(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 10 月 27 日 (27.10.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/169502 A1

(51) 国际专利分类号:
H04W 74/00 (2009.01)

(21) 国际申请号: PCT/CN2016/079953

(22) 国际申请日: 2016 年 4 月 22 日 (22.04.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510202082.2 2015 年 4 月 24 日 (24.04.2015) CN

(71) 申请人: **维沃移动通信有限公司 (VIVO MOBILE COMMUNICATION CO.,LTD.)** [CN/CN]; 中国广东省东莞市长安镇乌沙步步高大道 283 号, Guangdong 523860 (CN)。

(72) 发明人: **齐好鑫 (QI, Haoxin)**; 中国广东省东莞市长安镇乌沙步步高大道 283 号, Guangdong 523860 (CN)。

(74) 代理人: **北京银龙知识产权代理有限公司 (DRAGON INTELLECTUAL PROPERTY LAW FIRM)**; 中国北京市海淀区西直门北大街 32 号院枫蓝国际中心 2 号楼 10 层, Beijing 100082 (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: WIRELESS CONNECTION AUTHENTICATION METHOD AND DEVICE

(54) 发明名称 : 无线连接认证方法和装置

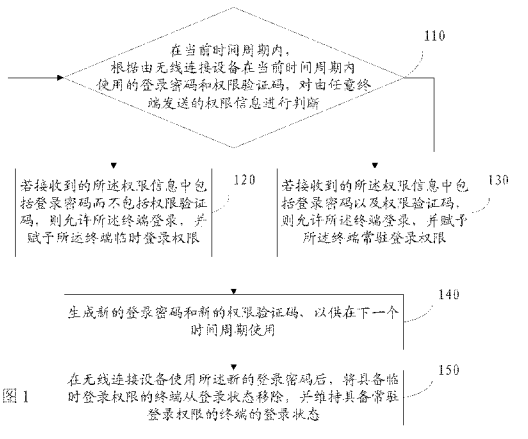


图 1

110 WITHIN A CURRENT TIME PERIOD, JUDGING AUTHORITY INFORMATION SENT BY ANY TERMINAL ACCORDING TO A LOGIN PASSWORD AND AN AUTHORITY VERIFICATION CODE USED BY A WIRELESS CONNECTION DEVICE WITHIN THE CURRENT TIME PERIOD
120 IF THE RECEIVED AUTHORITY INFORMATION INCLUDES THE LOGIN PASSWORD RATHER THAN THE AUTHORITY VERIFICATION CODE, ALLOWING THE TERMINAL TO LOG IN, AND ENDOWING THE TERMINAL WITH A TEMPORARY LOGIN AUTHORITY
130 IF THE RECEIVED AUTHORITY INFORMATION INCLUDES THE LOGIN PASSWORD AND THE AUTHORITY VERIFICATION CODE, ALLOWING THE TERMINAL TO LOG IN, AND ENDOWING THE TERMINAL WITH A PERMANENT LOGIN AUTHORITY
140 GENERATING A NEW LOGIN PASSWORD AND A NEW AUTHORITY VERIFICATION CODE, FOR USE IN THE NEXT TIME PERIOD
150 AFTER THE WIRELESS CONNECTION DEVICE USES THE NEW LOGIN PASSWORD, REMOVING THE TERMINAL WITH A TEMPORARY LOGIN AUTHORITY FROM A LOGIN STATE, AND MAINTAINING THE LOGIN STATE OF THE TERMINAL WITH A PERMANENT LOGIN AUTHORITY

(57) **Abstract**: Disclosed are a wireless connection authentication method and device. The wireless connection authentication method comprises: within a current time period, if received authority information about a terminal includes a login password rather than an authority verification code, allowing the terminal to log in, and endowing the terminal with a temporary login authority; if the received authority information about the terminal includes the login password and the authority verification code, allowing the terminal to log in, and endowing the terminal with a permanent login authority; generating a new login password and a new authority verification code, for use in a next time period; and after a wireless connection device uses the new login password, removing the terminal with a temporary login authority from a login state, and maintaining the login state of the terminal with a permanent login authority.

(57) **摘要**: 本公开文本公开了一种无线连接认证方法和装置。所述无线连接认证方法包括在当前时间周期内，若接收到终端的权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并赋予所述终端临时登录权限；若接收到终端的权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并赋予所述终端常驻登录权限；生成新的登录密码和新的权限验证码，以供在下一个时间周期使用；在无线连接设备使用所述新的登录密码后，将具备临时登录权限的终端从登录状态移除，并维持具备常驻登录权限的终端的登录状态。

WO 2016/169502 A1

无线连接认证方法和装置

相关申请的交叉引用

本申请主张在 2015 年 4 月 24 日在中国提交的中国专利申请号 No. 201510202082.2 的优先权，其全部内容通过引用包含于此。

技术领域

本公开实施例涉及计算机技术领域，具体涉及一种无线连接认证方法和装置。

背景技术

随着技术的发展，很多终端设备可以通过无线连接以接入某个无线连接设备进行联网等操作，如移动终端通过 wifi（Wireless Fidelity，无线保真，又称 802.11b 标准，是一种可以将个人电脑、手持设备等终端以无线方式互相连接的技术）接入到路由器等无线连接设备，从而联入互联网。当然，很多终端设备也可以通过其他无线连接的方式接入其它无线连接设备，比如手机通过蓝牙等无线方式接入到其他终端，以传输文件等操作。

而且，为了无线网络或者说无线连接设备的安全，一般均会在无线连接设备侧设置登录密码。比如具备 wifi 功能的路由器，需要用户首先登录路由器后设置登录密码。此后对于未登录过该路由器的终端，如果要使用该路由器联网，则需要在终端中输入登录密码以连接到路由器，然后才能通过该路由器联网。又比如将手机的蓝牙功能设置登录密码，其他终端通过蓝牙连接该手机时则需要输入登录密码以连接。

但是传统的无线连接设备的密码管理方式，存在如下缺点：

1、密码设定后是固定的，暴利破解难度小，安全系数过低，无线信号容易被蹭。

2、使用不够灵活。比如某个用户 A 想暂时使用无线连接设备的无线(如 wifi、蓝牙等)，在无线连接设备的拥有者 B 提供该无线连接设备的登录密码后，用户 A 可将其终端联入上述无线连接设备。而当用户 A 的终端在使用完后，如果拥有者 B 不主动更改其无线连接设备中原来的登录密码,用户 A 的终端存在后续继续连接拥有者 B 的无线连接设备的可能性。但往往拥有者 B 很

少会主动更改其无线连接设备的登录密码，因为更改登录密码意味着拥有者 B 所有的连接该无线连接设备的终端都需要重新设置登录密码，才能连接到该无线连接设备。因而，对拥有者 B 来说，其无线连接设备的密码管理不够灵活、方便。

发明内容

鉴于上述问题，提出了本公开实施例以便提供一种克服上述问题的无线连接认证装置和相应的无线连接认证方法。

依据本公开实施例的一个方面，提供了一种无线连接认证方法，包括：

在当前时间周期内，根据无线连接设备在当前时间周期内使用的登录密码和权限验证码，对终端发送的权限信息进行判断；

若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并赋予所述终端临时登录权限；

若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并赋予所述终端常驻登录权限；

生成新的登录密码和新的权限验证码，以供在下一个时间周期使用；

在无线连接设备使用所述新的登录密码后，将具备临时登录权限的终端从登录状态移除，并维持具备常驻登录权限的终端的登录状态。

可选的，所述在当前时间周期内，根据无线连接设备在当前时间周期内使用的登录密码和权限验证码，对终端发送的权限信息进行判断之前的步骤，还包括：

根据收到的触发指令，获取所述登录密码以及权限验证码进行展示。

可选的，所述根据收到的触发指令，获取所述登录密码以及权限验证码进行展示的步骤，包括：

接收到第一次触发指令，获取所述登录密码进行展示；

如果在预定时间间隔内接收到第二次触发指令，则获取所述权限验证码进行展示。

可选的，所述当前时间周期内使用的权限验证码为将要在下一个时间周期内由无线连接设备使用的登录密码。

可选的，所述赋予所述终端临时登录权限的步骤，包括：

将所述终端的身份信息写入在无线连接设备中预置的临时用户表；

进一步的，所述将具备临时登录权限的终端从登录状态移除的步骤，包括：

清空所述临时用户表所记录的各终端的身份信息。

可选的，所述赋予所述终端常驻登录权限的步骤，包括：

将所述终端的身份信息写入在无线连接设备中预置的常驻用户表。

可选的，所述赋予所述终端临时登录权限的步骤，包括：

将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入临时用户标记；

进一步的，所述将具备临时登录权限的终端从登录状态移除的步骤，包括：

将所述用户表中临时用户标记对应的身份信息，从所述用户表中移除。

可选的，所述赋予所述终端常驻登录权限的步骤，包括：

将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入常驻用户标记。

可选的，所述将具备临时登录权限的终端从登录状态移除的步骤之前，包括：

对于各具备临时登录权限的终端，判断所述终端的登录时间长度是否大于等于阈值;所述登录时间长度为所述终端从登录时间点到当前时间周期结束的时间点之间的时间长度；

如果所述终端的登录时间长度大于等于阈值，则将具备临时登录权限的终端从登录状态移除；

如果所述终端的登录时间长度小于阈值，则不将具备临时登录权限的终端从登录状态移除。

依据本公开的另外一个方面，提供了一种无线连接认证装置，包括：

连接判断模块，适于在当前时间周期内，根据无线连接设备在当前时间周期内使用的登录密码和权限验证码，对终端发送的权限信息进行判断；

临时登录权限赋予模块，适于若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并赋予所述终端临时登录权限；

常驻登录权限赋予模块，适于若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并赋予所述终端常驻登录权限；

更新模块，适于生成新的登录密码和新的权限验证码，以供在下一个时间周期使用；

权限管理模块，适于在无线连接设备使用所述新的登录密码后，将具备临时登录权限的终端从登录状态移除，并维持具备常驻登录权限的终端的登录状态。

可选的，还包括：

展示模块，适于根据收到的触发指令，获取所述登录密码以及权限验证码进行展示。

可选的，所述展示模块包括：

第一展示子模块，适于如果接收到第一次触发指令，则获取所述登录密码进行展示；

第二展示子模块，适于如果在预定时间间隔内接收到第二次触发指令，则获取所述权限验证码进行展示。

可选的，所述当前时间周期内使用的权限验证码为将要在下一个时间周期内由无线连接设备使用的登录密码。

可选的，所述临时登录权限赋予模块包括：

第一临时登录权限赋予子模块，适于将所述终端的身份信息写入在无线连接设备中预置的临时用户表；

进一步的，所述权限管理模块包括：

临时用户表清空子模块，适于清空所述临时用户表所记录的各终端的身份信息。

可选的，所述常驻登录权限赋予模块包括：

第一常驻登录权限赋予子模块，适于将所述终端的身份信息写入在无线连接设备中预置的常驻用户表。

可选的，所述临时登录权限赋予模块包括：

临时用户添加子模块，适于将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入临时

用户标记；

进一步的，所述权限管理模块包括：

用户表临时移除子模块，适于将所述用户表中临时用户标记对应的身份信息，从所述用户表中移除。

可选的，所述常驻登录权限赋予模块包括：

常驻用户添加子模块，适于将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入常驻用户标记。

可选的，所述权限管理模块还包括：

临时用户时间判断子模块，适于在将具备临时登录权限的终端从登录状态移除之前，对于各具备临时登录权限的终端，判断所述终端的登录时间长度是否大于等于阈值;所述登录时间长度为所述终端从登录时间点到当前时间周期结束的时间点之间的时间长度；

临时用户移除子模块，适于如果所述终端的登录时间长度大于等于阈值，则将具备临时登录权限的终端从登录状态移除；

临时用户维持子模块，适于如果所述终端的登录时间长度小于阈值，则不将具备临时登录权限的终端从登录状态移除。

相对背景技术，本公开实施例存在以下优点：

1、本公开实施例对于无线连接设备的登录密码，根据时间周期进行自动更新，如此密码是随着时间的变化而变化的，每个密码只使用一段时间即变更为新的密码，无线连接设备被暴力破解的难度增大，并且无线信号也不容易被蹭。

另一方面，本公开实施例通过设置登录密码和权限验证码两种验证方式，将无线连接设备拥有者所认可的终端赋予常驻登录权限，如果某个用户想破解上述两种验证方式，以使其终端被赋予常驻登录权限，由于存在两个两种验证方式，无线连接设备被暴力破解难度更大。

2、对于无线连接设备的拥有者 B 来说，拥有者 B 可使其终端发送登录密码以及权限验证码到所述无线连接设备，以获得常驻登录权限；而对临时使用所述无线连接设备的用户 A 来说，拥有者 B 可以让用户 A 的终端只发送

登录密码以获得临时登录权限。由于无线连接设备可根据时间周期自动更新登录密码，在登录密码更新后，无线连接设备则自动断开该临时登录权限的终端的登录状态，使该终端不能继续登录无线连接设备。因此，无需拥有者 B 主动修改无线连接设备的登录密码，进一步的也无需所述拥有者在该登录密码自动修改后，再去修改自己的各个终端的登录密码，即可保证拥有者 B 的终端一直处于无线连接设备的登录状态。大大方便了无线连接设备的拥有者 B，无需其进行多余的操作，提高了无线连接设备的使用灵活性。无论登录密码如何更新，都不会影响常驻登录权限的终端的上网体验。

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

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，而并不认为是对本公开实施例的限制。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 示出了根据本公开实施例一个实施例的一种无线连接认证方法的流程示意图；

图 2 示出了根据本公开实施例一个实施例的另一种无线连接认证方法的流程示意图；

图 3 示出了根据本公开实施例一个实施例的另一种无线连接认证方法的流程示意图；

图 4 示出了根据本公开实施例一个实施例的另一种无线连接认证方法的流程示意图；

图 5 示出了根据本公开实施例一个实施例的另一种无线连接认证方法的流程示意图；

图 6 示出了根据本公开实施例一个实施例的一种无线连接认证装置的结构示意图；

图 7 示出了根据本公开实施例一个实施例的另一种无线连接认证装置的结构示意图；

图 8 示出了根据本公开实施例一个实施例的另一种无线连接认证装置的结构示意图；

图 9 示出了根据本公开实施例一个实施例的另一种无线连接认证装置的结构示意图；

图 10 示出了根据本公开实施例一个实施例的另一种无线连接认证装置的结构示意图；

图 11 示出了根据本公开实施例一个实施例的另一种无线路由器的结构示意图。

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。

本公开实施例的核心思想之一在于：本公开实施例的无线连接设备在每个时间周期中提供了登录密码和权限验证码。那么针对只发送了上述登录密码的终端，赋予临时登录权限；而针对同时输入了上述登录密码和权限验证码的终端，赋予常驻登录权限。在每次登录密码更新后，将具备临时登录权限的终端从无线连接设备的登录状态移除，而无论密码如何修改，可将具备常驻登录权限的终端，继续保持其对从无线连接设备的登录状态。如此，可以自动定期修改无线连接设备的登录密码，并且由于登录密码和权限验证码的两重验证方式，使无线连接设备被暴力破解的难度增大，并且无线信号也不容易被蹭。并且，对于需要长期的连接无线连接设备的终端，在登录密码修改后也可继续维持登录状态，无需该终端的使用者再次输入密码的操作，使无线连接设备使用更灵活。

在本公开实施例的实施例中，所述无线连接设备包括具备 wifi 功能、蓝牙、红外等的设备，比如路由器、手机、平板电脑、智能手环、笔记本电脑、带无线网卡的台式电脑等设备。所述终端可以是任意可发起无线连接的终端，

如手机、平板电脑、智能手环等。

在本公开实施例的实施例中，其应用环境可以如：

（1）路由器(可以理解为本公开实施例的无线连接设备)可以设置其 wifi 的登录密码，用户想要将其手机或者其他终端联入该路由器的 wifi 中。

（2）用户 A 将其已经联入网络的手机(可以理解为本公开实施例的无线连接设备)设置为 wifi 热点，并设置 wifi 的登录密码，用户 B 想要将其手机或者其他终端联入该手机对应的 wifi 中。

（3）用户 A 将其手机(可以理解为本公开实施例的无线连接设备)的蓝牙打开，并设置针对蓝牙的登录密码，用户 B 想要将其手机或者其他终端联入该手机的蓝牙中。

实施例一

参照图 1，其示出了本公开实施例的一种无线连接认证方法的流程示意图，具体可以包括：

步骤 110，在当前时间周期内，根据由无线连接设备在当前时间周期内使用的登录密码和权限验证码，对由任意终端发送的权限信息进行判断。

在本公开实施例中，对于每个时间周期，无线连接设备都会获得用于在当前时间周期内登录无线连接设备的登录密码，以及用于确认常驻用户权限的权限验证码。

而用户在任意一个时间周期内都可以发送权限信息到上述无线连接设备中，那么无线连接设备则根据上述登录密码和权限验证码，对接收到的上述权限信息进行判断。

在实际应用中，上述判断过程是将上述终端发送的权限信息与无线连接设备的登录密码 000000 和权限验证码 111111 进行匹配。

在本公开实施例的一个具体实现中，初始化时，本公开实施例生成在第一个时间周期中使用的登录密码和权限验证码。然后在每个时间周期中或者结束时，生成下一个时间周期中使用的登录密码和权限验证码。比如在第一个时间周期结束时生成第二个时间周期使用的登录密码和权限验证码。如此类推，登录密码和权限验证码随着时间周期的变化而变更。

在本公开实施例中，可以理解，对于任意终端发送在任意时刻向无线连

接设备发送权限信息时，该时刻所在时间周期，均可以理解为前述的当前时间周期。

比如，无线连接设备初始化时刻为 12：00，时间周期为 2 个小时，那么终端在 12:30 向无线连接设备发送登录密码，则当前时间周期为 12:00-14:00，相应的，其下一个时间周期为 14:00-16:00；当终端在 14:30 向无线连接设备发送登录密码，则当前时间周期为 14:00-16:00，相应的，其下一个时间周期为 16:00-18:00；终端在 17:00 向无线连接设备发送登录密码，则当前时间周期为 16:00-18:00，相应的，其下一个时间周期为 18:00-20:00。

当然，如果在两个时间周期的交接时刻接收到由终端发送的权限信息，那么当前时间周期可以为交接时刻之后的一个时间周期。比如在 14:00 接收到上述权限信息，那么当前时间周期可以为 14:00-16:00。

可以理解，在本公开实施例中，用户发送的权限信息可分为两个字段，第一个字段为用户输入的登录密码，对应匹配登录密码，第二个字段为用户输入的权限验证码，对应匹配权限验证码。其中，第二个字段可以为空。当然，第一个字段和第二个字段的匹配对象可以根据需要调换。

可以理解，在本公开实施例中，某个终端发送的权限信息可能包括前述正确登录密码，也可能包括不正确其他密码，该终端发送的权限信息还可能包括前述正确的权限验证码，也可能包括不正确的其他验证码。本公开实施例在当前时间周期内，根据当前时间周期内的登录密码和权限验证码，对由任意终端发送的权限信息进行匹配。

对于匹配的情况，以前述时间周期 12:00-14:00 为例，无线连接设备在该时间周期内的登录密码为 000000，在该时间周期内的权限验证码为 111111，那么存在至少如下几种情况：

（1）、终端发送权限信息，其中包括登录密码 123456，没有权限验证码；无线连接设备接收到该 123456 之后，与无线连接设备的登录密码 000000 和权限验证码 111111 进行匹配，发现均匹配不上，不予理会终端的连接。

（2）、终端发送权限信息，其中包括登录密码 000000，没有权限验证码；无线连接设备接收到该 000000 之后，与无线连接设备的登录密码 000000 和权限验证码 111111 进行匹配，发现匹配上登录密码 000000，则确定终端 A

发送了正确的登录密码而未发送权限验证码。

（3）、终端发送权限信息，其中包括登录密码 000000 和权限验证码 121212；无线连接设备接收到该 000000 和 121212 之后，分别与无线连接设备的登录密码 000000 和权限验证码 111111 进行匹配，发现匹配上登录密码 000000 而不能匹配上权限验证码，则确定终端 A 发送了正确的登录密码而发送了错误的权限验证码。

（4）、终端发送权限信息，其中包括登录密码 000000 和权限验证码 111111，无线连接设备接收到该 000000 和 111111 之后，分别与无线连接设备的登录密码 000000 和权限验证码 111111 进行匹配，发现匹配上登录密码 000000，也匹配上权限验证码 111111，则确定终端 A 发送了正确的登录密码以及权限验证码。

（5）终端发送权限信息，其中包括登录密码 222222 和权限验证码 333333，无线连接设备接收到该 222222 之后，与无线连接设备的登录密码 000000 和权限验证码 111111 进行匹配，发现匹配不上登录密码 000000，则不再验证权限验证码。

可以理解，在本公开实施例中，无线连接设备对接收到的登录密码若匹配不上其在当前时间段内使用的登录密码，则不会再匹配权限验证码。

可选的，为了方便用户输入登录密码以及权限验证码，不用用户对其进行记忆，减轻用户的记忆负担，本公开实施例在步骤 110 之前还包括：

步骤 105，根据收到的触发指令，获取所述登录密码以及权限验证码进行展示。

在本公开实施例中，用户可以对无线连接设备进行触发操作，以使无线连接设备对当前时间周期内的登录密码以及权限验证码进行展示。而无线连接设备根据用户的触发操作接收到触发指令，则获取当前时间周期内的登录密码和权限验证码，在显示屏上进行展示。

当然，在展示了一定时间后，比如 30 秒之后，可停止该次展示。

而为了避免一次性就将登录密码和权限验证码都暴露给无线连接设备的临时用户，避免临时用户一次性的就获得了当前时间周期内使用的登录密码和权限验证码，导致临时用户通过终端把登录密码和权限验证码都发送到无

线连接设备而获得常驻登录权限。可选的，上述步骤 105 包括：

子步骤 1051，如果接收到第一次触发指令，则获取所述登录密码进行展示。

在本公开实施例中，操作者第一次在无线连接设备上进行无线连接的触发操作时，无线连接设备根据该触发操作接收到触发指令，然后根据触发指令获取当前时间段内的登录密码，再将该登录密码发送到无线连接设备的显示屏中进行展示。临时用户则可直接根据显示的登录密码，在其终端中进行输入，然后发送到无线连接设备中。

可以理解，对于临时用户来说，由于其已经根据该登录密码使其终端登录了无线连接设备，操作者可以不再进行触发操作，因而可不用再向临时用户展示权限验证码。

子步骤 1052，如果在预定时间间隔内接收到第二次触发指令，则获取所述权限验证码进行展示。

而对于需要长期登录的常驻用户来说，当操作者在预定时间间隔内在无线连接设备上进行再次触发操作时，无线连接设备根据该触发操作接收到第二次触发指令，然后根据第二次触发指令获取当前时间段内的权限验证码，将该权限验证码发送到无线连接设备的显示屏中进行展示。那么常驻用户即可从显示屏中再次获得权限验证码，然后与前述登录密码一起其发送到无线连接设备。

可以理解，本公开实施例中，用户可以发送只包括登录密码的权限信息，也可以发送包括了登录密码和权限验证码的权限信息。

其中，上述预定时间间隔可以设置为 30 秒，也可以设置为从当前时刻到当前时间段结束之前。

当然，对于超过预定时间间隔的触发操作，本公开实施例可以认为接收到第一次触发指令，那么则触发对当前时间周期内的登录密码的显示。

在实际应用中，本公开实施例为未登录的终端提供连接认证页面，即当用户连接到无线连接设备后，未登录的终端会跳转到连接认证页面，该连接认证页面可以显示两个输入栏，其中一个输入栏提示输入登录密码，另外一个输入栏提示输入权限验证码。那么用户可以在该连接认证页面中进行相应

输入，然后点击登录按钮，将其输入的信息发送至无线连接设备。当然，用户可以只输入登录密码，也可以同时输入登录密码和权限验证码。

进一步的，可以理解，任意未认证的终端均可以直接连接到本公开实施例的无线连接设备，但是当用户想要操作该终端进行联网或者其他操作时，由于终端未被赋予任何登录权限，则会转入上述连接认证页面，以供用户输入登录密码和权限验证码。若只有登录密码验证通过，则未登录的终端可进行联网或者其他操作，并被赋予临时登录权限；若登录密码和权限验证码同时验证通过，则未登录的终端可进行联网或者其他操作，并被赋予常驻登录权限。

可选的，所述当前时间周期内使用的权限验证码为将要在下一个时间周期内由无线连接设备使用的登录密码。

可以理解，在本公开实施例中，每个时间周期中，其使用的权限验证码均为下一个时间周期使用的登录密码。

以前述时间周期 12:00-14:00 为例， 12:00-14:00 中，无线连接设备的登录密码 000000 和权限验证码 111111，而该权限验证码 111111 为 14:00-16:00 中使用的登录密码。14:00-16:00 中，无线连接设备的登录密码 111111 和权限验证码 222222，而该权限验证码 222222 为 16:00-18:00 中使用的登录密码。其他情况以此类推。

步骤 120，若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并赋予所述终端临时登录权限。

在本公开实施例中，对于前述（2）和（3）情况，本公开实施例均可认为接收到的终端的权限信息中包括登录密码而不包括权限验证码，因为情况（2）无线连接设备侧根本就没有接收到权限验证码，而情况（3）的接收的权限验证码是错误的，无线连接设备侧实际上也可以理解为没有接收到权限验证码。那么，在上述情况下，允许前述终端登录，并赋予前述终端临时登录权限。

步骤 130，若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并赋予所述终端常驻登录权限。

在本公开实施例中，对于前述（4）情况，本公开实施例认为接收到终端

的权限信息中包括登录密码以及权限验证码，在上述情况下，允许前述终端登录，并赋予前述终端常驻登录权限。

步骤 140，生成新的登录密码和新的权限验证码，以供在下一个时间周期使用。

在本公开实施例的每个时间周期中，均可生成新的登录密码和新的权限验证码，上述新的登录密码和新的权限验证码在转入下一个时间周期时，由无线连接设备使用。

在具体实现中，本公开实施例的第一个时间周期的密码由初始化而来，即第一个时间周期开始时获得。在第一个时间周期结束时，生成新的登录密码和新的权限验证码，那么转入第二个时间周期之时，无线连接设备使用该新的登录密码和新的权限验证码，以为未登录的终端赋予临时登录权限或者常驻登录权限。在第二时间周期结束时，再生成新的登录密码和新的权限验证码，那么转入第三个时间周期之时，则无线连接设备使用上述第二周期结束时生成的新的登录密码和新的权限验证码，以为未登录的终端赋予临时登录权限或者常驻登录权限。依次类推，无线连接设备登录密码和权限验证码随时间周期的变化而变化。

当然，在每个时间周期中，生成供在下一个时间周期使用的新的登录密码和新的权限验证码也可在其他时刻进行，本公开实施例不限定于每个时间周期结束。

本公开实施例在生成了以供在下一个时间周期使用的新的登录密码和新的权限验证码后，那么在进入下一个时间周期时，则在下一个时间周期内使用新的登录密码和权限验证码，那么如果在下一个时间周期中再次接收到其他终端发送的登录密码、或者登录密码和权限验证码，则可进入步骤 110 以进行后续操作。

以前述时间周期 12:00-14:00 为例，时间周期为 2 小时，无线连接设备在该时间周期内的登录密码为 000000，在该时间周期内的权限验证码为 111111。那么在该时间周期结束时，可以生成新的登录密码 222222，和新的权限验证码 333333。那么进入 14:00-16:00 这个时间周期时，采用登录密码 222222，和权限验证码 333333。

可选的，所述当前时间周期内使用的权限验证码为将要在下一个时间周期内由无线连接设备使用的登录密码。

在本公开实施例中，无线连接设备在初始化时，获取第一时间周期的登录密码，并获取第二时间周期的登陆密码作为第一时间周期中的权限验证码。比如以前述时间周期 12:00-14:00 为例，无线连接设备生成该时间周期内的登录密码 000000，同时生成 14:00-16:00 要使用的登录密码 111111，将 111111 作为 12:00-14:00 中使用的权限验证码。

可以理解，由于当前时间周期使用的权限验证码为将要在下一个时间周期内由无线连接设备使用的登录密码。那么每个时间周期中使用的权限验证码均为相应的下一个时间周期内的登录密码。

比如，前述 12:00-14:00 时间周期内使用的登录密码为 000000，使用的权限验证码为 111111，其中 111111 是将要在 14:00-16:00 中使用的登录密码。那么在 12:00-14:00 时间周期结束时，将 12:00-14:00 的登录密码 000000 修改为 12:00-14:00 中使用的权限验证码 111111，同时生成将要在 16:00-18:00 中使用的登录密码 222222。那么在进入 14:00-16:00 之后，无线连接设备使用的登录密码为 111111，使用的权限验证码为 222222。如此，每个时间周期结束时，循环执行上述操作过程。

上述过程可以降低无线连接设备的计算量，并且可快速对登录密码进行切换。

当然，动态密码和权限验证码也可以采用其他形式生成，也可以不与时间周期关联，本公开实施例不对其加以限制。

在本公开实施例中，将登录密码进行更新时，对于新的登录密码，可以自动按照动态密码算法计算生成。而具体采用哪一种动态密码算法本公开实施例不对其加以限制。

步骤 150，在无线连接设备使用所述新的登录密码后，将具备临时登录权限的终端从登录状态移除，并维持具备常驻登录权限的终端的登录状态。

在本公开实施例中，由于当前时间周期内或者结束时，会生成新的登录密码和新的权限验证码，以供在下一个时间周期使用。那么在进入下一个周期之时，无线连接设备的登录密码会被更新，即无线连接设备会采用新的登

录密码。而在登录密码被更新后，本公开实施例将具备临时登录权限的终端从登录状态移除，使其在下一个时间周期再不能登录无线连接设备。而维持具备常驻登录权限的终端的登录状态，使其在下一个时间周期可以继续登录无线连接设备。

本公开实施例的无线连接设备在每个时间周期中提供了登录密码和权限验证码。那么针对只发送了登录密码的终端，赋予临时登录权限；而针对同时输入了登录密码和权限验证码的终端，赋予常驻登录权限。在每次登录密码更新后，将具备临时登录权限的终端从无线连接设备的登录状态移除，而无论密码如何修改，可将具备常驻登录权限的终端，继续保持其对从无线连接设备的登录状态。本公开实施例至少具备如下优点之一：

1、本公开实施例对于无线连接设备的密码，根据时间周期进行自动更新，如此密码是随着时间的变化而变化的，每个密码只使用一段时间即变更为新的密码，并且由于登录密码和权限验证码的两重验证方式，使无线连接设备被暴力破解的难度增大，并且无线信号也不容易被蹭。

例如，以 6 位的登录密码和权限验证码来说，每一位上 26 个字母加上 10 个数字有 36 种可能，那么对于 6 位数的密码就有 36 的 6 次方种可能，那么两个 6 位数密码就有 36 的 12 次方（4.7×10^{18}）种可能，破解难度大大提高。另外，本公开实施例采用动态的两个密码验证方式，登录密码和权限验证码会随着时间进行变化，安全性更高。假设某个终端破解了登录密码，但该终端会被认定为临时登录权限的终端，而过一段时间之后，登录密码自动更新后，该终端的登录状态将被自动剔除。

2、对于无线连接设备的拥有者 B 来说，拥有者 B 可使其终端发送登录密码以及权限验证码到无线连接设备，以获得常驻登录权限；而对临时使用该无线连接设备的用户 A 来说，拥有者 B 可以让用户 A 的终端只发送登录密码以获得临时登录权限。由于无线连接设备可根据时间周期自动更新登录密码，在登录密码更新后，无线连接设备则自动断开该临时登录权限的终端的登录状态，使该终端不能继续登录无线连接设备。因此，无需拥有者 B 主动修改无线连接设备的登录密码，进一步的也无需该拥有者在该登录密码自动修改后，再去修改自己的各个终端的登录密码，即可保证拥有者 B 的终端一

直处于无线连接设备的登录状态。大大方便了无线连接设备的拥有者 B，无需其进行多余的操作，提高了无线连接设备的使用灵活性。

3、对登录密码和权限验证码进行显示，可以方便用户进行输入，降低用户记忆负担。

实施例二

本公开实施例在实施例一的基础之上，在无线连接设备中采用临时用户表对临时用户的终端赋予临时登录权限，采用常驻用户表对常驻用户的终端赋予常驻用户的登录权限。

参照图 2，其示出了本公开实施例的一种无线连接认证方法的流程示意图，具体可以包括：

步骤 210，在当前时间周期内，根据由无线连接设备在当前时间周期内使用的登录密码和权限验证码，对由任意终端发送的权限信息进行判断。

步骤 220，若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并将所述终端的身份信息写入在无线连接设备中预置的临时用户表。

在本公开实施例中，在无线连接设备中预置临时用户表，对于发送了包括登录密码而不包括权限验证码的终端，将该终端的身份信息写入上述临时用户表的方式，是赋予上述终端临时登录权限的一种可选方式。

其中，终端的身份信息可以包括物理地址等信息。

步骤 230，若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并将所述终端的身份信息写入在无线连接设备中预置的常驻用户表。

在本公开实施例中，在无线连接设备中预置常驻用户表，对于发送了包括登录密码以及权限验证码的终端，将该终端的身份信息写入上述常驻用户表的方式，是赋予上述终端常驻登录权限的一种可选方式。

步骤 240，生成新的登录密码和新的权限验证码，以供在下一个时间周期使用。

步骤 250，在无线连接设备使用所述新的登录密码后，清空所述临时用户表所记录的各终端的身份信息，并对于常驻用户表中的终端的身份信息，

维持相应终端的登录状态。

在本公开实施例中，设置了两张表，一张是临时用户表，一张是常驻用户表，临时用户表和常驻用户表均用于接收终端发送的数据包进行后续处理。比如联网时，接收在上述用户表中记录的终端所发送的数据包，然后向互联网转发，又比如传输文件时，接收在上述用户表中记录的终端所发送的文件等。

其中，临时用户表中维护的终端的身份信息，在每个时间周期结束时，无线连接设备侧就将临时用户表中记录的身份信息清空。而常驻用户表中的身份信息，在密码变更后，还予以保留，继续维持具备常驻登录权限的终端的登录状态。

本公开实施例至少具备如下优点之一：

1、对于无线连接设备的密码，根据时间周期进行自动更新，如此密码是随着时间的变化而变化的，每个密码只使用一段时间即变更为新的密码，并且由于登录密码和权限验证码的两重验证方式，使无线连接设备被暴力破解的难度增大，并且无线信号也不容易被蹭。

2、对于无线连接设备的拥有者 B 来说，采用临时用户表维护临时登录权限，采用常驻用户表维护常驻登录权限，那么在无线连接设备在登录密码变更后，进行登录权限维护时，不用遍历每个终端的身份信息，可以直接根据表的性质进行维护，维护简单，计算量低。并且无需连接设备的拥有者进行多余的操作，提高了无线连接设备的使用灵活性。

实施例三

本公开实施例在实施例一的基础之上，采用预置了权限字段的用户表，在用户表对临时用户的终端以临时标记的形式赋予其临时登录权限，对常驻用户的终端以常驻标记的形式赋予其常驻用户的登录权限。

参照图 3，其示出了本公开实施例的一种无线连接认证方法的流程示意图，具体可以包括：

步骤 310，在当前时间周期内，根据由无线连接设备在当前时间周期内使用的登录密码和权限验证码，对由任意终端发送的权限信息进行判断。

步骤 320，若接收到的所述权限信息中包括登录密码而不包括权限验证

码，则允许所述终端登录，并将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入临时用户标记。

在本公开实施例中，在无线连接设备中预置用户表，并在该用户表中预置权限字段。对于发送了包括登录密码而不包括权限验证码的终端，将该终端的身份信息写入上述用户表，并在上述用户表中对应该身份信息的权限字段写入临时用户标记的方式，是赋予上述终端临时登录权限的一种可选方式。

其中，终端的身份信息可以包括物理地址等信息。在本公开实施例中，在通常的用户表中添加了一个权限字段，在该字段下对终端的身份信息进行临时标记，比如设置 0 为临时标记，表示对应的终端身份信息为临时登录权限。

步骤 330，若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入常驻用户标记。

在本公开实施例中，在本公开实施例中，在无线连接设备中预置用户表，并在该用户表中预置权限字段。对于发送了包括登录密码以及权限验证码的终端，将该终端的身份信息写入上述用户表，并在上述用户表中对应该身份信息的权限字段写入临时用户标记的方式，是赋予上述终端常驻登录权限的一种可选方式。

如前所述，在上述用户表的权限字段下，对需要赋予常驻登录权限的终端身份信息，对其进行常驻标记，比如设置 1 为常驻标记，表示对应的终端身份信息为常驻登录权限。

步骤 340，生成新的登录密码和新的权限验证码，以供在下一个时间周期使用。

步骤 350，在无线连接设备使用所述新的登录密码后，将所述用户表中临时用户标记对应的身份信息，从所述用户表中移除息，并对于常驻用户表中的终端的身份信息，维持相应终端的登录状态。

本公开实施例在一张用户表中预置一个新的权限字段，对于终端的身份

信息，进行临时登录权限和常驻登陆权限的标记，然后在密码更新之后，将该用户表根据权限标记，将临时登录权限的标记对应的身份信息删除，保留常驻登录权限标记的身份信息，那么由于用户表中没有临时登录权限终端的身份信息，其登录状态就被移出，而对于所述用户表中常驻用户标记对应的身份信息，维持相应终端的登录状态。

本公开实施例至少具备如下优点之一：

1、对于无线连接设备的密码，根据时间周期进行自动更新，如此密码是随着时间的变化而变化的，每个密码只使用一段时间即变更为新的密码，并且由于登录密码和权限验证码的两重验证方式，使无线连接设备被暴力破解的难度增大，并且无线信号也不容易被蹭。

2、对于无线连接设备的拥有者 B 来说，采用一张用户表，通过权限字段的不同值维护不同的登录权限，那么在无线连接设备在登录密码变更后，进行登录权限维护时，可以只遍历一张用户表即可进行维护，其维护的用户表少，占用系统资源少。并且无需连接设备的拥有者进行多余的操作，提高了无线连接设备的使用灵活性。

实施例四

参照图 4，其示出了本公开实施例的一种无线连接认证方法的流程示意图，具体可以包括：

步骤 410，在当前时间周期内，根据由无线连接设备在当前时间周期内使用的登录密码和权限验证码，对由任意终端发送的权限信息进行判断。

步骤 420，若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并赋予所述终端临时登录权限。

步骤 430，若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并赋予所述终端常驻登录权限。

步骤 440，生成新的登录密码和新的权限验证码，以供在下一个时间周期使用。

步骤 450，在无线连接设备使用所述新的登录密码后，判断所述终端的登录时间长度是否大于等于阈值；如果所述终端的登录时间长度大于等于阈值，则进入步骤 460；如果所述终端的登录时间长度小于阈值，则进入步骤

470。

其中，上述登录时间长度为所述终端从登录时间点到当前时间周期结束的时间点之间的时间长度。

步骤 460，将具备临时登录权限的终端从登录状态移除。

步骤 470，不将具备临时登录权限的终端从登录状态移除。

以前述时间周期 12:00-14:00 为例，时间周期为 2 小时，无线连接设备在该时间周期内的登录密码为 000000，在该时间周期内的权限验证码为 111111。设针对时间长度的阈值为 1 个小时。对于登录无线连接设备的终端，记录其登录时间长度。那么对在 13:00-14:00 之间登录的具有临时登录权限的终端，在 14:00 时无线连接设备使用新的登录密码 111111 后，其登录时间长度小于 1 小时，上述终端可以继续保留登录状态；对于 13:00 登录的具有临时登录权限的终端，在 14:00 时无线连接设备使用新的登录密码 111111 后，其登录时间长度等于 1 小时，上述终端则会被移除登录状态；而对于 12:00-13:00 之间登录的具有临时登录权限的终端，在 14:00 时无线连接设备使用新的登录密码 111111 后，其登录时间长度大于 1 小时，上述终端则会被移除登录状态。

更进一步，比如临时登录权限的终端 A 在 12:15 登录，临时登录权限的终端 B 在 13:15 登录。那么在 14:00 时，无线连接设备使用新的登录密码 111111 后，终端 A 的登录时间长度为 105 分钟，其大于 1 小时，则终端 A 的登录状态则被移除；而终端 B 的登录时间长度为 45 分钟，其小于 1 小时，则终端 B 的登录状态保留。而在 16:00 时，无线连接设备使用新的登录密码 222222 后，终端 B 的登录时间长度为 165 分钟，其大于 1 小时，则终端 B 的登录状态则被移除。

在本公开实施例中，时间周期长度可以根据需求设置，可选的，上述登录时间长度不大于时间周期的长度。

当然，对于实施例二中的临时用户表和常驻用户表的情况，则可在临时用户表中添加一个时间字段，在各终端的身份信息条目下记录其登录时间长度。那么在步骤 450 中，对于判断终端的登录时间长度，可直接读取上述临时用户表中各个终端的时间字段下的登录时间长度，如果登录时间长度达到阈值，则在步骤 460 中，将临时用户表中相应终端身份信息的条目删除；如

果登录时间长度未达到阈值，则在步骤 470 中，将临时用户表中相应终端身份信息的条目保留。

也可以理解，对于实施例三中的一张用户表，还会进一步添加一个时间字段，在各终端的身份信息条目下记录其登录时间长度。那么在步骤 450 中，对于判断具备临时登录权限的终端的登录时间长度，直接读取所述临时用户表中各个终端的时间字段下的登录时间长度，如果登录时间长度达到阈值，则在步骤 460 中，将用户表中相应终端身份信息的条目删除；如果登录时间长度未达到阈值，则在步骤 470 中，将用户表中相应终端身份信息的条目保留。

步骤 480，在无线连接设备使用所述新的登录密码后，维持具备常驻登录权限的终端的登录状态。

本公开实施例在实施例一的基础之上，在对具备临时登录权限的终端进行移出其登录状态操作之前，根据终端的登录时间长度，确定是否将所述终端的登录状态移出，如果终端的登录时间长度小于阈值，则不将终端的登录状态移出。那么可以避免临时登录权限的终端的登录时间长度过短，而影响正常的临时终端的使用。

实施例五

参照图 5，其示出了本公开实施例最优的一种无线连接认证方法的流程示意图，具体可以包括：

步骤 510，如果接收到第一次触发指令，获取所述登录密码进行展示。

步骤 512，如果在预定时间间隔内接收到第二次触发指令，获取所述权限验证码进行展示。

步骤 514，在未登录的终端连接到无线连接设备后，将所述终端展示界面跳转到连接认证页面。

那么未登录终端连接到无线连接设备之后，其展示的界面则会跳转到前述连接认证页面，以通过链接认证页面发送登录密码和权限验证码。

步骤 516，在当前时间周期内，根据由无线连接设备在当前时间周期内使用的登录密码和权限验证码，对由任意终端发送的权限信息进行判断；所述当前时间周期内使用的权限验证码为将要在下一个时间周期内由无线连接

设备使用的登录密码。

步骤 518，若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并赋予所述终端临时登录权限；

步骤 520，若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并赋予所述终端常驻登录权限。

步骤 522，生成新的登录密码和新的权限验证码，以供在下一个时间周期使用。

步骤 524，在无线连接设备使用所述新的登录密码后，对于各具备临时登录权限的终端，判断所述终端的登录时间长度是否大于等于阈值;所述登录时间长度为所述终端从登录时间点到当前时间周期结束的时间点之间的时间长度；如果所述终端的登录时间长度达到阈值，则进入步骤 526；如果所述终端的登录时间长度未达到阈值，则进入步骤 528。

步骤 526，将具备临时登录权限的终端从登录状态移除。

步骤 528，不将具备临时登录权限的终端从登录状态移除。

步骤 530，在无线连接设备使用所述新的登录密码后，维持具备常驻登录权限的终端的登录状态。

在本公开实施例中，在每个时间周期结束时，登录密码会被更新，而在登录密码被更新后，本公开实施例将具备临时登录权限的终端从登录状态移除，使其在下一个时间周期再不能登录无线连接设备。而维持具备常驻登录权限的终端的登录状态，使其在下一个时间周期可以继续登录无线连接设备。

本公开实施例在实施例一的基础之上至少具备如下优点之一：

1、本公开实施例对于无线连接设备的密码，根据时间周期进行自动更新，如此密码是随着时间的变化而变化的，每个密码只使用一段时间即变更为新的密码，暴力破解的难度增大，并且无线信号也不容易被蹭。

2、无线连接设备可自动根据时间周期将临时用户踢出登录状态，保留常驻用户的登录状态。大大方便了有常驻需求的用户对无线连接设备的使用，也方便了无线连接设备的拥有者对无线设备的管理，无需其进行多余的操作，提高了无线连接设备的使用灵活性。

3、对登录密码和权限验证码进行显示，可以方便用户进行输入，降低用

户记忆负担。

4、在对具备临时登录权限的终端进行移出其登录状态操作之前，根据终端的登录时间长度，确定是否将所述终端的登录状态关闭。那么可以避免临时登录权限的终端的登录时间长度过短，而影响正常的临时终端的使用。

实施例六

参照图 6，其示出了本公开实施例最优的一种无线连接认证装置的结构示意图，具体可以包括：

连接判断模块 610，适于在当前时间周期内，根据由无线连接设备在当前时间周期内使用的登录密码和权限验证码，对由任意终端发送的权限信息进行判断。

临时登录权限赋予模块 620，适于若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并赋予所述终端临时登录权限。

常驻登录权限赋予模块 630，适于若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并赋予所述终端常驻登录权限；

更新模块 640，适于生成新的登录密码和新的权限验证码，以供在下一个时间周期使用。

权限管理模块 650，适于在无线连接设备使用所述新的登录密码后，将具备临时登录权限的终端从登录状态移除，并维持具备常驻登录权限的终端的登录状态。

在本公开实施例中，所述无线连接认证装置可嵌入无线连接设备之中。

可选的，所述当前时间周期内使用的权限验证码为将要在下一个时间周期内由无线连接设备使用的登录密码。

可选的，还包括：

展示模块，适于根据收到的触发指令，获取所述登录密码以及权限验证码进行展示。

可选的，所述展示模块包括：

第一展示子模块，适于如果接收到第一次触发指令，则获取所述登录密码进行展示。

第二展示子模块，适于如果在预定时间间隔内接收到第二次触发指令，则获取所述权限验证码进行展示。

可选的，所述当前时间周期内使用的权限验证码为将要在下一个时间周期内由无线连接设备使用的登录密码。

本公开实施例至少具备如下优点之一：

1、本公开实施例对于无线连接设备的密码，根据时间周期进行自动更新，如此密码是随着时间的变化而变化的，每个密码只使用一段时间即变更为新的密码，并且由于登录密码和权限验证码的两重验证方式，使无线连接设备被暴力破解的难度增大，并且无线信号也不容易被蹭。

2、对于无线连接设备的拥有者 B 来说，拥有者 B 可使其终端发送登录密码以及权限验证码到无线连接设备，以获得常驻登录权限；而对临时使用该无线连接设备的用户 A 来说，拥有者 B 可以让用户 A 的终端只发送登录密码以获得临时登录权限。由于无线连接设备可根据时间周期自动更新登录密码，在登录密码更新后，无线连接设备则自动断开该临时登录权限的终端的登录状态，使该终端不能继续登录无线连接设备。因此，无需拥有者 B 主动修改无线连接设备的登录密码，进一步的也无需该拥有者在该登录密码自动修改后，再去修改自己的各个终端的登录密码，即可保证拥有者 B 的终端一直处于无线连接设备的登录状态。大大方便了无线连接设备的拥有者 B，无需其进行多余的操作，提高了无线连接设备的使用灵活性。

3、对登录密码和权限验证码进行显示，可以方便用户进行输入，降低用户记忆负担。

实施例七

参照图 7，其示出了本公开实施例最优的一种无线连接认证装置的结构示意图，具体可以包括：

连接判断模块 710，适于在当前时间周期内，根据由无线连接设备在当前时间周期内使用的登录密码和权限验证码，对由任意终端发送的权限信息进行判断。

临时登录权限赋予模块 720，具体包括：

第一临时登录权限赋予子模块 722，适于若接收到的所述权限信息中包

括登录密码而不包括权限验证码，则允许所述终端登录，并将所述终端的身份信息写入在无线连接设备中预置的临时用户表。

常驻登录权限赋予模块 730，具体包括：

第一常驻登录权限赋予子模块 732，适于若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并将所述终端的身份信息写入在无线连接设备中预置的常驻用户表。

更新模块 740，适于生成新的登录密码和新的权限验证码，以供在下一个时间周期使用。

权限管理模块 750，具体包括：

临时用户表清空子模块 752，适于在无线连接设备使用所述新的登录密码后，清空所述临时用户表所记录的各终端的身份信息适。

常驻用户表维持子模块 754，适于在无线连接设备使用所述新的登录密码后，对于常驻用户表中的终端的身份信息，维持相应终端的登录状态。

本公开实施例至少具备如下优点之一：

1、对于无线连接设备的密码，根据时间周期进行自动更新，如此密码是随着时间的变化而变化的，每个密码只使用一段时间即变更为新的密码，并且由于登录密码和权限验证码的两重验证方式，使无线连接设备被暴力破解的难度增大，并且无线信号也不容易被蹭。

2、对于无线连接设备的拥有者 B 来说，采用临时用户表维护临时登录权限，采用常驻用户表维护常驻登录权限，那么在无线连接设备在登录密码变更后，进行登录权限维护时，不用遍历每个终端的身份信息，可以直接根据表的性质进行维护，维护简单，计算量低。并且无需连接设备的拥有者进行多余的操作，提高了无线连接设备的使用灵活性。

实施例八

参照图 8，其示出了本公开实施例最优的一种无线连接认证装置的结构示意图，具体可以包括：

连接判断模块 810，适于在当前时间周期内，根据由无线连接设备在当前时间周期内使用的登录密码和权限验证码，对由任意终端发送的权限信息进行判断；

临时登录权限赋予模块 820，具体包括：

临时用户添加子模块 822，适于若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入临时用户标记；

常驻登录权限赋予模块 830，具体包括：

常驻用户添加子模块 832，适于若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入常驻用户标记；

更新模块 840，适于生成新的登录密码和新的权限验证码，以供在下一个时间周期使用；

权限管理模块 850，具体包括：

用户表临时移除子模块 852，适于在无线连接设备使用所述新的登录密码后，将所述用户表中临时用户标记对应的身份信息，从所述用户表中移除；

用户表常驻维持子模块 854，适于在无线连接设备使用所述新的登录密码后，对于所述用户表中常驻用户标记对应的身份信息，维持相应终端的登录状态。

本公开实施例至少具备如下优点之一：

1、对于无线连接设备的密码，根据时间周期进行自动更新，如此密码是随着时间的变化而变化的，每个密码只使用一段时间即变更为新的密码，并且由于登录密码和权限验证码的两重验证方式，使无线连接设备被暴力破解的难度增大，并且无线信号也不容易被蹭。

2、对于无线连接设备的拥有者 B 来说，采用一张用户表，通过权限字段的不同值维护不同的登录权限，那么在无线连接设备在登录密码变更后，进行登录权限维护时，可以只遍历一张用户表即可进行维护，其维护的用户表少，占用系统资源少。并且无需连接设备的拥有者进行多余的操作，提高了无线连接设备的使用灵活性。

实施例九

参照图 9，其示出了本公开实施例最优的一种无线连接认证装置的结构示意图，具体可以包括：

连接判断模块 910，适于在当前时间周期内，根据由无线连接设备在当前时间周期内使用的登录密码和权限验证码，对由任意终端发送的权限信息进行判断。

临时登录权限赋予模块 920，适于若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并赋予所述终端临时登录权限。

常驻登录权限赋予模块 930，适于若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并赋予所述终端常驻登录权限；

更新模块 940，适于生成新的登录密码和新的权限验证码，以供在下一个时间周期使用。

权限管理模块 950，具体包括：

临时用户时间判断子模块 952，适于在将具备临时登录权限的终端从登录状态移除之前，对于各具备临时登录权限的终端，判断所述终端的登录时间长度是否大于等于阈值;所述登录时间长度为所述终端从登录时间点到当前时间周期结束的时间点之间的时间长度。

临时用户移除子模块 954，适于如果所述终端的登录时间长度大于等于阈值，则将具备临时登录权限的终端从登录状态移除。

临时用户维持子模块 956，适于如果所述终端的登录时间长度小于阈值，则不将具备临时登录权限的终端从登录状态移除。

常驻用户维持子模块 958，适于在无线连接设备使用所述新的登录密码后，维持具备常驻登录权限的终端的登录状态。

本公开实施例在实施例六的基础之上，在对具备临时登录权限的终端进行移出其登录状态操作之前，根据终端的登录时间长度，确定是否将所述终端的登录状态移出，如果终端的登录时间长度小于阈值，则不将终端的登录状态移出。那么可以避免临时登录权限的终端的登录时间长度过短，而影响正常的临时终端的使用。

实施例十

参照图 10，其示出了本公开实施例最优的一种无线连接认证系统的结构示意图，具体可以包括：

展示模块 1010，具体包括：

第一展示子模块 1011，适于如果接收到第一次触发指令，获取所述登录密码进行展示；

第二展示子模块 1012，适于如果在预定时间间隔内接收到第二次触发指令，获取所述权限验证码进行展示。

页面跳转模块 1020，适于在未登录的终端连接到无线连接设备后，将所述终端展示界面跳转到连接认证页面；

连接判断模块 1030，适于在当前时间周期内，根据由无线连接设备在当前时间周期内使用的登录密码和权限验证码，对由任意终端发送的权限信息进行判断；所述当前时间周期内使用的权限验证码为将要在下一个时间周期内由无线连接设备使用的登录密码；

临时登录权限赋予模块 1040，适于若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并赋予所述终端临时登录权限；

常驻登录权限赋予模块 1050，适于若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并赋予所述终端常驻登录权限；

更新模块 1060，适于生成新的登录密码和新的权限验证码，以供在下一个时间周期使用；

权限管理模块 1070，还包括：

临时用户时间判断子模块 1071，适于在将具备临时登录权限的终端从登录状态移除之前，对于各具备临时登录权限的终端，判断所述终端的登录时间长度是否大于等于阈值;所述登录时间长度为所述终端从登录时间点到当前时间周期结束的时间点之间的时间长度；

临时用户移除子模块 1072，适于如果所述终端的登录时间长度大于等于阈值，则将具备临时登录权限的终端从登录状态移除；

临时用户维持子模块 1073，适于如果所述终端的登录时间长度小于阈值，则不将具备临时登录权限的终端从登录状态移除。

常驻用户维持子模块 1074，适于在无线连接设备使用所述新的登录密码后，维持具备常驻登录权限的终端的登录状态。

本公开实施例在实施例六的基础之上，至少具备如下优点之一：

1、本公开实施例对于无线连接设备的密码，根据时间周期进行自动更新，如此密码是随着时间的变化而变化的，每个密码只使用一段时间即变更为新的密码，暴力破解的难度增大，并且无线信号也不容易被蹭。

2、无线连接设备可自动根据时间周期将临时用户踢出登录状态，保留常驻用户的登录状态。大大方便了有常驻需求的用户对无线连接设备的使用，也方便了无线连接设备的拥有者对无线设备的管理，无需其进行多余的操作，提高了无线连接设备的使用灵活性。

3、对登录密码和权限验证码进行显示，可以方便用户进行输入，降低用户记忆负担。

4、在对具备临时登录权限的终端进行移出其登录状态操作之前，根据终端的登录时间长度，确定是否将所述终端的登录状态关闭。那么可以避免临时登录权限的终端的登录时间长度过短，而影响正常的临时终端的使用。

实施例十一

参照图 11，其为本公开实施例提供的一种无线路由器，其中包括：

第一展示子模块（在图中未显示），适于如果接收到第一次触发指令，则获取所述登录密码进行展示；

第二展示子模块（在图中未显示），适于如果在预定时间间隔内接收到第二次触发指令，则获取所述权限验证码进行展示。

其他模块（在图中未显示）与前述实施例所述类似。其中 1110 为无线路由器的天线，1120 为接收用户触发操作的实体按钮，1130 为显示登录密码和权限验证码的显示屏。当用户点击一次实体按钮 1120 后，显示屏中显示当前时间周期内使用的登录密码 123456，而当用户再次点击一次实体按钮后 1120 显示屏中显示当前时间周期内使用的权限验证码。

当然，如前所述，本公开实施例也可应用于移动终端（比如手机），该移动终端包括无线连接认证装置。在用户将移动终端设置为无线连接设备之后，比如将移动终端设置为 wifi 热点、打开移动终端的蓝牙等，即可应用本公开

实施例的技术方案。当然，对于登录密码和权限验证码的显示可以直接显示在移动终端的显示屏中。对于前述用户的触发操作，可以通过触发移动终端的触摸屏实现，也可以通过触发移动终端的固定按钮（比如音量按钮）实现。

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，本公开实施例也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本公开实施例的内容，并且上面对特定语言所做的描述是为了披露本公开实施例的最佳实施方式。

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，本公开实施例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，在上面对本公开实施例的示例性实施例的描述中，本公开实施例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：即所要求保护的本公开实施例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公开实施例的单独实施例。

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公开实施例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。

本公开实施例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）来实现根据本公开实施例的无线连接认证设备中的一些或者全部部件的一些或者全部功能。本公开实施例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）。这样的实现本公开实施例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。

应该注意的是上述实施例对本公开实施例进行说明而不是对本公开实施例进行限制，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“包含”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。本公开实施例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。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、一种无线连接认证方法，包括：

在当前时间周期内，根据无线连接设备在当前时间周期内使用的登录密码和权限验证码，对终端发送的权限信息进行判断；

若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并赋予所述终端临时登录权限；

若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并赋予所述终端常驻登录权限；

生成新的登录密码和新的权限验证码，以供在下一个时间周期使用；

在无线连接设备使用所述新的登录密码后，将具备临时登录权限的终端从登录状态移除，并维持具备常驻登录权限的终端的登录状态。

2、如权利要求1所述的方法，其中，所述在当前时间周期内，根据无线连接设备在当前时间周期内使用的登录密码和权限验证码，对终端发送的权限信息进行判断之前的步骤，还包括：

根据收到的触发指令，获取所述登录密码以及权限验证码进行展示。

3、如权利要求2所述的方法，其中，所述根据收到的触发指令，获取所述登录密码以及权限验证码进行展示的步骤，包括：

接收到第一次触发指令，获取所述登录密码进行展示；

如果在预定时间间隔内接收到第二次触发指令，则获取所述权限验证码进行展示。

4、如权利要求1所述的方法，其中，所述当前时间周期内使用的权限验证码为将要在下一个时间周期内由无线连接设备使用的登录密码。

5、如权利要求1所述的方法，其中，所述赋予所述终端临时登录权限的步骤，包括：

将所述终端的身份信息写入在无线连接设备中预置的临时用户表；

进一步的，所述将具备临时登录权限的终端从登录状态移除的步骤，包括：

清空所述临时用户表所记录的各终端的身份信息。

6、如权利要求1或5所述的方法，其中，所述赋予所述终端常驻登录权限的步骤，包括：

将所述终端的身份信息写入在无线连接设备中预置的常驻用户表。

7、如权利要求1所述的方法，其中，所述赋予所述终端临时登录权限的步骤，包括：

将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入临时用户标记；

进一步的，所述将具备临时登录权限的终端从登录状态移除的步骤，包括：

将所述用户表中临时用户标记对应的身份信息，从所述用户表中移除。

8、如权利要求1或7所述的方法，其中，所述赋予所述终端常驻登录权限的步骤，包括：

将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入常驻用户标记。

9、如权利要求1所述的方法，其中，所述将具备临时登录权限的终端从登录状态移除的步骤之前，包括：

对于各具备临时登录权限的终端，判断所述终端的登录时间长度是否大于等于阈值;所述登录时间长度为所述终端从登录时间点到当前时间周期结束的时间点之间的时间长度；

如果所述终端的登录时间长度大于等于阈值，则将具备临时登录权限的终端从登录状态移除；

如果所述终端的登录时间长度小于阈值，则不将具备临时登录权限的终端从登录状态移除。

10、一种无线连接认证装置，包括：

连接判断模块，适于在当前时间周期内，根据无线连接设备在当前时间周期内使用的登录密码和权限验证码，对终端发送的权限信息进行判断；

临时登录权限赋予模块，适于若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并赋予所述终端临时登录权限；

常驻登录权限赋予模块，适于若接收到的所述权限信息中包括登录密码

以及权限验证码，则允许所述终端登录，并赋予所述终端常驻登录权限；

更新模块，适于生成新的登录密码和新的权限验证码，以供在下一个时间周期使用；

权限管理模块，适于在无线连接设备使用所述新的登录密码后，将具备临时登录权限的终端从登录状态移除，并维持具备常驻登录权限的终端的登录状态。

11、如权利要求10所述的装置，还包括：

展示模块，适于根据收到的触发指令，获取所述登录密码以及权限验证码进行展示。

12、如权利要求11所述的装置，其中，所述展示模块包括：

第一展示子模块，适于如果接收到第一次触发指令，则获取所述登录密码进行展示；

第二展示子模块，适于如果在预定时间间隔内接收到第二次触发指令，则获取所述权限验证码进行展示。

13、如权利要求10所述的装置，其中，所述当前时间周期内使用的权限验证码为将要在下一个时间周期内由无线连接设备使用的登录密码。

14、如权利要求10所述的装置，其中，所述临时登录权限赋予模块包括：

第一临时登录权限赋予子模块，适于将所述终端的身份信息写入在无线连接设备中预置的临时用户表；

进一步的，所述权限管理模块包括：

临时用户表清空子模块，适于清空所述临时用户表所记录的各终端的身份信息。

15、如权利要求10或14所述的装置，其中，所述常驻登录权限赋予模块包括：

第一常驻登录权限赋予子模块，适于将所述终端的身份信息写入在无线连接设备中预置的常驻用户表。

16、如权利要求10所述的装置，其中，所述临时登录权限赋予模块包括：

临时用户添加子模块，适于将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入临时

用户标记；

进一步的，所述权限管理模块包括：

用户表临时移除子模块，适于将所述用户表中临时用户标记对应的身份信息，从所述用户表中移除。

17、如权利要求10或16所述的装置，其中，所述常驻登录权限赋予模块包括：

常驻用户添加子模块，适于将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入常驻用户标记。

18、如权利要求10所述的装置，其中，所述权限管理模块还包括：

临时用户时间判断子模块，适于在将具备临时登录权限的终端从登录状态移除之前，对于各具备临时登录权限的终端，判断所述终端的登录时间长度是否大于等于阈值;所述登录时间长度为所述终端从登录时间点到当前时间周期结束的时间点之间的时间长度；

临时用户移除子模块，适于如果所述终端的登录时间长度大于等于阈值，则将具备临时登录权限的终端从登录状态移除；

临时用户维持子模块，适于如果所述终端的登录时间长度小于阈值，则不将具备临时登录权限的终端从登录状态移除。

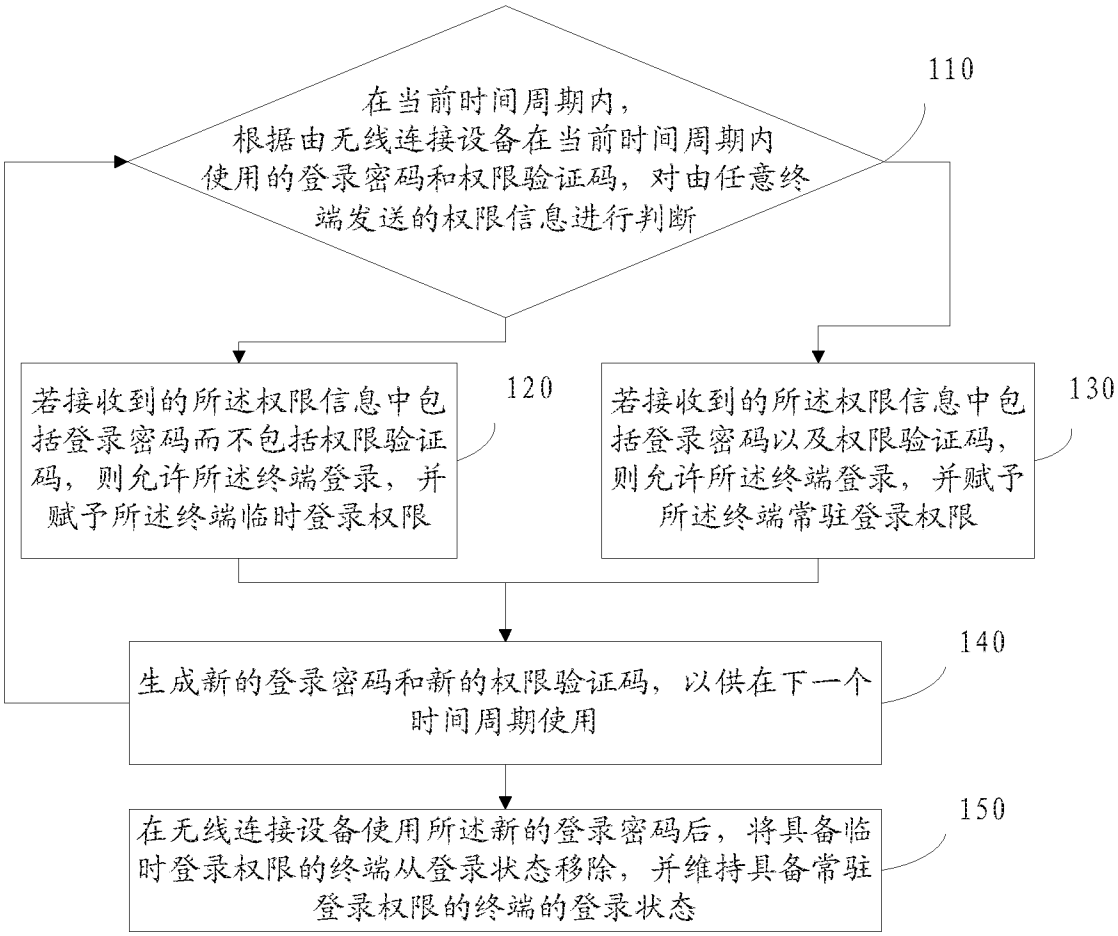

在当前时间周期内，根据由无线连接设备在当前时间周期内使用的登录密码和权限验证码，对由任意终端发送的权限信息进行判断
110
若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并赋予所述终端临时登录权限
120
若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并赋予所述终端常驻登录权限
130
生成新的登录密码和新的权限验证码，以供在下一个时间周期使用
140
在无线连接设备使用所述新的登录密码后，将具备临时登录权限的终端从登录状态移除，并维持具备常驻登录权限的终端的登录状态
150

图 1

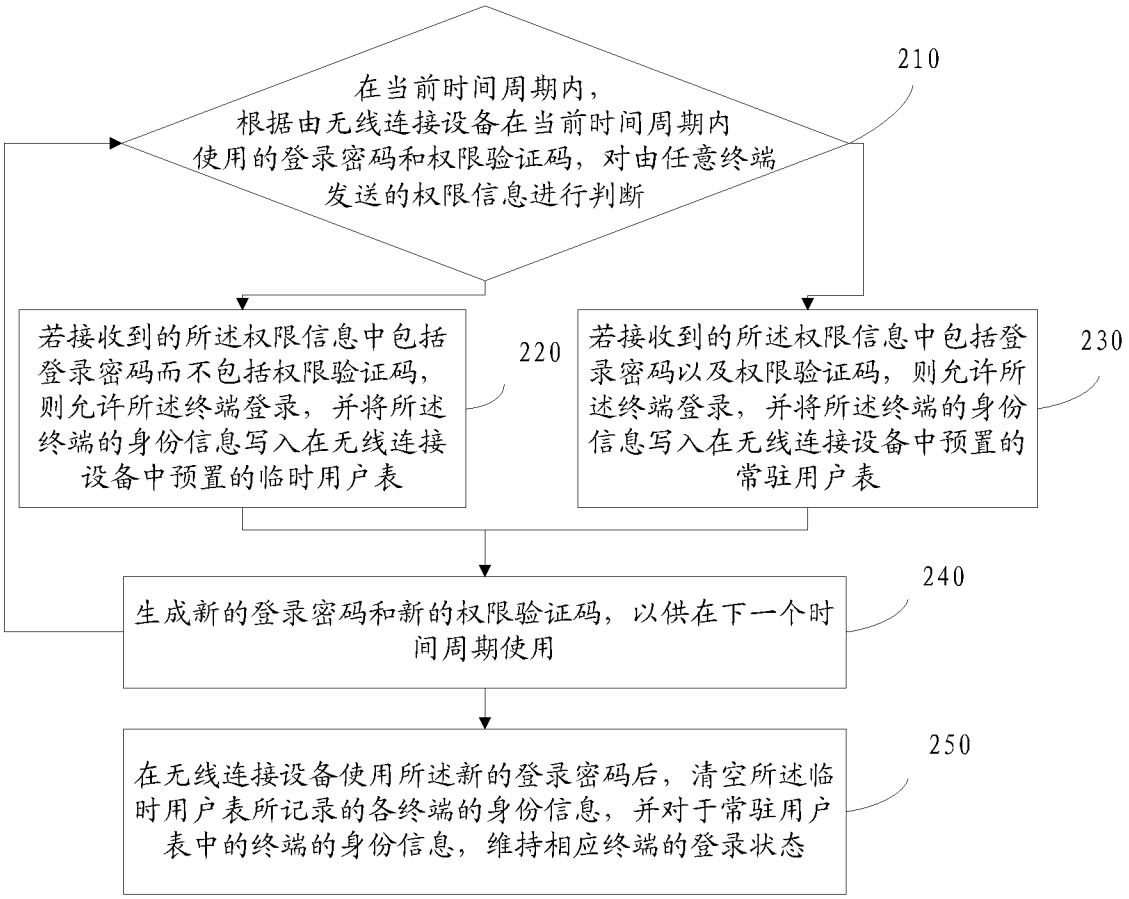

在当前时间周期内，
根据由无线连接设备在当前时间周期内
使用的登录密码和权限验证码，对由任意终端
发送的权限信息进行判断
210
若接收到的所述权限信息中包括
登录密码而不包括权限验证码，
则允许所述终端登录，并将所述
终端的身份信息写入在无线连接
设备中预置的临时用户表
220
若接收到的所述权限信息中包括登
录密码以及权限验证码，则允许所
述终端登录，并将所述终端的身份
信息写入在无线连接设备中预置的
常驻用户表
230
生成新的登录密码和新的权限验证码，以供在下一个时
间周期使用
240
在无线连接设备使用所述新的登录密码后，清空所述临
时用户表所记录的各终端的身份信息，并对于常驻用户
表中的终端的身份信息，维持相应终端的登录状态
250

图 2

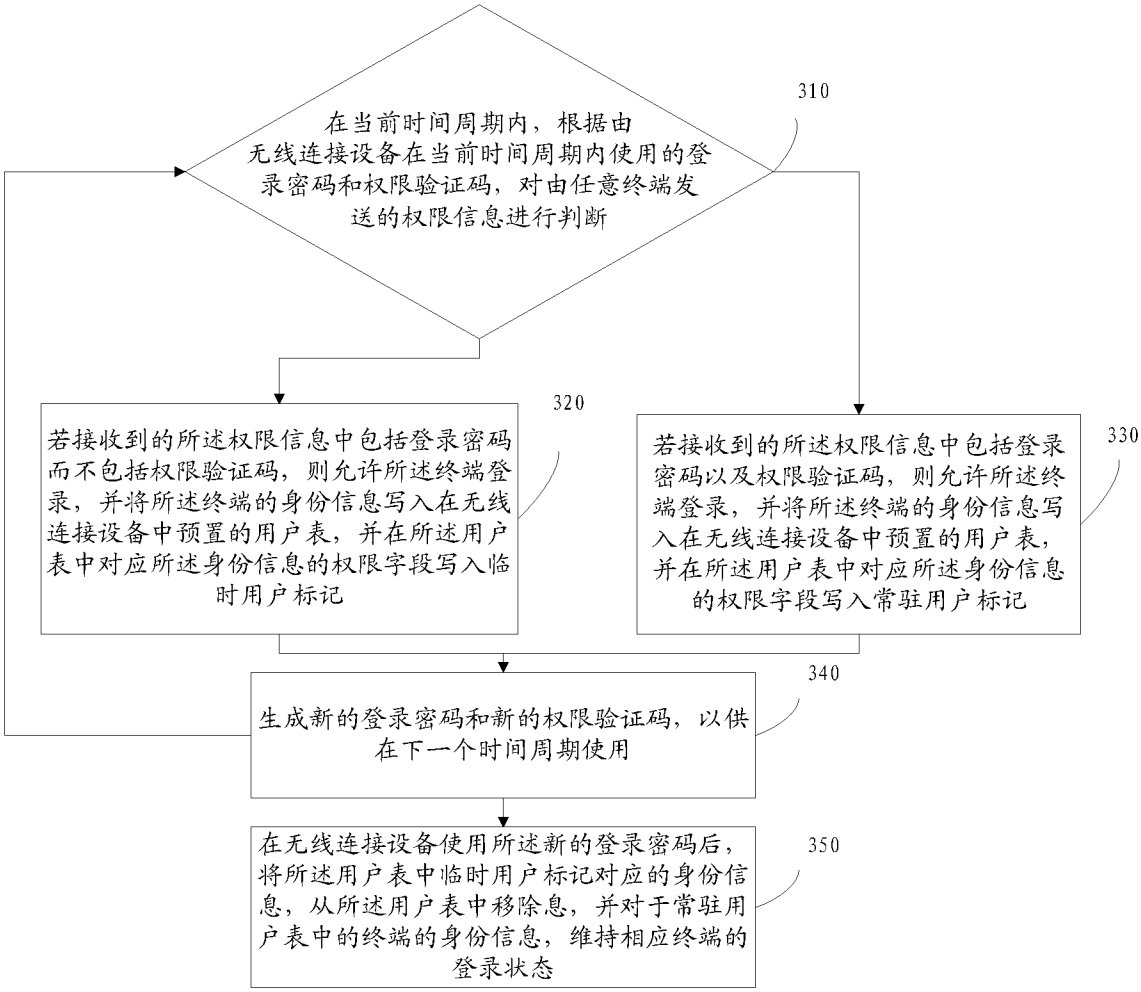

在当前时间周期内，根据由无线连接设备在当前时间周期内使用的登录密码和权限验证码，对由任意终端发送的权限信息进行判断
310
若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入临时用户标记
320
若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并将所述终端的身份信息写入在无线连接设备中预置的用户表，并在所述用户表中对应所述身份信息的权限字段写入常驻用户标记
330
生成新的登录密码和新的权限验证码，以供在下一个时间周期使用
340
在无线连接设备使用所述新的登录密码后，将所述用户表中临时用户标记对应的身份信息，从所述用户表中移除息，并对于常驻用户表中的终端的身份信息，维持相应终端的登录状态
350

图 3

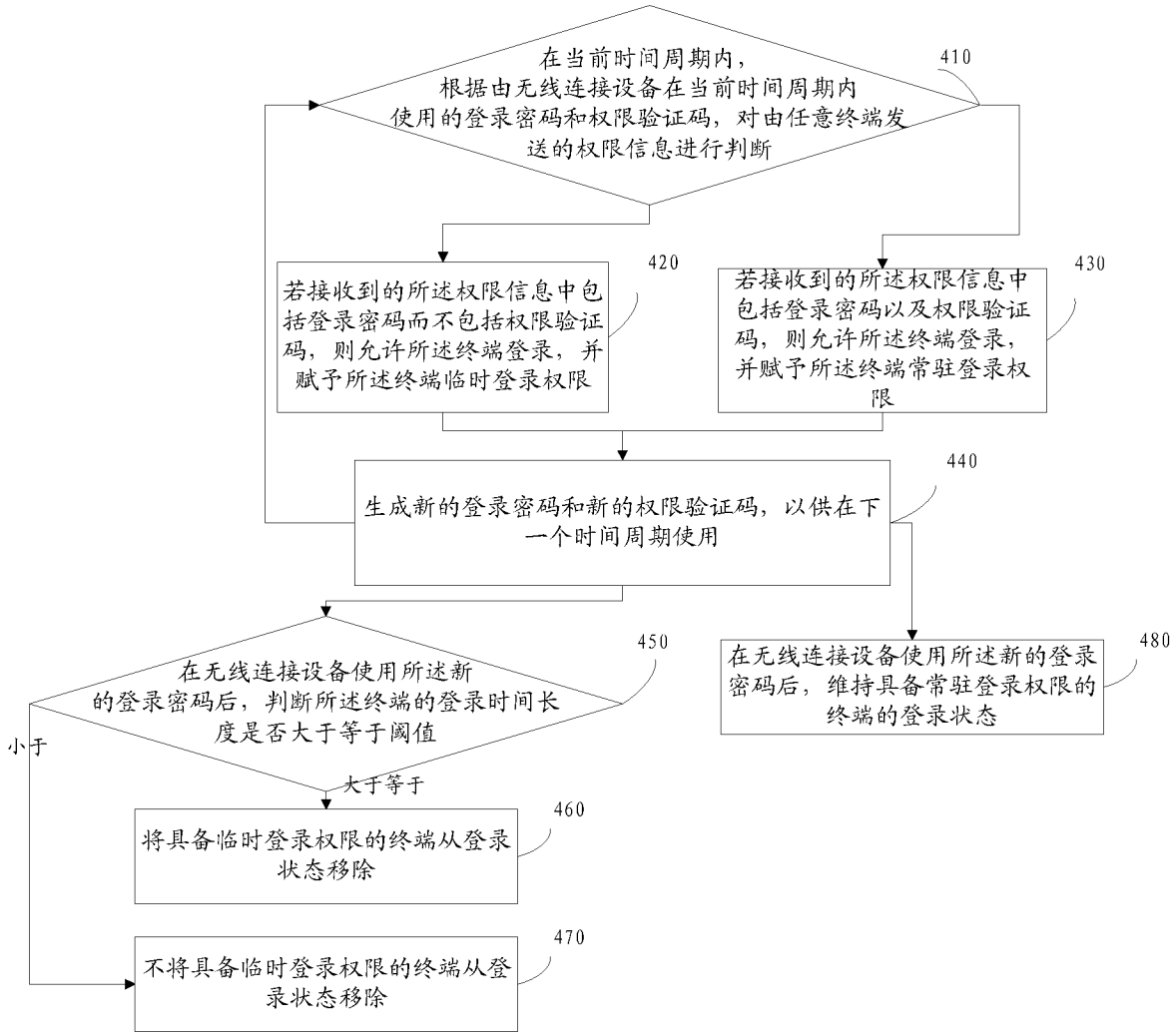

在当前时间周期内，
根据由无线连接设备在当前时间周期内
使用的登录密码和权限验证码，对由任意终端发
送的权限信息进行判断
410
若接收到的所述权限信息中包
括登录密码而不包括权限验证
码，则允许所述终端登录，并
赋予所述终端临时登录权限
420
若接收到的所述权限信息中
包括登录密码以及权限验证
码，则允许所述终端登录，
并赋予所述终端常驻登录权
限
430
生成新的登录密码和新的权限验证码，以供在下
一个时间周期使用
440
在无线连接设备使用所述新
的登录密码后，判断所述终端的登录时间长
度是否大于等于阈值
450
小于
大于等于
在无线连接设备使用所述新的登录
密码后，维持具备常驻登录权限的
终端的登录状态
480
将具备临时登录权限的终端从登录
状态移除
460
不将具备临时登录权限的终端从登
录状态移除
470

图 4

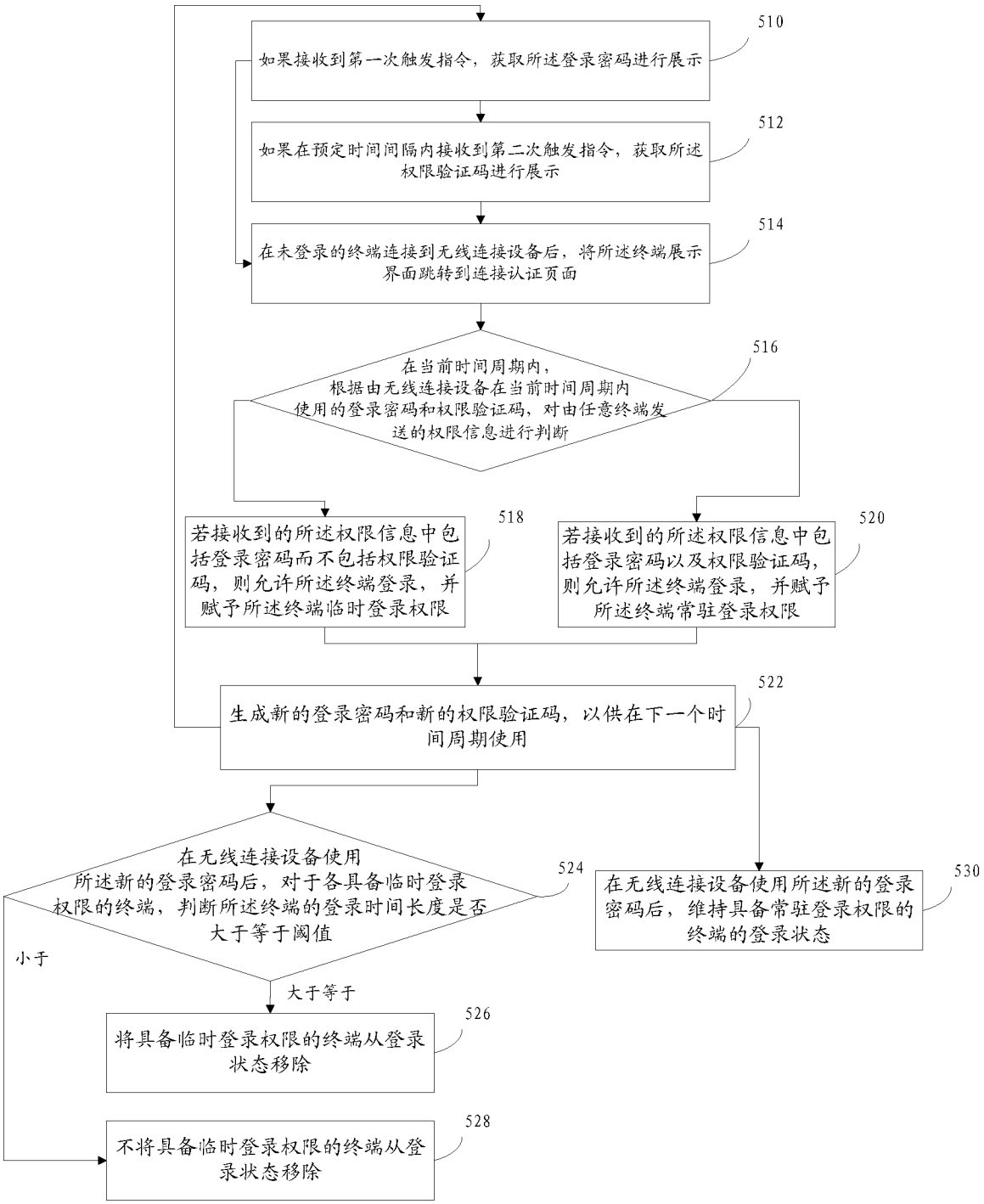

如果接收到第一次触发指令，获取所述登录密码进行展示
510
如果在预定时间间隔内接收到第二次触发指令，获取所述权限验证码进行展示
512
在未登录的终端连接到无线连接设备后，将所述终端展示界面跳转到连接认证页面
514
在当前时间周期内，根据由无线连接设备在当前时间周期内使用的登录密码和权限验证码，对由任意终端发送的权限信息进行判断
516
若接收到的所述权限信息中包括登录密码而不包括权限验证码，则允许所述终端登录，并赋予所述终端临时登录权限
518
若接收到的所述权限信息中包括登录密码以及权限验证码，则允许所述终端登录，并赋予所述终端常驻登录权限
520
生成新的登录密码和新的权限验证码，以供在下一个时间周期使用
522
在无线连接设备使用所述新的登录密码后，对于各具备临时登录权限的终端，判断所述终端的登录时间长度是否大于等于阈值
524
小于
大于等于
将具备临时登录权限的终端从登录状态移除
526
不将具备临时登录权限的终端从登录状态移除
528
在无线连接设备使用所述新的登录密码后，维持具备常驻登录权限的终端的登录状态
530

图 5

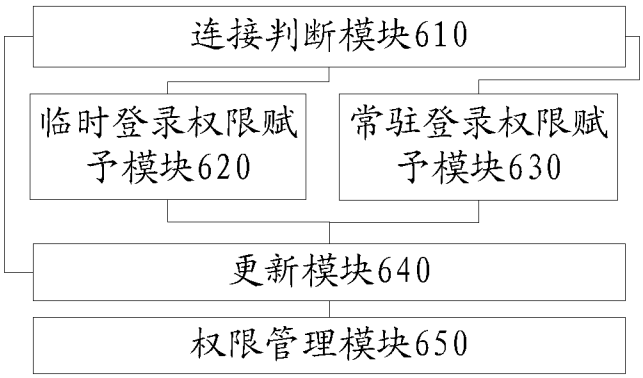

连接判断模块610
临时登录权限赋予模块620
常驻登录权限赋予模块630
更新模块640
权限管理模块650

图 6


连接判断模块710
临时登录权限赋予模块720
第一临时登录权限赋予子模块722
常驻登录权限赋予模块730
第一常驻登录权限赋予子模块732
更新模块740
权限管理模块750
临时用户表清空子模块752
常驻用户表维持子模块754

图 7


连接判断模块810
临时登录权限赋予模块820
临时用户添加子模块822
常驻登录权限赋予模块830
常驻用户添加子模块832
更新模块840
权限管理模块850
用户表临时移除子模块852
用户表常驻维持子模块854

图 8

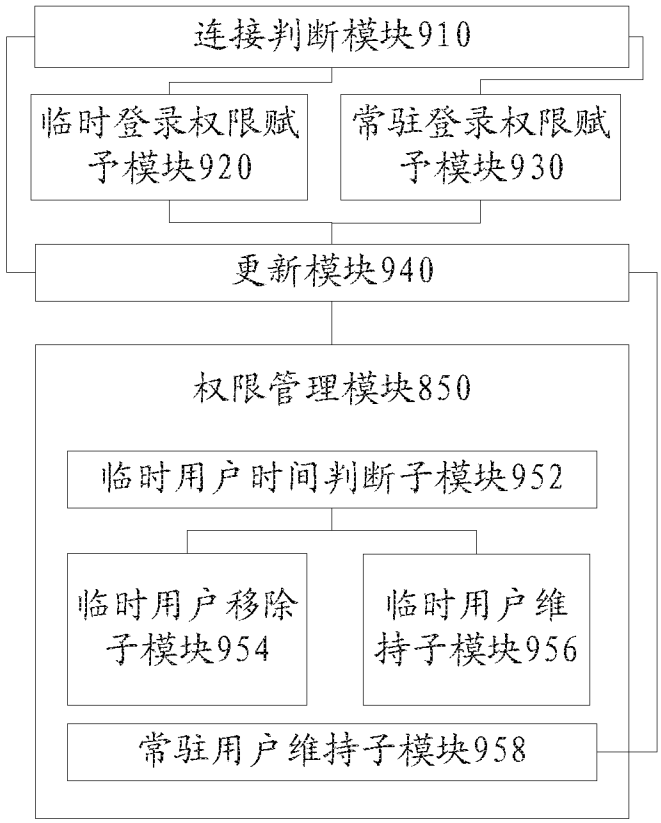

连接判断模块910
临时登录权限赋予模块920
常驻登录权限赋予模块930
更新模块940
权限管理模块850
临时用户时间判断子模块952
临时用户移除子模块954
临时用户维持子模块956
常驻用户维持子模块958

图 9

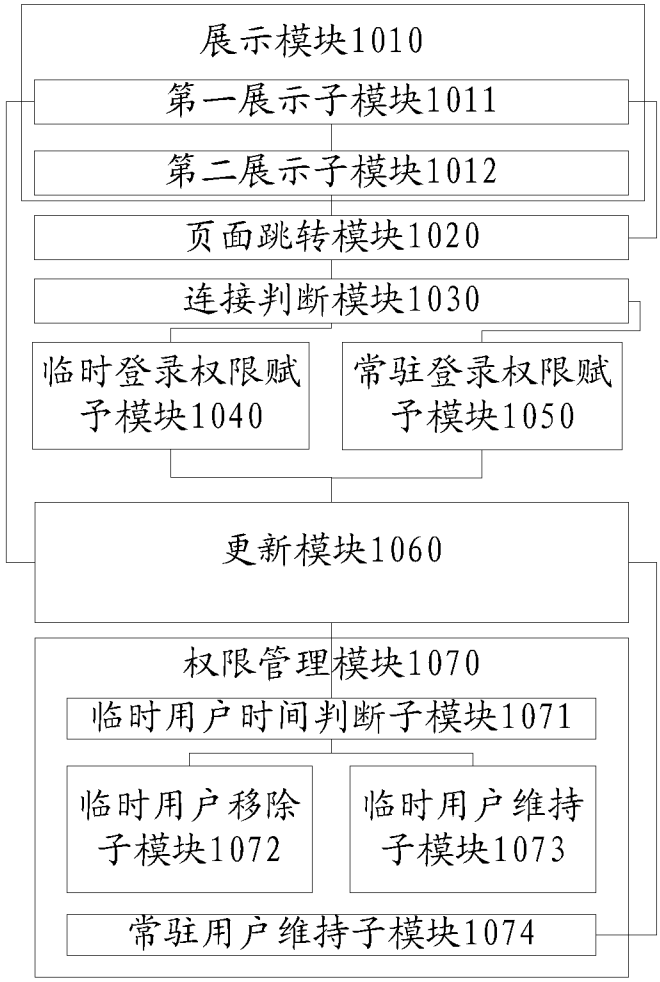

展示模块1010
第一展示子模块1011
第二展示子模块1012
页面跳转模块1020
连接判断模块1030
临时登录权限赋予模块1040
常驻登录权限赋予模块1050
更新模块1060
权限管理模块1070
临时用户时间判断子模块1071
临时用户移除子模块1072
临时用户维持子模块1073
常驻用户维持子模块1074

图 10

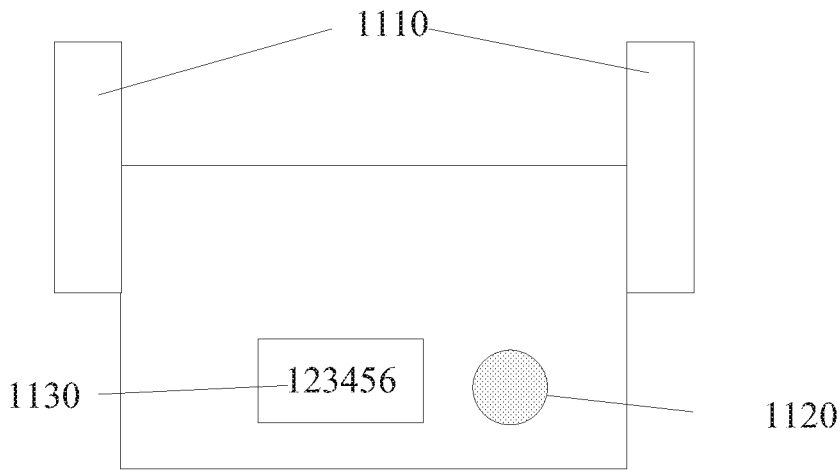

1110
1130
123456
1120

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/079953

A. CLASSIFICATION OF SUBJECT MATTER

H04W 74/00 (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)

H04L; H04W

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)

CNPAT; WPI; EPODOC; IEEE; CNKI: temporar+, short, password, key, login+, connect+, access+, resident, permanent, hotspot, (hot w spot), wifi, wi-fi, wlan, AP, (access point?), validity, term, period, dynamic, authority

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104378758 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.) 25 February 2015 (25.02.2015) description, paragraphs [0070], [0108]	1-18
A	CN 104363213 A (JOYOUNG CO., LTD.) 18 February 2015 (18.02.2015) the whole document	1-18
A	CN 102185838 A (HANGZHOU YUQIANG TECHNOLOGY CO., LTD.) 14 September 2011 (14.09.2011) the whole document	1-18
A	CN 101185308 A (FRANCE TELECOM) 21 May 2008 (21.05.2008) the whole document	1-18
A	WO 2014075056 A2 (ASSA ABLOY AB) 15 May 2014 (15.05.2014) the whole document	1-18

☐ 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

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
02 June 2016	15 July 2016
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 XU, Hongyan Telephone No. (86-10) 62413251

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/079953

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104378758 A	25 February 2015	WO 2015172684 A1	19 November 2015
CN 104363213 A	18 February 2015	None	
CN 102185838 A	14 September 2011	None	
CN 101185308 A	21 May 2008	US 2010024003 A1	28 January 2010
		EP 1884100 A1	06 February 2008
		WO 2006125885 A1	30 November 2006
WO 2014075056 A2	15 May 2014	US 2015254915 A1	10 September 2015
		EP 2917863 A2	16 September 2015

国际检索报告

国际申请号
PCT/CN2016/079953

A. 主题的分类

H04W 74/00(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)

H04L; H04W

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））

CNPAT;WPI;EPODOC;IEEE;CNKI:长期，密码，密钥，连接，有效期，无线连接，长久，无线保真，无线局域网，暂时，周期，登录，临时，常驻，短期，动态，接入点，长驻，接入，热点，权限，临时登录，无线接入,temporar+, short, password, key, login+, connect+, access+, resident, permanent, long, hotspot, (hot w spot), wifi, wi-fi, wlan, AP, (access point?)

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
A	CN 104378758 A (腾讯科技深圳有限公司) 2015年 2月 25日 (2015-02-25) 说明书第[0070]段，第[0108]段	1-18
A	CN 104363213 A (九阳股份有限公司) 2015年 2月 18日 (2015-02-18) 全文	1-18
A	CN 102185838 A (杭州驭强科技有限公司) 2011年 9月 14日 (2011-09-14) 全文	1-18
A	CN 101185308 A (法国电信公司) 2008年 5月 21日 (2008-05-21) 全文	1-18
A	WO 2014075056 A2 (ASSA ABLOY AB) 2014年 5月 15日 (2014-05-15) 全文	1-18

☐ 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
2016年 6月 2日	2016年 7月 15日
ISA/CN的名称和邮寄地址	**受权官员**
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	许洪岩
传真号 (86-10)62019451	电话号码 (86-10)62413251

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/079953

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	104378758	A	2015年2月25日	WO	2015172684	A1	2015年11月19日
CN	104363213	A	2015年2月18日		无		
CN	102185838	A	2011年9月14日		无		
CN	101185308	A	2008年5月21日	US	2010024003	A1	2010年1月28日
				EP	1884100	A1	2008年2月6日
				WO	2006125885	A1	2006年11月30日
WO	2014075056	A2	2014年5月15日	US	2015254915	A1	2015年9月10日
				EP	2917863	A2	2015年9月16日