(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 113261319 A
(43)申请公布日 2021.08.13

(21)申请号 202080008670.1

(22)申请日 2020.01.09

(30)优先权数据
19151166.6 2019.01.10 EP

(85)PCT国际申请进入国家阶段日
2021.07.09

(86)PCT国际申请的申请数据
PCT/EP2020/050351 2020.01.09

(87)PCT国际申请的公布数据
WO2020/144248 EN 2020.07.16

(71)申请人 昕诺飞控股有限公司
地址 荷兰埃因霍温

(72)发明人 M•M•西拉吉
H•U•O•N•范德拉尔斯霍特

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 刘红 陈岚

(51)Int.Cl.
H04W 12/122(2021.01)
H04L 29/06(2006.01)
H05B 47/19(2020.01)
H04L 12/28(2006.01)

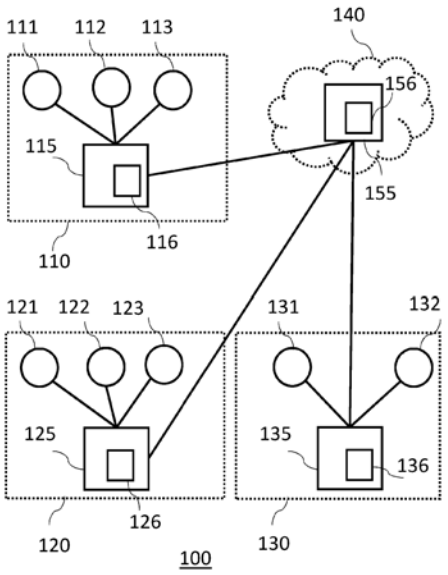
权利要求书2页 说明书11页 附图5页

(54)发明名称

提供照明网络的安全操作的方法

(57)摘要

一种提供照明网络的安全操作的方法，该照明网络包括被布置用于照亮环境的照明设备和用于控制照明设备的本地控制器，其中照明网络进一步是由照明网络外部的外部控制器可控的，其中该方法包括：确定照明网络的配置状态；分析所确定的配置状态；基于分析，在正常模式与安全模式之间切换照明网络的操作模式；其中在正常模式中，照明网络被可操作地连接至外部控制器，并且照明设备的灯光渲染功能正由外部控制器根据预定功能集合来控制，以及其中在安全模式中，照明设备的灯光渲染功能正由外部控制器根据预定功能集合的子集来控制。



CN 113261319 A

1.一种提供照明网络的安全操作的方法,所述照明网络包括被布置用于照亮环境的照明设备和用于控制所述照明设备的本地控制器,其中所述照明网络进一步是由所述照明网络外部的外部控制器可控的,其中所述方法包括:

确定所述照明网络的配置状态,其中配置包括所述照明网络的元件的功能布置,以及其中所述配置状态包括所述元件之中的一些或所有元件的表示;

分析所确定的配置状态,其中所确定的配置状态的分析基于所述照明网络的脆弱性;

基于所述分析,在正常模式与安全模式之间切换所述照明网络的操作模式;

其中在所述正常模式中,所述照明网络被可操作地连接至所述外部控制器,并且所述照明设备的灯光渲染功能正由所述外部控制器根据预定功能集合来控制,以及

其中在所述安全模式中,所述照明设备的所述灯光渲染功能正由所述外部控制器根据所述预定功能集合的子集来控制。

2.根据权利要求1所述的方法,其中分析的所述步骤包括:

检测是否所确定的配置状态需要改变;以及

其中所述方法进一步包括:

基于所述检测,将所述照明网络的操作模式从所述正常模式切换到所述安全模式;

在所述安全模式中改变所述照明网络的配置;

在所述配置被改变之后,将所述照明网络的操作模式从所述安全模式切换到所述正常模式。

3.根据权利要求2所述的方法,其中当所确定的配置状态指示所述照明网络的不安全操作时,所确定的配置状态需要改变。

4.根据权利要求2所述的方法,其中所述配置的改变由所述外部控制器执行。

5.根据权利要求2所述的方法,其中所述配置的改变由所述本地控制器执行,以及其中所需的配置被存储在所述本地控制器中,并且所述照明网络的配置基于所述存储的所需配置来改变。

6.根据权利要求1所述的方法,其中在所述安全模式中,所述照明网络进一步被布置成可操作地与所述外部控制器断开连接,并且所述照明渲染功能正由所述本地控制器控制。

7.根据权利要求6所述的方法,其中在所述安全模式中,旨在用于所述外部控制器的信息被存储在所述本地控制器中,并且所述信息在恢复所述正常模式时被传送。

8.根据权利要求7所述的方法,其中所述照明网络进一步包括传感设备,以及其中所述信息是传感数据、状态数据、控制数据、配置数据、诊断数据、维护请求、数据处理请求之中的一个或多个。

9.根据权利要求1所述的方法,其中在所述安全模式中,所述照明网络被布置用于广告安全危害的类型和/或所需的配置。

10.根据权利要求1所述的方法,其中确定所述照明网络的配置状态的所述步骤基于触发器,以及其中所述触发器生成是基于时间的,以致所述触发器被周期性地生成。

11.根据权利要求1所述的方法,其中确定所述照明网络的配置状态的所述步骤基于触发器,以及其中所述触发器生成是基于事件的,以致在所述照明网络中观察到恶意活动时,所述触发器被生成。

12.根据权利要求1所述的方法,其中确定所述照明网络的配置状态的所述步骤基于触

发器,以及其中在针对当前配置的更新是可用的时候,所述触发器被生成。

13.根据权利要求1所述的方法,其中所述分析通过使用网络行为分析中的异常检测来执行,以及其中所述异常检测使用统计方法、基于规则的方法、基于距离的方法、基于剖析的方法和基于模型的方法之中的至少一个。

14.一种用于提供照明网络的安全操作的控制器,所述照明网络包括被布置用于照亮环境的照明设备和用于控制所述照明设备的本地控制器,其中所述照明网络进一步是由所述照明网络外部的外部控制器可控的,其中所述控制器包括:

输入和输出接口;

通信单元;

存储器;和

处理器,用于执行根据任一前述权利要求的方法。

15.一种计算机程序产品,其包括被配置成执行权利要求1-13的方法的步骤的指令。

提供照明网络的安全操作的方法

技术领域

[0001] 本发明涉及提供照明网络的安全操作的方法。本发明进一步涉及提供照明网络的安全操作的控制器和计算机程序产品。

背景技术

[0002] 连接的照明指的是非利用(或不仅利用)传统的有线、电气开关或调光电路而是经由有线的或更经常无线的连接例如有线或无线网络、通过使用数据通信协议来控制的一个或多个照明设备的系统。这些连接的照明网络形成俗称的Internet of Things(物联网)(IoT)或更具体地说Internet of Lighting(照明因特网)(IoL)。典型地,照明设备或甚至照明设备内的个别灯可以各自被配备有无线接收机或收发机,用于根据无线联网协议诸如Zigbee、Wi-Fi或Bluetooth(蓝牙)从照明控制设备接收照明控制命令。

[0003] IoT解决方案诸如连接的照明是通过网络和云来交换数据和提供控制功能的设备与传感器的复杂网络。随着越来越多的数据被暴露于越来越多的应用,安全性变成主要的挑战。具有网络连接性的网络设备诸如照明网络中连接的照明设备是脆弱的。

[0004] 利用IoT照明设备收集的个人数据对数据黑客和身份窃贼具有价值。并且,针对IoT解决方案的网络攻击具有削弱(cripple)物理服务和照明基础设施的潜力。虽然IoT安全性的重要性得到广泛理解和认同,但是IoT安全性的实际设计和实现带来新的挑战和机遇。为了提高安全性和降低黑客攻击的风险,使用不同的安全措施,诸如使用端到端密码算法,从而提供安全修复(fix)和软件更新。

[0005] US20160315955A1披露一种用于从网络内的智能家电中检测恶意行为的方法。收集有关网络内的智能家电的网络流量(traffic)数据和识别数据。数据被发送至行为分析引擎,而行为分析引擎计算可能由于恶意行为而引起的网络流量内的异常的置信水平。基于置信水平,与异常有关的网络流量被阻塞。

发明内容

[0006] 发明人已认识到:IoT设备诸如资源受限的照明设备经常具有有限的计算能力和存储容量,从而使之难以使用需要比照明设备所提供的更多的资源的复杂密码算法。发明人已进一步认识到:利用定期安全修复和更新进行的IoT照明设备的更新经常没有按时执行。例如,在基于家庭的环境中,用户或没有意识到更新的需求或相信更新是需要训练有素的技术人员的困难过程。这在其中用户可能没有认证(authentication)权限来执行更新(例如,只有楼宇或办公室管理员才可以这样做)的基于办公室或室外环境中可能变得甚至更加复杂。因此,大量的IoT照明设备将利用旧的软件(固件)来操作并且可能引起安全威胁。

[0007] 因此,尤其鉴于照明网络中的照明设备的限制,本发明的目的是克服至少一些上面提出的问题和其他相关的网络安全问题并且提供照明网络的安全操作。在本发明的上下文中,因为几乎不可能提供无风险的绝对安全的操作,所以应该明白:“with secure

operation(利用安全操作)”,这意味着提供增强的操作安全性。

[0008] 根据第一方面,该目的利用一种提供照明网络的安全操作的方法来实现,该照明网络包括被布置用于照亮环境的照明设备和用于控制照明设备的本地控制器,其中照明网络进一步是由照明网络外部的外部控制器可控的,其中该方法包括:确定照明网络的配置状态;分析所确定的配置状态;基于分析,在正常模式与安全模式之间切换照明网络的操作模式;其中在正常模式中,照明网络被可操作地连接至外部控制器,并且照明设备的灯光渲染功能正由外部控制器根据预定功能集合来控制,以及其中在安全模式中,照明设备的灯光渲染功能正由外部控制器根据预定功能集合的子集来控制。

[0009] 该方法给照明网络的操作提供增强的安全性。该方法包括:确定照明网络的配置状态。配置可以包括元素诸如软件和/或硬件的功能布置;其中配置状态可以是一些或所有这样的元素的表示,诸如硬件、软件和/或设备设置的版本。在示例中,软件可以是固件,并且配置状态可以是固件的版本。配置状态的确定可以包括:确定所使用的软件和/或照明网络的设备设置的版本。照明网络的配置状态可以表示照明网络的照明设备或照明设备的个别组件的配置状态。

[0010] 该方法进一步包括:分析所确定的照明网络的配置状态。例如,针对所确定的配置状态的分析可以鉴于以下之中的一个或多个来执行:是否所确定的配置状态是例如可用于软件的最新版本;是否所确定的配置状态容易受到已知的安全威胁;是否网络流量显示任何恶意活动的迹象,诸如网络流量中操作的恶意软件。该分析可以在网络行为分析中使用异常检测来执行,这是通过监控流量和注意不寻常的动作或与正常操作的偏离(departure)来增强网络安全性的一种方式。

[0011] 基于分析,该方法进一步包括:在正常模式和安全模式之间切换照明网络的操作模式。在正常模式中,照明网络被可操作地连接至外部控制器,并且照明设备的灯光渲染功能正由外部控制器根据预定功能集合来控制。预定功能集合可以包括:照亮环境;和/或改变照明设备的光源之中的一个或多个光源的颜色、色温、强度、光束宽度、光束方向、光照强度、其他参数之中的一个或多个。

[0012] 在安全模式中,照明设备的灯光渲染功能正由外部控制器根据预定功能集合的子集来控制。预定功能集合的子集可以包括例如照亮环境。在典型的IoT系统中,IoT设备的操作基于连接性,例如,至互联网的连接性,并且与这样的外部网络断开连接引起整个系统的操作故障。这对于仍然能够利用有限的连接性或没有至外部控制器的连接性而在安全模式中本地操作的照明网络来说是不同的。因此,尽管具有在照明网络中的照明设备的限制,该方法仍提供照明网络的安全操作。

[0013] 在实施例中,其中分析的步骤可以包括:检测是否所确定的配置状态需要改变;以及其中该方法可以进一步包括:在安全模式中改变照明网络的配置;在配置被改变时,将照明网络的操作模式从安全模式切换到正常模式。当所确定的配置状态指示照明网络的不安全操作时,所确定的配置状态可能需要改变。

[0014] 例如,当在网络流量中检测到异常和/或接收到关于与所确定的配置状态相关联的脆弱性的指示时,不安全的操作可以指示照明网络对于安全风险的脆弱操作。基于这样的检测,该方法可以包括将照明网络的操作模式例如从正常模式切换到安全模式并且可以进一步包括改变配置。配置的改变可以包括更新、升级或降级配置和/或改变设备设置。例

如,利用不同的版本来更新固件。配置的改变可以例如在安全模式中由外部控制器执行。在指示照明网络的安全操作的配置已被改变之后,照明网络的操作模式可以被切换至正常模式。对于预定测试时间周期,操作模式可以被切换到正常模式,例如,以测试网络安全性。如果网络流量被观察为安全的,例如,没有异常被发现,则操作模式可以被保持为正常模式。可供选择地,操作模式被切换回到安全模式,并且可以使用不同的配置。

[0015] 在实施例中,配置的改变可以由本地控制器执行,以及其中所需的配置可以被存储在本地控制器中,并且照明网络的配置可以基于所述存储的所需配置来改变。

[0016] 作为经由外部控制器改变配置的替代方案,所需的配置可以被存储在本地控制器中。例如,本地控制器可以从外部控制器接收所需的配置,例如,软件和/或设备设置,并且可以将它存储在存储器中。本地控制器随后可以被布置用于例如在安全模式中改变照明网络的配置。

[0017] 在安全模式中,照明网络可以进一步被布置成可操作地与外部控制器断开连接,并且照明渲染功能正由本地控制器控制。

[0018] 当照明网络与外部控制器的任何形式的连接可能引起安全风险时,照明网络可以进一步被布置成可操作地与外部控制器断开连接。在这个示例中,预定功能集合的子集是空集,即,外部控制器不控制照明设备的灯光渲染功能。本地控制器可以被布置用于根据预定功能集合的子集来控制照明设备的灯光渲染功能,例如,本地控制器可以被布置用于控制照明设备,以照亮环境。

[0019] 在安全模式中,旨在用于外部控制器的信息可以被存储在本地控制器中,并且所述信息可以在恢复正常模式时进行传送。照明网络可以进一步包括传感设备,以及其中所述信息是传感数据、状态数据、控制数据、配置数据、诊断数据、维护请求、数据处理请求之中的一个或多个。

[0020] 此外,照明网络可以进一步包括传感设备、HVAC装备、火警警报器等等。这些设备可能必须与外部控制器传送传感信号或其他信号。这个信息可能旨在用于外部控制器,以致该信息被处理,例如,用于控制、维护、诊断、End-of-Life(临终)(EoL)分析等等。外部控制器可以被定位在远程服务器诸如云中,这提供在远程服务器中处理信息的计算优势。在安全模式中,旨在用于外部控制器的信息可以被存储在本地控制器中,并且所述信息在恢复正常模式时被传送。

[0021] 在安全模式中,照明网络可以被布置用于广告(advertise)安全危害的类型和/或所需的配置。

[0022] 例如,基于分析,照明网络可以广告安全危害的类型,例如,检测到的某些异常和/或可能最适合于解决脆弱性的所需配置。

[0023] 确定照明网络的配置状态的步骤可以基于触发器(trigger),以及其中触发器生成可以是基于时间的,以致触发器周期性地、在随机时刻或在预定时刻被生成。

[0024] 确定能够基于触发器来启动,以致触发器可以及时例如周期性地、随机等等被生成。这样的基于时间的触发器维持针对配置状态的及时检查并且使得配置状态保持为最新的。

[0025] 确定照明网络的配置状态的步骤可以基于触发器,以及其中触发器生成可以是基于事件的,以致在照明网络中观察到恶意活动时,可以生成触发器。

[0026] 附加地或可供选择地，触发器可以基于事件来生成。这样的事件的示例可以包括以下之中的一个或多个：当在照明网络中观察到恶意活动时，当照明设备开始以意想不到的方式行为时，通信信号被丢弃和/或被改道(reroute)至错误的目的地，缺乏或没有控制照明设备。

[0027] 确定照明网络的配置状态的步骤可以基于触发器，以及其中触发器在针对当前配置的更新是可用的时候被生成。

[0028] 附加地或可供选择地，触发器可以基于接收到更新配置的可用性的指示来生成，以致使得用户意识到：配置是较旧的并且必须被改变。

[0029] 可以通过使用网络行为分析中的异常检测来执行分析，以及其中异常检测可以使用至少以下之一：统计方法；基于规则的方法；基于距离的方法；基于剖析(profiling)的方法；基于模型的方法。

[0030] 根据第二方面，该目的利用一种用于提供照明网络的安全操作的控制器来实现，该照明网络包括被布置用于照亮环境的照明设备和用于控制照明设备的本地控制器，其中照明网络进一步是由照明网络外部的外部控制器可控的，该控制器包括用于执行根据第一方面的方法的处理器。该控制器可以进一步包括分别输入与输出接口以及存储器。至控制器的输入可以是触发信号，用于根据第一方面来启动确定。控制器的输出可以是至用户的更新信号，其指示：配置被改变。存储器可以用于存储所需的配置。

[0031] 根据第三方面，该目的利用计算机程序产品来实现，其中计算机程序产品包括被配置成当在根据第二方面的控制器上执行时根据第一方面执行的指令。

[0032] 应明白：计算机程序产品和系统可以具有与上述方法相类似和/或相同的实施例和优点。

附图说明

[0033] 所披露的系统、设备和方法的上面以及附加的目的、特性和优点通过参考附图的系统、设备和方法的实施例的以下说明性的且非限制的详细描述将被更好地理解，其中：

图1示意性地和例示性地显示包括照明网络和用于提供照明网络的安全操作的外部控制器的系统，

图2示意性地和例示性地显示举例说明提供照明网络的安全操作的方法的实施例的流程图，

图3示意性地和例示性地显示举例说明提供照明网络的安全操作的方法的另一实施例的流程图，

图4示意性地和例示性地显示照明网络和举例说明改变照明网络的配置的实施例的本地控制器，和

图5示意性地和例示性地显示用于提供照明网络的安全操作的控制器。

[0034] 所有的图是示意性的而不一定按比例，并且一般仅显示为了阐明本发明而是必要的部分，其中其他的部分可以被省略或只是被建议。

具体实施方式

[0035] IoT系统中的IoT设备诸如连接的照明系统中的照明设备的安全性面临着许多公

开的挑战。具体地，IoT照明设备具有的常见问题是：它们时常是资源受限的，以致它们并不包含实现高级安全措施诸如端到端加密技术所必要的计算资源。

[0036] 如所提及的，利用IoT照明设备所收集的个人数据对数据黑客和身份盗贼具有价值。并且，针对IoT解决方案的网络攻击具有削弱物理服务和照明基础设施的潜力。在基于家庭的环境中，由于安全漏洞，例如，用户可能失去远程控制他/她家的照明设备，用于照明设备的通信和/或控制信号可能被丢弃和/或被改道至错误的目的地。此外，照明设备可能开始以反常的方式行为，例如，突然地照明设备在晚上以全亮度被通电或在用户家中的所有照明设备停电。在安全破坏(breach)的极端情况中，照明网络可能将关于用户存在/缺席的信号发射至未知的远程设备/服务器，从而导致盗窃或其他的严重后果。

[0037] 在办公环境中，停电可能导致若干安全问题。在任何拥挤的位置诸如剧院或电影院，照明设备的反常行为诸如停电、反常闪烁等等可能在人群中引起混乱，从而导致严重后果。在人们正在其中工作的工厂，这样的照明设备的反常可能危及人类生命。这些是其中连接的照明系统的安全性是非常必要的这样的情况的一些示例，并且安全破坏可能导致经济后果而且甚至危及人类生命。也可以考虑其他的示例。本发明为照明网络的操作提供增强的安全性，以致能够避免这些安全折中(compromise)。

[0038] 图1示意性地和例示性地显示包括照明网络110的系统100。在这个示例中，照明网络110包括三个照明设备111-113。照明网络110可以包括一个或多个照明设备。照明设备111-113是这样的设备或结构，其被布置成发出适合于照亮环境的光，从而在足以达到那个目的的规模上提供光照或实质上有助于光照。照明设备111-113包括至少一个光源或灯，诸如基于LED的灯、气体放电灯或白炽灯泡等等，任选地，任何相关联的支架、外壳或其他这样的外罩。照明设备111-113之中的每一个可以采取各种各样形式之中的任何形式，例如吸顶式照明器、壁挂式照明器、洗墙灯(wall washer)或落地式照明器(并且这些照明器不一定都必须是同一类型的)。

[0039] 照明网络110进一步包括本地控制器115和通信单元116，其中通信单元116被例示性地显示为被包括在本地控制器115中。然而，通信单元116对于本地控制器115而言能够是外部的。通信单元116能够是用于从照明网络110接收通信信号和发射通信信号至照明网络110的网关。网关是用于网络的一块联网(networking)硬件，其允许数据从一个离散网络流向另一离散网络。例如，照明网络110可以进一步包括：(未显示在图中)传感设备；火警警报器；HVAC装备，用于加热、通风和冷却等等。传感设备可以包括运动传感器(诸如PIR传感器)、用于检测环境光水平的光传感器、温度传感器、湿度传感器、气体传感器诸如CO2传感器、粒子测量传感器、音频传感器和成像传感器诸如照相机。取决于应用或情况，多种传感器类型的不同组合是可能的。

[0040] 本地控制器115可以被布置用于控制照明设备111-113的操作。本地控制器115可以是开关，例如，传统的墙壁开关。本地控制器115可以是传感设备，例如，温度传感器、存在传感器，并且可以被布置用于生成传感信号，其中照明设备111-113可以被布置成基于所生成的传感信号来控制。本地控制器115可以被布置用于经由有线装置或无线装置例如通过使用无线协议诸如Wi-Fi、Bluetooth或Zigbee等等来控制照明设备111-113。本地控制器115可以是计算机软件，其可以基于编程的规则。本地控制器115可以被实现在照明设备111-113之中的每一个照明设备中。本地控制器115可以被实现在照明设备111-113的外部。

[0041] 本地控制器115可以进一步包括处理器(未显示)和存储器(未显示),其中本地控制器115可以被提供在单芯片或集成电路或者多芯片或集成电路中,任选地,本地控制器115可以作为芯片组、专用集成电路(ASIC)、现场可编程门阵列(FPGA)、数字信号处理器(DSP)、图形处理单元(GPU)等等来提供。

[0042] 系统100可以进一步包括照明网络110外部的外部网络120和130。这些网络120-130被例示性地显示为照明网络,但是它们可以是其他形式的网络,例如,计算机网络。外部网络120包括三个照明设备121-123、控制器125和通信单元126,其中通信单元126被例示性地显示为被包括在控制器125中。然而,通信单元126对于本地控制器125而言能够是外部的。通信单元126能够是用于从外部网络120接收通信信号和发射通信信号至外部网络120的网关。外部网络130包括两个照明设备131-132、控制器135和通信单元136,其中通信单元136被例示性地显示为被包括在控制器135中。然而,通信单元136对于本地控制器135而言能够是外部的。通信单元136能够是用于从外部网络130接收通信信号和发射通信信号至外部网络130的网关。例如,外部网络120-130可以进一步包括:(未显示)传感设备;HVAC装备(未显示),用于加热、通风和冷却等等。

[0043] 系统100可以进一步包括外部控制器155和通信单元156,其中通信单元156被例示性地显示为被包括在外部控制器155中。外部控制器155对于照明网络110而言是外部的。在这个例示图中,外部控制器155被显示为被定位在远程服务器140中。外部控制器155可以被定位在外部网络120-130中。外部控制器155经由通信单元156被布置用于与照明网络110和外部网络120-130通信。在这个例示图中,外部网络120-130被布置用于经由外部控制器155与照明网络110通信。可供选择地或附加地,照明网络110可以具有与外部网络120-130的直接通信链路。

[0044] 在示例中,系统100可以位于建筑物例如办公室、住宅小区、购物中心、杂货店、电影院、剧院、工厂等等中。照明网络110 可以被定位在建筑物的房间中。外部网络120-130可以被定位在建筑物的其他房间中。外部控制器155可以被定位在远程服务器140中,例如,被定位在用户设备诸如移动电话、膝上型计算机或平板计算机等等、云、互联网等等上。外部控制器155可以是楼宇管理系统(BMS),其又被称为楼宇自动化系统(BAS),这是在建筑物中安装的控制和监视建筑物的机电装备诸如通风、照明、电力系统、消防系统和安全系统的基于计算机的控制系统。

[0045] 在另一示例中,系统100可以位于室外环境中,例如,位于城镇或城市中。这样的系统100的示例是Philips CityTouch,其是包括智能街灯的街道照明管理(系统)。照明网络110可以被定位在城市的城镇中并且可以包括照明设备111-113例如作为路灯。外部网络120-130可以被定位在城市的其他城镇中。外部控制器155可以被定位在远程服务器140诸如软件系统中,以便远程监视、控制和管理街道照明。

[0046] 由于照明网络110可能具有与外部控制器155和外部网络120-130的网络连接性,从而使之容易受到安全威胁。针对照明网络110和/或外部网络120-130的网络攻击具有削弱物理服务和照明基础设施的潜力。具体地,鉴于照明设备111-113具有有限的计算能力和存储容量,使之难以使用需要比照明设备111-113能够提供的更多的资源的复杂密码算法。本发明的目的是呈现一种方法来提供照明网络110 的安全操作,其中该方法示意性地和例示性地在图2中进行举例说明。

[0047] 图2示意性地和例示性地显示举例说明提供照明网络110的安全操作的方法200的实施例的流程图。在确定步骤210中，照明网络110的配置状态被确定。配置状态的确定可以包括确定所使用的软件的版本或照明网络的设备设置的值。可以在外部控制器155中和/或在本地控制器115中执行确定210。照明网络110的配置状态可以是照明网络110的照明设备111-113的配置状态。照明网络110的配置状态可以是照明设备111-113的个别组件例如驱动器、联网芯片(收发机)、微控制器等等的配置状态。照明网络110的配置状态可以是本地控制器115或照明网络110中的任何其他元件的配置状态。照明网络110的配置状态读至任一上面实例(case)。

[0048] 配置可以包括诸如软件和/或硬件之类的元素的功能布置;其中配置状态可以是一些或所有这样的元素的表示，诸如硬件、软件和/设备设置的版本。配置可以包括在照明网络110中存储的软件或数据;其中配置状态是例如软件的版本或配置参数的值。配置可以是照明网络110的固件，其中配置状态可以是固件的版本。固件是在照明网络110的只读存储器中编程的永久软件，其中方法200进一步包括确定210固件的当前版本。配置可以是数据诸如配置参数和/和设备设置，例如，照明设备可以被配置成为某灯光渲染功能分配特定大小的存储器。

[0049] 确定210照明网络110的配置状态的步骤可以基于触发器，以及其中触发器生成可以是基于时间的，以致周期性地、在随机时刻或在预定时刻生成触发器。用于触发器生成的预定时刻可以由用户设置，或者它可以基于来自照明网络110的历史数据来自动生成。

[0050] 触发器生成可以是基于事件的，以致触发器可以在照明网络中观察到恶意活动时被生成。网络流量可以被监控，以检测任何的恶意活动，例如，恶意软件正操作在网络流量中。恶意软件是故意被设计成对网络造成损害的任何软件。生成攻击者使用来在网络中得到最初立足点的恶意软件模型，其用于已知与未知恶意软件、恶意工具和零日利用(zero-day exploit)的不言而喻的迹象(tell-tale sign)。恶意活动可以通过使用异常检测从照明网络110中观察到。可视化工具可以用于监控网络流量。当系统检测到任何这样的恶意活动时，可以生成触发器来确定照明网络110的配置状态。可供选择地，事件可以是针对类似网络的最近的网络攻击或者关于由于脆弱的配置而引起的潜在网络攻击的信息。

[0051] 在更新的配置例如软件和/或设备设置的可用性的指示被接收到时，可以生成触发器。通常在补丁中提供更新的配置，其是被设计成更新、修复或改进配置的针对配置的一组改变。这包括修复安全脆弱性和其他缺陷(bug)，其中这样的补丁通常被称为漏洞修复(bugfix)或缺陷修复并且提高可用性或性能。

[0052] 方法200可以进一步包括:分析220所确定的配置状态。所确定的配置状态的分析220可以基于照明网络110的脆弱性。能够在外部控制器155中和/或在本地控制器115中执行分析220。通过使用网络行为分析中的异常检测来执行分析220。Network Behavior Analysis(网络行为分析)(NBA)是通过监控流量和注意不寻常的动作或与正常操作的偏离来增强网络的安全性的一种方式。常规的入侵防御系统解决方案通过使用分组检查、签名检测和实时阻塞来保卫网络的周界(perimeter)。NBA程序观看在网络内正发生什么，从而聚合(aggregate)来自许多点的数据来支持离线分析。在为正常流量建立基准之后，NBA程序被动监视网络活动和标记未知的、新的或不寻常的可能指示威胁存在的图案(pattern)。

[0053] 例如，在NBA中，异常检测可以使用至少统计方法、基于规则的方法、基于距离的方

法、基于剖析的方法、基于模型的方法之一，如下所解释的：

统计方法：统计方法通过随时间(例如，在入侵检测域中每个会话的登入和登出时间)测量某些变量来监视用户或系统行为。基本模型保持这些变量的平均值并且基于变量的标准偏差来检测是否超过阈值。更高级的统计模型也比较长期与短期用户活动的配置文件；

基于距离的方法：基于距离的方案试图克服统计异常值(outlier)检测方案的限制，并且它们通过计算点之间的距离来检测异常值。若干基于距离的异常值检测算法用于检测网络流量中的异常；

基于规则的方法：在异常检测中使用的基于规则的系统利用一组规则来表征(characterize)用户、网络和/或计算机系统的正常行为；

基于剖析的方法：在剖析方法中，正常行为的配置文件针对不同类型的网络流量、用户、程序等等来建立，并且与它们的偏差被认为是入侵；

基于模型的方法：在基于模型的方案中，异常被检测为针对表示正常行为的模型的偏差。

[0054] 方法200可以进一步包括：基于分析220，在正常模式和安全模式之间切换230照明网络110的操作模式。

[0055] 在正常模式中，照明网络110被可操作地连接至外部控制器155，并且照明设备111-113的灯光渲染功能正由外部控制器155根据预定功能集合来控制。外部控制器155可以控制一个或多个照明设备111-113的灯光渲染功能。预定功能集合可以包括照亮环境和/或改变照明设备111-113的一个或多个光源的颜色、色温、强度、光束宽度、光束方向、光照强度、其他参数之中的一个或多个。在正常模式中，外部控制器155可以改变照明网络110的配置状态。在正常模式中，照明网络110可以被布置用于与外部控制器155传送信息，例如传感数据、状态数据、控制数据、配置数据、诊断数据、维护请求、数据处理请求。该信息旨在用于外部控制器155，以致该信息被处理，例如，用于控制、维护、诊断、End-of-Life(EoL)分析等等。外部控制器155可以被定位在远程服务器140诸如云上，这提供在远程服务器140上处理信息的计算优势。

[0056] 在安全模式中，照明设备111-113的灯光渲染功能正由外部控制器155根据预定功能集合的子集来控制。例如，预定功能集合的子集可以包括照亮环境和/或改变光照强度。作为示例，在安全模式中，照明网络110可以仅被布置用于与外部控制器155通信，但是可能不被布置用于与外部网络120-130通信。作为另一示例，在安全模式中，旨在用于外部控制器155的信息可以被存储在本地控制器115中，并且所述信息在恢复正常模式时进行传送。该信息可以在本地控制器115中本地进行处理。照明网络可以被布置用于广告安全危害的类型和/或所需的配置。基于分析220，本地控制器115可以广告暴露照明网络110的脆弱性和/或可以解决脆弱性的潜在配置。在网络中，安全修复例如补丁用于改变配置状态。虽然补丁意味着修复安全脆弱性的问题，但是设计不良的补丁有时能够带来新的问题。因此，本地控制器115可以广告：以前的或不同的补丁是合适的。

[0057] 在安全模式中，照明网络110可以被进一步布置成可操作地与外部控制器155断开连接，并且灯光渲染功能可以由本地控制器115控制。在这个示例中，预定功能集合的子集是空集，即，外部控制器155不控制照明设备111-113的灯光渲染功能。空集或零集是没有

元素的独特集合。在这个示例中，照明网络110也可以与(多个)外部网络120-130断开连接，无论照明网络110与外部网络120-130的通信可能是直接的或经由外部控制器155。本地控制器115可以被布置用于控制照明设备111-113的操作。照明网络110可能不与外部控制器155传送信息，例如传感数据、状态数据、控制数据、配置数据、诊断数据、维护请求、数据处理请求。旨在用于外部控制器155的信息可以被存储在本地控制器155 中，并且该信息可以例如为了控制、维护、诊断、End-of-Life(EoL)分析等等而在本地控制器115中本地进行处理。本地控制器115可以执行信息处理的子集，诸如控制与维护。该信息可以在正常模式中进行传送。在系统100是建筑物的示例中，本地控制器115可以是房间中的开关，其被布置用于控制照明设备111-113的灯光渲染功能。在这个示例中，外部控制器155例如楼宇中央控制(控件)和外部网络120-130例如其他房间中的照明网络与照明网络110断开连接。

[0058] 图3示意性地和例示性地显示举例说明提供照明网络的安全操作的方法300的另一实施例的流程图。在确定步骤210中，照明网络110的配置状态被确定，并且所确定的配置状态在步骤220中进行分析，其中分析220包括：检测325是否所确定的配置状态需要改变。所确定的配置状态在以下情况中可能需要改变：当检测到照明网络是脆弱的时候，例如，当在网络流量中检测到异常时，与所确定的配置相比而言较新的配置是可用的，所确定的配置状态已知是性能不佳的配置并且被暴露于安全风险，等等。在异常的情况下，网络流量被监控，以检测任何的恶意活动，例如，恶意软件正操作在网络流量中。

[0059] 本地控制器115和/或外部控制器155可能接收到更新配置的可用性的指示。在检测325的步骤中，所确定的配置状态可以与可用的配置状态进行比较。例如，配置可以是固件，并且安装固件的版本与该固件的目前可用版本进行比较。如果所安装的固件是较旧的版本，则检测步骤325指示：配置需要改变。可供选择地，例如，在所确定的配置中发现缺陷，以致这使得照明网络110容易受到安全破坏，检测步骤325指示：配置状态需要改变。

[0060] 方法300可以进一步包括：基于检测325，将照明网络的操作模式从正常模式切换330到安全模式。在步骤340中，照明网络110的配置被改变。在目前可用的配置与所确定的配置相比而言是较新的情况下，照明网络110的配置被更新。当恶意活动被检测到时，配置可以被改变为对于检测到的恶意活动提供安全性的更合适的版本。并且，在指示所确定的配置状态容易出现安全脆弱性的情况下，配置可以被改变为不同的配置，例如，较新或较旧的配置，其提供更好的安全性并且不是脆弱的。配置的改变可以由本地控制器115和/或由外部控制器155执行。在图4中示意性地和例示性地显示改变配置的过程。

[0061] 方法300可以进一步包括：当配置被改变时，将操作模式从安全模式切换350到正常模式。一旦潜在的安全威胁被处理并且照明网络110对于安全折中的脆弱性被解决，照明网络110被切换回到正常模式。针对测试时间周期，照明网络110可以被保持在正常模式中，并且网络流量被严格观察。如果脆弱性没有被完全解决，照明网络110可以再次被切换回到安全模式，例如，以便使用不同的配置。

[0062] 图4示意性地和例示性地显示照明网络410和举例说明实施例来改变照明网络410的配置的本地控制器415。照明网络410可以包括照明设备411-413、本地控制器415和通信单元416，其中通信单元416被例示性地显示为被包括在本地控制器415中。配置的改变可以是自动的，例如基于触发器，或者配置的改变可以是手动的，例如基于用户输入。在实施例中，照明网络410的配置可以经由本地控制器415来改变，其中本地控制器可以被布置用于

接收和存储配置。本地控制器415可以被布置用于在正常模式中接收配置并且可以被布置用于在正常模式中改变照明网络410的配置。可供选择地，本地控制器415可以被布置用于在正常模式中接收配置并且可以被布置用于在安全模式中改变照明网络410的配置。进一步，本地控制器415可以被布置用于在安全模式中接收和改变配置。

[0063] 可供选择地，外部控制器455可以被布置用于改变照明网络410的配置。在这个例示图中的外部控制器455被显示为被定位在用户设备455例如移动电话、平板计算机、膝上型计算机中，其具有用户界面来指示配置的可用性和改变配置。外部控制器455可以被连接至远程服务器例如互联网，以接收配置。外部控制器455可以被可操作地连接至照明网络410的通信单元416。在实施例中，外部控制器455可以被无线连接至通信单元416，其包括无线收发机并且通过射频、使用协议诸如Wi-Fi、Bluetooth或Zigbee来提供通信。配置可以在正常模式中或在安全模式中经由外部控制器455来改变。

[0064] 在系统100是建筑物的示例中，在这个示例中是用户移动设备的外部控制器455被连接至Wi-fi网络并且接收配置诸如软件。移动设备与通信单元416例如网关例如通过Wi-fi链路来通信并且指示配置的可用性。在确定照明设备411-413的配置状态需要改变的情况下，网关例如通过Zigbee链路与照明设备411-413通信。移动设备经由照明网络416的网关来改变照明设备411-413的配置。在实施例中，移动设备可能需要认证来改变配置状态。认证可能需要以下之中的一个或多个：口令，个人识别码(pin code)，指纹等等。认证可以是单因素或多因素认证。本地控制器可以被包括在本地用户设备(未显示)中，其中本地用户设备可能与照明设备411-413具有例如无线或有线的通信链路。本地用户设备可以例如在正常模式中接收配置诸如软件并且可以例如在安全模式中改变照明设备411-413的配置。

[0065] 图5示意性地和例示性地显示用于提供照明网络的安全操作的控制器510。本地控制器510可以包括处理器515、通信单元516、分别输入与输出接口517-518和存储器530。处理器515被布置用于执行方法200-300的步骤。控制器510可以被实现在与照明网络110和/或外部控制器155分开的诸如墙面板、桌面计算机终端或甚至便携式终端诸如膝上型计算机、平板计算机或智能手机之类的单元中。可供选择地，控制器510可以被并入照明网络110或外部控制器155中。进一步，控制器510可以在单个单元中或采用在多个单独单元之间分布的分布式功能(例如，包括在一个或多个地理网站(site)上的多个服务器单元的分布式服务器，或者在照明网络110之间或在照明网络110和外部控制器155之间分布的分布式控制功能)的形式来实现。此外，控制器510可以采用在存储器(其包括一个或多个存储设备)上存储的软件的形式来实现并且被布置用于在处理器(其包括一个或多个处理单元)上执行，或者控制器510可以采用专用硬件电路或者可配置的或可重新配置的电路诸如PGA或FPGA或者这些的任何组合的形式来实现。

[0066] 方法200-300可以在计算机程序产品在计算设备的处理单元诸如控制器510的处理器515上运行时利用计算机程序产品的计算机程序代码来执行。

[0067] 应注意：上述的实施例举例说明而非限制本发明，并且本领域的技术人员将能够设计许多可供选择的实施例而不偏离所附权利要求书的范畴。

[0068] 在权利要求书中，被放置在括号之间的任何参考符号不应被解释为限制权利要求。动词“包括”及其词形变化的使用并不排除除了在权利要求中所陈述的元素或步骤之外

的其他元素或步骤的存在。在元素前面的冠词“一”或“一个”并不排除多个这样的元素的存在。本发明可以借助于包括若干不同元件的硬件并且借助于合适编程的计算机或处理单元来实现。在枚举若干装置的设备权利要求中，这些装置之中的若干装置可以利用同一项硬件来体现。在互不相同的从属权利要求中叙述某些措施的纯粹事实并不指示不能有利使用这些措施的组合。

[0069] 本发明的各方面可以被实现在计算机程序产品中，其中计算机程序产品可以是可以由计算机执行的在计算机可读存储设备上存储的计算机程序指令集。本发明的指令可以在任何的包括但不限于脚本、可解释程序、动态链接库(DLL)或Java类的可解释的或可执行的代码机制中。这些指令能够作为完全可执行程序、部分可执行程序、作为针对现有程序的修改(例如，更新)或用于现有程序的扩展(例如，插件)来提供。此外，本发明的处理的各部分可以被分布在多个计算机或处理器或者甚至“云”上。

[0070] 适于存储计算机程序指令的存储媒体包括所有形式的非易失性存储器，其包括但不限于EPROM、EEPROM和闪存设备、磁盘诸如内部与外部硬盘驱动器、可移除盘和CD-ROM盘。计算机程序产品可以被分布在这样的存储介质上或者可以被供应用于通过HTTP、FTP、电子邮件或通过被连接至网络诸如Internet(因特网)的服务器进行的下载。

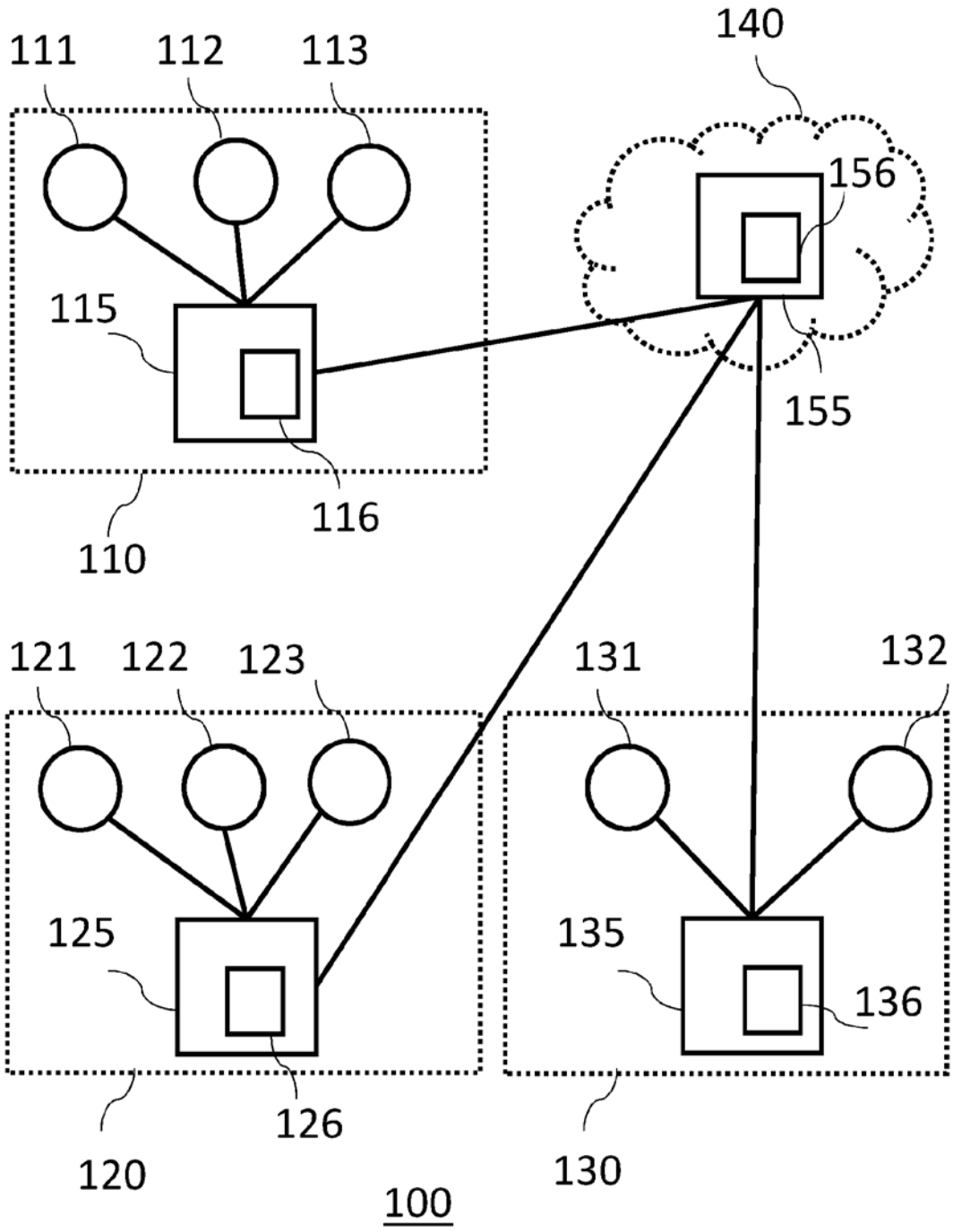
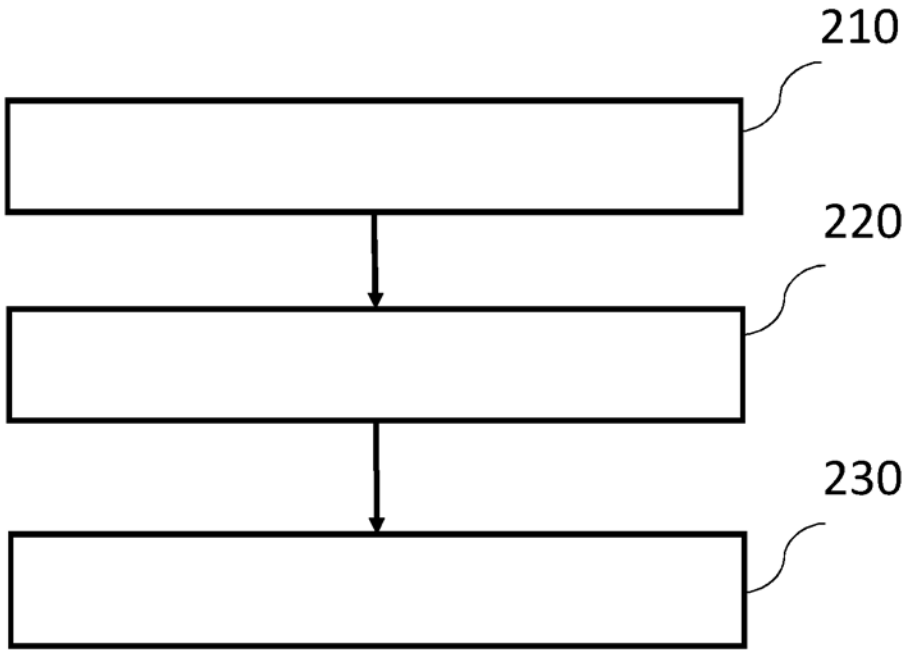

111
112
113
140
156
115
155
116
110
121
122
123
131
132
125
135
136
126
120
130
100

图 1



200

图 2

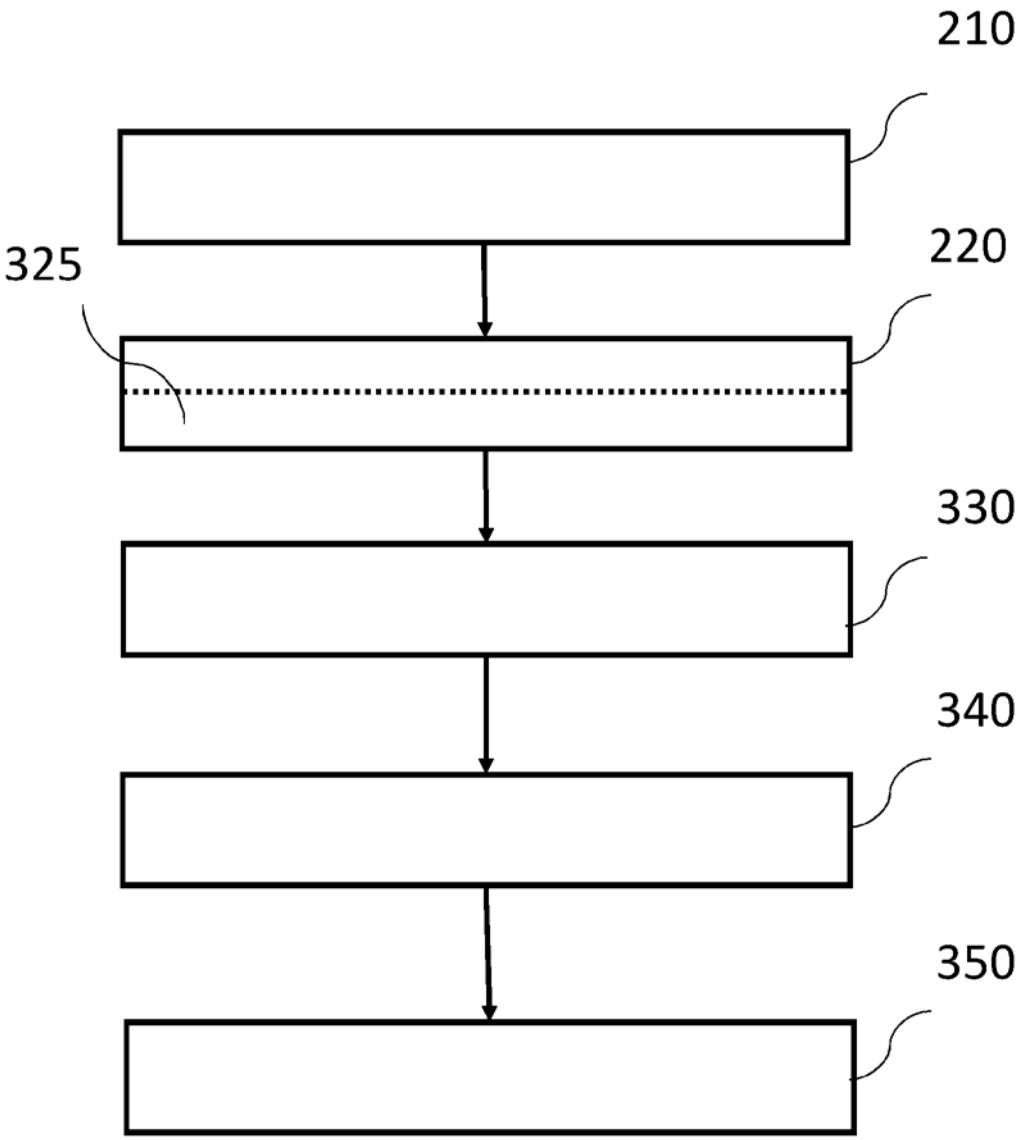


图 3

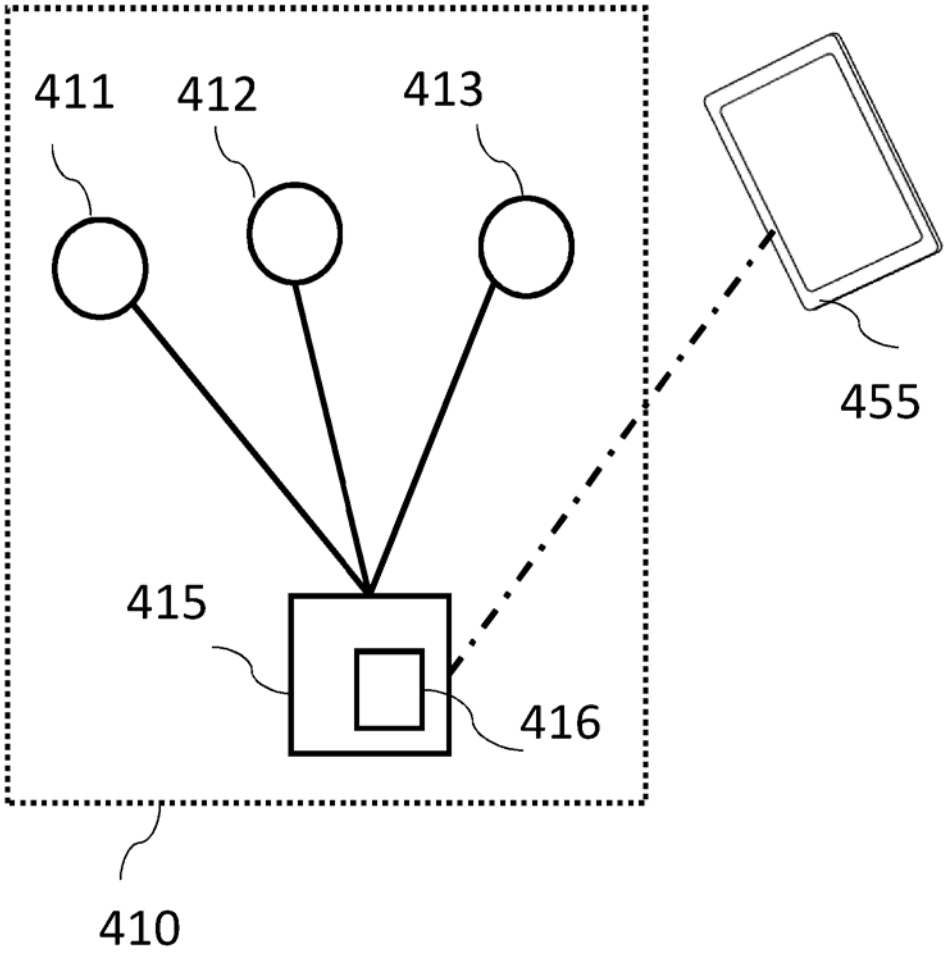


图 4

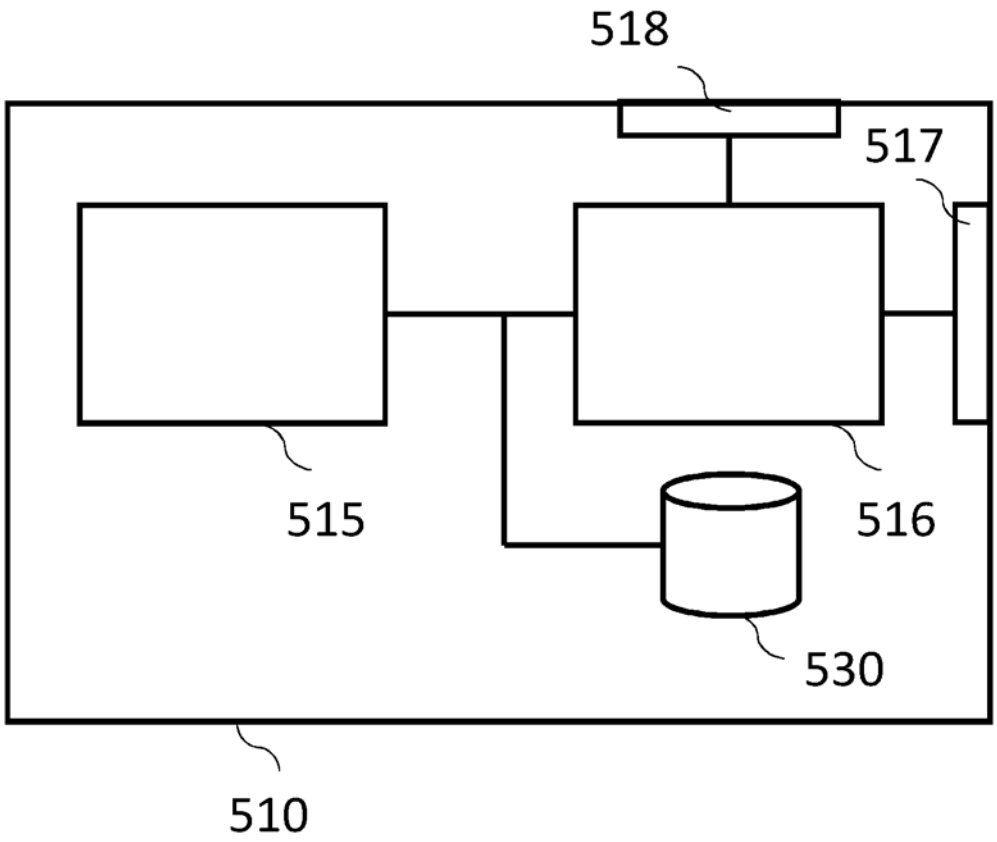


图 5