(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 102687547 B
(45)授权公告日 2015.09.02

(21)申请号 201080059882.9
(22)申请日 2010.12.28
(30)优先权数据
61/290,482 2009.12.28 US
61/293,599 2010.01.08 US
61/311,089 2010.03.05 US
(85)PCT国际申请进入国家阶段日
2012.06.28
(86)PCT国际申请的申请数据
PCT/US2010/062196 2010.12.28
(87)PCT国际申请的公布数据
WO2011/082150 EN 2011.07.07
(73)专利权人 交互数字专利控股公司
地址 美国特拉华州
(72)发明人 S·B·帕塔尔 I·查 Y·C·沙阿
A·施米特 A·莱切尔
P·R·季塔布 L·凯斯
(74)专利代理机构 北京润平知识产权代理有限公司 11283
代理人 南毅宁 刘国平
(51)Int.Cl.
H04W 12/06(2006.01)
H04L 12/24(2006.01)
H04L 29/06(2006.01)
(56)对比文件
CN 101617346 A,2009.12.30,
US 2007150945 A1,2007.06.28, 全文.
审查员 马洁

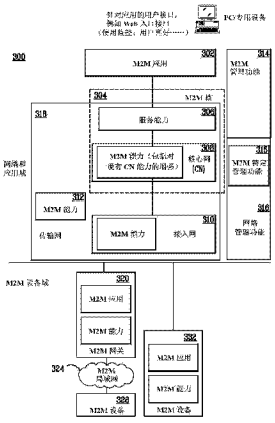
权利要求书2页 说明书23页 附图20页

(54)发明名称

机器对机器网关体系结构

(57)摘要

公开了用于使网络域之外的网关向多个设备提供服务的系统、方法和手段。举例来讲,该网关可用作管理实体或网络域的代理。作为管理实体,网关可执行与多个设备中的每一个相关的安全功能。网关可在网络域不参与,或不知道特定设备的情况下执行安全功能。作为网络的代理,网关可从网络域接收命令,执行与多个设备中的每一个相关的安全功能。网络可以获知多个设备中的每一个的标识。网关可为多个设备中的每一个执行安全功能,并在将相关信息发送至网络域之前对该信息进行聚合。



CN 102687547 B

1. 一种将网络域的特定功能卸载至位于该网络域之外的机器对机器网关的方法，该方法包括，由所述机器对机器网关：

作为管理实体与所述网络域建立信任；

与多个设备中的每一个设备建立连接，所述多个设备与所述网络域进行通信；

独立于所述网络域，为所述多个设备中的每一个设备执行安全功能；以及

将与所述多个设备中的每一个设备相关的信息报告给所述网络域。

2. 根据权利要求 1 所述的方法，其中，所述信息被聚合自所述多个设备中的每一个设备。

3. 根据权利要求 1 所述的方法，其中针对所述多个设备中的每一个设备来解析并执行经过聚合的安全功能。

4. 根据权利要求 1 所述的方法，其中所述报告是响应于来自所述网络域的请求的。

5. 根据权利要求 1 所述的方法，其中周期性地执行所述报告。

6. 根据权利要求 1 所述的方法，其中所述安全功能包括将所述多个设备中的每一个设备与所述网络域进行登记和认证。

7. 根据权利要求 6 所述的方法，其中所述登记和认证包括使用启动证书。

8. 根据权利要求 1 所述的方法，其中所述安全功能包括向所述多个设备中的每一个设备进行证书的提供和迁移。

9. 根据权利要求 1 所述的方法，其中所述安全功能包括向所述多个设备中的每一个设备提供安全策略。

10. 根据权利要求 1 所述的方法，其中所述安全功能包括在所述多个设备中的每一个设备中建立可信功能，其中为所述多个设备中的每一个设备执行完整性校验。

11. 根据权利要求 1 所述的方法，其中所述安全功能包括为所述多个设备中的每一个设备提供设备管理。

12. 根据权利要求 11 所述的方法，其中向所述网络域发送与所述多个设备中的至少一个设备相关联的严重失败警告。

13. 根据权利要求 1 所述的方法，其中所述安全功能包括为所述多个设备中的至少一个设备建立以下中的至少一者：安全关联、通信信道、或通信链路。

14. 根据权利要求 1 所述的方法，该方法还包括：

确定与所述多个设备中的一个或多个设备相关联的完整性破坏或失败；和

对所述多个设备中的所述一个或多个设备进行隔离。

15. 根据权利要求 1 所述的方法，其中代表所述网络域来执行所述安全功能，而不需要网络域的参与。

16. 一种网络域之外的机器对机器网关，该机器对机器网关包括：

用于作为管理实体与所述网络域建立信任的装置；

用于与多个设备中的每一个设备建立连接的装置，所述多个设备与所述网络域进行通信；

用于独立于所述网络域为所述多个设备中的每一个设备执行安全功能的装置；以及

用于将与所述多个设备中的每一个设备相关的信息报告给所述网络域的装置。

17. 根据权利要求 16 所述的机器对机器网关，其中，所述信息被聚合自所述多个设备

中的每一个设备。

18. 根据权利要求 16 所述的机器对机器网关，其中针对所述多个设备中的每一个设备来解析并执行经过聚合的安全功能。

19. 根据权利要求 16 所述的机器对机器网关，其中所述报告是响应于来自所述网络域的请求的。

20. 根据权利要求 16 所述的机器对机器网关，其中所述报告被周期性地执行。

21. 根据权利要求 16 所述的机器对机器网关，其中所述安全功能包括将所述多个设备中的每一个设备与所述网络域进行登记和认证。

22. 根据权利要求 21 所述的机器对机器网关，其中所述登记和认证包括使用启动证书。

23. 根据权利要求 16 所述的机器对机器网关，其中所述安全功能包括向所述多个设备中的每一个设备进行证书的提供和迁移。

24. 根据权利要求 16 所述的机器对机器网关，其中所述安全功能包括向所述多个设备中的每一个设备提供安全策略。

25. 根据权利要求 16 所述的机器对机器网关，其中所述安全功能包括在所述多个设备中的每一个设备中建立可信功能，其中为所述多个设备中的每一个设备执行完整性校验。

26. 根据权利要求 16 所述的机器对机器网关，其中所述安全功能包括为所述多个设备中的每一个设备提供设备管理。

27. 根据权利要求 26 所述的机器对机器网关，该机器对机器网关还包括 ：

用于向所述网络域发送与所述多个设备中的至少一个设备相关联的严重失败警告的装置。

28. 根据权利要求 16 所述的机器对机器网关，其中所述安全功能包括为所述多个设备中的至少一个设备建立以下中的至少一者 ：安全关联、通信信道、或通信链路。

29. 根据权利要求 16 所述的机器对机器网关，该机器对机器网关还包括 ：

用于确定与所述多个设备中的一个或多个设备相关联的完整性破坏或失败的装置 ；和

用于对所述多个设备中的所述一个或多个设备进行隔离的装置。

30. 根据权利要求 16 所述的机器对机器网关，其中代表所述网络域来执行所述安全功能，而不需要网络域的参与。

机器对机器网关体系结构

[0001] 相关申请的交叉引用

[0002] 本申请基于以下申请并要求享有以下申请的权益：于 2009 年 12 月 28 日提交的美国临时申请 61/290,482、于 2010 年 1 月 8 提交的美国临时申请 61/293,599、于 2010 年 3 月 5 日提交的美国临时申请 61/311,089，其全部内容通过引用而被视为在此加入。

背景技术

[0003] 机器对机器（M2M）体系结构可使用 M2M 网关，可将该网关描述为使用 M2M 功能来确保 M2M 设备交互工作，并交互连接至网络和应用域的设备。该 M2M 网关还可运行 M2M 应用，并可与 M2M 设备位于同处。现有的 M2M 网关体系结构具有缺点。

发明内容

[0004] 公开了用于使位于网络域之外的网关向多个设备提供服务的系统、方法和手段（instrumentality）。网关还可向网络域的设备提供服务能力，这样可以使网络域不再需要提供此功能。

[0005] 该网关可用作管理实体。该网关可与网络域建立信任。例如，该网关可与网络域建立信任级，从而使网关与网络域进行交互。该网关可与多个设备中的每一个建立连接。该网关可执行与每个设备有关的安全功能。该网关可以代表网络域执行安全功能。该网关可以在网络域不直接参与或最少地参与的情况下来执行安全功能。该网关可以在网络不知道特定设备的情况下执行安全功能。该网关可向网络域报告有关每个设备的设备信息。

[0006] 该网关可用作网络的代理。该网关可与网络域建立信任。例如，该网关可与网络域建立信任级，从而使网关与网络域进行交互。该网关可从网络域接收命令，执行与多个设备中每一个相关的安全功能。例如，该网关可从网络域接收单个命令，并响应于该命令，而对多个设备执行安全功能。网络可知道多个设备中每一个的标识。该网关可为多个设备中的每一个执行安全功能。该网关可将从多个设备中的每一个所接收的与所执行的安全功能有关的信息进行聚合，并将聚合后的信息发送至网络域。网关可处理该聚合后的信息，并将该处理后的聚合信息发送至网络域。

[0007] 网关执行的安全功能可包括以下中的一者或多者：使用或不使用启动证书将设备登记至网络域或对设备认证；对针对多个设备中的每一个的证书进行提供和迁移；对多个设备中的每一个提供安全策略；对多个设备中的每一个执行认证；在多个设备中的每一个中建立可信功能，其中，对多个设备中的每一个执行完整性校验（integrity validation）；对多个设备中的每一个提供设备管理，包括故障查找和故障修复；或对多个设备中的至少一个建立以下至少一者：安全关联、通信信道或通信链路。

附图说明

[0008] 可从以下描述中获得更详细的理解，该描述是以结合附图的方式举例说明的，在附图中：

[0009] 图 1 表示无线通信系统示例；

[0010] 图 2 表示 WTRU 和节点 B 示例；

[0011] 图 3 表示 M2M 体系结构示例；

[0012] 图 4 表示情况 3 网关功能示例；

[0013] 图 5 表示情况 3 连接设备的启动 (bootstrapping) 和登记流示例；

[0014] 图 6 表示情况 4 连接设备的启动和登记流示例；

[0015] 图 7 表示分级连接性体系结构示例；

[0016] 图 8 表示用于情况 3 和 4 的设备完整性校验的呼叫流示例结构图；

[0017] 图 9 表示用于情况 1 的设备完整性和登记的呼叫流示例结构图；

[0018] 图 10 表示用于情况 2 的设备和网关完整性和登记的呼叫流示例结构图；

[0019] 图 11 表示用于情况 3 的设备和网关完整性和登记的呼叫流示例结构图；

[0020] 图 12 表示用于情况 4 的设备和网关完整性和登记的呼叫流示例结构图；

[0021] 图 13 表示分层验证的示例场景；

[0022] 图 14 表示 M2M 体系结构示例；

[0023] 图 15 表示 M2M 网络层的服务能力的体系结构示例；以及

[0024] 图 16A 和 16B 表示 M2M 网关和接口的体系结构示例；

[0025] 图 17A 是可实现所公开的一个或多个实施方式的示例通信系统的系统结构图；

[0026] 图 17B 是可在图 17A 中所示的通信系统中所使用的示例无线发射 / 接收单元 (WTRU) 的系统结构图；

[0027] 图 17C 是可在图 17A 中所示的通信系统中所使用的示例无线电接入网和示例核心网的系统结构图。

具体实施方式

[0028] 图 1- 图 17 可涉及用于实现所公开的系统、方法和手段的示例实施方式。但是，虽然结合示例实施方式对本发明进行了描述，但是，其不限于此，并应当理解，可使用其他实施方式，或对所述实施方式进行修改或增加，以执行与本发明相同的功能，而不偏离本发明。例如，可结合 M2M 实施方式来描述所公开的系统、方法和手段，但是，其实施方式并不限于此。此外，可结合无线实施来描述所公开的系统、方法和手段，但是，其实施方式并不限于此。例如，所公开的系统、方法和功能可用于有线连接。并且，附图中表示了呼叫流，该呼叫流仅用于作为示例。应当理解，还可使用其他实施方式。并且，可在合适的位置改变流的顺序。此外，如果不需要可省略流，而且还可增加额外的流。

[0029] 当在下文中提及时，术语“无线发射 / 接收单元 (WTRU)”可包括，但不限于，用户设备 (UE)、移动站、固定或移动用户单元、寻呼机、蜂窝电话、个人数字助理 (PDA)、计算机或能够在无线环境中进行操作的任何其他类型的用户设备。当在下文中提及时，术语“基站”可包括，但不限于，节点 B、站点控制器、接入点 (AP) 或能够在无线环境中进行操作的任何其他类型的接口设备。

[0030] 图 1 示出了无线通信系统 100 的典型示例，该系统包括多个 WTRU 110、基站 (例如节点 B120)、控制无线电网络控制器 (CRNC) 130、服务无线电网络控制器 (SRNC) 140 和核心网 150。节点 B 120 和 CRNC 130 可统称为 UTRAN。

[0031] 如图 1 所示，WTRU 110 可与节点 B 120 进行通信，节点 B 120 则与 CRNC130 和 SRNC 140 进行通信。虽然在图 1 中仅示出了三个 WTRU 110、一个节点 B 120、一个 CRNC 130 和一个 SRNC 140，但是应当注意，在无线通信系统 100 中可包括任何的无线和有线设备的组合。

[0032] 图 2 是图 1 的无线通信系统 100 的示例 WTRU 110 和节点 B 120 的功能框图 200。如图 2 所示，WTRU 110 可与节点 B 120 进行通信，并可将两者配置为协助机器对机器（M2M）网关，该 M2M 网关使用 M2M 功能来确保 M2M 设备之间的交互工作以及 M2M 设备与网络和设备域的互连。

[0033] 除了典型 WTRU 中所具有的组件以外，WTRU 110 可包括处理器 115、接收机 116、发射机 117、存储器 118 和天线 119。存储器 118 可储存软件，该软件包括操作系统、应用和其他功能模块。处理器 115 可单独或与软件一起执行方法，以协助机器对机器（M2M）网关，其中该 M2M 网关使用 M2M 功能来确保 M2M 设备之间的交互工作以及 M2M 设备与网络和设备域的互连。接收机 116 和发射机 117 可以与处理器 115 通信。天线 119 可以同时与接收机 116 和发射机 117 通信，以促进无线数据的发送和接收。

[0034] 除了典型基站中所具有的组件以外，节点 B 120 可包括处理器 125、接收机 126、发射机 127 和天线 128。处理器 125 可被配置为与机器对机器（M2M）网关共同工作，其中该 M2M 网关使用 M2M 功能来确保 M2M 设备之间的交互工作以及 M2M 设备与网络和设备域的互连。接收机 126 和发射机 127 可以与处理器 125 通信。天线 128 可以同时与接收机 126 和发射机 127 通信，以促进无线数据的发送和接收。

[0035] 所公开的系统、方法和手段可使网络域之外的网关能够向多个设备提供服务。网关可向设备提供网络域的服务功能，这可减少否则需要由网络域所提供的功能。

[0036] 该网关可用作管理实体。该网关可与网络域建立信任。例如，该网关可与网络域建立信任级别，以使该网关与网络域进行交互。该网关可与多个设备中的每一个建立连接。该网关可执行与每个设备有关的安全功能。该网关可代表网络域执行安全功能。该网关可在网络域不直接参与或最少程度地参与的情况下执行安全功能。该网关可以在网络不知道特定设备的情况下执行安全功能。该网关可向网络域报告有关每个设备的设备信息。

[0037] 该网关可用作网络的代理。该网关可与网络域建立信任。例如，该网关可与网络域建立信任级别，以使网关与网络域进行交互。该网关可从网络域接收命令，执行与多个设备中的每一个设备相关的安全功能。例如，该网关可从网络域接收单个命令，并响应于此而为多个设备执行安全功能。网络可知道多个设备中每一个的标识。该网关可为多个设备中的每一个执行安全功能。该网关可对来自多个设备中每一个的、与所执行的安全功能有关的信息进行聚合，并将聚合后的信息发送至网络域。该网关可对聚合后的信息进行处理，并将处理后的聚合信息发送至网络域。

[0038] 该网关所执行的安全功能可包括以下中的一者或多者：使用或不使用启动证书将设备登记至网络域或对设备认证；对针对多个设备中的每一个的证书进行提供和迁移；对多个设备中的每一个提供安全策略；对多个设备中的每一个执行认证；在多个设备中的每一个中建立可信功能，其中，对多个设备中的每一个执行完整性校验；对多个设备中的每一个提供设备管理，包括故障查找和故障修复；或对多个设备中的至少一个建立以下至少一者：安全关联、通信信道或通信链路。

[0039] 图 3 表示可在所公开的系统、方法和手段中所使用的 M2M 体系结构的实施方式。该

M2M 网关 320 可被配置为针对经由 M2M 局域网 324 与其相连接的 M2M 设备(例如 M2M 设备 328)用作聚合器。每个连接至该 M2M 网关 320 的 M2M 设备可包括 M2M 设备标识,并与 M2M 网络进行认证。

[0040] 在 M2M 设备域 360 中,具有 M2M 设备 332,其使用 M2M 能力和网络域功能运行应用。M2M 设备可直接连接至接入网 310 (例如,M2M 设备 332),或通过 M2M 局域网 324 与 M2M 网关 320 相连接(例如,M2M 设备 328)。M2M 局域网 324 可在 M2M 设备与 M2M 网关之间提供连接。一些 M2M 局域网的例子包括 :个人局域网技术,例如 IEEE 802.15、Zigbee、蓝牙和其他类似技术。术语 M2M 局域网和 M2M 毛细网(capillary network)可交换使用。M2M 网关 320 可以是使用 M2M 能力来确保 M2M 设备能够交互工作以及互连至网络域 350 的设备,该网络域 350 还可称为网络和应用域 350。该 M2M 网关 320 还可运行 M2M 应用。该 M2M 网关功能可与 M2M 设备位于同处。例如,M2M 网关,例如 M2M 网关 320,可实施本地智能,从而激活由收集和处理各种信息源(例如,来自传感器和上下文参数)所产生的自动处理。

[0041] 在网络域 350 中,具有 M2M 接入网 310,其可使 M2M 设备域 360 与核心网 308 进行通信。基于现有接入网的 M2M 功能可能需要向 M2M 服务的传递提供增强。接入网的例子包括 :数字用户线技术(xDSL)、混合同轴光纤(HFC)、电力线通信(PLC)、用于卫星、移动全球系统(GSM)演进型 GSM 增强型数据速率(EDGE)无线电接入网(GERAN)、通用移动电信系统(UMTS)陆地无线电接入网(UTRAN)、演进型 UTRAN (eUTRAN)、无线局域网(W-LAN)和 WiMAX。

[0042] 还可具有传输网络,例如传输网络 318,其可使得数据能够在网络域 350 内传输。基于现有传输网的 M2M 功能可能需要向 M2M 服务的传递提供增强。M2M 核 304 由核心网 308 和服务功能所组成。M2M 核心网 308 可提供 IP 连接、服务和网络控制功能、互连(与其他网络)、漫游(用于公共陆地移动网(PLMN))等。不同的核心网可提供不同的能力集合。基于现有核心网的 M2M 功能可能需要向 M2M 服务的传递提供增强。核心网的例子可包括第三代合作伙伴计划(3GPP)核心网(例如,通用分组无线电服务(GPRS)、演进型分组核心(EPC))、用于高级连网(networking)的 ETSI 电信和互联网融合服务和协议(TISPAN)核心网。在具有 IP 服务供应商网络的情况中,核心网提供有限的功能。

[0043] 服务能力 306 所提供的功能可由不同应用共享。服务能力 306 通过一组开放的接口来提供功能。此外,服务能力 306 可使用核心网功能。可使用服务能力 306 来优化应用开发和配置,并向应用隐藏网络特性。服务能力 306 可以是 M2M 特定的,或通用的,例如向除了 M2M 之外的应用提供支持。其例子包括数据存储和聚合、单播和多播消息传递等。

[0044] 该 M2M 应用 302 可包括运行服务逻辑并使用能够经由开放接口接入的服务功能的应用。网络管理功能 316 可包括用于管理接入网 310、传输网 318 和核心网 308 所需的功能,包括相关的 M2M 能力,例如提供、监督、故障管理和其他功能。网络管理功能 316 中可包括 M2M 特定管理功能 315,用于管理接入网 310、传输网 318 和核心网 308 中的 M2M 能力。该 M2M 管理功能 314 可包括用于管理 M2M 应用 302 和服务能力 306 的功能,以及 M2M 设备和网关(例如,M2M 网关 320、M2M 设备 328 和 M2M 设备 332 等)的功能。M2M 设备和网关的管理可使用服务能力(例如设备管理服务能力)。该 M2M 管理功能 314 可包括用于 M2M 设备 328 或 M2M 网关 320 的故障查找和故障修复的功能。

[0045] 现在描述 M2M 体系结构和多个 M2M 设备的连接方法。M2M 设备可以以多种方式与 M2M 网络进行连接。此处表示了四种示例情况。在第一种情况中(情况 1),M2M 设备直接经

由接入网连接至 M2M 系统。M2M 设备向 M2M 系统进行登记和认证。在第二种情况中(情况 2),M2M 设备经由 M2M 网关局域网连接至 M2M 系统。该 M2M 网关经由接入网连接至 M2M 系统。该 M2M 设备经由 M2M 网关向 M2M 系统进行认证。该局域网可以是或者不是蜂窝网、WLAN、BT 和其他系统。在第二种情况中,该 M2M 网关对 M2M 设备仅起隧道的作用。由 M2M 网络来对 M2M 设备执行例如登记、认证、授权、管理和提供的过程。

[0046] 现在描述另两种情况。在情况 3 中,网关,例如 M2M 网关 320 可用作管理实体。该 M2M 设备(例如 M2M 设备 328)可例如通过 M2M 局域网 324 连接至 M2M 网关 320。该 M2M 网关 320 可连接至 M2M 网络域 350,并与之建立信任,其中该连接可以是经由接入网 310 的。该 M2M 网关 320 可以通过独立于 M2M 网络域 350 的控制的方式,对与其相连接的 M2M 设备进行管理,该管理可以通过例如重新使用局域网 310 所提供的现有的登记、认证、授权、管理和提供方法来执行。连接至这种网关的设备可以是或者不是可由 M2M 网络域 350 寻址的。该 M2M 局域网 324 可以是或者不是蜂窝网、WLAN、BT 或其他此类网络。网关可对每个与其相连接的 M2M 设备执行安全功能。该网关可在 M2M 网络域 350 不直接参与或不知道特定设备,或者 M2M 网络域 350 尽少地参与的情况下,执行安全功能。该 M2M 网关 320 可针对所执行的安全功能向网络域报告有关每个设备的信息。

[0047] 在情况 4 中,网关,例如 M2M 网关 320,可用作网络(例如网络域 350)的代理。该 M2M 设备(例如 M2M 设备 328)经由例如 M2M 局域网 324 连接至 M2M 网关 320。连接至该网关的设备可以是或者不是可由 M2M 网络寻址的。该 M2M 网关 320 可连接至 M2M 网络域 350,并与之建立信任,其中,该连接可以是经由接入网 310 的。该 M2M 网关 320 对于与其相连接的 M2M 设备(例如 M2M 设备 328)来说,可用作 M2M 网络域 350 的代理。该 M2M 网关可从网络域接收命令,执行与每个与其相连接的 M2M 设备有关的安全功能。例如,该网关可从网络域接收单个命令,并作为响应,为多个设备执行安全功能。该网关可执行安全功能。该网关可执行诸如认证、授权、登记、设备管理和提供等过程,并还可代表 M2M 网络所执行应用。网关可对来自多个设备中每一个的与所执行的安全功能有关的信息进行聚合,并向 M2M 网络域 350 发送聚合信息。该网关可对聚合信息进行处理,并将处理后的聚合信息发送至网络域。

[0048] 图 4 表示情况 3 的网关功能示例。该 M2M 网关 410 连接至 M2M 网络域 350,为 M2M 局域网(例如毛细网)所连接的 M2M 设备 430 维护本地 AAA 服务器 420。该 AAA 服务器 420 可促进本地登记、认证、授权、计费和设备完整性校验。

[0049] 对于情况 3 中所连接的设备,使用了用于登记、认证、授权和设备管理的 M2M 局域网协议和过程。该设备可以是或者不是可由 M2M 网络域 350 寻址的。该网关对于 M2M 网络表现为 M2M 设备,并执行登记和认证。图 5 表示用于情况 3 中所连接的设备或连接场景中的启动和登记流示例。

[0050] 图 5 表示 M2M 设备 502、M2M 网关 504、接入网 506 (例如与网络运营商相关联)、认证服务器 508 (例如与网络运营商相关联)、安全能力 510、AAA/GMAE 512 和其他能力 514。在 522,M2M 网关 504 通过接入网 506 获取网络。在 524 和 528,可在 M2M 网关 504 与接入网 506 之间,以及接入网 506 与认证服务器 508 之间,进行接入认证。在 526,可在 M2M 网关 504 与接入网 506 之间执行链路与网络会话建立。启动包括 529 和 530 处的流。可将启动限于在提供期间的执行。在 529,可在 M2M 网关 504 与安全能力 510 之间执行启动请求。在

530，可在 M2M 网关 504 与安全能力 510 之间执行 M2M 安全启动。在 536，可在安全能力 510 与 AAA/GMAE 512 之间执行设备提供（例如，提供数据，例如 M2M 网络地址标识符（NAI）和根密钥，或其他设备或应用级的参数或数据）。在 532，在 M2M 网关 504 与安全能力 510 之间进行 M2M 登记，其中包括认证和生成会话密钥。在 538，可在安全能力 510 与 AAA/GMAE 512 之间进行 M2M 认证，该 M2M 认证可包括认证 M2M 设备、服务能力、服务能力组、或 M2M 设备的一个或多个应用。在 540，安全能力 510 可向其他能力 514 提供加密密钥。在 534，可在 M2M 设备 502 与 M2M 网关 504 之间进行局域协议、登记、认证和提供。

[0051] 对于情况 4 所连接的设备，可使用局域网协议和过程来进行登记认证、授权和设备管理。该 M2M 网关中可具有连网功能，其可向 M2M 设备翻译 M2M 网络命令。该设备可以是或者不是可由 M2M 网络域寻址的。图 6 表示用于情况 4 所连接的设备的启动和登记流示例。图 6 中所示的情况 4 的流包括图 5 的流。此外，在 644，可在 M2M 网关 504 与 M2M 网络域的安全能力 510 之间进行设备登记 / 认证状态报告。

[0052] 仍然参考情况 4 的示例，M2M 网关向网络进行登记和认证，以在网络中建立信任，从而用作网络的代理。在这种情况下，M2M 网关可以 ：执行 M2M 设备提供 ；执行 M2M 设备本地登记（包括本地区域认证）和标识管理 ；执行 M2M 认证（例如，对于一个或多个 M2M 设备，M2M 设备的一个或多个服务或 M2M 设备的一个或多个应用）、授权和计费 ；执行 M2M 设备完整性校验 ；用作网络的代理，从而其可以 ：向网络对其自身进行验证（verify）；验证附属至 M2M 接入网的设备 ；管理安全和信任（包括 M2M 设备的认证和标识管理），包括管理和维护 M2M 设备的安全关联 ；和执行本地 IP 接入路由。

[0053] 可在多种应用中使用该 M2M 网关。例如，但不限于，其可用于演进型毫微微蜂窝、演进型家庭节点 B 或具有有线或无线回程的家庭节点 B 实现。其还可用作网络和 / 或用户的数字代理。网络可以不知道 M2M 设备 ；该网关可代表网络来管理和维护 M2M 设备连接。用作数字代理的 M2M 网关可具有听筒或其他移动终端形式的因素。其还可用于电子健康（eHealth）的情况中，其中将传感器和致动器（actuator）连接至该 M2M 网关。该传感器 / 致动器可以不向 M2M 网络域进行登记和认证。而是，这些 M2M 设备（传感器 / 致动器）可向 M2M 网关进行登记。在这些应用中，M2M 网关可以是手持设备，例如 PDA 或移动电话或流量聚合器，例如接入点或路由器。所述连接可以使 M2M 网关能够为相连接的 M2M 设备的子集执行代理功能，并且，对于与其相连接的 M2M 设备，其可用作情况 2 的 M2M 网关。所述连接可使 M2M 网关针对 M2M 接入网和核心网用作情况 1 中所连接的 M2M 设备，而该 M2M 网关可独立地对连接至该 M2M 网关的 M2M 设备进行管理。所述连接可使 M2M 网关针对另一 M2M 网关用作 M2M 设备，如图 7 所示，例如，M2M 网关 720 可针对 M2M 网关 710 用作 M2M 设备。该 M2M 网关 710 可为由 M2M 局域网（又称为毛细网）所连接的 M2M 设备 712 维护本地 AAA 服务器 715。该 M2M 网关 720 可为由 M2M 局域网（例如毛细网）所连接的 M2M 设备 722 维护本地 AAA 服务器 725。

[0054] 完整性校验可包括本地化操作以及基于在本地执行的测量所进行的报告和远程操作，例如，可直接或间接地通过信令来进行校验。为了实现设备完整性检查和校验，该 M2M 设备可包括可信的操作环境。从该可信的操作环境中，该设备可检查其软件的完整性，并在安全启动过程装载和执行前，将其完整性相对于可信参考值进行验证。该可信参考值可由可信第三方或可信制造商颁发，并且是所验证的单元的测量值（例如是哈什值）。可本地地

(例如,自主校验)或远程地(例如,半自主校验和完全远程校验)来执行该软件的完整性校验。如果远程地执行设备完整性校验,则该执行校验的实体可以是 M2M 网关或用作校验实体的 M2M 网关的指定实体或代理。如果校验目标是连接至 M2M 网关的 M2M 设备,和 / 或 M2M 网络上基于网络的校验实体或 M2M 网络的指定实体或代理,则校验目标可以是 M2M 设备或 M2M 网关,或两者的结合。

[0055] 在完全远程校验中,目标实体(需要校验完整性的实体)可向校验实体发送其完整性的测量,而不需要本地所执行的验证的证据或结果。而另一方面,在半自主校验中,目标实体可同时对其完整性进行测量,并对测量进行验证 / 评价,并可向校验实体发送与验证结果有关的证据或信息。

[0056] 如果在本地执行完整性校验进程,则可将可信参考值存储在安全存储器内,并将访问限制为授权访问。如果在远程校验实体(例如,用作校验实体的 M2M 网关,或 M2M 网络上的基于网络的校验实体)处进行验证,则网关或基于网络的校验实体可在校验过程中从可信第三方或可信制造商处获取这些可信参考值,或预先获取该可信参考值并将其在本地保存。还可由运营商或用户在 M2M 网关或 M2M 网络中的校验实体处提供这些可信参考值。可由可信第三方或可信制造商通过无线、通过有线或在安全介质中(例如安全通用串行总线(USB)、安全智能卡、安全数字(SD)卡)来颁发该可信参考值,其中用户或运营商可在 M2M 网关(例如,对于半自主校验)或在 M2M 设备(例如,对于自主校验)中插入该安全介质。对于基于 M2M 网络的半自主校验,校验实体可直接从可信制造商或可信第三方获得该信息。

[0057] 需要对 M2M 局域网协议进行新的更新,以将完整性结果从设备发送至 M2M 网关中的验证实体。可通过更新协议区域,或通过在初始的随机接入消息中或在建立了连接之后以应答或非应答形式来发送报文来实现该更新,该报文包括完整性结果和度量。

[0058] 可使用以下方法示例中的一者或多者来进行自主或半自主的设备完整性校验。

[0059] 可向情况 1 的设备提供设备校验过程。

[0060] 在这种情况下,设备直接通过核心网连接至 M2M 网络。在支持自主校验的设备中,设备对接入网的初始接入可包括本地完整性检查和校验的结果。由于设备已经尝试在网络中登记,因此网络可假设设备完整性校验已经成功。如果设备完整性检查失败,则可在呼救信号中包含该失败实体或功能的列表,并且网络可采取必要的步骤来修复或恢复所述设备。

[0061] 对于半自主校验,在接入网或 M2M 网络,或两者中,可能需要验证实体。该验证实体可以是平台校验实体,并可与认证、授权和计费(AAA)服务器位于同处。可向该平台校验实体(PVE)发送本地完整性检查的结果,该 PVE 判断完整性校验是成功还是失败。对于成功的检查,该 PVE 可允许设备在接入网和 / 或 M2M 服务能力层或 M2M 网络中登记。对于失败的校验,该 PVE 可将设备重定向至修复服务器,以便下载更新或补丁。对于失败的校验,PVE 可隔离该设备,并用信号通知 OAM 派出相关人员来维修该设备。

[0062] 可对情况 2 的设备和网关提供设备校验过程。

[0063] 在这种情况下,设备可经由 M2M 网关连接至 M2M 网络。该设备可由 M2M 网络寻址。该 M2M 网关在这种情况下用作隧道提供方。单独考虑网关和设备的完整性检查会很有帮助。首先,可以以此处所述的半自主或自主的方式来对验证网关的完整性,只是其中将设备换为网关。在对网关成功地进行了完整性检查之后,可允许设备连接至 M2M 网关。之后可

以对设备进行完整性检查。可由接入网中的PVE通过M2M服务能力层或M2M网络来自主或半自主地执行该校验。

[0064] 对于半自主校验，M2M网关可执行安全网关的任务，其中，其可对M2M设备执行接入控制。在对M2M设备的设备完整性检查过程完成之前，其可阻止对PVE进行接入，并且，如果M2M设备的完整性检查失败，则其可通过对M2M设备进行隔离或将其接入限制在修复实体的范围内来执行接入控制并限制M2M设备的接入。

[0065] 可对情况3和情况4的设备和网关提供设备校验过程。

[0066] 设备可执行自主校验，其中，由网关或网络隐式地检查和校验设备完整性。设备可执行半自主或完全远程校验，其中设备向验证实体发送完整性检查结果或信息或结果的概要(例如，对应于完整性检查失败组件的失败功能的列表)。

[0067] 在情况3的连接中，M2M设备的验证实体可以是M2M网关。该M2M网络(和/或接入网)可需要另一实体(或另外的多个实体，如果需要M2M网络和接入网两者都进行(但单独进行)完整性校验的话)用作M2M网关完整性的验证实体。该M2M网络和/或接入网可以通过验证M2M网关的完整性而以间接地方式来“校验”M2M设备的完整性，其中在对网关完成了完整性验证之后，网关被认为是“可信”的，以执行其在验证M2M设备完整性中担当的角色。

[0068] 在情况4的连接中，可在M2M网关与M2M网络之间划分用于M2M设备完整性的验证实体的角色。用于M2M网关的完整性的验证实体的角色需要由M2M网络或接入网上的实体来担当。可由一个或多个策略来定义是否和怎样(包括程度)在M2M网关与M2M网络(和/或接入网)之间划分(验证实体的)任务。如果使用采用树状结构(例如，树状验证)的划分校验，则策略可指示M2M网关对设备执行粗略的完整性校验，并将结果报告给M2M网络(和/或接入网)中的一个或多个验证实体。该验证实体可查看并评估这些结果，并根据评估和其自身策略的结果，直接或间接地通过网关，执行精细的完整性验证。

[0069] 一种该策略可来自M2M运营商，另一种该策略可来自接入网运营商。其他利害关系方(stakeholder)也可调用并使用其自身的策略。

[0070] 如果设备完整性校验通过，则该设备可向网络进行登记和认证。对于情况3的连接，可在M2M局域网内在本地对设备进行登记和认证。对于情况4的链接，也可在M2M网关与M2M网络(和/或接入网)之间，划分执行这些任务的实体。

[0071] 在情况3和情况4的连接的情况中，根据所配置的策略，M2M网关可在M2M设备向该M2M网关登记之前，非同步地向M2M接入网和M2M核心网进行登记和认证。该M2M网关可延迟向M2M接入网和M2M核心网进行登记和认证，直到设备完成了认证之后。在从设备接受登记并开始向M2M核心网/M2M接入网登记之前，M2M设备可进行其自身的完整性检查和校验过程，例如自主地或半自主地进行。

[0072] 情况3和4的设备完整性校验可包括图8中所示的流中的一个或多个。图8示出了一个或多个M2M设备802、M2M网关804(其可包括本地AAA)、网络运营商806(其可包括接入网)和M2M运营商808(其可包括M2M核(GMAE/DAR))。在820，M2M网关804可自主地或半自主地执行其自身的完整性检查和校验。在824，M2M设备802可执行其完整性检查和校验，如果成功，则进入在828的网关获取、登记和认证。网关可在本地AAA服务器的协助下对M2M设备802进行认证。该网关可开始接受设备登记和认证请求，当：1)一旦其完

成了自身的完整性检查和校验；或 2）在其与 M2M 接入网和 / 或 M2M 核心网登记之后。在 832，网关可向 M2M 接入网（例如，网络运营商 806）和 / 或 M2M 核心网（M2M 运营商 808）进行登记和认证，该过程与 M2M 设备登记和认证是异步的且不可知的，或者，网关可延迟其登记和认证，直至 M2M 设备 802 在 M2M 网关 804 进行了登记和认证为止。

[0073] 在 836，可在 M2M 网关 804 与 M2M 运营商 808 之间进行 M2M 登记和认证。如果一个或多个连接至 M2M 网关 804 的设备的设备完整性检查失败，则可从 M2M 网关 804 向 M2M 核心网（M2M 运营商 808）发送失败设备的列表或失败功能（例如，在设备是传感器的情况下）的列表。根据所述失败（例如，全部失败或特定功能失败），可拒绝该完整性检查失败的设备进行网络接入，或对其接入进行限制（例如，在时间、类型或范围方面）。在一些情况下，例如人体局域网中，或其他无线传感器局域网中，如果认为任何一个或多个设备的完整性检查失败，并且如果所述毛细网和网关中存在该能力的话，则 M2M 网关 804 可尝试对剩余设备的功能或拓扑更新进行协调，这样其余设备的新拓扑或新功能可对完整性检查失败的设备的失败或所减少的功能进行补偿。如果网络需要对 M2M 局域网（例如，毛细网）中的设备进行高级的保证，则在检测到该 M2M 局域网中一个或多个设备的完整性发生破坏（breach）或失败之后，M2M 网关可通过其自身或与 M2M 网络域协同或在 M2M 网络域的监督下，将 M2M 局域网中的所有设备或其子集进行隔离。

[0074] 对于情况 4 的连接，在 840，可在 M2M 网关 804 与网络运营商 806 之间进行较精细的完整性验证。在 844，可在 M2M 网关 804 与 M2M 设备 802 之间进行较精细的完整性验证。在 848，可向网络运营商 806 报告 844 的结果。

[0075] 在 852，可在 M2M 设备 802 与 M2M 网关 804 之间确定 / 报告设备运行时间的完整性失败和 / 或执行设备解除登记。在 856，可在 M2M 网关 804 与 M2M 运营商 808 之间报告经过更新的功能和 / 或经过更新的设备列表。

[0076] 情况 1 的设备完整性和登记可包括图 9 中所示的流中的一个或多个。图 9 表示了 M2M 设备 902、网络运营商接入网 904、网络运营商认证服务器 906（可用作平台校验实体）、安全能力 908、AAA/GMAE 910 和其他能力 912。对于情况 1 的连接，M2M 设备 902 可直接连接至 M2M 接入网、网络运营商接入网 904。

[0077] 在 920，M2M 设备 902 可执行完整性检查。在 922，M2M 设备 902 可获取网络运营商接入网 904。在 924，可在网络运营商接入网 904 与网络运营商认证服务器 906 之间建立接入认证（其可包括完整性校验信息）。在 928，可在 M2M 设备 902 与网络运营商接入网 904 之间建立接入认证（其可包括完整性校验信息）。通过使用安全启动进程，M2M 设备 902 可启动，并执行自主校验，或涉及半自主校验中涉及的步骤。作为半自主校验的替换方式，还可执行远程校验过程。

[0078] 如果在 M2M 设备 902 处使用了自主校验，在则设备完整性检查和校验之后，设备可继续获取 M2M 接入网，并尝试向 M2M 接入网连接和登记。

[0079] 如果在 M2M 设备 902 处使用了半自主校验，则设备可执行本地设备完整性检查，随后，在网络获取之后，设备可向 M2M 网络运营商和 / 或 M2M 接入网平台校验实体发送本地设备完整性检查的结果，两种方式都可用。如图 9 的流程图所述，平台校验实体可与运营商的认证服务器（M2M 运营商或接入网络运营商）位于同处，但是，平台校验实体可以是网络中的单独实体。设备完整性检查的结果可以是失败的组件、模块或功能的列表。平台校验实体

可执行设备完整性校验，并继续进行设备认证。

[0080] 如果接入网或 M2M 运营商网络密钥还没有启动，则设备所使用的标识可以是可信平台标识符。如果存在所述密钥的话，则也可额外对该密钥进行使用或单独使用。

[0081] 如果认证成功，则在 930，可继续进行链路和网络会话建立。如果 M2M 接入网认证成功，则在 926，可使用该结果用于到 M2M 系统的单一签名。这样，可在 M2M 系统标识和认证中使用该 M2M 接入网标识和认证结果。对 M2M 接入网的成功认证可表明对另一 M2M 接入网、对 M2M 系统或对 M2M 核、或对 M2M 网络或其他服务提供商所提供的特定服务能力或应用的成功标识和认证。之后可进行启动和 M2M 登记。例如，在 932，M2M 设备 902 可向安全能力 908 发送 M2M 启动请求。在 934，可在 M2M 设备 902 与安全能力 908 之间进行 M2M 安全启动。在 936，可在安全能力 908 与 AAA/GMAE 910 之间进行设备提供（M2M NAI 和根密钥）。在 938，可在 M2M 设备 902 与安全能力 908 之间进行 M2M 登记，该 M2M 登记可包括认证和会话密钥。在 940，可在安全能力 908 与 AAA/GMAE 910 之间进行 M2M 认证。在 942，安全能力 908 可向其他能力 912 提供加密密钥。

[0082] 情况 2 的设备和网关的完整性和登记可包括图 10 中所示的流中的一个或多个。图 10 示出了 M2M 设备 1002、M2M 网关 1004、接入网 1006（例如，与网络运营商相关联）、认证服务器 1008（例如，与网络运营商相关联）、安全能力 1010、AAA/GMAE 1012 和其他能力 1014。

[0083] 在 1020，M2M 设备 1002 可执行本地完整性检查。在 1024，M2M 网关 1004 可执行本地完整性检查。在 1028，可在 M2M 网关 1004 与接入网 1006 之间共享完整性校验信息。在 1032，M2M 设备 902 可获取接入网 1006。在 1036，可在 M2M 设备 1002 与接入网 1006 之间建立接入认证（其可包括完整性校验信息）。在 1040，可在接网 1006 与认证服务器 1008 之间建立接入认证（其可包括完整性校验信息）。在情况 2 的连接中，M2M 设备可通过 M2M 网关连接至 M2M 系统。需要在 M2M 设备和 / 或 M2M 网关处执行完整性检查和校验。该 M2M 网关可执行自主校验或半自主校验。该校验可独立于在设备处进行的自主或半自主校验而进行。

[0084] 网关可使用安全启动进程，并执行本地完整性检查，并且，如果使用了自主校验，则可在本地对本地完整性检查的结果进行校验。如果使用了半自主校验，则网关可向运营商网络中的平台校验实体发送本地完整性检查的结果。该平台校验实体可与运营商的 AAA 服务器，例如 AAA/GMAE 1012，位于同处。在成功地进行了完整性检查和校验之后，网关可启动至准备状态，在该状态中，其可用于向 M2M 设备提供服务。该 M2M 设备可使用安全启动进程，并执行本地完整性检查，如果使用自主校验，则在本地对本地完整性检查的结果进行校验。如果使用半自主校验，则其可通过搜索 M2M 网关，并向运营商网络中的平台校验实体发送结果来获取网络。该 M2M 网关可用作安全网关，并执行接入控制，向 M2M 设备提供对网络的接入，该网络可受限于设备的完整性校验过程。平台校验实体可执行设备完整性校验，并向设备和网关通知结果。如果结果成功，则在 1048，可在 M2M 设备 1002 与接入网 1006 之间建立链路与网络会话，用于启动、向接入网和核心网进行登记和认证的过程。如果 M2M 接入网认证成功，则在 1044，可将该结果用于到 M2M 系统的单一签名。可在 M2M 系统标识和认证中使用该 M2M 接入网标识和认证结果。与 M2M 接入网 1006 的成功认证可表明在另一 M2M 局域网中与 M2M 系统或 M2M 核，或由 M2M 网络或其他服务提供商所提供的一个或多个服务能力或应用的成功标识和认证。之后，可进行启动和 M2M 登记。例如，在 1052，M2M 设备

1002 可向安全能力 1010 产生 M2M 启动请求。在 1056，可在 M2M 设备 1002 与安全能力 1010 之间进行 M2M 安全启动。在 1060，可在安全能力 1010 与 AAA/GMAE 1012 之间进行设备提供（M2M NAI 和根密钥）。在 1064，可在 M2M 设备 1002 与安全能力 1010 之间进行 M2M 登记，该 M2M 登记可包括认证和会话密钥。在 1068，可在安全能力 1010 与 AAA/GMAE 1012 之间进行 M2M 认证。在 1072，安全能力 1010 可向另一能力 1014 提供加密密钥。

[0085] 情况 3 的设备和网关完整性和登记可包括图 11 中所示的流中的一个或多个。图 11 示出了 M2M 设备 1102、M2M 网关 1104、接入网 1106（例如，与网络运营商相关联）、认证服务器 1108（例如，与网络运营商相关联）、安全能力 1110、AAA/GMAE 1112 和其他能力 1114。

[0086] 在 1120，M2M 设备 1102 可执行本地完整性检查。在 1124，M2M 网关 1104 可执行本地完整性检查。在 1128，可在 M2M 网关 1104 和认证服务器 1108 之间进行接入认证，该接入认证可包括完整性校验信息。在 1132，可在 M2M 设备 1102 与 M2M 网关 1104 之间进行毛细网登记和认证，包括设备完整性校验。

[0087] 在 1136，M2M 网关 1104 可获取接入网 1106。在 1140，可在 M2M 网关 1104 与接入网 1106 之间建立接入认证（可包括完整性校验信息）。在 1144，可在接入网 1106 与认证服务器 1108 之间建立接入认证（可包括完整性校验信息）。如果 M2M 接入网认证成功，则可在 1148，将该结果用于向 M2M 系统的单一签名。

[0088] 在情况 3 的连接中，M2M 网关对于网络可用作 M2M 设备。如图 11 所示，可进行以下完整性检查和登记过程中的一个或多个。

[0089] 网关可使用安全启动进程，并进行本地完整性检查，如果使用自主校验，则在本地对本地完整性检查的结果进行校验。如果使用了半自主校验，则网关可向运营商（接入网运营商或 M2M 网络运营商）网络中的平台校验实体发送本地的完整性检查的结果。平台校验实体可与运营商（接入网运营商或 M2M 网络运营商）的 AAA 服务器位于同处。在完整性检查和校验成功之后，网关可启动至准备状态，在该状态中，其可用于向 M2M 设备提供服务。注意，在这种情况下，M2M 对于网络来说表现为 M2M 设备，其与网络按情况 1 的连接进行连接。对于可执行上述用于情况 1 的连接的过程，随后 M2M 网关 1104 可用作 M2M 设备。

[0090] 在 M2M 网关完成了其对 M2M 接入网和 M2M 服务能力的完整性检查和登记之后，该 M2M 网关对于想要与其连接的 M2M 设备是可用的。该 M2M 设备可使用安全启动进程，执行本地完整性检查，如果使用自主校验，则在本地执行对本地完整性检查的结果的验证。如果使用半自主校验，则 M2M 设备可通过搜索 M2M 网关，并向 M2M 网关发送结果来获取网络。该 M2M 网关可用作平台校验实体，并执行设备完整性校验过程，并向设备通知结果。如果结果成功，则在 1152，可在 M2M 网关 1104 与接入网 1106 之间建立链路与网络会话，用于启动、向 M2M 网关进行登记和认证的过程。

[0091] 之后该 M2M 设备可执行启动、向接入网和 / 或核心网进行登记和认证的过程。例如，在 1156，M2M 网关 1104 可向安全能力 1110 做出 M2M 启动请求。在 1160，可在 M2M 网关 1104 与安全能力 1110 之间进行 M2M 安全启动。在 1164，可在安全能力 1110 与 AAA/GMAE 1112 之间进行设备提供（M2M NAI 和根密钥）。在 1068，可在 M2M 网关 1104 与安全能力 1110 之间进行 M2M 登记，可包括认证和会话密钥。在 1172，可在安全能力 1110 与 AAA/GMAE 1112 之间进行 M2M 认证。在 1176，安全能力 1110 可向其他能力 1114 提供加密密钥。

[0092] 在情况 3 的连接中，连接至 M2M 网关的 M2M 设备可以对 M2M 系统不可见。可替换

地，M2M 设备或 M2M 设备的子集作为独立的 M2M 设备对于 M2M 系统是可见的。在这种情况下，M2M 网关可用作网络代理，并执行认证，并对与之相连接的设备、设备子集用作平台完整性校验实体。

[0093] 情况 4 的设备和网关完整性和登记可包括图 12 中所示的流中的一个或多个。图 12 示出了 M2M 设备 1210、M2M 网关 1204、接入网 1206（例如，与网络运营商相关联）、认证服务器 1208（例如，与网络运营商相关联）、安全能力 1210、AAA/GMAE 1212 和其他能力 1214。

[0094] 在 1220，M2M 设备 1202 可执行本地完整性检查。在 1224，M2M 网关 1204 可执行本地完整性检查。在 1228，可在 M2M 网关 1204 与认证服务器 1208 之间进行接入认证，其可包括完整性校验信息。在 1232，可在 M2M 设备 1202 与 M2M 网关 1204 之间进行毛细网登记和认证，其可包括设备完整性校验。

[0095] 在 1236，M2M 网关 1204 可获取接入网 1206。在 1240，可在 M2M 网关 1204 与接入网 1206 之间建立接入认证（其可包括完整性校验信息）。在 1244，可在接入网 1206 与认证服务器 1208 之间进行接入认证（其可包括完整性校验信息）。如果 M2M 接入网认证成功，则可使用该结果在 1248，向 M2M 进行单一签名。

[0096] 在情况 4 的连接中，M2M 网关对设备用作网络的代理。如图 12 所示，可进行以下完整性检查和登记过程中的一者或多者。

[0097] 网关可使用安全启动进程，并进行本地完整性检查，如果使用自主校验，则在本地对本地完整性检查的结果进行校验。如果使用半自主校验，则网关可将本地完整性检查的结果发送至运营商网络（例如，接入网运营商或 M2M 网络运营商）中的平台验证实体。该平台校验实体可与运营商（例如，接入网运营商或 M2M 网络运营商）的 AAA 服务器位于同处。在完整性检查和校验之后，网关可启动至准备状态，在该状态中，其可用于向 M2M 设备提供服务。在 M2M 网关完成了其完整性检查，并向 M2M 接入网登记后，其对于想要对其进行连接的 M2M 设备是可用的。

[0098] 该 M2M 设备可使用安全启动进程，并进行本地完整性检查，如果使用自主校验，则其可在本地对本地完整性检查的结果进行校验。如果使用半自主校验，则其可通过搜索 M2M 网关，并向 M2M 网关发送结果来获取网络。可由 M2M 网关和 M2M 接入网和 M2M 服务层能力的平台校验实体以分离的方式进行设备校验。进行校验的实例方法包括：可以排他地方式在 M2M 网关处进行校验；可由接入网进行校验；可由位于校验实体中的 M2M 服务层能力来进行校验；或由以分离的方式来执行校验的粒度（granularity）的校验实体来进行校验。

[0099] 该 M2M 网关的平台校验实体可进行粗略的校验，之后由更高级的校验实体来进行更精细的校验，或反之亦然。可在 M2M 网关 1204 与认证服务器 1208 之间进行更精细的完整性验证。可在 M2M 设备 1202 与 M2M 网关 1204 之间使用局域网协议消息进行更精细的完整性验证。可结合树状校验来使用这种方法，其中以树状的形式来收集设备完整性检查的结果，该树状结构反映了设备体系结构。可将该树状构造为使得母节点的校验能够指示叶节点模块。可递归地应用这种方式，直到形成了根节点，并且对根节点度量的验证能够校验整个树，并进而校验代表软件模块的叶节点。可根据软件结构来组织子树。该 M2M 网关校验实体可通过检查一组子树的根来执行粗略粒度检查。该信息可馈送至接入运营商或 M2M 运营商的校验实体。网络中的校验实体可评价该结果，并根据所述评价，来决定需要进行更精细的校验。之后，其指示 M2M 网关中的验证实体获得更精细的完整性测试的结果。可在

M2M 网关 1204 与认证服务器 1208 之间交换报告结果。这样，M2M 网关可以分层的方式用作平台校验实体，并表现为网络的代理，并执行设备完整性校验过程，并将结果通知设备。如果结果是成功，则在 1252，设备可在 M2M 网关 1204 与接入网 1206 之间开始链路与网络会话建立的进程，以进行启动、向 M2M 网关 1204 登记和认证的过程。可替换地，设备可开始启动、向接入网和核心网登记和认证的过程。连接至 M2M 网关的 M2M 设备可对 M2M 系统不可见。可替换地，M2M 设备或 M2M 设备子集可作为独立的 M2M 设备对 M2M 系统可见。在这种情况下，M2M 网关用作网络代理，进行认证，并对与其相连接的设备或设备子集用作平台完整性校验实体。

[0100] 该 M2M 网络可以使用由 M2M 网关所促进的分层校验方法来校验大量设备（例如，整个网络范围的设备）以及它们的网关的完整性。

[0101] 该 M2M 网关可首先从与其相连接的设备（例如，所有设备、设备组、设备子集等）收集各个设备的完整性证据（例如哈什）。该完整性证据可以是树状结构的，其中，各个树的根表示各个设备的设备完整性最高级的概要（digest），而其分支表示各个设备的功能或能力，而树的树叶可表示各个文件 / 组件，例如，但不限于，SW 二进制文件、配置文件或硬件组件完整性的各个指示符。

[0102] 通过启动 M2M 网关，或通过启动 M2M 服务器（其可为校验服务器、家庭节点 B 中的平台校验实体（PVE）或 M2M 中的平台校验授权（PVA）），该 M2M 网关可向 M2M 服务器发送有关以下的设备完整性的聚合信息 1）其自身，网关功能，和 2）关于与该 M2M 网关相连接的 M2M 设备（例如，所有设备、设备组、设备子集等）的的完整性的高级简要信息。

[0103] 在从 M2M 网关接收和评价了信息之后，该 M2M 服务器可请求关于之前已经对其完整性进行过报告的 M2M 网关或 M2M 设备的完整性的更详细的信息（例如，所有设备、设备组、设备子集等）。在接收到该请求之后，M2M 网关可以例如 1）向 M2M 服务器发送更详细的信息，该信息有关其自身或其之前所收集并存储的 M2M 设备的完整性，或者，2）收集这种更详细的信息，之后将所述信息发送至 M2M 服务器。可从树状或树型结构的数据获得该“更详细的信息”，其中，树根可表示整个子网的完整性的非常高级的概要，该子网包括 M2M 网关和与之相连接的 M2M 设备（例如，所有设备、设备组、设备子集等），低级节点和叶可表示关于设备（例如其功能）的较低层的更详细的信息。图 13 表示分层校验的示例场景。大三角形 1310 可表示树状或树类结构，其中该三角形的顶端表示完整性数据的非常高级的概要版本，其表示 M2M 网关 1300 所协调的整个子网的整体健康状况。较大的树可将一个或多个较小的三角形 1315 包括为其一部分，每个较小的三角形都表示关于设备 1330 中的一个或多个的完整性信息，其中该设备 1330 包括由 M2M 网关 1300 所协调的子网。

[0104] 并且，M2M 网关 1300 可根据类型、级别或其他描述符来对所连接的设备进行分组，并可能的向其完整性树提供组证书。这在图 13 中进行了表示，其中较小的三角形 1370 中具有证书。使用这种可信证书可促进多网络运营商（MNO）网络 1320 对所报告的完整性值具有更大的信任。

[0105] 上述场景还可用于，或包括端对端（P2P）方法，其中，M2M 设备相互之间或在具有验证节点的簇（cluster）中（其中可存在专用的校验节点）、或在 ad-hoc 节点中（其中任何节点都可承担校验节点的角色）交换并证明树或树型完整性证明数据结构。

[0106] 网络和应用域中服务能力（SC）的服务能力可提供以下中的一者或多者 :密钥管

理、认证和会话密钥管理或设备完整性验证。

[0107] 密钥管理可包括怎样在用于认证的设备中通过启动安全密钥(例如,预先共享的安全密钥、证书等)的方式来管理安全密钥。

[0108] 可将认证和会话密钥管理配置为执行以下中的一者或多者:通过认证的服务层登记;在 M2M 设备 / M2M 网关与 SC 之间的服务会话密钥管理;在提供服务之前的认证应用;向消息能力传递经过协商的会话密钥,从而执行(由消息能力)对与 M2M 设备和 M2M 网关所交换的数据进行加密 / 完整性保护;或者,如果应用需要隧道安全,建立来自 M2M 网关安全隧道会话(例如,在家庭网关和服务功能实体之间用于消息的隧道)。可将设备完整性验证配置为校验设备或网关的完整性。

[0109] 可将该 M2M 设备或 M2M 网关中的 SC 配置为执行以下中的一者或多者:以启动用于认证的设备中的安全密钥(例如,预先共享的安全密钥或证书)的方式来管理安全密钥;如果应用需要的话,在建立会话之前进行认证;与会话安全相关的功能,例如信令消息的流量加密和完整性保护;(用于能够适用的设备 / 网关)对设备(或网关)的完整性进行测量、验证和 / 或报告;安全时间同步的支持过程;协商和使用可用的安全特定服务等级属性;支持故障恢复机制;或者,支持 M2M 设备对 M2M 核的接入控制。

[0110] 虽然上面以特定组合的方式描述了特征和元素,但是每个特征或元素都可在没有其他特征和元素的情况下单独使用,或与其他特征和元素进行各种组合或不进行组合。此处所述的方法或流程可在计算机程序、软件或结合至计算机可读存储介质中的固件中实现,以由通用目的计算机或处理器执行。计算机可读存储介质的例子包括只读存储器(ROM)、随机存储存储器(RAM)、寄存器、缓存、半导体存储设备、例如内置磁盘和可移动磁盘的磁介质、磁光介质和光介质(例如 CD-ROM 盘和数字多用途盘(DVD))。

[0111] 合适的处理器包括,例如,通用目的处理器、专门目的处理器、常规处理器、数字信号处理器(DSP)、多个微处理器、与 DSP 核相关联的一个或多个微处理器、控制器、微控制器、特定用途集成电路(ASIC)、现场可编程门阵列(FPGA)电路、任何其他类型的集成电路(IC)和 / 或状态机。

[0112] 可使用与软件相关联的处理器来实现射频收发信机,以用于无线发射接收单元(WTRU)、用户设备(UE)、终端、基站、无线电网络控制器(RNC)或任何主机计算机。WTRU 可与模块相结合使用,在硬件和 / 或软件中实现,例如照相机、视频照相模块、视频电话、扬声电话、振动设备、扬声器、麦克风、电视收发机、免提电话、键盘、蓝牙®模块、调频(FM)无线电单元、液晶显示(LCD)显示单元、有机发光二极管(OLED)显示单元、数字音乐播放器、媒体播放器、视频游戏机模块、互联网浏览器和或任何无线局域网(WLAN)或超宽带(UWB)模块。

[0113] 下面所公开的是可与上述所公开的主题相结合或作为这些主题的一部分的系统、方法和手段。

[0114] 图 14 表示 M2M 体系结构示例。该结构图包括在机器对机器(M2M)网络和 M2M 设备 / 网关实体上的 M2M 服务能力 1430。图 14 包括 M2M 设备 / M2M 网关 1410、能力级别接口 1460、M2M 服务能力 1430、M2M 应用 1420、资源接口 1490、核心网 A 1440 和核心网 B 1450。该 M2M 设备 / M2M 网关 1410 可包括 M2M 应用 1412、M2M 能力 1414 和通信模块 1416。该 M2M 服务能力 1430 可包括能力 C1、C2、C3、C4 和 C5,以及通用的 M2M 应用使能能力 1470。

[0115] 图 15 表示 M2M 网络层的 M2M 服务能力的内部功能性体系结构示例。如图所示,

图 15 可包括图 14 的组件。在图 15 中，M2M 网络服务层可包括一个或多个能力，包括：通用消息传递（GM）60；可达性（reachability）、寻址和设备应用储藏库（repository）（RADAR）30；网络和通信服务选择（NCSS）20；M2M 设备和 M2M 网关管理（MDGM）10；历史化和数据保留（retention）（HDR）70；通用 M2M 应用使能（GMAE）1470；安全能力（SC）50；或事务管理（TM）40。

[0116] 在情况 A 的连接中，从服务能力的角度来看，M2M 设备可直接连接至 M2M 接入网。这样，可认为此处所述的连接情况 1 和 2 是连接情况 A 的示例。如果存在 M2M 网关，其在连接至外围设备（M2M 网络通过毛细网不知道该外围设备）的同时，还连接至 M2M 接入网，那么，该 M2M 网关可被认为是直接连接至 M2M 接入网的 M2M 设备，例如，实现了情况 1 的连接。

[0117] 在情况 B 的连接中，M2M 网关可用作网络代理，其代表 M2M 网络和应用域，对与其相连接的 M2M 设备执行认证、授权、登记、设备管理和提供，并且还执行应用。在情况 B 的连接中，M2M 网关可决定将 M2M 设备上的应用所产生的服务层请求在本地进行路由或将其路由至 M2M 网络和应用域。此处所述的连接情况 3 和 4 可以是连接情况 B 的示例。

[0118] 下面更详细地描述用于 M2M 网关的服务能力的新体系结构和特定功能。

[0119] 图 16A 和 16B 表示了 M2M 网关及其接口的功能体系结构示例。图 16A 和 16B 包括网关 M2M 服务能力 1610、网络 M2M 服务能力 1650、M2M 应用 1612、M2M 应用 1652、能力级别接口 1615、能力级别接口 1655、M2M 设备 1630、毛细网 1635 和毛细网 1675，以及此处所述的其他组件。所述服务能力可包括 gGMAE 1620、gGM 26、gMDGM 21、gNCSS 22、gRADAR 23 和 gSC 24。这些能力中每一个都可认为是 M2M 网关的能力，其分别对应于，并用作 M2M 核的能力 GMAE 1650、GM 65、MDGM 61、NCSS 62、RADAR63 和 SC 64 的代理。

[0120] 下面更详细地描述适用于被用作 M2M 网络的代理的 M2M 网关的这些 M2M 网关能力中的每一个的高级功能。

[0121] 该 gGMAE 1620 是用作网络和应用域（NAD）的 GMAE 1660 的代理的 M2M 网关的能力，其可提供 1）用于连接至网络代理 M2M 网关的 M2M 设备的应用，以及 2）用于 M2M 网关自身的应用。

[0122] 该 gGM 26 是用作 NAD 的 GM 65 的代理的 M2M 网关能力，并可提供用来在以下一个或多个对象之间传输消息的能力：M2M 设备、网络代理 M2M 网关、位于网络代理 M2M 网关内的代理服务能力、和 gGMAE 1620 所实现的 M2M 应用、和 NAD 的服务能力、和位于 NAD 内的 M2M 应用。

[0123] 该 gMDGM 21 是用作 NAD 的 MDGM 61 的代理的 M2M 网关能力，并可同时为与其相连接的 M2M 设备以及 M2M 网关自身的所有能力和接口提供管理功能，例如配置管理（CM）、性能管理（PM）和错误管理（FM）。

[0124] 该 gNCSS 22 是用作 NAD 的 NCSS 62 的代理的 M2M 网关能力，并可为与其相连接的 M2M 设备以及 M2M 网关自身提供通信和网络服务选择能力。

[0125] 该 gRADAR 23 是用作 NAD 的 RADAR 63 的代理的 M2M 网关能力。其功能包括以下描述。

[0126] 该 gSC 24 是用作 NAD 的 SC 64 的代理的 M2M 网关能力。

[0127] 除了在 NAD 中具有对应部分的能力以外，还可包括称作 gMMC 25 的 M2M 网关能力，其可用于管理服务和应用域中的各个 M2M 网关之间的 M2M 设备移动性。在上述图 15 中未

示出功能 gMMC 25，但是仍然可认为其位于网络代理网关中。

[0128] 网关服务能力可包括多个(例如三个)子能力，由“DG”、“G”和“GN”来表示，如图 16A 所示。对于功能“gX”，“gX_DG”可表示负责与连接至网关的 M2M 设备进行交互的子能力，“gX_G”可表示负责网关的自主功能的子能力，其可作为“gX”功能的一部分，而“gX_GN”可表示负责与 M2M 服务核进行交互的子能力。

[0129] 除了这些能力以外，如图 16A 和 16B 所示，网络代理 M2M 网关的体系结构可包括上述能力之间的多个接口、以及从网络代理 M2M 网关向 M2M 设备或 M2M 网络及其各种功能的接口。在图 16A 和 16B 中表示了接口名称示例。

[0130] 以下中的一者或多者可用于网关通用 M2M 应用使能(gGMAE)能力。

[0131] 该 M2M 应用可位于 M2M 设备、M2M 网关或 M2M 网络和应用域之中。

[0132] 针对基于网络的 GMAE 1660，gGMAE (例如 gGMAE 1620)的功能可包括以下中的一者或多者。

[0133] 该 gGMAE 可通过单个接口(例如图 16A 中所示的 gIa)来暴露(expose)在 M2M 核的服务能力中和在 M2M 网关的网络代理服务能力中实施的功能。其可隐藏网关服务能力拓扑，从而可将 M2M 应用为了使用 M2M 网关的不同网络代理服务能力而需要的信息限制为 gGMAE 能力的地址。其还可使 M2M 应用向网关服务能力进行登记。

[0134] 还可将该 gGMAE 配置为在允许 M2M 应用接入特定能力集合之前，先进行认证和授权。M2M 应用有资格接入的能力集合可在 M2M 应用提供商与运行服务能力的提供商之间假设具有预先的协定。在这种情况下，可由同一个实体来运行该 M2M 应用和所述服务能力，这样可免于认证要求。还可在将接口 gIa 上的特定请求路由至其他能力之前，检查其是否有效。如果该请求无效，则可向 M2M 应用报告错误。

[0135] 该 gGMAE 可进一步被配置为在 M2M 应用与代理服务能力中的能力之间进行路由。可将该路由定义为，例如当进行负责均衡时，将特定请求发送至特定能力，或发送至该能力的实例的机制。其可在不同代理服务能力之间进行路由。并且，其可产生关于针对服务能力的使用的计费纪录。

[0136] 此外，可将 M2M 网关中的 gGMAE 能力配置为向 M2M NAD 中的 GMAE 能力报告对 M2M 设备进行登记、认证和授权的状态和 / 或结果。可由以下中的一者或多者来执行上述报告：

[0137] 通过其自身的启动，例如周期性地使用计时器，该计时器可由设备在本地提供和 / 或通过外部定时同步来提供。

[0138] 响应于来自 M2M 网络的 GMAE 能力的命令(即，请求式)。

[0139] 通过其自身启动向 NAD 的 GMAE 发送请求，并之后从该 NAD 的 GMAE 接收响应。

[0140] 可将以下中的一者或多者用于可达性、寻址和设备应用储存库能力。

[0141] 可将 M2M 网关中的 RADAR 能力(例如 gRADAR 23)配置为根据 M2M 网络和应用域的策略和 / 或应用来显示或隐藏潜在的毛细网拓扑、从 M2M 网络和应用域中的服务能力进行寻址和路由的能力。其还可通过中继 M2M 应用以及服务层消息和数据，来支持 M2M 网关之间的 M2M 设备移动性。

[0142] 可将 M2M 网关中的 RADAR 能力(例如 gRADAR 23)进一步配置为通过将 M2M 设备的 M2M 设备应用登记信息存储在设备应用储存库中，并保持该信息为最新的，来提供维护网关设备应用储存库(gDAR)的能力。此外，其还可具有向网络和应用域中的认证和授权实体提

供查询接口的能力，从而使其检索 M2M 设备应用登记信息。此外，其还可具有一旦接收到请求便将该信息提供给位于网络和应用域中的实体的能力，例如，假设该发出请求的实体被认证和授权能够进行该查询。

[0143] 可将（NAD 的）gRADAR 23 和 RADAR 63 配置为提供以下中的一者或多者：1）云状的基于网络的应用执行；2）可下载的，类似应用存储的应用储存库，或 3）以与颁发 DRM 授权相似的方式，来登记和授权 / 激活对设备上所提供的应用的使用。

[0144] 可将以下中的一者或多者用于网络和通信服务选择（NCSS）能力。

[0145] 该 NCSS 能力，例如 NCSS 62，可包括以下能力中的一者或多者。

[0146] 可将该 NCSS 能力配置为对 M2M 应用隐藏网络地址使用。当可通过多个网络经由多个订阅访问 M2M 设备或 M2M 网关时，其可提供网络选择。此外，当 M2M 设备或 M2M 网关具有多个网络地址时，其可提供通信服务选择。

[0147] 此外，可将 NCSS 能力配置为为了网络和通信服务选择的目的，而考虑所请求的服务等级。并且，其可在通信失败后，例如使用第一个所选的网络或通信服务来提供替代的网络或通信服务选择。

[0148] 可将 M2M 网关中的 NCSS 能力，例如 gNCSS 22，配置为对 M2M 应用和服务层隐藏接入网使用。当有多个接入网可用时，其可提供接入网选择。

[0149] 可将该 gNCSS 进一步配置为为了网络和通信服务选择的目的，考虑所请求的服务等级。并且，其可在通信失败之后，例如使用第一个所选的网络或通信服务来提供替代的网络或通信服务选择。

[0150] 可将以下中的一者或多者应用于安全能力（SC）。

[0151] 可将网络和应用域的服务能力中的 SC，例如 SC 64，配置为提供以下中的一者或多者：密钥管理、认证和会话密钥管理、或设备完整性校验。

[0152] 密钥管理可包括在用于认证的设备中使用安全密钥（例如，预先共享的安全密钥、证书等）的启动来管理安全密钥。其还可包括从应用获得提供信息，并按需要通知运营商网络。

[0153] 认证和会话密钥管理可包括通过认证执行服务层登记。其还可包括在 M2M 设备 / M2M 网关和 SC 之间进行服务会话密钥管理。其还可包括在提供服务之前，对应用进行认证。

[0154] 认证和会话密钥管理可进一步包括与 AAA 服务器进行交互，从而获得执行 M2M 设备应用或 M2M 网关应用认证和会话密钥管理所需的认证数据。该 SC 可用作 AAA 术语中的“认证器”。其还可向消息能力发送经过协商的会话密钥，从而对与 M2M 设备和 M2M 网关所交换的数据进行（通过消息能力）加密和完整性保护。

[0155] 认证和会话密钥管理可进一步包括：如果应用需要隧道安全，（例如，家庭网关与服务能力实体之间的隧道：发送消息），则可建立来自 M2M 网关和服务的安全隧道会话。

[0156] 设备完整性校验可涉及 M2M 网络针对支持设备完整性校验的 M2M 设备和网关来校验设备或网关的完整性。此外，M2M 网络还可触发验证后的操作，例如接入控制。

[0157] 还可将 M2M 设备或 M2M 网关中的 SC 配置为通过启动用于认证的设备中的安全密钥（例如，预先共享的安全密钥、证书等）来管理安全密钥。其还可从应用获得提供信息，并按需要通知运营商网络。其可进一步配置为（例如在应用需要时）在建立会话前进行认证。

[0158] 可进一步将 M2M 设备或 M2M 网关中的 SC 配置为执行与会话安全相关的能力，例如

为信令消息进行流量加密和完整性保护。同时，(对于可用的设备 / 网关)，其可对设备或网关的完整性进行验证和 / 或报告。此外，其可(对于可用的设备 / 网关)支持安全定时同步过程。

[0159] 可进一步将 M2M 设备或 M2M 网关中的 SC 配置为协商和使用可适用的安全特定服务等级属性。并且，受 M2M 运营商策略的限制，如果能够进行完整性验证的 M2M 设备在该过程中失败，则其可拒绝任何 M2M 设备对网络和应用域的访问。

[0160] 除上述能力以外，可将基于 NAD 的 SC 配置为启动 MDGM 能力，以更新 M2M 设备的固件或软件。

[0161] 此外，对于网络代理 M2M 网关的网关安全能力(gSC)来说，可将 SC 配置为管理安全密钥，以用于 M2M 设备或 M2M 应用。

[0162] 该 SC 可对 M2M 设备进行服务级别认证(作为 NAD 中 SC 的认证功能的代理)，从而支持服务层和应用登记。

[0163] 该 SC 可基于单个 M2M 设备或设备组向 NAD 中的安全能力报告上述认证的结果。该 SC 可对 NAD 中的 SC 执行对自身的服务级别认证。

[0164] 如果应用需要隧道安全的话，该 SC 可从 M2M 网关(向 M2M 设备或 M2M 核)建立并连网(interwork)安全隧道会话。此外，SC 可代表 NAD 的 SC 对 M2M 设备的完整性进行验证和校验。

[0165] 可进一步将该 SC 配置为基于单个 M2M 设备或设备组，将所述验证和校验的结果报告给 NAD 中的安全能力。此外，SC 可执行过程，以向 NAD 中的安全能力证明其自身的完整性。此外，SC 可为 M2M 设备触发验证后的操作，例如接入控制和修复，其中包括启动 gMDGM 能力或 MDGM (NAD 中的)，以更新 M2M 设备的固件或软件。

[0166] 可进一步将该 SC 配置为执行以下功能中的一者或多者 1)作为对 M2MNAD 能力所产生的命令的响应，2)作为在用于该操作的自主地从 M2M 网关所产生的请求之后，从 M2M NAD 所接收的命令的响应，或 3) 自主地对能力启动操作，从而之后 gSC 向 M2M NAD 的能力报告该操作的过程或结果。

[0167] 虽然上面以特定组合的方式描述了特征和元素，但是每个特征或元素都可在没有其他特征和元素的情况下单独使用，或与其他特征和元素进行各种组合或不进行组合。此处所述的方法或流程可在结合至计算机可读存储介质中的计算机程序、软件或固件中实现，以由通用目的计算机或处理器执行。计算机可读存储介质的例子包括只读存储器(ROM)、随机存储存储器(RAM)、寄存器、缓存、半导体存储设备、例如内置磁盘和可移动磁盘的磁介质、磁光介质和光介质(例如 CD-ROM 盘和数字多用途盘(DVD))。

[0168] 合适的处理器包括，例如，通用目的处理器、专门目的处理器、常规处理器、数字信号处理器(DSP)、多个微处理器、与 DSP 核相关联的一个或多个微处理器、控制器、微控制器、特定用途集成电路(ASIC)、现场可编程门阵列(FPGA) 电路、任何其他类型的集成电路(IC) 和 / 或状态机。

[0169] 可使用与软件相关联的处理器来实现射频收发信机，以用于无线发射接收单元(WTRU)、用户设备(UE)、终端、基站、无线电网络控制器(RNC)或任何主机计算机。WTRU 可与模块相结合使用，在硬件和 / 或软件中实现，例如照相机、视频照相模块、视频电话、扬声电话、振动设备、扬声器、麦克风、电视收发机、免提电话、键盘、蓝牙®模块、调频(FM) 无线电

单元、液晶显示(LCD)显示单元、有机发光二极管(OLED)显示单元、数字音乐播放器、媒体播放器、视频游戏机模块、互联网浏览器和或任何无线局域网(WLAN)或超宽带(UWB)模块。

[0170] 虽然上面以特定组合的方式描述了特征和元素,但是本领域技术人员应该理解到,每个特征或元素都可在没有其他特征和元素的情况下单独使用,或与其他特征和元素进行各种组合或不进行组合。此处所述的方法可在结合至计算机可读介质中的计算机程序、软件或固件中实现,以由计算机或处理器执行。计算机可读介质包括电子信号(经由有线或无线连接传送)和计算机可读存储介质。计算机可读存储介质的例子包括,但不限于,只读存储器(ROM)、随机存储存储器(RAM)、寄存器、缓存、半导体存储设备、例如内置磁盘和可移动磁盘的磁介质、磁光介质和光介质(例如 CD-ROM 盘和数字多用途盘(DVD))。可使用与软件相关的处理器来实现 WTRU、UE、终端、基站、RNC 或任何主机计算机中所使用的射频收发信机。

[0171] 图 17A 是能够实施一种或多种公开实施方式的示例通信系统 1700 的示意图。通信系统 1700 可以是向多个无线用户提供诸如语音、数据、视频、消息、广播等内容的多路接入系统。通信系统 1700 可以使得多个无线用户能够通过对包括无线带宽在内的系统资源进行共享来接入此类内容。例如,通信系统 1700 可以使用一种或多种信道接入方法,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。

[0172] 如图 17A 所示,通信系统 1700 可以包括无线发射接收单元(WTRU)1702a、1702b、1702c、1702d、无线电接入网络(RAN)1704、核心网 1706、公共交换电话网(PSTN)1708、因特网 1710、以及其它网络 1712,但是应认识到公开的实施方式可以涉及任何数目的 WTRU、基站、网络、和/或网络元件。WTRU 1702a、1702b、1702c、1702d 中的每一个可以是被配置为在无线环境中进行操作和/或通信的任何类型的设备。举例来说,WTRU1702a、1702b、1702c、1702d 可以被配置为发射和/或接收无线电信号,并且可以包括用户设备(UE)、移动站、固定或移动订户单元、寻呼机、蜂窝电话、个人数字助理(PDA)、智能电话、膝上电脑、上网本、个人计算机、无线传感器、消费电子设备等等。

[0173] 通信系统 1700 还可以包括基站 1714a 和基站 1714b。基站 1714a、1714b 中的每一个可以是被配置为与 WTRU 1702a、1702b、1702c、1702d 中的至少一者无线对接的任何类型的设备,以促进到诸如核心网 1706、因特网 1710、和/或网络 1712 的一个或多个通信网络的接入。举例来说,基站 1714a、1714b 可以是基站收发站(BTS)、节点 B、e 节点 B、家庭节点 B、家庭 e 节点 B、站点控制器、接入点(AP)、无线路由器等。虽然基站 1714a、1714b 每个都被描绘为单个元件,但应认识到基站 1714a、1714b 可以包括任何数目的互连基站和/或网络元件。

[0174] 基站 1714a 可以是 RAN 1704 的一部分,其还可以包括其它基站和/或网络元件(未示出),诸如基站控制器(BSC)、无线电网络控制器(RNC)、中继节点等等。基站 1714a 和/或基站 1714b 可以被配置为在可被称为小区(未示出)的特定地理区域内发射和/或接收无线信号。所述小区还可以被划分成小区扇区。例如,与基站 1714a 相关联的小区可以被划分成三个扇区。因此,在一个实施方式中,基站 1714a 可以包括三个收发信机,即小区的每个扇区一个。在另一实施方式中,基站 1714a 可以使用多输入多输出(MIMO)技术,因此,可以针对小区的每个扇区使用多个收发信机。

[0175] 基站 1714a、1714b 可以通过空中接口 1716 与 WTRU 1702a、1702b、1702c、1702d 中的一个或多个通信，所述空中接口 1716 可以是任何适当的无线通信链路(例如射频(RF)、微波、红外线(IR)、紫外线(UV)、可见光等等)。可以使用任何适当的无线电接入技术(RAT)来建立空中接口 1716。

[0176] 更具体而言，如上所述，通信系统 1700 可以是多路接入系统且可以采用一种或多种信道接入方案，诸如 CDMA、TDMA、FDMA、OFDMA、SC-FDMA 等等。例如，RAN 1704 中的基站 1714a 和 WTRU 1702a、1702b、1702c 可以实现诸如通用移动通信系统(UMTS)陆地无线电接入(UTRA)的无线电技术，其中该无线电技术可以使用宽带 CDMA (WCDMA)来建立空中接口 1716。WCDMA 可以包括诸如高速分组接入(HSPA)和 / 或演进型 HSPA (HSPA+)的通信协议。HSPA 可以包括高速下行链路分组接入(HSDPA)和 / 或高速上行链路分组接入(HSUPA)。

[0177] 在另一实施方式中，基站 1714a 和 WTRU 1702a、1702b、1702c 可以实现诸如演进型 UMTS 陆地无线电接入(E-UTRA)的无线电技术，其中该无线电技术可以使用长期演进(LTE)和 / 或高级 LTE (LTE-A)来建立空中接口 1716。

[0178] 在其它实施方式中，基站 1714a 和 WTRU 1702a、1702b、1702c 可以实现诸如 IEEE 802.16 (即微波接入全球互通(WiMAX))、CDMA2000、CDMA20001X、CDMA2000EV-DO、临时标准 2000 (IS-2000)、临时标准 95 (IS-95)、临时标准 856 (IS-856)、全球移动通信系统(GSM)、GSM 演进增强型数据速率(EDGE)、GSM EDGE (GERAN)等的无线电技术。

[0179] 举例来讲，图 17A 中的基站 1714b 可以是无线路由器、家庭节点 B、家庭 e 节点 B、或接入点，并且可以利用任何适当 RAT 来促进诸如营业场所、家庭、车辆、校园等局部区域中的无线连接。在一个实施方式中，基站 1714b 和 WTRU 1702c、1702d 可以实现诸如 IEEE 802.11 的无线电技术以建立无线局域网(WLAN)。在另一实施方式中，基站 1714b 和 WTRU 1702c、1702d 可以实现诸如 IEEE 802.15 的无线电技术以建立无线个域网(WPAN)。在另一实施方式中，基站 1714b 和 WTRU 1702c、1702d 可以利用蜂窝式 RAT(例如 WCDMA、CDMA2000、GSM、LTE、LTE-A 等)以建立微微小区或毫微微小区。如图 17A 所示，基站 1714b 可以具有到因特网 1710 的直接连接。因此，可以不要求基站 1714b 经由核心网络 1706 接入因特网 1710。

[0180] RAN 1704 可以与核心网络 1706 通信，核心网络 1706 可以是被配置为向 WTRU 1702a、1702b、1702c、1702d 中的一个或多个提供语音、数据、应用程序、和 / 或网际协议语音(VoIP)服务的任何类型的网络。例如，核心网络 1706 可以提供呼叫控制、计费服务、基于移动定位的服务、预付费呼叫、因特网连接、视频分发等，和 / 或执行诸如用户认证等高级安全功能。虽然图 17A 未示出，但应认识到 RAN 1704 和 / 或核心网络 1706 可以与采用与 RAN 1704 相同的 RAT 或不同 RAT 的其它 RAN 进行直接或间接通信。例如，除连接到可以利用 E-UTRA 无线电技术的 RAN 1704 之外，核心网络 1706 还可以与采用 GSM 无线电技术的另一 RAN (未示出)通信。

[0181] 核心网络 1706 还可以充当用于 WTRU 1702a、1702b、1702c、1702d 接入 PSTN 1708、因特网 1710、和 / 或其它网络 1712 的网关。PSTN 1708 可以包括提供简单老式电话服务(POTS)的电路交换电话网。因特网 1710 可以包括使用公共通信协议的互连计算机网络和设备的全局系统，所述公共通信协议诸如传输控制协议(TCP) / 网际协议(IP)因特网协议组中的 TCP、用户数据报协议(UDP)和 IP。网络 1712 可以包括由其它服务提供商所有和 /

或操作的有线或无线通信网络。例如，网络 1712 可以包括连接到可以采用与 RAN 1704 相同的 RAT 或不同 RAT 的一个或多个 RAN 的另一核心网络。

[0182] 通信系统 1700 中的某些或全部 WTRU 1702a、1702b、1702c、1702d 可以包括多模式能力，即 WTRU 1702a、1702b、1702c、1702d 可以包括用于通过不同的无线链路与不同的无线网络通信的多个收发信机。例如，图 17A 所示的 WTRU 1702c 可以被配置为与采用蜂窝式无线电技术的基站 1714a 通信，且与可以采用 IEEE 802 无线电技术的基站 1714b 通信。

[0183] 图 17B 是示例性 WTRU 1702 的系统图。如图 17B 所示，WTRU 1702 可以包括处理器 1718、收发信机 1720、发射 / 接收元件 1722、扬声器 / 扩音器 1724、小键盘 1726、显示器 / 触摸屏 1728、不可移除存储器 1730、可移除存储器 1732、电源 1734、全球定位系统（GPS）芯片组 1736、及其它外围设备 1738。应认识到 WTRU 1702 可以在保持与实施方式一致的同时，包括前述元件的任何子组合。

[0184] 处理器 1718 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、任何其它类型的集成电路（IC）、状态机等等。处理器 1718 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 WTRU 能够在无线环境中操作的任何其它功能。处理器 1718 可以是耦合到收发信机 1720，收发信机 1720 可以耦合到发射 / 接收元件 1722。虽然图 17B 将处理器 1718 和收发信机 1720 描绘为单独的元件，但应认识到处理器 1718 和收发信机 1720 可以被一起集成在电子组件或芯片中。

[0185] 发射 / 接收元件 1722 可以被配置为通过空中接口 1716 向基站（例如基站 1714）发射信号或从基站（例如基站 1714）接收信号。例如，在一个实施方式中，发射 / 接收元件 1722 可以被配置为发射和 / 或接收 RF 信号的天线。在另一实施方式中，发射 / 接收元件 1722 可以被配置为发射和 / 或接收例如 IR、UV、或可见光信号的发射体 / 检测器。在另一实施方式中，发射 / 接收元件 1722 可以被配置为发射和接收 RF 和光信号两者。应认识到发射 / 接收元件 1722 可以被配置为发射和 / 或接收无线信号的任何组合。

[0186] 另外，虽然发射 / 接收元件 1722 在图 17B 中被描绘为单个元件，但 WTRU1702 可以包括任何数目的发射 / 接收元件 1722。更具体而言，WTRU 1702 可以采用 MIMO 技术。因此，在一个实施方式中，WTRU 1702 可以包括用于通过空中接口 1716 来发射和接收无线信号的两个或更多发射 / 接收元件 1722（例如多个天线）。

[0187] 收发信机 1720 可以被配置为调制将由发射 / 接收元件 1722 发射的信号并将由发射 / 接收元件 1722 接收到的信号解调。如上所述，WTRU 1702 可以具有多模式能力。因此，例如，收发信机 1720 可以包括用于使得 WTRU 1702 能够经由诸如 UTRA 和 IEEE 802.11 等多个 RAT 通信的多个收发信机。

[0188] WTRU 1702 的处理器 1718 可以耦合到扬声器 / 扩音器 1724、小键盘 1726、和 / 或显示器 / 触控板 1728（例如液晶显示器（LCD）显示单元或有机发光二极管（OLED）显示单元），并且可以从这些组件接收用户输入数据。处理器 1718 还可以向扬声器 / 扩音器 1724、小键盘 1726、和 / 或显示器 / 触控板 1728 输出用户数据。另外，处理器 1718 可以访问来自诸如不可移除存储器 1730 和 / 或可移除存储器 1732 等任何类型的适当存储器的信息并能够将数据存储在这些存储器中。不可移除存储器 1730 可以包括随机存取存储器（RAM）、

只读存储器(ROM)、硬盘、或任何其它类型的存储器存储设备。可移除存储器1732可以包括订户身份模块(SIM)卡、记忆棒、安全数字(SD)存储卡等。在其它实施方式中,处理器1718可以访问来自在物理上位于WTRU 1702上(诸如在服务器或家用计算机(未示出))的存储器的信息并将数据存储在该存储器中。

[0189] 处理器1718可以从电源1734接收功率,并且可以被配置为向WTRU1702分配功率和/或控制功率。电源1734可以是用于对WTRU 1702供电的任何适当设备。例如,电源1734可以包括一个或多个干电池(例如镍镉(NiCd)、镍锌铁氧体(NiZn)、镍金属氢化物(NiMH)、锂离子(Li)等等)、太阳能电池、燃料电池等等。

[0190] 处理器1718还可以耦合到GPS芯片组1736,GPS芯片组1736可以被配置为提供关于WTRU 1702的当前位置的位置信息(例如,经度和纬度)。除来自GPS芯片组1736的信息之外或作为其替代,WTRU 1702可以通过空中接口1716从基站(例如基站1714a、1714b)接收位置信息和/或基于从两个或更多附近基站接收到信号的时刻来确定其位置。应认识到WTRU 1702可以在保持与实施方式一致的同时,通过任何适当的位置确定方法来获取位置信息。

[0191] 处理器1718还可以耦合到其它外围设备1738,外围设备1738可以包括提供附加特征、功能和/或有线或无线连接的软件和/或硬件模块。例如,外围设备1738可以包括加速计、电子指南针、卫星收发信机、数字式照相机(用于拍照或视频)、通用串行总线(USB)端口、振动设备、电视收发信机、免提耳麦、Bluetooth®模块、调频(FM)无线电单元、数字音乐播放器、媒体播放器、视频游戏机模块、因特网浏览器等等。

[0192] 图17C是根据一种实施方式的RAN 1704和核心网1706的系统结构图。如上所述,RAN 1704可使用UTRA无线电技术通过空中接口1716来与WTRU 1702a、1702b、1702c进行通信。该RAN 1704还可与核心网1706进行通信。如图17C所示,RAN 1704可包括节点B 1740a、1740b、1740c,其中每个可包含一个或多个收发信机,用于通过空中接口1716与WTRU1702a、1702b、1702c进行通信。节点B 1740a、1740b、1740c中的每一个可与RAN 1704中的特定小区(未示出)相关联。该RAN 1704还可包括RNC1742a、1742b。应当理解,RAN 1704可包括任何数量的节点B和RNC,并仍与实施方式保持一致。

[0193] 如图17C所示,节点B 1740a、1740b可与RNC 1742a进行通信。此外,节点B 1740c可与RNC 1742b进行通信。节点B 1740a、1740b、1740c可经由Iub接口与各个RNC 1742a、1742b进行通信。该RNC 1742a、1742b可通过Iur接口相互通信。RNC 1742a、1742b中每一个都可被配置为控制所连接的各个节点B 1740a、1740b、1740c。此外,可将RNC 1742a、1742b的每一个配置为实现或支持其他功能,例如外环功率控制、负载控制、允许控制、分组调度、切换控制、宏分集、安全功能、数据加密等。

[0194] 图17C中所示的核心网1706可包括媒体网关(MGW)1744、移动交换中心(MSC)1746、服务GPRS支持节点(SGSN)1748和/或网关GPRS支持节点(GGSN)1750。虽然将上述各个组件表示为核心网1706的一部分,但是应当理解,任何一个组件都可由核心网运营商以外的实体所拥有和/或操作。

[0195] RAN 1704中的RNC 1742a可通过IuCS接口连接至核心网1706中的MSC 1746。可将MSC 1746连接至MGW 1744。该MSC 1746和MGW 1744可向WTRU 1702a、1702b、1702c提供到电路交换网络(例如PSTN 1708)的接入,从而促进WTRU 1702a、1702b、1702c与传统陆

地线通信设备之间的通信。

[0196] 还可将 RAN 1704 中的 RNC 1742a 通过 IuPS 接口连接至核心网 1706 中的 SGSN 1748。该 SGSN 1748 可连接至 GGSN 1750。该 SGSN 1748 和 GGSN1750 可向 WTRU 1702a、1702b、1702c 提供到分组交换网络(例如互联网 1710)的接入,从而促进 WTRU 1702a、1702b、1702c 与 IP 使能设备之间的通信。

[0197] 如上所述,还可将核心网 1706 连接至网络 1712,其可包括由其他服务提供商所拥有和 / 或操作的有线或无线网络。

[0198] 虽然上面以特定组合的方式描述了特征和元素,但是本领域技术人员应该理解到,每个特征或元素都可在没有其他特征和元素的情况下单独使用,或与其他特征和元素进行各种组合或不进行组合。此处所述的方法可在结合至计算机可读介质中的计算机程序、软件或固件中实现,以由计算机或处理器执行。计算机可读介质包括电子信号(经由有线或无线连接传送)和计算机可读存储介质。计算机可读存储介质的例子包括,但不限于,只读存储器(ROM)、随机存储存储器(RAM)、寄存器、缓存、半导体存储设备、例如内置磁盘和可移动磁盘的磁介质、磁光介质和光介质(例如 CD-ROM 盘和数字多用途盘(DVD))。可使用与软件相关的处理器来实现 WTRU、UE、终端、基站、RNC 或任何主机计算机中所使用的射频收发信机。

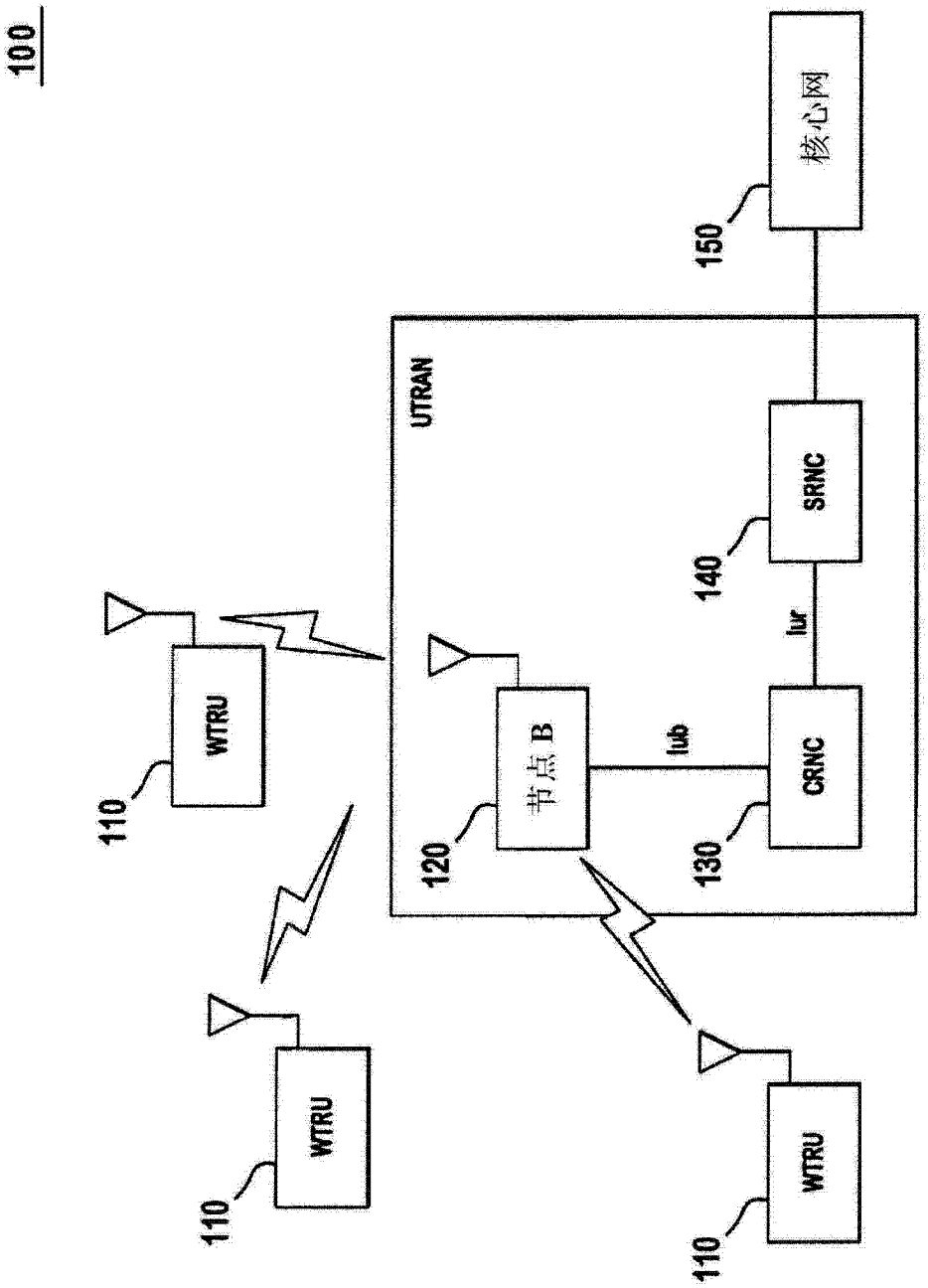

100
核心网
150
UTRAN
SRNC
140
Iur
WTRU
110
节点 B
120
Iub
CRNC
130
WTRU
110
WTRU
110

图 1

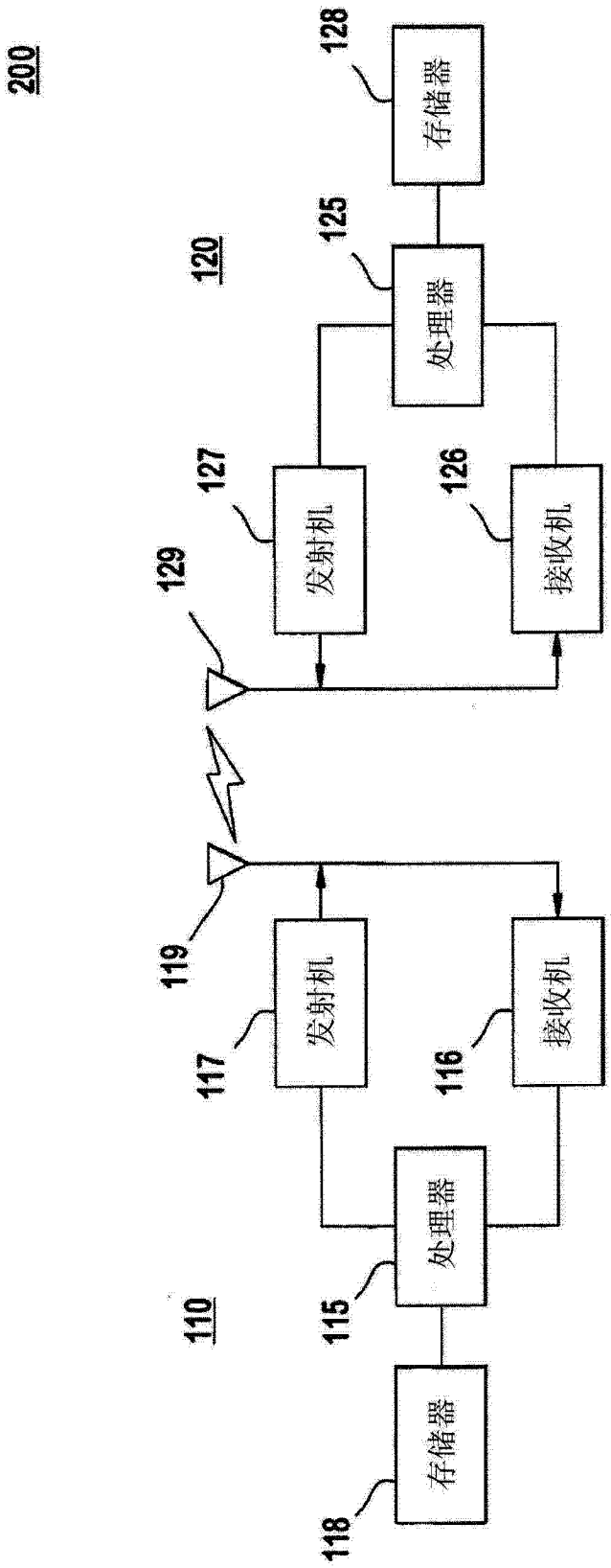

200
128
存储器
125
120
处理器
127
发射机
126
接收机
129
119
117
发射机
116
接收机
110
115
处理器
118
存储器

图 2

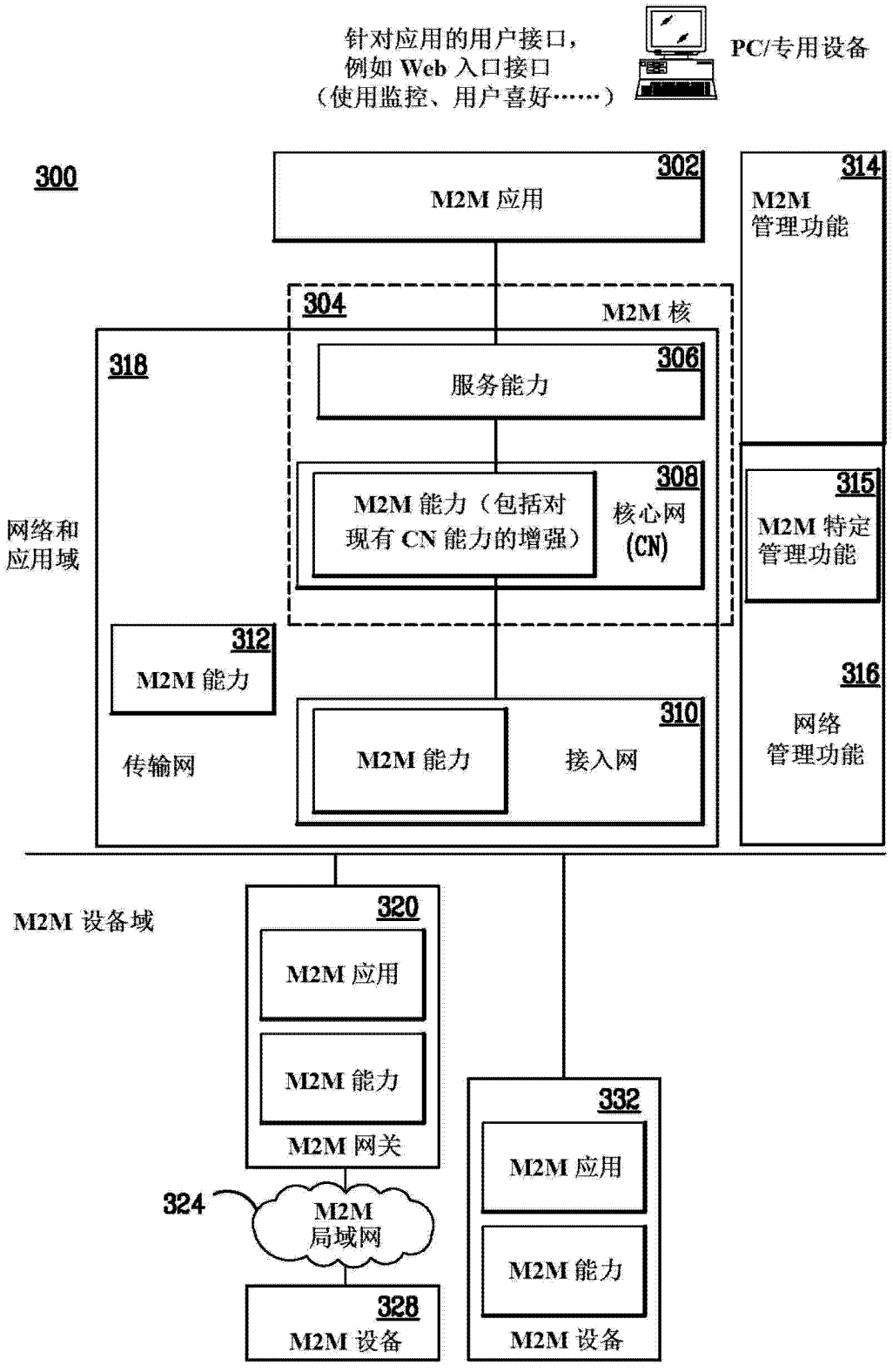

针对应用的用户接口，
例如 Web 入口接口
（使用监控、用户喜好……）
PC/专用设备
300
302
M2M 应用
314
M2M
管理功能
304
M2M 核
318
306
服务能力
308
M2M 能力（包括对
现有 CN 能力的增强）
核心网
(CN)
315
M2M 特定
管理功能
网络和
应用域
312
M2M 能力
316
网络
管理功能
310
M2M 能力
接入网
传输网
M2M 设备域
320
M2M 应用
M2M 能力
M2M 网关
332
M2M 应用
M2M 能力
M2M 设备
324
M2M
局域网
328
M2M 设备

图 3

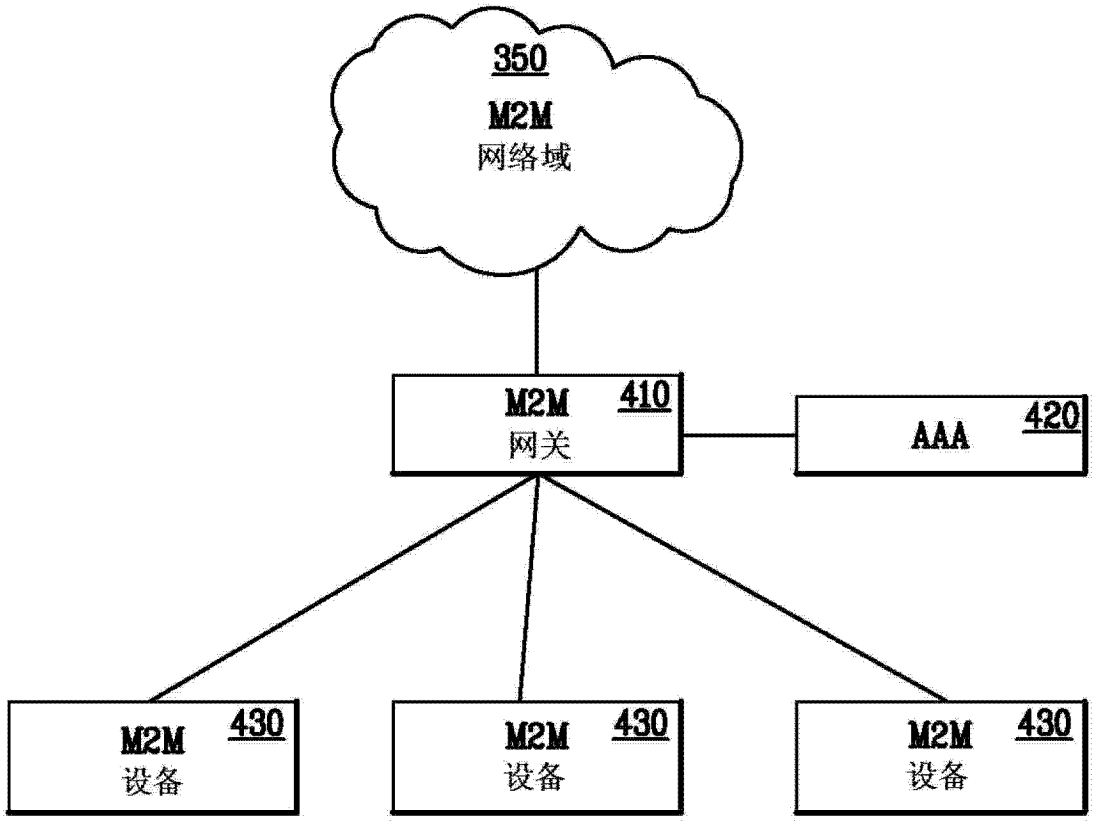


图 4

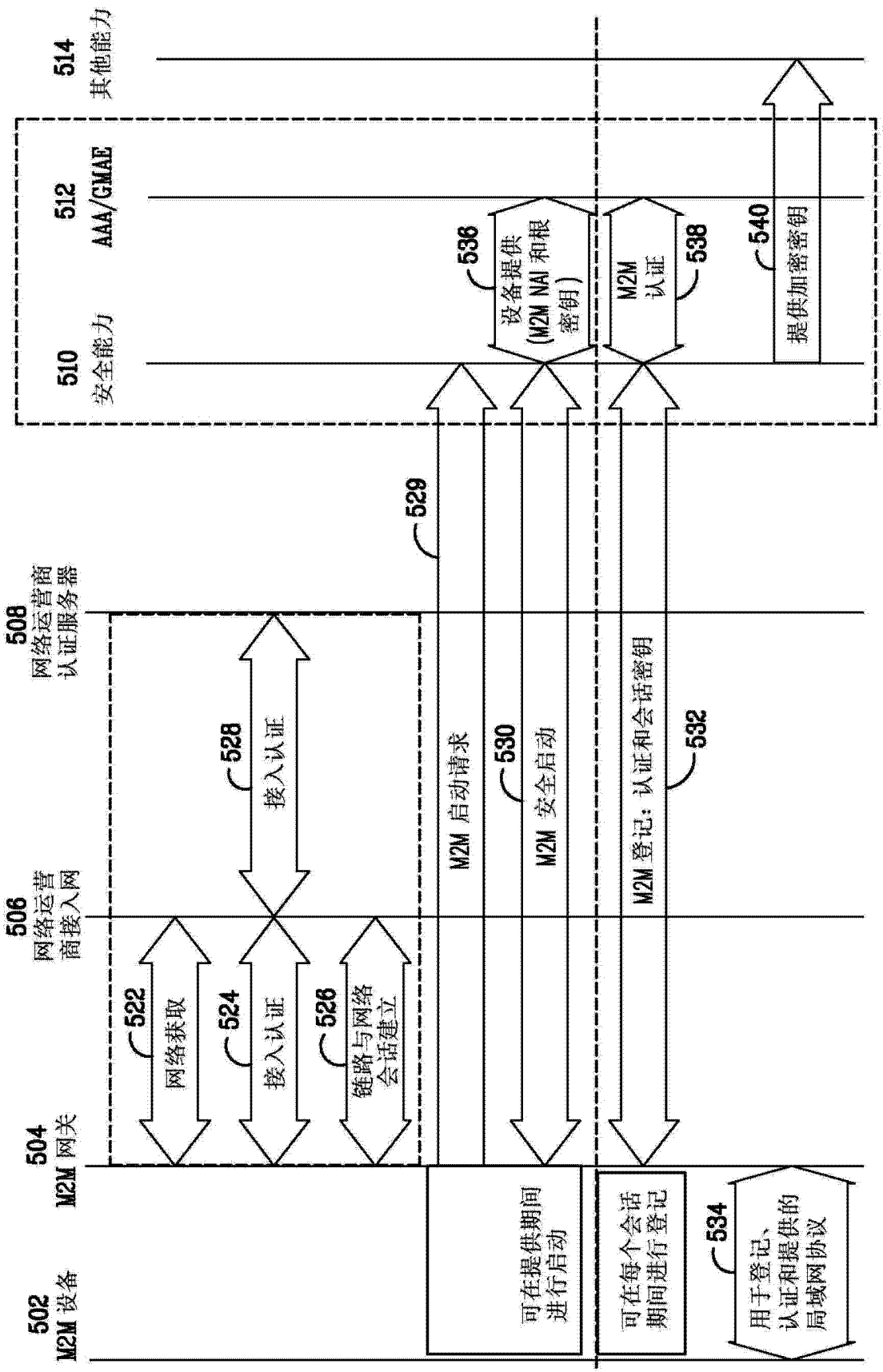

502
M2M 设备
504
M2M 网关
506
网络运营商接入网
508
网络运营商认证服务器
510
安全能力
512
AAA/GMAE
514
其他能力
522
网络获取
524
接入认证
526
链路与网络会话建立
528
接入认证
529
M2M 启动请求
530
M2M 安全启动
532
M2M 登记：认证和会话密钥
534
用于登记、认证和提供的局域网协议
536
设备提供 (M2M NAI 和根密钥)
538
M2M 认证
540
提供加密密钥
可在提供期间进行启动
可在每个会话期间进行登记

图 5

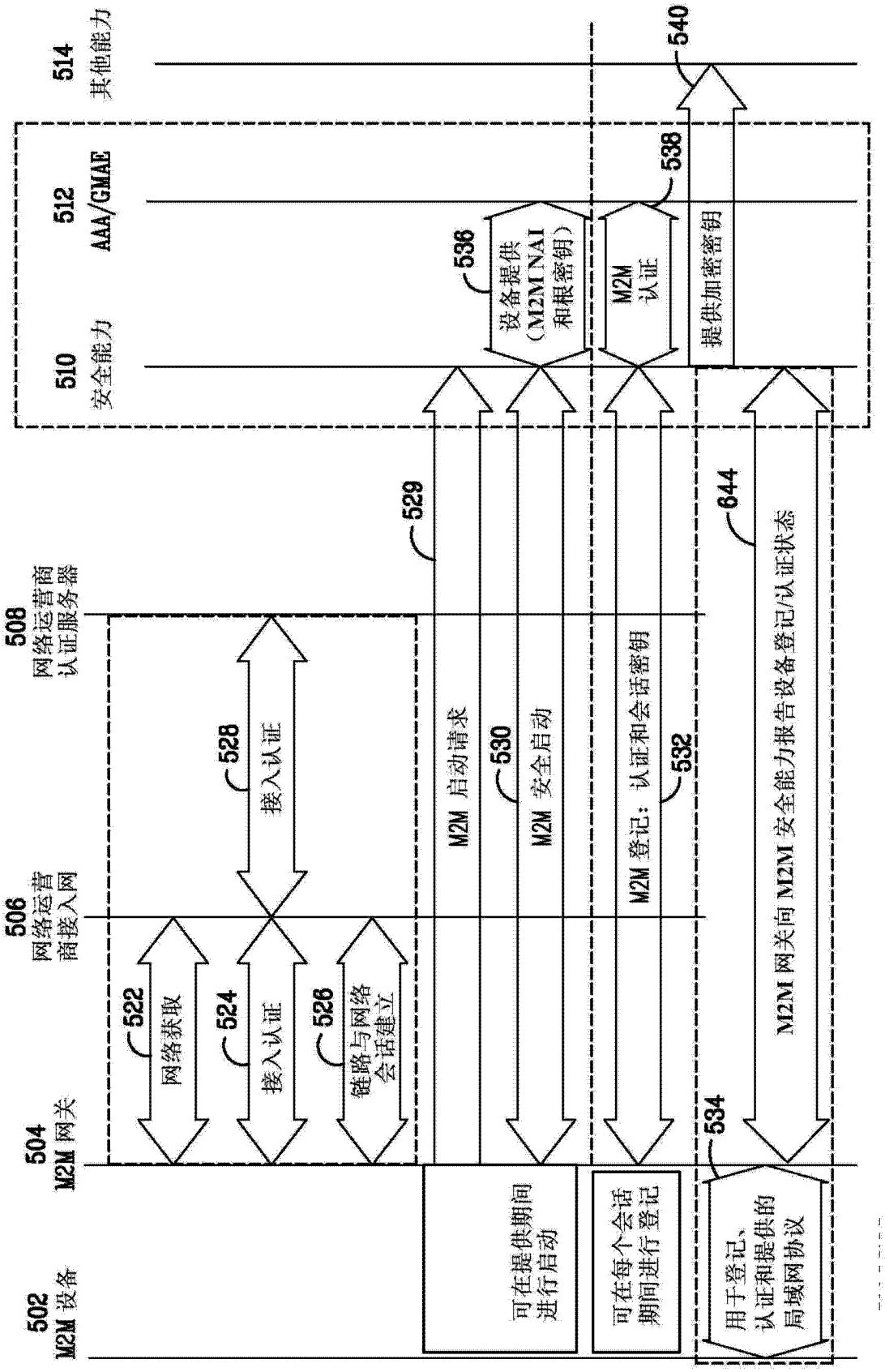

502
M2M 设备
504
M2M 网关
506
网络运营商接入网
508
网络运营商认证服务器
510
安全能力
512
AAA/GMAE
514
其他能力
522
网络获取
524
接入认证
526
链路与网络会话建立
528
接入认证
529
M2M 启动请求
530
M2M 安全启动
532
M2M 登记：认证和会话密钥
534
M2M 网关向 M2M 安全能力报告设备登记/认证状态
536
设备提供（M2M NAI 和根密钥）
538
M2M 认证
540
提供加密密钥
644
可在提供期间进行启动
可在每个会话期间进行登记
用于登记、认证和提供的局域网协议

图 6

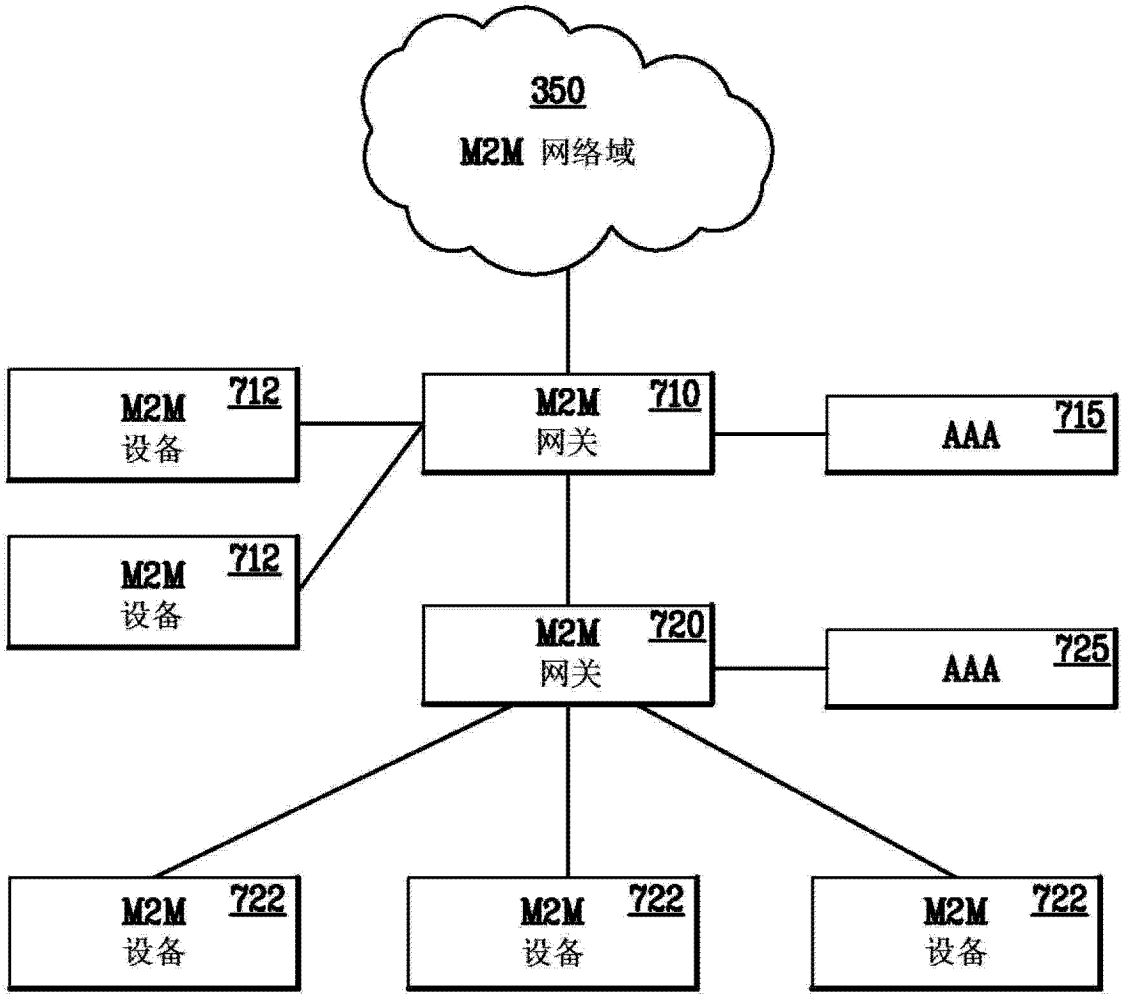

350
M2M 网络域
M2M 712
设备
M2M 712
设备
M2M 710
网关
AAA 715
M2M 720
网关
AAA 725
M2M 722
设备
M2M 722
设备
M2M 722
设备

图 7

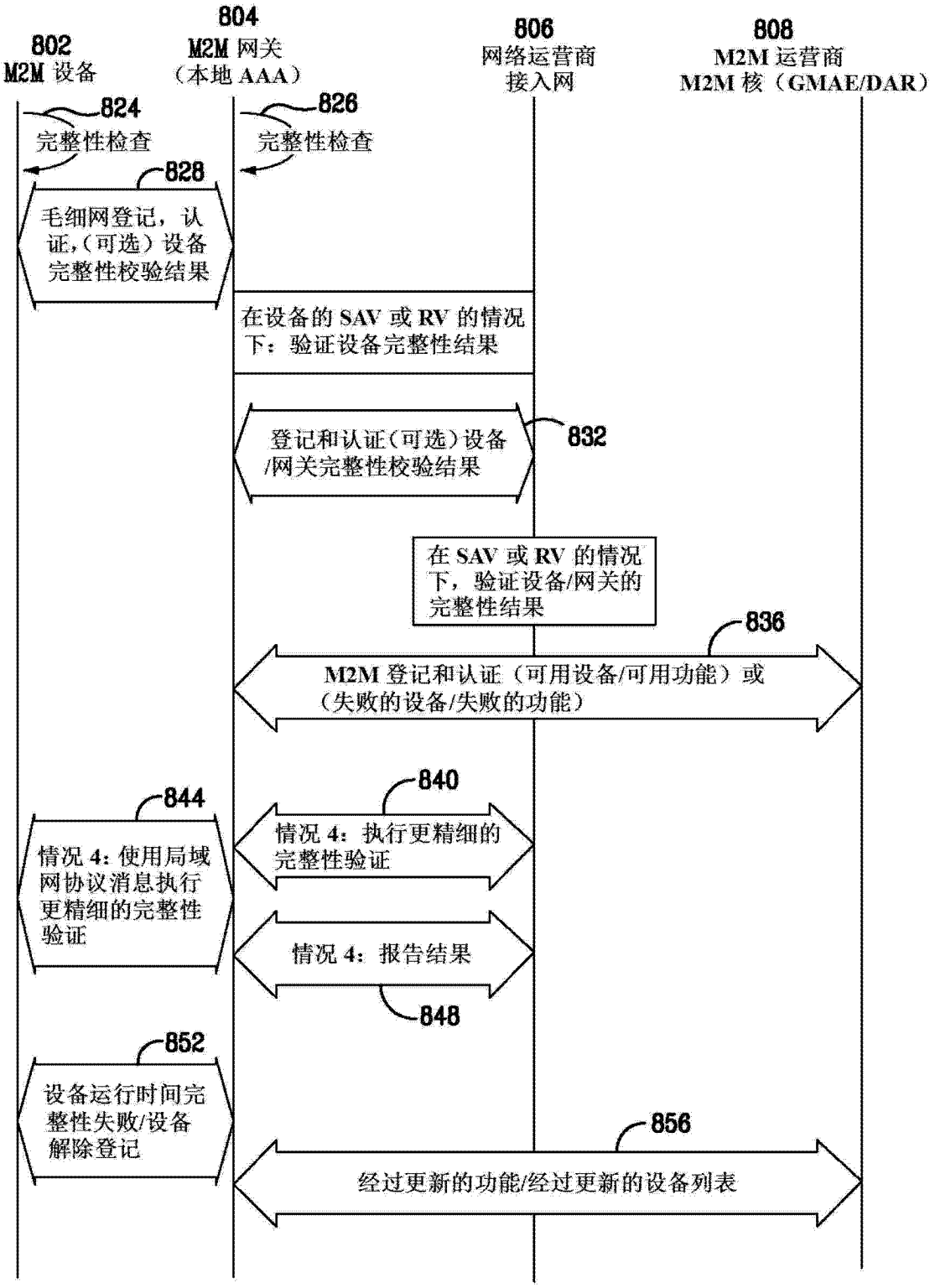

802
M2M 设备
804
M2M 网关
（本地 AAA）
806
网络运营商
接入网
808
M2M 运营商
M2M 核（GMAE/DAR）
824
完整性检查
826
完整性检查
828
毛细网登记，认证，（可选）设备完整性校验结果
在设备的 SAV 或 RV 的情况下：验证设备完整性结果
登记和认证（可选）设备/网关完整性校验结果
832
在 SAV 或 RV 的情况下，验证设备/网关的完整性结果
836
M2M 登记和认证（可用设备/可用功能）或（失败的设备/失败的功能）
840
情况 4：执行更精细的完整性验证
844
情况 4：使用局域网协议消息执行更精细的完整性验证
情况 4：报告结果
848
852
设备运行时间完整性失败/设备解除登记
856
经过更新的功能/经过更新的设备列表

图 8

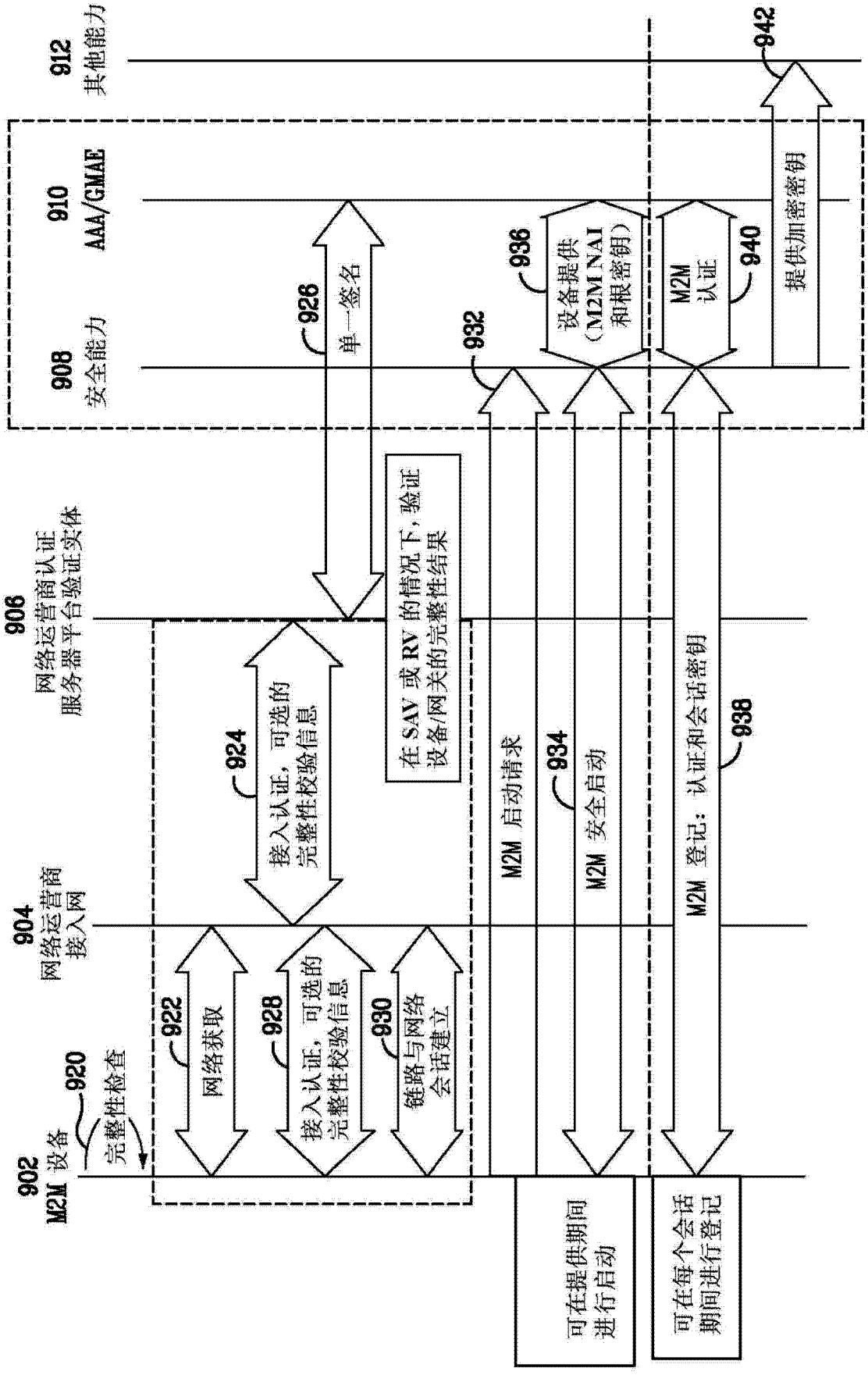

902
M2M 设备
920
完整性检查
904
网络运营商
接入网
906
网络运营商认证
服务器平台验证实体
908
安全能力
910
AAA/GMAE
912
其他能力
922
网络获取
924
接入认证，可选的
完整性校验信息
926
单一签名
928
接入认证，可选的
完整性校验信息
930
链路与网络
会话建立
932
在 SAV 或 RV 的情况下，验证
设备/网关的完整性结果
936
设备提供
（M2M NAI
和根密钥）
940
M2M
认证
942
提供加密密钥
M2M 启动请求
934
M2M 安全启动
M2M 登记：认证和会话密钥
938
可在提供期间
进行启动
可在每个会话
期间进行登记

图 9

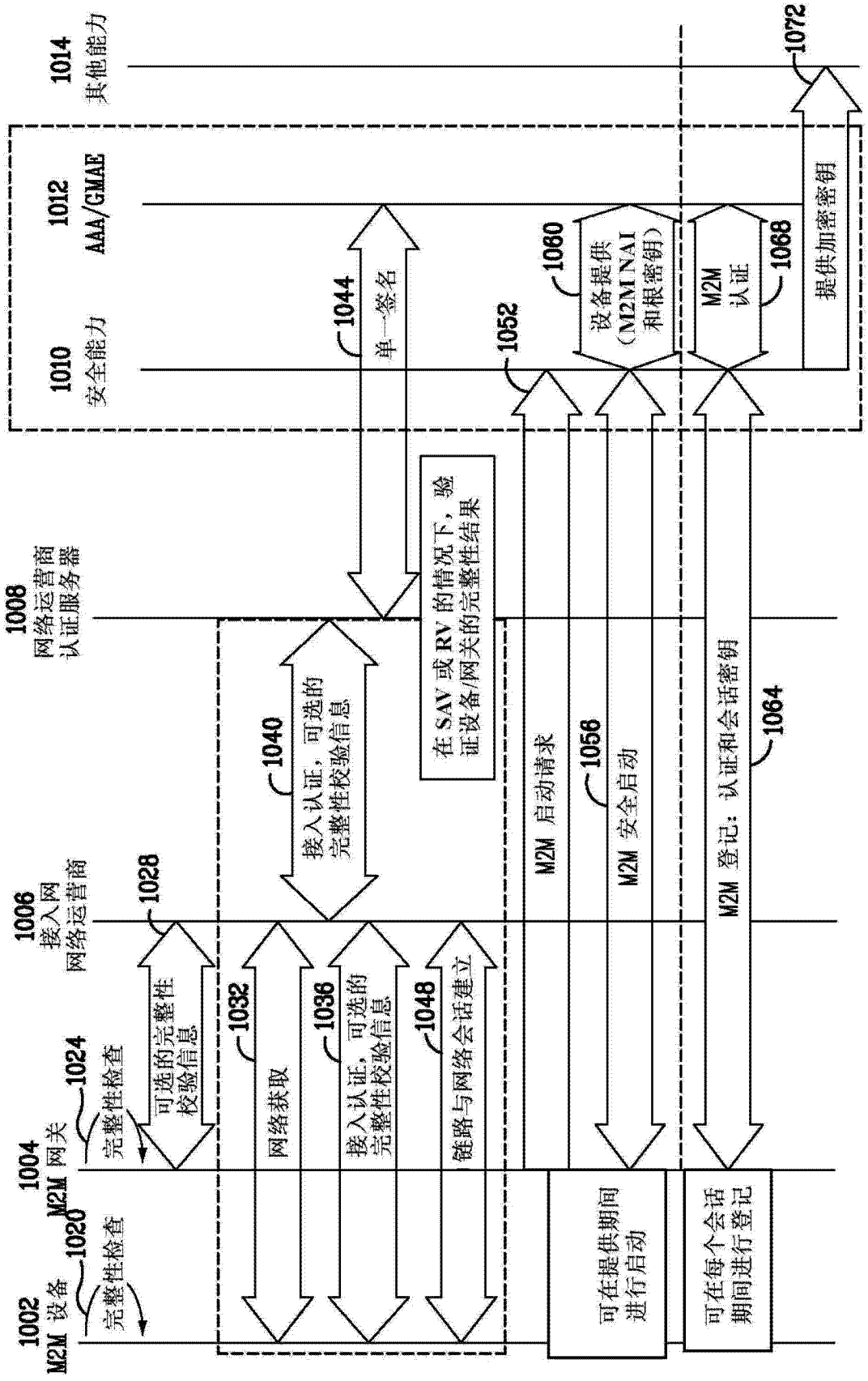

1002
M2M 设备
1004
M2M 网关
1006
接入网
网络运营商
1008
网络运营商
认证服务器
1010
安全能力
1012
AAA/GMAE
1014
其他能力
1020
完整性检查
1024
完整性检查
可选的完整性
校验信息
1028
网络获取
1032
接入认证，可选的
完整性校验信息
1036
链路与网络会话建立
1048
接入认证，可选的
完整性校验信息
1040
单一签名
1044
在 SAV 或 RV 的情况下，验
证设备/网关的完整性结果
1052
M2M 启动请求
1056
M2M 安全启动
设备提供
(M2M NAI
和根密钥)
1060
M2M
认证
1068
提供加密密钥
1072
M2M 登记：认证和会话密钥
1064
可在提供期间
进行启动
可在每个会话
期间进行登记

图 10

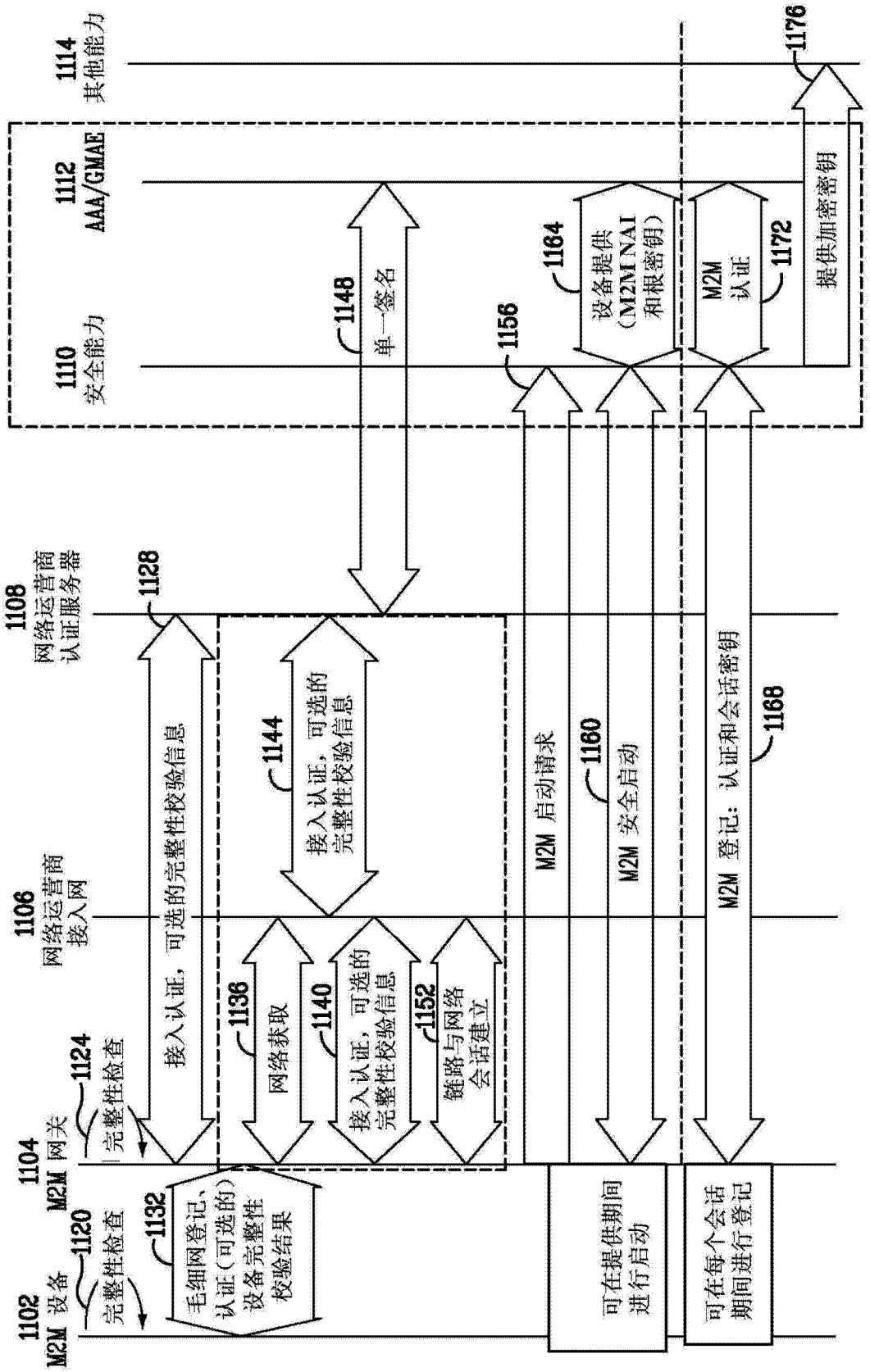

1102 M2M 设备
1104 M2M 网关
1106 网络运营商 接入网
1108 网络运营商 认证服务器
1110 安全能力
1112 AAA/GMAE
1114 其他能力
1120 完整性检查
1124 完整性检查
1128
1132 毛细网登记、认证(可选的)设备完整性校验结果
接入认证，可选的完整性校验信息
1136 网络获取
1140 接入认证，可选的完整性校验信息
1144 接入认证，可选的完整性校验信息
1148 单一签名
1152 链路与网络会话建立
1156
M2M 启动请求
1160 M2M 安全启动
1164 设备提供(M2M NAI和根密钥)
1168 M2M 登记：认证和会话密钥
1172 M2M 认证
1176 提供加密密钥
可在提供期间进行启动
可在每个会话期间进行登记

图 11

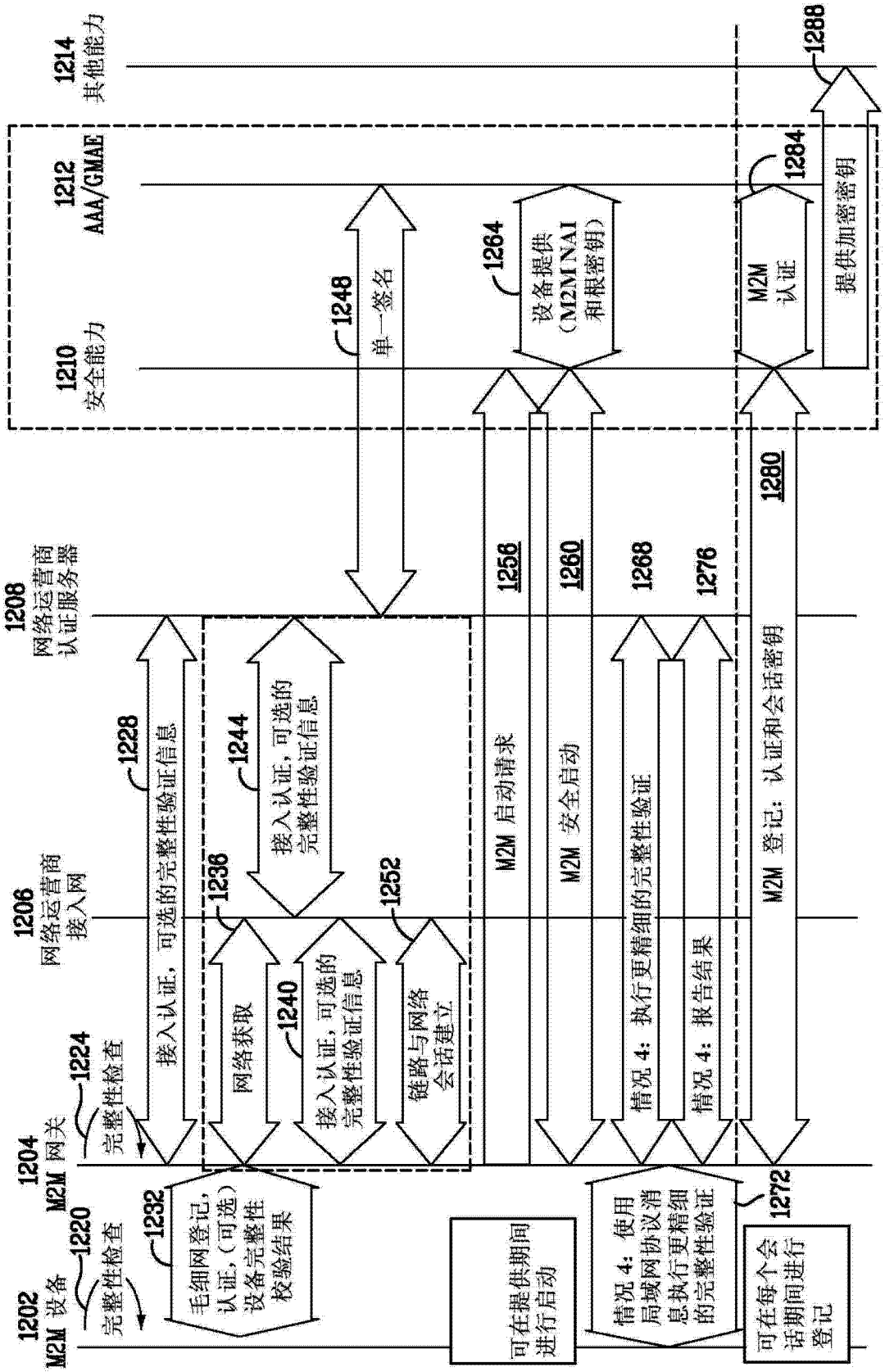

1202 M2M 设备
1204 M2M 网关
1206 网络运营商 接入网
1208 网络运营商 认证服务器
1210 安全能力
1212 AAA/GMAE
1214 其他能力
1220 完整性检查
1224 完整性检查
1228 接入认证，可选的完整性验证信息
1232 毛细网登记，认证，（可选）设备完整性校验结果
1236
1240 网络获取
1244 接入认证，可选的完整性验证信息
1248 单一签名
1252 链路与网络会话建立
1256 M2M 启动请求
1260 M2M 安全启动
1264 设备提供（M2M NAI 和根密钥）
1268 情况 4：执行更精细的完整性验证
1272
1276 情况 4：报告结果
1280 M2M 登记：认证和会话密钥
1284 M2M 认证
1288 提供加密密钥
可在提供期间进行启动
情况 4：使用局域网协议消息执行更精细的完整性验证
可在每个会话期间进行登记

图 12

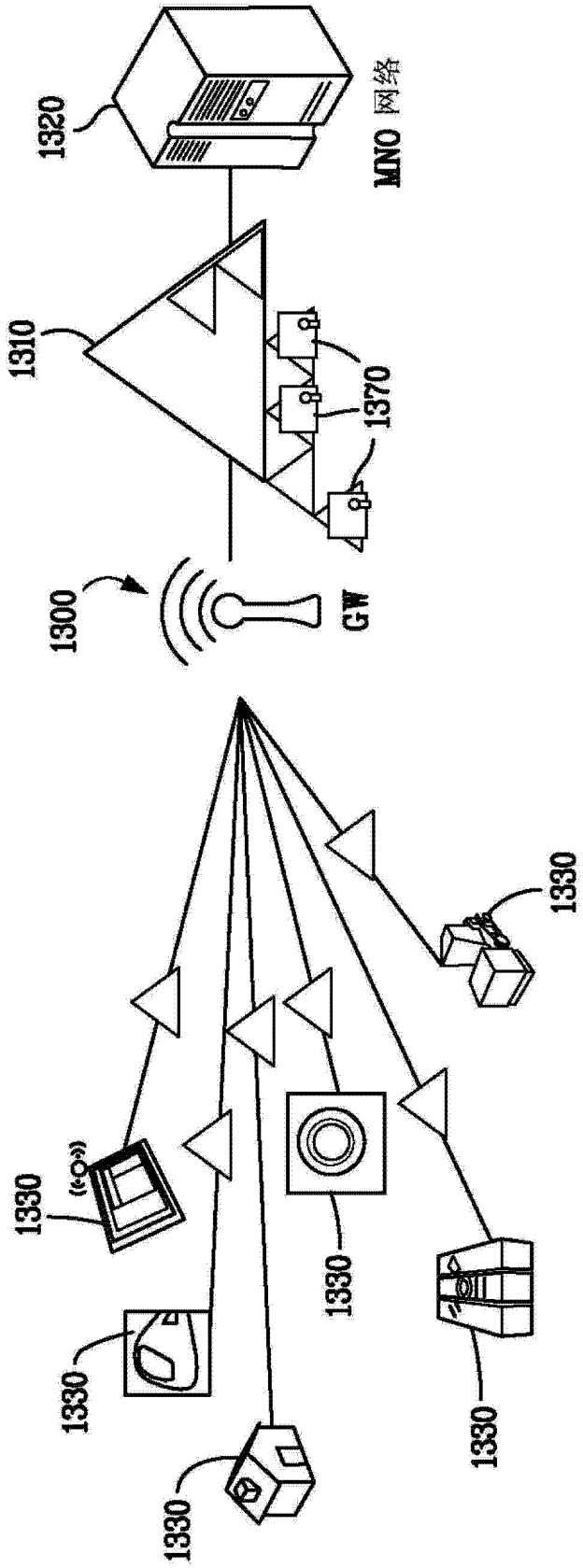


图 13

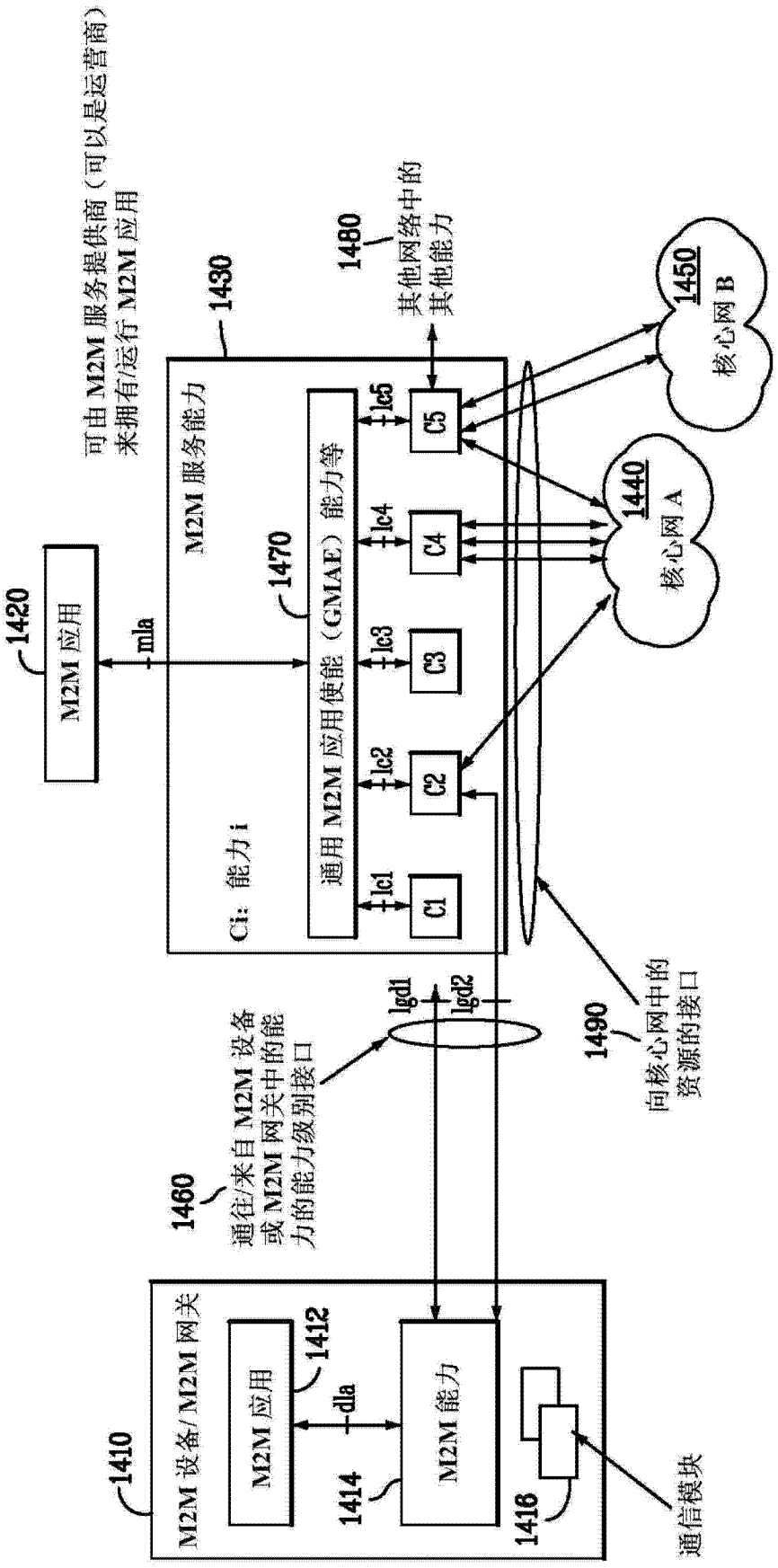

可由 M2M 服务提供商（可以是运营商）
来拥有/运行 M2M 应用
1420
M2M 应用
mIa
1430
M2M 服务能力
1470
通用 M2M 应用使能（GMAE）能力等
Ci：能力 i
Ic1
Ic2
Ic3
Ic4
Ic5
C1
C2
C3
C4
C5
1480
其他网络中的
其他能力
1450
核心网 B
1440
核心网 A
1460
通往/来自 M2M 设备
或 M2M 网关中的能
力的能力级别接口
Igd1
Igd2
1490
向核心网中的
资源的接口
1410
M2M 设备/ M2M 网关
M2M 应用
1412
dIa
1414
M2M 能力
1416
通信模块

图 14

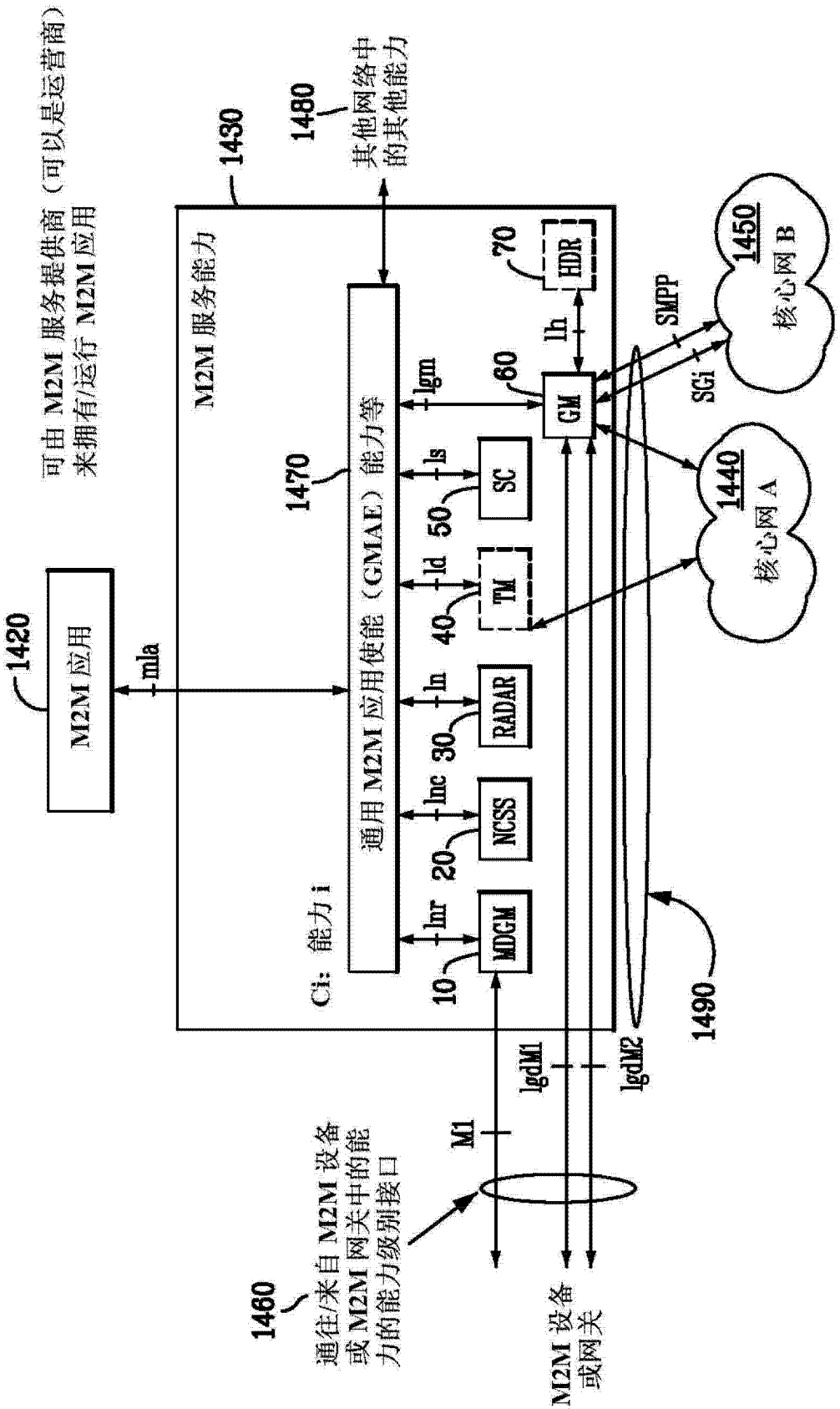

可由 M2M 服务提供商（可以是运营商）来拥有/运行 M2M 应用
1420
M2M 应用
mIa
1430
M2M 服务能力
1480
其他网络中的其他能力
1470
通用 M2M 应用使能（GMAE）能力等
Ci：能力 i
10
MDGM
lmr
20
NCSS
lmc
30
RADAR
ln
40
TM
ld
50
SC
ls
60
GM
lgm
70
HDR
lh
SMPP
SGi
1450
核心网 B
1440
核心网 A
1490
lgdM1
lgdM2
M1
1460
通往/来自 M2M 设备或 M2M 网关中的能力的能力级别接口
M2M 设备或网关

图 15

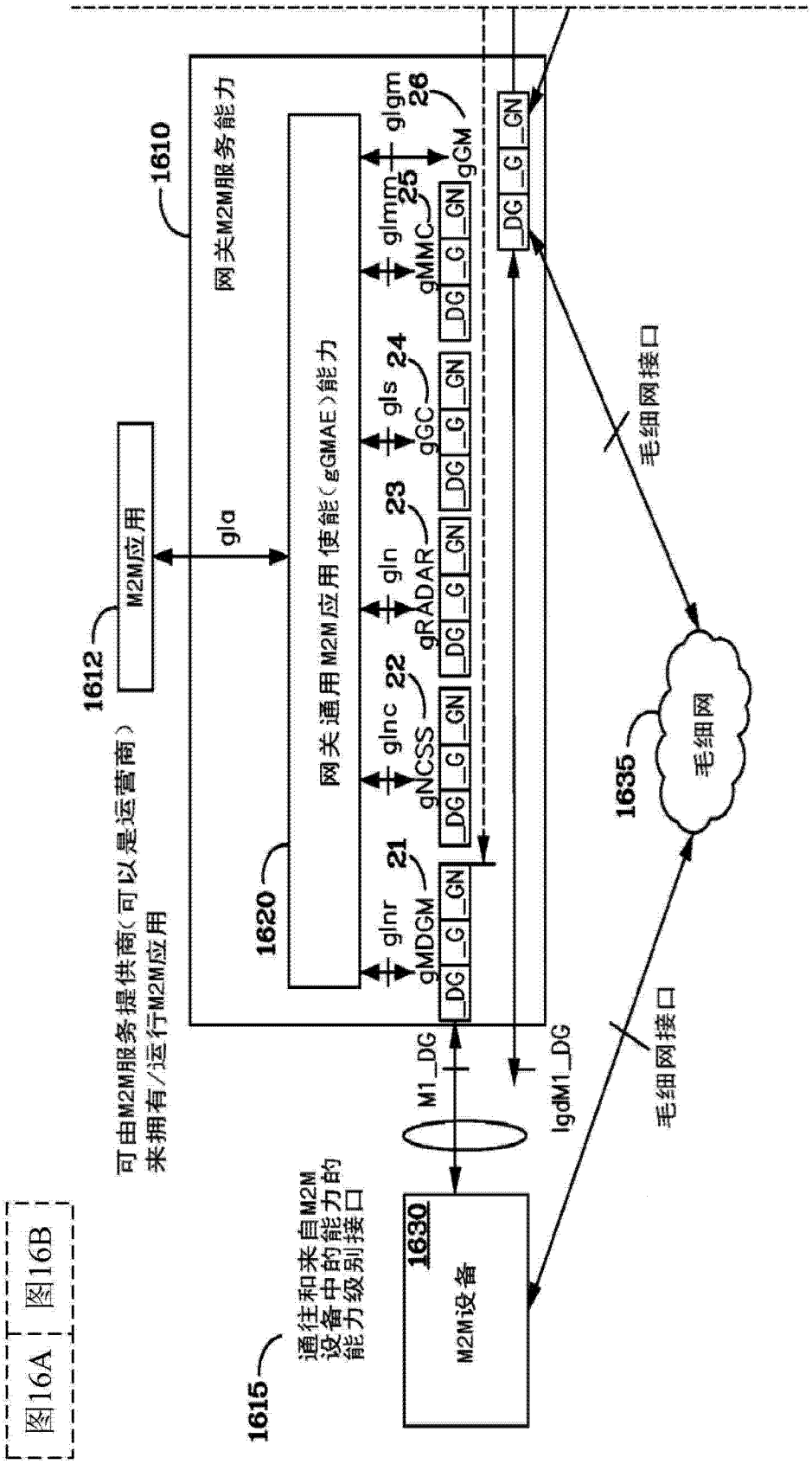


图16A 图16B
1610
网关M2M服务能力
1612
M2M应用
可由M2M服务提供商(可以是运营商)
来拥有/运行M2M应用
gla
1620
网关通用M2M应用使能(gGMAE)能力
glr 21 gMDGM
glnc 22 gNCSS
gln 23 gRADAR
gls 24 gGC
glmm 25 gMMC
glgm 26 gGM
DG G GN
1615
通往和来自M2M
设备中的能力的
能力级别接口
M1_DG
lgdM1_DG
1630
M2M设备
毛细网接口
毛细网接口
1635
毛细网

图 16A

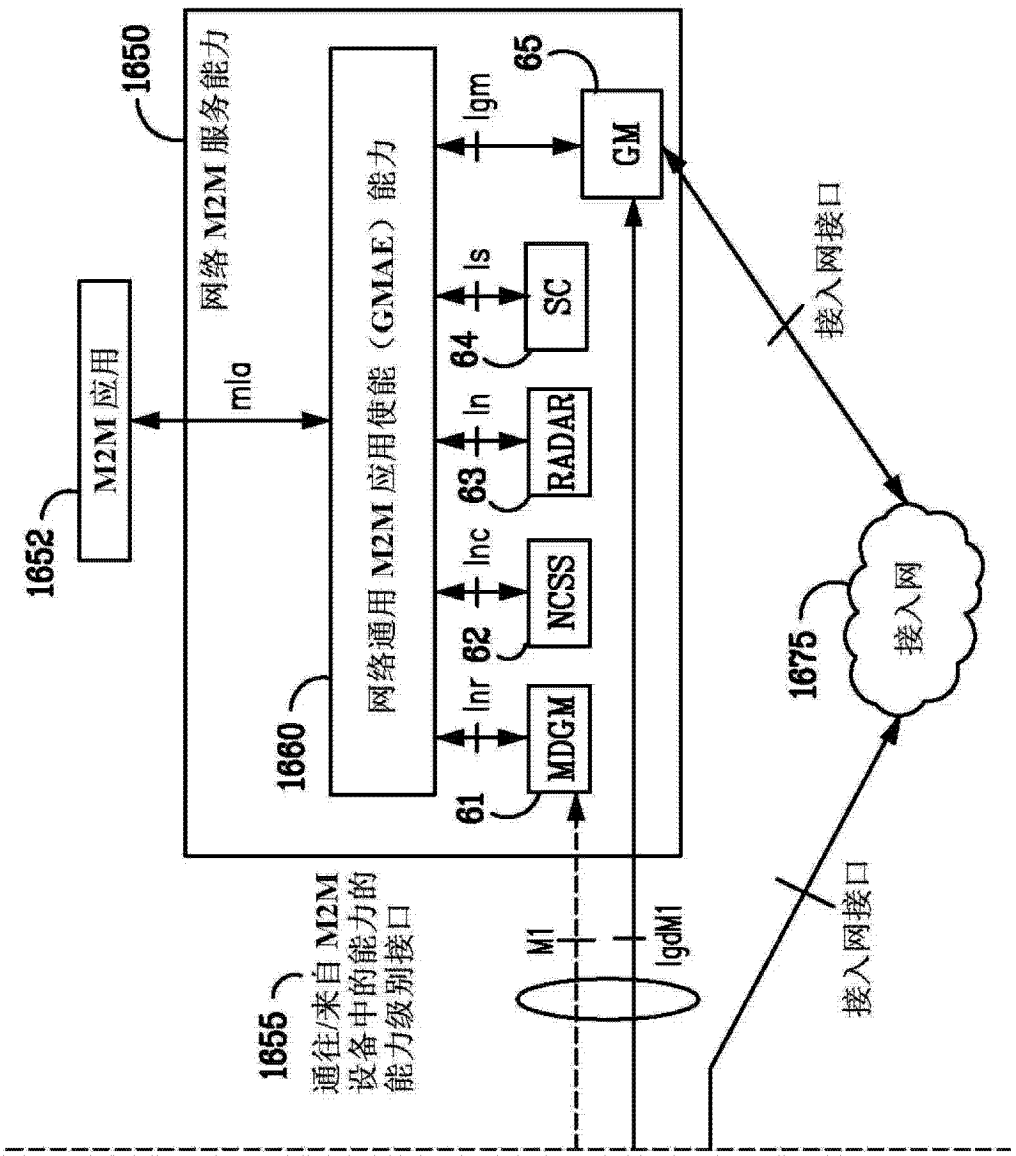

1650
网络 M2M 服务能力
M2M 应用
1652
mIa
网络通用 M2M 应用使能（GMAE）能力
1660
MDGM
NCSS
RADAR
SC
GM
61
62
63
64
65
Inr
Inc
In
Is
Igm
1655
通往/来自 M2M 设备中的能力的能力级别接口
M1
IgdM1
接入网接口
接入网接口
接入网
1675

图 16B

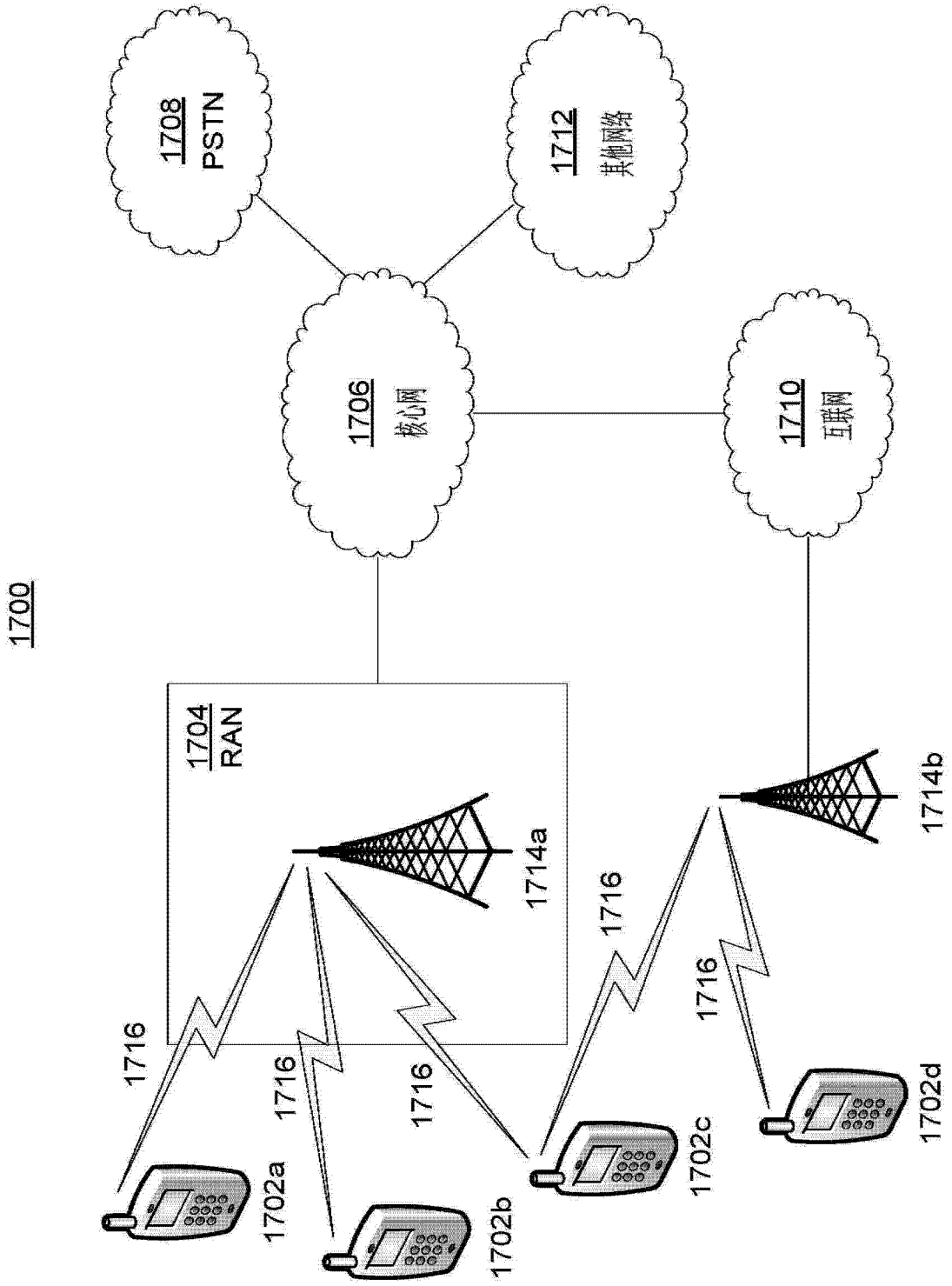

1700
1708
PSTN
1712
其他网络
1706
核心网
1710
互联网
1704
RAN
1714a
1714b
1716
1716
1716
1716
1716
1702a
1702b
1702c
1702d

图 17A

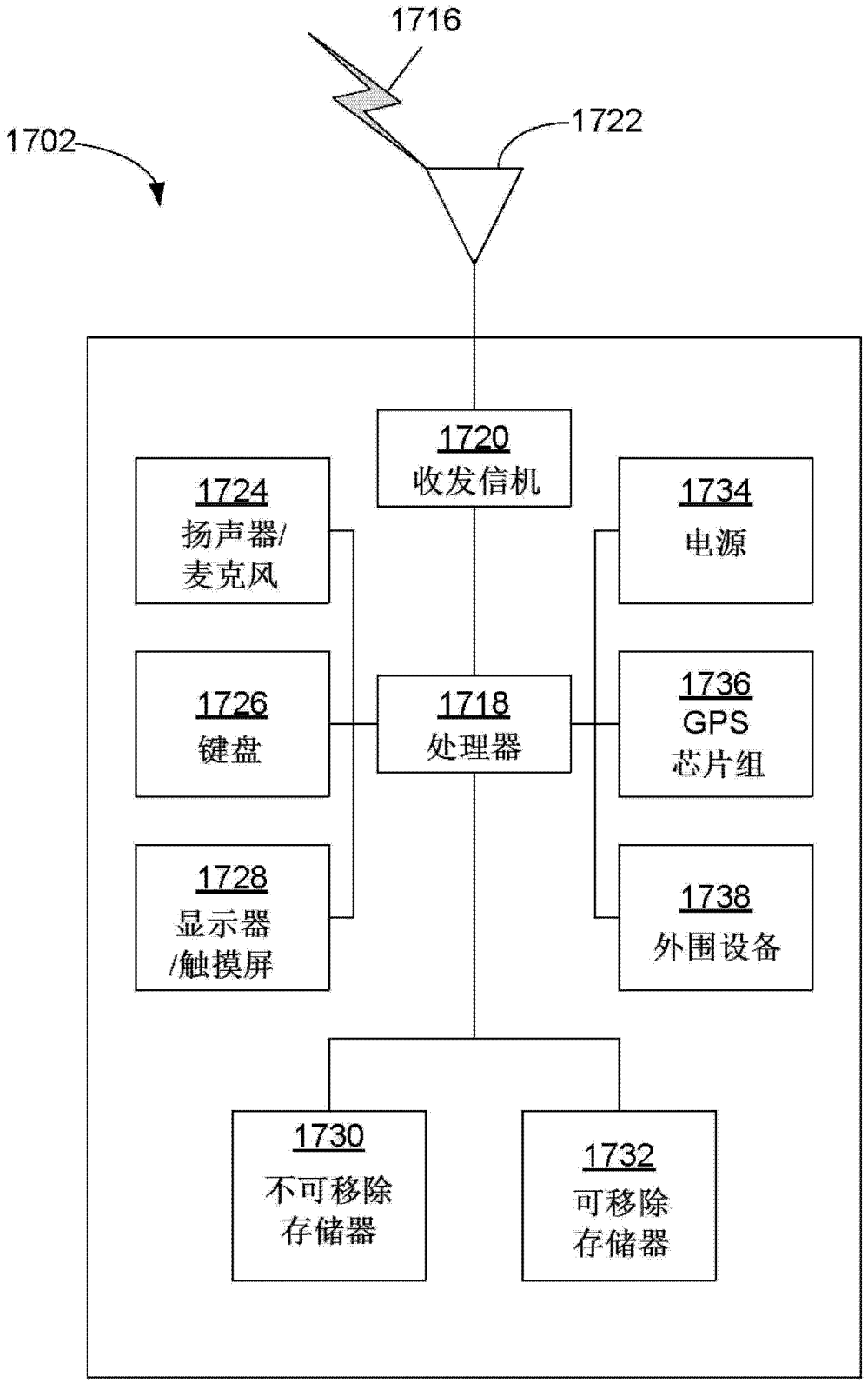

1716
1722
1702
1720
收发信机
1724
扬声器/
麦克风
1734
电源
1726
键盘
1718
处理器
1736
GPS
芯片组
1728
显示器
/触摸屏
1738
外围设备
1730
不可移除
存储器
1732
可移除
存储器

图 17B

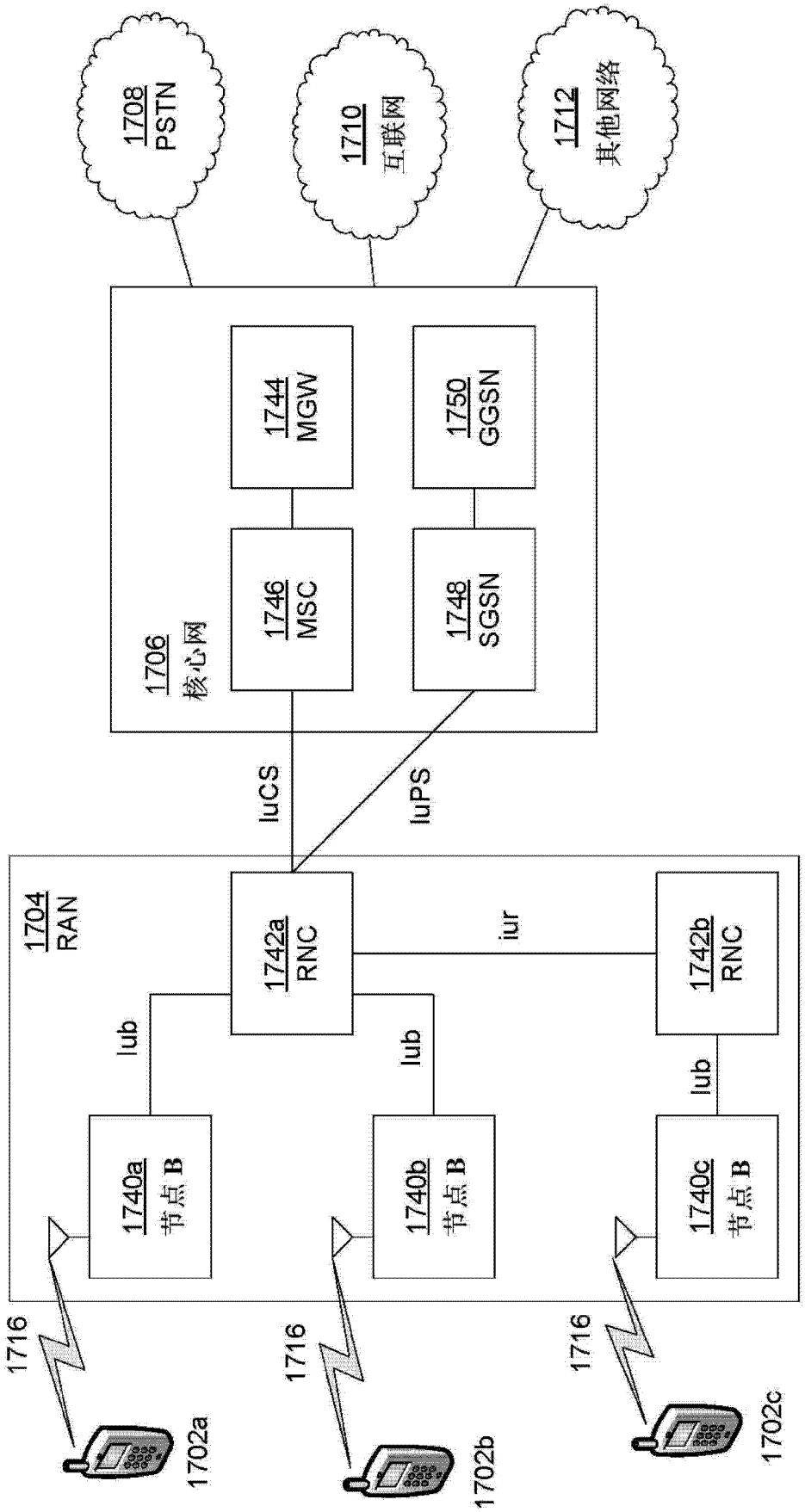

1708
PSTN
1710
互联网
1712
其他网络
1706
核心网
1744
MGW
1746
MSC
1748
SGSN
1750
GGSN
IuCS
IuPS
1704
RAN
1742a
RNC
1742b
RNC
iur
Iub
Iub
Iub
1740a
节点 B
1740b
节点 B
1740c
节点 B
1716
1716
1716
1702a
1702b
1702c

图 17C