

(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
2016 年 4 月 28 日 (28.04.2016)



(10) 国际公布号
WO 2016/062002 A1

- (51) 国际专利分类号:
H04W 12/06 (2009.01) *H04W 12/08* (2009.01)
- (21) 国际申请号: PCT/CN2015/074944
- (22) 国际申请日: 2015 年 3 月 24 日 (24.03.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410559632.1 2014 年 10 月 20 日 (20.10.2014) CN
- (71) 申请人: 小米科技有限责任公司 (XIAOMI INC.)
[CN/CN]; 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层, Beijing 100085 (CN)。
- (72) 发明人: 陈勇 (CHEN, Yong); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。 黄秋志 (HUANG, Qiuzhi); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。 董玉泉 (DONG, Yuquan); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。
- (74) 代理人: 北京律智知识产权代理有限公司 (BEIJING INTELLEGAL INTELLECTUAL PROP-

ERTY AGENT LTD.); 中国北京市朝阳区慧忠路 5 号远大中心 B 座 1802, 1803, 1805, Beijing 100101 (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, 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, KN, KP, KR, 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。

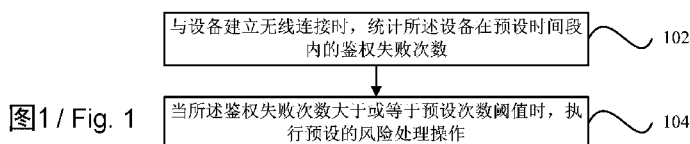
(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), 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: CONNECTION MANAGEMENT METHOD AND APPARATUS, ELECTRICAL DEVICE

(54) 发明名称: 连接管理方法及装置、电子设备



102 WHEN A WIRELESS CONNECTION TO THE DEVICE IS ESTABLISHED, COUNT AUTHENTICATION FAILURE TIMES OF THE DEVICE WITHIN A PRESET PERIOD OF TIME
104 WHEN THE AUTHENTICATION FAILURE TIMES IS GREATER THAN OR EQUAL TO THE THRESHOLD OF PRESET TIMES, CONDUCT A PRESET RISK MANAGEMENT OPERATION

(57) Abstract: The present disclosure relates to a connection management method and apparatus, and an electrical device, the method comprising: when a wireless connection to the device is established, counting authentication failure times of the device within a preset period of time; when the authentication failure times is greater than or equal to a threshold of preset times, conducting a preset risk management operation. The technical solution of the present invention identifies Wifi-squatting behavior and corrects the Wifi-squatting behavior in a timely manner, thus avoiding Wifi-squatting risk.

(57) 摘要: 本公开是关于连接管理方法及装置、电子设备, 包括: 与设备建立无线连接时, 统计所述设备在预设时间段内的鉴权失败次数; 当所述鉴权失败次数大于或等于预设次数阈值时, 执行预设的风险处理操作。通过本公开的技术方案, 可以识别出蹭网行为并予以及时处理, 以规避蹭网风险。



WO 2016/062002 A1

连接管理方法及装置、电子设备

本申请基于申请号为 201410559632.1、申请日为 2014/10/20 的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

5

技术领域

本发明涉及通信技术领域，尤其涉及连接管理方法及装置、电子设备。

背景技术

10 随着网络技术的发展，越来越多的电子设备都具备无线连接功能，则通过加入无线路由器建立的 WIFI（无线保真）网络，即可实现互联网访问以及设备之间的访问和控制。虽然无线连接技术给用户带来了使用上的便捷，但部分用户希望通过接入其他用户建立的 WIFI 网络，以避免产生 WIFI 网络的建立和维持所需的费用，即“蹭网”行为。

如果蹭网用户正常使用 WIFI 网络，可能会造成对无线资源的占用，使得每台设备可使用的网络资源降低、影响原始用户的使用体验；然而，由于所有的设备都需要接入同一台无线路由器，因而蹭网用户还可能对 WIFI 网络内的设备进行非法访问，甚至造成原始用户的隐私泄露、账户安全风险等问题。

为此，相关技术中提出了对请求接入 WIFI 网络的设备进行鉴权，即需要蹭网用户输入正确的访问密码；然而，通过对访问密码进行有限次数的尝试，蹭网用户很容易对访问密码实现破解，从而无法有效阻止蹭网用户的非法接入和访问。

20

发明内容

本公开提供连接管理方法及装置、电子设备，以解决相关技术中的无线网络容易被蹭网的技术问题。

25 根据本公开实施例的第一方面，提供一种连接管理方法，包括：
与设备建立无线连接时，统计所述设备在预设时间段内的鉴权失败次数；
当所述鉴权失败次数大于或等于预设次数阈值时，执行预设的风险处理操作。

可选的，还包括：

当接收到所述设备发送的连接建立请求时，获取所述设备的标识信息；

30 若所述标识信息存在于预设的黑名单列表中，则忽略所述连接建立请求，否则执行与所述设备的无线连接操作。

可选的，所述执行预设的风险处理操作，包括：

将所述标识信息添加至所述黑名单中。

可选的，所述执行预设的风险处理操作，包括：

35 向预设的管理终端发送风险提示信息；

根据所述管理终端返回的控制指令，将所述标识信息添加至所述黑名单中。

可选的，所述执行预设的风险处理操作，还包括：

在发送所述风险提示信息之后、接收到所述控制指令之前，暂停对所述设备的鉴权操作，或将对所述设备的鉴权结果设置为鉴权失败。

5 根据本公开实施例的第二方面，提供一种连接管理装置，包括：

统计单元，用于与设备建立无线连接时，统计所述设备在预设时间段内的鉴权失败次数；

执行单元，用于当所述鉴权失败次数大于或等于预设次数阈值时，执行预设的风险处理操作。

10 可选的，还包括：

获取单元，用于当接收到所述设备发送的连接建立请求时，获取所述设备的标识信息；

处理单元，用于在所述标识信息存在于预设的黑名单列表的情况下，忽略所述连接建立请求，否则执行与所述设备的无线连接操作。

可选的，所述执行单元包括：

15 第一添加子单元，用于将所述标识信息添加至所述黑名单中。

可选的，所述执行单元包括：

信息发送子单元，用于向预设的管理终端发送风险提示信息；

第二添加子单元，用于根据所述管理终端返回的控制指令，将所述标识信息添加至所述黑名单中。

20 可选的，所述执行单元还包括：

鉴权处理子单元，用于在发送所述风险提示信息之后、接收到所述控制指令之前，暂停对所述设备的鉴权操作，或将对所述设备的鉴权结果设置为鉴权失败。

根据本公开实施例的第三方面，提供一种电子设备，包括：

处理器；

25 用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

与设备建立无线连接时，统计所述设备在预设时间段内的鉴权失败次数；

当所述鉴权失败次数大于或等于预设次数阈值时，执行预设的风险处理操作。

本公开的实施例提供的技术方案可以包括以下有益效果：

30 本公开通过对设备的鉴权失败次数进行统计，可以准确识别出蹭网用户对鉴权密码的“尝试”行为，并通过及时执行风险处理操作，以避免蹭网用户对无线网络的破解，有助于提升无线网络的安全性。

应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

35

附图说明

此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本发明的实施例，并与说明书一起用于解释本发明的原理。

图 1 是根据一示例性实施例示出的一种连接管理方法的流程图。

5 图 2 是根据一示例性实施例示出的一种连接管理的应用场景示意图。

图 3 是根据一示例性实施例示出的另一种连接管理方法的流程图。

图 4 是根据一示例性实施例示出的另一种连接管理的应用场景示意图。

图 5 是根据一示例性实施例示出的另一种连接管理方法的流程图。

图 6 是根据一示例性实施例示出的一种连接管理的界面示意图。

10 图 7 是根据一示例性实施例示出的一种连接管理装置的框图。

图 8 是根据一示例性实施例示出的另一种连接管理装置的框图。

图 9 是根据一示例性实施例示出的另一种连接管理装置的框图。

图 10 是根据一示例性实施例示出的另一种连接管理装置的框图。

图 11 是根据一示例性实施例示出的另一种连接管理装置的框图。

15 图 12 是根据一示例性实施例示出的一种用于连接管理的装置的结构示意图。

具体实施方式

这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中
20 所描述的实施方式并不代表与本发明相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本发明的一些方面相一致的装置和方法的例子。

图 1 是根据一示例性实施例示出的一种连接管理方法的流程图，如图 1 所示，该方法用于无线路由器中，包括以下步骤。

在步骤 102 中，与设备建立无线连接时，统计设备在预设时间段内的鉴权失败次数。

25 在本实施例中，设备在接入无线路由器建立的无线网络时，无线路由器需要对该设备进行身份鉴权，例如可以判断用户通过该设备发送的鉴权密码是否正确。因此，本公开中的“鉴权失败”可以由鉴权密码不正确所导致。

在本实施例中，当一台设备首次接入某个无线网络时，用户需要手动输入鉴权密码等鉴权信息；其中，如果鉴权成功，则设备可以通过记录下本次使用的鉴权密码，并用于以后接入相同的无线网络。因此，在无线网络的配置未发生改变的情况下，已连接过的设备
30 不会由于鉴权密码不正确而出现鉴权失败事件，而可能在首次接入的设备上出现鉴权密码不正确的情况。

在步骤 104 中，当鉴权失败次数大于或等于预设次数阈值时，执行预设的风险处理操作。

35 在本实施例中，鉴权密码由用户手动输入时，用户可能知道正确的鉴权密码，该用户

为正常用户。但可能由于输入错误而导致鉴权失败，此时该用户必然会及时纠正错误，不会导致鉴权失败次数过多。或者，用户可能并不知道正确的鉴权密码，即该用户为蹭网用户，则该蹭网用户只能够通过不断尝试的方式来接入无线网络，从而导致在短时间发送多次鉴权失败事件。所以，通过监测预设时间段内发生的鉴权失败次数，即可有效区分用户身份，规避蹭网风险。

在本实施例中，作为一示例性实施方式，风险处理操作可以包括将多次鉴权失败的设备记录至黑名单中，从而拒绝该设备加入无线网络中。作为另一示例性实施方式，风险处理操作可以包括将多次鉴权失败的设备标识信息告知正常用户，并由正常用户决定是否将其记录至黑名单中，或采取其他处理方式。

由上述实施例可知，本公开通过对设备的鉴权失败次数进行统计，可以准确识别出蹭网用户对鉴权密码的“尝试”行为，并通过及时执行风险处理操作，以避免蹭网用户对无线网络的破解，有助于提升无线网络的安全性。

请参考图 2，图 2 是根据一示例性实施例示出的一种连接管理的应用场景示意图。在图 2 所示的应用场景中，包括一无线路由器和一支持无线功能的设备，比如设备 1，且设备 1 向无线路由器发起连接请求，以期加入无线路由器建立的无线网络中。对应于图 2 所示的应用场景，图 3 是根据一示例性实施例示出的另一种连接管理方法的流程图，包括以下步骤。

在步骤 302 中，设备 1 向无线路由器发起连接建立请求。

在本实施例中，设备 1 可以为图 2 所示的笔记本电脑，或者其他支持无线通信的任意设备，比如智能手机、平板电脑等。

在本实施例中，“连接建立请求”只是对“请求建立无线连接”这一操作的概述，而并不用于限制该操作过程中交互的报文名称及交互次数。

在步骤 304 中，无线路由器获取设备 1 的标识信息。

在本实施例中，标识信息可以设备 1 的硬件信息，比如 MAC (Media Access Control, 媒介访问控制) 地址等，或者其他用于区分和识别不同设备的信息。

在本实施例中，可以在设备 1 发送的连接建立请求中，获取上述标识信息，比如当标识信息为设备 1 的 MAC 地址时，该 MAC 地址即来自设备 1 的报文的源 MAC 地址。

在步骤 306 中，将设备 1 的标识信息与预设的黑名单列表进行匹配。

在步骤 308 中，如果在黑名单列表中未查找到设备 1 的标识信息，则由无线路由器与设备 1 之间执行无线连接操作，否则可以忽略来自设备 1 的连接建立请求，拒绝与设备 1 建立无线连接。

在步骤 310 中，获取无线路由器与设备 1 之间建立无线连接的过程中，是否鉴权成功，比如设备 1 发送的鉴权密码是否正确；如果鉴权失败，则对鉴权失败次数进行统计。

在步骤 312 中，当预设时间段内的鉴权失败次数大于或等于预设次数阈值时，将设备 1 的标识信息添加至上述的黑名单列表中，从而解决设备 1 接入无线路由器创建的无线网

络中。

在本实施例中，只有当设备 1 所属用户为蹭网用户时，即该用户并不知道真正的鉴权密码，该蹭网用户需要通过反复尝试的方式，以期猜测出鉴权密码，因而会导致短时间内的多次鉴权失败事件，明显区分于正常用户偶然出现的误输入行为，从而区分出蹭网行为以及相应的设备。

在本实施例中，预设时间段的长度可以由厂商默认，或者由用户根据需要进行设置，比如 3 分钟。

在上述实施例中，无线路由器通过对短时间内的鉴权失败事件的统计，可以自动识别出蹭网行为，并将蹭网设备添加至黑名单中，以禁止该蹭网设备加入无线路由器创建的无线网络中，从而确保无线网络的正常使用和高安全性。

请参考图 4，图 4 是根据一示例性实施例示出的另一种连接管理的应用场景示意图。在图 4 所示的应用场景中，包括一无线路由器和两台支持无线功能的设备，比如设备 1 和设备 2，且设备 1 向无线路由器发起连接请求，以期加入无线路由器建立的无线网络中，而设备 2 是预先配置的管理终端。对应于图 4 所示的应用场景，图 5 是根据一示例性实施例示出的另一种连接管理方法的流程图，包括以下步骤。

在步骤 502 中，设备 1 向无线路由器发起连接建立请求。

在本实施例中，设备 1 可以为图 4 所示的笔记本电脑，或者其他支持无线通信的任意设备，比如智能手机、平板电脑等。

在本实施例中，“连接建立请求”只是对“请求建立无线连接”这一操作的概述，而并不用于限制该操作过程中交互的报文名称及交互次数。

在步骤 504 中，无线路由器获取设备 1 的标识信息。

在本实施例中，标识信息可以设备 1 的硬件信息，比如 MAC 地址等，或者其他用于区分和识别不同设备的信息。

在本实施例中，可以在设备 1 发送的连接建立请求中，获取上述标识信息；比如当标识信息为设备 1 的 MAC 地址时，该 MAC 地址即来自设备 1 的报文的源 MAC 地址。

在步骤 506 中，将设备 1 的标识信息与预设的黑名单列表进行匹配。

在步骤 508 中，如果在黑名单列表中未查找到设备 1 的标识信息，则由无线路由器与设备 1 之间执行无线连接操作，否则可以忽略来自设备 1 的连接建立请求，拒绝与设备 1 建立无线连接。

在步骤 510 中，获取无线路由器与设备 1 之间建立无线连接的过程中，是否鉴权成功，比如设备 1 发送的鉴权密码是否正确；如果鉴权失败，则对鉴权失败次数进行统计。

在步骤 512 中，当鉴权失败次数大于或等于预设次数阈值时，无线路由器向设备 2 发送风险提示信息。

在本实施例中，作为一示例性实施方式，图 6 示出了设备 2 的屏幕界面上显示出的风险提示信息，比如“风险类型”、“风险等级”、“设备信息”等，以供用户对当前可能

存在的风险状况进行分析；然后，在用户确定当前设备（即图 4 所示的设备 1）为蹭网设备并且希望禁止其加入当前无线网络时，可以选择“加入黑名单”，或者选择“忽略”等处理方式。

在本实施例中，作为一示例性实施方式，设备 2 可以处于无线路由器创建的无线网络内，则设备 2 与无线路由器可以基于该无线网络进行信息交互；作为另一示例性实施方式，设备 2 可以不处于无线路由器创建的无线网络内，则设备 2 与无线路由器可以分别接入互联网内，并基于互联网进行信息交互，则设备 2 所属用户可以实现远程控制，比如在公司上班期间，管理家中的无线网络。

在步骤 514 中，无线路由器接收来自设备 2 的控制指令。

在本实施例中，在步骤 510 与步骤 514 之间，即无线路由器检测出设备 1 的蹭网风险之后、但尚未接收到返回的控制指令时，为避免设备 1 在此期间完成对无线路由器的破解，可以暂停对设备 1 的鉴权操作，或将对设备 1 的鉴权结果全部设置为鉴权失败，防止设备 1 接入无线网络中。

在步骤 516 中，若设备 2 返回的控制指令对应于“加入黑名单”，则无线路由器将设备 1 的标识信息添加至上述的黑名单列表中；或者，若设备 2 返回的控制指令对应于“忽略”，则无线路由器可以恢复对设备 1 的正常鉴权操作。

在上述实施例中，无线路由器通过对短时间内的鉴权失败事件的统计，可以自动识别出蹭网行为，并结合用户的简单交互操作，确定是否将“疑似蹭网设备”添加至黑名单中，从而在确保无线网络的正常使用和高安全性的同时，避免对正常设备的误判断。

此外，在图 3 和图 5 所示的实施例中，对于被添加至黑名单中的设备，若用户认为存在误判断，可以通过登录无线路由器，取消对黑名单中的任意设备的记录，从而将误判断的“蹭网设备”恢复为“正常设备”。

与前述的信息显示方法的实施例相对应，本公开还提供了连接管理装置的实施例。

图 7 是根据一示例性实施例示出的一种连接管理装置框图。参照图 7，该装置包括统计单元 71 和执行单元 72。

其中，统计单元 71，被配置为与设备建立无线连接时，统计所述设备在预设时间段内的鉴权失败次数；

执行单元 72，被配置为当所述鉴权失败次数大于或等于预设次数阈值时，执行预设的风险处理操作。

在上述实施例中，通过对设备的鉴权失败次数进行统计，可以准确识别出蹭网用户对鉴权密码的“尝试”行为，并通过及时执行风险处理操作，以避免蹭网用户对无线网络的破解，有助于提升无线网络的安全性。

如图 8 所示，图 8 是根据一示例性实施例示出的另一种连接管理装置的框图，该实施

例在前述图 7 所示实施例的基础上，该装置还可以包括：获取单元 73 和处理单元 74。

其中，获取单元 73，被配置为当接收到所述设备发送的连接建立请求时，获取所述设备的标识信息；

处理单元 74，被配置为在所述标识信息存在于预设的黑名单列表的情况下，忽略所述连接建立请求，否则执行与所述设备的无线连接操作。

如图 9 所示，图 9 是根据一示例性实施例示出的另一种连接管理装置的框图，该实施例在前述图 8 所示实施例的基础上，执行单元 72 可以包括：第一添加子单元 721。

其中，第一添加子单元 721，被配置为将所述标识信息添加至所述黑名单中。

如图 10 所示，图 10 是根据一示例性实施例示出的另一种连接管理装置的框图，该实施例在前述图 8 所示实施例的基础上，执行单元 72 可以包括：信息发送子单元 722 和第二添加子单元 723。

其中，信息发送子单元 722，被配置为向预设的管理终端发送风险提示信息；

第二添加子单元 723，被配置为根据所述管理终端返回的控制指令，将所述标识信息添加至所述黑名单中。

如图 11 所示，图 11 是根据一示例性实施例示出的另一种连接管理装置的框图，该实施例在前述图 10 所示实施例的基础上，执行单元 72 还可以包括：鉴权处理子单元 724。

其中，鉴权处理子单元 724，被配置为在发送所述风险提示信息之后、接收到所述控制指令之前，暂停对所述设备的鉴权操作，或将对所述设备的鉴权结果设置为鉴权失败。

关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本公开方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

相应的，本公开还提供一种连接管理装置，包括：处理器；用于存储处理器可执行指令的存储器；其中，所述处理器被配置为：与设备建立无线连接时，统计所述设备在预设时间段内的鉴权失败次数；当所述鉴权失败次数大于或等于预设次数阈值时，执行预设的风险处理操作。

相应的，本公开还提供一种终端，所述终端包括有存储器，以及一个或者一个以上的

程序，其中一个或者一个以上程序存储于存储器中，且经配置以由一个或者一个以上处理器执行所述一个或者一个以上程序包含用于进行以下操作的指令：与设备建立无线连接时，统计所述设备在预设时间段内的鉴权失败次数；当所述鉴权失败次数大于或等于预设次数阈值时，执行预设的风险处理操作。

5

图 12 是根据一示例性实施例示出的一种用于连接管理的装置 1200 的框图。例如，装置 1200 可以被提供为一无线路由器或具有无线路由功能的智能终端。参照图 12，装置 1200 包括处理组件 1222，其进一步包括一个或多个处理器，以及由存储器 1232 所代表的存储器资源，用于存储可由处理部件 1222 的执行的指令，例如应用程序。存储器 1232 中存储的应用程序可以包括一个或一个以上的每一个对应于一组指令的模块。此外，处理组件 1222 被配置为执行指令，以执行上述连接管理方法。

10

装置 1200 还可以包括一个电源组件 1226 被配置为执行装置 1200 的电源管理，一个有线或无线网络接口 1250 被配置为将装置 1200 连接到网络，和一个输入输出（I/O）接口 1258。装置 1200 可以操作基于存储在存储器 1232 的操作系统，例如 Windows Server™，Mac OS X™，Unix™，Linux™，FreeBSD™ 或类似。

15

本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本发明的其它实施方案。本申请旨在涵盖本发明的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本发明的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本发明的真正范围和精神由下面的权利要求指出。

20

应当理解的是，本发明并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本发明的范围仅由所附的权利要求来限制。

权利要求

1. 一种连接管理方法，其特征在于，包括：

与设备建立无线连接时，统计所述设备在预设时间段内的鉴权失败次数；
当所述鉴权失败次数大于或等于预设次数阈值时，执行预设的风险处理操作。

5 2. 根据权利要求1所述的方法，其特征在于，还包括：

当接收到所述设备发送的连接建立请求时，获取所述设备的标识信息；
若所述标识信息存在于预设的黑名单列表中，则忽略所述连接建立请求，否则执行与
所述设备的无线连接操作。

10 3. 根据权利要求2所述的方法，其特征在于，所述执行预设的风险处理操作，包括：
将所述标识信息添加至所述黑名单中。

4. 根据权利要求1或2所述的方法，其特征在于，所述执行预设的风险处理操作，
包括：

向预设的管理终端发送风险提示信息；
根据所述管理终端返回的控制指令，将所述标识信息添加至所述黑名单中。

15 5. 根据权利要求4所述的方法，其特征在于，所述执行预设的风险处理操作，还包括：

在发送所述风险提示信息之后、接收到所述控制指令之前，暂停对所述设备的鉴权操作，
或将对所述设备的鉴权结果设置为鉴权失败。

6. 一种连接管理装置，其特征在于，包括：

20 统计单元，用于与设备建立无线连接时，统计所述设备在预设时间段内的鉴权失败次数；

执行单元，用于当所述鉴权失败次数大于或等于预设次数阈值时，执行预设的风险处理操作。

7. 根据权利要求6所述的装置，其特征在于，还包括：

25 获取单元，用于当接收到所述设备发送的连接建立请求时，获取所述设备的标识信息；
处理单元，用于在所述标识信息存在于预设的黑名单列表的情况下，忽略所述连接建立请求，
否则执行与所述设备的无线连接操作。

8. 根据权利要求7所述的装置，其特征在于，所述执行单元包括：

第一添加子单元，用于将所述标识信息添加至所述黑名单中。

30 9. 根据权利要求6或7所述的装置，其特征在于，所述执行单元包括：

信息发送子单元，用于向预设的管理终端发送风险提示信息；

第二添加子单元，用于根据所述管理终端返回的控制指令，将所述标识信息添加至所述黑名单中。

10. 根据权利要求9所述的装置，其特征在于，所述执行单元还包括：

35 鉴权处理子单元，用于在发送所述风险提示信息之后、接收到所述控制指令之前，暂

停对所述设备的鉴权操作，或将对所述设备的鉴权结果设置为鉴权失败。

11. 一种电子设备，其特征在于，包括：

处理器；

用于存储处理器可执行指令的存储器；

5 其中，所述处理器被配置为：

与设备建立无线连接时，统计所述设备在预设时间段内的鉴权失败次数；

当所述鉴权失败次数大于或等于预设次数阈值时，执行预设的风险处理操作。

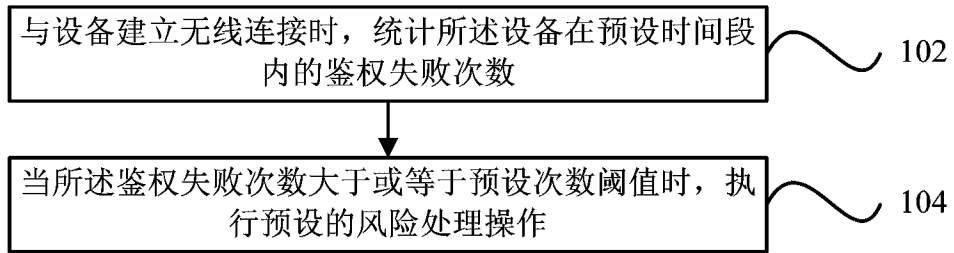


图1

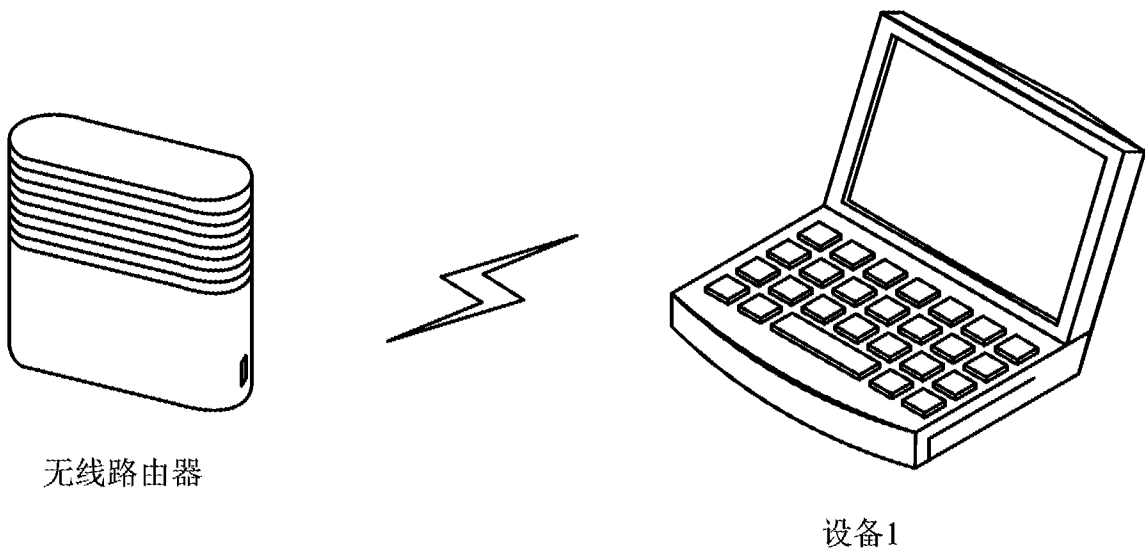


图2

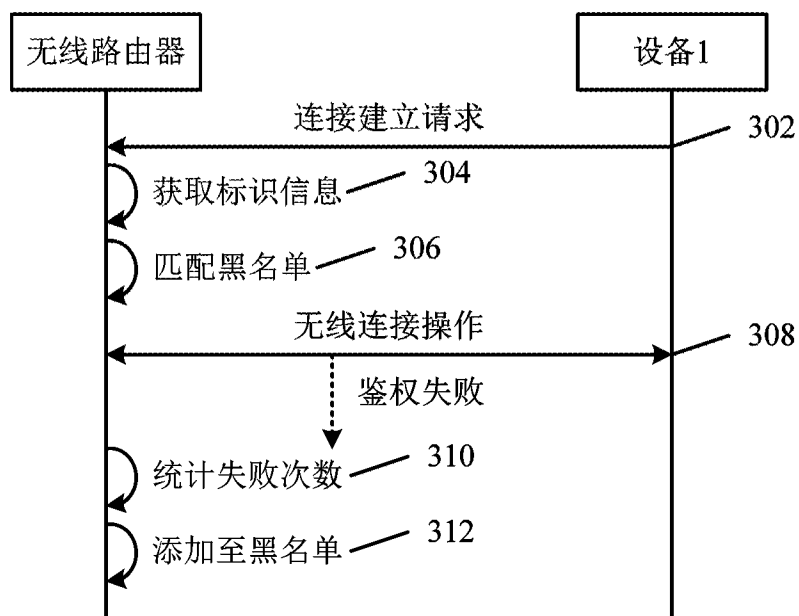


图3

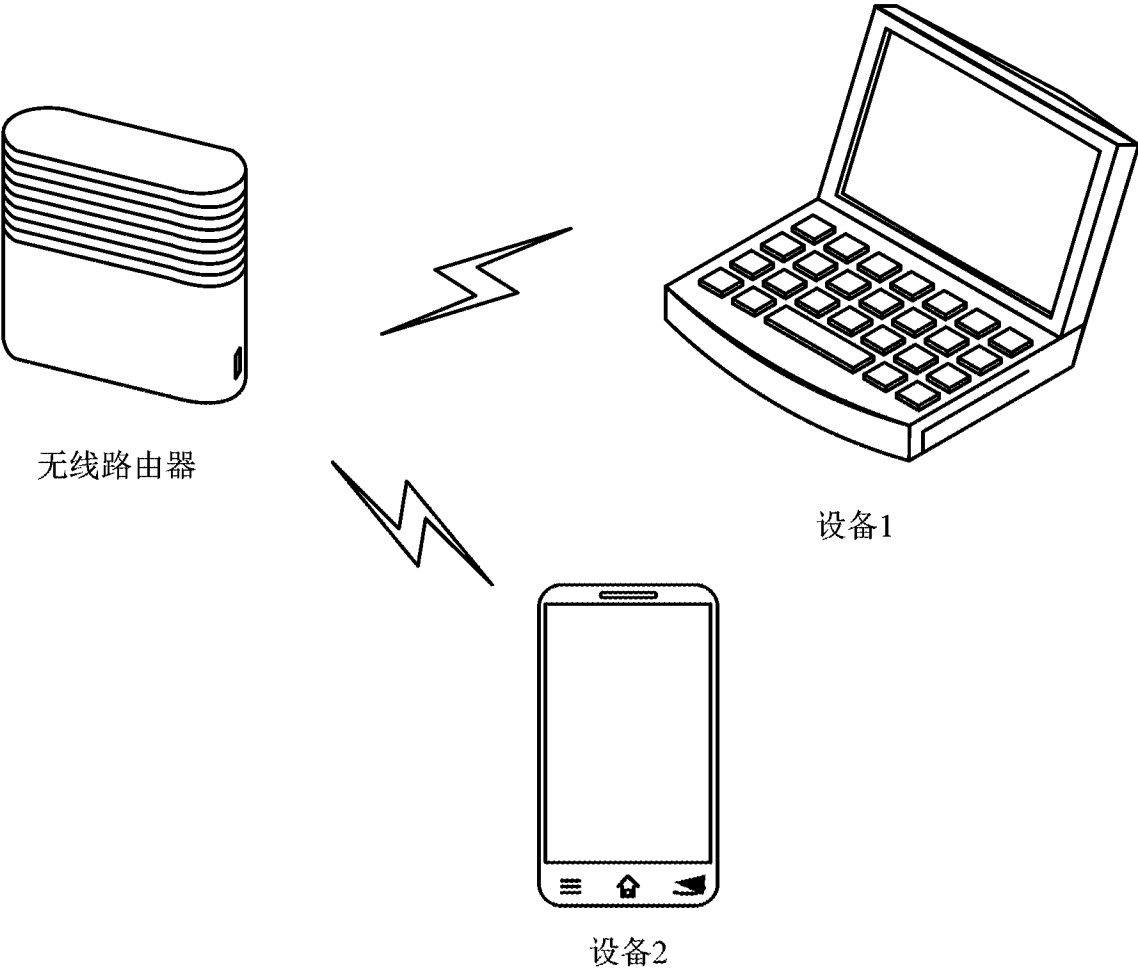


图4

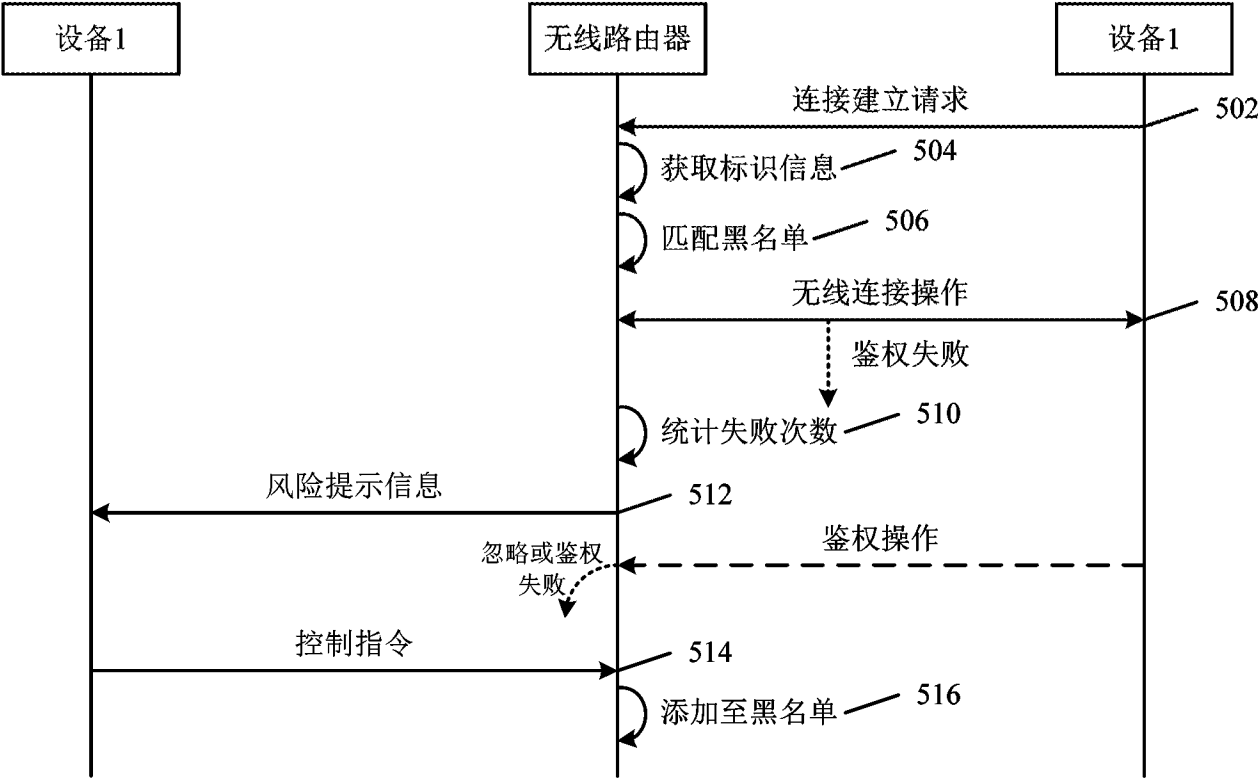


图5



图6

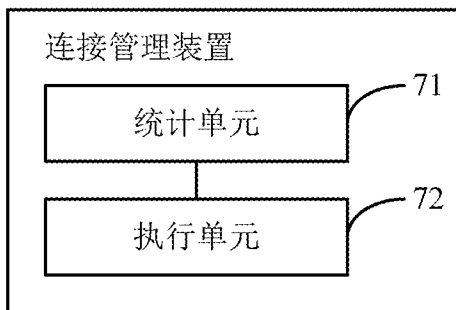


图7

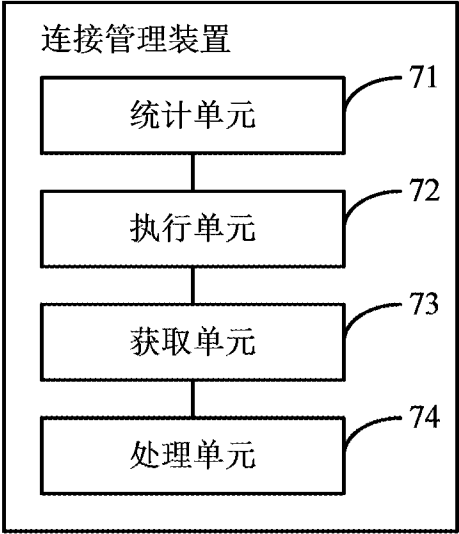


图8

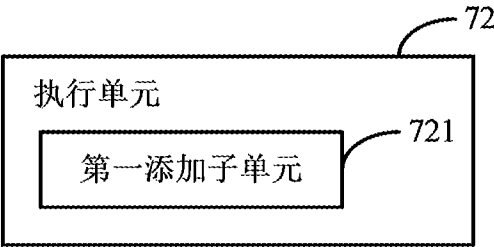


图9

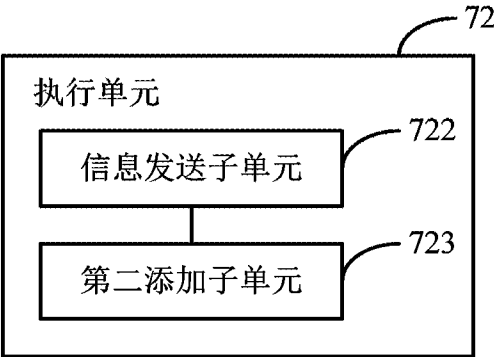


图10

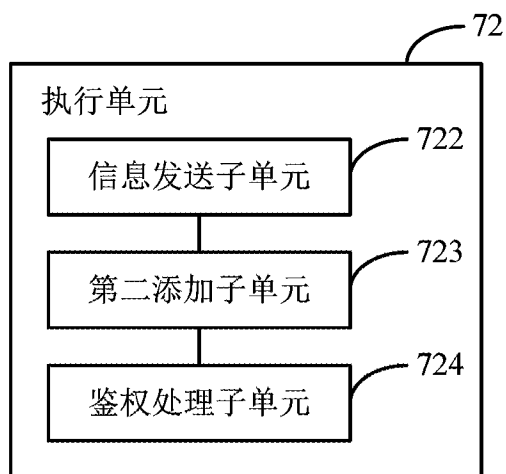


图11

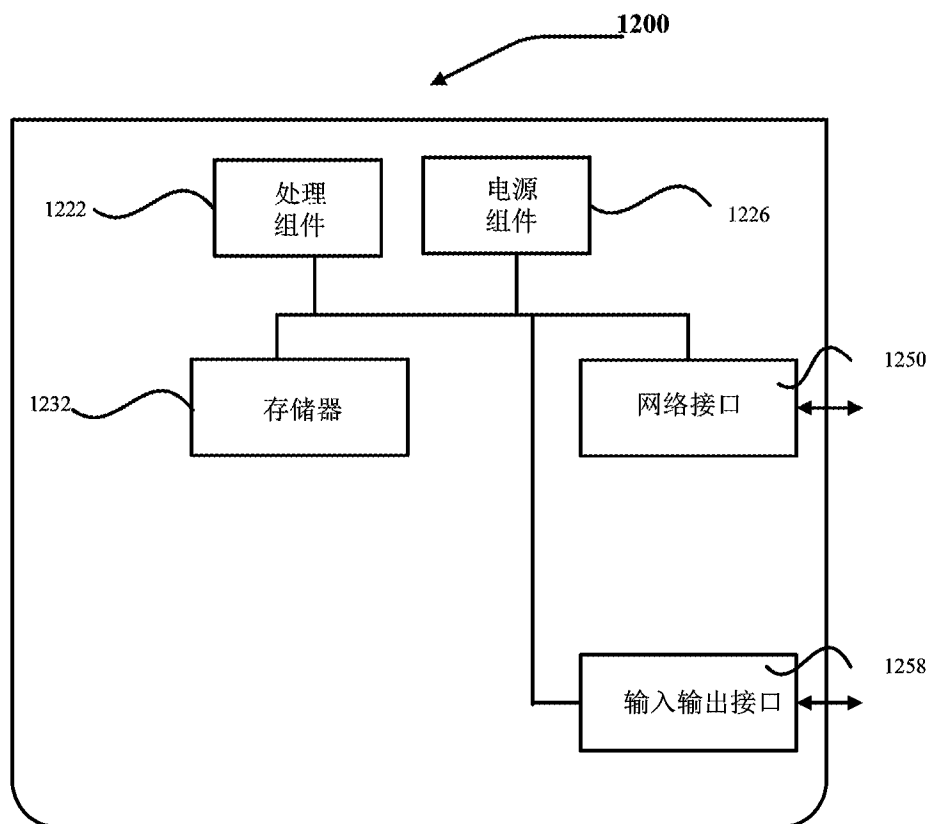


图12

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/074944

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06 (2009.01) i; H04W 12/08 (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; G06F; 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)

CNABS; CNTXT; CNKI; VEN: authenticat+, time?, period, threshold, failure, fault, attack

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104333863 A (BEIJING XIAOMI TECHNOLOGY CO., LTD.), 04 February 2015 (04.02.2015), see claims 1-11	1-11
X	CN 101355556 A (FUJI XEROX CO., LTD.), 28 January 2009 (28.01.2009), see description, page 11, line 1 to page16, line 5, and figure 9	1-11
A	CN 101226575 A (ZTE CORP.), 23 July 2008 (23.07.2008), see the whole document	1-11

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

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 05 June 2015 (05.06.2015)	Date of mailing of the international search report 25 June 2015 (25.06.2015)
Name and mailing address of the ISA/CN: 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 ZOU, Ting Telephone No.: (86-10) 62089393

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2015/074944

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104333863 A	04 February 2015	None	
CN 101355556 A	28 January 2009	JP 2009031963 A	12 February 2009
		CN 101355556 B	05 June 2013
		JP 5098487 B2	12 December 2012
		US 2009031406 A1	29 January 2009
CN 101226575 A	23 July 2008	WO 2009094886 A1	06 August 2009
		US 2011010550 A1	13 January 2011
		US 8375454 B2	12 February 2013
		CN 101226575 B	20 April 2011
		IN 201001725 P3	03 December 2010

A. 主题的分类		
H04W 12/06(2009.01)i; H04W 12/08(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; G06F; 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))		
CNABS;CNTXT; CNKI; VEN: 鉴权, 认证, 时间, 期间, 次数, 阈值, 门限, 失败, 错误, 攻击, authenticat+, time?, period, threshold, failure, fault, attack		
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
PX	CN 104333863 A (小米科技有限责任公司) 2015年 2月 4日 (2015 - 02 - 04) 参见权利要求1-11	1-11
X	CN 101355556 A (富士施乐株式会社) 2009年 1月 28日 (2009 - 01 - 28) 参见说明书第11页第1行至第16页第5行, 图9	1-11
A	CN 101226575 A (中兴通讯股份有限公司) 2008年 7月 23日 (2008 - 07 - 23) 参见全文	1-11
☐ 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		国际检索报告邮寄日期
2015年 6月 5日		2015年 6月 25日
ISA/CN的名称和邮寄地址		授权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国		邹婷
传真号 (86-10)62019451		电话号码 (86-10)62089393

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/074944

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	104333863	A	2015年 2月 4日	无			
CN	101355556	A	2009年 1月 28日	JP	2009031963	A	2009年 2月 12日
				CN	101355556	B	2013年 6月 5日
				JP	5098487	B2	2012年 12月 12日
				US	2009031406	A1	2009年 1月 29日
CN	101226575	A	2008年 7月 23日	WO	2009094886	A1	2009年 8月 6日
				US	2011010550	A1	2011年 1月 13日
				US	8375454	B2	2013年 2月 12日
				CN	101226575	B	2011年 4月 20日
				IN	201001725	P3	2010年 12月 3日