

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017 年 6 月 29 日 (29.06.2017)



(10) 国际公布号
WO 2017/107966 A1

- (51) 国际专利分类号:
H04W 12/08 (2009.01) H04W 76/02 (2009.01)
H04W 12/12 (2009.01)
- (21) 国际申请号: PCT/CN2016/111624
- (22) 国际申请日: 2016 年 12 月 23 日 (23.12.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510991478.X 2015 年 12 月 24 日 (24.12.2015) CN
- (71) 申请人: 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。北京奇安信科技有限公司 (BEIJING QIANXIN TECHNOLOGY CO., LTD.) [CN/CN]; 中国北京市朝阳区酒仙桥路甲 10 号 3 号楼 15 层 17 层 1701-26, Beijing 100015 (CN)。
- (72) 发明人: 吉艳敏 (JI, Yanmin); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。江爱军 (JIANG, Aijun); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。
- (74) 代理人: 北京润泽恒知识产权代理有限公司 (BEIJING RUN ZEHENG INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区中关村南大街 31 号神舟大厦 702-703, 715, Beijing 100081 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(54) Title: LOCAL AREA NETWORK-BASED WIRELESS HOTSPOT CONTROL METHOD AND DEVICE

(54) 发明名称: 基于局域网的无线热点控制方法和装置

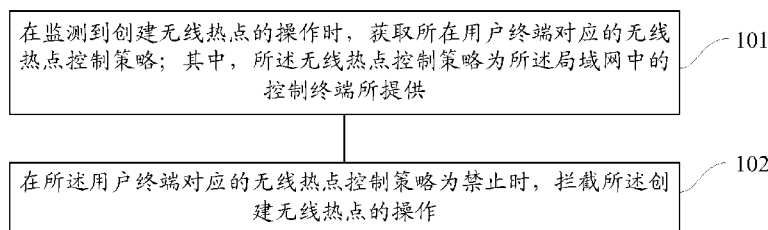


图 1

101 Upon monitoring an operation for creating a wireless hotspot, acquire a wireless hotspot control strategy corresponding to a user terminal performing the operation, wherein the wireless hotspot control strategy is provided by a control terminal in a local area network
102 If the wireless hotspot control strategy corresponding to the user terminal is prohibition, intercept the operation for creating a wireless hotspot

(57) Abstract: Provided are a local area network-based wireless hotspot control method and device. Specifically, the method comprises: upon monitoring an operation for creating a wireless hotspot, acquiring a wireless hotspot control strategy corresponding to a user terminal performing the operation, wherein the wireless hotspot control strategy is provided by a control terminal in a local area network; and if the wireless hotspot control strategy corresponding to the user terminal is prohibition, intercepting the operation for creating a wireless hotspot. An embodiment of the invention can intercept an operation for creating a wireless hotspot performed by a user terminal, so that the user terminal fails in creating a wireless hotspot, thereby increasing a security level of a local area network.

(57) 摘要: 一种基于局域网的无线热点控制方法和装置, 其中的方法具体包括: 在监测到创建无线热点的操作时, 获取所在用户终端对应的无线热点控制策略; 其中, 所述无线热点控制策略为所述局域网中的控制终端所提供; 在所述用户终端对应的无线热点控制策略为禁止时, 拦截所述创建无线热点的操作。本发明实施例能够拦截用户终端中执行创建无线热点的操作, 使得用户终端创建无线热点失败, 从而可以提高局域网的安全性。

WO 2017/107966 A1

说明书

基于局域网的无线热点控制方法和装置

本申请要求在 2015 年 12 月 24 日提交中国专利局、申请号为 201510991478.X、发明名称为“基于局域网的无线热点控制方法和装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5 技术领域

本发明涉及局域网技术领域，特别是涉及一种基于局域网的无线热点控制方法和装置。

背景技术

随着网络技术的迅猛发展，无线热点（Hotspot）的应用也越来越广泛。
10 无线热点是在公共场所提供 WLAN（Wireless Local Area Networks，无线局域网）接入 Internet（因特网）服务的地点。上述公共场所可以是大型企业内部，也可以是咖啡馆、机场、车站、商务酒店、高等院校、大型展览会馆等。在无线热点覆盖的公共场所，用户可以通过使用装有内置或外置无线网卡的笔记本电脑等设备来实现对 Internet 的接入，因此无线热点为用户的网络接入提供了极大的便利。
15

然而，无线热点在提供便利的同时也带来了信息安全的问题。例如对于企业网等局域网而言，如果企业员工通过笔记本电脑建立无线热点，其它终端设备则可以通过连接该无线热点接入局域网，有可能造成企业的数据泄露，为企业带来经济损失。此外，如果连接该无线热点的其它终端设备携带
20 有恶意程序，则恶意程序很有可能通过该无线热点的连接对局域网进行攻击，为企业带来极大的安全隐患。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的一种基于局域网的无线热点控制方法和装置。

25 依据本发明的一个方面，提供了一种基于局域网的无线热点控制方法，

包括:

在监测到创建无线热点的操作时,获取所在用户终端对应的无线热点控制策略;其中,所述无线热点控制策略为所述局域网中的控制终端所提供;

在所述用户终端对应的无线热点控制策略为禁止时,拦截所述创建无线热点的操作。

根据本发明的另一方面,提供了一种于局域网的无线热点控制装置,包括:

监测模块,用于在监测到创建无线热点的操作时,获取所在用户终端对应的无线热点控制策略;其中,所述无线热点控制策略为所述局域网中的控制终端所提供;及

拦截模块,用于在所述用户终端对应的无线热点控制策略为禁止时,拦截所述创建无线热点的操作。

根据本发明的又一个方面,提供了一种计算机程序,其包括计算机可读代码,当所述计算机可读代码在计算设备上运行时,导致所述计算设备执行所述的基于局域网的无线热点控制方法。

根据本发明的再一个方面,提供了一种计算机可读介质,其中存储了所述的计算机程序。

根据本发明实施例的一种基于局域网的无线热点控制方法和装置,在监测到创建无线热点的操作时,获取所在用户终端对应的无线热点控制策略,在所述用户终端对应的无线热点控制策略为禁止时,拦截所述创建无线热点的操作,从而可以使得所述用户终端中创建无线热点的操作失败。本发明实施例可以按照控制终端提供的无线热点控制策略对用户终端中创建无线热点的操作进行控制,例如通过设置用户终端对应的无线热点控制策略为禁止,可以拦截该用户终端中执行创建无线热点的操作,使得该用户终端创建无线热点失败,从而可以提高局域网的安全性。

上述说明仅是本发明技术方案的概述,为了能够更清楚了解本发明的技术手段,而可依照说明书的内容予以实施,并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂,以下特举本发明的具体实施方式。

附图说明

通过阅读下文可选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出可选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示出了根据本发明一个实施例的一种基于局域网的无线热点控制方法的步骤流程图；

图 2 示出了根据本发明一个实施例的一种基于局域网的无线热点控制方法的步骤流程图；

图 3 示出了根据本发明一个实施例的一种基于局域网的无线热点控制方法的步骤流程图；以及

图 4 示出了根据本发明一个实施例的一种基于局域网的无线热点控制装置的结构框图；

图 5 示意性地示出了用于执行根据本发明的方法的计算设备的框图；

图 6 示意性地示出了用于保持或者携带实现根据本发明的方法的程序代码的存储单元。。

具体实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

参照图 1，示出了根据本发明一个实施例的一种基于局域网的无线热点控制方法的步骤流程图，具体可以包括如下步骤：

步骤 101、在监测到创建无线热点的操作时，获取所在用户终端对应的无线热点控制策略；其中，所述无线热点控制策略为所述局域网中的控制终端所提供；

步骤 102、在所述用户终端对应的无线热点控制策略为禁止时，拦截所述创建无线热点的操作。

本发明实施例可以应用于企业网、政府网、校园网等局域网中；在上述局域网中，用户终端指具有可设置为无线热点的网卡的终端设备，例如台式电脑，笔记本电脑等，该终端设备可以有线方式连接局域网络，也可以无线方式连接局域网络。其中，可设置为无线热点的网卡具体可以是终端设备内
5 置的无线网卡或者是可设置为无线热点的 USB 无线网卡。所述控制终端可用于提供无线热点控制策略，例如可以设置禁止/允许哪些用户终端创建无线热点等，以防止局域网内数据泄露或者恶意程序的入侵。

在本发明的一种应用示例中，为了保证局域网的安全性，可以设置所述无线热点控制策略为禁止局域网内的所有用户终端创建无线热点，例如，通
10 过对局域网内的用户终端进行监测，一旦发现存在用户终端正在执行尝试创建无线热点的操作，则拦截该创建无线热点的操作，以使该用户终端创建无线热点失败。

在本发明的另一种应用示例中，还可以根据企业内各部门的工作性质制定对应的无线热点控制策略。例如，由于研发部门的工作人员经常接触到企业内部的核心技术数据，为了防止公司的核心技术外泄，可以设置研发部门
15 的用户终端对应的无线热点控制策略为禁止。而行政部门的工作人员通常不接触企业内部的核心技术，因此，可以设置行政部门的用户终端的无线热点控制策略为允许。

在本发明的又一种应用示例中，还可以通过控制终端周期性地收集来自
20 局域网内各用户终端的安全扫描结果，通过对各用户终端的安全扫描结果进行分析，确定各用户终端的安全级别，对于安全级别较高的用户终端可以设置对应的无线热点控制策略为允许，而对于安全级别较低的用户终端设置对应的无线热点控制策略为禁止。通过周期性的收集来自局域网内各用户终端的安全扫描结果，在用户终端的安全级别发生变化时，可以对无线热点控制
25 策略进行相应的更新。

可以理解，上述制定无线热点控制策略的方式仅作为本发明的应用示例，在实际应用中，本领域技术人员可以根据实际需要灵活制定无线热点控制策略。

其中，上述用户终端和上述控制终端之间可以通过标准协议或者私有协议进行通信，其中，私有协议具有封闭性和安全性高的优点；可以理解，本发明实施例对于用户终端和控制终端之间的具体通信方式不加以限制。

在实际应用中，控制终端的用户可以是网络管理员等具有一定的网络安全知识的高级用户，因此，控制终端的用户可以根据局域网的当前安全需求和实际情况，灵活地制定相应的无线热点控制策略，以提高局域网的安全性。

在本发明实施例中，在用户终端上可以设置有监测模块，用于监测用户终端上是否有创建无线热点的操作。在监测到用户终端上有执行创建无线热点的操作时，则可以从所述局域网内的控制终端读取所述用户终端对应的无线热点控制策略；根据所述控制终端中设置的所述用户终端对用的无线热点控制策略，执行对应的控制操作。具体地，在所述用户终端对应的无线热点控制策略为禁止时，拦截所述用户终端执行创建无线热点的操作。

可以理解，本发明对于上述无线热点控制策略的获取方式不加以限制，例如，可以将无线热点控制策略存储在控制终端，用户终端通过局域网访问控制终端在线查询对应的无线热点控制策略，或者，控制终端可以将上述无线热点控制策略下发至用户终端，以使用户终端可以在本地进行查询。

在本发明的一种可选实施例中，上述方法还可以包括：

在所述用户终端对应的无线热点控制策略为允许时，允许继续执行所述创建无线热点的操作。

在本发明的一种应用示例中，控制终端可以为每个用户终端制定对应的无线热点控制策略，并通过企业局域网下发到对应的用户终端。其中，无线热点控制策略可以通过一张映射表来表示，在该映射表中可以包括用户终端的终端标识以及对应无线热点控制策略的映射关系，参照表 1，示出了本发明的一种无线热点控制策略对应的映射表的具体示意。

表 1

终端标识	无线热点控制策略
00-01-02-03-04-05	允许
00-01-02-03-04-06	禁止

00-01-02-03-04-07	禁止
00-01-02-03-04-08	允许

在上述表 1 中，终端标识采用的是用户终端的 MAC（Media Access Control，媒体访问控制）地址，可以理解，在实际应用中，本发明对于终端标识不加以限制，例如还可以采用用户终端的 IP 地址等。

5 在具体应用中，在拦截所述用户终端执行创建无线热点的操作之后，还可以在显示界面显示提示信息，以告知用户当前的终端设备禁止执行创建无线热点的操作。

10 综上，在本发明实施例中，在监测到创建无线热点的操作时，获取所在用户终端对应的无线热点控制策略，在所述用户终端对应的无线热点控制策略为禁止时，拦截所述创建无线热点的操作，从而可以使得所述用户终端中创建无线热点的操作失败。本发明实施例可以按照控制终端提供的无线热点控制策略对用户终端中创建无线热点的操作进行控制，例如通过设置用户终端对应的无线热点控制策略为禁止，可以拦截该用户终端中执行创建无线热点的操作，使得该用户终端创建无线热点失败，从而可以提高局域网的安全性。

15 参照图 2，示出了根据本发明一个实施例的一种基于局域网的无线热点控制方法的步骤流程图，具体可以包括如下步骤：

 步骤 201、在监测到创建无线热点对应的服务集标识的操作时，确定所述用户终端正在执行创建无线热点的操作；

20 步骤 202、获取所述用户终端对应的无线热点控制策略；其中，所述无线热点控制策略为所述局域网中的控制终端所提供；

 步骤 203、在所述用户终端对应的无线热点控制策略为禁止时，向调用创建服务集标识的应用编程接口的调用方返回失败信息，以使所述用户终端创建服务集标识的操作失败；其中，所述服务集标识与所述无线热点具有对应关系。

25 在具体应用中，服务集标识（Service Set Identifier， SSID）是无线接入

点（Access Point，AP）或无线路由器的标志字符。每个创建的无线热点都有一个与之对应的唯一的 SSID，SSID 主要用来区分不同的无线网络，最多可以由 32 个字符组成，它是无线接入的身份证。只要电子设备的无线网卡支持扫描功能，就能很轻松的通过 SSID 接入无线热点。

5 在本发明实施例中，可以通过一个后台进程对用户终端中创建服务集标识的事件进行监测，例如监测用户通过手动配置 SSID 的操作，或者用户终端中通过进程自动创建 SSID 的操作等。具体地，可以通过多种方式实现该监测过程。例如，可以监听用户终端操作系统发出的广播消息，通过对系统广播消息的过滤，获知创建服务集标识的事件。也即，后台进程可以对每一个广播的系统消息进行判断，如果消息类型为创建服务集标识的事件，则可
10 以对该事件进行拦截。

或者，也可以利用用户终端操作系统的 API（Application Programming Interface，应用程序编程接口）钩子函数，对创建服务集标识的事件进行监听。在本发明实施例中，利用后台进程提供钩子函数，并将系统原本创建服务集标识操作的调用函数转向钩子函数（通常通过修改函数入口地址实现），
15 这样钩子函数就能够获得创建的 SSID 名称等信息，完成对创建服务集标识事件的监听。

可以理解，通过上述两种方式监测创建服务集标识的操作仅作为本发明的一种应用示例，在实际应用中，本发明对创建服务集标识操作的监测方式
20 不加以限制，既可以在应用层监测，也可以在驱动层进行监测。

本发明实施例通过对创建服务集标识的操作进行监测，来实现监测创建无线热点操作的过程，在监测到创建无线热点对应的服务集标识的操作，并且所在用户终端对应的无线热点控制策略为禁止时，向调用创建服务集标识的应用编程接口的调用方返回失败信息，以使所述用户终端创建服务集标识
25 的操作失败，进而使得用户终端创建无线热点的操作失败。本发明实施例可以在底层发现创建无线热点的初始步骤，即创建 SSID 的步骤，此时即可根据控制终端提供的无线热点控制策略对该创建无线热点的操作进行控制，从而可以尽早地中断该创建无线热点的操作，以及时保证局域网的安全性。

参照图 3，示出了根据本发明一个实施例的一种基于局域网的无线热点控制方法的步骤流程图，具体可以包括如下步骤：

步骤 301、在监测到创建无线热点的操作时，获取所在用户终端对应的无线热点控制策略；其中，所述无线热点控制策略为所述局域网中的控制终端所提供；

步骤 302、在所述用户终端对应的无线热点控制策略为允许时，允许继续执行所述创建无线热点的操作；

步骤 303、在所述创建无线热点的操作完成之后，保存所述无线热点对应的连接记录；其中，所述连接记录中包括如下信息中的至少一种：创建所述无线热点的用户终端对应的终端标识、连接所述无线热点的用户终端对应的终端标识、以及无线热点的热点标识；

步骤 304、将所述无线热点对应的连接记录上传至所述控制终端。

参照表 2，示出了本发明的一种无线热点对应的连接记录的具体示意。

表 2

创建无线热点的终端	连接无线热点的终端	热点标识
00-01-02-03-04-05	00-01-02-03-04-07	Hotspot1
00-01-02-03-04-06	00-01-02-03-04-08	Hotspot2

本发明实施例在创建无线热点的操作完成之后，可以记录该无线热点对应的连接记录，并将该连接记录上传至局域网内的控制终端，以使局域网的管理员可以通过控制终端查询用户终端的无线热点和连接信息，由于该无线热点对应的连接记录中可以包括创建所述无线热点的用户终端对应的终端标识、连接所述无线热点的用户终端对应的终端标识、以及无线热点的热点标识，因此，通过该连接记录可以得知企业内部那台用户终端创建了无线连接，以及哪些用户终端连接了该无线连接，并且可以根据用户终端的终端标识定位到该用户终端，以对该用户终端进行管控，例如可以断开该用户终端的局域网连接以防止重要文件外泄或者恶意程序的入侵，从而可以及早发现并阻止可能会给企业带来损失或者安全威胁的事件发生。

进一步地，还可以根据该无线热点对应的连接记录制定更加合理的无线

热点控制策略。具体地，控制终端可以根据接收到的来自局域网内用户终端创建的无线热点对应的连接记录，对用户终端进行行为分析，在发现用户终端存在可疑行为时，例如，通过连接记录得知企业内某台用户终端 A 创建了无线热点，但连接该无线热点的用户终端 B 对应的终端标识为未知标识，在控制终端没有记录信息，则用户终端 B 可能为企业人员带入企业内部的外来终端设备，为了防止用户终端 A 向用户终端 B 传输企业内的重要文件，可以断开用户终端 A 的局域网连接，并且将用户终端 A 对应的无线热点控制策略更新为禁止，以防止重要文件外泄或者恶意程序的入侵。

参照图 4，示出了根据本发明一个实施例的一种基于局域网的无线热点控制装置的结构框图，具体可以包括如下模块：

监测模块 401，用于在监测到创建无线热点的操作时，获取所在用户终端对应的无线热点控制策略；其中，所述无线热点控制策略为所述局域网中的控制终端所提供；及

拦截模块 402，用于在所述用户终端对应的无线热点控制策略为禁止时，拦截所述创建无线热点的操作。

在本发明的一种可选实施例中，所述监测模块，具体用于在监测到创建无线热点对应的服务集标识的操作时，确定所述用户终端正在执行创建无线热点的操作。

在本发明的另一种可选实施例中，所述拦截模块，具体用于在所述用户终端对应的无线热点控制策略为禁止时，向调用创建服务集标识的应用编程接口的调用方返回失败信息，以使所述用户终端创建服务集标识的操作失败；其中，所述服务集标识与所述无线热点具有对应关系。

在本发明的又一种可选实施例中，所述装置还可以包括：

允许模块，用于在所述用户终端对应的无线热点控制策略为允许时，允许继续执行所述创建无线热点的操作。

在本发明的再一种优选实施例中，所述装置还可以包括：

记录模块，用于在所述创建无线热点的操作完成之后，保存所述无线热点对应的连接记录；其中，所述连接记录中包括如下信息中的至少一种：创

建所述无线热点的用户终端对应的终端标识、连接所述无线热点的用户终端对应的终端标识、以及无线热点的热点标识；

上传模块，用于将所述无线热点对应的连接记录上传至所述控制终端。

5 对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

10 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据
15 本发明实施例的基于局域网的无线热点控制方法和装置中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

20 例如，图 5 示出了可以实现根据本发明的基于局域网的无线热点控制方法的计算设备。该计算设备传统上包括处理器 510 和以存储器 520 形式的计算机程序产品或者计算机可读介质。存储器 520 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。
25 存储器 520 具有用于执行上述方法中的任何方法步骤的程序代码 531 的存储空间 530。例如，用于程序代码的存储空间 530 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 531。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图 6 所述的便携式或者固定存储单元。该存储单元可以具有与图 5 的计算设备中的存储器 520 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 531'，即可以由例如诸如 510 之类的处

理器读取的代码，这些代码当由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定
5 编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未
10 详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以
20 把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴
25 随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其

它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

- 5 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包括”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。
- 10 在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

权 利 要 求 书

1、一种基于局域网的无线热点控制方法，包括：

在监测到创建无线热点的操作时，获取所在用户终端对应的无线热点控制策略；其中，所述无线热点控制策略为所述局域网中的控制终端所提供；

5 在所述用户终端对应的无线热点控制策略为禁止时，拦截所述创建无线热点的操作。

2、如权利要求 1 所述的方法，其特征在于，通过如下步骤监测创建无线热点的操作：

在监测到创建无线热点对应的服务集标识的操作时，确定所述用户终端正在执行创建无线热点的操作。

10 3、如权利要求 2 所述的方法，其特征在于，所述在所述用户终端对应的无线热点控制策略为禁止时，拦截所述创建无线热点的操作的步骤，包括：

在所述用户终端对应的无线热点控制策略为禁止时，向调用创建服务集标识的应用编程接口的调用方返回失败信息，以使所述用户终端创建服务集标识的操作失败；其中，所述服务集标识与所述无线热点具有对应关系。

15 4、如权利要求 1 所述的方法，其特征在于，所述方法还包括：

在所述用户终端对应的无线热点控制策略为允许时，允许继续执行所述创建无线热点的操作。

5、如权利要求 4 所述的方法，其特征在于，所述方法还包括：

20 在所述创建无线热点的操作完成之后，保存所述无线热点对应的连接记录；其中，所述连接记录中包括如下信息中的至少一种：创建所述无线热点的用户终端对应的终端标识、连接所述无线热点的用户终端对应的终端标识、以及无线热点的热点标识；

将所述无线热点对应的连接记录上传至所述控制终端。

25 6、一种基于局域网的无线热点控制装置，包括：

监测模块，用于在监测到创建无线热点的操作时，获取所在用户终端对应的无线热点控制策略；其中，所述无线热点控制策略为所述局域网中的控

制终端所提供；及

拦截模块，用于在所述用户终端对应的无线热点控制策略为禁止时，拦截所述创建无线热点的操作。

7、如权利要求 6 所述的装置，其特征在于，

5 所述监测模块，具体用于在监测到创建无线热点对应的服务集标识的操作时，确定所述用户终端正在执行创建无线热点的操作。

8、如权利要求 7 所述的装置，其特征在于，

10 所述拦截模块，具体用于在所述用户终端对应的无线热点控制策略为禁止时，向调用创建服务集标识的应用编程接口的调用方返回失败信息，以使所述用户终端创建服务集标识的操作失败；其中，所述服务集标识与所述无线热点具有对应关系。

9、如权利要求 6 所述的装置，其特征在于，所述装置还包括：

允许模块，用于在所述用户终端对应的无线热点控制策略为允许时，允许继续执行所述创建无线热点的操作。

15 10、如权利要求 9 所述的装置，其特征在于，所述装置还包括：

记录模块，用于在所述创建无线热点的操作完成之后，保存所述无线热点对应的连接记录；其中，所述连接记录中包括如下信息中的至少一种：创建所述无线热点的用户终端对应的终端标识、连接所述无线热点的用户终端对应的终端标识、以及无线热点的热点标识；

20 上传模块，用于将所述无线热点对应的连接记录上传至所述控制终端。

11、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求 1-5 中的任一个所述的基于局域网的无线热点控制方法。

25 12、一种计算机可读介质，其中存储了如权利要求 11 所述的计算机程序。

说明书附图

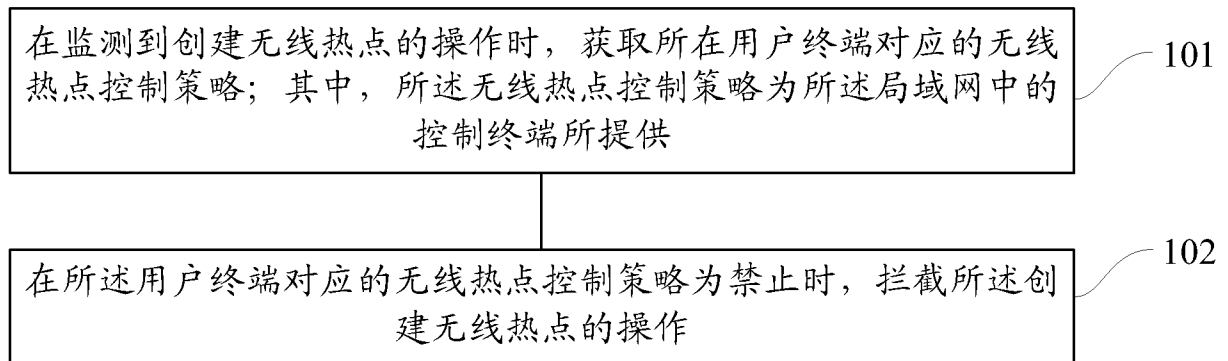


图 1

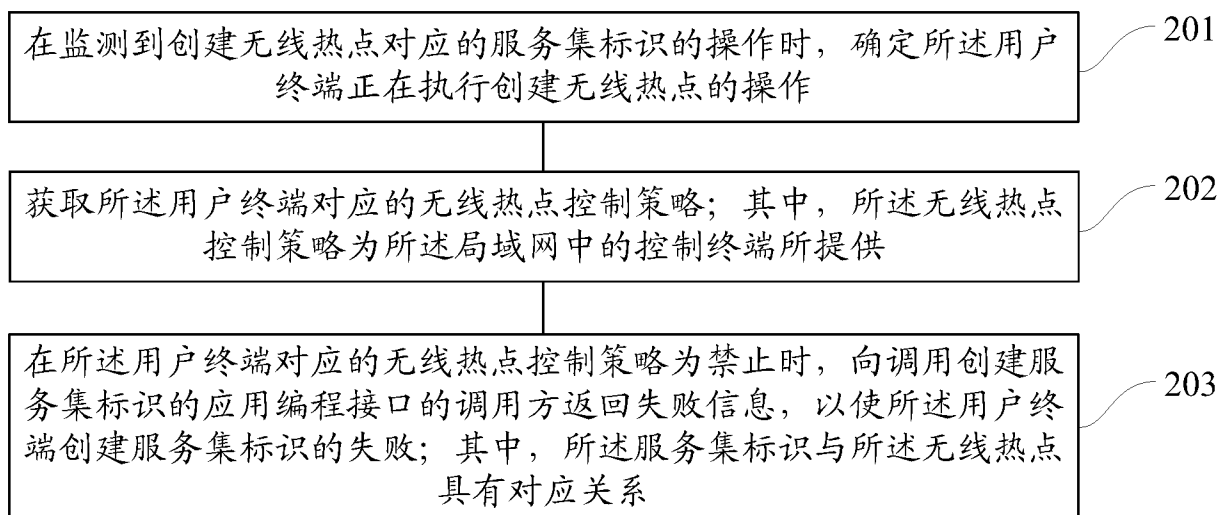


图 2

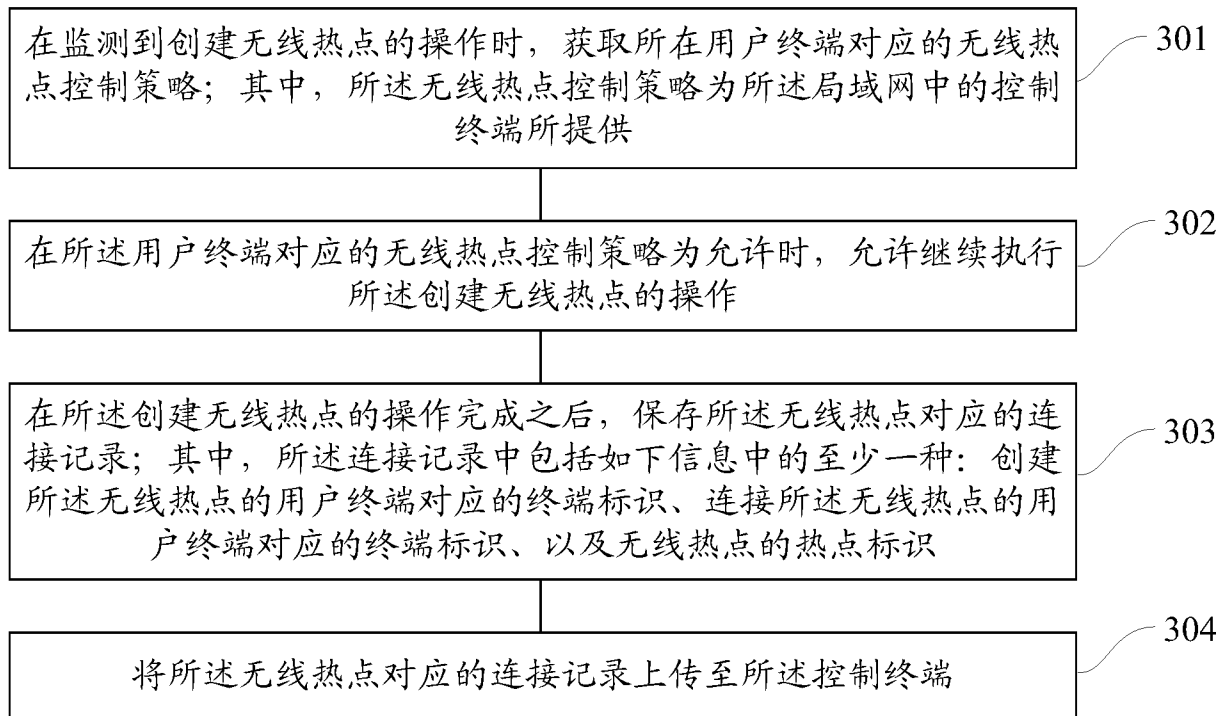


图 3

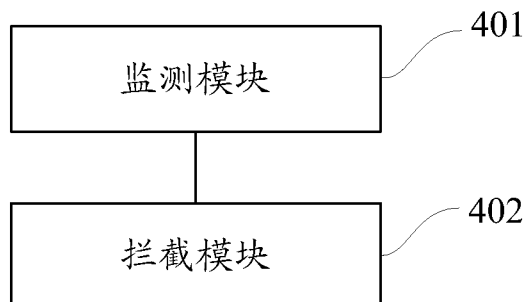


图 4

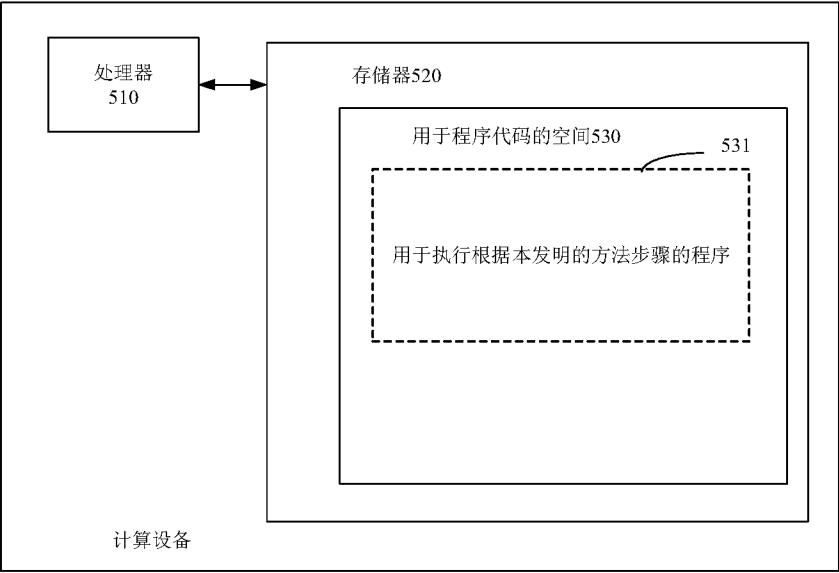


图 5

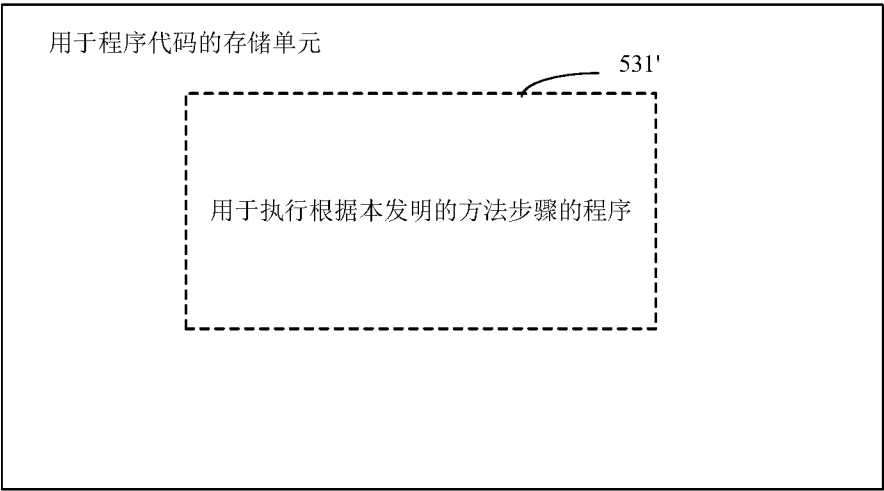


图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/111624

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/08 (2009.01) i; H04W 12/12 (2009.01) i; H04W 76/02 (2009.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS, CNTXT, CNKI, VEN: hotspot, wifi, Access Point, AP, establish, set up, creat, forbid, prohibit, prevent, intercept, LAN, wireless network, share

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 103260262 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 21 August 2013 (21.08.2013) description, paragraphs [0005]-[0107]	1-12
Y	CN 103619018 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 05 March 2014 (05.03.2014) description, paragraphs [0070]-[0105]	1-12
A	CN 104540183 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 22 April 2015 (22.04.2015) the whole document	1-12
A	CN 103929798 A (ZTE CORPORATION) 16 July 2014 (16.07.2014) the whole document	1-12
A	US 2012030351 A1 (PFU LIMITED) 02 February 2012 (02.02.2012) the whole document	1-12

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	
“A” document defining the general state of the art which is not considered to be of particular relevance	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“E” earlier application or patent but published on or after the international filing date	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	“&” document member of the same patent family

Date of the actual completion of the international search 28 February 2017	Date of mailing of the international search report 07 March 2017
---	---

Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer CHU, Yanling Telephone No. (86-10) 62089543
---	--

INTERNATIONAL SEARCH REPORTInternational application No.
PCT/CN2016/111624

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105682095 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.) 15 June 2016 (15.06.2016) claims 1-10, and description, paragraphs [0037]-[0094]	1-12

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/111624

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103260262 A	21 August 2013	None	
CN 103619018 A	05 March 2014	None	
CN 104540183 A	22 April 2015	None	
CN 103929798 A	16 July 2014	US 2015350929 A1	03 December 2015
		WO 2013178179 A1	05 December 2013
		EP 2945433 A1	18 November 2015
US 2012030351 A1	02 February 2012	JP 2012034129 A	16 February 2012
		JP 5581141 B2	27 August 2014
		US 9444821 B2	13 September 2016
CN 105682095 A	15 June 2016	None	

国际检索报告

国际申请号

PCT/CN2016/111624

A. 主题的分类

H04W 12/08(2009.01)i; H04W 12/12(2009.01)i; H04W 76/02(2009.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W, H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CPRSABS, CNTXT, CNKI, VEN: 热点, 无线保真, 接入点, 创建, 建立, 禁止, 阻止, 拦截, 局域网, 无线网, 共享, 分享, hotspot, wifi, Access Point, AP, establish, set up, creat, forbid, prohibit, prevent, intercept, LAN, wireless network, share

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
Y	CN 103260262 A (北京奇虎科技有限公司 等) 2013年 8月 21日 (2013 - 08 - 21) 说明书第[0005]-[0107]段	1-12
Y	CN 103619018 A (北京奇虎科技有限公司 等) 2014年 3月 5日 (2014 - 03 - 05) 说明书第[0070]-[0105]段	1-12
A	CN 104540183 A (北京奇虎科技有限公司 等) 2015年 4月 22日 (2015 - 04 - 22) 全文	1-12
A	CN 103929798 A (中兴通讯股份有限公司) 2014年 7月 16日 (2014 - 07 - 16) 全文	1-12
A	US 2012030351 A1 (PFU LIMITED) 2012年 2月 2日 (2012 - 02 - 02) 全文	1-12
PX	CN 105682095 A (北京奇虎科技有限公司 等) 2016年 6月 15日 (2016 - 06 - 15) 权利要求1-10, 说明书第[0037]-[0094]段	1-12

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2017年 2月 28日

国际检索报告邮寄日期

2017年 3月 7日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

初艳玲

电话号码 (86-10)62089543

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/111624

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	103260262	A	2013年 8月 21日	无			
CN	103619018	A	2014年 3月 5日	无			
CN	104540183	A	2015年 4月 22日	无			
CN	103929798	A	2014年 7月 16日	US	2015350929	A1	2015年 12月 3日
				WO	2013178179	A1	2013年 12月 5日
				EP	2945433	A1	2015年 11月 18日
US	2012030351	A1	2012年 2月 2日	JP	2012034129	A	2012年 2月 16日
				JP	5581141	B2	2014年 8月 27日
				US	9444821	B2	2016年 9月 13日
CN	105682095	A	2016年 6月 15日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)