

(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



(10) 国际公布号

(43) 国际公布日
2016 年 11 月 24 日 (24.11.2016) W I P O | P C T

W O 2016/184380 A 1

- (51) 国际分类号 :
H04W 48/04 (2009 .01)
- (21) 国际申请号 : PCT/CN2016/082354
- (22) 国际申请日 : 2016 年 5 月 17 日 (17.05.2016)
- (25) 申报语言 : 中文
- (26) 公布语言 : 中文
- (30) 优先权 :
2015 10257791 .0 2015 年 5 月 19 日 (19.05.2015) CN
- (71) 申请人 :中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦 ,Guangdong 518057 (CN)。
- (72) 发明人 :范贤友 (FAN, Xianyou); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交 ,Guangdong 518057 (CN)。
- (74) 代理人 :北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW
- OFFICE); 中国北京市海淀区学清路 8 号 B 座 1601A, Beijing 100192 (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)。

[见续页]

(54) Title: PROCESSING METHOD AND DEVICE FOR NETWORK ACCESS

(54) 发明名称 :接入网络的处理方法及装置

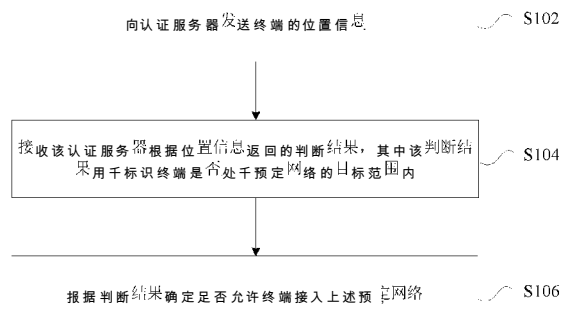


图 1

- S102 TRANSMIT POSITION INFORMATION OF A TERMINAL TO AN AUTHENTICATION SERVER
- S104 RECEIVE A JUDGMENT RESULT RETURNED BY THE AUTHENTICATION SERVER ACCORDING TO THE POSITION INFORMATION, WHEREIN THE JUDGMENT RESULT IS USED FOR MARKING WHETHER THE TERMINAL IS POSITIONED WITHIN A TARGET RANGE OF A SCHEDULED NETWORK OR NOT
- S106 DETERMINE, ACCORDING TO THE JUDGMENT RESULT, WHETHER TO ALLOW THE TERMINAL TO ACCESS THE SCHEDULED NETWORK OR NOT

(57) Abstract: A processing method and device for network access. The method comprises: transmitting position information of a terminal to an authentication server; receiving a judgment result returned by the authentication server according to the position information, wherein the judgment result is used for marking whether the terminal is positioned within a target range of a scheduled network or not; and determining, according to the judgment result, whether to allow the terminal to access the scheduled network or not. The solution solves the problem of low control efficiency of network access existing in the related art, thereby realizing an effect of improving the control efficiency of network access.

(57) 摘要: 一种接入网络的处理方法及装置, 其中, 该方法包括: 向认证服务器发送终端的位置信息; 接收该认证服务器根据位置信息返回的判断结果, 其中该判断结果用于标识终端是否处于预定网络的目标范围内; 根据判断结果确定是否允许终端接入上述预定网络。通过上述方案, 解决了相关技术中存在的网络接入控制效率低的问题, 进而达到了提高网络接入控制效率的效果。



根据细则 4.17 的声明：

本国际公布：

- 关于申请人有权申请并被授予专利(细则 4.17(ii))
- 包括国际检索报告(条约第 21 条(3))。
- 发明人资格(细则 4.17(iv))

接入网络的处理方法及装置

技术领域

本申请涉及但不限于通信领域，尤其是一种接入网络的处理方法及装置。

5

背景技术

随着移动互联网的飞速发展，各种智能终端以及 Wi-Fi 无线网络已经遍布人们活动的各个场所。然而入侵 Wi-Fi 无线网络并盗用其他可上网终端的带宽的现象却一直未能被有效禁止，其不仅仅影响网络体验，拖慢网速，更大的危害是让不可信的设备连入局域网络之中，带来更大的网络安全风险。Wi-Fi 无线网络虽有多种加密方案，如有线等效保密 (Wired Equivalent Privacy, 简称为 WEP)、Wi-Fi 网络安全接入 (Wi-Fi Protected Access, 简称为 WPA)、以及更高级的 WPA2 等等，其中 WEP 已被淘汰，WPA/WPA2 以及其他方式在密码足够复杂的情况下是比较安全的，但是由于大量的类似于 wifi 万能钥匙的软件收集各 Wi-Fi 无线网络的密码信息并共享给其他使用者，尽管使用者不一定能看到明文的密码，但事实上密码已泄露；更加安全的方法是在防火墙上设置媒体接入控制 (Media Access Control, 简称为 MAC) 地址白名单，但这一种方法配置繁琐，且仅适合网络使用者较少且固定的情况。

而在商业/公共区域，通常将 Wi-Fi 无线网络的密码写在墙上，或者由店员提供，这种方法没有安全性；更安全的方法是无密码接入，通过短信验证码或者微信关注等方式认证，这一类方法需要在路由器上进行配置，未认证的客户端发起的请求将会被重定向到指定的认证网页，验证通过后才可使用 Wi-Fi 无线网络，现在一般的智能路由器都可以支持这样的认证方式，主流的开源插件 wifidog 可较好的实现该功能。

通过短信/微信认证，商家可以收集到更精确的客户信息，精准地推送相关信息，但是仍然不能控制非目标群体使用 Wi-Fi 无线网络，比如某宾馆提供的无线网络，自然是仅希望员工和入住的客人可以使用，入侵 Wi-Fi 无线网络并盗用其他可上网终端的带宽的行为不仅加大网络安全风险，也很可能影响入住客人的网络体验，降低网速。由此可知，在相关技术中存在着网络

接入控制效率低的问题。

针对相关技术中存在的网络接入控制效率低的问题，目前尚未提出有效的解决方案。

5 发明内容

以下是对本文详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

本申请提供了一种接入网络的处理方法及装置，以至少解决相关技术中存在的网络接入控制效率低的问题。

10 根据本申请的一个方面，提供了一种接入网络的处理方法，包括：向认证服务器发送终端的位置信息；接收所述认证服务器根据所述位置信息返回的判断结果，其中所述判断结果用于标识所述终端是否处于预定网络的目标范围内；根据所述判断结果确定是否允许所述终端接入所述预定网络。

15 可选地，所述位置信息包括以下信息至少之一：所述终端检测到的 Wi-Fi 信号携带的 Wi-Fi 信号发射端的媒体接入控制 MAC 地址和所述终端检测到的 Wi-Fi 信号的信号强度、所述终端检测到的蓝牙信号携带的蓝牙信号发射端的地址和所述终端检测到的蓝牙信号的信号强度。

20 可选地，当所述判断结果为所述终端处于所述目标范围内时，所述根据所述判断结果确定是否允许所述终端接入所述预定网络的步骤包括：获取所述判断结果中携带的令牌信息；依据所述令牌信息通过路由器接入所述预定网络。

根据本申请的另一方面，提供了一种接入网络的处理方法，包括：接收终端的位置信息；根据所述位置信息判断所述终端是否处于预定网络的目标范围内；根据判断结果控制所述终端接入所述预定网络。

25 可选地，所述根据所述判断结果控制所述终端接入所述预定网络的步骤包括：当所述判断结果为所述终端位于所述目标范围内时，向所述终端发送令牌信息，其中，所述令牌信息用于所述终端通过路由器接入所述预定网络；当所述判断结果为所述终端位于所述目标范围外时，向所述终端发送拒绝所

述终端接入所述预定网络的信息。

5 可选地，所述当所述判断结果为所述终端位于所述目标范围内时，向所述终端发送所述令牌信息的步骤之后，所述处理方法还包括：接收所述路由器发送的预定令牌信息，其中，所述预定令牌信息为所述路由器在接收到终端发送的所述预定令牌信息后发送的；验证所述预定令牌信息与发送给所述终端的令牌信息是否一致；若验证结果为一一致，将允许所述终端接入所述预定网络的允许信息发送给所述路由器。

本申请另外提供一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令被执行时实现上述方法。

10 根据本申请的另一方面，提供了一种接入网络的处理装置，包括：发送模块，设置成向认证服务器发送终端的位置信息；第一接收模块，设置成接收所述认证服务器根据所述位置信息返回的判断结果，其中所述判断结果用于标识所述终端是否处于预定网络的目标范围内；处理模块，设置成根据所述判断结果确定是否允许所述终端接入所述预定网络。

15 可选地，所述位置信息包括以下信息至少之一：所述终端检测到的 Wi-Fi 信号携带的 Wi-Fi 信号发射端的媒体接入控制 MAC 地址和所述终端检测到的 Wi-Fi 信号的信号强度、所述终端检测到的蓝牙信号携带的蓝牙信号发射端的地址和所述终端检测到的蓝牙信号的信号强度。

20 可选地，所述处理模块包括：获取单元，设置成当所述判断结果为所述终端处于所述目标范围内时，获取所述判断结果中携带的令牌信息；接入单元，设置成依据所述令牌信息通过路由器接入所述预定网络。

25 根据本申请的另一方面，提供了一种接入网络的处理装置，包括：第二接收模块，设置成接收终端的位置信息；判断模块，设置成根据所述位置信息判断所述终端是否处于预定网络的目标范围内；控制模块，设置成根据判断结果控制所述终端接入所述预定网络。

可选地，所述控制模块包括：第一发送单元，设置成当所述判断结果为所述终端位于所述目标范围内时，向所述终端发送令牌信息，其中，所述令牌信息用于所述终端通过路由器接入所述预定网络；第二发送单元，设置成当所述判断结果为所述终端位于所述目标范围外时，向所述终端发送拒绝所

述终端接入所述预定网络的信息。

5 可选地，所述装置还包括：接收单元，设置成接收所述路由器发送的预定令牌信息，其中，所述预定令牌信息为所述路由器在接收到终端发送的所述预定令牌信息后发送的；验证单元，设置成验证所述预定令牌信息与发送给所述终端的令牌信息是否一致；第三发送单元，设置成若所述验证单元的验证结果为一一致，将允许所述终端接入所述预定网络的允许信息发送给所述路由器。

10 通过本申请的方案，采用向认证服务器发送终端的位置信息；接收所述认证服务器根据所述位置信息返回的判断结果，其中所述判断结果用于标识所述终端是否处于预定网络的目标范围内；根据所述判断结果确定是否允许所述终端接入所述预定网络，解决了相关技术中存在的网络接入控制效率低的问题，进而达到了提高网络接入控制效率的效果。

在阅读并理解了附图和详细描述后，可以明白其他方面。

15 附图概述

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

20 图 1 是根据本发明实施例的第一种接入网络的处理方法的流程图；

图 2 是根据本发明实施例的第二种接入网络的处理方法的流程图；

图 3 是根据本发明实施例的第一种接入网络的处理装置的结构框图；

图 4 是根据本发明实施例的第一种接入网络的处理装置的一种可选实施例的结构框图；

图 5 是根据本发明实施例的第二种接入网络的处理装置的结构框图；

25 图 6 是根据本发明实施例的第二种接入网络的处理装置的一种可选实施例的结构框图；

图 7 是根据本发明实施例的第二种接入网络的处理装置的另一种可选实施例的结构框图；

图 8 是根据本发明实施例一的路由器/AC 控制器与认证服务器分离情况下的交互流程图；

图 9 是根据本发明实施例的样本库和被验证点分别位于区域内和区域外的示意图；

5 图 10 是根据本发明实施例二的路由器/AC 控制器与认证服务器在同一个设备中的情况下的交互流程图。

本发明的较佳实施方式

下文中将参考附图并结合实施例来详细说明本申请。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

需要说明的是，本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。

15 随着室内定位技术逐渐成熟，利用 Wi-Fi/ 蓝牙指纹定位技术、惯导传感等技术，定位精度已能达到米级。基于相关技术中存在的上述问题，本发明实施例中，将室内定位技术与无线网络认证结合，提出了一种将终端的位置作为 Wi-Fi 无线网络的认证参数的方案，实现根据终端的位置决定终端是否可以访问网络。

20 在本实施例中提供了一种接入网络的处理方法，图 1 是根据本发明实施例的第一种接入网络的处理方法的流程图，如图 1 所示，该处理方法包括如下步骤：

步骤 S102，向认证服务器发送终端的位置信息；

步骤 S104，接收该认证服务器根据位置信息返回的判断结果，其中该判断结果用于标识终端是否处于预定网络的目标范围内；

25 步骤 S106，根据判断结果确定是否允许终端接入上述预定网络。

通过上述步骤，在对终端进行接入网络的控制时，通过判断终端的位置信息来确定是否允许终端接入预定网络，从而使得处于预定网络的目标范围内的终端才可以接入预定网络，提高了网络连接的安全系数，也保障了合法

使用者的利益。解决了相关技术中存在的网络接入控制效率低的问题，进而达到了提高网络接入控制效率的效果。

其中，上述的位置信息可以通过多种方式进行确定，在一个可选的实施例中，上述位置信息可以包括以下信息至少之一：上述终端检测到的 Wi-Fi 信号携带的 Wi-Fi 信号发射端的媒体接入控制 MAC 地址和上述终端检测到的 Wi-Fi 信号的信号强度、上述终端检测到的蓝牙信号携带的蓝牙信号发射端的地址和上述终端检测到的蓝牙信号的信号强度；还可以通过终端的定位功能确定终端的具体位置，并将所确定的位置信息上报给认证服务器；或通过其他方式确定终端的位置信息。

在一个可选的实施例中，当上述判断结果为终端处于目标范围内时，所述根据判断结果确定是否允许终端接入上述预定网络的步骤包括：获取判断结果中携带的令牌信息；依据该令牌信息通过路由器接入上述预定网络。所述依据令牌信息通过路由器接入上述预定网络的步骤可以包括，当终端获取到令牌信息后，将该令牌信息发送给路由器，路由器将接收的令牌信息发送给认证服务器，认证服务器通过对比路由器发送过来的令牌信息和预先发送给终端的令牌信息来确定是否允许终端接入预定网络。当对比结果为一小时，确定该终端处于目标范围内，则允许该终端接入预定网络，从而使得终端通过路由器接入预定网络。若对比结果不一致，则不允许上述终端接入预定网络。进而拦截了非法用户接入网络，保障了合法用户的利益。提高了接入网络的安全系数。

图 2 是根据本发明实施例的第二种接入网络的处理方法的流程图，如图 2 所示，该处理方法包括如下步骤：

步骤 S202，接收终端的位置信息；

步骤 S204，根据该位置信息判断终端是否处于预定网络的目标范围内；

步骤 S206，根据判断结果控制终端接入上述预定网络。

通过上述步骤，在控制终端接入网络时，通过验证终端的位置信息来确定是否允许终端接入预定网络，从而使得处于预定位位置范围内的终端才可以接入预定网络，提高了网络连接的安全系数，也保障了合法使用者的利益。解决了相关技术中存在的网络接入控制效率低的问题，进而达到了提高网络

接入控制效率的效果。

在一个可选的实施例 5 中，根据上述判断结果控制终端接入预定网络的步骤包括：当上述判断结果为终端位于目标范围内时，向终端发送令牌信息，其中，该令牌信息用于终端通过路由器接入上述预定网络；当上述判断结果为终端位于目标范围外时，向上述终端发送拒绝终端接入上述预定网络的信息。从而实现了依据终端的具体位置控制终端接入预定网络。

在一个可选的实施例 10 中，在所述向上述终端发送令牌信息的步骤之后，所述第二种接入网络的处理方法还包括：接收路由器发送的预定令牌信息，其中，该预定令牌信息为路由器在接收到终端发送的预定令牌信息后发送的；验证该预定令牌信息与发送给终端的令牌信息是否一致，若验证结果为一 致，将允许上述终端接入预定网络的允许信息发送给路由器。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对相关技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端设备（可以是手机，计算机，服务器，或者网络设备等）执行本申请各个实施例的方法。

本发明实施例另外提供一种计算机可读存储介质，存储有计算机可执行指令，所述计算机可执行指令被执行时实现上述方法。

在本实施例中还提供了一种接入网络的处理装置，该装置用于实现上述实施例及可选实施方式，已经进行过说明的不再赘述。如以下所使用的，术语“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。

图 3 是根据本发明实施例的第一种接入网络的处理装置的结构框图，如图 3 所示，该装置包括发送模块 32、第一接收模块 34 和处理模块 36，下面对该装置进行说明：

发送模块 32，设置成向认证服务器发送终端的位置信息；第一接收模块

34, 连接至上述发送模块 32, 设置成接收认证服务器根据位置信息返回的判断结果, 其中该判断结果用于标识终端是否处于预定网络的目标范围内; 处理模块 36, 连接至上述第一接收模块 34, 设置成根据判断结果确定是否允许终端接入上述预定网络。

- 5 在一个可选的实施例中, 上述的位置信息包括以下信息至少之一: 终端检测到的 Wi-Fi 信号携带的 Wi-Fi 信号发射端的媒体接入控制 MAC 地址和终端检测到的 Wi-Fi 信号的信号强度、终端检测到的蓝牙信号携带的蓝牙信号发射端的地址和终端检测到的蓝牙信号的信号强度。

10 图 4 是根据本发明实施例的第一种接入网络的处理装置的一种可选实施例的结构框图 如图 4 所示, 该处理模块 36 包括获取单元 42 和接入单元 44, 下面对该处理模块 36 进行说明。

获取单元 42, 设置成当上述判断结果为终端处于目标范围内时, 获取判断结果中携带的令牌信息; 接入单元 44, 连接至上述获取单元 42, 设置成依据上述令牌信息通过路由器接入预定网络。

- 15 图 5 是根据本发明实施例的第二种接入网络的处理装置的结构框图, 如图 5 所示, 该装置包括第二接收模块 52、判断模块 54 和控制模块 56, 下面对该装置进行说明。

20 第二接收模块 52, 设置成接收终端的位置信息; 判断模块 54, 连接至第二接收模块 52, 设置成根据上述位置信息判断终端是否处于预定网络的目标范围内; 控制模块 56, 连接至判断单元 54, 设置成根据判断结果控制上述终端接入预定网络。

图 6 是根据本发明实施例的第二种接入网络的处理装置的一种可选实施例的结构框图, 如图 6 所示, 该控制模块 56 包括第一发送单元 62 和/或第二发送单元 64, 下面对该控制模块 56 进行说明。

- 25 第一发送单元 62, 设置成当上述判断结果为终端位于目标范围内时, 向终端发送令牌信息, 其中, 该令牌信息用于终端通过路由器接入预定网络; 第二发送单元 64, 设置成当上述判断结果为终端位于目标范围外时, 向终端发送拒绝该终端接入预定网络的信息。

图 7 是根据本发明实施例的第二种接入网络的处理装置的另一种的可选实施例的结构框图，如图 7 所示，该装置除包括图 6 所示的所有单元外，还包括接收单元 72、验证单元 74 和第三发送单元 76，下面对该控制模块 56 进行说明。

5 接收单元 72，连接至第一发送单元 62，设置成接收路由器发送的预定令牌信息，其中，该预定令牌信息为路由器在接收到终端发送的预定令牌信息后发送的；验证单元 74，连接至接收单元 72，设置成验证上述预定令牌信息与发送给终端的令牌信息是否一致；第三发送单元 76，连接至验证单元 74，设置成若上述验证单元的验证结果为一一致，将允许终端接入预定网络的允许
10 信息发送给路由器。

下面对整体流程进行说明。该整体流程涉及三种设备：终端设备，无线路由器和/或无线 AC 控制器（以下简称为无线路由器/无线 AC 控制器，或者简称为路由器/AC 控制器），认证服务器。

其中终端设备以目前最为普遍的安卓手机为例，安卓系统提供了现成的
15 用于获取终端在所处位置的 Wi-Fi 信号、蓝牙信号、基站信号的接口。可用于描述终端的位置信息非常多，为简化描述，本实施例仅以 Wi-Fi 信号提供的终端的位置信息为例，实际实施时并不局限于此。

无线路由器/无线 AC 控制器 (Wireless Access Point Controller)：对于家庭用户，AC 控制器即为无线路由器，一般采用常见的 linux 系统，内核版本
20 2.4 以上，其自带的 iptables 程序可以快捷地实现本申请方案。

认证服务器：存储位置样本库，并提供接口用于验证位置是否满足条件。在 AC 控制器性能较强的情况下，AC 控制器可以与认证服务器合一。

该流程包括如下步骤：

a 终端通过 Wi-Fi 接入网络并发出访问任意某个地址的请求；
25 b 路由器根据从终端收到的请求中的报文源 MAC 地址（即终端的 MAC 地址），判断所述终端是否已认证，若未认证，则将该请求重定向至认证服务器，并且在重定向的地址中附加上路由器的标识，用于接收令牌 token 的接口地址等信息。

c 认证服务器向终端返回一个认证页面，该认证页面用于终端向认证服务器发送位置指纹信息。

d 终端向认证服务器发送收集到的相关位置指纹信息：位置指纹信息可以包含多个 Wi-Fi 信号携带的 Wi-Fi 信号发射端的 MAC 地址和多个 Wi-Fi 信号的信号强度，或者也可以包含蓝牙信号携带的蓝牙信号发射端的地址以及蓝牙信号的信号强度，当然，该位置指纹信息也可以是其他的信息或信息之间的组合。

e 认证服务器根据终端发送的位置指纹信息判断终端是否在网络提供者限定的目标范围内，若终端在限定的目标范围内，则向终端发送令牌 token，并将该终端的请求重定向至路由器。

f 路由器将收到的令牌 token 以及路由器的标识发送到认证服务器进行验证，如验证成功，则将该终端的 MAC 地址加入允许访问网络的列表，允许该终端通过路由器访问网络；

g 客户端（即终端）定期向认证服务器反馈其收集到的位置指纹信息、令牌 token、以及终端的 MAC 地址等信息，认证服务器根据这些信息判断该终端是否可继续访问网络，同时路由器定期向认证服务器询问 MAC 是否处于可用状态，若不可用，将该 MAC 重新设置为一旦访问网络就重定向至认证页面。

20 实施例一：

本实施例将描述 AC 控制器与认证服务器分离，即处于不同设备的情况。

本实施例假定实施的环境下已有既有的室内地图及其位置指纹样本库。

AC 控制器的初始配置：保存一个 MAC 地址列表，该 MAC 地址列表设置成若从终端收到报文源 MAC 地址在 MAC 地址列表中，允许该终端访问网络；而若从终端收到报文源 MAC 地址不在 MAC 地址列表中，将报文重定向至认证服务器，实现方法可首先利用 iptables 规则，将该报文做目的网络地址转换（Destination Network Address Translation，简称为 DNAT）跳转至本地处理进程，再由本地处理进程将该请求重定向至认证服务器，并且在

重定向的链接中携带接入控制器 (Access Controller, 简称为 AC) 的相关信息。为 MAC 地址列表中的 MAC 地址设置有效期, 为了方便管理, 对网络管理员或常用客户的终端的 MAC 地址, 可设置为无限期永久访问, 即不参与基于位置的认证; 对于普通的 MAC 地址, 设置生命周期为相对较短的时间, 比如 5 分钟。

图 8 是根据本发明实施例一的路由器/AC 控制器与认证服务器分离情况下的交互流程图, 如图 8 所示, 该流程包括如下步骤:

步骤 S802, 终端连入 Wi-Fi 网络后发出任意的一个 HTTP 请求。

步骤 S804, AC 控制器判断报文源 MAC 是否在允许访问网络的 MAC 地址列表中, 若该 MAC 不在允许访问网络的 MAC 地址列表之中, 即未经过认证, 则向终端返回包括重定向的地址的响应, 所述包括重定向的地址的响应可为: 超文本传输协议 (Hyper Text Transfer Protocol, 简称为 HTTP) 状态码, 以及 AC 控制器的相关信息: 包括 AC 控制器的标识 (本实施例中以 AC 控制器的 MAC 地址作为标识), AC 控制器接收令牌的地址 (端口的 IP 地址和端口)、终端的 MAC 地址信息等, 例如, 最终终端将访问的目的地址为:

http://auth-server/index&&gwid=00:d0:d0:00:00:01&&gwip=192.168.1.1&&gwport=8080&&client=00:d0:d0:00:00:0A。

步骤 S806, 终端向认证服务器发送请求。

步骤 S808, 认证服务器收到终端的请求后, 提取步骤 S804 中终端传来的参数并存储终端 MAC 与 AC 控制器信息的对应关系, 向终端返回包含一个隐含的 form 表单的页面, 该 form 表单的目的地址例如: http://auth-server/auth, 用于终端向认证服务器发送其当前 Wi-Fi 信号携带的位置指纹信息, 类似于基于短信的上网认证时被输入短信验证码的 form 表单, 而本方案基于位置认证, 无需用户手工输入数据, 由终端自行采集数据。

步骤 S810, 客户端 (即, 上述的终端) 加载认证服务器返回的 web 页面后, 将收集到的 Wi-Fi 信号携带的位置指纹信息发送到步骤 S804 中向终端返回的包括重定向的地址的响应中的地址 http://auth-server/auth: 用 JSON 格式 (JavaScript Object Notation, 是一种轻量级的数据交换格式) 描述如下:

```

{
  "mac": "00:d0:d0:00:00:0A",
  "wifi": [{
    "mac": "00:d0:d0:00:01", "rssi": 31
  },
    { "mac": "00:d0:d0:00:02", "rssi": 42},
    { "mac": "00:d0:d0:00:03", "rssi": 53
  }]
}

```

其中 rssi 为 Wi-Fi 信号的信号强度，一般表示为负值，单位为 dbm，值越小代表信号强度越大，为了简洁，此处用正数表示，省略了单位。

- 步骤 S812，认证服务器对收到的 Wi-Fi 信号携带的位置指纹信息进行判断，若满足预设约束条件，则根据终端的 MAC 查询出其对应的网关信息，生成重定向地址发送到客户端，在重定向的地址中包含有用于表示验证成功的令牌 token 以及生命周期，如 `http://192.168.1.1:8080&&token=ezakl02s&&lifetime=300`，其中 300 为该令牌 token 的生命周期，AC 控制器应在 300 秒之后向服务器询问是否仍然有效。
- 10 判断 Wi-Fi 等信号携带的位置指纹信息表征的位置是否在区域内的方法：首先根据 Wi-Fi 信号携带的位置指纹信息查找到最匹配的位置，然后通过射线法判断是否在预设的多边形（区域边缘形成的点连线形成一个多边形）：从被判断的点向 x 轴发射一条射线，如果射线与多边形的边有偶数次相交，那么点不在多边形内；奇数次相交，那么点在多边形内。
- 15 步骤 S814，终端将收到的令牌 token 发送给 AC 控制器。

步骤 S816，AC 控制器从终端收到重定向的请求后，将终端的 MAC 地址、AC 控制器标识、令牌 token 发送至认证服务器验证进行验证，用 JSON 格式描述如下：

```
{
  "gwmac": "00:d0:d0:00:00:0B"    ,
  "clentmac": "00:d0:d0:00:00:0A"  ",
  "token": "ezakl02s",
  "lifetime" : 300
}
```

步骤 S818 , 认证服务器检查终端的 MAC 地址和令牌 token 、 AC 控制器标识等是否匹配。认证服务器向 AC 控制器返回认证结果 : 0 为匹配 , -1 为匹配失败。

5 步骤 S820 , 如果验证匹配 , AC 控制器将终端的 MAC 地址加入允许访问网络的列表 , 且将步骤 S816 的重定向的请求重定向至认证服务器的心跳页面 , 例如 `http :// auth-server/alive` 。

步骤 S822 , 终端在使用网络过程中 , 一直保持心跳页面开启 , 定期向认证服务器反馈其当前 Wi-Fi 信号携带的位置指纹信息 , 以及令牌 token。

```
{
  "mac": "00:d0:d0:00:00:0A",
  "wifi": [{ "mac": "00:d0:d0:00:01", "rssi": 31    },
             { "mac": "00:d0:d0:00:02", "rssi": 42},
             { "mac": "00:d0:d0:00:03", "rssi": 53    } ],
  "token" : "ezakl02s"
}
```

10 心跳页面处理 : 若 Wi-Fi 信号携带的位置指纹信息表征的位置不在区域内 , 则认证服务器将该 MAC 地址对应的记录置为非法状态 ; 若 Wi-Fi 信号携带的位置指纹信息表征的位置在区域内 , 则更新其生命周期。由于终端很可能处于移动状态 , 所以当发现其在区域外 , 并不立即停止 , 而是等待 AC 控制器去查询某 MAC 地址是否可以继续使用网络。

步骤 S824 AC 控制器定期向认证服务器询问 MAC 列表中的 MAC 是否到期，若到期，则将其从 MAC 列表中删除。

步骤 S826，认证服务器向 AC 控制器返回查询结果。

在整个认证过程中，终端总是客户端的角色，无需提供对外的服务接口；

- 5 AC 控制器需要提供一个接口，用于接收终端发送的令牌 token 验证请求；
认证服务器需要提供三个接口：

接口 1：用于接收未经认证的终端上线后被重定向的认证首页
`http://auth-server/index;`

接口 2：接收终端发起的验证请求 `http://auth-server/auth;`

- 10 接口 3：心跳接口用于接收 AC 控制器发起的、查询终端的 MAC 地址是否已经失效的请求：`http://auth-server/alive`。

实施例二：

- 本实施例描述 AC 控制器与认证服务器在同一个设备中的方案，即在处
15 理性能较强且具备一定存储能力的无线路由器上实现，操作系统可以 Linux
系统，或者基于 openwrt（一种 Linux 系统）进行修改，这种方案中 AC 控制
器与认证服务器之间的交互会更加简单，下面描述中统称为路由器。

- 在本实施例中假定没有既有的室内定位系统，也即没有室内地图，也就
没有既有的位置指纹库，需要重新建立简化的位置样本库：通过携带能够通
20 过 Wi-Fi 等方式访问网络的移动终端在设定的区域内外行进，在行进的过程
中收集各位置的 Wi-Fi 信号/蓝牙信号等的标识和信息，每个位置都将会被标
注为区域内或外，为了保证定位的效果，在区域边缘进行密集覆盖地标注
Wi-Fi 信号/蓝牙信号等的标记和信息，并且在区域内和区域外以距离稍大的
间隔标注 Wi-Fi 信号/蓝牙信号等的标记和信息，以保证匹配效果。图 9 是根
25 据本发明实施例的样本库和被验证点分别位于区域内和区域外的示意图。

图 10 是根据本发明实施例二的路由器/AC 控制器与认证服务器在同一个设备中的情况下的交互流程图，如图 10 所示，该流程包括如下步骤：

在路由器上通过 iptables 程序初始设置访问规则 :保存一个 MAC 地址列表 , 若从终端收到的报文源 MAC 地址在 MAC 地址列表中 , 则可以正常访问网络 , 而若从终端收到的报文源 MAC 地址不在 MAC 地址列表中 , 将报文重定向至认证服务器 , 运行认证进程 , 本实施例中 , 因认证服务器和 AC 控制器是同一个设备 , 所以认证服务器的地址可用本地环回地址 : 127.0.0.1:8080. 与实施例一相同的是 , 为方便管理 , 为 MAC 地址列表中的 MAC 地址分别设置生命周期 , 允许特殊地址可以不经过认证就能一直访问网络。

步骤 S1002 , 终端连接网络后发出任意的 HTTP 请求 , 例如 , 访问网址为 www.xxx.com 的网页。

步骤 S1004, 路由器根据终端 MAC 地址判断其是否已经过认证 , 若判断终端没有经过认证 , 则将报文重定向至本地进程 127.0.0.1:8080 以进行处理 , 在该进程中向终端返回包含一个隐含的 form 表单的页面 , 该 form 表单的目的地址为 http:// 127.0.0.1 :8080/auth, 用于终端向认证服务器发送其当前位置 , 该页面将一直处于活动状态 , 并且定期自动向认证服务器发送位置信息。

步骤 S1006, 客户端将收集到的 Wi-Fi 信号携带的指纹信息发送到步骤 S1004 中的目的地址 , 用 JSON 格式描述如下 :

```
{
  "mac": "00:d0:d0:00:00:0A",
  "wifi": [{
    "mac": "00:d0:d0:00:01", "rssi": 31
  },
    { "mac": "00:d0:d0:00:02", "rssi": 42 },
    { "mac": "00:d0:d0:00:03", "rssi": 53
  }]
}
```

路由器将收到的 MAC 地址和信号强度等与样本库进行比较 , 以进行判断 , 判断的方法有多种 , 比如欧式距离方法 , 极大似然概率法 , 支持向量机算法等等 , 如果在样本库中查找到的最为匹配的条目属于区域内 , 则认为该

位置满足预设约束条件，将该 MAC 地址加入前述 MAC 地址列表，更新其生命周期；如果不满足预设约束条件，则从 MAC 地址列表中将该 MAC 地址去除。

步骤 S1008，路由器定期扫描 MAC 地址列表，将生命周期已经结束的 MAC 地址删除，使其下一次访问网络时，继续被重定向至认证页面。

在上述实施例中，由于 AC 控制器和认证服务器都在路由器中实现，终端和路由器之间需要两个接口：一是当未经认证的终端接入后被跳转到的重定向的地址；二是验证接口，在具体实施过程中，可以使用同一个地址，入口使用 get 指令动作，验证则使用 post 指令动作进行区分。

需要说明的是，上述各个模块是可以通过软件或硬件来实现的，对于后者，可以通过以下方式实现，但不限于此：上述模块均位于同一处理器中；或者，上述模块分别位于多个处理器中。

本发明的实施例还提供了一种存储介质。可选地，在本实施例中，上述存储介质可以被设置为存储用于执行以下步骤的程序代码：

S1，向认证服务器发送终端的位置信息；

S2，接收该认证服务器根据位置信息返回的判断结果，其中该判断结果用于标识终端是否处于预定网络的目标范围内；

S3，根据判断结果确定是否允许终端接入上述预定网络。

可选地，存储介质还被设置为存储用于执行以下步骤的程序代码：

S1，接收终端的位置信息；

S2，根据该位置信息判断终端是否处于预定网络的目标范围内；

S3，根据判断结果控制终端接入上述预定网络。

可选地，在本实施例中，上述存储介质可以包括但不限于：U 盘、只读存储器 (Read-Only Memory，简称为 ROM)、随机存取存储器 (Random Access Memory，简称为 RAM)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

可选地，本实施例中的具体示例可以参考上述实施例及可选实施方式中

所描述的示例，本实施例在此不再赘述。

显然，本领域的技术人员应该明白，上述的本申请的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，并且在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本申请不限制于任何特定的硬件和软件结合。

以上所述仅为本申请的可选实施例而已，并不用于限制本申请，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件（例如处理器）完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块/单元可以采用硬件的形式实现，例如通过集成电路来实现其相应功能，也可以采用软件功能模块的形式实现，例如通过处理器执行存储于存储器中的程序/指令来实现其相应功能。本发明实施例不限制于任何特定形式的硬件和软件的结合。

工业实用性

通过本申请的方案，采用向认证服务器发送终端的位置信息；接收所述认证服务器根据所述位置信息返回的判断结果，其中所述判断结果用于标识所述终端是否处于预定网络的目标范围内；根据所述判断结果确定是否允许所述终端接入所述预定网络，解决了相关技术中存在的网络接入控制效率低的问题，进而达到了提高网络接入控制效率的效果。

权 利 要 求 书

1、一种接入网络的处理方法，包括：

向认证服务器发送终端的位置信息；

5 接收所述认证服务器根据所述位置信息返回的判断结果，其中，所述判断结果用于标识所述终端是否处于预定网络的目标范围内；

根据所述判断结果确定是否允许所述终端接入所述预定网络。

2、根据权利要求1所述的方法，其中，所述位置信息包括以下信息至少之一：

10 所述终端检测到的Wi-Fi信号携带的Wi-Fi信号发射端的媒体接入控制MAC地址和所述终端检测到的Wi-Fi信号的信号强度、所述终端检测到的蓝牙信号携带的蓝牙信号发射端的地址和所述终端检测到的蓝牙信号的信号强度。

3、根据权利要求1所述的方法，其中，当所述判断结果为所述终端处于所述目标范围内时，所述根据所述判断结果确定是否允许所述终端接入所述
15 预定网络的步骤包括：

获取所述判断结果中携带的令牌信息；

依据所述令牌信息通过路由器接入所述预定网络。

4、一种接入网络的处理方法，包括：

接收终端的位置信息；

20 根据所述位置信息判断所述终端是否处于预定网络的目标范围内；

根据判断结果控制所述终端接入所述预定网络。

5、根据权利要求4所述的方法，其中，所述根据所述判断结果控制所述终端接入所述预定网络的步骤包括：

25 当所述判断结果为所述终端位于所述目标范围内时，向所述终端发送令牌信息，其中，所述令牌信息用于所述终端通过路由器接入所述预定网络；

当所述判断结果为所述终端位于所述目标范围外时，向所述终端发送拒绝所述终端接入所述预定网络的信息。

6、根据权利要求5所述的方法，所述当所述判断结果为所述终端位于所述目标范围内时，向所述终端发送所述令牌信息的步骤之后，所述处理方法还包括：

5 接收所述路由器发送的预定令牌信息，其中，所述预定令牌信息为所述路由器在接收到终端发送的所述预定令牌信息后发送的；

验证所述预定令牌信息与发送给所述终端的令牌信息是否一致；

若验证结果为一一致，将允许所述终端接入所述预定网络的允许信息发送给所述路由器。

7、一种接入网络的处理装置，包括：

10 发送模块，设置成向认证服务器发送终端的位置信息；

第一接收模块，设置成接收所述认证服务器根据所述位置信息返回的判断结果，其中所述判断结果用于标识所述终端是否处于预定网络的目标范围内；

15 处理模块，设置成根据所述判断结果确定是否允许所述终端接入所述预定网络。

8、根据权利要求7所述的装置，其中，所述位置信息包括以下信息至少之一：

20 所述终端检测到的Wi-Fi信号携带的Wi-Fi信号发射端的媒体接入控制MAC地址和所述终端检测到的Wi-Fi信号的信号强度、所述终端检测到的蓝牙信号携带的蓝牙信号发射端的地址和所述终端检测到的蓝牙信号的信号强度。

9、根据权利要求7所述的装置，其中，所述处理模块包括：

获取单元，设置成当所述判断结果为所述终端处于所述目标范围内时，获取所述判断结果中携带的令牌信息；

25 接入单元，设置成依据所述令牌信息通过路由器接入所述预定网络。

10、一种接入网络的处理装置，包括：

第二接收模块，设置成接收终端的位置信息；

判断模块，设置成根据所述位置信息判断所述终端是否处于预定网络的目标范围内；

控制模块，设置成根据判断结果控制所述终端接入所述预定网络。

11、根据权利要求 10 所述的装置，其中，所述控制模块包括：

5 第一发送单元，设置成当所述判断结果为所述终端位于所述目标范围内时，向所述终端发送令牌信息，其中，所述令牌信息用于所述终端通过路由器接入所述预定网络；

第二发送单元，设置成当所述判断结果为所述终端位于所述目标范围外时，向所述终端发送拒绝所述终端接入所述预定网络的信息。

10 12、根据权利要求 11 所述的装置，所述处理装置还包括：

接收单元，设置成接收所述路由器发送的预定令牌信息，其中，所述预定令牌信息为所述路由器在接收到终端发送的所述预定令牌信息后发送的；

验证单元，设置成验证所述预定令牌信息与发送给所述终端的令牌信息是否一致；

15 第三发送单元，设置成若所述验证单元的验证结果为一一致，将允许所述终端接入所述预定网络的允许信息发送给所述路由器。

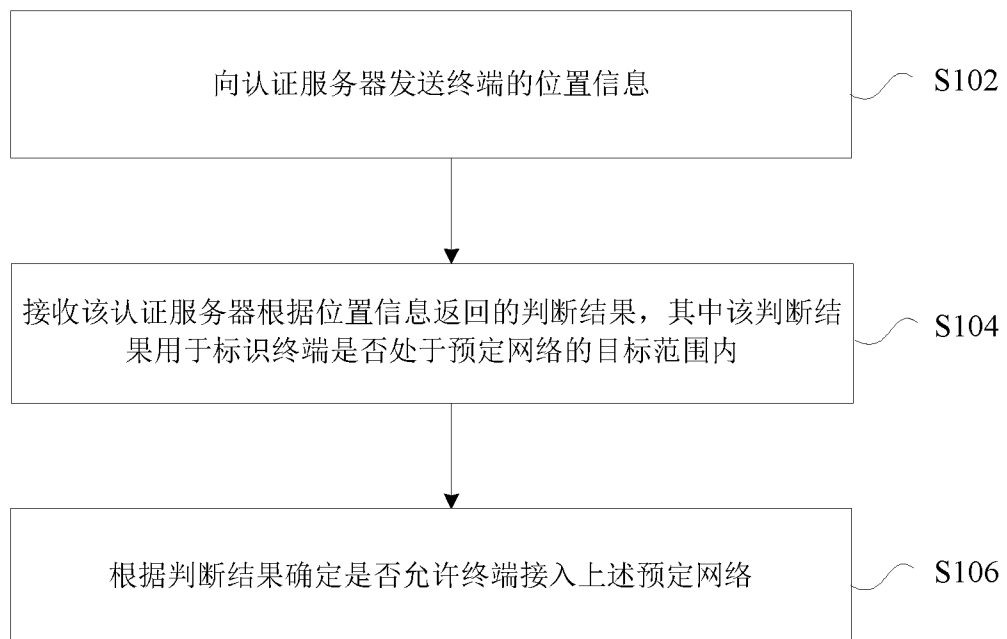


图 1

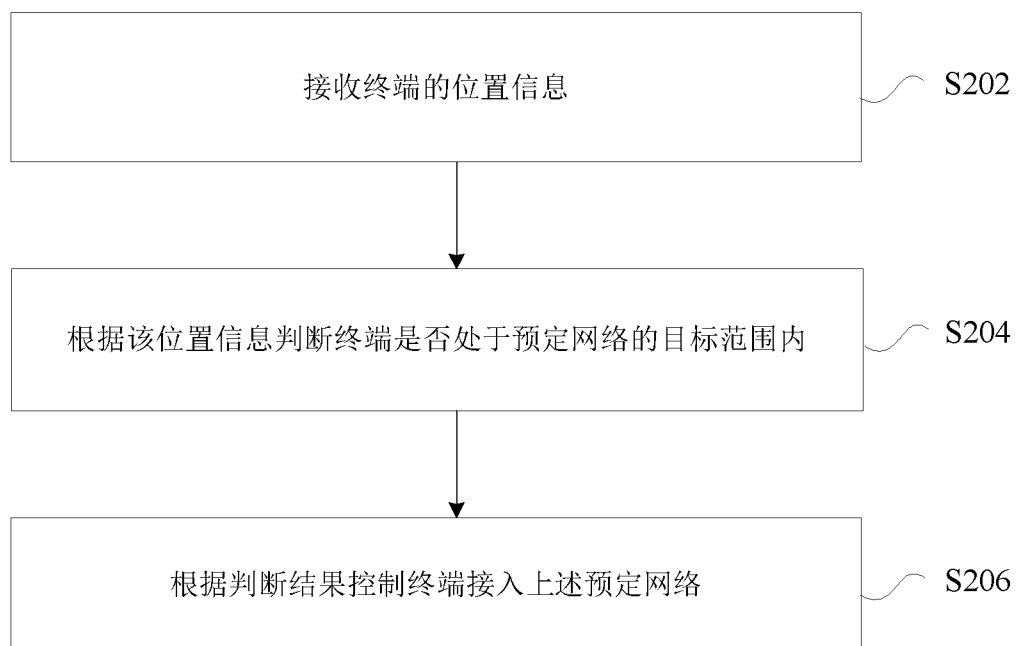


图 2

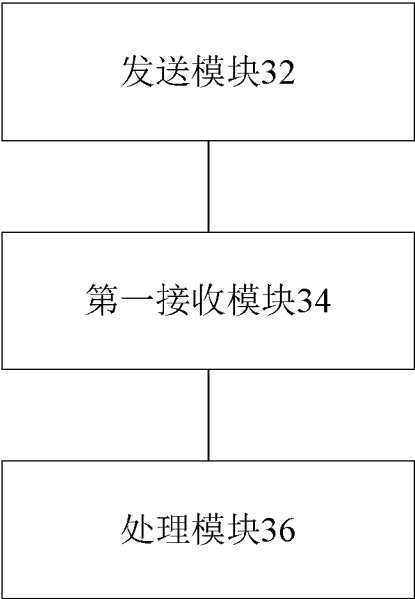


图 3

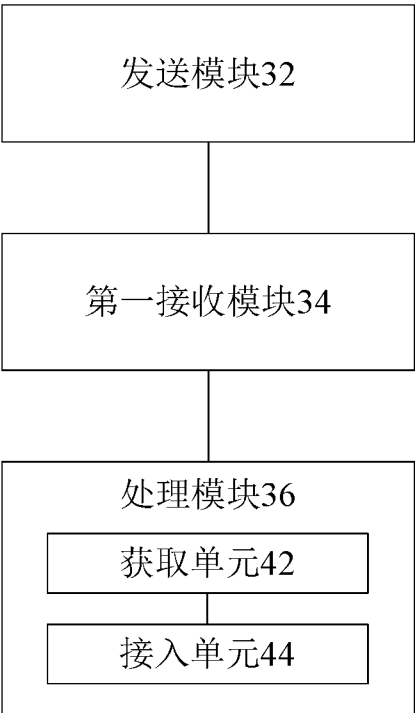


图 4

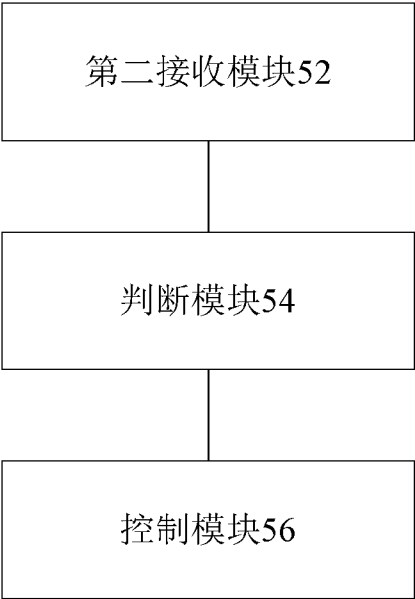


图 5

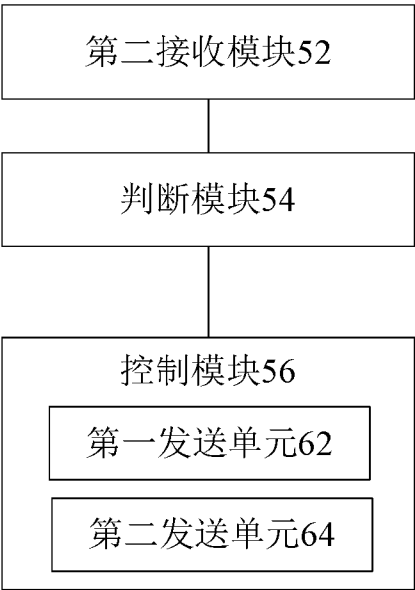


图 6

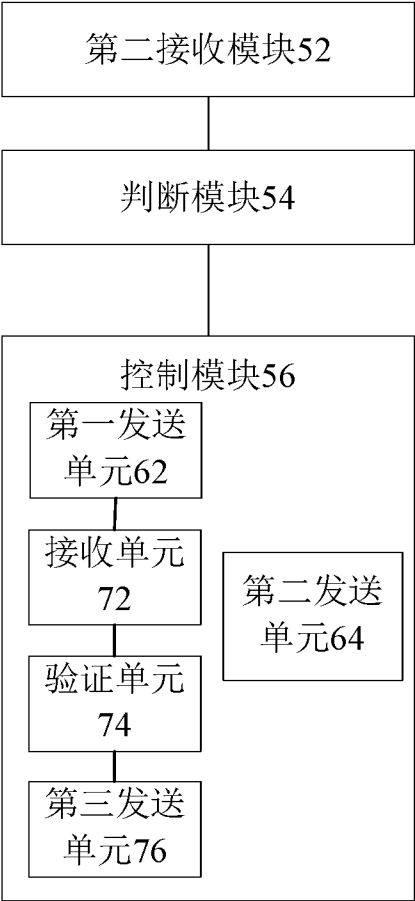


图 7

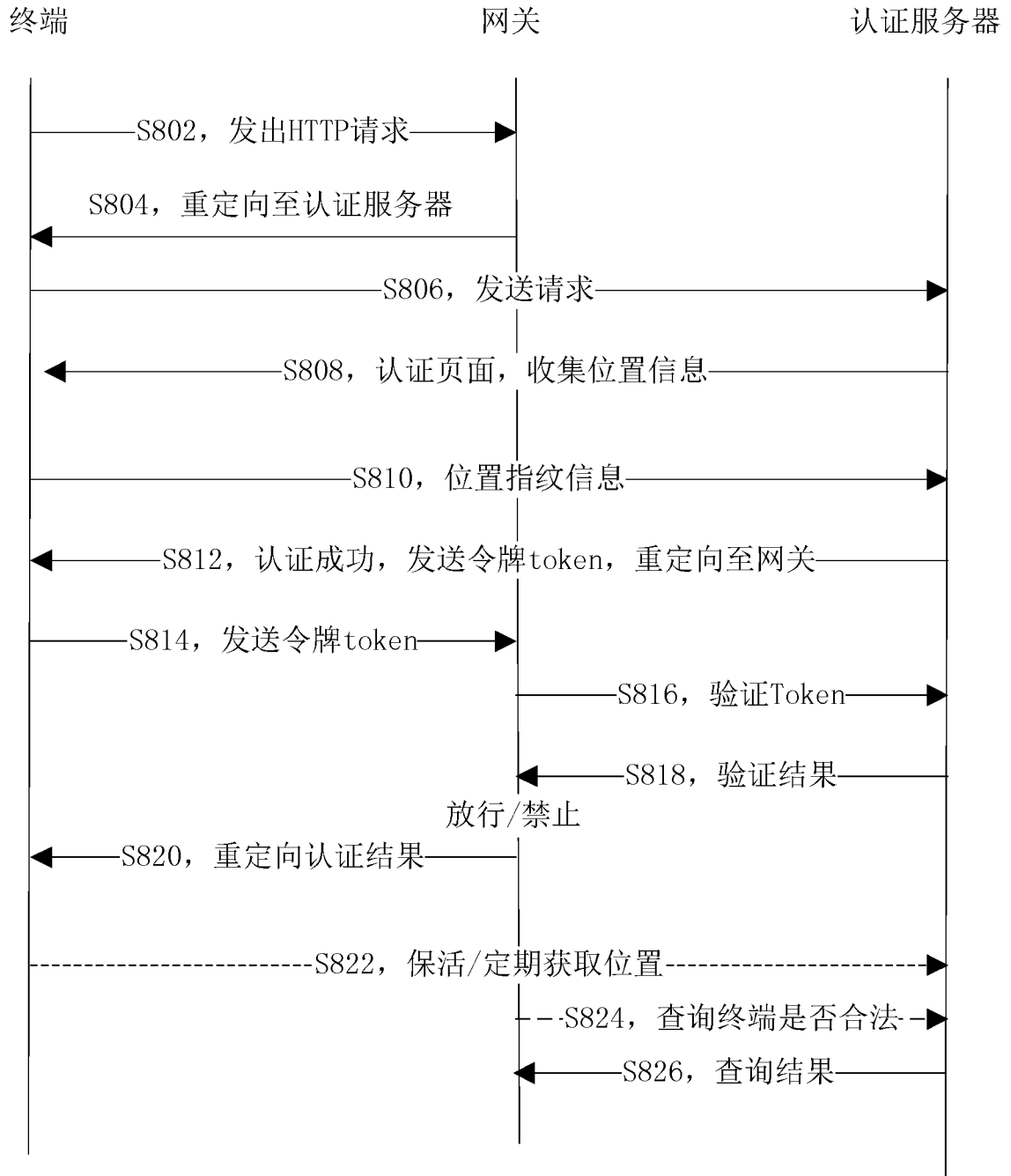


图 8

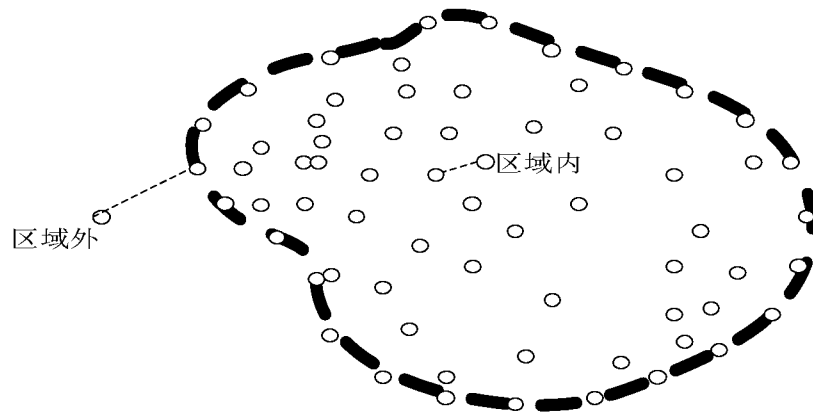


图 9

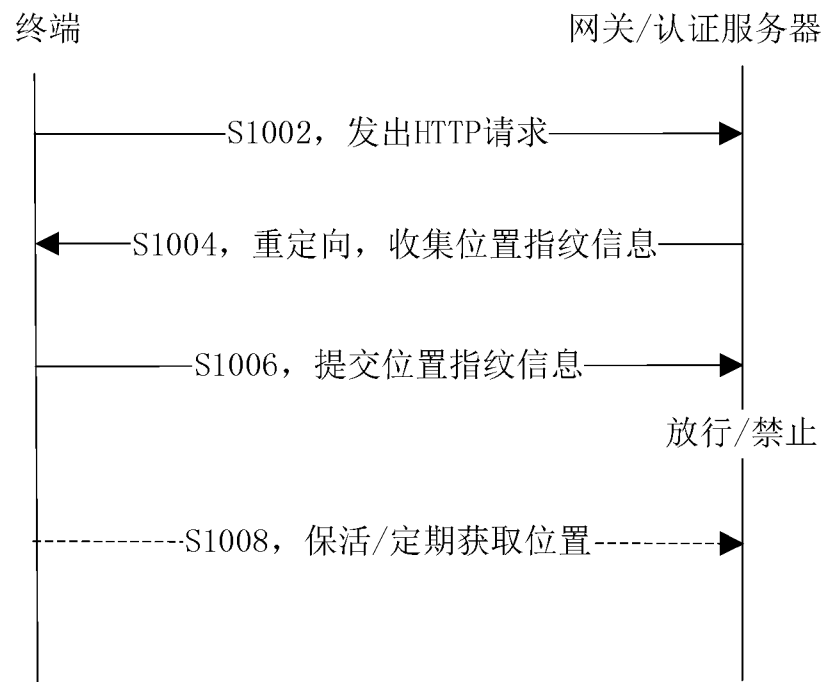


图 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/082354

A. CLASSIFICATION OF SUBJECT MATTER

H04W 48/04 (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; H04Q

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)

WPI; EPODOC; CNKI; CNPAT: limit, authority, terminal, access, access point, network, admission, admit, approve, reject, control, allow, location, distance, signal, strength, range, scope

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
x	CN 104159271 A (HUAWEI TECHNOLOGIES CO., LTD.), 19 November 2014 (19.11.2014), description, paragraphs 0108-0140, and figures 8-9	1-12
x	CN 104581830 A (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.), 29 April 2015 (29.04.2015), description, paragraphs 0038-0047, and figure 1	1-12
x	CN 1673925 A (BROADCOM CORPORATION), 28 September 2005 (28.09.2005), description, pages 7-10, and figures 2-4	1-12
A	EP 2648126 A I (LG CNS CO., LTD.), 09 October 2013 (09.10.2013), the whole document	1-12

II Further documents are listed in the continuation of Box C. ☒ See patent family annex.

<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"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)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>		<p>"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</p> <p>"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</p> <p>"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</p> <p>"&" document member of the same patent family</p>
Date of the actual completion of the international search 14 July 2016 (14.07.2016)	Date of mailing of the international search report 18 August 2016 (18.08.2016)	
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 LIU, Qingfeng Telephone No.: (86-10) 62413279	

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/082354

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104159271 A	19 November 2014	None	
CN 104581830 A	29 April 2015	None	
CN 1673925 A	28 September 2005	EP 1580641 A 2	28 September 2005
		US 2005213519 A I	29 September 2005
		US 2008248812 A I	09 October 2008
		US 2006020960 A I	26 January 2006
		TW 200635313 A	01 October 2006
EP 2648126 A I	09 October 2013	KR 20130113293 A	15 October 2013
		CN 103368939 A	23 October 2013
		US 2014215563 A I	31 July 2014

A. 主题的分类 H04W 48/04 (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 ; H04Q 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)) WPI ; EPODOC ; CNKI ; CNPAT : 终端, 接入, 访问, 网络, 接入点, 限制, 控制, 权限, 允许, 位置, 距离, 信号, 强度, 范围, terminal , access, access point, network, admission, admit, approve, reject, control , allow, location, distance, signal , strength, range, scope																	
c. 相关文件 <table border="1"> <thead> <tr> <th>类 型 *</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 104159271 A (华为技术有限公司) 2014 年 11 月 19 日 (2014 - 11 - 19) 说明书第 0108-0140 段, 图 8-9</td> <td>1-12</td> </tr> <tr> <td>X</td> <td>CN 104581830 A (大唐移动通信设备有限公司) 2015 年 4 月 29 日 (2015 - 04 - 29) 说明书第 0038-0047 段, 图 1</td> <td>1-12</td> </tr> <tr> <td>X</td> <td>CN 1673925 A (美国博通公司) 2005 年 9 月 28 日 (2005 - 09 - 28) 说明书第 7-10 页, 图 2-4</td> <td>1-12</td> </tr> <tr> <td>A</td> <td>EP 2648126 A1 (LG CNS CO., LTD.) 2013 年 10 月 9 日 (2013 - 10 - 09) 全文</td> <td>1-12</td> </tr> </tbody> </table>			类 型 *	引用文件, 必要时, 指明相关段落	相关的权利要求	X	CN 104159271 A (华为技术有限公司) 2014 年 11 月 19 日 (2014 - 11 - 19) 说明书第 0108-0140 段, 图 8-9	1-12	X	CN 104581830 A (大唐移动通信设备有限公司) 2015 年 4 月 29 日 (2015 - 04 - 29) 说明书第 0038-0047 段, 图 1	1-12	X	CN 1673925 A (美国博通公司) 2005 年 9 月 28 日 (2005 - 09 - 28) 说明书第 7-10 页, 图 2-4	1-12	A	EP 2648126 A1 (LG CNS CO., LTD.) 2013 年 10 月 9 日 (2013 - 10 - 09) 全文	1-12
类 型 *	引用文件, 必要时, 指明相关段落	相关的权利要求															
X	CN 104159271 A (华为技术有限公司) 2014 年 11 月 19 日 (2014 - 11 - 19) 说明书第 0108-0140 段, 图 8-9	1-12															
X	CN 104581830 A (大唐移动通信设备有限公司) 2015 年 4 月 29 日 (2015 - 04 - 29) 说明书第 0038-0047 段, 图 1	1-12															
X	CN 1673925 A (美国博通公司) 2005 年 9 月 28 日 (2005 - 09 - 28) 说明书第 7-10 页, 图 2-4	1-12															
A	EP 2648126 A1 (LG CNS CO., LTD.) 2013 年 10 月 9 日 (2013 - 10 - 09) 全文	1-12															
<input type="checkbox"/> 其余文件在 c 栏的续页中列出。 <input checked="" type="checkbox"/> 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 2016 年 7 月 14 日	国际检索报告邮寄日期 2016 年 8 月 18 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 刘庆峰 电话号码 (86-10) 62413279																

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/082354

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	104159271	A	2014 年 11 月 19 日	无	
CN	104581830	A	2015 年 4 月 29 日	无	
CN	1673925	A	2005 年 9 月 28 日	EP	1580641 A2 2005 年 9 月 28 日
				US	2005213519 AI 2005 年 9 月 29 日
				US	2008248812 AI 2008 年 10 月 9 日
				US	2006020960 AI 2006 年 1 月 26 日
				TW	200635313 A 2006 年 10 月 1 日
EP	2648126	AI	2013 年 10 月 9 日	KR	201301 13293 A 2013 年 10 月 15 日
				CN	103368939 A 2013 年 10 月 23 日
				US	2014215563 AI 2014 年 7 月 31 日