA1)、HMAC-SHA256,或其他类似的哈希函数;MSK是由运行的EAP方法导出的主会话密钥;constant_string是常量字符串值,诸如“M2M shared secret between Device and Device Management Server”(“设备和设备管理服务器之间的M2M共享秘密钥”),而且字符串可以包含一个或多个NULL字符(“\0”);DM-server-ID是设备管理服务器标识符的值;Assigned-Device-ID是由网络分配的设备标识符的值,其中,如果网络没有分配ID,则设备可以使用其自己的标识符作为分配的ID;而且other_parameters是可以被添加到此公式的变量的零个或多个参数。

[0056] 根据本发明的另一示例性实施例,使用扩展的MSK(EMSK)代替MSK的共享秘密钥公式如下:

[0057] KD-DM=Hash(EMSK,constant_string|DM-server-ID|Assigned-Device-ID|other_parameters)。

[0058] PANA会话标识符和PANA密钥ID的组合作为密钥索引用于给定的设备。如果给定的设备只有一个PANA会话,则单独使用密钥ID足以索引KD-DM密钥。

[0059] 根据本发明的另一示例性实施例,共享秘密钥公式可以使用根秘密钥(root secret key,KR)。然而,这个共享秘密钥公式应用于在运行设备配置之前生成KR的情况。这个共享秘密钥公式为:KD-DM=Hash(KR,constant_string|DM-server-ID|Assigned-Device-ID|other_parameters)。

[0060] 接着,在步骤330中,运行设备预置(例如,使用开放移动联盟(OMA)设备管理(DM))。然而,步骤330是可选的,并且,可以根据运行步骤320的本发明的示例性实施例的配置来运行步骤330。当运行步骤330时,它可以使用在较早的PANA程序期间生成的标识符(诸如Assigned-Device-ID和DM-server-ID)和共享密钥(KD-DM)来保护。在步骤330,可以如在步骤320中所描述的计算保护这样的程序所需的标识符和加密密钥。

[0061] 接下来,在步骤340,阶段2的相互验证被运行,而且涉及通过PANA运行EAP验证方法。一些验证方法可以使用步骤340,而且其它验证方法也可以省略步骤340。例如,使用EAP-TLS只运行验证的一个阶段,而基于IBAKE的验证使用两个阶段,而且第二阶段涉及运行EAP-IBAKE。

[0062] 自举程序的一个结果是建立KR作为设备300和网络之间的共享秘密钥。在步骤320或步骤340结束时取决于步骤的可用性和使用这个方案的网络架构的配置生成KR。如果在步骤320期间没有传送Assigned-Device-ID，则它可以在步骤340结束时传送，而且由携带验证结果的最后的PANA消息携带。

[0063] 可以通过使用以下替代技术之一生成KR。例如，在成功的验证程序结束时可以从由EAP方法产生的MSK来推导KR。在这种情况下，KR由存在于设备300上的EAP对等体和存在于MAS308或MSBF306上的验证服务器产生。验证服务器与验证器，即，NESC302，共享MSK。因此，MSK在成功的验证结束时构成动态生成的共享秘密钥，而且它被用作种子以用于根据以下公式的KR推导：

[0064] KR=Hash(MSK,constant_string|Assigned-Device-ID|Network-ID|other_parameters)，

[0065] 其中，Hash是单向密钥哈希函数，诸如HMAC-SHA1、HMAC-SHA256；MSK是由运行的EAP方法导出的主会话密钥；constant_string是常量字符串值，诸如“M2M shared secret root key between Device and network”(“设备和网络之间的M2M共享根密钥”)，而且可以包含一个或多个NULL字符(“\0”)；Assigned-Device-ID是由网络分配的设备标识符的值，其中，如果网络没有分配ID，则设备可以使用其自己的标识符作为分配的ID；Network-ID是网络标识符的值；而且other_parameters是可以被添加到此公式的变量的零个或多个参数。

[0066] PANA会话标识符和PANA密钥ID的组合作为密钥索引用于给定的设备。如果给定的设备只有一个PANA会话，则单独使用密钥ID足以索引KR密钥。

[0067] 可替换地，在成功的验证程序结束时可以从由EAP方法产生的EMSK来推导KR。在这种情况下，KR由存在于设备上的EAP对等体和存在于MAS308或MSBF306上的验证服务器产生。因此，EMSK在成功的验证结束时构成动态生成的共享秘密钥，而且被用作种子以用于根据以下公式的KR推导：KR=Hash(EMSK,constant_string|Assigned-Device-ID|Network-ID|other_parameters)。

[0068] PANA会话标识符和PANA密钥ID的组合作为密钥索引用于给定的设备。如果给定的设备只有一个PANA会话，则单独使用密钥ID足以索引KR密钥。可替换地，以下新定义的公式可以用于计算密钥索引：Key-index=Hash(KR,constant_string|other_parameters)。

[0069] 接下来，在步骤350中，运行到MAS的设备信息预置，以使得M2M核心网络向MAS308发送设备预置信息(例如，KR、设备ID等)。如果成功 运行阶段2的相互验证，则只运行此步骤。

[0070] 注意的是，根据本发明的另一示例性实施例，NESC302可以从上述示例性实施例中移除。在这种情况下，MSBF306和/或MAS308与设备30直接彼此交互，而无需经由NESC302发送消息。在这种情况下，PANA协议可以用于MSBF306和/或MAS308与设备300通信(即，运行在MSBF306和/或MAS308与NESC302之间的协议也可以被移除)。

[0071] 参照图3，设备300、NESC302、NREM304、MSBF306和MAS308中的每一个可以分别包括用于控制和执行各个设备的操作的控制器、用于从各个设备发送信号的发送器、用于在各个设备处接收信号的接收器、用于在各个设备处发送和接收信号的收发器、以及用于生成密钥的密钥生成器。

[0072] 图4A描绘了根据本发明的示例性实施例的设备的自举程序的流程图。

[0073] 参照图4A，在步骤401中，设备确定自举程序是否是由设备发起的。如果自举程序是由设备发起的，则过程移动到步骤404。否则，过程移动到步骤402。在步骤402中，设备确定自举邀请是否被MSBF或NESC发送。如果自举邀请未被发送，则设备等待直到自举邀请被发送。否则，过程移动到步骤403。在步骤403中，设备发起自举程序并且过程移动到步骤404。

[0074] 在步骤404中，设备确定阶段1相互验证是否被确认。如果验证未被确认，则过程移动到步骤408。否则，过程移动到步骤405。在步骤405中，设备运行阶段1的相互验证，并且过程移动到步骤406。在步骤406中，设备确定阶段1的相互验证是否成功。如果阶段1的相互验证没有成功，则过程终止。否则，过程移动到步骤407。在步骤407中，设备运行设备预置，而且过程移动到步骤408。在步骤408中，设备运行阶段2的相互验证。

[0075] 图4B描绘了根据本发明的示例性实施例的NESC的自举程序的流程图。

[0076] 参照图4B，在步骤411中，NESC确定自举程序是否由NESC发起。如果自举程序由NESC发起，则过程移动到步骤412，否则过程移动到步骤413。在步骤413中，NESC确定是否从MSBF接收到邀请。如果从MSBF接收到邀请，则过程移动到步骤412，否则过程移动到步骤414。在步骤414中，NESC确定是否从设备接收到引导消息。如果从设备接收到引导消息，则过程移动到步骤415，否则过程移动到步骤413。在步骤412中，NESC发送自举邀请到设备。自举邀请可以作为PANA验证请求(PAR)发送，而且过程移动到步骤415。

[0077] 在步骤415中，NESC确定阶段1的相互验证是否被确认。如果阶段1的相互验证未被确认，则过程移动到步骤418，否则过程移动到步骤416。在步骤416中，NESC运行阶段1的相互验证。在步骤417中，NESC确定阶段1的相互验证是否成功。如果阶段1的相互验证没有成功，则过程终止，否则，过程移动到步骤418。在步骤418中，NESC运行阶段2的相互验证。

[0078] 图4C描绘了根据本发明的示例性实施例的NREM的自举程序的流程图。

[0079] 参照图4C，在步骤421中，NREM运行设备预置。

[0080] 图4D描绘了根据本发明的示例性实施例的MSBF的自举程序的流程图。

[0081] 参照图4D，在步骤431中，MSBF确定自举程序是否是由MSBF发起的。如果自举程序由MSBF发起，则过程移动到步骤432，否则过程移动到步骤433。在步骤432中，MSBF发送自举邀请到设备，而且过程移动到步骤433。在步骤433中，MSBF运行阶段2的相互验证，而且过程移动到步骤434。在步骤434中，MSBF确定阶段2的相互验证是否成功。如果阶段2的相互验证成功，则过程移动到步骤435，否则过程终止。在步骤435中，MSBF运行MAS预置。

[0082] 图4E描绘了根据本发明的示例性实施例的MAS的自举程序的流程图。

[0083] 参照图4E，在步骤441中，MAS确定阶段1的相互验证是否被确认。如果阶段1的相互验证未被确认，则过程移动到步骤443，否则过程移动到步骤442。在步骤442中，MAS运行阶段1的相互验证，而且过程移动到步骤443。在步骤443中，MAS运行MAS预置。

[0084] 本发明的示例性实施例可以被应用于需要M2M设备的自动自举的M2M系统。在设备能够预先预置(例如，在制造期间预置)的网络中，这样的解决方案不是必需的。然而，由于M2M部署的动态和大规模的性质，依靠预先预置是不切实际的。

[0085] 根据另一示例性实施例，提供了使用基于EAP的网络访问验证程序的M2M服务层自举。上面已经相对于图4A至图4E的示例性实施例描述了只运行自举的自举程序。本示例性

实施例是利用网络访问验证以对于M2M服务层自举设备的优化程序。设备执行网络访问验证，以便在开始使用任何更高层服务(诸如M2M服务)之前连接到给定的网络。为了执行这样的验证，本示例性实施例中描述了很好地利用已运行的验证的关联程序。

[0086] 图5描绘了根据本发明的示例性实施例的设备功能模型。

[0087] 参照图5，设备500包括网络注册管理器510和M2M自举管理器520。网络注册管理器510为了网络访问服务将设备500注册到网络(即，获得对IP网络的访问)。M2M自举管理器520管理设备500的自举的状态。

[0088] 网络注册管理器510包括以下讨论的元素。设备配置管理器512管理用于IP网络访问的诸如设备ID和网络ID的配置参数。设备配置管理器512与网络发现和选择管理器接口连接以导出预先配置的网络ID和导入动态学习的网络ID。设备配置管理器512还与EAP对等体接口连接以导出在EAP验证期间使用的网络用户凭据。网络发现和选择管理器514针对IP网络运行网络发现和选择程序，并且与EAP对等体516接口连接以导出所选择的网络ID。EAP对等体516与EAP更低层接口连接以实施EAP验证方法。EAP更低层518执行EAP对等体516的更低层服务。

[0089] M2M自举管理器520包括以下讨论的元素。设备配置管理器522管理用于M2M网络访问的诸如设备ID和网络ID的配置参数。设备配置管理器522与网络发现和选择管理器接口连接以导出预配置的网络ID并且导入动态学习的网络ID，并且与EAP对等体526接口连接以导出在EAP验证期间使用的M2M用户凭据。网络发现和选择管理器524针对M2M网络运行网络发现和选择程序，并且与EAP对等体526接口连接以导出所选择的网络ID。EAP对等体526与EAP更低层接口连接以实施EAP验证方法。EAP更低层528与EAP对等体526接口连接。

[0090] 存在针对M2M自举定义的程序，其涉及运行设备和MSBF之间的协议以用于彼此相互验证，以及生成所需的M2M根密钥。在大多数M2M网络中，设备在获取访问网络之前要进行验证。代替运行自举程序的单独验证，本示例性实施例可以利用网络访问验证，以减少由自举程序所施加的执行、延迟和处理负荷。

[0091] 图6描绘了根据本发明的示例性实施例的单独的网络访问验证和M2M自举程序。

[0092] 网络访问服务器(NAS)602实现EAP验证器和AAA客户端功能。在图6中还示出了MAS604和设备601，而且AAA605实现验证、授权和计费服务器以及EAP验证服务器功能。NESC603执行安全功能，而且MSBF606提供M2M服务自举功能。

[0093] 在图6的示例性实施例中，M2M自举程序变成网络访问验证程序的一部 分。利用网络访问验证程序生成KR。代替验证设备601两次(一次用于网络访问，一次用于M2M自举)，设备601针对网络访问验证一次，并且得到的密钥被用于生成KR。在步骤610中，在设备601与NAS602之间执行网络访问验证。在步骤615中，在NAS602和AAA605之间执行网络访问验证。在步骤620中，在设备601和NESC603之间执行M2M自举程序。在步骤625中，在NESC603和MSBF606之间执行M2M自举程序。在步骤630中，在MAS604和MSBF606之间执行M2M自举程序。

[0094] 图6的示例性实施例适用于使用基于EAP的网络访问验证的网络。与此相反，图4A至图4E的示例性实施例更适用于通过PANA使用EAP的网络。

[0095] 图7描绘了根据本发明的示例性实施例的通过PANA使用EAP的网络和使用EAP的任何网络二者的呼叫流。

[0096] 参照图7，AAA被并入MSBF以便形成(have)AAA/MSBF704。当访问网络通过PANA使用

EAP进行网络访问验证时，利用这种方法。在步骤710和715中，设备701经由NAS702与AAA/MSBF704执行基于EAP的网络访问验证。在步骤710中，EAP在设备701和NAS702之间通过PANA携带，而且在步骤715中，EAP在NAS702和AAA/MSBF704之间通过RADIUS、Diameter或等效协议携带。

[0097] 除了用于常规的网络访问验证的常规PANA呼叫流和有效载荷，附加的有效载荷被交换以便执行M2M自举。PANA消息中的一个或多个应该包含Usage-Type AVP，其中Type(类型)值被设置为指示M2M自举的值。此外，指示验证结果的最后的PANA消息可以包括零个或多个Assigned-Device-ID，以携带由网络分配的设备标识符。此外，PANA消息中的一个或多个应该包含Network-ID AVP。附加的有效载荷和AVP在上面已经描述，而且为简洁起见将避免进一步的描述。

[0098] 在步骤710和715中成功的EAP验证结束时，生成EMSK。这个密钥被设备701和AAA/MSBF704知道。此外，KR可以从EMSK推导，如参照图3的示例性实施例所描述的。

[0099] PANA会话标识符和PANA密钥ID的组合作为密钥索引用于给定的设备。如果给定的设备只有一个PANA会话，则单独使用密钥ID足以索引KR密钥。可替换地，可以以参考图3的示例性实施例所讨论的方式计算密钥索引。因此，KR可以由网络随机生成，并且使用专用PANA AVP安全地传送 到设备701。KR在发送到设备701之前被加密，而且设备701在接收到KR之后解密KR。对于这样的加密/解密程序，定义了另一密钥，其可以在设备和网络侧二者上推导。KR由验证服务器加密并且由设备解密。这个加密/解密程序使用的密钥基于EMSK，并根据下面的公式计算：AS_ENCR_KEY=Hash(EMSK,constant_string|other_parameters)。

[0100] PANA会话标识符和PANA密钥ID的组合作为密钥索引用于给定的设备。如果给定的设备只有一个PANA会话，则单独使用密钥ID足以索引KR密钥。可替换地，以下新定义的公式可以用于计算密钥索引：Key-index=Hash(AS_ENCR_KEY,constant_string|other_parameters)。

[0101] 加密形式的KR被使用AAA协议从AAA/MSBF704发送到NAS702，而且被使用携带验证结果的最后的PANA消息中的PANA AVP从NAS702中继到设备701。M2M-KR AVP可以被包括在上述PANA消息中，其中M2M-KR被用于将KR传送到设备701。M2M-KR AVP的值字段包括以下数据元素：Key-ID，其携带KR的标识符(索引)，其中标识符的值由网络分配；以及KR-Encr，其是KR的加密值。用于加密的密钥是AS_ENCR_KEY。

[0102] 接着，在步骤720中，运行从AAA704到MAS703的设备信息预置。步骤720涉及AAA704与MAS703共享设备预置信息(例如，KR、设备ID等)。

[0103] 图7的示例性实施例可以应用于PANA或类似的可扩展的EAP传输都无法用于携带EAP的部署。在这种情况下，专用有效载荷，诸如Network-ID和Assigned-Device-ID，无法传达到设备。因此，假设这些参数以与本示例性实施例不相关的方式确定。然而，设备可能已经被配置有设备ID，而且设备在由链路层呈现的网络发现设备的帮助下发现网络ID。下面的公式用于从EMSK推导KR：KR=Hash(EMSK,constant_string|Assigned-Device-ID|Network-ID|other_parameters)。

[0104] 根据以下新定义的公式计算KR的密钥索引：Key-index=Hash(KR,constant_string|other_parameters)。

[0105] 图8描绘了根据本发明的示例性实施例的设备功能模型。

[0106] 参照图8，设备800包括网络注册管理器810和M2M自举管理器820。网络注册管理器810为了网络访问服务将设备800注册到网络(即，获取对IP网络的访问)。M2M自举管理器820管理设备的自举的状态。

[0107] 网络注册管理器810包括以下讨论的元素。设备配置管理器811管理用于IP网络访问的诸如设备ID和网络ID的配置参数。设备配置管理器811与网络发现和选择管理器812接口连接以导出预先配置的网络ID和导入动态学习的网络ID，而且与EAP对等体811连接以导出在EAP验证期间使用的网络用户凭据。此外，设备配置管理器811与EAP更低层814接口连接以导入动态学习的设备ID，并且与M2M自举管理器820接口连接以导出预配置的设备ID。

[0108] 网络发现和选择管理器812针对IP网络运行网络发现和选择程序，并且与EAP对等体813接口连接以便导出所选择的网络ID。网络发现和选择管理器812还与M2M自举器815接口连接，以便导出所选择的网络ID。EAP对等体813与EAP更低层814接口连接以实施EAP验证方法，并且与M2M自举器815接口连接以便导出EMSK。

[0109] EAP更低层814与M2M自举器815接口连接以便导出动态学习的网络ID和分配的设备ID。M2M自举器815从网络注册管理器810之内的其他实体接收输入的参数，并根据示例性实施例的公式产生KR和密钥索引。M2M自举器815与M2M自举管理器820，即，M2M自举管理器820中的设备配置管理器连接，以导出这些信息元素。

[0110] 这些M2M自举管理器820包括用于管理诸如设备ID、网络ID和KR的、用于M2M网络访问的配置参数的设备配置管理器，并且从存在于网络注册管理器810中的M2M自举器815导出这些参数。

[0111] 本示例性实施例可以被应用于运行M2M设备的自举的M2M系统。在设备可以被预先预置(例如，在制造期间)的网络中，这样的解决方案可以被跳过。在具有动态和大规模M2M部署的网络中，由于M2M部署的大规模，依靠预先预置成为问题。因此，示例性实施例适用于使用基于EAP的网络访问验证的网络。根据本示例性实施例，访问网络提供者和M2M网络提供者是相同实体或者具有业务关系，以使得它们能够共享如图3的示例性实施例的步骤320中所要求的密钥材料(keying material)。

[0112] 虽然已经参照本发明的某些示例性实施例示出和描述了本发明，但是本领域术人员应当清楚地理解，可以在形式和细节上对其做出各种改变而不脱离由所附权利要求及其等同物定义的本发明的精神和范围。

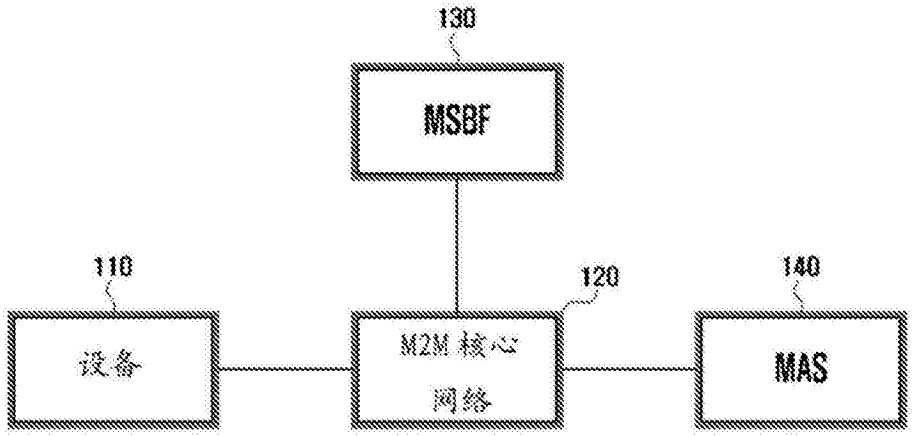

130
MSBF
110
设备
120
M2M 核心
网络
140
MAS

图1

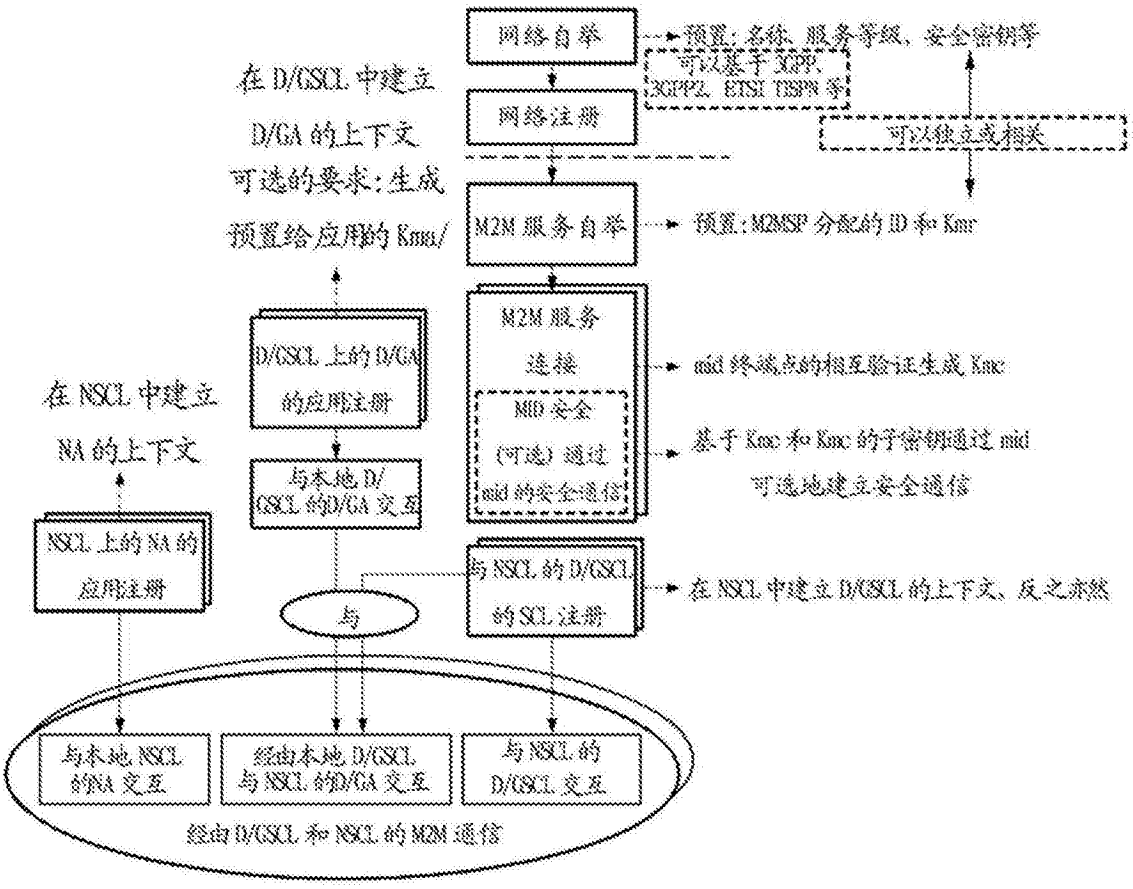

网络自举
预置：名称、服务等级、安全密钥等
可以基于 3GPP2、ETSI TISPN 等
网络注册
可以独立或相关
在 D/GSCL 中建立
D/GA 的上下文
可选的要求：生成
预置给应用的 Kmc/
M2M 服务自举
预置：M2MSP 分配的 ID 和 Kmr
M2M 服务
连接
mid 终端点的相互验证生成 Kmc
MID 安全
(可选) 通过
mid 的安全通信
基于 Kmc 和 Kmc 的子密钥通过 mid
可选地建立安全通信
D/GSCL 上的 D/GA
的应用注册
与本地 D/
GSCL 的D/GA 交互
在 NSCL 中建立
NA 的上下文
NSCL 上的 NA 的
应用注册
与 NSCL 的 D/GSCL
的 SCL 注册
在 NSCL 中建立 D/GSCL 的上下文、反之亦然
与
与本地 NSCL
的NA 交互
经由本地 D/GSCL
与 NSCL 的D/GA 交互
与 NSCL 的
D/GSCL 交互
经由 D/GSCL 和 NSCL 的 M2M 通信

图2

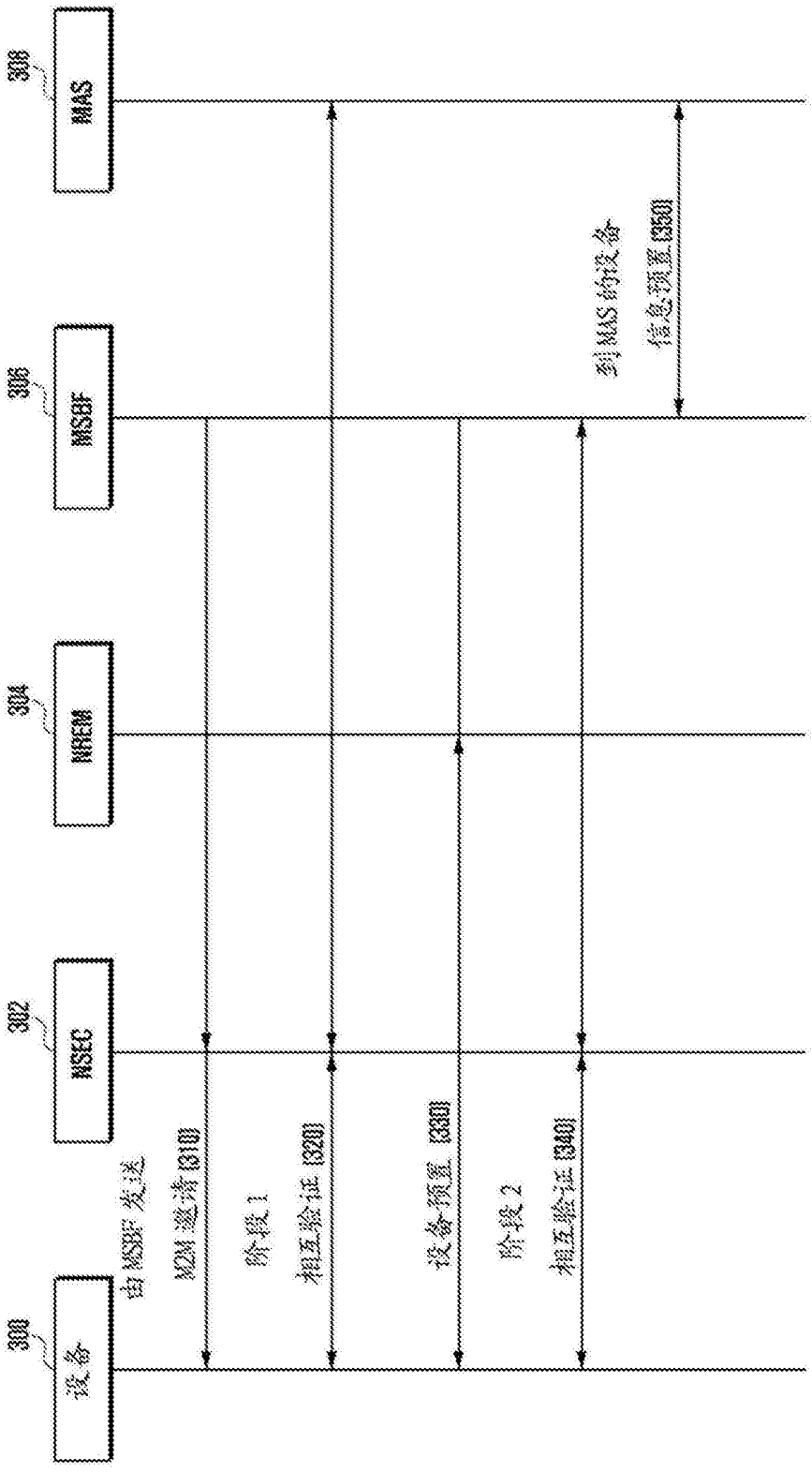

308
MAS
306
MSBF
304
MRCM
302
MSEC
300
设备
由MSBF发送
M2M邀请(310)
阶段1
相互验证(320)
设备预置(330)
阶段2
相互验证(340)
到MAS的设备
信息预置(350)

图3

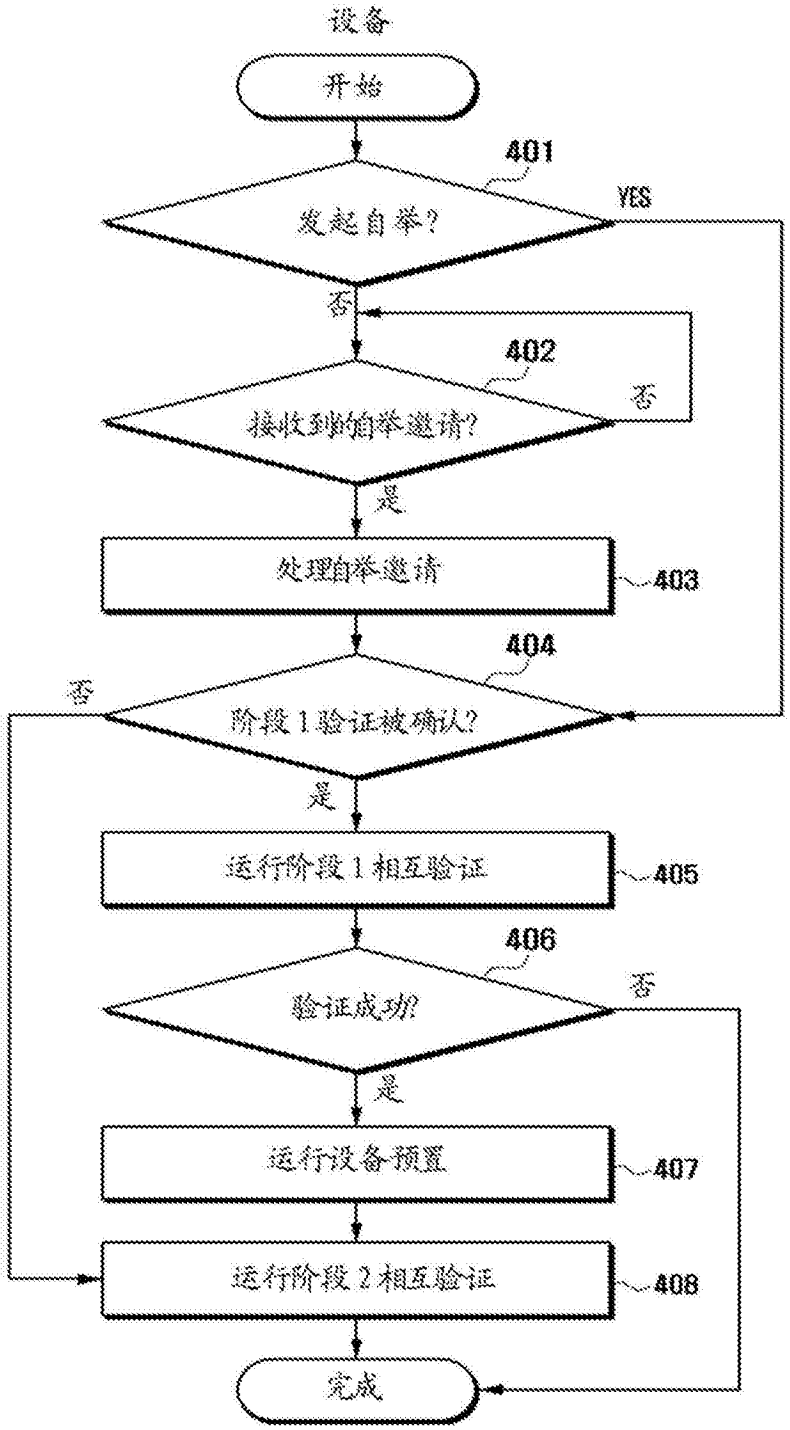

设备
开始
401
发起自举?
YES
否
402
接收到自举邀请?
否
是
处理自举邀请
403
404
阶段1验证被确认?
否
是
运行阶段1相互验证
405
406
验证成功?
否
是
运行设备预置
407
运行阶段2相互验证
408
完成

图4a

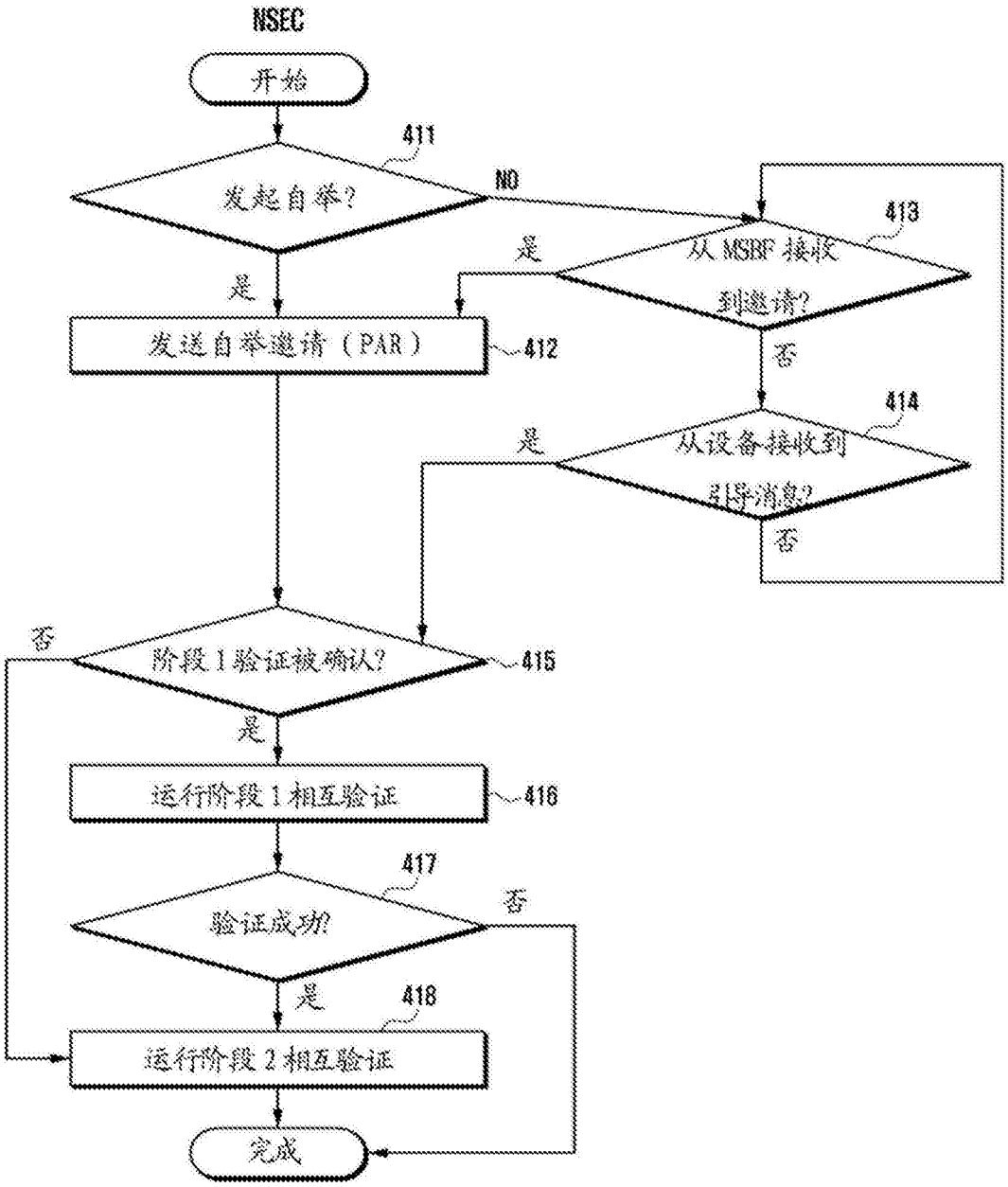

NSEC
开始
411
发起自举?
NO
是
413
从 MSBF 接收到邀请?
是
否
发送自举邀请（PAR）
412
414
从设备接收到引导消息?
是
否
否
阶段 1 验证被确认?
415
是
运行阶段 1 相互验证
416
417
验证成功?
否
是
418
运行阶段 2 相互验证
完成

图4b

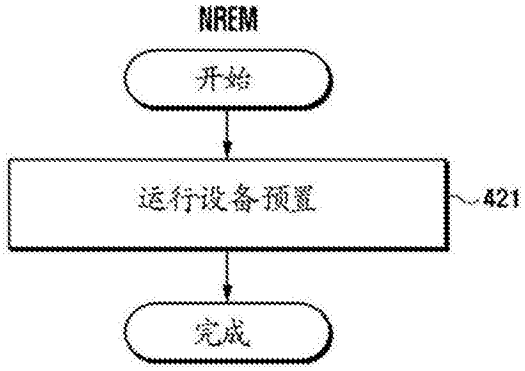

NREM
开始
运行设备预置
421
完成

图4c

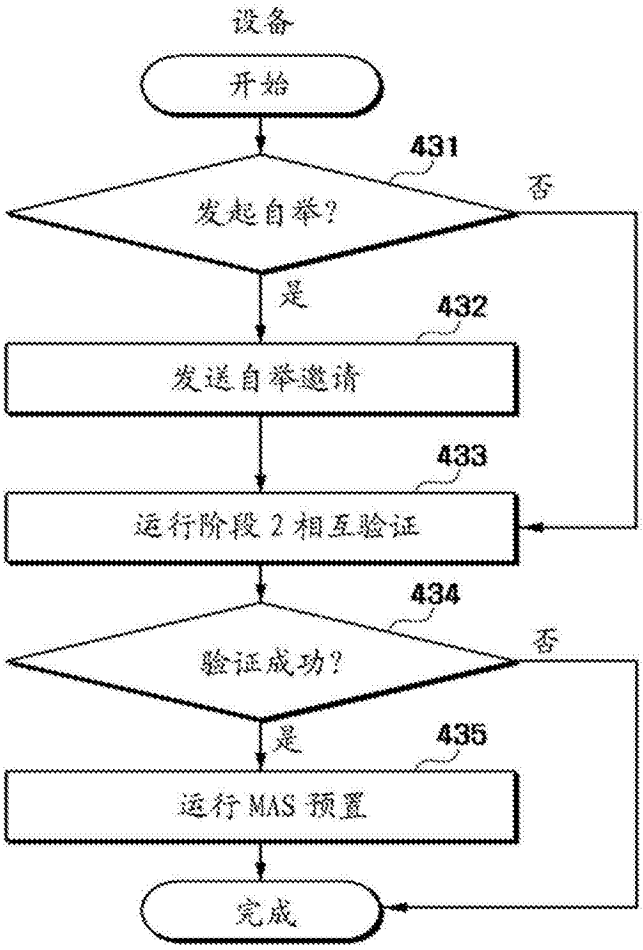

设备
开始
431
发起自举?
否
是
432
发送自举邀请
433
运行阶段 2 相互验证
434
验证成功?
否
是
435
运行 MAS 预置
完成

图4d

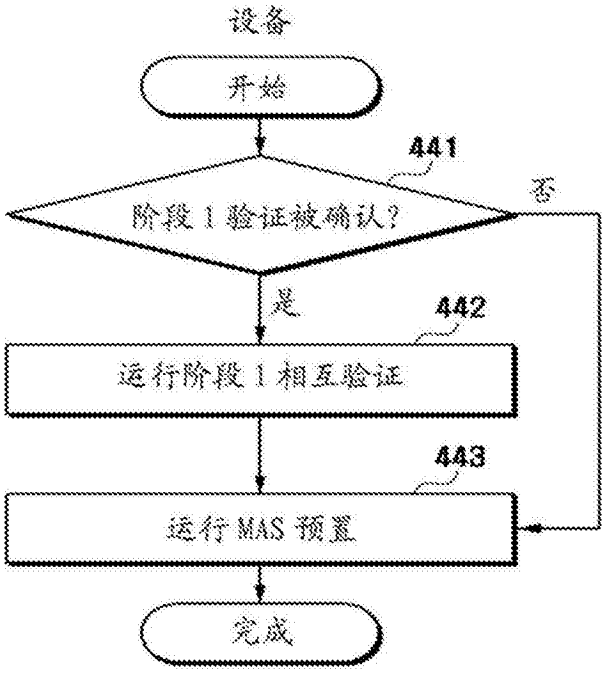


图4e

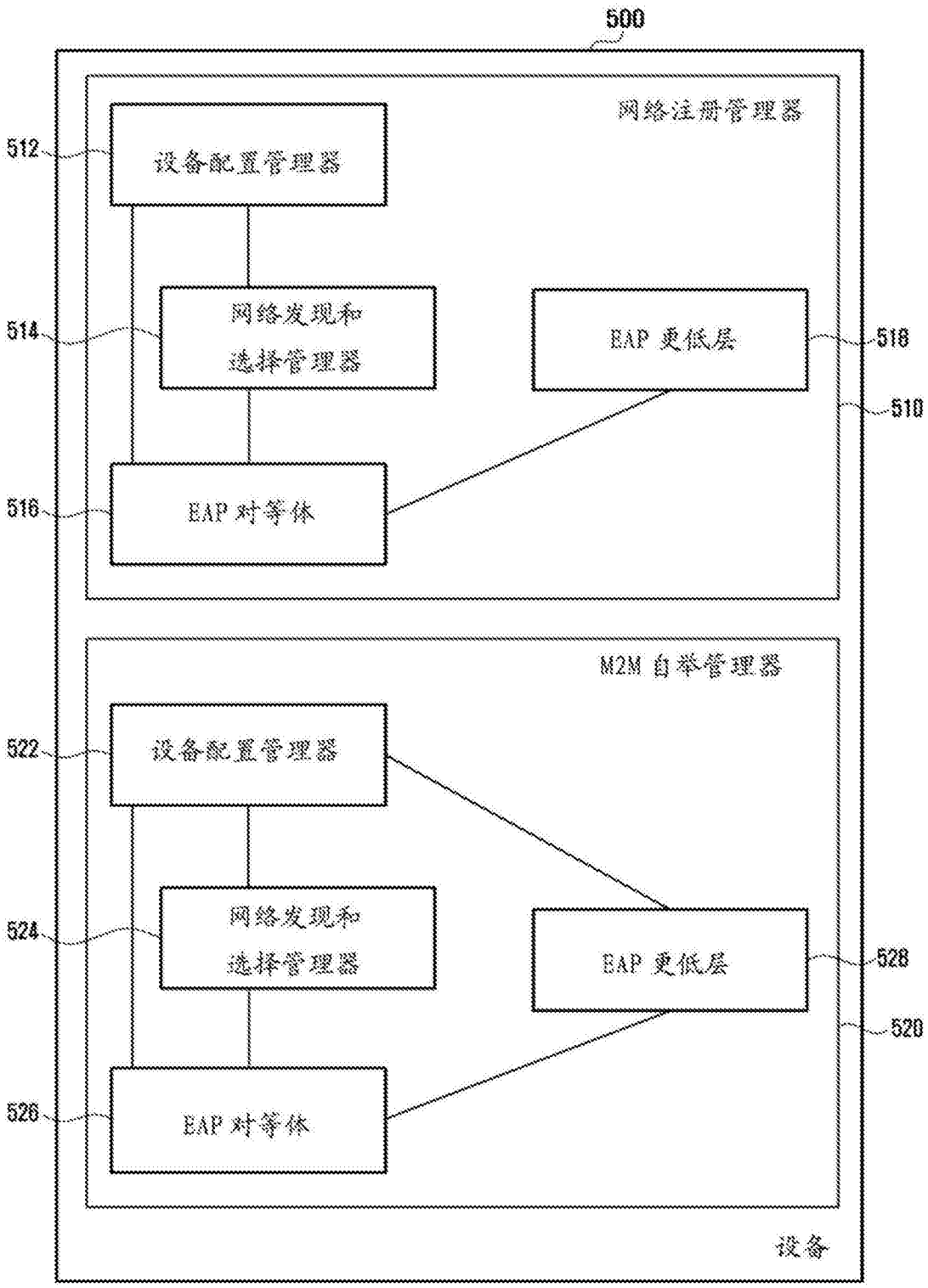

500
网络注册管理器
512
设备配置管理器
514
网络发现和
选择管理器
EAP 更低层
518
510
516
EAP 对等体
M2M 自举管理器
522
设备配置管理器
524
网络发现和
选择管理器
EAP 更低层
528
520
526
EAP 对等体
设备

图5

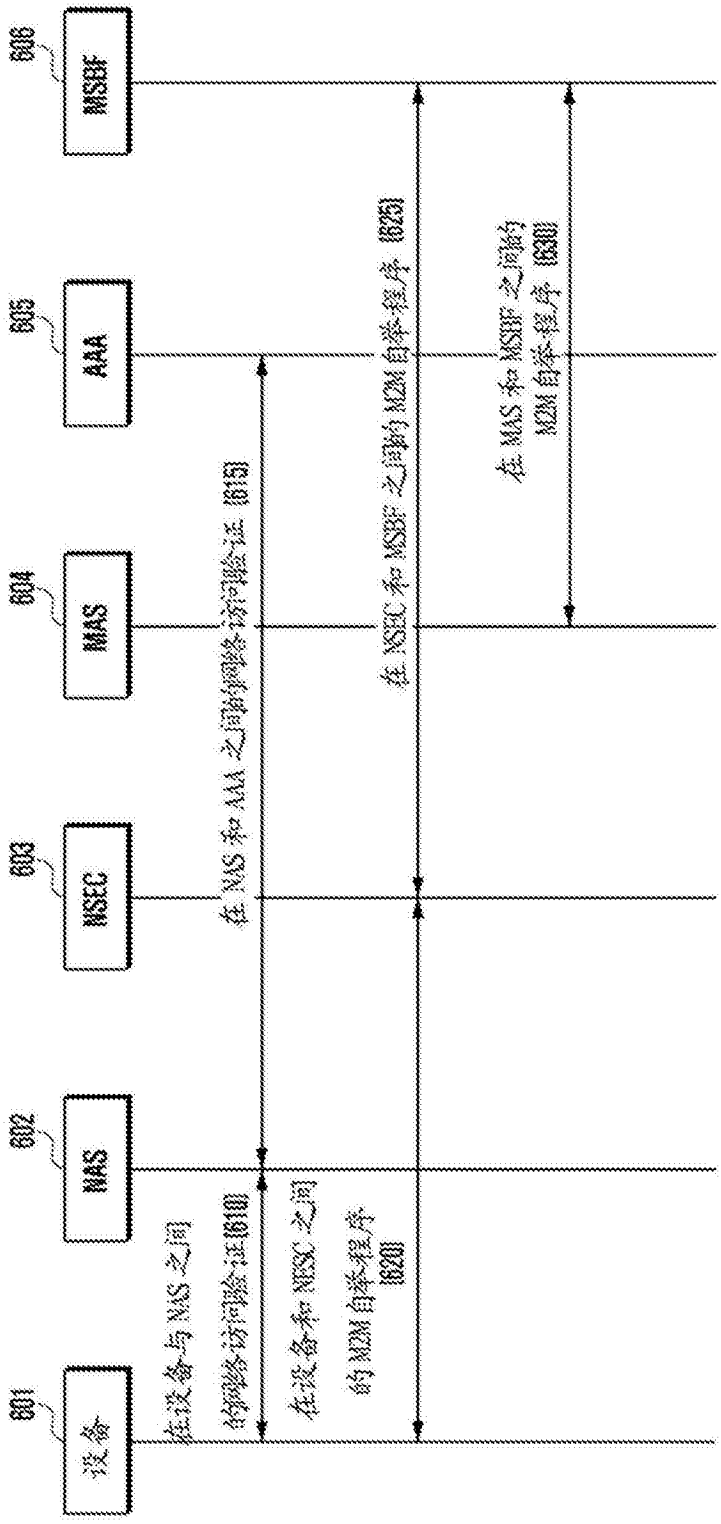

601
设备
602
NAS
603
NSEC
604
MAS
605
AAA
606
MSBF
在设备与 NAS 之间的物理访问验证 [610]
在 NAS 和 AAA 之间的网络访问验证 [615]
在设备和 NSEC 之间的 M2M 自举程序 [620]
在 NSEC 和 MSBF 之间的 M2M 自举程序 [625]
在 MAS 和 MSBF 之间的 M2M 自举程序 [630]

图6

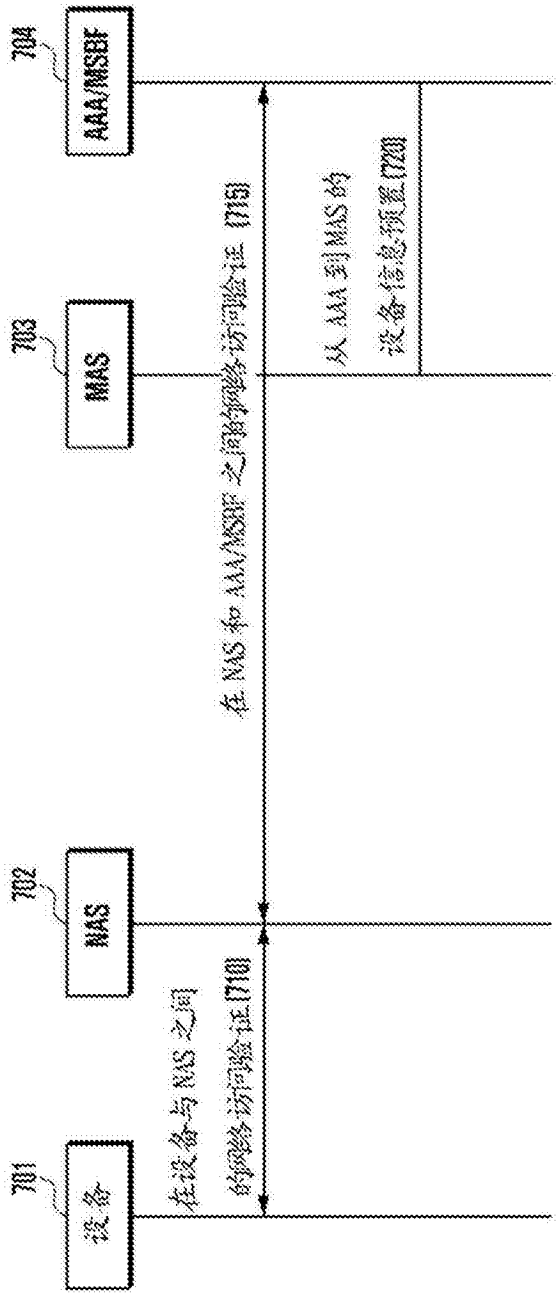

704
AAA/MSEF
703
MAS
702
MAS
701
设备
在设备与NAS之间的网络访问验证[710]
在NAS和AAA/MSEF之间的网络访问验证[715]
从AAA到MAS的设备信息预置[720]

图7

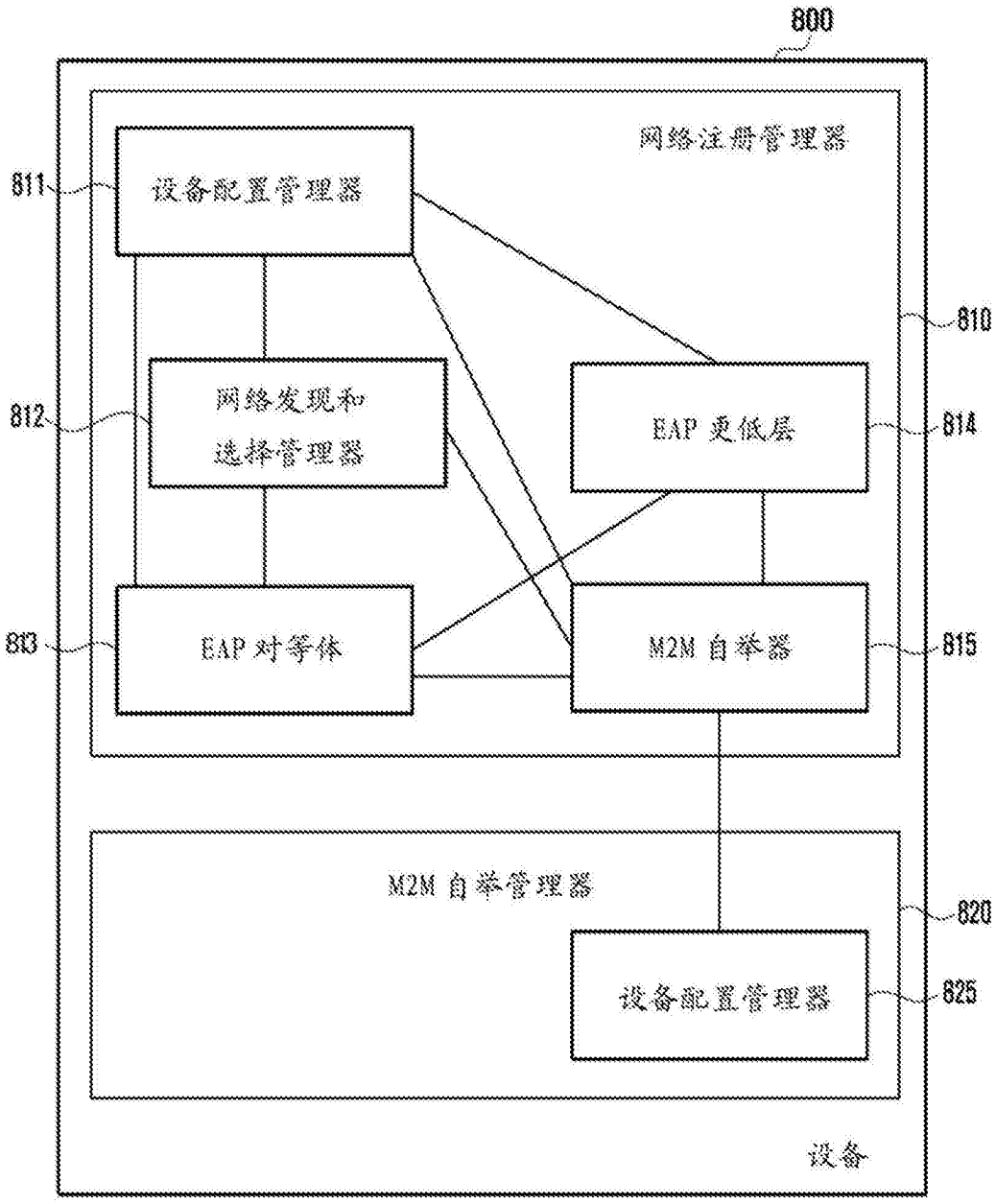

800
网络注册管理器
811
设备配置管理器
810
812
网络发现和
选择管理器
EAP 更低层
814
813
EAP 对等体
M2M 自举器
815
M2M 自举管理器
820
设备配置管理器
825
设备

图8