(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 105340235 B
(45)授权公告日 2019.08.06

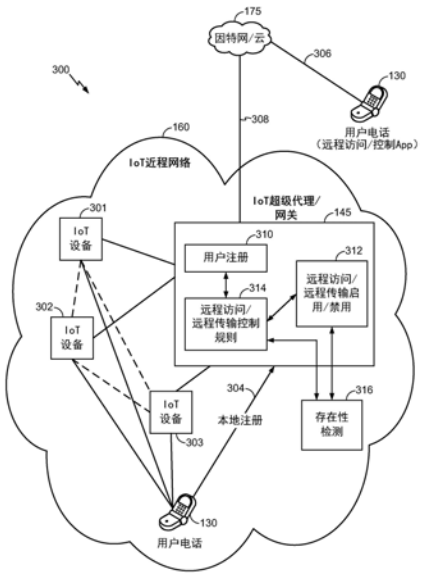
(21)申请号 201480036245.8
(22)申请日 2014.06.26
(65)同一申请的已公布的文献号
申请公布号 CN 105340235 A
(43)申请公布日 2016.02.17
(30)优先权数据
61/839,815 2013.06.26 US
14/314,498 2014.06.25 US
(85)PCT国际申请进入国家阶段日
2015.12.24
(86)PCT国际申请的申请数据
PCT/US2014/044371 2014.06.26
(87)PCT国际申请的公布数据
WO2014/210330 EN 2014.12.31
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州
(72)发明人 B·吉普塔
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 李小芳
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04M 1/725(2006.01)
H04W 4/021(2018.01)
H04W 4/70(2018.01)
H04W 12/08(2009.01)
H04W 48/04(2009.01)
(56)对比文件
WO 03/098909 A1,2003.11.27,
WO 03/098909 A1,2003.11.27,
JP 2008067199 A,2008.03.21,
JP 2001251312 A,2001.09.14,
US 2009/0254980 A1,2009.10.08,
审查员 王勇
权利要求书3页 说明书12页 附图4页

(54)发明名称

基于用户存在性来控制与物联网(IoT)设备的远程通信

(57)摘要

所公开的系统和方法包括用于控制与包括一个或多个物联网(IoT)设备的IoT近程网络的远程通信的IoT超级代理/网关。检测IoT用户设备在IoT近程网络中的存在性。如果IoT用户设备存在于IoT近程网络中并且如果满足用于禁用远程通信的远程通信准则,则禁用远程通信。如果IoT用户设备不存在于IoT近程网络中并且如果满足用于启用远程通信的远程通信准则,则启用远程通信。远程通信包括由IoT用户设备对这些IoT设备中的一者或多者的远程访问、以及将来自一个或多个IoT设备的通知远程传输至IoT用户设备。



CN 105340235 B

1.一种控制与包括一个或多个物联网(IoT)设备的IoT近程网络的远程通信的方法,所述方法包括:

检测IoT用户设备是否存在于所述IoT近程网络内;

确定是否满足用于禁用与所述IoT近程网络中的所述一个或多个IoT设备的远程通信的一个或多个远程通信准则;以及

如果所述IoT用户设备存在于所述IoT近程网络中并且如果满足用于禁用所述远程通信的所述一个或多个远程通信准则,则禁用所述远程通信,

其中用于禁用至所述IoT近程网络的远程通信的所述一个或多个远程通信准则包括能够与所述IoT近程网络中的所述IoT设备通信的一个或多个IoT设备的集合中的所述IoT用户设备的指定或优先级级别,所述指定或优先级级别基于所述IoT用户设备在所述IoT近程网络中的注册。

2.如权利要求1所述的方法,其特征在于,所述远程通信包括由所述IoT用户设备对所述IoT近程网络中的所述一个或多个IoT设备的远程访问。

3.如权利要求1所述的方法,其特征在于,所述远程通信包括由云服务对所述IoT近程网络中的所述一个或多个IoT设备的远程访问。

4.如权利要求1所述的方法,其特征在于,所述远程通信包括将来自所述IoT近程网络中的所述一个或多个IoT设备的关于消息或事件的通知远程传输至所述IoT用户设备。

5.如权利要求1所述的方法,其特征在于,检测所述IoT用户设备存在于所述IoT近程网络中是基于用于将所述IoT用户设备的存在或不存在传达给IoT超级代理/网关的控制应用,所述IoT超级代理/网关用于控制所述IoT近程网络中的远程通信,其中所述控制应用在所述IoT用户设备上执行。

6.如权利要求1所述的方法,其特征在于,检测所述IoT用户设备存在于所述IoT近程网络中是基于所述IoT用户设备向IoT超级代理/网关的注册的周期性刷新,所述IoT超级代理/网关用于控制所述IoT近程网络中的远程通信。

7.如权利要求1所述的方法,其特征在于,用于禁用至所述IoT近程网络的远程通信的所述一个或多个远程通信准则包括以下至少一者:一个或多个事件、或者一个或多个时间实例。

8.如权利要求1所述的方法,其特征在于,所述一个或多个远程通信准则基于所述远程通信的方向。

9.如权利要求1所述的方法,其特征在于,禁用所述远程通信包括选择性地禁用与所述一个或多个IoT设备的所选功能性有关的远程通信能力。

10.如权利要求1所述的方法,其特征在于,进一步包括检测一个或多个附加IoT用户设备存在于所述IoT近程网络中;以及基于所述IoT用户设备中的一者或多者的子集存在于所述IoT近程网络中和与存在于所述IoT近程网络中的所述一个或多个IoT设备的所述子集中的每一个IoT设备有关的远程通信准则来禁用所述远程通信。

11.一种控制与包括一个或多个物联网(IoT)设备的IoT近程网络的远程通信的方法,所述方法包括:

检测IoT用户设备是否不存在于所述IoT近程网络中;

确定是否满足用于启用与所述IoT近程网络中的所述一个或多个IoT设备的远程通信

的一个或多个远程通信准则;以及

如果所述IoT用户设备不存在于所述IoT近程网络中并且如果满足用于启用所述远程通信的所述一个或多个远程通信准则,则启用所述远程通信,

其中用于启用至所述IoT近程网络的远程通信的所述一个或多个远程通信准则包括能够与所述IoT近程网络中的所述一个或多个IoT设备通信的一个或多个IoT用户设备的集合中的所述IoT用户设备的指定或优先级级别,所述指定或优先级级别基于所述IoT用户设备在所述IoT近程网络中的注册。

12.如权利要求11所述的方法,其特征在于,所述远程通信包括由所述IoT用户设备或云服务对所述IoT近程网络中的所述一个或多个IoT设备的远程访问。

13.如权利要求11所述的方法,其特征在于,所述远程通信包括将来自所述IoT近程网络中的所述一个或多个IoT设备的关于消息或事件的通知远程传输至所述IoT用户设备。

14.如权利要求11所述的方法,其特征在于,检测所述IoT用户设备不存在于所述IoT近程网络中是基于用于将所述IoT用户设备的存在或不存在传达给IoT超级代理/网关的控制应用,所述IoT超级代理/网关用于控制所述IoT近程网络中的远程通信,其中所述控制应用在所述IoT用户设备上执行。

15.如权利要求11所述的方法,其特征在于,检测所述IoT用户设备不存在于所述IoT近程网络中是基于所述IoT用户设备向IoT超级代理/网关的注册的周期性刷新,所述IoT超级代理/网关用于控制所述IoT近程网络中的远程通信。

16.如权利要求11所述的方法,其特征在于,用于启用至所述IoT近程网络的远程通信的所述一个或多个远程通信准则包括以下至少一者:一个或多个事件、或者一个或多个时间实例。

17.如权利要求11所述的方法,其特征在于,所述一个或多个远程通信准则基于所述远程通信的方向。

18.一种用于通信的装置,包括:

物联网(IoT)超级代理/网关,其被配置成控制与包括一个或多个IoT设备的IoT近程网络的远程通信;

存在性检测块,其被配置成检测IoT用户设备是否存在于所述IoT近程网络中;

远程访问/远程传输控制规则块,其被配置成确定是否满足用于禁用与所述IoT近程网络中的所述一个或多个IoT设备的远程通信的一个或多个远程通信准则;以及

远程访问/远程传输启用/禁用块,其被配置成如果所述IoT用户设备存在于所述IoT近程网络中并且如果满足用于禁用所述远程通信的所述一个或多个远程通信准则,则禁用所述远程通信,

其中用于启用或禁用远程通信的所述一个或多个远程通信准则包括所述IoT用户设备的指定或优先级级别,所述指定或优先级级别基于所述IoT用户设备在所述IoT近程网络中的注册。

19.如权利要求18所述的装置,其特征在于,所述远程访问/远程传输启用/禁用块被进一步配置成如果所述IoT用户设备不存在于所述IoT近程网络中并且如果满足用于启用所述远程通信的所述一个或多个远程通信准则,则启用所述远程通信。

20.如权利要求18所述的装置,其特征在于,所述远程通信包括由所述IoT用户设备或

云服务对所述IoT近程网络中的所述一个或多个IoT设备的远程访问。

21.如权利要求18所述的装置，其特征在于，所述远程通信包括将来自所述IoT近程网络中的所述一个或多个IoT设备的关于消息或事件的通知远程传输至所述IoT用户设备。

22.如权利要求18所述的装置，其特征在于，所述存在性检测块被配置成基于来自所述IoT用户设备上的控制应用的关于所述IoT用户设备在所述IoT近程网络中的存在或不存在的通信来检测所述IoT用户设备是否存在于所述IoT近程网络中。

23.如权利要求18所述的装置，其特征在于，进一步包括用户注册块，其中所述存在性检测块被配置成基于所述IoT用户设备向所述用户注册块的注册的周期性刷新来检测所述IoT用户设备是否存在于所述IoT近程网络中。

24.如权利要求23所述的装置，其特征在于，所述用户注册块被配置成存储能够与所述IoT近程网络中的所述一个或多个IoT设备通信的一个或多个IoT用户设备的集合的指定或优先级级别。

25.如权利要求18所述的装置，其特征在于，用于启用或禁用至所述IoT近程网络的远程通信的所述一个或多个远程通信准则包括以下至少一者：一个或多个事件、或者一个或多个时间实例。

26.一种通信系统，包括：

用于控制与包括一个或多个物联网(IoT)设备的IoT近程网络的远程通信的装置；

用于检测IoT用户设备是否存在于所述IoT近程网络中的装置；

用于确定是否满足用于禁用与所述IoT近程网络中的一个或多个IoT设备的远程通信的一个或多个远程通信准则的装置；以及

用于如果所述IoT用户设备存在于所述IoT近程网络中并且如果满足用于禁用所述远程通信的所述一个或多个远程通信准则，则禁用所述远程通信的装置，

其中用于禁用至所述IoT近程网络的远程通信的所述一个或多个远程通信准则包括能够与所述IoT近程网络中的所述IoT设备通信的一个或多个IoT设备的集合中的所述IoT用户设备的指定或优先级级别，所述指定或优先级级别基于所述IoT用户设备在所述IoT近程网络中的注册。

27.如权利要求26所述的通信系统，其特征在于，进一步包括用于如果所述IoT用户设备不存在于所述IoT近程网络中并且如果满足用于启用所述远程通信的所述一个或多个远程通信准则，则启用所述远程通信的装置。

28.如权利要求26所述的通信系统，其特征在于，所述远程通信包括：

由所述IoT用户设备或云服务对所述IoT近程网络中的所述一个或多个IoT设备的远程访问；以及

将来自所述IoT近程网络中的所述一个或多个IoT设备的关于消息或事件的通知远程传输至所述IoT用户设备。

基于用户存在性来控制与物联网(IoT)设备的远程通信

[0001] 根据35 U.S.C.§119的优先权要求

[0002] 本专利申请要求于2013年6月26日提交的题为“USER PRESENCE BASED CONTROL OF REMOTE ACCESS TO INTERNET OF THINGS(IoT)DEVICES(基于用户存在性来控制对物联网(IoT)设备的远程访问)”的待决临时专利申请No.61/839,815的权益,该临时专利申请被转让给本申请受让人并由此通过援引明确地整体纳入于此。

[0003] 公开领域

[0004] 本公开的实施例涉及对IoT设备的远程访问和/或从IoT设备接收远程通知。更具体地,示例性实施例涉及用于基于IoT设备的指定近程网络内的一个或多个用户的远程通信准则(包括用户的存在或不存在)及其他远程通信准则来禁用或启用远程通信(包括对IoT设备的远程访问/远程传输来自IoT设备的通知)的系统和方法。

背景技术

[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))来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] 市场趋势(例如,涉及家居改善的市场趋势)正驱动对新的“智能”服务的开发,包括由服务提供者将营销多业务('N' play)(例如,数据、语音、视频、安全性、能量管理等)与扩展家庭网络进行整合。针对IoT的一些应用包括能够具有对家里或办公室中的几乎任何设备或器具的集中式控制的智能家居和建筑。

[0007] 如此,在不久的将来,IoT技术的不断发展将导致在家里、在交通工具内、在工作场所、以及在许多其他位置处围绕用户的众多IoT设备。例如,在家庭环境中,在指定邻域内可能存在连接至家庭WiFi网络的众多IoT设备。此类网络也可被称为“近程网络”,其与用户可籍以远程地访问近程网络上的IoT设备的远程网络形成对比。更具体地,数百个IoT设备(诸如,器具、TV、灯具、空调、音乐系统、车库门、家庭安防系统、风扇、洒水系统、微波炉、烤箱、洗碗机、洗衣机和干衣机等)可连接至近程家庭IoT网络。用户可能希望从家庭IoT网络外部(例如,从用户的办公室)远程地访问和控制这些设备中的一者或多者。因此,期望提供对家庭IoT网络的远程访问能力。

[0008] 然而,允许此类远程访问会引起安全性问题。例如,启用对用户的家庭IoT网络的远程访问/控制导致易受网络安全威胁并使家庭IoT网络易受来自未获授权用户或恶意代理的攻击。IoT设备也可被配置成向用户提供状态更新和重要事件通知。然而,如果这些通知是在用户处于远程位置时在可能进行远程通信的网络上被提供给用户的,则未获授权用户可能获得对这些远程通知的访问,这也可能导致对授权用户的安全性和隐私威胁。

[0009] 因此,需要降低可能因允许与IoT设备进行远程通信而产生的攻击的风险。

[0010] 概述

[0011] 示例性实施例包括与用于控制与包括一个或多个物联网(IoT)设备的IoT近程网

络的远程通信的物联网(IoT)超级代理/网关有关的系统和方法。检测IoT用户设备在IoT近程网络中的存在性。如果IoT用户设备存在于IoT近程网络中并且如果满足用于禁用远程通信的远程通信准则,则禁用远程通信。如果IoT用户设备不存在于IoT近程网络中并且如果满足用于启用远程通信的远程通信准则,则启用远程通信。远程通信包括由IoT用户设备对这些IoT设备中的一者或多者的远程访问、以及将来自一个或多个IoT设备的关于消息或事件的通知远程传输至IoT用户设备。

[0012] 例如,示例性实施例涉及一种控制与包括一个或多个物联网(IoT)设备的IoT近程网络的远程通信的方法,该方法包括:检测IoT用户设备存在于IoT近程网络中,以及确定是否满足用于禁用与该IoT近程网络中的一个或多个IoT设备的远程通信的一个或多个远程通信准则。如果IoT用户设备存在于IoT近程网络中并且如果满足用于禁用远程通信的远程通信准则,则禁用远程通信。

[0013] 另一示例性实施例涉及一种控制与包括一个或多个物联网(IoT)设备的IoT近程网络的远程通信的方法,该方法包括:检测IoT用户设备不存在于IoT近程网络中,以及确定是否满足用于启用与IoT近程网络中的一个或多个IoT设备的远程通信的一个或多个远程通信准则。如果IoT用户设备不存在于IoT近程网络中并且如果满足用于启用远程通信的远程通信准则,则启用远程通信。

[0014] 又一示例性实施例涉及一种装置,包括:物联网(IoT)超级代理/网关,其配置成控制与包括一个或多个IoT设备的IoT近程网络的远程通信;存在性检测块,其配置成检测IoT用户设备是否存在于IoT近程网络中;以及远程访问/远程传输控制规则块,其配置成确定是否满足用于启用或禁用与IoT近程网络中的一个或多个IoT设备的远程通信的一个或多个远程通信准则。该装置进一步包括远程访问/远程传输启用/禁用块,其配置成如果IoT用户设备存在于IoT近程网络中并且如果满足用于禁用远程通信的远程通信准则,则禁用远程通信。

[0015] 又一示例性实施例涉及一种通信系统,包括:用于控制与包括一个或多个物联网(IoT)设备的IoT近程网络的远程通信的装置,用于检测IoT用户设备是否存在于IoT近程网络中的装置,用于确定是否满足用于启用或禁用与IoT近程网络中的一个或多个IoT设备的远程通信的一个或多个远程通信准则的装置,以及用于如果IoT用户设备存在于IoT近程网络中并且如果满足用于禁用远程通信的远程通信准则,则禁用远程通信的装置。

[0016] 附图简述

[0017] 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:

[0018] 图1解说了根据本公开的一方面的无线通信系统的高级系统架构。

[0019] 图2解说了根据本公开的诸方面的包括IoT近程网络的示例性无线通信系统,该无线通信系统能够与近程网络中的IoT设备进行远程通信。

[0020] 图3解说了本公开涉及基于示例性远程通信准则来控制与IoT近程网络中的IoT设备的远程通信的诸方面。

[0021] 图4-5解说了基于示例性远程通信准则来控制与IoT近程网络的IoT设备的远程通信的示例性方法。

[0022] 详细描述

[0023] 以下描述和相关附图中公开了各种方面以示出与物联网(IoT)设备之间的近程度检测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,且可被构造并实践,而不脱离本公开的范围或精神。另外,众所周知的元素将不被详细描述或可被省去以免模糊本文所公开的各方面和实施例的相关细节。

[0024] 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。

[0025] 本文使用的术语仅描述了特定实施例并且不应该被解释成限定本文所公开的任何实施例。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。

[0026] 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被描述为例如“配置成执行所描述的动作的逻辑”。

[0027] 如本文所使用的,术语“物联网设备”(或即“IoT设备”)可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,器具、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或类似物等中和/或由其控制/监视,并被配置成用于连接至IoT网络(诸如局部自组织网络或因特网)。

[0028] 示例性实施例可涉及可远程地访问的IoT设备。远程访问可用于位于用户家中或者更一般地位于任何“近程网络”中的IoT设备,其可指代在预定义地理边界内或直接连接至家庭网络的设备。例如,用户可以能够从远程位置或在用户远离近程家庭网络时监视安防摄像机,操作制热、制冷空调(AC)系统,操作入户门,打开车库门等。进一步,IoT设备也可以能够向用户发送关于消息或事件的通知(例如,后院门已开锁)。此类通知也可在用户处于远程位置或者远离家或预定义近程位置时提供。由IoT设备向远程位置处的用户发送此类通知在本文中被称为“远程传输”通知或通知“被远程传输”,其中该通知包括对消息或事件的通知。更一般地,本文中讨论的“远程通信”包括通过远程网络或通信介质对IoT近程网络中的一个或多个IoT设备的远程访问、以及由IoT近程网络中的一个或多个IoT设备通过

远程网络或通信介质来传送或广播的对通知的远程传输。此类远程通信可能在启用远程通信的远程网络或通信介质上易受到或暴露于安全威胁。

[0029] 如此，示例性方面涉及提高针对IoT设备的指定近程网络的远程访问和/或远程传输功能性的安全性、以及减少将IoT设备暴露于安全威胁。在一些方面，通过减少准许去往/来自近程网络中的IoT设备的远程通信的历时和/或控制准许该远程通信的情形来减少这种暴露。例如，可仅在用户远离家庭或近程网络时才准许远程访问和远程传输。当用户处于近程网络内时，可能不需要用户通过远程连接来访问IoT设备，因为用户可以能够通过本地或家庭网络来访问IoT设备。因此，当用户在家时，可通过在不需要远程访问时完全关闭远程访问来使通过远程连接向外部威胁的暴露最小化。类似地，也可在用户处于家庭网络内时关闭远程传输。例如，当用户在家时，可以防止将来自IoT设备的关于用户家中的后院门被开锁或用户家的窗户被打破的通知在远程网络上被发出或被远程传输。

[0030] 因此，各实施例被配置成检测或识别一个或多个用户在近程网络内的存在或不存在，并基于此检测或识别来禁用或启用远程访问和远程传输。以此方式，至少在远程访问和/或远程传输被禁用的时间期间，可以使家庭网络或任何其他指定近程网络内的IoT设备免遭外部攻击。因此，在一些情形中，可使用一个或多个主用户在近程网络的邻域或附近内的存在性来启用或禁用远程访问和/或远程传输。本公开中将提供若干其他附加或替换的准则和/或事件作为可用于对远程访问和/或远程传输施加限制的示例性因素。现在将参照附图描述根据各实施例的示例性系统和方法。

[0031] 参照图1，解说了根据本公开的一方面的无线通信系统100的系统架构的高级视图。无线通信系统100包括多个IoT设备，如图所示，这些IoT设备包括电视110、空调(AC)单元112、恒温器114、冰箱116、以及洗衣机和干衣机118。IoT设备110-118被配置成在空中接口108和/或直接有线连接109上与接入网(例如，接入点125)通信。空中接口108可遵循无线网际协议(IP)，诸如IEEE 802.11。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1中示出)，并且是使用标准网际协议套集(例如，传输控制协议(TCP)和IP)在相异的设备/网络间通信的互联的计算机和计算机网络的全球系统。在示例性实施例中，例如，通过因特网175进行远程访问和/或远程传输是可能的，如以下将进一步讨论的。

[0032] 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的网络上)。计算机120可替换地或附加地具有至因特网175的有线连接，或者计算机120可直接连接至接入点125。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。

[0033] IoT服务器170可以是可任选的，并且可被实现为多个在结构上分开的服务器、或替换地可对应于单个服务器。IoT设备110-120的群可以是对等(P2P)网络，并且可在空中接口108和/或有线连接109上彼此直接通信。替换地或附加地，IoT设备110-120中的一些或所有设备可配置有独立于空中接口108和有线连接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中的某些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的设备通信。

[0034] 此外，无线通信系统100可包括控制器设备130，控制器设备130可替换地被称为IoT监督器或管理器。尽管控制器设备130已被解说为自立设备或单元，但在一些实现中，控

制器设备130可被集成在IoT设备110-120之一(诸如计算机120)中。例如,控制器设备130可被集成在实现为智能电话的计算机120中。在一些方面,控制器设备130可以是物理设备或是在物理设备上运行的软件应用。在一个实施例中,控制器设备130一般可观察、监视、控制、或以其他方式管理无线通信系统100中的各种其他组件。例如,控制器设备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)通信以与IoT设备交互,其中此类交互可包括监视或管理与无线通信系统100中的各种IoT设备110-120相关联的属性、活动、或其他状态。交互也可包括从各种IoT设备110-120接收对事件或状态更新的通知,在一些实例中这些通知可被远程传输。在示例性实施例中,包括空中接口108和/或直接有线连接109的接入网可以是包括IoT设备110-120的近程网络的一部分。如先前提到的,控制器设备130可以是智能电话或便携式设备、或者驻留在智能电话或便携式设备上,用户可通过该智能电话或便携式设备在近程网络上与IoT设备110-120交互。控制器设备130的诸方面还可使用软件应用(诸如,可包括用户接口的智能电话"App(应用)")来实现。

[0035] 控制器设备130还可具有至因特网175的有线或无线连接以及可任选地至IoT服务器170的有线或无线连接(被示为点线)。控制器设备130可从因特网175和/或IoT服务器170获得信息,该信息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。在示例性实施例中,控制器设备130例如可从空间上远离近程网络的远程位置连接至因特网175以与IoT设备110-120交互。这可包括对IoT设备110-120的远程访问以及从IoT设备110-120进行远程传输。将参照图2对此作进一步描述。

[0036] 无线通信系统100还可包括网关或IoT超级代理/网关145,其将在以下小节中进一步详细讨论。简言之,IoT超级代理/网关145可与近程网络中的IoT设备110-120通信以监视和控制它们,以及从IoT设备110-120接收通知,其中此类通知可由设备自身基于事件检测或状态变化来发起,因此,来自IoT设备110-120的通知不必仅基于来自例如超级代理145的询问。网关或IoT超级代理/网关145可提供由用户远程地访问IoT设备110-120和/或用于由IoT设备110-120向用户远程传输通知的接口。

[0037] 参照图2,解说了包括无线通信系统200的示例性实施例。一般而言,无线通信系统200可包括与图1的无线通信系统100相同和/或基本相似的各种组件,并且出于描述的简洁和方便起见,与无线通信系统200中的某些组件相关的各种细节在上面已关于无线通信系统100提供了相同或相似细节的情况下可在本文中省略。无线通信系统200解说了IoT近程网络160,IoT近程网络160包括局部连接的IoT设备110-118的群。虽然在控制器设备130与IoT设备110-118之间示出了示意性的通信链路(其可以是有线或无线的),然而如本领域公知的,IoT设备110-118以及控制器设备130之间的各种其他对等通信是可能的,但出于简明起见从本文的解说中省略。

[0038] 近程网络160在一些示例中可以是用户的家庭网络。IoT设备110-118可经由连接至因特网175的IoT超级代理/网关145彼此连接和/或通信。IoT超级代理/网关145可提供用于管理和控制近程网络160中的IoT设备110-118的功能性。IoT超级代理/网关145可提供用于从近程网络160中的IoT设备110-118接收通知的功能性,其中在一些情形中,IoT超级代理/网关145可以能够在因特网175上将这些通知远程传输至用户。在一些方面,控制器设备130可位于近程网络160外部(图2中未解说,但在图3中解说),并且IoT超级代理/网关145还可提供用于远程地访问和控制IoT设备110-118以及用于例如通过控制器设备130来远程传

输来自IoT设备110-118的通知的接口。在未在此详细讨论的诸方面，IoT超级代理/网关145还可以能够与近程网络外部的一个或多个IoT设备(或在一些情形中，一个或多个IoT设备群)通信并对其进行管理。在高层级，控制器设备130可通过IoT超级代理/网关145从近程网络160外部与IoT设备110-118通信。IoT超级代理/网关145可对应于或包括接入点125的功能性。替换地，IoT超级代理/网关145可对应于或包括IoT服务器(诸如IoT服务器170)的功能性。一般而言，IoT超级代理/网关145可封装网关功能性145，这将参考实施例来进一步详细讨论。

[0039] 参照图3，解说了无线通信系统300的简化示意图以突出本公开的某些关键方面。在许多方面，无线通信系统300类似于图1和图2的无线通信系统100和200，因此出于简洁起见，本文将省略对共同特征的详细描述。在图3中，控制器设备130被解说为用户电话，在两个分开的位置描绘了用户电话——一次在IoT近程网络160的邻域内，以及一次在远程位置。IoT设备301-303是示例性IoT设备(诸如图1-2中的IoT设备110-118)的一般性描绘。IoT设备301-303位于IoT近程网络160内。IoT设备301-303能够彼此通信(以虚线示出)，并且还能与IoT超级代理/网关145以及在用户电话130处于IoT近程网络160内时与控制器设备/用户电话130直接通信。在某些方面，如果对象(诸如IoT设备301-303)物理地位于预定义的地理边界或类似物理界限内，则这些对象可被定义为属于IoT近程网络160。在一些方面，可能需要能从IoT近程网络160外部的设备/对象访问和/或控制IoT近程网络160内的设备。例如，当用户处于远程位置(诸如，用户的办公室)时，用户可能想要控制和/或接收来自近程网络160中的IoT设备110-118的通知。在一些方面，远程访问还可通过云服务(示为因特网175的一部分)发起，而非由用户或用户的电话130发起。为了支持用户或云服务的此类访问，IoT超级代理/网关145可充当至IoT近程网络160的网关，并且提供用于远程地访问IoT设备110-118和/或用于远程传输来自IoT设备110-118的通知的接口。然而，为了保护IoT近程网络160免遭攻击(诸如，因特网175上的基于因特网的攻击)，IoT超级代理/网关145可基于哪个远程访问和/或远程传输可被启用或禁用来实现一组规则或强加要满足的某些准则。

[0040] 在一个方面，该准则可涉及用户电话130在IoT近程网络160内的存在或不存在。各种其他远程访问和远程传输规则或准则(其可基于例如事件或时间)也是可能的。如本文所讨论的，由用户对近程网络内的IoT设备的远程“访问”可基本上指代由用户发起的第一通信方向(尽管此通信可能涉及IoT设备与用户之间的一些来回交互)。进一步，将注意到，该第一方向还包括可由云服务发起的通信。然而，出于描述的方便起见，本公开将专注于由用户发起的通信，但是将理解，此类通信也可由云服务发起。另一方面，从近程网络内的IoT设备至用户的“远程传输”可指代由IoT设备发起的相反的第二通信方向。这两个通信方向可被统称为“远程通信”，其可包括远程访问以及远程传输，视情况而定。相应地，用于启用或禁用远程通信(远程访问和/或远程传输)的准则可被称为远程通信准则。本文将参照具体示例和场景来描述在远程用户与近程网络中的IoT设备之间的通信的上下文中的各种远程通信准则。然而将理解，这些示例和场景仅是为了说明而提供的，而不应被解释为限定。因此，这些远程通信准则可涵盖可用于基于一个或多个用户在近程网络内的存在或不存在来启用或禁用该用户与近程网络的IoT设备之间的远程通信的任何其他规则或准则。

[0041] 因此，在远程访问规则可基于用户存在性的方面，可实现这些远程访问规则以使

得当用户电话130处于远程位置时，用户电话130可以能够通过IoT超级代理/网关145在因特网175上(在路径306、308上)与IoT设备301-303通信或交互。如先前提到的，因特网175还可包括云服务，该云服务可以能够根据所公开的诸方面来发起远程通信。用户电话130可包括移动应用(诸如控制应用)，该移动应用可被用于远程地控制IoT设备301-303、以及接收来自IoT设备301-303的远程通知。如先前讨论的，允许此类远程访问和/或远程传输可能使IoT近程网络160暴露于来自IoT近程网络160外部的恶意代理或未获授权用户的安全威胁。这些攻击有可能可通过在因特网175上(例如，经由路径308)访问IoT近程网络160和/或通过使用对来自IoT设备301-303的在因特网175上被远程传输的通知的未获授权访问来攻击用户隐私/安全性的方式执行。因此，IoT超级代理/网关145可被配置成在用户可能不需要远程访问时(例如，当用户存在于IoT近程网络160内并因此可以能够访问IoT设备301-303而不依赖于因特网175进行此类访问时)拒绝在此类易受影响的路径上的远程通信(例如，远程访问和/或远程传输)。出于完整性起见，还将注意到，在此情形中拒绝远程通信将意味着云服务(若有)也将被拒绝进行远程通信。

[0042] 在相关方面，IoT超级代理/网关145可首先在用户注册块310将用户电话130注册为授权或注册用户。在一些情形中，这可在用户电话130存在于IoT近程网络160内时通过本地注册(例如，使用用户电话130的电话号码或其他身份)来执行。还可替代或结合用户的身份使用前述控制应用来执行该注册。该注册可涉及本领域技术人员将认识到的附加认证过程(例如要求用户连接至家庭Wi-Fi网络和/或清除口令认证等)。一经注册，用户电话130将作为认识的授权用户(例如，作为主用户)被存储在IoT超级代理/网关145上。在此情形中，假定用户电话130为主用户。

[0043] 尽管未针对多个用户来具体解说，但将领会，在类似的字段下可注册一个或多个用户设备。例如，家庭中的住户或住户子集的移动电话可被注册为授权用户。在一些情形中，用户可以是分等级的，其中不同的规则基于用户等级而适用于不同的用户——例如，在常规家庭中，一个或多个父母或者成人的移动电话可被注册为主用户，而孩子或未成年人的移动电话可被注册为较低等级的二级用户，以使得可基于与用户指定相关联的预定义规则来启用/禁用远程通信。换言之，基于IoT近程网络中的IoT用户设备的注册，用于启用或禁用至IoT近程网络160的远程通信的一个或多个远程通信准则可包括能够与IoT近程网络160中的IoT设备通信的一个或多个IoT设备的集合中的每个IoT用户设备的指定或优先级级别。该IoT用户设备集合可以是基于它们的注册来分等级的。可定义远程通信准则以使得当在IoT近程网络160中检测到一个或多个主用户或高优先级IoT用户设备的存在时禁用针对一个或多个IoT设备的第一集合(例如，热水器、大门进入、烤箱等，未显式地解说)的远程访问/远程传输。然而，仍可为其他等级的用户(诸如二级用户)启用针对IoT设备的第二集合(例如，卧室照明，未显式地解说)的远程通信(包括远程访问/远程传输)。

[0044] 进一步，在一些情形中，禁用远程通信可涉及选择性地禁用与该一个或多个IoT用户设备的所选功能性有关的远程通信能力。例如，关于包括烤箱的IoT设备，有可能在检测到一个或多个主用户存在于IoT近程网络160中时禁用对烤箱的开/关功能性。然而，虽然可在一个或多个主用户存在时针对二级用户禁用该开/关功能性，但该烤箱的功能性子集仍可以是可用的。例如，可使得该子集或所选功能性对二级用户可用。因此，二级用户可以能够监视烤箱是否是开启以及烤箱内正烹饪什么，即使该一个或多个主用户存在于IoT近程

网络160内亦然。

[0045] 远程访问控制规则以及涉及何时可允许远程传输的规则可以是可定制的、提前定义的、以及存储于IoT超级代理/网关145中描绘为远程访问/远程传输控制规则的块314中。IoT超级代理/网关145的图解中还示出了远程访问/远程传输启用/禁用块312，其可被配置成根据块314中确定的远程访问/远程传输控制规则来启用或禁用远程访问或远程传输。

[0046] 存在性检测块316被描绘在IoT超级代理/网关145外部，且至少与远程访问/远程传输启用/禁用块312处于通信中。将理解，不要求存在性检测块316物理地位于IoT超级代理/网关145外部，但在一些方面，存在性检测块316的功能性可在IoT超级代理/网关145内实现，并且甚至更具体地与块310-314中的任一者或多者合并。实质上，存在性检测块316可被配置成检测注册用户或用户电话130在IoT近程网络160内的存在或不存在。存在性检测块316可使用任何已知的发现机制来检测用户电话130的存在/不存在，包括但不限于检测用户电话130至仅在IoT近程网络160内可用的本地网络的连接、基于用户电话130的地理位置(例如，基于全球定位系统(GPS))、和/或借助于发现用户电话130上的控制应用。在一些情形中，存在性检测块316可基于用户电话130的注册(例如，通过周期性地检查用户电话130的注册是否是当前的)来检测存在/不存在。用户电话130可生成向用户注册块310的周期性注册，该周期性注册可被用于将存在性检测块316更新为用户电话130存在于IoT近程网络160内。替换地，存在性检测块316可例如在家庭网络上生成至用户电话130的周期性请求或查验(ping)，以获得对该查验的响应或确认、或获得对注册的周期性刷新。如果阈值数目个此类查验没有得到答复或阈值数目个注册缺失，则存在性检测块316可推断用户电话130已离开IoT近程网络160的场所或邻域。存在性检测块316还可使用用于检测用户存在性的间接手段。例如，IoT设备301-303之一可以是用户的汽车，而用户的汽车存在或不存在可与用户存在或不存在相关。以此方式，来自其他IoT设备的事件/状态更新也可被用于检测用户的存在性。在进一步方面，用户电话130上的控制应用可与存在性检测块316通信以告知存在性检测块关于用户电话130在IoT近程网络160中的存在或不存在(或在一些情形中，对应于用户电话130进入或离开IoT近程网络160)。存在性检测块316还可利用其他平台或发现机制来检测一个或多个注册用户或用户电话130的存在/不存在。

[0047] 基于用户电话130是存在还是不存在于IoT近程网络160中(例如，如由存在性检测块316检测到的)，可在块314中更新用于远程访问/远程传输的控制规则，并可在块312中相应地启用或禁用远程访问/远程传输。再一次，在块314中更新远程访问/远程传输控制规则可进一步基于如由块310提供的用户注册(例如，用户电话130的特定用户是否为其存在/不存在应当确定针对远程通信的启用/禁用决定的主用户)。在一些方面，可为对IoT设备的远程访问、以及为来自IoT设备的通知的远程传输定义相同或共用的控制规则集合。在另一实施例中，可为远程访问和远程传输特征定义分开的控制规则集合。

[0048] 更详细地，远程访问/远程传输控制规则块314将基于用户的注册来确定是否准许远程访问/远程传输。在一种情形中，可仅在用户电话130被指定为主用户且用户电话130位于IoT近程网络160外部(如从存在性检测块316确定的)时启用远程访问/远程传输。类似地，可在用户电话130被指定为主用户且用户电话130存在于IoT近程网络160内(如由存在性检测块316确定的)时禁用远程访问/远程传输。再一次，这些规则更新可基于以下假定：当主用户存在于例如他或她的家里时，对IoT设备301-303的远程访问和/或来自IoT设备

301-303的远程传输是不必要的，因此，IoT超级代理/网关145可关闭用于远程访问和远程传输的路径。

[0049] 在一些情形中，在存在一个以上主用户的情况下，可用若干方式来定制块314中的远程访问/远程传输控制规则。例如，如果IoT近程网络160中有一个或多个附加IoT用户设备(诸如用户电话130，但未显式地示出)，则启用/禁用远程通信可基于对这多个IoT用户设备的子集或任一者在IoT近程网络160中的存在/不存在检测。可单独地配置与该一个或多个IoT用户设备中的每个IoT用户设备有关的远程通信准则。禁用/启用远程通信可基于涉及特定IoT用户设备以及对应的远程通信准则的各种组合。

[0050] 例如，可仅在被指定为主用户的所有IoT用户设备都在IoT近程网络160内时禁用远程访问/远程传输(例如，当一个家庭的父母双方都在家时，远程访问/远程传输可以是不需要的，因而可被禁用)。替换地，可在主用户中的任一者或任何预定义子集在IoT近程网络160内时禁用远程访问/远程传输(例如，当父母一方在家时，可针对父母另一方禁用远程访问/远程传输)。在又一替换方案中，可在检测到主用户中的任一者在IoT近程网络160外部时启用远程访问/远程传输(例如，当检测到父母双方中的任一方已离开家时，可启用远程访问/远程传输)。遵循以上方式的各种其他替换方案和定制也落在各实施例的范围之内。一般而言，一个或多个控制器设备在近程网络中的存在或不存在可被用作确定是禁用还是启用去往/来自近程网络中的IoT设备的远程访问/远程传输的准则。

[0051] 虽然块314中的远程访问/远程传输控制规则可按以上方式涉及用户电话130的存在或不存在，但附加地或替换地，远程访问/远程传输控制规则也可涉及事件或时间功能。作为可用于影响对启用/禁用远程访问/远程传输的决定的事件的示例，IoT近程网络160内的一个或多个IoT设备301-303可触发更新(诸如紧急情况或故障)，该更新可与其他远程访问/远程传输控制规则结合使用。在具体解说中，IoT设备(诸如热水器)的崩溃或故障可触发去往IoT超级代理160的紧急情况通知。在此情形中，如果IoT超级代理160意识到即使第二主用户存在于IoT近程网络160内但一个主用户(例如先前被指定为在此类紧急状况中要求远程访问的第一主用户)不在IoT近程网络160内(例如，基于来自存在性检测块316的输入)，也可在块314中更新远程访问/远程传输控制规则以指令远程访问/远程传输启用/禁用块312为该第一主用户准予远程访问/启用远程传输。此远程访问/远程传输控制规则更新可超驰先前配置的控制规则(例如，仅在所有主用户都不存在时启用远程访问/远程传输)。各种其他此类定制可能基于事件，而不会脱离本公开的范围。

[0052] 块314中的远程访问/远程传输控制规则还可基于一天或一周里的时间。例如，无论所指定的主用户是否存在于IoT近程网络160中，块314中的远程访问/远程传输控制规则可被设置成使得在某些时段期间禁用远程访问/远程传输。例如，可从10PM到6AM关闭远程访问/远程传输。在办公室环境的情形中，取决于特定偏好和安全性要求，远程访问/远程传输可在一周中的工作时间期间关闭，而仅在下班后或周末启用，或者反之。块314中的远程访问/远程传输控制规则还可基于用户存在/不存在与一天里的时间的组合来定义。例如，如果家庭的给定主用户(例如，妻子)存在于IoT近程网络160内，则远程访问/远程传输控制规则可能涉及禁用对IoT设备(诸如烤箱(未显式地示出))的远程访问，除了星期五晚上5pm到8pm之间，此时该家庭的另一主用户(例如，丈夫)很可能操作烤箱准备星期五晚餐。

[0053] 因此，各实施例可涉及基于用户存在性、一天/一周里的时间、和/或一般地基于上

述准则中的一者或多者的任何其他组合来控制对远程访问/远程传输的启用或禁用。启用远程访问/远程传输的相关方面还可类似地基于用户存在/不存在、以及可任选地基于附加远程访问准则。例如，如果授权用户(例如，主用户)被确定为将不会存在于(或被确定为将不存在于)IoT近程网络160中，则在启用远程访问/远程传输之前，可在远程访问/远程传输控制规则块314中可任选地检查某些附加准则。如果这些附加准则也被满足，则可在块312中启用远程访问/远程传输。在一些情形中，可能没有附加准则，且如果检测到用户不存在，则可启用远程访问/远程传输。

[0054] 在一些方面，块314中的远程访问/远程传输控制规则还可被配置成基于操作不同IoT设备的一个或多个主用户来针对这些不同IoT设备不同地定义远程通信准则。例如，远程访问/远程传输控制规则可被配置成用于如果已确定第一主用户(例如，丈夫)不存在于IoT近程网络160中，则启用对IoT设备(诸如热水器、HVAC系统、以及家庭影院系统(这些设备未显式地解说))的远程访问/远程传输。进一步，远程访问/远程传输控制规则可被配置成用于在确定该第一主用户存在于IoT近程网络160中时禁用对这些IoT设备的远程访问/远程传输。在另一相关示例中，远程访问/远程传输控制规则可被配置成用于当确定第二主用户(例如，妻子)不存在于IoT近程网络160中时，启用对IoT设备(诸如洗衣机/干衣机和烤箱(未显式地解说))的远程访问/远程传输。进一步，远程访问/远程传输控制规则可被配置成用于在确定该第二主用户存在于IoT近程网络160中时禁用对这些IoT设备的远程访问/远程传输。因此，远程访问/远程传输控制规则可被配置成使得所选的一个或多个IoT设备与一个或多个主用户中的一个特定主用户相关联，并且在确定相关联的主用户不存在于IoT近程网络中时启用针对这些所选的一个或多个IoT设备的远程访问/远程传输，以及在确定相关联的主用户存在于IoT近程网络中时禁用其相应的远程访问/远程传输。

[0055] 将领会，各实施例包括用于执行本文中所公开的过程、功能和/或算法的各种方法。例如，如图4中解说的，实施例可包括控制对包括一个或多个物联网(IoT)设备(例如，IoT设备301-303)的IoT近程网络(例如图3的IoT近程网络160)的远程访问的方法，该方法包括：检测IoT用户设备存在于IoT近程网络中(例如使用存在性检测块316来检测用户电话130在IoT近程网络中的存在/不存在)-框402；确定是否满足用于禁用与IoT近程网络中的一个或多个IoT设备的远程通信的一个或多个远程通信准则(例如，块314的远程访问/远程传输控制规则)-框404；以及如果IoT用户设备存在于IoT近程网络中并且如果满足用于禁用远程通信的远程通信准则，则(例如由IoT超级代理/网关145的远程访问/远程传输启用/禁用块312)禁用远程通信-框406。

[0056] 类似地，另一实施例可包括控制与包括一个或多个物联网(IoT)设备(例如，IoT设备301-303)的IoT近程网络(例如图3的IoT近程网络160)的远程通信的方法，该方法包括：检测IoT用户设备不存在于IoT近程网络中(例如使用存在性检测块316来检测用户电话130在IoT近程网络中的存在/不存在)-框502；确定是否满足用于启用与IoT近程网络中的一个或多个IoT设备的远程通信的一个或多个远程通信准则(例如，借助于块314的远程访问/远程传输控制规则)-框504；以及如果IoT用户设备不存在于IoT近程网络中并且如果满足用于启用远程通信的远程通信准则，则启用远程通信-框506。

[0057] 一般而言，除非另外明确声明，否则如贯穿本公开所使用的短语“配置成……的逻辑”旨在援引至少部分地用硬件实现的方面，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(经由硬件或经由硬件和软件的组合)。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。

[0058] 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。

[0059] 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。

[0060] 结合本文中公开的方面描述的各种解说性逻辑块、模块、以及电路可用设计成执行本文中描述的功能的通用处理器、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)。

[0061] 结合本文所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。在替换方案中，处理器和存储介质可作为分立组件驻留在用户终端中。

[0062] 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。

[0063] 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公开的范围。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。

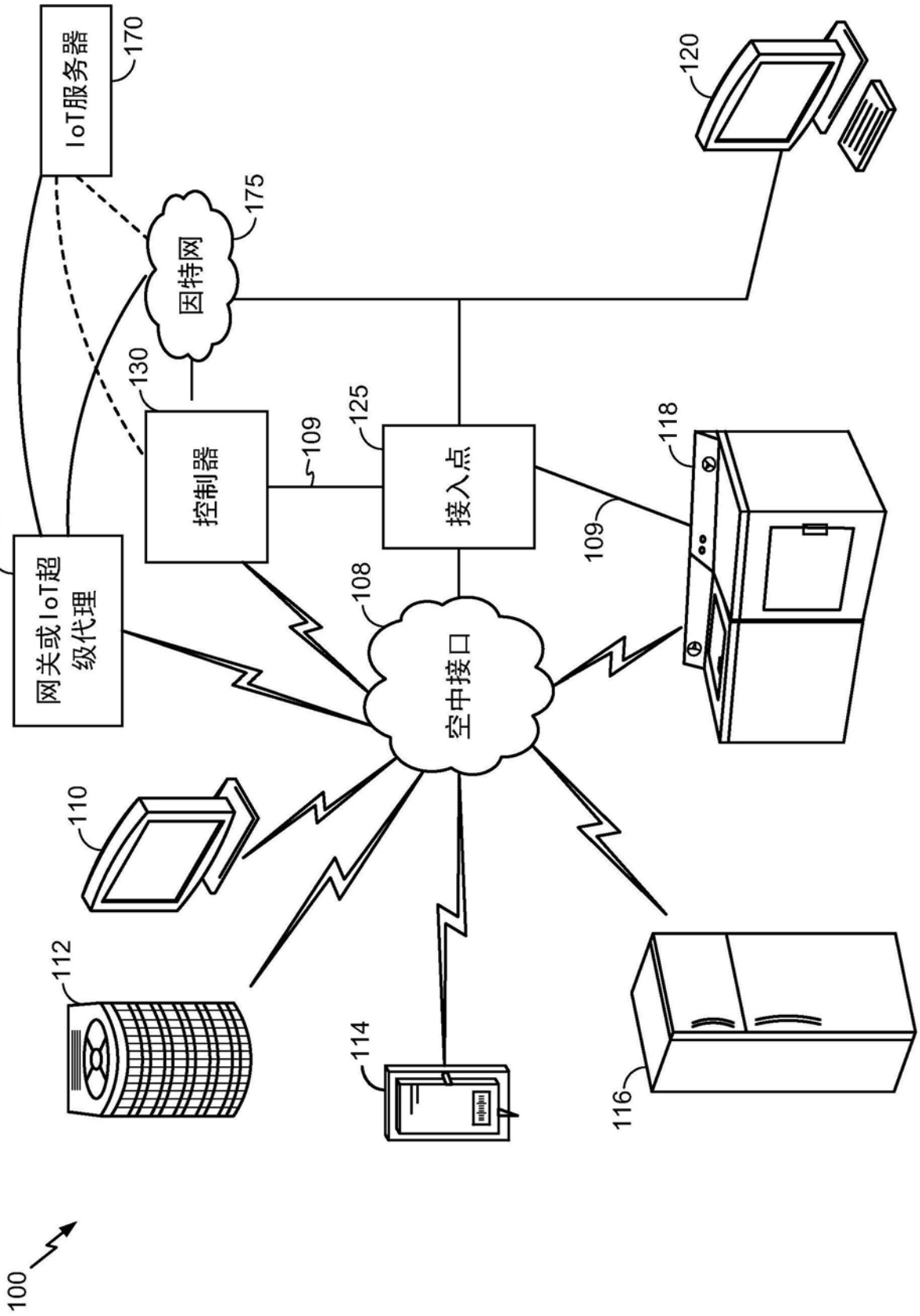

IoT服务器
170
120
因特网
175
130
125
109
控制器
接入点
118
145
网关或IoT超级代理
108
空中接口
109
110
112
114
116
100

图1

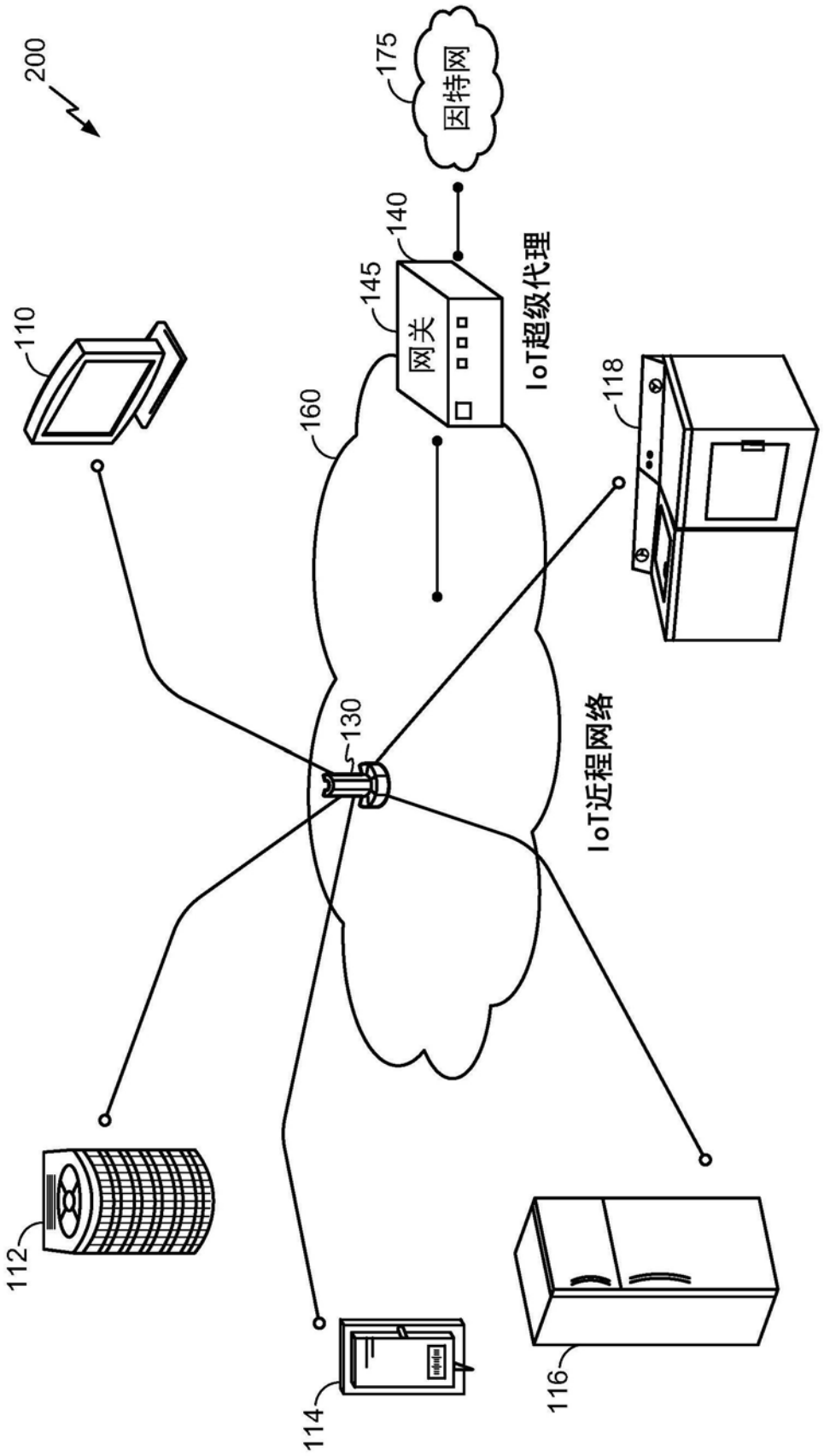

200
175
因特网
140
145
网关
IoT超级代理
110
160
118
130
IoT近程网络
112
114
116

图2

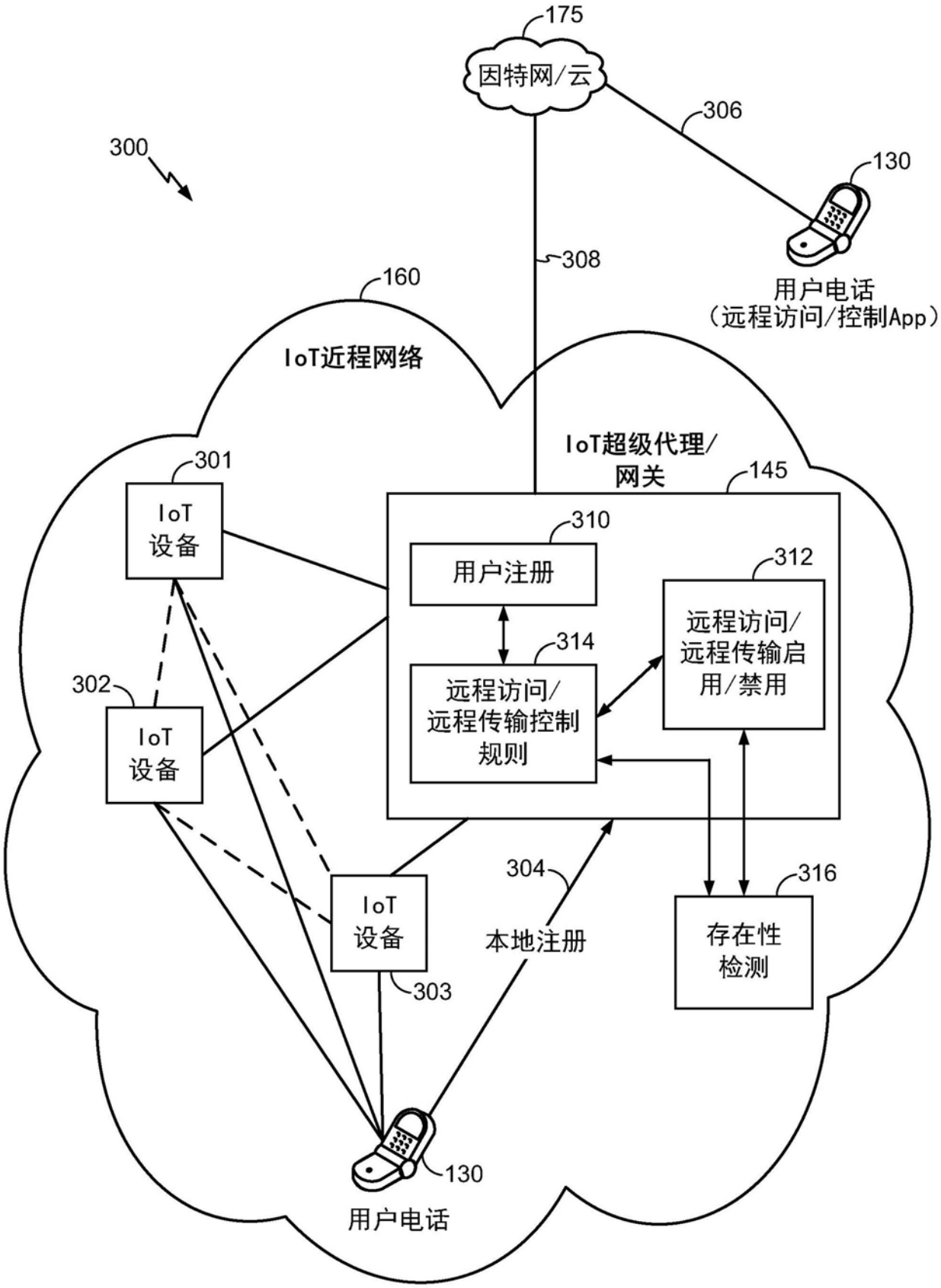

175
因特网/云
306
300
130
308
用户电话
（远程访问/控制App）
160
IoT近程网络
IoT超级代理/
网关
145
301
IoT
设备
310
用户注册
312
远程访问/
远程传输启
用/禁用
314
302
IoT
设备
远程访问/
远程传输控制
规则
304
316
IoT
设备
本地注册
存在性
检测
303
130
用户电话

图3

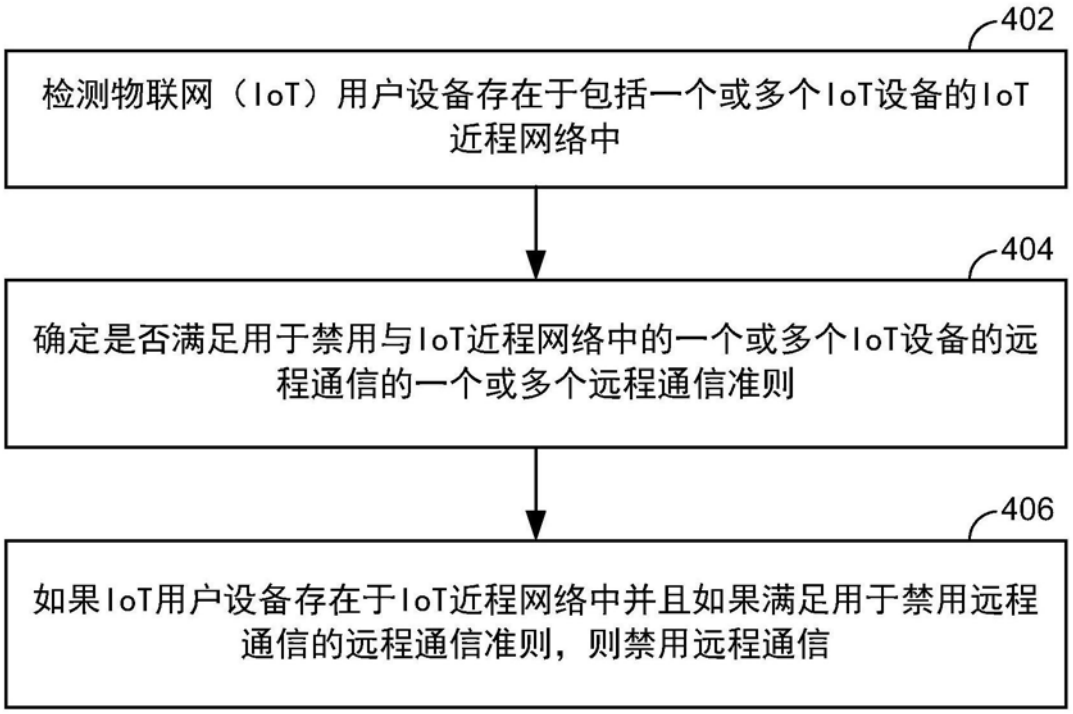

402
检测物联网（IoT）用户设备存在于包括一个或多个IoT设备的IoT近程网络中
404
确定是否满足用于禁用与IoT近程网络中的一个或多个IoT设备的远程通信的一个或多个远程通信准则
406
如果IoT用户设备存在于IoT近程网络中并且如果满足用于禁用远程通信的远程通信准则，则禁用远程通信

图4

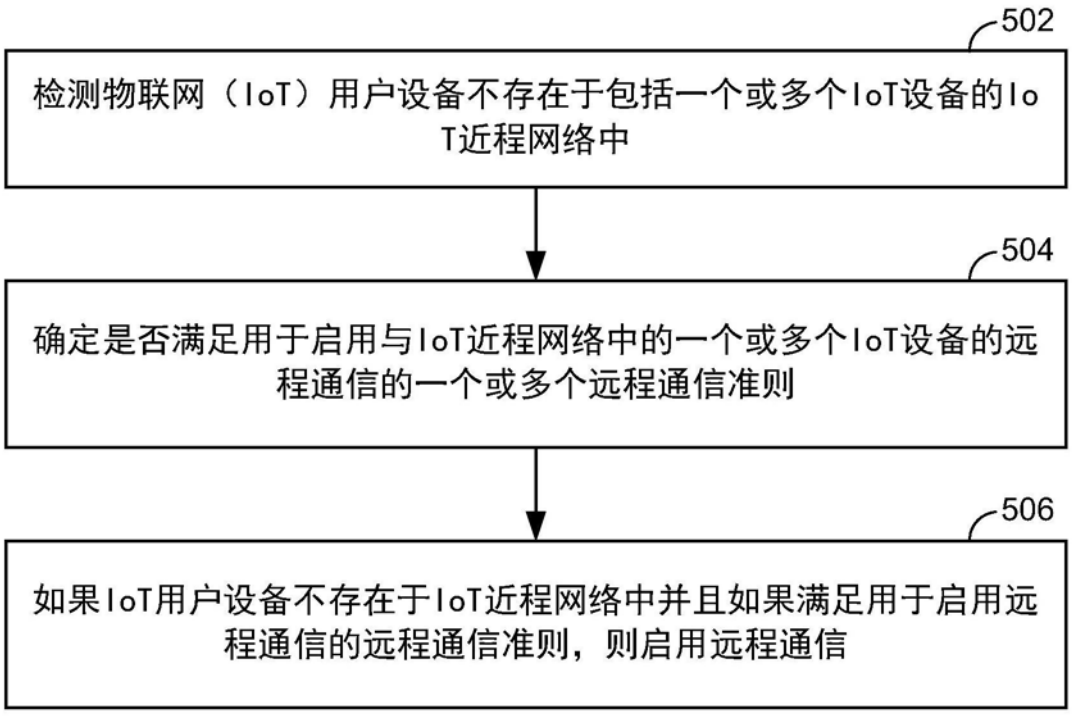

502
检测物联网（IoT）用户设备不存在于包括一个或多个IoT设备的IoT近程网络中
504
确定是否满足用于启用与IoT近程网络中的一个或多个IoT设备的远程通信的一个或多个远程通信准则
506
如果IoT用户设备不存在于IoT近程网络中并且如果满足用于启用远程通信的远程通信准则，则启用远程通信

图5