(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105340236 A
(43)申请公布日 2016.02.17

(21)申请号 201480036462.7
(22)申请日 2014.06.26
(30)优先权数据
61/841,068 2013.06.28 US
14/314,999 2014.06.25 US
(85)PCT国际申请进入国家阶段日
2015.12.25
(86)PCT国际申请的申请数据
PCT/US2014/044362 2014.06.26
(87)PCT国际申请的公布数据
WO2014/210322 EN 2014.12.31
(71)申请人 高通股份有限公司
地址 美国加利福尼亚州
(72)发明人 J·M·林
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 周敏
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/801(2006.01)

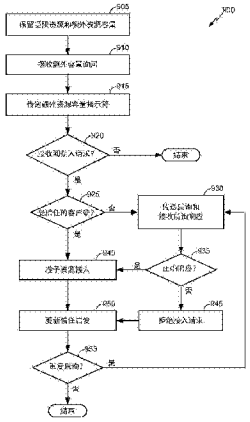
权利要求书3页 说明书26页 附图16页

(54)发明名称

用于减少 IoT 资源接入网中的控制负载的信任启发式模型

(57)摘要

本公开涉及用于减少 IoT 资源接入网中的控制负载的信任启发式模型。例如，认证方节点可质询请求接入资源的客户端节点，并且如果客户端节点正确地响应质询则准予接入，或者替换地如果客户端节点不正确地响应质询则拒绝接入。此外，基于对质询的响应，客户端节点可被指派信任等级，该信任等级可基于连续的质询和响应交换和/或与其它 IoT 网络节点的交互来动态更新。例如，为了减少资源接入控制负载，如果客户端节点随时间推移正确地响应连续的质询，则后续的质询和响应间隔可被增大或消除，而随时间推移不正确地响应连续质询的客户端节点可被阻止接入资源或者从 IoT 网络中禁止。



CN 105340236 A

1. 一种用于物联网 (IoT) 网络中的受控资源接入的方法，包括 ：

由请求方节点请求对所述 IoT 网络中的第一受控资源的接入，其中对所述第一受控资源的接入包括周期性地完成认证规程的要求 ；

对从第一监督者节点接收到的质询消息进行响应 ；以及

响应于对所述质询消息正确地响应而接收所请求的对所述第一受控资源的接入，其中所述第一监督者节点响应于所述请求方节点对一个或多个连续质询消息正确地响应而降低周期性地完成所述认证规程的要求。

2. 如权利要求 1 所述的方法，其特征在于，所述质询消息和对所述质询消息的响应通过与所述 IoT 网络相关联的控制信道来交换。

3. 如权利要求 1 所述的方法，其特征在于，所述第一监督者节点响应于所述请求方节点对所述质询消息正确地响应而提高与所述请求方节点相关联的信任等级。

4. 如权利要求 1 所述的方法，其特征在于，所述第一监督者节点增大向所述请求方节点传送后续质询消息之前的间隔以降低周期性地完成所述认证规程的要求。

5. 如权利要求 1 所述的方法，其特征在于，所述第一监督者节点响应于从所述请求方节点接收到对所述质询消息的不正确响应而降低与所述请求方节点相关联的信任等级。

6. 如权利要求 1 所述的方法，其特征在于，响应于所述请求方节点对所述质询消息不正确地响应和对一个或多个连续质询消息不正确地响应，所述第一监督者节点临时地阻止所述请求方节点在所述 IoT 网络上通信。

7. 如权利要求 1 所述的方法，其特征在于，响应于所述请求方节点对所述质询消息不正确地响应并且随时间推移继续对一个或多个连续质询消息不正确地响应，所述第一监督者节点永久地禁止所述请求方节点在所述 IoT 网络上通信。

8. 如权利要求 1 所述的方法，其特征在于，响应于所述 IoT 网络迁移至新的网络接入层，所述第一监督者节点根据指派给所述请求方节点的信任等级来调整周期性地完成所述认证规程的要求。

9. 如权利要求 1 所述的方法，其特征在于，进一步包括 ：

向第二监督者节点请求对第二受控资源的接入，其中所述第二监督者节点仅基于所述请求方节点与具有同所述请求方节点的一个或多个先前交互的受信任节点之间的信任等级来确定是否要向所述请求方节点准予对所述第二受控资源的接入。

10. 如权利要求 9 所述的方法，其特征在于，第二 IoT 网络包括以下一者或多者 ：第二受控资源、第二监督者节点、或者具有与所述请求方节点的一个或多个先前交互的受信任节点。

11. 如权利要求 9 所述的方法，其特征在于，与所述请求方节点相关联的信任等级包括信任启发式逻辑模型中的 N 个信任等级之一，所述信任启发式逻辑模型定义与具有每个相应信任等级的节点相关联的所准许的资源接入。

12. 如权利要求 1 所述的方法，其特征在于，所述第一监督者节点包括管控对所述第一受控资源的接入的管控节点。

13. 如权利要求 1 所述的方法，其特征在于，所述第一监督者节点包括在所述请求方节点与管控对所述第一受控资源的接入的管控节点之间中继消息的中间节点。

14. 如权利要求 1 所述的方法，其特征在于，所述第一受控资源包括具有等于或超过消

耗速率的生产速率的无限资源。

15. 如权利要求 1 所述的方法，其特征在于，所述第一受控资源包括具有超过生产速率的消耗速率的有限资源。

16. 如权利要求 15 所述的方法，其特征在于，所述第一监督者节点包括具有所分配的对所述有限资源的接入的中间节点，并且其中被分配给所述中间节点的接入包括所述中间节点需要的第一部分以及能被供应给一个或多个请求方节点的额外部分。

17. 如权利要求 16 所述的方法，其特征在于，请求对所述第一受控资源的接入进一步包括：

联系具有所分配的对所述有限资源的接入的一个或多个中间节点以确定向其分配的有限资源的总额外部分；以及

响应于确定向其分配的有限资源的总额外部分满足或超过所述请求方节点需要的有限资源量而请求所述一个或多个中间节点供应所述请求方节点需要的有限资源量。

18. 如权利要求 17 所述的方法，其特征在于，对所述质询消息进行响应进一步包括：

响应于请求所述一个或多个中间节点供应所述请求方节点需要的有限资源量而接收来自所述一个或多个中间节点的质询消息；以及

响应于向每个中间节点传送对所述质询消息的正确响应而接收来自所述一个或多个中间节点的所需有限资源量。

19. 一种物联网 (IoT) 设备，包括：

用于请求对 IoT 网络中的受控资源的接入的装置，其中对所述受控资源的接入包括周期性地完成认证规程的要求；

用于对从监督者节点接收到的质询消息进行响应的装置；以及

用于响应于对所述质询消息正确地响应而接收所请求的对所述受控资源的接入的装置，其中所述监督者节点响应于所述 IoT 设备对一个或多个连续质询消息正确地响应而降低周期性地完成所述认证规程的要求。

20. 一种其上记录有计算机可执行指令的计算机可读存储介质，其中在物联网 (IoT) 设备上执行所述计算机可执行指令使得所述 IoT 设备：

请求对 IoT 网络中的受控资源的接入，其中对所述受控资源的接入包括周期性地完成认证规程的要求；

对从监督者节点接收到的质询消息进行响应；以及

响应于对所述质询消息正确地响应而接收所请求的对所述受控资源的接入，其中所述监督者节点响应于所述 IoT 设备对一个或多个连续质询消息正确地响应而降低周期性地完成所述认证规程的要求。

21. 一种用于控制物联网 (IoT) 网络中的资源接入的方法，包括：

在监督者节点处接收来自请求方节点的对所述 IoT 网络中的受控资源的接入的请求，其中对所述受控资源的接入包括周期性地完成认证规程的要求；

向所述请求方节点传送质询消息；

接收来自所述请求方节点的对所述质询消息的响应；以及

基于所接收到的对所述质询消息的响应来确定是否要向所述请求方节点准予对所述受控资源的接入，其中所述监督者节点进一步基于所接收到的对所述质询消息的响应是否

正确来调整对所述请求方节点周期性地完成所述认证规程的要求。

22. 如权利要求 21 所述的方法，其特征在于，进一步包括：

响应于确定所接收到的对所述质询消息的响应是正确的而向所述请求方节点准予对所述受控资源的接入；以及

响应于确定所接收到的对所述质询消息的响应是正确的而提高被指派给所述请求方节点的信任等级并且增大在向所述请求方节点传送后续质询消息之前的间隔。

23. 如权利要求 21 所述的方法，其特征在于，进一步包括：

响应于确定所接收到的对所述质询消息的响应不正确而向所述请求方节点拒绝对所述受控资源的接入；以及

响应于确定所接收到的对所述质询消息的响应不正确而降低被指派给所述请求方节点的信任等级。

24. 如权利要求 23 所述的方法，其特征在于，进一步包括：

响应于所述请求方节点对一个或多个连续质询消息不正确地响应而阻止所述请求方节点在所述 IoT 网络上通信。

25. 如权利要求 21 所述的方法，其特征在于，进一步包括：

响应于所述 IoT 网络迁移至新的网络接入层，根据指派给所述请求方节点的信任等级来调整周期性地完成所述认证规程的要求。

26. 如权利要求 21 所述的方法，其特征在于，进一步包括：

基于所接收到的对所述质询消息的响应来向所述请求方节点指派信任等级，其中被指派给所述请求方节点的信任等级包括信任启发式逻辑模型中的 N 个信任等级之一，所述信任启发式逻辑模型定义与具有每个相应信任等级的节点相关联的所准许的资源接入；以及

向管控对所述 IoT 网络中的一个或多个资源的接入的另一节点传达被指派给所述请求方节点的信任等级，其中所述 IoT 网络中的所述另一节点仅基于被指派给所述请求方节点的信任等级来确定是否要向所述请求方节点准予对所述一个或多个受管控的资源的接入。

27. 如权利要求 21 所述的方法，其特征在于，所述监督者节点具有所分配的对所述受控资源的接入，并且其中被分配给所述监督者节点的接入包括所述监督者节点需要的部分以及能被供应给所述请求方节点的额外部分。

28. 如权利要求 27 所述的方法，其特征在于，确定是否要向所述请求方节点准予对所述受控资源的接入进一步包括：

响应于确定所接收到的对所述质询消息的响应是正确的而向所述请求方节点供应所分配的对所述受控资源的接入的额外部分。

29. 如权利要求 28 所述的方法，其特征在于，响应于所述请求方节点请求所述监督者节点供应所分配的对所述受控资源的接入的额外部分，所述监督者节点向所述请求方节点传送所述质询消息。

30. 如权利要求 21 所述的方法，其特征在于，所述受控资源包括以下一者或多者：具有等于或超过消耗速率的生产速率的无限资源、或者具有超过生产速率的消耗速率的有限资源。

用于减少 IoT 资源接入网中的控制负载的信任启发式模型

[0001] 相关申请的交叉引用

[0002] 本专利申请要求于 2014 年 6 月 28 日提交的题为“TRUST HEURISTIC MODEL FOR REDUCING CONTROL LOAD IN IOT RESOURCE ACCESS NETWORKS(用于减少 IoT 资源接入网中的控制负载的信任启发式模型)”的专利申请 No.61/841,068 的权益,并且该专利申请由此通过援引明确地整体纳入于此。

技术领域

[0003] 本文所描述的各个实施例一般涉及使用信任启发式模型来减少物联网 (IoT) 资源接入网中的控制负载。

[0004] 背景

[0005] 因特网是使用标准网际协议套件 (例如,传输控制协议 (TCP) 和网际协议 (IP)) 以彼此通信的互联的计算机和计算机网络的全球系统。物联网 (IoT) 基于日常对象 (不仅是计算机和计算机网络) 可经由 IoT 通信网络 (例如,自组织系统或因特网) 可读、可识别、可定位、可寻址、以及可控制的理念。

[0006] 数个市场趋势正推动 IoT 设备的开发。例如,增加的能源成本正推动政府在智能电网以及将来消费支持 (诸如电动车辆和公共充电站) 中的战略性投资。增加的卫生保健成本和老龄化人口正推动对远程 / 联网卫生保健和健康服务的开发。家庭中的技术革命正推动对新的“智能”服务的开发,包括由营销 ‘N’ 种活动 (‘N’ play)(例如,数据、语音、视频、安全性、能源管理等) 并扩展家庭网络的服务提供者所进行的联合。作为降低企业设施的运作成本的手段,建筑物正变得更智能和更方便。

[0007] 存在用于 IoT 的数个关键应用。例如,在智能电网和能源管理领域,公共事业公司可以优化能源到家庭和企业的递送,同时消费者能更好地管理能源使用。在家庭和建筑物自动化领域,智能家居和建筑物可具有对家或办公室中的实质上任何设备或系统的集中式控制,从电器到插入式电动车辆 (PEV) 安全性系统。在资产跟踪领域,企业、医院、工厂和其他大型组织能准确跟踪高价值装备、患者、车辆等的位置。在卫生和健康领域,医生能远程监视患者的健康,同时人们能跟踪健康例程的进度。

[0008] 如此,在不久的将来,IoT 技术的持续增进的发展将导致住宅中用户周围、车辆中、工作中、和许多其它位置处的众多 IoT 设备。在许多情形中,IoT 网络可包括具有不同 IoT 能力的设备可能要求接入的各种资源,由此控制机制可被用来认证或以其它方式管控对受控资源的接入。相应地,接入特定受控资源的具有 IoT 能力的设备可能需要“常通”网络连接以周期性地认证对受控资源的接入,这可导致各种问题,因为管控或以其它方式控制对受控资源的接入的服务器或其它认证实体可能经历相当大的控制负载,该控制负载可中断接入受控资源的服务和阻止客户端接入这些服务。在被适配到 IoT 概念时,如果网络包括通过控制信道通信以接入受控资源的各种设备,则该控制信道上的额外话务可能潜在地中断资源使用。相应地,存在对于可被用来减少用于认证或以其它方式控制对 IoT 网络中的受控资源的接入的控制负载的机制的需求。

[0009] 概述

[0010] 下文给出了关于与本文所公开的用于使用信任启发式模型来减少物联网（IoT）资源接入网中的控制负载的机制相关联的一个或多个方面和／或实施例的简要概述。如此，以下概述既不应被视为与所有构想的方面和／或实施例相关的详尽纵览，以下概述也不应被认为标识与所有构想的方面和／或实施例相关的关键性或决定性要素或描绘与任何特定方面和／或实施例相关联的范围。相应地，以下概述仅具有在以下给出的详细描述之前以简化形式呈现关于与本文所公开的用于使用信任启发式模型来减少 IoT 资源接入网中的控制负载的机制相关的一个或多个方面和／或实施例的某些概念的目的。

[0011] 根据一个示例性方面，用来减少 IoT 资源接入网中的控制负载的信任启发式模型可以基于在想要接入受控资源的请求方节点与管控受控资源或充当在请求方节点与管控受控资源的节点之间中继接入的中介（例如，如果请求方节点不能与管控节点直接联系）的认证方节点之间的质询和响应机制。例如，认证方节点可向请求对受控资源的接入的节点发送质询并且基于对质询的响应来确定是否要准予所请求的接入。由此，如果请求方节点正确地响应质询，则认证方节点通常可准予所请求的接入，或者替换地如果请求方节点不正确地响应质询，则认证方节点可拒绝所请求的接入。此外，认证方节点可基于对初始质询的响应是否正确来向请求方节点指派恰适的信任等级，并且被指派给请求方节点的信任等级可以基于连续质询和响应交换和／或与 IoT 网络中的其它节点的交互来动态更新。

[0012] 根据另一示例性方面，质询和响应机制常规地以规则的间隔重复以确保在对质询的初始正确响应之后的时间内没有什么改变并且周期性地重新认证请求方节点，这可因控制信道上的额外话务而占据不必要的带宽并且降低性能（例如，在无线系统中）。相反，本文所公开的信任启发式模型可减少与质询和响应交换相关联的控制负载或者可以其它方式用来控制资源接入的其它话务。例如，在一个实施例中，在请求方节点正确地响应初始质询之后，如果请求方节点随时间推移继续正确地响应一个或多个连续质询，则后续质询之间的间隔可增大。此外，如果认证方节点和／或 IoT 网络中的其它节点根据先前交互而信任请求方节点，则请求方节点可被准予对受控资源的接入而无需正确地响应质询。替换地，如果请求方节点随时间推移继续向一个或多个连续质询提供不正确的响应，则请求方节点可被阻止接入受控资源或者从 IoT 网络中被完全禁止。

[0013] 根据另一示例性方面，本文所公开的信任启发式模型由此可基于随时间推移而发生的连续质询和响应交换来对 IoT 网络中的两个或更多个节点之间的信任进行建模。此外，该信任可按照类似于人可根据熟人、同事、朋友、密友等来对与其他人的关系进行分类的方式以不同等级来建模，其中对受控资源的接入可沿相似路径对准以允许 IoT 网络中的节点对信任进行建模。例如，信任启发式模型可包括请求方节点可被允许进入 IoT 网络和／或被允许使消息在 IoT 网络内转发或以其他方式中继的未知信任等级，请求方节点可被允许接入丰富或无限资源的初步信任等级，请求方节点可被允许接入受限、受约束或其它有限资源的受信任等级、请求方节点可被允许接入受保护资源的信赖等级，以及未能正确地响应多个连续质询的请求方节点可从 IoT 网络禁止的不受信任等级。相应地，信任启发式模型通常可具有 N 个信任等级（例如，在以上描述的示例性信任启发式模型中为 5 个）并且节点可基于随时间推移与 IoT 网络中的其它节点和资源的交互而被指派特定信任等级。例如，在一个实施例中，信任启发式逻辑模型中的 N 个信任等级可被定义在特定范围内，并

且特定节点可初始地被指派该范围内的默认信任度量，该默认信任度量随后可随时间推移基于质询和响应交换、与其它节点和资源的交互、或其它合适准则来增大或减小以确定要指派给该节点的恰适信任等级。

[0014] 根据另一示例性方面，一种用于 IoT 网络中的受控资源接入的方法可包括：由请求方节点请求对 IoT 网络中的第一受控资源的接入，其中对该资源的接入可包括周期性地完成认证规程的要求，以及该方法可进一步包括对从第一监督者节点（例如，管控受控资源的管控节点、在请求方节点与管控受控资源的管控节点之间中继消息的中间节点等）接收到的质询消息进行响应，以及响应于对质询消息正确响应而接收所请求的对资源的接入，其中第一监督者节点可响应于请求方节点对一个或多个连续质询消息正确响应而降低周期性地完成认证规程的要求。例如，在一个实施例中，监督者节点可增大在向请求方节点传送后续质询消息之前的间隔以降低周期性地完成认证规程的要求并且由此减少用来交换质询消息以及对其的响应的控制信道上的负载。

[0015] 根据另一示例性方面，该用于 IoT 网络中的受控资源接入的方法可进一步包括：第一监督者节点响应于接收到请求方节点提供对质询消息的不正确响应而降低与请求方节点相关联的信任等级。此外，响应于请求方节点对质询消息不正确地响应并且随时间推移继续对一个或多个连续质询消息不正确地响应，第一监督者节点可临时地阻止请求方节点在 IoT 网络上通信和 / 或永久地禁止请求方节点在 IoT 网络上通信。再进一步，在一个实施例中，响应于 IoT 网络迁移至新的网络接入层，第一监督者节点可根据指派给请求方节点的信任等级来调整周期性地完成认证规程的要求。（例如，具有初步信任等级的节点仍可被发给质询，具有受信任状态的节点可被发给单个质询，并且具有信赖状态的节点可不被发给任何质询）

[0016] 根据另一示例性方面，该用于受控资源接入的方法可进一步包括：向第二监督者节点请求对（例如，在该 IoT 网络或不同 IoT 网络中的）第二受控资源的接入，其中第二监督者节点可仅基于请求方节点与具有同请求方节点的一个或多个先前交互的受信任节点之间的信任等级来确定是否要向请求方节点准予对第二受控资源的接入（例如，不要求请求方节点完成认证规程）。例如，在一个实施例中，与请求方节点相关联的信任等级可包括信任启发式逻辑模型中的 N 个信任等级之一，该信任启发式逻辑模型定义与具有每个相应信任等级的节点相关联的所准许的资源接入。此外，在不同使用情形中，第二受控资源、第二监督者节点和 / 或受信任节点可位于该 IoT 网络或不同 IoT 网络中。

[0017] 根据另一示例性方面，IoT 网络中的受控资源通常可包括：具有等于或超过消耗速率的生产速率的无限资源、或者具有超过生产速率的消耗速率的有限资源。在后一种情形中，其中受控资源包括具有超过生产速率的消耗速率的有限资源，监督者节点可包括具有所分配的对有限资源的接入的中间节点，并且被分配给中间节点的接入可包括中间节点需要的第一部分以及能被供应给一个或多个请求方节点的额外部分。如此，在请求对受控资源的接入时，请求方节点可以联系已被分配对有限资源的接入的一个或多个中间节点以确定向其分配的有限资源的总额外部分，以及响应于确定向其分配的有限资源的总额外部分满足或超过请求方节点需要的有限资源量而请求一个或多个中间节点供应请求方节点需要的有限资源量。在此上下文中，请求方节点可以响应于请求一个或多个中间节点供应请求方节点需要的有限资源量而接收来自一个或多个中间节点的质询消息，以及响应于向

每个中间节点传送对质询消息的正确响应而接收来自一个或多个中间节点的所需要的有限资源量。

[0018] 根据另一示例性方面，一种 IoT 设备可包括：用于请求对 IoT 网络中的受控资源的接入的装置，其中对受控资源的接入可包括周期性地完成认证规程的要求；用于对从监督者节点接收到的质询消息进行响应的装置；以及用于响应于对质询消息正确响应而接收所请求的对受控资源的接入的装置，其中监督者节点可响应于 IoT 设备对一个或多个连续质询消息正确响应而降低周期性地完成认证规程的要求。

[0019] 根据另一示例性方面，一种计算机可读存储介质可具有记录于其上的计算机可执行指令，其中在 IoT 设备上执行该计算机可执行指令可使得该 IoT 设备：请求对 IoT 网络中的受控资源的接入，其中对受控资源的接入可包括周期性地完成认证规程的要求；对从监督者节点接收到的质询消息进行响应；以及响应于对质询消息正确响应而接收所请求的对受控资源的接入，其中监督者节点可响应于 IoT 设备对一个或多个连续质询消息正确响应而降低周期性地完成认证规程的要求。

[0020] 根据另一示例性方面，一种用于控制 IoT 网络中的资源接入的方法可尤其包括：接收来自请求方节点的对 IoT 网络中的受控资源的接入的请求，其中对受控资源的接入包括周期性地完成认证规程的要求；向请求方节点传送质询消息；接收来自请求方节点的对质询消息的响应；以及基于所接收到的对质询消息的响应来确定是否要向请求方节点准予对受控资源的接入，其中可基于所接收到的对质询消息的响应是否正确来调整对请求方节点周期性地完成认证规程的要求。

[0021] 基于附图和详细描述，与本文所公开的用于使用本文所描述的信任启发式模型来减少 IoT 资源接入网中的控制负载相关联的其它目标和优点对本领域的技术人员而言是显而易见的。

[0022] 附图简述

[0023] 对本公开的各方面及其许多伴随优点的更完整领会将因其在参考结合附图考虑的以下详细描述时变得更好理解而易于获得，附图仅出于解说目的被给出而不对本公开构成任何限定，并且其中：

[0024] 图 1A-1E 解说了根据本公开的各方面的无线通信系统的示例性高级系统架构。

[0025] 图 2A 解说了根据本公开的各个方面的示例性物联网 (IoT) 设备，而图 2B 解说了根据本公开的各个方面的示例性无源 IoT 设备。

[0026] 图 3 解说了根据本公开的各个方面的包括被配置成执行功能性的逻辑的示例性通信设备。

[0027] 图 4 解说了根据本公开的各个方面的示例性服务器。

[0028] 图 5 解说了根据本公开的一个方面的可被用来减少 IoT 资源接入网中的控制负载的示例性信任启发式模型。

[0029] 图 6 解说了根据本公开的一个方面的示例性通信场景，其中一个或多个客户端可请求接入 IoT 资源接入网中的受控资源。

[0030] 图 7 解说了根据本公开的一个方面的示例性通信场景，其中 IoT 资源接入网中的控制负载可使用信任启发式模型来减少。

[0031] 图 8 解说了根据本公开的一个方面的示例性方法，IoT 网络中的客户端可执行该

示例性方法以请求对受控资源的接入并基于信任启发式模型来减少与其相关联的控制负载。

[0032] 图 9 解说了根据本公开的一个方面的示例性方法，具有对 IoT 网络中的受控资源的保留接入的中间节点可执行该示例性方法以基于信任启发式模型来减少 IoT 网络中的控制负载。

[0033] 图 10 解说了根据本公开的一个方面的示例性方法，不具有对 IoT 网络中的受控资源的保留接入的中间节点可执行该示例性方法以基于信任启发式模型来减少 IoT 网络中的控制负载。

[0034] 图 11 解说了根据本公开的一个方面的示例性方法，管控对 IoT 网络中的受控资源的接入的节点可执行该示例性方法以基于信任启发式模型来减少 IoT 网络中的控制负载。

[0035] 详细描述

[0036] 在以下描述和相关附图中公开各个方面以展示与其中可使用信任启发式模型来减少物联网 (IoT) 资源接入网中的控制负载的示例性实施例相关的具体示例。替换实施例在相关领域的技术人员阅读本公开之后将是显而易见的，且可被构造并实施，而不背离本文公开的范围或精神。另外，众所周知的元素将不被详细描述或可将被省去以便不模糊本文公开的各方面和实施例的相关细节。

[0037] 措辞“示例性”在本文中用于表示“用作示例、实例或解说”。本文中描述为“示例性”的任何实施例不必被解释为优于或胜过其他实施例。同样，术语“实施例”并不要求所有实施例都包括所讨论的特征、优点、或工作模式。

[0038] 本文使用的术语仅描述了特定实施例并且应该被构想成限定本文公开的任何实施例。如本文所使用的，单数形式的“一”、“一个”和“该”旨在也包括复数形式，除非上下文另有明确指示并非如此。还将理解，术语“包括”、“具有”、“包含”和 / 或“含有”在本文中使用时指定所陈述的特征、整数、步骤、操作、要素、和 / 或组件的存在，但并不排除一个或多个其他特征、整数、步骤、操作、要素、组件和 / 或其群组的存在或添加。

[0039] 此外，许多方面以将由例如计算设备的元件执行的动作序列的方式来描述。将认识到，本文描述的各种动作能由专用电路（例如，专用集成电路 (ASIC)）、由正被一个或多个处理器执行的程序指令、或由这两者的组合来执行。另外，本文描述的这些动作序列可被认为是完全体现在任何形式的计算机可读存储介质内，其内存储有一经执行就将使相关联的处理器执行本文所描述的功能性的相应计算机指令集。因此，本公开的各方面可以用数种不同形式来体现，所有这些形式都已被构想为落在所要求保护的主题内容的范围内。另外，对于本文所描述的诸方面中的每一个方面，任何此类方面的相应形式可在本文中描述为例如“配置成执行所描述的动作的逻辑”。

[0040] 如本文所使用的，术语“物联网设备”（或即“IoT 设备”）可被用于指代具有可寻址接口（例如，网际协议 (IP) 地址、蓝牙标识符 (ID)、近场通信 (NFC) ID 等）并且能在有线或无线连接上向一个或多个其他设备传送信息的任何物体（例如，电器、传感器等）。IoT 设备可具有无源通信接口（诸如快速响应 (QR) 码、射频标识 (RFID) 标签、NFC 标签或类似物）或有源通信接口（诸如调制解调器、收发机、发射机 - 接收机或类似物）。IoT 设备可具有特定属性集（例如，设备状态或状况（诸如该 IoT 设备是开启还是关断、打开还是关闭、空闲还是活跃、可用于任务执行还是繁忙等）、冷却或加热功能、环境监视或记录功能、发光

功能、发声功能等），其可被嵌入到中央处理单元（CPU）、微处理器、ASIC 等中，和 / 或由其控制 / 监视，并被配置用于连接至 IoT 网络（诸如局域自组织网络或因特网）。例如，IoT 设备可包括但不限于：冰箱、烤面包机、烤箱、微波炉、冷冻机、洗碗机、器皿、手持工具、洗衣机、干衣机、炉子、空调、恒温器、电视机、灯具、吸尘器、洒水器、电表、燃气表等，只要这些设备装备有用于与 IoT 网络通信的可寻址通信接口即可。IoT 设备还可包括蜂窝电话、台式计算机、膝上型计算机、平板计算机、个人数字助理（PDA）等等。相应地，IoT 网络可由“传统的”可接入因特网的设备（例如，膝上型或台式计算机、蜂窝电话等）以及通常不具有因特网连通性的设备（例如，洗碗机等）的组合构成。

[0041] 图 1A 解说了根据本公开一方面的无线通信系统 100A 的高级系统架构。无线通信系统 100A 包含多个 IoT 设备，包括电视机 110、室外空调单元 112、恒温器 114、冰箱 116、以及洗衣机和干衣机 118。

[0042] 参照图 1A，IoT 设备 110-118 被配置成在物理通信接口或层（在图 1A 中被示为空中接口 108 和直接有线连接 109）上与接入网（例如，接入点 125）通信。空中接口 108 可遵循无线网际协议（IP），诸如 IEEE 802.11。尽管图 1A 解说了 IoT 设备 110-118 在空中接口 108 上通信，并且 IoT 设备 118 在直接有线连接 109 上通信，但每个 IoT 设备可在有线或无线连接、或这两者上通信。

[0043] 因特网 175 包括数个路由代理和处理代理（出于方便起见未在图 1A 中示出）。因特网 175 是互联的计算机和计算机网络的全球系统，其使用标准网际协议套件（例如，传输控制协议（TCP）和 IP）在不同的设备 / 网络之间通信。TCP/IP 提供了端到端连通性，该连通性指定了数据应当如何被格式化、寻址、传送、路由和在目的地处被接收。

[0044] 在图 1A 中，计算机 120（诸如台式计算机或个人计算机（PC））被示为直接连接至因特网 175（例如在以太网连接或者基于 Wi-Fi 或 802.11 网络上）。计算机 120 可具有到因特网 175 的有线连接，诸如到调制解调器或路由器的直接连接，在一示例中该路由器可对应于接入点 125 自身（例如，对于具有有线和无线连通性两者的 Wi-Fi 路由器）。替换地，并非在有线连接上被连接至接入点 125 和因特网 175，计算机 120 可在空中接口 108 或另一无线接口上被连接至接入点 125，并在空中接口 108 上接入因特网 175。尽管被解说为台式计算机，但计算机 120 可以是膝上型计算机、平板计算机、PDA、智能电话、或类似物。计算机 120 可以是 IoT 设备和 / 或包含用于管理 IoT 网络 / 群（诸如 IoT 设备 110-118 的网络 / 群）的功能性。

[0045] 接入点 125 可例如经由光学通信系统（诸如 FiOS）、电缆调制解调器、数字订户线（DSL）调制解调器等被连接至因特网 175。接入点 125 可使用标准网际协议（例如，TCP/IP）与 IoT 设备 110-120 和因特网 175 通信。

[0046] 参照图 1A，IoT 服务器 170 被示为连接至因特网 175。IoT 服务器 170 可被实现为多个在结构上分开的服务器，或者替换地可对应于单个服务器。在一方面，IoT 服务器 170 是可任选的（如由点线所指示的），并且 IoT 设备 110-120 的群可以是对等（P2P）网络。在此种情形中，IoT 设备 110-120 可在空中接口 108 和 / 或直接有线连接 109 上彼此直接通信。替换或附加地，IoT 设备 110-120 中的一些或所有 IoT 设备可配置有独立于空中接口 108 和直接有线连接 109 的通信接口。例如，如果空中接口 108 对应于 Wi-Fi 接口，则 IoT 设备 110-120 中的一个或多个 IoT 设备可具有蓝牙或 NFC 接口以用于彼此直接通信或者与

其他启用蓝牙或 NFC 的设备直接通信。

[0047] 在对等网络中，服务发现方案可多播节点的存在、它们的能力、和群成员资格。对等设备可基于此信息来建立关联和后续交互。

[0048] 根据本公开的一方面，图 1B 解说了包含多个 IoT 设备的另一无线通信系统 100B 的高级架构。一般而言，图 1B 中示出的无线通信系统 100B 可包括与以上更详细地描述的在图 1A 中示出的无线通信系统 100A 相同和 / 或基本相似的各种组件（例如，各种 IoT 设备，包括被配置成在空中接口 108 和 / 或直接有线连接 109 上与接入点 125 通信的电视机 110、室外空调单元 112、恒温器 114、冰箱 116、以及洗衣机和干衣机 118，直接连接至因特网 175 和 / 或通过接入点 125 连接至因特网 175 的计算机 120，以及可经由因特网 175 来访问的 IoT 服务器 170 等）。如此，出于描述的简洁和方便起见，与图 1B 中示出的无线通信系统 100B 中的某些组件相关的各种细节可在本文中省略，既然上面已关于图 1A 中解说的无线通信系统 100A 提供了相同或类似细节。

[0049] 参照图 1B，无线通信系统 100B 可包括监管者设备 130，其可替换地被称为 IoT 管理器 130 或 IoT 管理器设备 130。如此，在以下描述使用术语“监管者设备”130 的情况下，本领域技术人员将领会，对 IoT 管理器、群主、或类似术语的任何引述可指代监管者设备 130 或提供相同或基本相似功能性的另一物理或逻辑组件。

[0050] 在一个实施例中，监管者设备 130 一般可观察、监视、控制、或以其他方式管理无线通信系统 100B 中的各种其他组件。例如，监管者设备 130 可在空中接口 108 和 / 或直接有线连接 109 上与接入网（例如，接入点 125）通信以监视或管理与无线通信系统 100B 中的各种 IoT 设备 110-120 相关联的属性、活动、或其他状态。监管者设备 130 可具有到因特网 175 的有线或无线连接，以及可任选地到 IoT 服务器 170 的有线或无线连接（被示为点线）。监管者设备 130 可从因特网 175 和 / 或 IoT 服务器 170 获得可被用来进一步监视或管理与各种 IoT 设备 110-120 相关联的属性、活动、或其他状态的信息。监管者设备 130 可以是自立设备或是 IoT 设备 110-120 之一，诸如计算机 120。监管者设备 130 可以是物理设备或在物理设备上运行的软件应用。监管者设备 130 可包括用户接口，其可输出与所监视的关联于 IoT 设备 110-120 的属性、活动、或其他状态相关的信息并接收输入信息以控制或以其他方式管理与其相关联的属性、活动、或其他状态。相应地，监管者设备 130 一般可包括各种组件且支持各种有线和无线通信接口以观察、监视、控制、或以其他方式管理无线通信系统 100B 中的各种组件。

[0051] 图 1B 中示出的无线通信系统 100B 可包括一个或多个无源 IoT 设备 105（与有源 IoT 设备 110-120 形成对比），其可被耦合至无线通信系统 100B 或以其他方式成为其一部分。一般而言，无源 IoT 设备 105 可包括条形码设备、蓝牙设备、射频 (RF) 设备、带 RFID 标签的设备、红外 (IR) 设备、带 NFC 标签的设备、或在短程接口上被查询时可向另一设备提供其标识符和属性的任何其他合适设备。有源 IoT 设备可对无源 IoT 设备的属性变化进行检测、存储、传达、动作等。

[0052] 例如，无源 IoT 设备 105 可包括咖啡杯和橙汁容器，其各自具有 RFID 标签或条形码。橱柜 IoT 设备和冰箱 IoT 设备 116 可各自具有恰适的扫描仪或读卡器，其可读取 RFID 标签或条形码以检测咖啡杯和 / 或橙汁容器无源 IoT 设备 105 何时已经被添加或移除。响应于橱柜 IoT 设备检测到咖啡杯无源 IoT 设备 105 的移除，并且冰箱 IoT 设备 116 检测到

橙汁容器无源 IoT 设备的移除，监管者设备 130 可接收到与在橱柜 IoT 设备和冰箱 IoT 设备 116 处检测到的活动相关的一个或多个信号。监管者设备 130 随后可推断出用户正在用咖啡杯喝橙汁和 / 或想要用咖啡杯喝橙汁。

[0053] 尽管前面将无源 IoT 设备 105 描述为具有某种形式的 RFID 标签或条形码通信接口，但无源 IoT 设备 105 也可包括不具有此类通信能力的一个或多个设备或其他物理对象。例如，某些 IoT 设备可具有恰适的扫描仪或读取器机构，其可检测与无源 IoT 设备 105 相关联的形状、大小、色彩、和 / 或其他可观察特征以标识无源 IoT 设备 105。以此方式，任何合适的物理对象可传达其身份和属性并且成为无线通信系统 100B 的一部分，且通过监管者设备 130 被观察、监视、控制、或以其他方式管理。此外，无源 IoT 设备 105 可被耦合至图 1A 中的无线通信系统 100A 或以其他方式成为其一部分，并且以基本类似的方式被观察、监视、控制、或以其他方式管理。

[0054] 根据本公开的另一方面，图 1C 解说了包含多个 IoT 设备的另一无线通信系统 100C 的高级架构。一般而言，图 1C 中示出的无线通信系统 100C 可包括与以上更详细地描述的分别在图 1A 和 1B 中示出的无线通信系统 100A 和 100B 相同和 / 或基本相似的各种组件。如此，出于描述的简洁和方便起见，与图 1C 中示出的无线通信系统 100C 中的某些组件相关的各种细节可在本文中省略，既然上面已关于分别在图 1A 和 1B 中解说的无线通信系统 100A 和 100B 提供了相同或类似细节。

[0055] 图 1C 中示出的通信系统 100C 解说了 IoT 设备 110-118 与监管者设备 130 之间的示例性对等通信。如图 1C 中所示，监管者设备 130 在 IoT 监管者接口上与 IoT 设备 110-118 中的每一个 IoT 设备通信。此外，IoT 设备 110 和 114 彼此直接通信，IoT 设备 112、114 和 116 彼此直接通信，以及 IoT 设备 116 和 118 彼此直接通信。

[0056] IoT 设备 110-118 组成 IoT 群 160。IoT 设备群 160 是本地连接的 IoT 设备（诸如连接至用户的家庭网络的 IoT 设备）的群。尽管未示出，但多个 IoT 设备群可经由连接至因特网 175 的 IoT 超级代理 140 来彼此连接和 / 或通信。在高层级，监管者设备 130 管理群内通信，而 IoT 超级代理 140 可管理群间通信。尽管被示为分开的设备，但监管者设备 130 和 IoT 超级代理 140 可以是相同设备或驻留在相同设备上（例如，自立设备或 IoT 设备，诸如图 1A 中示出的计算机 120）。替换地，IoT 超级代理 140 可对应于或包括接入点 125 的功能性。作为又一替换，IoT 超级代理 140 可对应于或包括 IoT 服务器（诸如 IoT 服务器 170）的功能性。IoT 超级代理 140 可封装网关功能性 145。

[0057] 每个 IoT 设备 110-118 可将监管者设备 130 视为对等方并且向监管者设备 130 传送属性 / 模式更新。当 IoT 设备需要与另一 IoT 设备通信时，它可向监管者设备 130 请求指向该 IoT 设备的指针，并且随后作为对等方与该目标 IoT 设备通信。IoT 设备 110-118 使用共用消息接发协议 (CMP) 在对等通信网络上彼此通信。只要两个 IoT 设备都启用了 CMP 并且通过共用通信传输来连接，它们就可彼此通信。在协议栈中，CMP 层 154 在应用层 152 之下并在传输层 156 和物理层 158 之上。

[0058] 根据本公开的另一方面，图 1D 解说了包含多个 IoT 设备的另一无线通信系统 100D 的高级架构。一般而言，图 1D 中示出的无线通信系统 100D 可包括与以上更详细地描述的分别在图 1A-C 中示出的无线通信系统 100A-C 相同和 / 或基本相似的各种组件。如此，出于描述的简洁和方便起见，与图 1D 中示出的无线通信系统 100D 中的某些组件相关的各种

细节可在本文中省略，既然上面已关于分别在图 1A-C 中解说的无线通信系统 100A-C 提供了相同或类似细节。

[0059] 因特网 175 是可使用 IoT 概念来管控的“资源”。然而，因特网 175 仅仅是被管控的资源的一个示例，并且任何资源可使用 IoT 概念来管控。可被管控的其他资源包括但不限于电力、燃气、存储、安全性等。IoT 设备可被连接至该资源并由此管控它，或者该资源可在因特网 175 上被管控。图 1D 解说了若干资源 180，诸如天然气、汽油、热水、以及电力，其中资源 180 可作为因特网 175 的补充和 / 或在因特网 175 上被管控。

[0060] IoT 设备可彼此通信以管控它们对资源 180 的使用。例如，IoT 设备（诸如烤面包机、计算机、和吹风机）可在蓝牙通信接口上彼此通信以管控它们对电力（资源 180）的使用。作为另一示例，IoT 设备（诸如台式计算机、电话、和平板计算机）可在 Wi-Fi 通信接口上通信以管控它们对因特网 175（资源 180）的接入。作为又一示例，IoT 设备（诸如炉子、干衣机、和热水器）可在 Wi-Fi 通信接口上通信以管控它们对燃气的使用。替换或附加地，每个 IoT 设备可被连接至 IoT 服务器（诸如 IoT 服务器 170），该服务器具有用于基于从各 IoT 设备接收到的信息来管控它们对资源 180 的使用的逻辑。

[0061] 根据本公开的另一方面，图 1E 解说了包含多个 IoT 设备的另一无线通信系统 100E 的高级架构。一般而言，图 1E 中示出的无线通信系统 100E 可包括与以上更详细地描述的分别在图 1A-D 中示出的无线通信系统 100A-D 相同和 / 或基本相似的各种组件。如此，出于描述的简洁和方便起见，与图 1E 中示出的无线通信系统 100E 中的某些组件相关的各种细节可在本文中省略，既然上面已关于分别在图 1A-D 中解说的无线通信系统 100A-D 提供了相同或类似细节。

[0062] 通信系统 100E 包括两个 IoT 设备群 160A 和 160B。多个 IoT 设备群可经由连接至因特网 175 的 IoT 超级代理彼此连接和 / 或通信。在高层级，IoT 超级代理可管理各 IoT 设备群之间的群间通信。例如，在图 1E 中，IoT 设备群 160A 包括 IoT 设备 116A、122A 和 124A 以及 IoT 超级代理 140A，而 IoT 设备群 160B 包括 IoT 设备 116B、122B 和 124B 以及 IoT 超级代理 140B。如此，IoT 超级代理 140A 和 140B 可连接至因特网 175 并通过因特网 175 彼此通信，和 / 或彼此直接通信以促成 IoT 设备群 160A 与 160B 之间的通信。此外，尽管图 1E 解说了两个 IoT 设备群 160A 和 160B 经由 IoT 超级代理 140A 和 140B 彼此通信，但本领域技术人员将领会，任何数目的 IoT 设备群可合适地使用 IoT 超级代理来彼此通信。

[0063] 在图 1A-E 中分别示出的示例性无线通信系统 100A-100E 中，IoT 服务器 170 和 / 或监管者设备 130 可将各种 IoT 设备 110-120 和 / 或无源 IoT 设备 105 组织成一个或多个小型且相关的 IoT 设备群 160 以启用 IoT 设备群 160 内和 / 或之间的共享资源 180（例如，以控制与可在 IoT 设备群 169 中的 IoT 设备 110-120 和 / 或无源 IoT 设备 105 之间共享的各种资源 180 相关联的使用）。例如，在一个实施例中，IoT 服务器 170 和 / 或监管者设备 130 可提供分布式网络服务（例如，云服务），其可用因设备而异的全球唯一性标识符（例如，D_GUID）和因群而异的全球唯一性标识符（例如，G_GUID）来表示无线通信系统 100A-100E 中的每个 IoT 设备 110-120 和 / 或无源 IoT 设备 105，并且可进一步用因资源而异的全球唯一性标识符（例如，R_GUID）来表示无线通信系统 100A-100E 中每个共享的资源 180。相应地，D_GUID、G_GUID 和 R_GUID 可被用来控制或以其他方式协调在特定 IoT 设备群 160 内和 / 或各种不同 IoT 设备群 160 之间共享资源 180。

[0064] 例如，在图 1A-E 中所示的示例性无线通信系统 100A-100E 中，IoT 服务器 170 和 / 或监管者设备 130 可置备有表示各种 IoT 设备 110-120 和 / 或无源 IoT 设备 150 的一个或多个 D_GUID。另外，响应于新设备上电或者以其他方式在连接至 IoT 网络之后向 IoT 服务器 170 和 / 或监管者设备 130 注册，可向该新设备分配新的 D_GUID 以允许该新设备被联系到，并且各种属性可与分配给该新设备的 D_GUID 相关联（例如，描述、位置、类型等）。在一个实施例中，IoT 服务器 170 和 / 或监管者设备 130 可进一步置备有对应于在 IoT 网络内共享的资源 180 的 R_GUID 以及可能需要对哪些设备操作或以其他方式与其交互。例如，资源 180 通常可包括水、电力、阳光、道路、食物或任何其他合适的资源 180，其可根据与资源 180 相关联的位置、家庭或其他合适的属性在上下文内被唯一性地标识。此外，IoT 服务器 170 和 / 或监管者设备 130 可置备有 G_GUID，其表示一起工作的每个 IoT 设备群 160（例如，在家庭中，草地洒水器、热水器、冰箱、浴缸等可以全部对共享水资源 180 进行操作）。G_GUID 可进一步包括各种属性，这些属性定义与 IoT 设备群 160（例如，家庭、位置、所有者等）相关联的上下文以及在其中共享的资源 180。在一个实施例中，IoT 服务器 170 和 / 或监管者设备 130 可进一步置备有各种策略，用以定义各种 IoT 设备 110-120 和无源 IoT 设备 105 之中的层次、级别、优先级或其他关系，以及它们被分配的 IoT 设备群 160、在其中共享的资源 180 以及用以控制争用对资源 180 的接入的任何策略。

[0065] 在一个实施例中，响应于已合适地使 IoT 服务器 170 和 / 或监管者设备 130 置备有各种 D_GUID、G_GUID、R_GUID 和策略，IoT 服务器 170 和 / 或监管者设备 130 随后可发现各种 IoT 设备群 160 和藉以共享的各种资源 180。例如，在一个实施例中，R_GUID 可被静态地置备给一个或多个 D_GUID 或以其他方式与一个或多个 D_GUID 相关联，该一个或多个 D_GUID 对应于要求接入某共享资源 180 的设备。在另一示例中，希望接入某共享资源 180 的设备可基于与其相关联的位置、描述或其他合适的属性来查询 IoT 服务器 170 和 / 或监管者设备 130，并且该设备随后可从 IoT 服务器 170 和 / 或监管者设备 130 返回给设备的列表中选择恰适的资源 180。再进一步，在一个实施例中，一个或多个资源 180 可用 RFID、条形码或者 IoT 设备 110-120 可读取以动态发现资源 180 的其他合适数据加标签。此外，在一个实施例中，IoT 服务器 170 和 / 或监管者设备 130 可采用查询机制基于上下文或者输入至合适用户接口的信息来发现 IoT 设备群 160（例如，与两个 IoT 设备群 160 相关联的各所有者可交换 G_GUID 以发起这两个 IoT 设备群 160 之间的交互）。在另一示例中，基于置备给 IoT 服务器 170 和 / 或监管者设备 130 的许可、规则或其他策略，两个或更多个 IoT 设备群 160 可永久或临时地合并以使得两个或更多个 IoT 设备群 160 能够使用在每个 IoT 设备群内共享的资源 180。此外，如以下进一步详细描述的，可在无线通信系统 100A-100E 中实现信任启发式模型以确保请求接入共享资源 180 的 IoT 设备具有正确的认证凭证、解决对同一共享资源 180 的竞争请求、或者以可减少与管控对共享资源 180 的接入相关联的控制负载的方式另行控制对共享资源 180 的接入。

[0066] 图 2A 解说了根据本公开各方面的 IoT 设备 200A 的高级示例。尽管外观和 / 或内部组件在各 IoT 设备之间可能显著不同，但大部分 IoT 设备将具有某种类别的用户接口，该用户接口可包括显示器和用于用户输入的装置。可在有线或无线网络上与没有用户接口（诸如图 1A、1B 和 1D 的空中接口 108）的 IoT 设备远程地通信。

[0067] 如图 2A 中所示，在关于 IoT 设备 200A 的示例配置中，IoT 设备 200A 的外壳可配

置有显示器 226、电源按钮 222、以及两个控制按钮 224A 和 224B、以及其他组件，如本领域已知的。显示器 226 可以是触摸屏显示器，在此情形中控制按钮 224A 和 224B 可以不是必需的。尽管未被明确地示为 IoT 设备 200A 的一部分，但 IoT 设备 200A 可包括一个或多个外部天线和 / 或被构建到外壳中的一个或多个集成天线，包括但不限于 Wi-Fi 天线、蜂窝天线、卫星定位系统 (SPS) 天线 (例如，全球定位系统 (GPS) 天线)，等等。

[0068] 尽管 IoT 设备 (诸如 IoT 设备 200A) 的内部组件可使用不同硬件配置来实施，但内部硬件组件的基本高级配置在图 2A 中被示为平台 202。平台 202 可接收和执行在网络接口 (例如图 1A、1B 和 1D 中的空中接口 108) 和 / 或有线接口上传送的软件应用、数据和 / 或命令。平台 202 还可独立地执行本地存储的应用。平台 202 可包括被配置用于有线和 / 或无线通信的一个或多个收发机 206(例如，Wi-Fi 收发机、蓝牙收发机、蜂窝收发机、卫星收发机、GPS 或 SPS 接收机等)，其可操作地耦合至一个或多个处理器 208，诸如微控制器、微处理器、专用集成电路、数字信号处理器 (DSP)、可编程逻辑电路、或其他数据处理设备，其将一般性地被称为处理器 208。处理器 208 可执行 IoT 设备的存储器 212 内的应用编程指令。存储器 212 可包括只读存储器 (ROM)、随机存取存储器 (RAM)、电可擦除可编程 ROM(EEPROM)、闪存卡、或计算机平台通用的任何存储器中的一者或多者。一个或多个输入 / 输出 (I/O) 接口 214 可被配置成允许处理器 208 与各种 I/O 设备 (诸如所解说的显示器 226、电源按钮 222、控制按钮 224A 和 224B，以及任何其他设备，诸如与 IoT 设备 200A 相关联的传感器、致动器、中继、阀、开关等) 通信并从其进行控制。

[0069] 相应地，本公开的一方面可包括含有执行本文描述的功能的能力的 IoT 设备 (例如，IoT 设备 200A)。如将由本领域技术人员领会的，各种逻辑元件可在分立元件、处理器 (例如，处理器 208) 上执行的软件模块、或软件与硬件的任何组合中实施以达成本文公开的功能性。例如，收发机 206、处理器 208、存储器 212、和 I/O 接口 214 可以全部协作地用来加载、存储和执行本文公开的各种功能，并且用于执行这些功能的逻辑因此可分布在各种元件上。替换地，该功能性可被纳入到一个分立的组件中。因此，图 2A 中的 IoT 设备 200A 的特征将仅被视为解说性的，且本公开不被限定于所解说的特征或安排。

[0070] 图 2B 解说了根据本公开各方面的无源 IoT 设备 200B 的高级示例。一般而言，图 2B 中示出的无源 IoT 设备 200B 可包括与以上更详细地描述的在图 2A 中示出的 IoT 设备 200A 相同和 / 或基本相似的各种组件。如此，出于描述的简洁和方便起见，与图 2B 中示出的无源 IoT 设备 200B 中的某些组件相关的各种细节可在本文中省略，既然上面已关于图 2A 中解说的 IoT 设备 200A 提供了相同或类似细节。

[0071] 图 2B 中示出的无源 IoT 设备 200B 一般可不同于图 2A 中示出的 IoT 设备 200A，不同之处在于无源 IoT 设备 200B 可不具有处理器、内部存储器、或某些其他组件。替代地，在一个实施例中，无源 IoT 设备 200B 可仅包括 I/O 接口 214 或者允许无源 IoT 设备 200B 在受控 IoT 网络内被观察、监视、控制、管理、或以其他方式知晓的其他合适的机构。例如，在一个实施例中，与无源 IoT 设备 200B 相关联的 I/O 接口 214 可包括条形码、蓝牙接口、射频 (RF) 接口、RFID 标签、IR 接口、NFC 接口、或者在短程接口上被查询时可向另一设备 (例如，有源 IoT 设备 (诸如 IoT 设备 200A)，其可对关于与无源 IoT 设备 200B 相关联的属性的信息进行检测、存储、传达、动作、或以其他方式处理) 提供与无源 IoT 设备 200B 相关联的标识符和属性的任何其他合适的 I/O 接口。

[0072] 尽管前面将无源 IoT 设备 200B 描述为具有某种形式的 RF、条形码、或其他 I/O 接口 214，但无源 IoT 设备 200B 可包括不具有此类 I/O 接口 214 的设备或其他物理对象。例如，某些 IoT 设备可具有恰适的扫描仪或读取器机构，其可检测与无源 IoT 设备 200B 相关联的形状、大小、色彩、和 / 或其他可观察特征以标识无源 IoT 设备 200B。以此方式，任何合适的物理对象可传达其身份和属性并且在受控 IoT 网络内被观察、监视、控制、或以其他方式被管理。

[0073] 图 3 解说了包括配置成执行功能性的逻辑的通信设备 300。通信设备 300 可对应于以上提及的通信设备中的任一者，包括但不限于 IoT 设备 110-120、IoT 设备 200A、耦合至因特网 175 的任何组件（例如，IoT 服务器 170）等等。因此，通信设备 300 可对应于被配置成在图 1A-E 的无线通信系统 100A-E 上与一个或多个其它实体通信（或促成与一个或多个其它实体的通信）的任何电子设备。

[0074] 参照图 3，通信设备 300 包括配置成接收和 / 或传送信息的逻辑 305。在一示例中，如果通信设备 300 对应于无线通信设备（例如，IoT 设备 200A 和 / 或无源 IoT 设备 200B），则配置成接收和 / 或传送信息的逻辑 305 可包括无线通信接口（例如，蓝牙、WiFi、Wi-Fi 直连、长期演进 (LTE) 直连等），诸如无线收发机和相关联的硬件（例如，RF 天线、调制解调器、调制器和 / 或解调器等）。在另一示例中，配置成接收和 / 或传送信息的逻辑 305 可对应于有线通信接口（例如，串行连接、USB 或火线连接、可藉以接入因特网 175 的以太网连接等）。因此，如果通信设备 300 对应于某种类型的基于网络的服务器（例如，应用 170），则配置成接收和 / 或传送信息的逻辑 305 在一示例中可对应于以太网卡，该以太网卡经由以太网协议将基于网络的服务器连接至其它通信实体。在进一步示例中，配置成接收和 / 或传送信息的逻辑 305 可包括传感或测量硬件（例如，加速计、温度传感器、光传感器、用于监视本地 RF 信号的天线等），通信设备 300 可藉由该传感或测量硬件来监视其本地环境。配置成接收和 / 或传送信息的逻辑 305 还可包括在被执行时准许配置成接收和 / 或传送信息的逻辑 305 的相关联硬件执行其接收和 / 或传送功能的软件。然而，配置成接收和 / 或传送信息的逻辑 305 不单单对应于软件，并且配置成接收和 / 或传送信息的逻辑 305 至少部分地依赖于硬件来实现其功能性。

[0075] 参照图 3，通信设备 300 进一步包括配置成处理信息的逻辑 310。在一示例中，配置成处理信息的逻辑 310 可至少包括处理器。可由配置成处理信息的逻辑 310 执行的处理类型的示例实现包括但不限于执行确定、建立连接、在不同信息选项之间作出选择、执行与数据有关的评价、与耦合至通信设备 300 的传感器交互以执行测量操作、将信息从一种格式转换为另一种格式（例如，在不同协议之间转换，诸如，.wmv 到 .avi 等），等等。例如，包括在配置成处理信息的逻辑 310 中的处理器可对应于被设计成执行本文描述功能的通用处理器、DSP、ASIC、现场可编程门阵列 (FPGA) 或其他可编程逻辑器件、分立的门或晶体管逻辑、分立的硬件组件、或其任何组合。通用处理器可以是微处理器，但在替换方案中，该处理器可以是任何常规的处理器、控制器、微控制器、或状态机。处理器还可以被实现为计算设备的组合（例如 DSP 与微处理器的组合、多个微处理器、与 DSP 核协作的一个或多个微处理器、或任何其他此类配置）。配置成处理信息的逻辑 310 还可包括在被执行时准许配置成处理信息的逻辑 310 的相关联硬件执行其处理功能的软件。然而，配置成处理信息的逻辑 310 不单单对应于软件，并且配置成处理信息的逻辑 310 至少部分地依赖于硬件来实现

其功能性。

[0076] 参照图 3，通信设备 300 进一步包括配置成存储信息的逻辑 315。在一示例中，配置成存储信息的逻辑 315 可至少包括非瞬态存储器和相关联的硬件（例如，存储器控制器等）。例如，包括在配置成存储信息的逻辑 315 中的非瞬态存储器可对应于 RAM、闪存、ROM、可擦除式可编程 ROM(EPROM)、EEPROM、寄存器、硬盘、可移动盘、CD-ROM、或本领域中已知的任何其他形式的存储介质。配置成存储信息的逻辑 315 还可包括在被执行时准许配置成存储信息的逻辑 315 的相关联硬件执行其存储功能的软件。然而，配置成存储信息的逻辑 315 不单单对应于软件，并且配置成存储信息的逻辑 315 至少部分地依赖于硬件来实现其功能性。

[0077] 参照图 3，通信设备 300 进一步可任选地包括配置成呈现信息的逻辑 320。在一示例中，配置成呈现信息的逻辑 320 可至少包括输出设备和相关联的硬件。例如，输出设备可包括视频输出设备（例如，显示屏、能承载视频信息的端口，诸如 USB、HDMI 等）、音频输出设备（例如，扬声器、能承载音频信息的端口，诸如话筒插孔、USB、HDMI 等）、振动设备和 / 或信息可此被格式化以供输出或实际上由通信设备 300 的用户或操作者输出的任何其它设备。例如，如果通信设备 300 对应于如图 2A 中所示的 IoT 设备 200A 和 / 或如图 2B 中所示的无源 IoT 设备 200B，则被配置成呈现信息的逻辑 320 可包括显示器 226。在进一步示例中，对于某些通信设备（诸如不具有本地用户的网络通信设备（例如，网络交换机或路由器、远程服务器等））而言，配置成呈现信息的逻辑 320 可被省略。配置成呈现信息的逻辑 320 还可包括在被执行时准许配置成呈现信息的逻辑 320 的相关联硬件执行其呈现功能的软件。然而，配置成呈现信息的逻辑 320 不单单对应于软件，并且配置成呈现信息的逻辑 320 至少部分地依赖于硬件来实现其功能性。

[0078] 参照图 3，通信设备 300 进一步可任选地包括配置成接收本地用户输入的逻辑 325。在一示例中，配置成接收本地用户输入的逻辑 325 可至少包括用户输入设备和相关联的硬件。例如，用户输入设备可包括按钮、触摸屏显示器、键盘、相机、音频输入设备（例如，话筒或可携带音频信息的端口，诸如话筒插孔等）、和 / 或可用来从通信设备 300 的用户或操作者接收信息的任何其它设备。例如，如果通信设备 300 对应于如图 2A 中所示的 IoT 设备 200A 和 / 或如图 2B 中所示的无源 IoT 设备 200B，则配置成接收本地用户输入的逻辑 325 可包括按钮 222、224A 和 224B、显示器 226（在触摸屏的情况下），等等。在进一步示例中，对于某些通信设备（诸如不具有本地用户的网络通信设备（例如，网络交换机或路由器、远程服务器等））而言，配置成接收本地用户输入的逻辑 325 可被省略。配置成接收本地用户输入的逻辑 325 还可包括在被执行时准许配置成接收本地用户输入的逻辑 325 的相关联硬件执行其输入接收功能的软件。然而，配置成接收本地用户输入的逻辑 325 不单单对应于软件，并且配置成接收本地用户输入的逻辑 325 至少部分地依赖于硬件来实现其功能性。

[0079] 参照图 3，尽管所配置的逻辑 305 到 325 在图 3 中被示出为分开或相异的块，但将领会，相应各个所配置的逻辑藉以执行其功能性的硬件和 / 或软件可部分交迭。例如，用于促成所配置的逻辑 305 到 325 的功能性的任何软件可被存储在与配置成存储信息的逻辑 315 相关联的非瞬态存储器中，从而所配置的逻辑 305 到 325 各自部分地基于由配置成存储信息的逻辑 315 所存储的软件的操作来执行其功能性（即，在这一情形中为软件执行）。同样地，直接与所配置的逻辑之一相关联的硬件可不时地被其它所配置的逻辑借用或使用。

例如，配置成处理信息的逻辑 310 的处理器可在数据由配置成接收和 / 或传送信息的逻辑 305 传送之前将此数据格式化为恰适格式，从而配置成接收和 / 或传送信息的逻辑 305 部分地基于与配置成处理信息的逻辑 310 相关联的硬件（即，处理器）的操作来执行其功能性（即，在这一情形中为数据传输）。

[0080] 一般而言，除非另外明确声明，如贯穿本公开所使用的短语“配置成……的逻辑”旨在调用至少部分用硬件实现的方面，而并非旨在映射到独立于硬件的仅软件实现。同样，将领会，各个框中的所配置的逻辑或“配置成……的逻辑”并不限于具体的逻辑门或元件，而是一般地指代执行本文描述的功能性的能力（经由硬件或硬件和软件的组合）。因此，尽管共享措词“逻辑”，但如各个框中所解说的所配置的逻辑或“配置成……的逻辑”不必被实现为逻辑门或逻辑元件。从以下更详细地描述的各方面的概览中，各个框中的逻辑之间的其它交互或协作将对本领域普通技术人员而言变得清楚。

[0081] 各个实施例可以在市售的服务器设备（诸如图 4 中解说的服务器 400）中的任一个上实现。在一示例中，服务器 400 可对应于上述 IoT 服务器 170 的一个示例配置。在图 4 中，服务器 400 包括耦合至易失性存储器 402 和大容量非易失性存储器（诸如盘驱动器 403）的处理器 401。服务器 400 还可包括耦合至处理器 401 的软盘驱动器、压缩碟 (CD) 或 DVD 碟驱动器 406。服务器 400 还可包括耦合至处理器 401 的用于建立与网络 407（诸如耦合至其他广播系统计算机和服务器或耦合至因特网的局域网）的数据连接的网络接入端口 404。在图 3 的上下文中，将领会，图 4 的服务器 400 解说了通信设备 300 的一个示例实现，藉此配置成传送和 / 或接收信息的逻辑 305 对应于由服务器 400 用来与网络 407 通信的网络接入点 404，配置成处理信息的逻辑 310 对应于处理器 401，而配置成存储信息的逻辑 315 对应于易失性存储器 402、盘驱动器 403 和 / 或碟驱动器 406 的任何组合。配置成呈现信息的可任选逻辑 320 和配置成接收本地用户输入的可任选逻辑 325 未在图 4 中明确示出，并且可以被或可以不被包括在其中。因此，图 4 帮助表明除了如图 2A 中的 IoT 设备实现之外，通信设备 300 还可被实现为服务器。

[0082] 一般而言，如以上所提及的，IoT 技术的持续增进的发展将导致住宅中用户周围、车辆中、工作中、和许多其它位置处的众多 IoT 设备，由此许多 IoT 网络可实现控制机制以认证或以其他方式管控对不同 IoT 设备可能想要接入的受控资源的接入。更具体而言，该控制机制可被用来确保请求接入受控资源的 IoT 设备具有恰适的认证凭证、解决对同一共享资源的竞争请求、或者以其他方式控制资源接入。例如，可使用 IoT 概念来管控的示例性资源可包括网络接入、电力、燃气、存储、安全性、天然气、汽油、热水或者 IoT 设备可能要求接入的任何其它合适的计算、物理或逻辑资源。相应地，由于 IoT 网络中用来管控对受控资源的接入的控制信道上的额外话务可能潜在地中断与受控资源相关联的使用（例如，如果各个设备通过控制信道通信以接入受控资源），因此本文进一步详细描述的方面和实施例可使用信任启发式模型来减少与管控对 IoT 网络中的受控资源的接入相关联的控制负载。

[0083] 更具体地，根据本公开的一个方面，图 5 解说了可被用来减少 IoT 资源接入网中的控制负载的示例性信任启发式模型 500。在一个实施例中，信任启发式模型 500 可以基于在想要接入受控资源（例如，资源 A、资源 B、资源 Z 等）的请求方节点与管控受控资源或充当在请求方节点与管控受控资源的节点之间中继接入的中介（例如，如果请求方节点不具有允许与管控节点直接联系的通信射程）的认证方节点之间使用的质询和响应机制。例如，

响应于从请求方节点接收到接入受控资源的请求，认证方节点可向请求方节点发送质询并且基于对质询的响应来确定是否要向请求方节点准予对受控资源的接入（例如，对质询的正确响应可取决于请求方节点具有可被用来基于口令、通用认证证书、或其它共享机密来验证信任的一个或多个凭证）。如此，认证方节点通常可在请求方节点对质询正确地响应的情况下向请求方节点准予对受控资源的接入，或者替换地在请求方节点提供对质询的不正确响应的情况下拒绝请求方节点接入受控资源。此外，认证方节点可基于对初始质询的响应是否正确来向请求方节点指派恰适的信任等级，并且被指派给请求方节点的信任等级可以基于连续质询和响应交换和 / 或与 IoT 网络中的其它节点的交互来动态更新。

[0084] 具体而言，常规质询和响应机制通常可以规则的间隔重复以确保在对质询的初始正确响应之后的时间内没有什么改变并且周期性地重新认证请求方节点，这可因控制信道上的额外话务而占据不必要的带宽并且降低性能（例如，在无线系统中）。相反，图 5 中所示的信任启发式模型 500 可被用来减少与质询和响应交换相关联的控制负载或者可以其它方式用来控制资源接入的其它话务。例如，在一个实施例中，认证方节点可响应于从请求方节点接收到接入受控资源的请求而向请求方接入发出初始质询，并且如果请求方节点对一个或多个连续质询正确响应，则后续质询之间的间隔可随后增大。此外，如果认证方节点和 / 或 IoT 网络中的其它节点根据先前的交互而信任请求方节点，则认证方节点可向请求方节点准予对受控资源的接入而无需采用质询和响应机制，或者替换地，如果请求方节点对一个或多个连续质询提供不正确的响应，则认证方节点可阻止请求方节点接入受控资源或从 IoT 网络中完全禁止请求方节点。

[0085] 相应地，信任启发式模型 500 可被用来基于随时间推移而发生的连续质询和响应交换来对 IoT 网络中的两个或更多个节点和 / 或不同 IoT 网络中的两个或更多个节点之间的信任进行建模。此外，该信任可按照类似于人可根据熟人、同事、朋友、密友等来对与其他人的关系进行分类的方式以不同等级进行建模，其中对受控资源的接入可沿相似路径对准以允许 IoT 网络中的节点和 / 或不同 IoT 网络中的节点对信任进行建模。例如，参照图 5，信任启发式模型 500 可包括请求方节点可被允许进入 IoT 网络和 / 或被允许使消息在 IoT 网络内转发或以其他方式中继的未知信任等级 510，请求方节点可被允许接入丰富或无限资源（例如，电力）的初步信任等级 520，请求方节点可被允许接入受限、受约束或其它有限资源（例如，Wi-Fi 带宽）的受信任等级 530、请求方节点可被允许接入受保护资源（例如，数据库记录）的信赖等级 540，以及未能正确响应多个连续质询的请求方节点可从 IoT 网络中禁止的不受信任等级 550。相应地，信任启发式模型 500 通常可具有 N 个信任等级（例如，在图 5 中所示的示例性信任启发式模型 500 中为 5 个）并且节点可基于随时间推移与 IoT 网络中的其它节点和资源的交互而被指派特定的信任等级。例如，在一个实施例中，信任启发式模型 500 中的 N 个信任等级可被定义在特定范围（例如，从 -100 到 +100）内，并且特定节点可初始地被指派零 (0) 信任度量，该信任度量可以随后可随时间推移基于质询和响应交换、与其它节点和资源的交互、或其它合适准则来增大或减小以确定要指派给该节点的恰适信任等级。

[0086] 例如，参照图 5，节点 _ 新在新引入到 IoT 网络之后可初始地具有未知信任等级 510，而节点 _abc 和节点 _def 可基于正确地响应来自认证方节点的初始质询而具有初步信任等级 520 并且被允许接入丰富资源 A。此外，节点 _klm 和节点 _nop 在正确地响应连续

质询之后可被指派受信任等级 530 并且除丰富资源 A 之外还被允许接入受限资源 B，并且节点 _klm 和节点 _nop 被要求响应连续质询之前的间隔可被增大。再进一步，节点 _xyz 在提供对连续质询的进一步正确响应之后可被指派信赖信任等级 540 并且除受限资源 B 和丰富资源 A 之外还被允许接入受保护资源 B，并且节点 _xyz 将被要求响应另一质询之前的间隔可被进一步增大或者响应另一质询的要求可被完全消除。然而，节点 _ 坏可能尚未能正确响应一个或多个质询，从而导致节点 _ 坏具有不受信任状态 550，由此节点 _ 坏可被禁止在 IoT 网络上通信达某一时段或者完全从 IoT 网络中禁止，以使得获授权节点可忽略来自节点 _ 坏的话务并由此避免因节点 _ 坏潜在地使控制信道充满垃圾数据而对 IoT 网络造成的中断（例如，以阻止垃圾邮件、暴力破解攻击、拒绝服务攻击等）。

[0087] 在另一实施例中，图 5 中所示的信任启发式模型 500 可被用来管控不同连接机制上的连接。具体而言，如以上关于图 1D 描述的，IoT 服务器 170 可管控具有或不具有因特网 175 情况下的连接。如此，如果图 5 中管制的下层网络迁移到新的网络接入层，则可基于在前经验而存在关于不同节点的不同行为。例如，在一个实施例中，迁移可以是所有节点从某一蜂窝接口改变成 Wi-Fi 接口的情形。在另一示例中，迁移可以是从一个 Wi-Fi 接口到另一 Wi-Fi 接口（例如，从 802.11a 接口到 802.11n 接口）的改变。在任何情形中，基于网络中发生的迁移或切换情景，图 5 中所示的信任启发式模型 500 可为具有不同信任等级的节点提供不同行为。例如，具有初步信任等级 520 的节点（例如，节点 _abc 和节点 _def）仍可被发给质询，具有受信任状态 530 的节点（例如，节点 _klm 和节点 _nop）可被发给单个质询，并且具有信赖状态 540 的节点（例如，节点 _xyz）可不被发给任何质询。如此，可响应于 IoT 网络迁移到新的网络接入层而根据信任启发式模型 500 中被指派给不同节点的信任等级来调整周期性地完成成功的质询和响应交换或另一合适的认证规程的要求。

[0088] 根据本公开的一个方面，图 6 解说了其中客户端 IoT 设备可请求接入 IoT 网络中的受控资源的某些示例性通信场景，而图 7 解说了其中 IoT 网络中的控制负载可使用本文所公开的信任启发式模型来减少的某些示例性通信场景。如图 6 和 / 或图 7 中所示且在本文中所使用的，术语“节点 R”通常可指代 IoT 网络中的受控资源，术语“节点 A”通常可指代想要保留对受控资源节点 R 的接入的客户端 IoT 设备，术语“节点 B”通常可指代 IoT 网络中管控对受控资源节点 R 的接入的节点，术语“节点 C”通常可指代已具有对受控资源节点 R 的保留接入的中间节点，术语“节点 D”通常可指代不具有对受控资源节点 R 的保留接入的中间节点，并且术语“节点 T”通常可指代具有与节点 A 的先前交互的节点，该先前交互可被用来对与节点 A 相关联的一个或多个信任关系进行建模。

[0089] 在一个实施例中，如本文将进一步详细描述的，IoT 网络中的特定节点 R 通常可被认为是有限资源或无限资源，其中用来管控对节点 R 的接入的机制可取决于节点 R 对应于有限资源还是无限资源而变化。更具体地，无限资源通常可具有等于或超过消耗速率的生产速率并且无接入瓶颈（例如，对数据库的访问可被认为是无限的，这是因为访问数据库并不耗尽存储于其中的信息，并且此外还因为可以其它方式限制对数据库的访问的无线带宽可不被认为是数据库处的瓶颈）。

[0090] 相反，有限资源通常可具有超过生产速率的消耗速率、受约束的递送机制、或这两者。例如，发电机产生的电能可被认为是有限资源，因为发电机通常以固定速率产生电能并且所产生的电能被消耗的速率在相当多的客户端接入发电机的时段期间可能超过生产速

率。在另一示例中，具有仅能支持一次记录一个节目的连接的数字录像机 (DVR) 可被认为是具有受约束递送机制的有限资源，因为两个同时的节目无法被记录于其上。在又一示例中，如果用户想要记录三个 DVR 上的节目并且连接仅支持一次记录两个节目而且这些 DVR 上可用的存储容量仅能容纳一个节目，则 DVR 可被认为是具有受限量和受约束递送机制的有限资源。本领域技术人员将领会，以上关于受控资源可被认为是无限的还是有限的概念可被应用于许多其它示例和使用情形。

[0091] 在被用来管控对受控资源的接入的传统接入模式中，特定实体（例如，认证服务器）可以是受控资源的监督者 (gatekeeper) 并且响应于客户端请求接入受控资源而决定是否准许客户端接入该受控资源。然而，在对等 (P2P) 接入模式中，客户端可能无法与监督者实体通信（例如，因为监督者实体未落在与客户端相关联的通信范围内），由此客户端可取而代之与具有对受控资源的接入的中介或边缘节点通信以便通过该中介或边缘节点来接入受控资源。相应地，图 6 中所示的示例性通信情景通常可表示可被用来管控对 IoT 网络中的受控资源的接入的各种传统接入模式和 / 或常规 P2P 接入模式，而与图 7 相关的后续描述可表明本文所描述的信任启发式模型可如何扩增传统接入模式和 / 或常规 P2P 接入模式以减少 IoT 网络中的控制负载。

[0092] 具体而言，图 6 解说了一个示例性通信情景 610，其中客户端节点 A 想要保留对受控资源节点 R 的接入，并且节点 B 管控对受控资源节点 R 的接入。此外，相应的虚线示出彼此相交的与节点 A 和节点 B 相关联的通信范围，由此节点 A 可直接与节点 B 通信并且常规机制可被用来管控对受控资源节点 R 的接入。在一个实施例中，可在节点 A 与节点 B 之间使用质询和响应机制以认证或以其它方式控制对受控资源节点 R 的接入，其中节点 B 可响应于来自节点 A 的接入请求而向节点 A 发送质询并且基于对质询的响应来确定是否要向节点 A 准予对受控资源节点 R 的接入。例如，质询和响应机制可取决于请求方节点和认证方节点具有可被用来基于共享机密（例如，口令、通用认证机制等）来验证信任的证书。此外，节点 B 可限制被授予节点 A 的接入或者替换地向节点 A 提供对受控资源的不受限接入（例如，取决于受控资源节点 R 是有限的还是无限的）。例如，节点 A 可代表 DSL 调制解调器，节点 B 可代表因特网服务供应商 (ISP)，并且节点 R 可代表 ISP 向 DSL 调制解调器分配的受限带宽。在相对示例中，节点 A 可代表连接到无线接入点 (WAP) 的无线设备，节点 B 可代表 WAP，并且节点 R 可代表 WAP 准予给节点 A 的不受限带宽（例如，尽管从 ISP 分配给 WAP 的带宽可能是受限的，但 WAP 可能不对无线设备接入分配给 WAP 的带宽施加任何限制）。

[0093] 仍参照图 6，响应于通信场景 610 导致节点 A 成功响应来自节点 B 的质询并且获得所请求的对受控资源节点 R 的接入，通信场景 620 示出节点 A 可如何变成具有对受控资源节点 R 的保留接入的中间节点 C。在通信场景 620 中，节点 C 由此可以是能将接入请求从不具有允许与节点 B 的直接联系的通信范围的另一节点 A 中继到节点 B 的中间节点。在类似方面，通信场景 630 包括中间节点 D，尽管不具有对受控资源节点 R 的保留接入，中间节点 D 仍可接收来自节点 A 的接入请求并将该接入请求中继给节点 B，。例如，在通信场景 620 和 630 中，节点 C 和节点 D 可相应地将从节点 A 接收到的接入请求中继到节点 B 并且随后在不能彼此直接通信的节点 A 与节点 B 之间中继质询和响应消息以便于控制对受控资源节点 R 的接入。然而，在节点 A 与节点 B 之间中继质询和响应消息的中间节点 C 和 D 可以不被准予对受控资源节点 R 的接入，因为节点 C 和节点 D 代替地通常实现除了通过中间节点之外

不能彼此直接通信的节点 A 与节点 B 之间的通信。如此，在通信场景 620 和 630 中，至少从管控对受控资源节点 R 的接入的节点 B 的视角来看，节点 C 和节点 D 通常可以是逻辑等同物。

[0094] 现在参照图 7，解说了某些示例性通信场景以表明本文所公开的信任启发式模型可如何减少 IoT 网络中的控制负载。例如，在通信场景 710 中，想要保留对受控资源节点 R 的接入的客户端节点 A 可具有允许节点 A 联系中间节点 C 和中间节点 D 的通信范围，中间节点 C 具有对受控资源节点 R 的保留接入，中间节点 D 不具有对受控资源节点 R 的保留接入。此外，中间节点 C 和中间节点 D 可具有允许与管控对受控资源节点 R 的接入的节点 B 的直接联系的相应通信范围。相应地，在一个实施例中，节点 A 通常可通过中间节点 C 和 / 或中间节点 D 接入受控资源节点 R，其可垂直和水平地一般化。更具体地，节点 C 和节点 D 可垂直地一般化，因为许多不同节点可能知道节点 A 和 / 或节点 B 或者在节点 A 和 / 或节点 B 的合适通信范围内。例如，在通信场景 710 中，节点 C 和节点 D 在与节点 A 相关联的通信范围和与节点 B 相关联的通信范围内具有相应的通信范围。类似地，在通信场景 720 中，节点 C_1、节点 C_2和节点 T 在与节点 A_1相关联的通信范围内具有相应的通信范围，并且此外，节点 T 从可被用来对与节点 A_1相关联的信任进行建模的先前交互中知道节点 A_1。此外，节点 C 和节点 D 可被水平地一般化，因为在节点 B 与请求方客户端之间可存在一个或多个中间节点。例如，如通信场景 710 中所示，节点 A 可通过一个中间节点（例如，节点 C 或节点 D）联系到节点 B。在另一示例中，通信场景 720 示出节点 A_1与节点 B 之间的多个中间节点，其中除节点 A_1与节点 B 之间的一个中间节点之外，节点 A_1还可通过节点 C_2和节点 D 联系到节点 B，其中节点 A_1可单独通过节点 C_1联系到节点 B。本领域技术人员将领会，以上与请求方客户端节点 A 如何通过可被水平和 / 或垂直一般化的一个或多个中介来联系节点 B 相关的概念可被应用于许多其它通信场景和使用情形。

[0095] 根据本公开的一个方面，现在将描述可用来使用信任启发式模型来减少与请求对 IoT 网络中的受控资源的接入相关联的控制负载的各种机制。在一个实施例中，具体参照通信场景 720，受控资源节点 R 可以是受限或有限资源并且保留对受限资源的接入的每个节点 C 可请求节点 B 向其分配 R+e，其中 R 可具有大于或等于零的值，该值表示节点 C 需要的受控资源节点 R 的量，并且 e 可具有大于零的值，该值表示节点 C 已保留的受控资源节点 R 的某一额外量（例如，节点 C 可向请求方节点 A 供应的盈余量）。相应地，当客户端节点 A_1随后想要保留对由节点 B 管控的受控资源节点 R 的接入时，客户端节点 A_1可初始地联系与其相关联的通信范围内的所有节点 C。例如，如通信场景 720 中所示，客户端节点 A_1可初始地联系节点 C_1和节点 C_2以询问关于每个节点 C 对其自己保留的额外容量 e。相应地，如果节点 A_1需要的受控资源的量（R_a）未超过每个节点 C 向其自己保留的额外容量 e 的总和（e_1+e_2），则中间节点 C_1和中间节点 C_2可向节点 A_1发出质询并且响应于节点 A_1返回对该质询的成功响应而向节点 A_1供应所请求的资源 R_a。

[0096] 此外，尽管质询和响应机制可常规地以规则的间隔重复以确保没有什么改变并且周期性地重新认证节点 A_1，但本文所公开的信任启发式模型可减少控制负载（例如，以避免占据无线系统中不必要的带宽）。例如，当节点 A_1向节点 C_1和节点 C_2请求资源时，节点 C_1和节点 C_2可向节点 A_1发出初始质询，在一个或多个连续响应之后减小质询间隔。替换地，如果节点 C_1和 / 或节点 C_2从其它交互知道节点 A_1，则节点 C_1和 / 或节点 C_2可在不采用质

询和响应机制的情况下向节点 A_1 准予接入。相应地，基于可随时间推移在 IoT 网络中的不同节点之间发生的连续质询和响应交换，IoT 网络中的两个或更多个节点之间的信任和 / 或不信任可被构建或者按照类似于人可根据熟人、同事、朋友、密友等来对与其他人的关系进行分类的方式另行以不同等级进行建模（例如，如图 5 中所示并且在以上进一步详细描述的）。

[0097] 此外，IoT 网络通常可在各种不同通信接口上创建或者以其它方式包括各种不同通信接口，这些通信接口可包括一个或多个有线接口和 / 或一个或多个空中接口（例如，Wi-Fi 空中接口、蜂窝空中接口等）。相应地，在一个实施例中，实现本文所描述的信任启发式模型的 IoT 网络可在不同有线和 / 或空中接口上创建或者以其它方式包括这些接口并且基于请求方节点用来在 IoT 网络上通信的通信接口来确定与某些请求方节点相关联的信任等级。例如，在一个实施例中，通过安全 Wi-Fi 连接通信的请求方节点可具有比通过不安全 Wi-Fi 连接通信的节点高的信任等级，通过蜂窝接口通信的请求方节点可具有比通过 Wi-Fi 接口通信的节点低的信任等级，通过有线连接通信的请求方节点可具有比通过空中接口通信的节点高的信任等级，等等。然而，本领域技术人员将领会，可被指派给请求方节点的基于被用来与 IoT 网络通信的特定接口的特定信任等级可取决于与 IoT 网络相关联的特定上下文而合适地改变。

[0098] 相应地，由于 IoT 网络中的所有节点都有可能通过若干受控资源交互，因此信任启发式模型可显著减少为控制对受控资源的接入所需的质询和响应消息并且由此显著减少 IoT 网络中的控制负载。例如，在一个示例性使用情形中，节点 C_1 可具有对受控资源 X、Y 和 Z 的接入，并且节点 C_2 可具有对受控资源 V、W 和 X 的接入。响应于新的客户端节点 A_1 正被引入环境并且与节点 C_1 第一次交互以接入受控资源 Z，可在节点 A_1 与节点 C_1 之间对信任进行建模。如果客户端节点 A_1 随后向不具有与节点 A_1 的任何先前交互的节点 C_2 请求资源 W，则节点 C_2 可询问其通信范围内的其它设备（例如，在设备的“邻域”中）以确定这些其它设备是否具有与节点 A_1 之间的任何信任关系。例如，如果节点 C_2 询问节点 C_1 并且具有与节点 C_1 的信任关系（例如，基于与受控资源 X 相关联的交互），则节点 C_2 可在不要求成功的质询和响应的情况下向节点 A_1 准予对资源 W 的接入。如此，信任启发式模型可减少用来管控对受控资源的接入的控制负载和询问并且仍使得所有设备能够接收对受控资源的接入。另外，由于可需要相当少的成功质询和响应来控制资源接入，因此用于开发复杂的质询和响应机制的处理负载可被显著减少。再进一步，信任启发式模型可提供更多的安全性扩展，其中多次未能成功响应质询的请求方节点 A 可被阻止在 IoT 网络上通信达某一时段或者完全从 IoT 网络中禁止（例如，以阻止垃圾邮件、暴力破解攻击、拒绝服务攻击等）。如此，信任启发式模型可允许获授权节点忽略来自恶意冒犯者的话务并且由此避免因垃圾数据充满控制信道而导致的 IoT 网络的中断。

[0099] 此外，在一个实施例中，本文所公开的信任启发式模型可被用来基于 IoT 网络中的每个受控资源来对信任进行建模，以及基于与受信任节点（例如，已成功完成一个或多个质询和响应交换的节点）相关联的身份来显著减少控制负载。例如，在一个实施例中，某些受控资源可要求节点具有与某一信任等级相关的第一净空等级以获得对其的接入（例如，图 5 中所示的初步信任等级 520）。如此，如果特定节点具有提供用于接入要求第一净空等级的受控资源的恰适净空的信任等级，并且该节点在接入该受控资源时表明职责（例

如，不超过所分配的配额），则该节点随后可获得用于接入原本要求较高净空等级的受控资源的某一标称信任。相应地，在一个实施例中，信任启发式模型可被用来在每资源基础上构建信任并且在不同资源之间转移信任的子部分，从而被指派给节点的净空等级可基于这些节点如何与这些节点被准许接入的资源交互来标称地增大和/或随后约定。

[0100] 根据图8的一个方面，图8解说了示例性方法800，IoT网络中的客户端可执行该示例性方法800以请求对受控资源的接入并基于信任启发式模型来减少与其相关联的控制负载。具体而言，客户端可在框805初始地标识客户端想要保留接入的所需资源并且随后在框810确定所标识的资源为受限（即，有限或以其他方式受约束）资源还是无限（即，不受限和不受约束）资源。响应于确定所标识的资源是受限的，客户端随后可在框815确定表示客户端需要的受控资源量的量R。客户端随后可联系与其相关联的通信范围内具有对所标识的资源的保留接入的所有邻居节点。例如，如以上所提及的，保留对受限资源的接入的每个邻居节点可向管控对受控资源的接入的节点请求R+e，其中R表示该节点需要的受控资源的量，并且e表示受控资源的某一额外量。相应地，客户端可初始地联系具有对受控资源的保留接入的所有邻居节点以询问每个邻居节点对其自己保留的额外容量e并且在框825确定客户端需要的受控资源量（R_a）是否不超过每个邻居节点对其自己保留的额外容量e的总和（$e_1+e_2+\ldots e_n$）。

[0101] 在一个实施例中，如果客户端确定每个邻居节点对其自己保留的额外容量e的总和足以满足框815处确定的资源要求，则客户端随后可在框835向这些邻居节点请求对额外资源容量的接入。替换地，如果客户端确定每个邻居节点对其自己保留的额外容量e的总和不足以满足框815处确定的资源要求或者所需资源是无限的，则客户端可在框830标识要向其请求资源接入的恰适中间节点，随后在框835向这些中间节点请求对资源的接入。在任一情形中，客户端随后可在框840确定是否响应于资源接入请求而接收到质询。

[0102] 例如，如果客户端不具有与请求被传送给的邻居节点和/或中间节点的任何先前交互，则接收方节点可在框840向客户端发出质询并且客户端可随后在框845传送对质询的响应。如此，发出质询的节点可响应于客户端在框845传送对质询的成功响应而在框850将所请求的资源供应给客户端和/或将该请求中继给管控对受控资源的接入的节点，在此情形中客户端可随后在框855接入资源。然而，如果客户端未能在框845传送对质询的成功响应，则客户端可在框850被拒绝接入资源，在此情形中客户端可返回框835以再次尝试请求接入。替换地，响应于在框850确定对资源的接入未被准予，则客户端可返回框830（未示出）以尝试通过另一中间节点来接入资源（例如，如果具有额外容量的邻居节点未能向客户端分配资源）和/或采取以上提到的传统接入模式（例如，尝试直接联系监督者，而不是继续尝试通过中间节点来请求对资源的接入）。

[0103] 回到框840，如果客户端的确具有与请求被传送给的邻居节点和/或中间节点的任何交互，或者邻居和/或中间节点以其他方式能够确定客户端能被信任，则客户端可以不在框840接收质询并且可以代替地在不要求成功的质询和响应的情况下在框855被准予对资源的接入。替换地，由于客户端可能多次未能成功地响应质询并且由此被阻止在IoT网络上通信达某一时段或者完全从IoT网络中禁止，因而客户端可不在框840接收质询。在此情形中，客户端可类似地返回到框835以尝试在客户端被阻止的时段已期满之后再次尝试请求接入和/或返回到框830（未示出）以尝试在客户端被阻止的时段已期满之后尝试

通过另一中间节点来接入资源。然而，本领域技术人员将领会，如果客户端已完全从 IoT 网络中禁止或以其他方式未能传送成功的对质询的响应，则客户端再次作出的请求接入的任何尝试可能同样失败，因为该客户端事实上不具有正确的认证凭证。

[0104] 根据本公开的一个方面，图 9 解说了示例性方法 900，具有对 IoT 网络中的受控资源的保留接入的中间节点可执行该示例性方法 900 以基于信任启发式模型来减少 IoT 网络中的控制负载。具体而言，中间节点可初始地在框 905 与管控对受控资源的接入的节点通信以请求管控节点向中间节点分配 R+e，其中 R 可具有大于或等于零的值，该值表示中间节点需要的受控资源量，并且 e 可具有大于零的值，该值表示中间节点已保留的某一额外受控资源量（例如，中间节点可向一个或多个请求方节点供应的盈余量）。在一个实施例中，管控节点可采用质询和响应机制来认证来自中间节点的请求，其中管控节点可响应于来自中间节点的请求而向中间节点发送质询并且在中间节点成功地响应该质询的情况下准予该请求。

[0105] 在一个实施例中，中间节点随后可在框 910 从想要接入受控资源的客户端节点接收额外容量查询。例如，当客户端节点想要保留对受控资源的接入时，客户端节点可在框 905 联系与该客户端节点相关联的通信范围内的所有中间节点以询问每个中间节点对其自己保留的额外容量 e。相应地，中间节点随后可在框 915 向客户端节点传送指示中间节点在框 905 保留的额外容量 e 的信息，其中如果客户端节点需要的受控资源量 (R_a) 未超过每个中间节点对其自己保留的额外容量 e 的总和 ($e_1+e_2+\ldots e_n$)，则客户端节点通常可向中间节点请求额外容量 e。如此，中间节点可在框 920 确定是否从客户端节点接收到接入请求，这在 R_a超过每个中间节点对其自己保留的额外容量 e 的总和的情况下可能不会发生，在此情形中，方法 900 可随后结束。此外，如果具有对资源的保留接入的中间节点处于最大容量或者以其他方式不能够向客户端节点供应额外容量 e，则客户端节点可向另一中间节点请求对受控资源的接入，该另一中间节点尽管尚未具有对受控资源的保留接入、但具有能联系到管控对受控资源的接入的节点的通信范围（例如，图 6 和 7 中所示的节点 D），并且节点 D 随后可保留对资源的接入并且由此响应于来自客户端节点的接入请求而成为节点 C。替换地，如果具有保留接入的中间节点不能够向客户端节点供应 R_a，则客户端节点可采取以上提到的传统接入模式并且尝试直接联系管控受控资源的节点（例如，如图 6 和 7 中所示的节点 B）。

[0106] 否则，如果 R_a未超过每个中间节点对其自己保留的额外容量 e 的总和，则中间节点可在框 920 接收接入请求。替换地，即使所有额外容量 e 都已被使用并且由此不能被用来向客户端节点供应 R_a，则在中间节点未处于最大容量的情况下中间节点可尝试接入受控资源以保留附加额外容量 e（未示出），在此情形中，中间节点随后可响应于成功地保留足够的附加额外容量 e 以向客户端节点供应 R_a而在框 915 向客户端节点传送经更新的额外资源容量指示符。如此，客户端节点随后可响应于在框 915 传送的额外资源容量指示符（或经更新的额外资源容量指示符）指示 R_a可通过中间节点来供应而向中间节点传送接入请求。在任何情形中，如果中间节点由于具有足以供应 R_a的额外容量而接收到来自客户端节点的接入请求，则中间节点随后可在框 925 确定客户端节点是否具有已知的信任关系。例如，响应于新的客户端节点被引入环境并且首先与中间节点交互以接入受控资源，如果该客户端节点对中间节点向该客户端节点发出的一个或多个质询成功作出响应，则可在该客

户端节点与中间节点之间对信任进行建模，在此情形中中间节点可在框 925 确定客户端节点是受信任客户端。替换地，如果中间节点不具有与客户端节点的任何先前交互，则该中间节点可询问其通信范围内（例如，设备的“邻域”中）的其它设备以确定这些其它设备是否具有与客户端节点的任何信任关系，在此情形中，中间节点可类似地在框 925 确定客户端节点是受信任客户端。如此，如果中间节点确定客户端节点是受信任客户端，则中间节点可在框 940 向客户端节点准予额外容量 e。否则，如果中间节点确定客户端节点不是受信任客户端（例如，由于中间节点不具有与客户端节点的任何先前交互并且没有相邻设备具有与客户端节点的先前交互），则中间节点可在框 930 向客户端节点传送质询并且在框 935 确定客户端节点是否正确地响应该质询。如果客户端节点正确地响应质询，则中间节点随后可在框 940 向客户端节点传送额外容量 e，或者替换地如果客户端节点未能成功地响应质询，则中间节点可在框 945 拒绝接入请求。

[0107] 在一个实施例中，中间节点随后可在框 950 更新与客户端节点相关联的信任启发。例如，中间节点可在来自客户端节点的一个或多个连续的对质询的正确响应之后减小质询间隔或者在客户端节点成功地响应质询许多次之后确定不需要进一步的质询和响应交换。相应地，可响应于随时间推移的成功质询和响应交换而构建或以其他方式建模 IoT 网络中两个或更多个节点之间的信任。此外，可按照类似于人可根据熟人、同事、朋友、密友等来对与其他人的关系进行分类的方式以不同等级对信任进行建模。例如，如图 5 所示并且在以上进一步详细描述的，资源可沿相似路径对准以允许节点构建信任，其中信任启发可在框 950 更新以允许客户端节点进入 IoT 网络、使消息被转发或中继、被允许接入丰富或无限资源（例如，电力）、被允许接入受限、受约束、或其它有限资源（例如，Wi-Fi）、和 / 或被允许接入受保护资源（例如，数据库记录）。替换地，如果客户端节点没有成功地响应质询并且中间节点由此在框 945 拒绝接入请求，则可在框 950 更新信任启发以降低与客户端节点相关联的信任等级，和 / 或在客户端节点未能成功地响应质询多次的情况下阻止客户端节点在 IoT 网络上通信达某一时段或者从 IoT 网络中完全禁止客户端节点。相应地，响应于合适地更新信任启发，中间节点随后可在框 955 确定是否可能需要附加的质询和响应交换（例如，如果客户端节点具有不同于足够高的信任等级的信任等级）并且返回框 930 以在质询间隔期满之后重复质询和响应交换。否则，如果中间节点在框 955 确定不需要进一步的质询和响应交换（例如，如果客户端节点具有足够高的信任等级），则方法 900 可结束，其中客户端节点已被准予接入受控资源而不必响应任何进一步的质询。

[0108] 根据本公开的一个方面，图 10 解说了示例性方法 1000，不具有对 IoT 网络中的受控资源的保留接入的中间节点可执行该示例性方法 1000 以基于信任启发式模型来减少 IoT 网络中的控制负载。具体而言，响应于客户端节点确定具有对受控资源的保留接入的某些中间节点不具有足够的额外容量来供应客户端节点需要的受控资源量，中间节点可在框 1005 接收来自客户端节点的中继请求。例如，如果客户端节点不具有允许客户端节点直接联系管控对受控资源的接入的节点的通信范围，则客户端节点通常可传送中继请求以便联系到该管控节点，由此中间节点可代表客户端节点经由一跳或多跳与管控节点通信。在一个实施例中，响应于接收到中继请求，中间节点随后可在框 1010 确定客户端节点是否具有已知信任关系。

[0109] 例如，响应于新的客户端节点被引入环境并且首先与中间节点交互以接入受控资

源，如果该客户端节点对中间节点向该客户端节点发出的一个或多个质询成功作出响应，则可在该客户端节点与中间节点之间对信任进行建模，在此情形中该中间节点可在框 1010 确定客户端节点是受信任客户端。替换地，如果中间节点不具有与客户端节点的任何先前交互，则该中间节点可询问其通信范围内（例如，设备的“邻域”中）的其它设备以确定这些其它设备是否具有与客户端节点的任何信任关系，在此情形中，中间节点可类似地在框 1010 确定客户端节点是受信任客户端。如此，如果中间节点确定客户端节点是受信任客户端，则中间节点可在框 1025 将来自客户端节点的接入请求中继到管控节点。否则，如果中间节点确定客户端节点不是受信任客户端（例如，由于中间节点不具有与客户端节点的任何先前交互并且没有相邻设备具有与客户端节点的先前交互），则中间节点可在框 1015 向客户端节点传送质询并且在框 1020 确定客户端节点是否正确响应该质询。如果客户端节点正确地响应质询，则中间节点随后可在框 1025 将来自客户端节点的接入请求中继到管控节点，或者如果客户端节点未能成功地响应质询，则中间节点可在框 1030 拒绝接入请求。

[0110] 在一个实施例中，中间节点随后可在框 1035 更新与客户端节点相关联的信任启发。例如，中间节点可在来自客户端节点的一个或多个连续的对质询的正确响应之后减小质询间隔或者在客户端节点成功响应质询许多次之后确定不需要进一步的质询和响应交换。相应地，可响应于随时间推移的成功质询和响应交换而构建或以其他方式建模 IoT 网络中两个或更多个节点之间的信任。例如，如图 5 所示并且在以上进一步详细描述的，信任启发可在框 1035 更新以允许客户端节点进入 IoT 网络、使消息被转发或中继、被允许接入丰富或无限资源（例如，电力）、被允许接入受限、受约束、或其它有限资源（例如，Wi-Fi）、和 / 或被允许接入受保护资源（例如，数据库记录）。替换地，如果客户端节点没有成功地响应质询并且中间节点由此在框 1030 拒绝中继请求，则可在框 1035 更新信任启发以降低与客户端节点相关联的信任等级，和 / 或在客户端节点未能成功地响应质询多次的情况下阻止客户端节点在 IoT 网络上通信达某一时段或者从 IoT 网络中完全禁止客户端节点。相应地，响应于合适地更新信任启发，中间节点随后可在框 1040 确定是否可能需要附加的质询和响应交换（例如，如果客户端节点具有不同于足够高的信任等级的信任等级）并且返回框 1015 以在质询间隔期满之后重复质询和响应交换。否则，如果中间节点在框 1040 确定不需要进一步的质询和响应交换（例如，如果客户端节点具有足够高的信任等级），则方法 1000 可结束，其中客户端节点已被授权使接入请求被自动中继而不必响应任何进一步的质询。

[0111] 根据本公开的一个方面，图 11 解说了示例性方法 1100，管控对 IoT 网络中的受控资源的接入的节点可执行该示例性方法 1100 以基于信任启发式模型来减少 IoT 网络中的控制负载。具体而言，在框 1105，管控节点可在框 1105 初始地接收一个或多个接入由其管控的受控资源的请求。在一个实施例中，管控节点可在框 1110 确定是否有多个接入受控资源的请求，其中管控节点可响应于确定已接收到多个接入受控资源的请求而在框 1115 解决接入受控资源的任何竞争请求。例如，在一个实施例中，各个客户端节点和 / 或中间节点可基于执行类似活动、在某些受控资源上一起工作或者以其他方式具有某些特性而被组织成一个或多个群，并且这些群可按阶层方式组织以在各个群和 / 或被组织成群的各个客户端节点和 / 或中间节点之间进行排名或以其它方式定义相对优先级。

[0112] 相应地，在一个实施例中，管控节点可在框 1115 基于与从其接收到多个请求的节点相关联的相对排名或优先级、控制对受控资源的接入的某些策略、使得不同节点能够彼此交互并且共享资源接入的策略、管控可如何利用受控资源的策略（例如，将对有限或以其他方式受限的资源的接入约束到一次一个或 N 个用户、最大使用历时、特定位置或时间等）来解决竞争的请求。例如，管控节点可解决竞争请求以确定传送接入请求的节点将被准予接入受控资源的次序、每个节点能接入受控资源的最大历时、为了确保每个接入请求可被合适地满足而分配给各个节点的受控资源量，或以其他方式解决对受控资源的任何竞争（尤其在受控资源具有受限量、受约束递送机制、或者其它有限性质的情况下）。在另一示例中，如果管控节点确定受控资源不可用（例如，由于受控资源被占据、不能被先占的较高优先级节点当前对受控资源具有发言权等），则管控节点可将在框 1105 已接收到的接入请求和 / 或与框 1115 竞争的其它接入请求进行排队直至资源变得足够可用，此时管控节点可行进至框 1120 以发起认证所接收到的接入请求的规程。

[0113] 在一个实施例中，在框 1120，管控节点随后可响应于在框 1115 合适地解决竞争的接入请求或者替换地在框 1110 确定没有多个接入受控资源的竞争请求待决而确定传送了在框 1105 接收到的接入请求的请求方节点是否具有已知信任关系。例如，响应于新的节点被引入环境并且首先与管控节点交互以接入受控资源，如果请求方节点对管控节点向该请求方节点发出的一个或多个质询成功作出响应，则可在请求方节点与管控节点之间对信任进行建模，在此情形中管控节点可在框 1120 确定请求方节点是受信任客户端。替换地，如果管控节点不具有与请求方节点的任何先前交互，则管控节点可询问其它设备以确定是否有任何与请求方节点的信任关系已被建模，在此情形中，管控节点可类似地在框 1120 确定请求方节点是受信任客户端。如此，如果管控节点确定请求方节点是受信任客户端，则管控节点可在框 1135 准予来自请求方节点的接入请求（例如，按照以上参照图 6 和图 7 进一步详细描述的方式）。否则，如果管控节点确定请求方节点不是受信任客户端（例如，由于管控节点不具有与请求方节点的任何先前交互并且没有相邻设备具有与请求方节点的先前交互），则管控节点可在框 1125 向请求方节点传送质询并且在框 1130 确定请求方节点是否正确地响应该质询。如果请求方节点正确地响应该质询，则管控节点随后可在框 1135 准予接入请求，或者替换地如果客户端节点未能成功地响应质询，则管控节点可在框 1140 拒绝接入请求。

[0114] 在一个实施例中，管控节点随后可在框 1145 更新与请求方节点相关联的信任启发。例如，管控节点可在来自请求方节点的一个或多个连续的对质询的正确响应之后减小质询间隔或者在请求方节点成功地响应质询许多次之后确定不需要进一步的质询和响应交换。相应地，可响应于随时间推移的成功质询和响应交换而构建或以其他方式建模 IoT 网络中两个或更多个节点之间的信任。例如，如图 5 所示并且在以上进一步详细描述的，信任启发可在框 1145 更新以允许请求方节点进入 IoT 网络、使消息被转发或中继、被允许接入丰富或无限资源（例如，电力）、被允许接入受限、受约束、或其它有限资源（例如，Wi-Fi）、和 / 或被允许接入受保护资源（例如，数据库记录）。替换地，如果请求方节点没有成功地响应质询并且管控节点由此在框 1140 拒绝中继请求，则可在框 1145 更新信任启发以降低与请求方节点相关联的信任等级，和 / 或在请求方节点未能成功地响应质询多次的情况下阻止请求方节点在 IoT 网络上通信达某一时段或者从 IoT 网络中完全禁止请求

方节点。相应地，响应于合适地更新信任启发，管控节点随后可在框 1150 确定是否可能需要附加的质询和响应交换（例如，如果请求方节点具有不同于足够高的信任等级的信任等级）并且返回框 1125 以在质询间隔期满之后重复质询和响应交换。否则，如果管控节点在框 1150 确定不需要进一步的质询和响应交换（例如，如果请求方节点具有足够高的信任等级），则方法 1100 可结束，其中请求方节点已被授权使接入请求被自动中继而不必响应任何进一步的质询。

[0115] 本领域技术人员将领会，信息和信号可使用各种不同技术和技艺中的任何一种来表示。例如，贯穿上面描述始终可能被述及的数据、指令、命令、信息、信号、位（比特）、码元、和码片可由电压、电流、电磁波、磁场或磁粒子、光场或光粒子、或其任何组合来表示。

[0116] 此外，本领域技术人员将领会，结合本文中所公开的方面描述的各种解说性逻辑块、模块、电路、和算法步骤可被实现为电子硬件、计算机软件、或两者的组合。为清楚地解说硬件与软件的这一可互换性，各种解说性组件、块、模块、电路、和步骤在上面是以其功能性的形式作一般化描述的。此类功能性是被实现为硬件还是软件取决于具体应用和施加于整体系统的设计约束。技术人员可针对每种特定应用以不同方式来实现所描述的功能性，但此类实现决策不应被解读为脱离本发明的范围。

[0117] 结合本文中公开的方面描述的各种解说性逻辑块、模块、以及电路可用通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现场可编程门阵列 (FPGA) 或其他可编程逻辑器件、分立的门或晶体管逻辑、分立的硬件组件、或其设计成执行本文中描述的功能的任何组合来实现或执行。通用处理器可以是微处理器，但在替换方案中，该处理器可以是任何常规的处理器、控制器、微控制器、或状态机。处理器还可以被实现为计算设备的组合（例如 DSP 与微处理器的组合、多个微处理器、与 DSP 核协作的一个或多个微处理器、或任何其他此类配置）。

[0118] 结合本文公开的方面描述的方法、序列和 / 或算法可直接在硬件中、在由处理器执行的软件模块中、或在这两者的组合中体现。软件模块可驻留在 RAM、闪存、ROM、EPROM、EEPROM、寄存器、硬盘、可移动盘、CD-ROM 或本领域中所知的任何其他形式的存储介质中。示例性存储介质耦合到处理器以使得该处理器能从 / 向该存储介质读写信息。替换地，存储介质可以被整合到处理器。处理器和存储介质可驻留在 ASIC 中。ASIC 可驻留在 IoT 设备中。替换地，处理器和存储介质可作为分立组件驻留在用户终端中。

[0119] 在一个或多个示例性方面，所描述的功能可在硬件、软件、固件或其任何组合中实现。如果在软件中实现，则各功能可以作为一条或多条指令或代码存储在计算机可读介质上或藉其进行传送。计算机可读介质包括计算机存储介质和通信介质两者，包括促成计算机程序从一地向另一地转移的任何介质。存储介质可以是能被计算机访问的任何可用介质。作为示例而非限定，这样的计算机可读介质可包括 RAM、ROM、EEPROM、CD-ROM 或其他光盘存储、磁盘存储或其他磁存储设备、或能用于携带或存储指令或数据结构形式的期望程序代码且能被计算机访问的任何其他介质。任何连接也被正当地称为计算机可读介质。例如，如果软件是使用同轴电缆、光纤电缆、双绞线、DSL、或诸如红外、无线电、以及微波之类的无线技术从 web 网站、服务器、或其它远程源传送而来，则该同轴电缆、光纤电缆、双绞线、DSL、或诸如红外、无线电、以及微波之类的无线技术就被包括在介质的定义之中。如本文所使用的，盘 (disk) 和 / 或碟 (disc) 包括 CD、激光碟、光碟、DVD、软盘和蓝光碟，其中盘

(disk)常常磁性地和/或用激光来光学地再现数据。上述的组合应当也被包括在计算机可读介质的范围内。

[0120] 尽管前面的公开示出了本公开的解说性方面,但是应当注意在其中可作出各种变更和修改而不会脱离如所附权利要求定义的本发明的范围。根据本文中所描述的本公开的方面的方法权利要求中的功能、步骤和/或动作不一定要以任何特定次序执行。此外,尽管本公开的要素可能是以单数来描述或主张权利的,但是复数也是已料想了的,除非显式地声明了限定于单数。

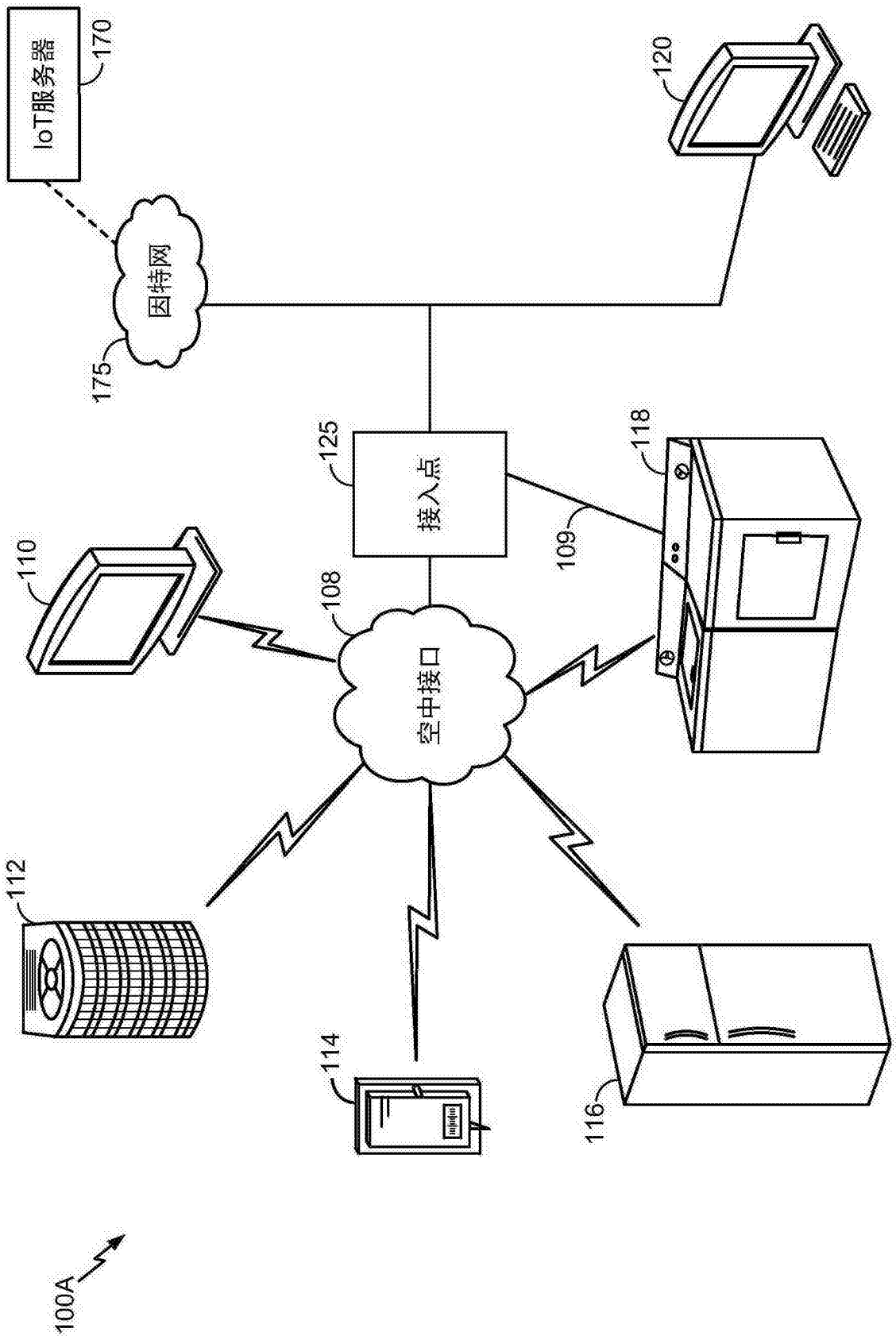

IoT服务器
170
120
因特网
175
125
接入点
118
109
110
108
空中接口
112
114
116
100A

图 1A

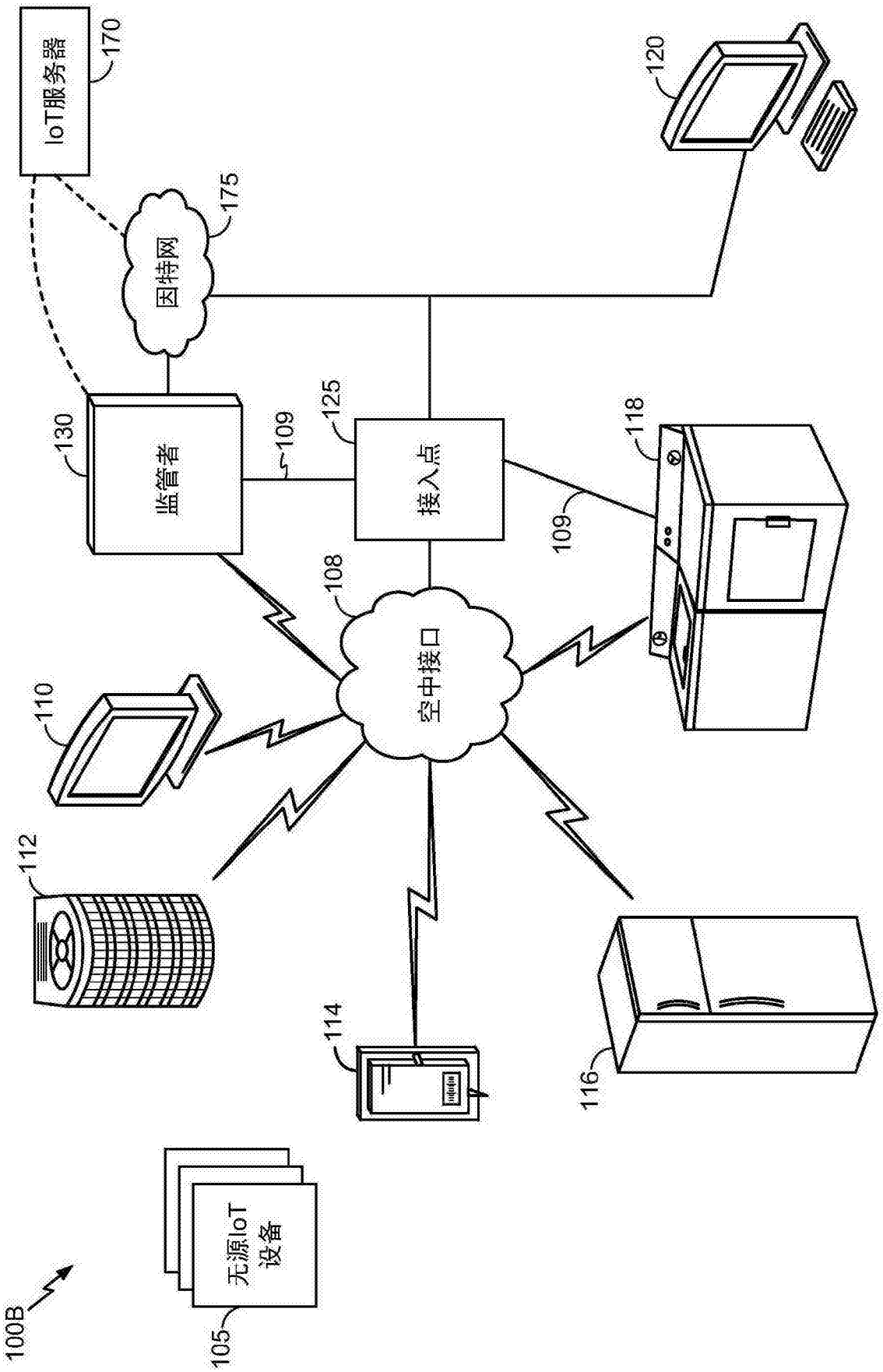

IoT服务器
170
120
因特网
175
监管者
130
109
接入点
125
118
109
108
空中接口
110
112
114
116
无源IoT
设备
105
100B

图 1B

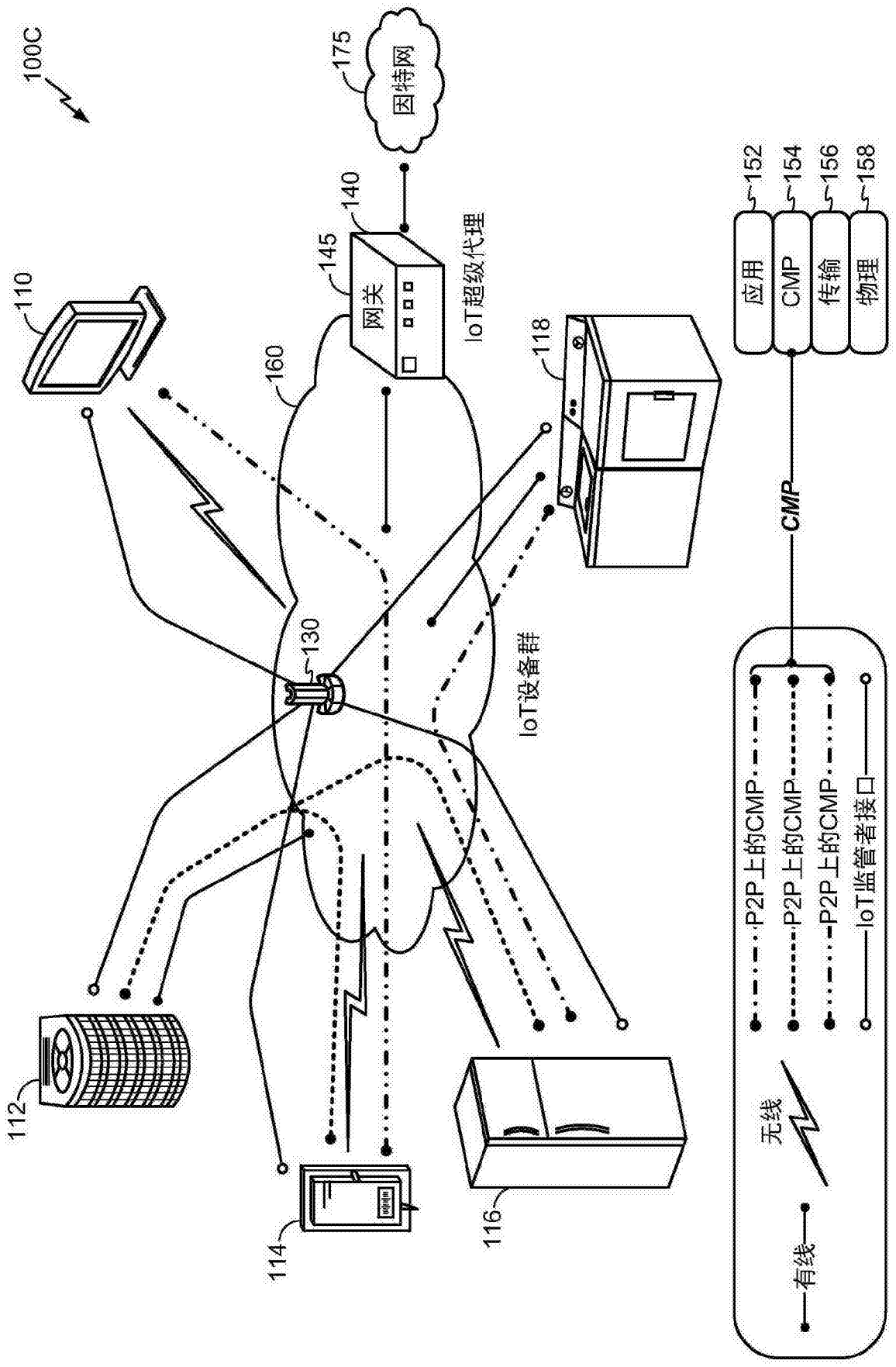

100C
175
因特网
140
145
网关
IoT超级代理
110
160
118
152
154
156
158
应用
CMP
传输
物理
CMP
130
IoT设备群
112
114
116
P2P上的CMP
P2P上的CMP
P2P上的CMP
IoT监管者接口
无线
有线

图 1C

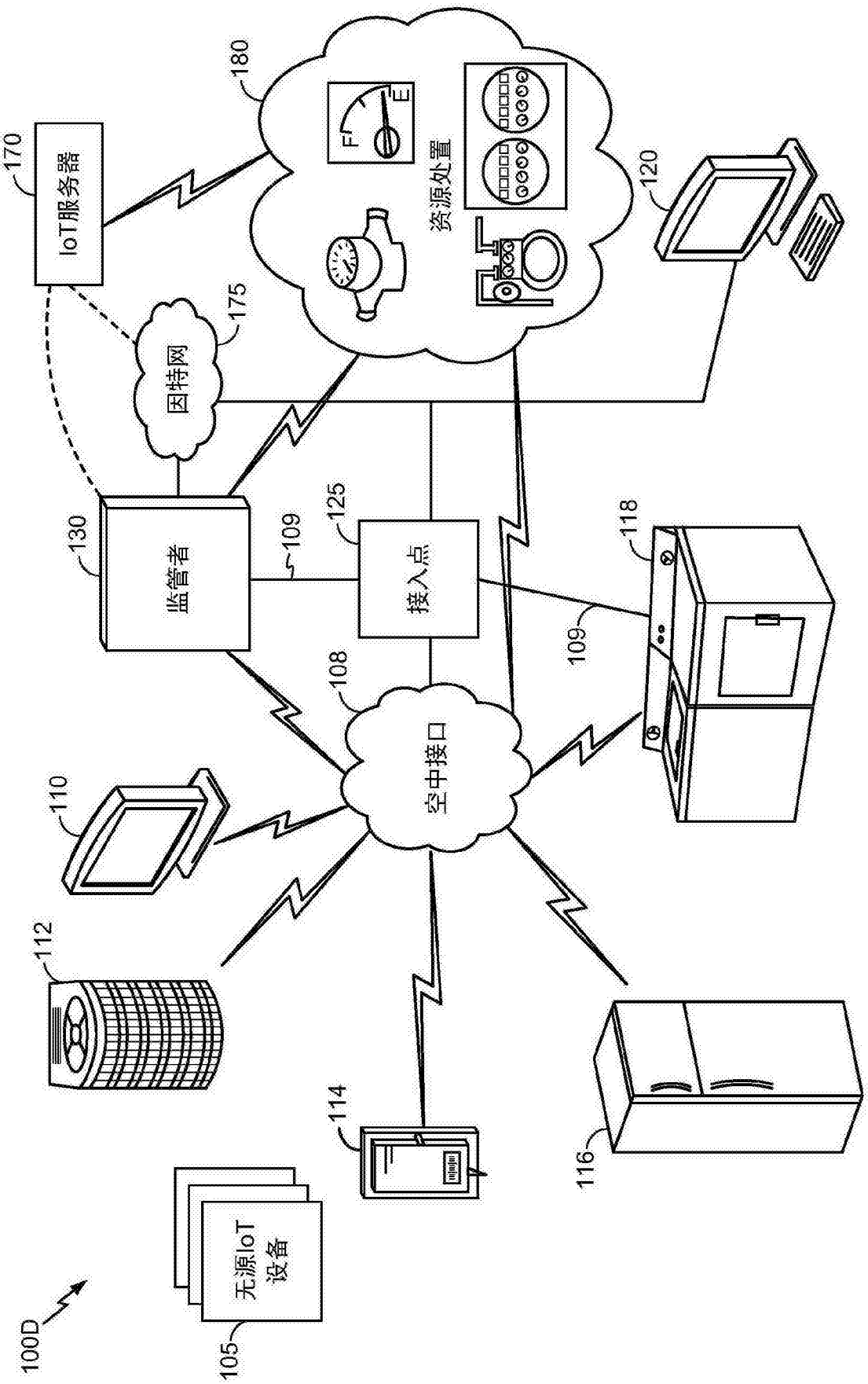

180
170
IoT服务器
资源处置
120
175
因特网
130
监管者
109
125
接入点
118
109
108
空中接口
110
112
114
116
无源IoT
设备
105
100D

图 1D

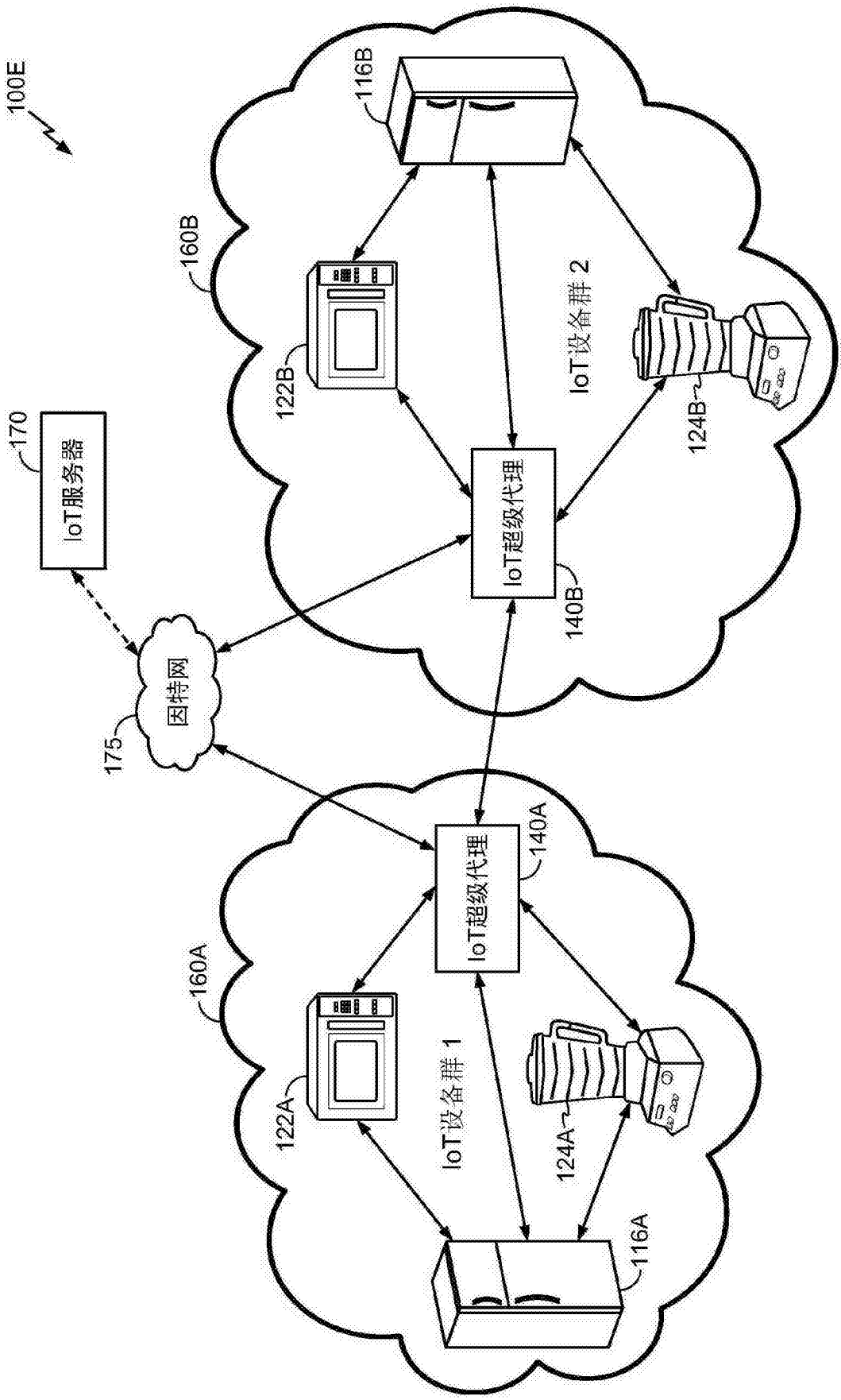

100E
116B
160B
122B
IoT设备群 2
124B
170
IoT服务器
IoT超级代理
140B
因特网
175
140A
160A
122A
IoT设备群 1
124A
116A

图 1E

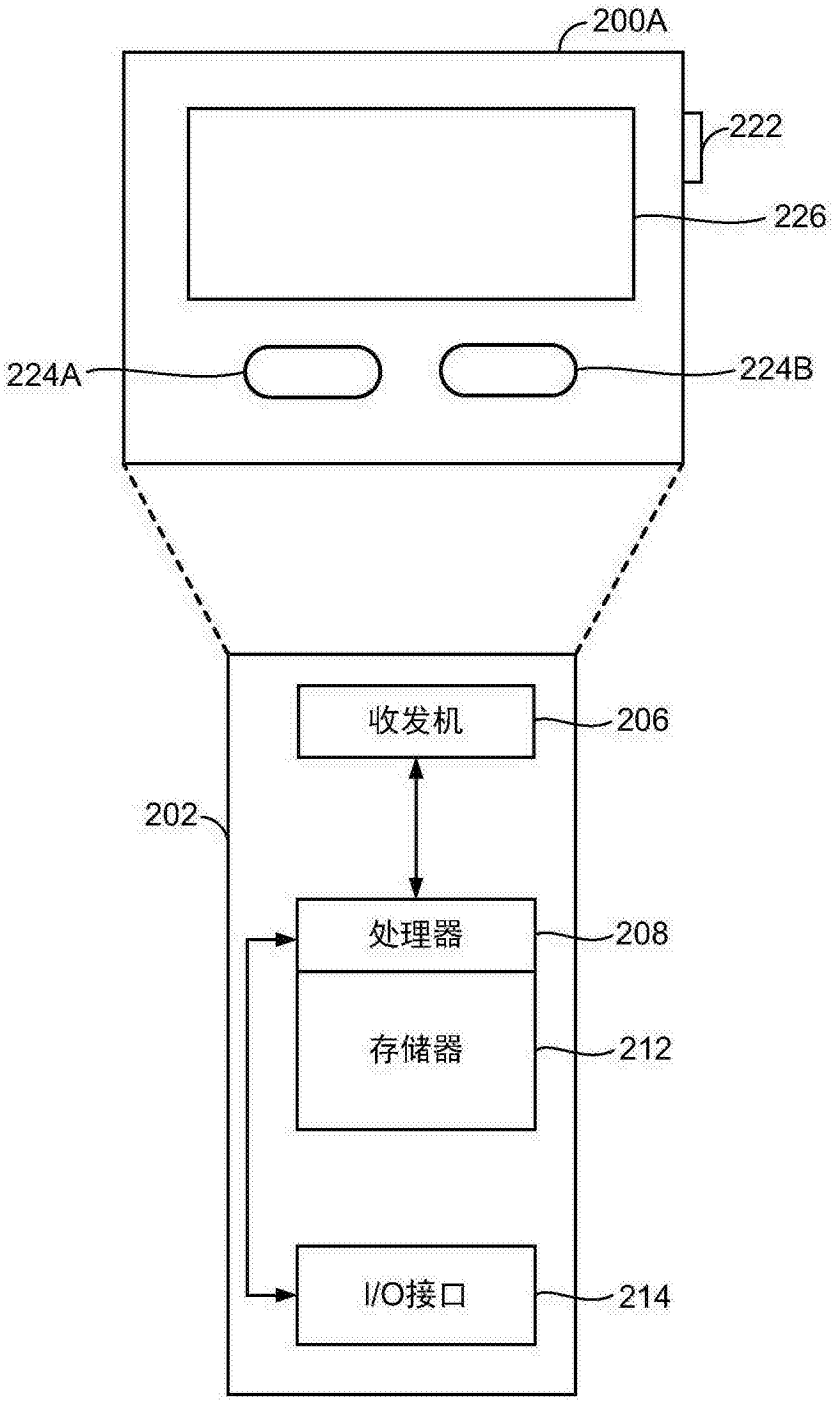


图 2A

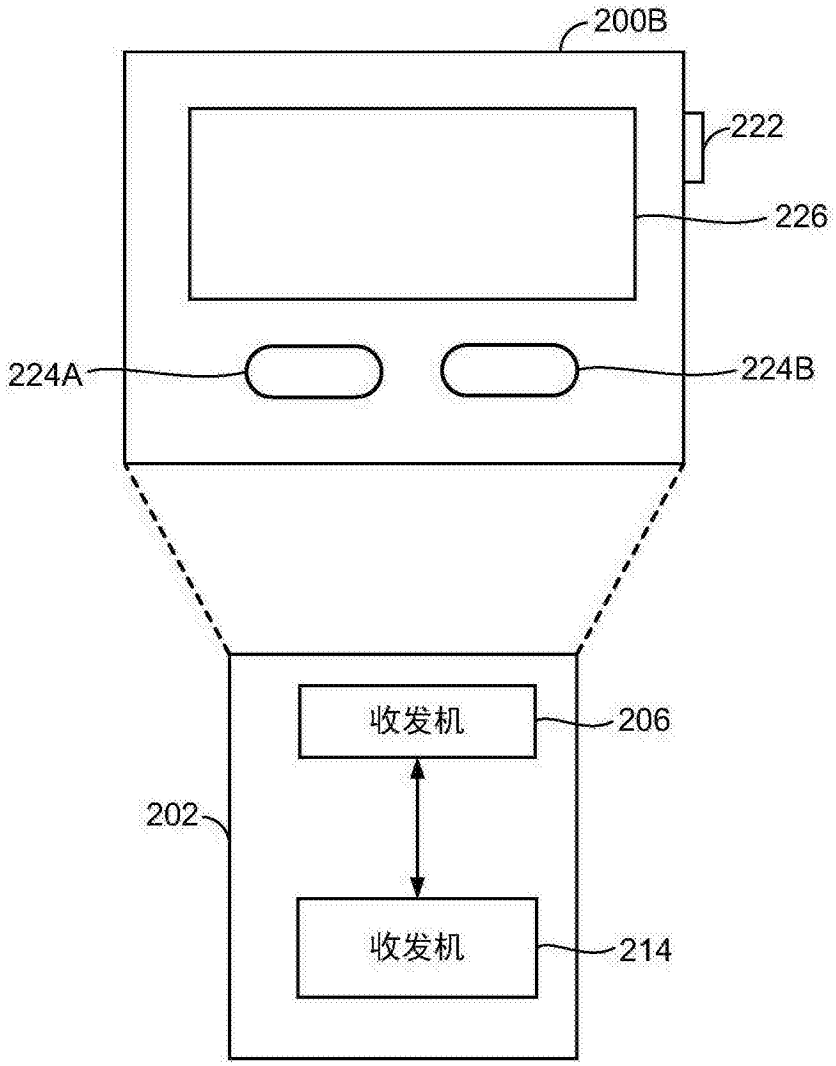


图 2B

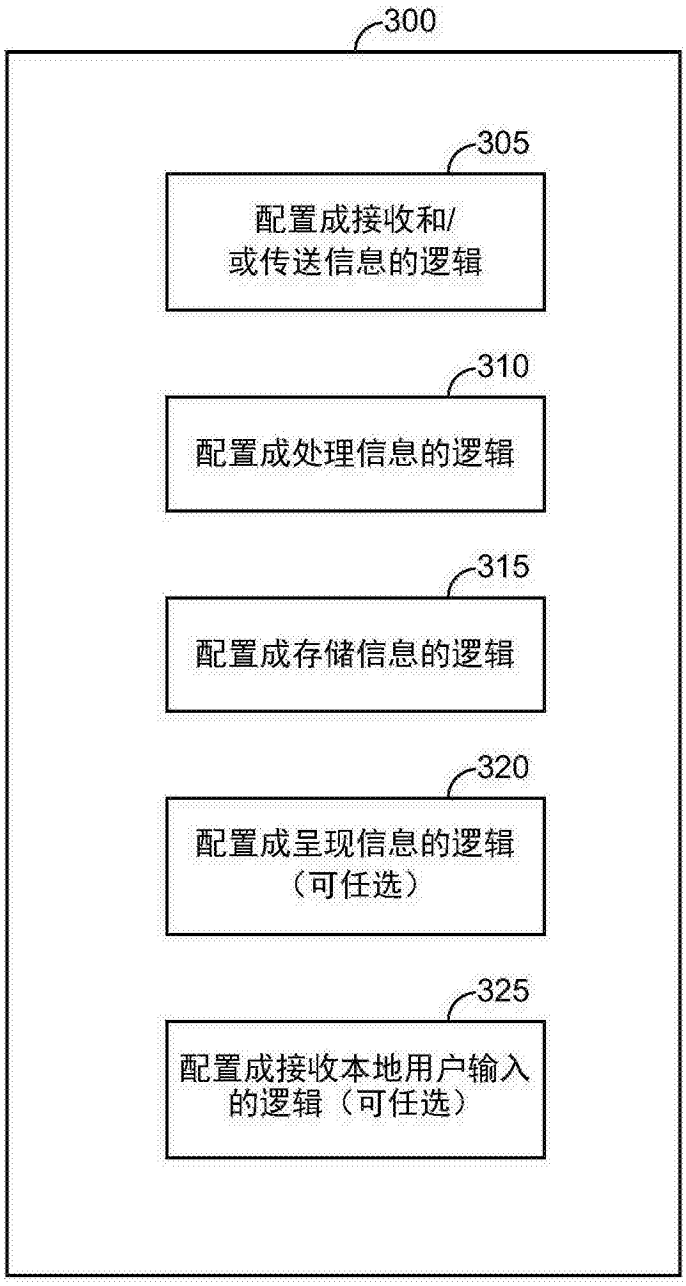

300
305
配置成接收和/
或传送信息的逻辑
310
配置成处理信息的逻辑
315
配置成存储信息的逻辑
320
配置成呈现信息的逻辑
（可任选）
325
配置成接收本地用户输入
的逻辑（可任选）

图 3

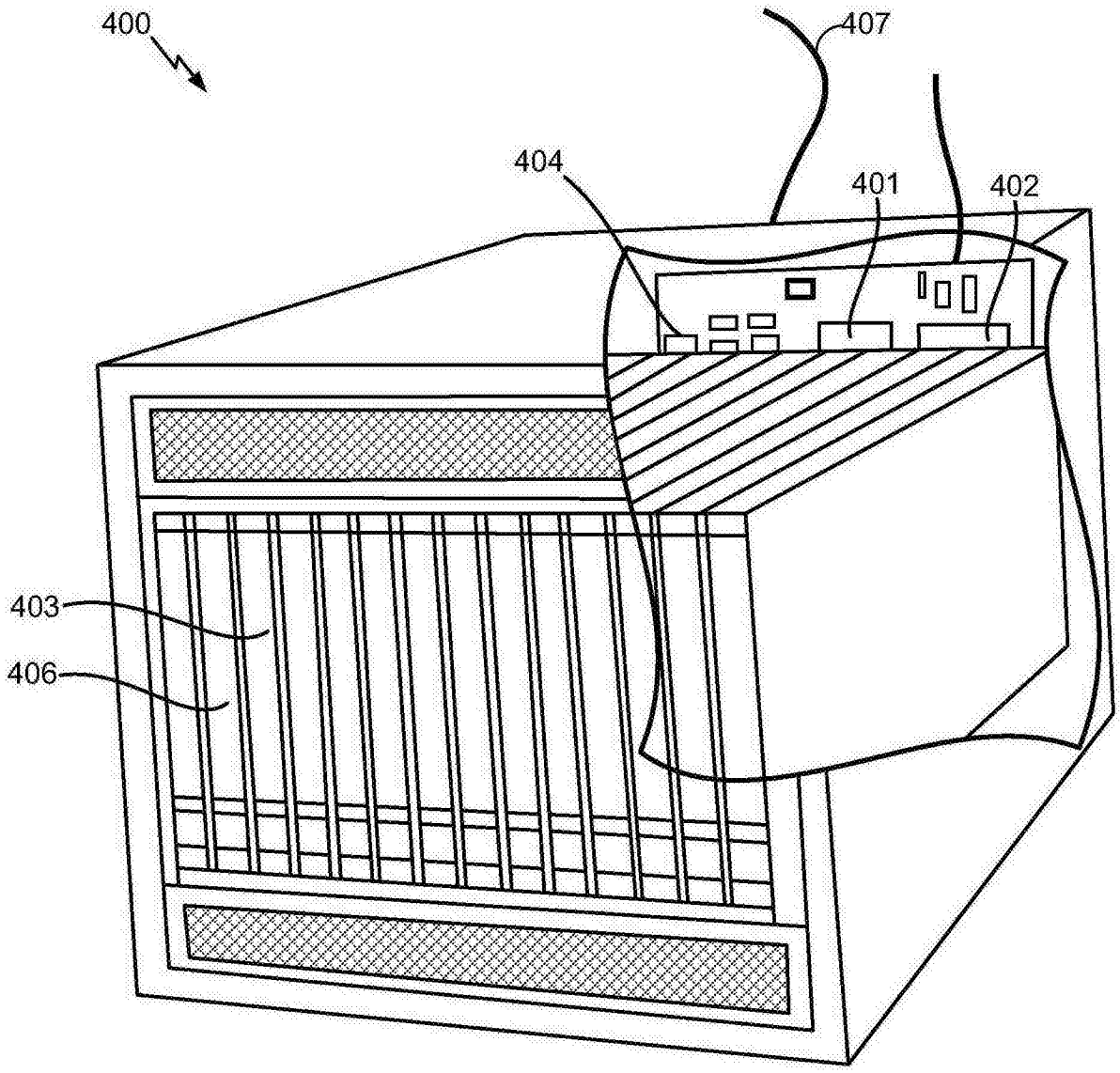


图 4

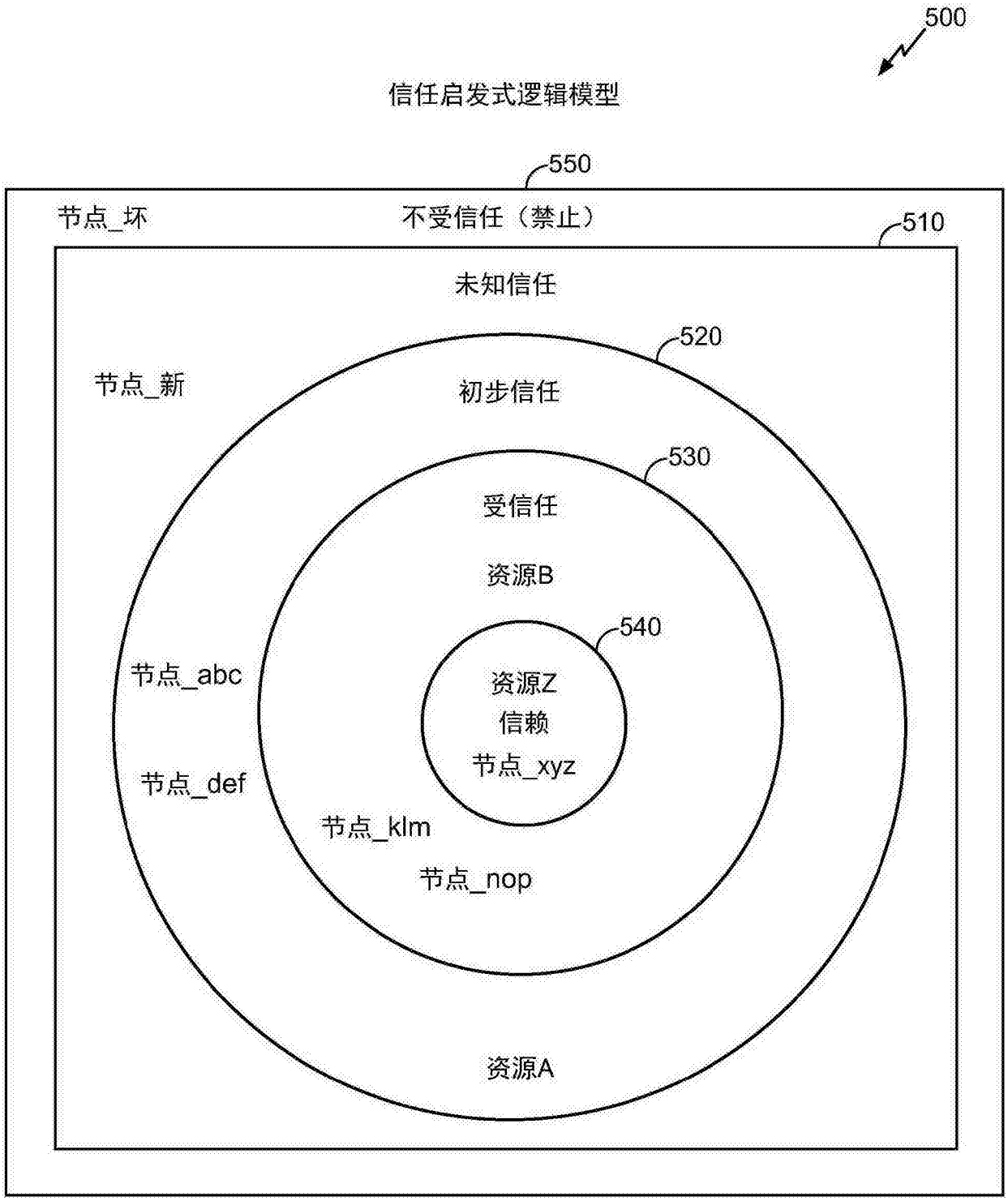

500
信任启发式逻辑模型
550
节点_坏
不受信任（禁止）
510
未知信任
520
节点_新
初步信任
530
受信任
资源B
540
节点_abc
资源Z
信赖
节点_xyz
节点_def
节点_klm
节点_nop
资源A

图 5

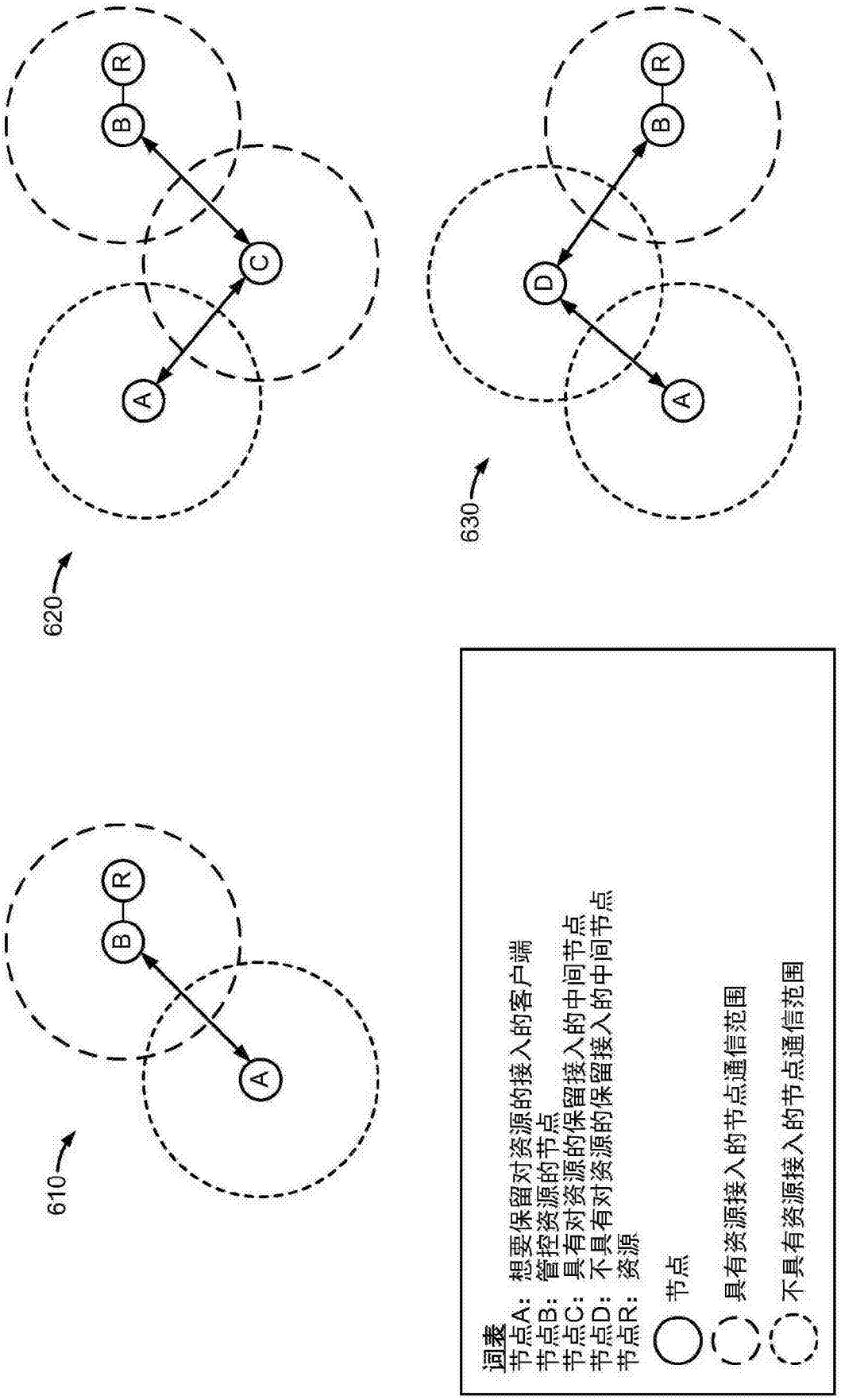

610
A
B
R
620
A
B
C
R
630
A
B
D
R
词表
节点A：想要保留对资源的接入的客户端
节点B：管控资源的节点
节点C：具有对资源的保留接入的中间节点
节点D：不具有对资源的保留接入的中间节点
节点R：资源
节点
具有资源接入的节点通信范围
不具有资源接入的节点通信范围

图 6

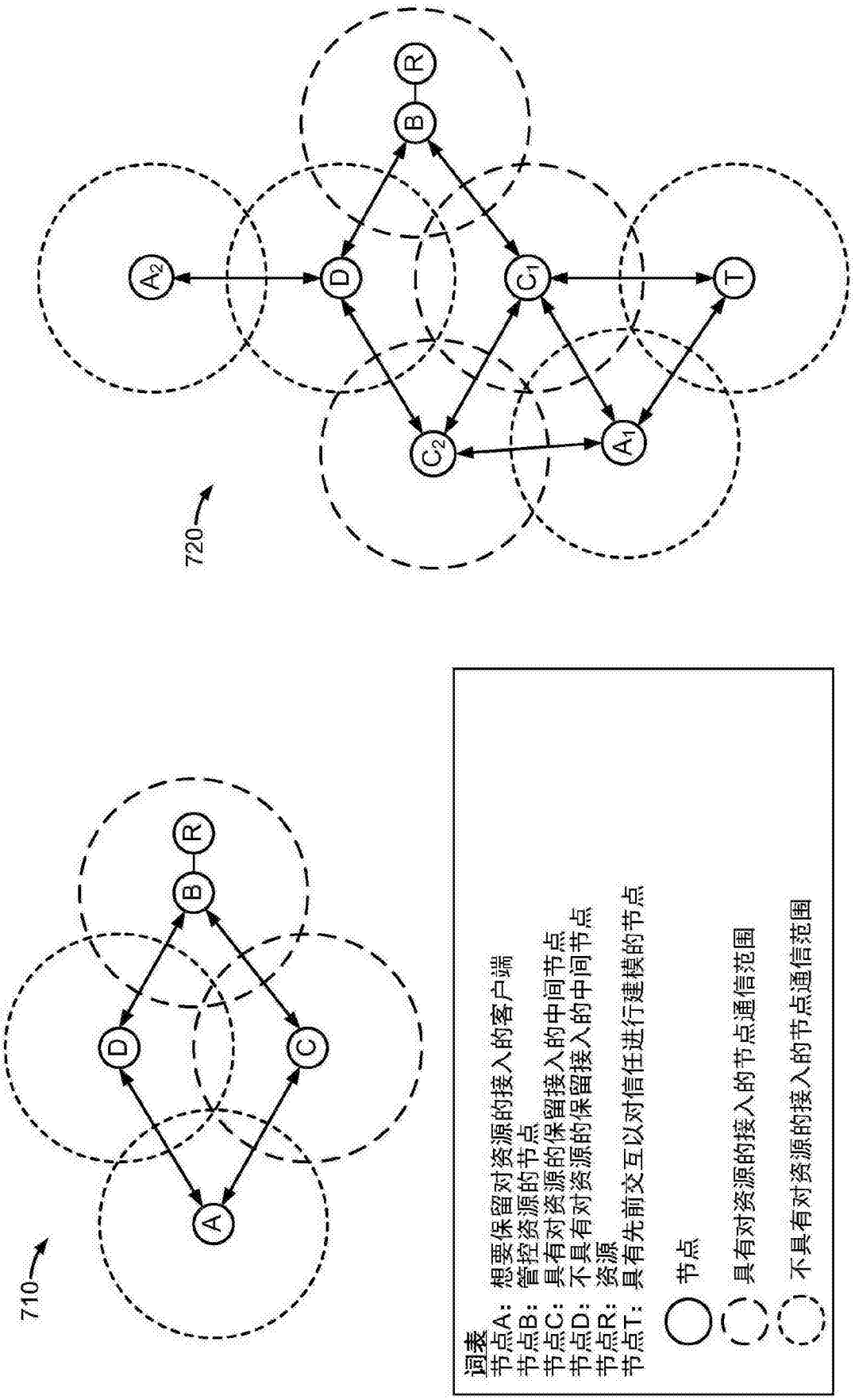

720
R
B
A2
D
C1
T
C2
A1
710
R
B
D
C
A
词表
节点A：想要保留对资源的接入的客户端
节点B：管控资源的节点
节点C：具有对资源的保留接入的中间节点
节点D：不具有对资源的保留接入的中间节点
节点R：资源
节点T：具有先前交互以对信任进行建模的节点
节点
具有对资源的接入的节点通信范围
不具有对资源的接入的节点通信范围

图 7

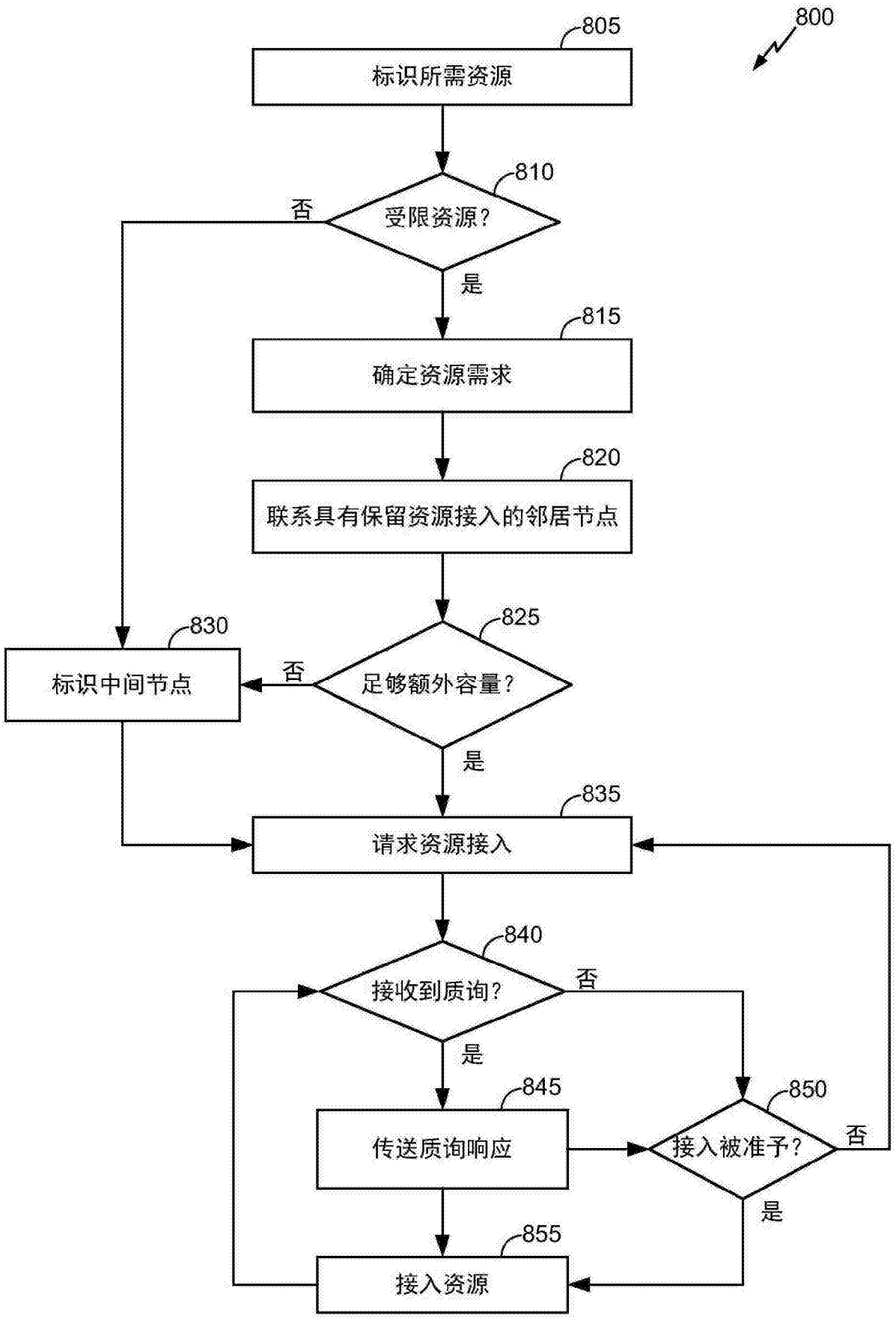

800
805
标识所需资源
810
受限资源？
否
是
815
确定资源需求
820
联系具有保留资源接入的邻居节点
825
足够额外容量？
否
830
标识中间节点
是
835
请求资源接入
840
接收到质询？
否
是
845
传送质询响应
850
接入被准予？
否
是
855
接入资源

图 8

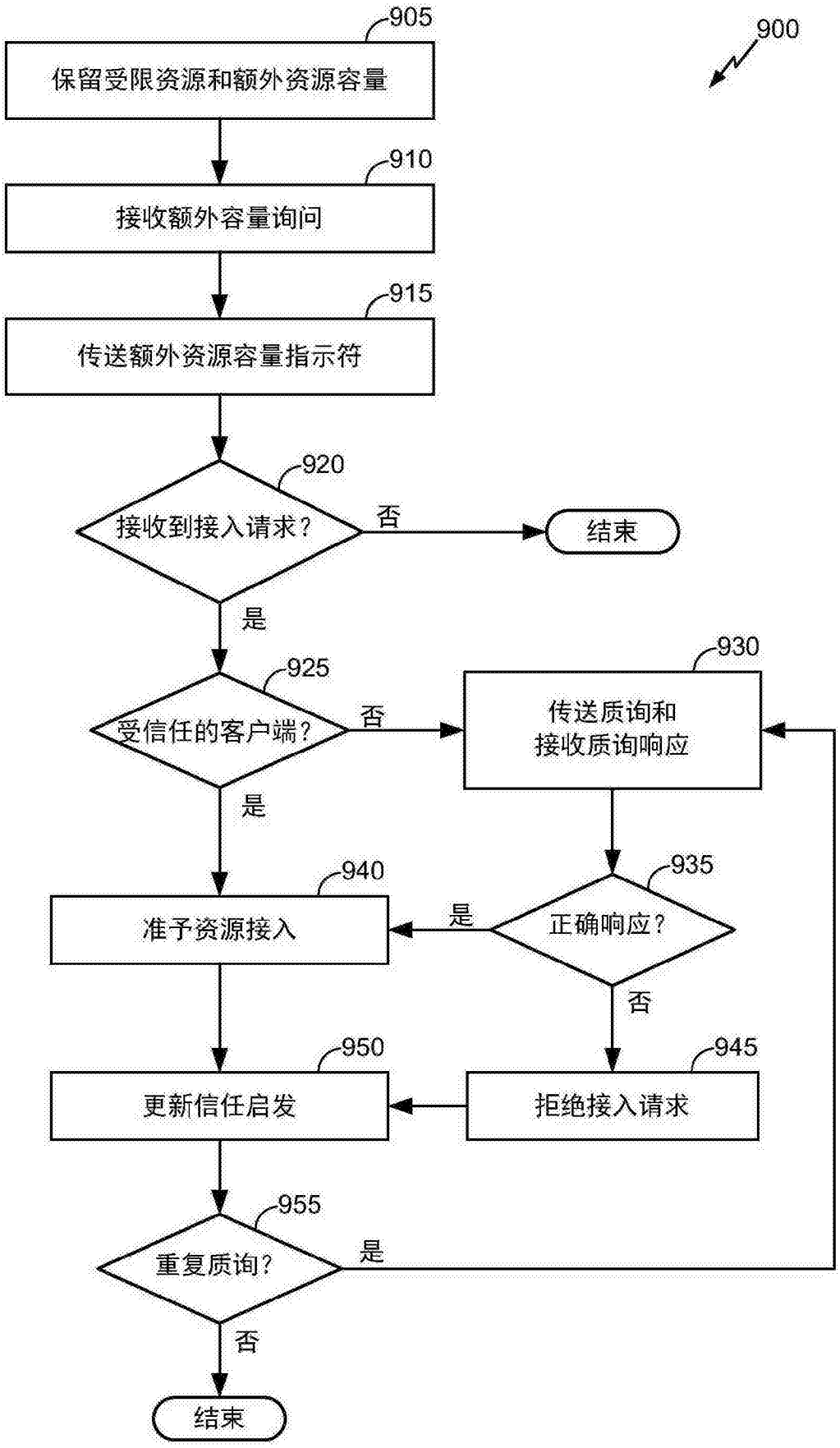

900
905
保留受限资源和额外资源容量
910
接收额外容量询问
915
传送额外资源容量指示符
920
接收到接入请求？
否
结束
是
925
受信任的客户端？
否
930
传送质询和
接收质询响应
是
935
正确响应？
是
940
准予资源接入
否
945
拒绝接入请求
950
更新信任启发
955
重复质询？
是
否
结束

图 9

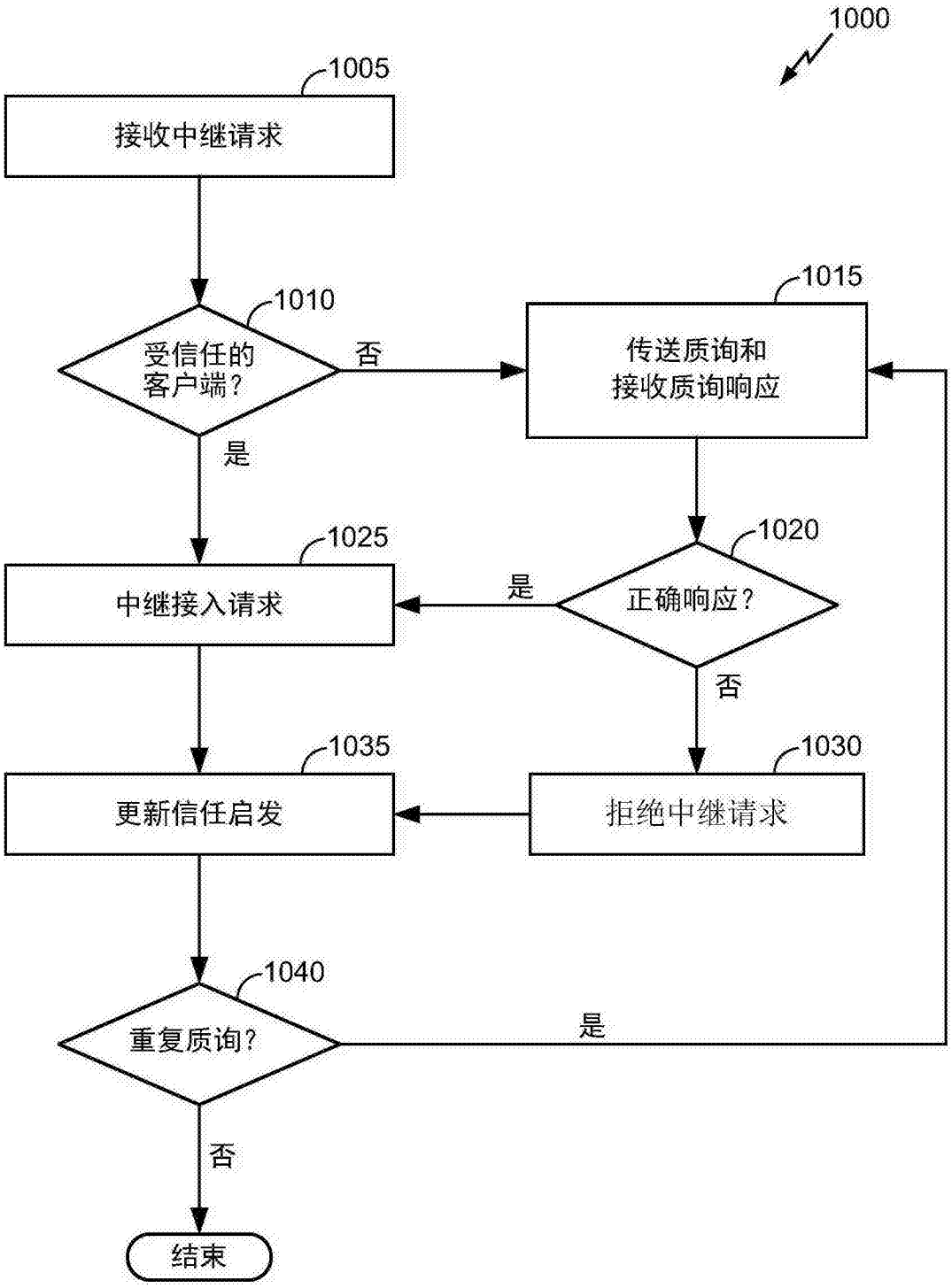

1000
1005
接收中继请求
1010
受信任的客户端？
否
是
1015
传送质询和接收质询响应
1020
正确响应？
是
否
1025
中继接入请求
1030
拒绝中继请求
1035
更新信任启发
1040
重复质询？
是
否
结束

图 10

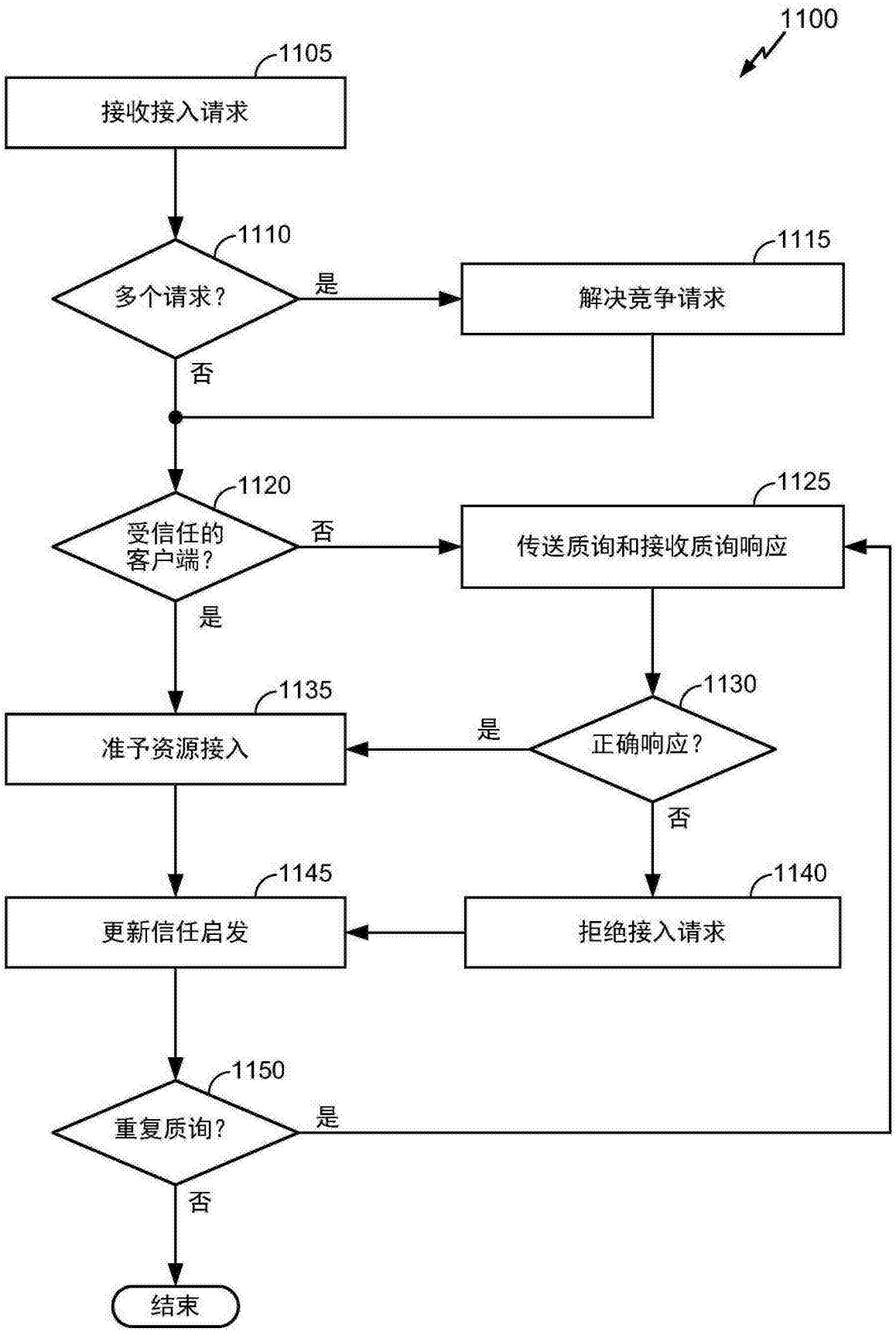

1100
1105
接收接入请求
1110
多个请求？
是
1115
解决竞争请求
否
1120
受信任的客户端？
否
1125
传送质询和接收质询响应
是
1130
正确响应？
是
1135
准予资源接入
否
1140
拒绝接入请求
1145
更新信任启发
1150
重复质询？
是
否
结束

图 11