(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
2012 年 12 月 20 日 (20.12.2012)

WIPO | PCT

(10) 国际公布号
WO 2012/171184 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2011/075754

(22) 国际申请日: 2011 年 6 月 15 日 (15.06.2011)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人 (对除美国外的所有指定国): **华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **李建 (LI, Jian)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **蔡成贵 (CAI, Chenggui)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **傅用成 (FU, Yongcheng)** [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

李媛霞 (LI, Aixia) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: **北京三高永信知识产权代理有限责任公司 (BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY)**; 中国北京市海淀区学院路蓟门里和景园 A-1-102, Beijing 100088 (CN)。

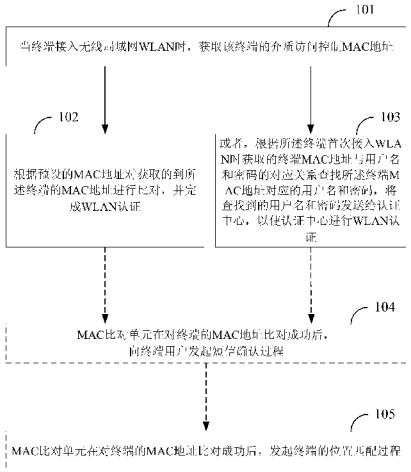
(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG,

[见续页]

(54) Title: WIRELESS LOCAL AREA NETWORK AUTHENTICATION METHOD BASED ON MEDIA ACCESS CONTROL ADDRESS AND DEVICE THEREOF

(54) 发明名称 : 基于 MAC 地址的 WLAN 认证方法和装置



101 OBTAINING A MAC ADDRESS OF A TERMINAL WHEN THE TERMINAL ACCESSES THE WLAN
102 COMPARING WITH THE OBTAINED MAC ADDRESS OF THE TERMINAL ACCORDING TO A PRESET MAC ADDRESS AND FINISHING THE WLAN AUTHENTICATION
103 ALTERNATIVELY, SEARCHING A USER NAME AND A PASSWORD CORRESPONDING TO THE MAC ADDRESS OF THE TERMINAL ACCORDING TO A CORRESPONDENCE RELATIONSHIP BETWEEN THE MAC ADDRESS AND THE USER NAME WITH THE PASSWORD, WHEREIN THE RELATIONSHIP IS OBTAINED WHEN THE TERMINAL ACCESSES THE WLAN FOR THE FIRST TIME, AND SENDING THE SEARCHED USER NAME AND PASSWORD TO AN AUTHENTICATION CENTER, SO THAT THE AUTHENTICATION CENTER CAN IMPLEMENT THE AUTHENTICATION TO THE TERMINAL
104 MAC COMPARING UNIT INITIALING A SHORT MESSAGE ACKNOWLEDGMENT PROCESS TO THE TERMINAL USER AFTER SUCCESSFULLY FINISHING THE MAC ADDRESS OF THE TERMINAL COMPARISON
105 MAC COMPARING UNIT INITIALING LOCATION MAPPING PROCEDURE OF THE TERMINAL AFTER SUCCESSFULLY FINISHING THE MAC ADDRESS OF THE TERMINAL COMPARISON

图 1 / FIG. 1

(57) **Abstract**: A Wireless Local Area Network (WLAN) method based on a Media Access Control (MAC) address and a device thereof are provided in the embodiments of the present invention. The WLAN method based on the MAC address includes: obtaining a MAC address of a terminal when the terminal accesses the WLAN; comparing with the obtained MAC address of the terminal according to a preset MAC address and finishing the WLAN authentication; alternatively searching a user name and a password corresponding to the MAC address of the terminal according to a correspondence relationship between the MAC address and the user name with the password, wherein the relationship is obtained when the terminal accesses the WLAN for the first time, and sending the searched user name and password to an authentication center, so that the authentication center can implement the authentication to the terminal. With the embodiments of the present invention, the number of manual input can be reduced extremely and the wide applicability can be achieved.

(57) 摘要:

[见续页]

WO 2012/171184 A1

KZ, MD, 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, 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))。

本发明实施例提供了一种基于 MAC 地址的 WLAN 认证方法及装置，其中，一种基于 MAC 地址的 WLAN 认证方法包括：当终端接入无线局域网 WLAN 时，获取所述终端的介质访问控制 MAC 地址；根据预设的 MAC 地址对获取的到所述终端的 MAC 地址进行比对，并完成 WLAN 认证；或者，根据所述终端首次接入 WLAN 时获取的终端 MAC 地址与用户名和密码的对应关系查找所述终端 MAC 地址对应的用户名和密码，将查找到的用户名和密码发送给认证中心，以使认证中心对所述终端进行 WLAN 认证。通过本发明实施例，可以大大减少用户进行手动输入的次数，并具有广泛的适用性。

基于 MAC 地址的 WLAN 认证方法和装置

技术领域

本发明涉及通信领域，特别涉及一种基于 MAC（Media Access Control，介质访问控制）地址的 WLAN（Wireless Local Area Network，无线局域网）认证方法和装置。

背景技术

随着 WLAN（Wireless Local Area Network，无线局域网）技术的发展，越来越多的用户开始选择 WLAN 作为互联网接入手段，运营商也大量部署 WLAN 接入点，在提供接入的过程中，运营商首先要对待接入的 WLAN 进行认证。

现有技术一在 WLAN 认证时，采用基于 Web 页面和 HTTP 的认证方式，每次接入网络时，需要用户输入用户名和密码，并由运营商相关验证设备基于该用户名和密码对待接入的 WLAN 进行认证，若验证成功，则允许用户接入，否则拒绝用户接入；现有技术二在 WLAN 认证时，采用基于 Web 页面和 Cookie 的认证方式，由终端设置 Cookie，在用户接入 WLAN 后且短时间内网络出现异常时，若终端用户打开 Cookie，则 Cookie 会根据保存的随机数接入 WLAN 网络，而不需要用户重新输入用户名和密码，若对于不信任的页面，终端用户没有打开 Cookie，则用户需要重新输入用户名和密码进行 WLAN 认证；现有技术三采用基于 (U)SIM 卡的自动认证，要求终端支持 3GPP（3rd Generation Partnership Project，第三代合作伙伴计划）定义的 I-WLAN（Interworking- Wireless Local Area Network，无线局域网互操作）规范。

在实现本发明的过程中，发明人发现现有技术至少存在以下问题：

现有技术一每次接入都需要输入用户名和密码，用户体验比较差；现有技术二取决于终端是否打开 Cookie，对终端的依赖性较强；现有技术三要求终端支持 802.1x EAP-SIM 和 AKA 认证，对终端的要求较高，无法广泛适用。

发明内容

本发明实施例提供了一种基于 MAC 地址的 WLAN 认证方法和装置，用以解决现有技术存在着的用户体验差、对终端要求较高而无法广泛适用的问题。

其中，本发明实施例 WLAN 认证方法包括：

当终端接入无线局域网 WLAN 时，获取所述终端的介质访问控制 MAC 地址；

根据预设的 MAC 地址对获取的到所述终端的 MAC 地址进行比对，并完成 WLAN 认证；

或者，根据所述终端首次接入 WLAN 时获取的终端 MAC 地址与用户名和密码的对应关系查找所述终端 MAC 地址对应的用户名和密码，将查找到的用户名和密码发送给认证中心，以使认证中心对所述终端进行 WLAN 认证。

本发明实施例 WLAN 认证装置包括：

获取模块，用于当终端接入无线局域网 WLAN 时，获取该终端的介质访问控制 MAC 地址；

认证模块，用于预设的 MAC 地址对通过获取模块 501 获取的终端的 MAC 地址进行比对，并完成 WLAN 认证；或者，所述认证模块 502 用于根据所述终端首次接入 WLAN 时获取的终端 MAC 地址与用户名和密码的对应关系查找该终端 MAC 地址对应的用户名和密码，将查找到的用户名和密码发送给认证中心，以使认证中心对所述终端进行 WLAN 认证。

在本发明实施例中，终端接入 WLAN 时，能够利用终端的 MAC 地址信息自动完成终端用户的接入认证，从而可以大大减少用户进行手动输入的次数，改善了用户体验。另外，本实施例不改动终端，只在网络侧优化流程，易部署，现网所有手机都能受益，适用性非常广。

附图说明

图 1 是本发明实施例 1 中提供的 WLAN 认证方法的流程图；

图 2 是本发明实施例 2 中提供的手机用户终端第一次接入 WLAN 网络的认证流程图；

图 3 是本发明实施例 2 中提供的后续手机用户终端接入 WLAN 网络的认证流程图；

图 4 是本发明实施例 2 中提供的执行异常处理流程图；

图 5 是本发明实施例 3 中提供的基于位置信息防止用户仿冒的流程示意图；

图 6 是本发明实施例 4 中提供的 WLAN 认证装置结构示意图；

图 7 是本发明实施例 4 中 WLAN 认证装置结构的一种硬件实现示意图。

具体实施方式

为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

实施例 1

参见图 1，本实施例提供了一种 WLAN 认证方法，该方法包括：

步骤 101：当终端接入无线局域网 WLAN 时，获取该终端的介质访问控制 MAC 地址；

本发明实施例 WLAN 认证方法应用于网络侧，可以不需要对终端进行改变。本发明实施例中，网络侧获取终端的 MAC 地址可以从终端发送的报文中获取，例如，HTTP、DHCP 等协议的报文中都会包括 MAC 地址，可以基于这些协议的报文进行获取，并采用一定的方式（如采用不同的协议）将终端 MAC 地址在不同功能单元之间传递。

本发明实施例中，网络侧设备包括无线接入服务器、MAC 比对单元等功能实体。其中，无线接入服务器可以是 BRAS（Broadband Remote Access Server，宽带远程接入服务器）或 AC（Access Controller，接入控制器）或 AP（Access Point，无线接入点），本实施例不对此进行限定；MAC 比对单元为一个功能模块，可以位于入口 Portal 服务器（在现有技术当中用于对终端提供登录界面，并获取和传递用户输入的用户名和密码）或 AAA（现有技术中完成认证、授权、计费功能）。网络侧获取终端的 MAC 地址具体可以为：

无线接入服务器先通过 HTTP、DHCP 等协议的报文获取终端的 MAC 地址，然后通过接口将 MAC 地址发送给 MAC 比对单元，所述接口可以采用 HTTP 报文头、Radius/Diameter 接口协议、Portal 接口协议等。

步骤 102：根据预设的 MAC 地址对获取的到所述终端的 MAC 地址进行比对，并完成 WLAN 认证；

在预设情况下，终端的 MAC 地址预先保存在 MAC 比对系统中，终端接入时，MAC 比对系统通过获取的终端 MAC 地址信息，在 MAC 地址表项中进行查找和比对，如果查找和比对成功，则返回 MAC 认证成功结果给无线接入服务器；

步骤 103：或者，根据所述终端首次接入 WLAN 时获取的终端 MAC 地址与用户名和密码的对应关系查找所述终端 MAC 地址对应的用户名和密码，将查找到的用户名和密码发送给认证中心，以使认证中心进行 WLAN 认证；

在非预设情况下，终端首次接入 WLAN 时，MAC 比对单元将获取到的终端 MAC 地址和对应的用户名及密码进行保存。后续终端再次发起接入请求时，则 MAC 比对单元先根据获取的终端 MAC 地址，在 MAC 地址表项中进行查找和比对，同时获取 MAC 地址对应的用户名和密码。并且，MAC 比对单元将查找到的 MAC 地址对应的用户名和密码发送给认证中心，以使认证中心进行 WLAN 认证。

认证中心为现有网络架构下的认证服务器设备，MAC 比对单元将终端 MAC 地址对应的用户名和密码替终端发送到认证中心进行认证，省掉了用户再次手动输入用户名和密码的步骤。

步骤 104：MAC 比对单元在对终端的 MAC 地址比对成功后，向终端用户发起短信确认过程。

MAC 比对单元在 MAC 比对成功后，根据对应的用户帐号向用户发送确认短信，如果用户返回拒绝，则进行相应的操作，比如对用户下线，清除 MAC 地址表项等。

步骤 105：MAC 比对单元在对终端的 MAC 地址比对成功后，发起终端的位置匹配过程。

在 MAC 比对成功后，MAC 比对系统分别从 WLAN 网络和移动蜂窝网络中获取终端的位置信息，并对两个位置信息进行匹配，如果匹配不成功，则进行相应的操作，比如对用户下线，清除 MAC 地址表项等。

本实施例中的步骤 104、步骤 105 为附加功能，在实际应用中可以根据情况进行组合，组合方式包括不限于：步骤 101～103 和步骤 104 的组合，步骤 101～103 和步骤 105 的组合，步骤 101～103、步骤 104 和步骤 105 的组合等。

本实施例提供的方法，终端下次接入 WLAN 时，能够在预设的或终端首次接入时获取的 MAC 地址进行查找和比对，自动完成认证过程，从而可以大大减少用户进行手动输入的次数，改善了用户体验。另外，本实施例不改动终端，只在网络侧优化流程，除了需要增加 MAC 比对单元外，其余网络设备都基于现有的设备，因此，很容易部署，使得现网所有手机都能受益，适用性非常广。

实施例 2

本实施例基于实施例1针对手机用户一段时间内使用同一个终端上网的特点，提出了一种手机用户终端基于MAC地址进行WLAN认证的技术方案。

参见图2，本实施例提出了一种手机用户终端第一次接入WLAN的认证流程，具体包括：

步骤 201：UE（User Equipment，用户终端）完成 WLAN 的关联并获得 IP 地址，根据 IP 地址向无线接入服务器发起 HTTP（Hyper Text Transfer Protocol，超文本传输协议）请求，使得所述无线接入服务器根据所述 HTTP 请求获取所述终端的 MAC 地址；

无线接入服务器可以根据 HTTP 请求的 MAC 层报文获取终端的 MAC 地址；或者，UE 在完成 WLAN 的关联后，无线接入服务器根据 UE 发来的 DHCP 请求报文获取 UE 的 MAC 地址。其中，无线接入服务器可以是 BRAS（Broadband Remote Access Server，宽带远程接入服务器）或 AC（Access Controller，存取控制器）或 AP（Access Point，无线接入点），本实施例不对此进行限定，仅以无线接入服务器为 BRAS 为例进行说明。

步骤 202：BRAS 将该 HTTP 请求重定向到 MAC 比对单元，并在该 HTTP 请求的报文

头中增加 UE 的 MAC 地址；

或者，BRAS 可以通过半径 Radius 协议或者直径 Diameter 协议或 Portal 协议向 MAC 比对单元传递终端的 MAC 地址。

其中，这里的 MAC 比对单元具体可以位于 Portal 服务器或者 AAA 服务器中，或者为一个独立的设备。

步骤 203：MAC 比对单元接收 BRAS 发送的 HTTP 协议，并根据 HTTP 请求识别 UE 的类型，若 UE 为手机用户终端，则在保存的对应关系中查找该 MAC 地址对应的用户名和密码，若没有查找到，MAC 比对单元向 UE 推送登录页面。

在非预设情况下，由于第一次接入，一般事先都不会保存对应关系，因此，MAC 比对单元向 UE 推送登录页面，用户在该界面下输入用户名、密码等信息。

其中，MAC 比对单元根据 HTTP 请求识别 UE 的类型具体包括，根据 HTTP 请求的报文头部携带的用户代理 User-Agent 字段识别 UE 的类型。User-Agent 字段会包含终端的类型（如手机类型）等信息，因此，可以根据该字段对 UE 类型进行识别，并针对不同的终端类型采取不同的策略，例如，针对终端类型为手机的用户，可以选择继续接入；针对 PC 用户，可以回退到 Portal 认证。

实际应用中，在对应关系中没有查找到的情况较多，如终端首次接入 WLAN，尚未建立该终端的 MAC 地址与用户名和密码的对应关系；若更换手机或修改密码时，则终端的 MAC 地址或密码已经发生变化，在对应关系中也查找不到对应的用户名和密码。在这些情况下，都需要重新通过用户输入用户名、密码，建立与 MAC 地址的连接关系。

在采用非 HTTP 方式获取终端 MAC 地址时（比如采用 DHCP 方式），无线接入服务器可以先识别 HTTP 报文中的 User-Agent，再通过 Radius/Diameter 接口或 Portal 协议接口传递给 MAC 比对单元。

本实施例中还可以设定 MAC 地址与用户名、密码对应关系的老化时间，其中，所有用户的对应关系可以统一设定成一个老化时间；或者根据某种策略对不同用户的对应关系设定不同的老化时间。如果保存的对应关系存在的时间超过了老化时间，则清除该 MAC 地址与用户名和密码的对应关系。例如，在 2011 年 3 月 1 日早上 9 点建立 UE1 的 MAC 地址与用户名和密码的对应关系，并预设该对应关系的老化时间为 1 个月，若 UE1 在 2011 年 4 月 1 日早上 10 点接入 WLAN 进行认证时，由于超过了 1 个月的老化时间，则删除该 UE 的 MAC 地址与用户名和密码的对应关系。

步骤 204：UE 在登录页面上输入用户名和密码；

步骤 205：MAC 比对单元根据 UE 输入的用户名和密码，及获取的 UE 的 MAC 地址，

保存 MAC 地址与用户名和密码的对应关系，并将该用户名和密码发送给 BRAS（如通过 Portal 协议），发起认证；

步骤 206：BRAS 将接收到的用户名和密码发给认证中心进行认证（如通过 Radius 协议）；

其中，本实施例中以认证中心为 AAA 为例进行说明；

步骤 207：BRAS 接收 AAA 返回的认证结果，并将该认证结果反馈给 Portal 服务器；

步骤 208：Portal 服务器判断认证结果，如果认证成功，则给 UE 推送登录成功页面，认证流程结束。

参见图 3，本实施例当 MAC 比对中心保存了 MAC 与用户名和密码的对应关系后，后续手机用户终端接入 WLAN 网络流程，具体包括：

步骤 301：手机用户终端基于 Web 浏览器完成 WLAN 的关联并获得 IP 地址，根据 IP 地址向 BRAS 发起 HTTP 请求；

或者，UE 在完成 WLAN 的关联后，无线接入服务器根据 UE 发来的 DHCP 请求报文获取 UE 的 MAC 地址。

步骤 302：BRAS 将该 HTTP 请求重定向到 MAC 比对单元，并在该 HTTP 请求的报文头中增加 UE 的 MAC 地址；

或者，无线接入服务器通过 Radius/Diameter 协议或 Portal 协议向 MAC 比对单元传递终端的 MAC 地址。

步骤 303：MAC 比对单元接收 BRAS 发送的 HTTP 协议，并根据 HTTP 请求识别 UE 的类型，若 UE 为手机用户终端，则在预设的或终端首次接入时获取的对应关系中查找 MAC 地址对应的用户名和密码，并将查找到的用户名和密码发送给 BRAS；

或者，MAC 比对单元根据无线接入服务器通过 Radius/Diameter 协议或 Portal 协议传递的 MAC 地址和终端类型，在本地保存的 MAC 地址表项中进行查找和比对。

步骤 304：BRAS 将用户名和密码发送给 AAA，以使 AAA 进行 WLAN 认证；

步骤 305：AAA 进行 WLAN 认证，并向 BRAS 返回认证结果；

步骤 306：BRAS 接收 AAA 返回的认证结果，并将该认证结果反馈给 MAC 比对单元；

步骤 307：MAC 比对单元判断认证结果，如果认证成功，通知短信中心向 UE 下发短信确认消息；

本实施例中 MAC 比对单元还可以携带用于指示“本次认证是否为 MAC 认证”的标识，作为是否进行短信确认流程的依据，当该标识指示本次认证为 MAC 认证时，则进行短信确认流程；否则，不进行短信确认流程。

其中，本实施例不对短信提醒消息的形式进行限定，该短信提醒消息可以为“成功登陆

WLAN，请回复“AA”进行确认”的字段等。

步骤 308：短信中心向 UE 下发短信提醒消息；

具体地，短信中心向 UE 对应的手机号码（对应 WLAN 用户帐号）下发短信提醒消息，UE 接收到该短信提醒消息后，向短信中心返回认证确认消息。

步骤 309：UE 根据收到的短信提醒消息，向短信中心返回认证确认消息；

其中，本实施例不对认证确认消息的形式进行限定，此处以认证确认消息为肯定消息为例进行说明，如该认证确认消息可以为“是”、“确认”的字段等。

步骤 310：短信中心根据接收到的认证确认消息通知 MAC 比对单元；

步骤 311：MAC 比对单元给 UE 推送登录成功页面，认证流程结束。

参见图 4，若上述步骤 309 中 UE 向短信中心返回的认证确认消息为否认消息或确认超时，则执行异常处理流程，具体步骤如下：

步骤 312：短信中心判断是否为仿冒用户，若判断为仿冒用户，则通知 MAC 比对单元；

具体地，该仿冒用户包括变更终端后，利用更换后的终端接入 WLAN 的用户；还包括了没有变更终端，但在返回认证确认消息进行了误操作的用户，本实施例中将进行了误操作的用户也视为仿冒用户，执行异常处理流程。

步骤 313：MAC 比对单元清除当前链接和 MAC 地址表项，异常处理流程结束。

本实施例提供的方法，通过在网络侧保存终端 MAC 地址与用户名和密码的对应关系，下次用户接入的时候，网络侧用终端 MAC 地址索引到用户名和密码作为认证凭证，从而可以大大减少用户进行手动输入的次数，方便用户使用。另外，本实施例不改动终端，只在网络侧优化流程，易部署，现网所有手机都能受益，适用性非常广。

实施例 3

本发明实施例基于上述实施例 1、2 提供了一种基于位置信息防止用户仿冒的方法，这种方法可以与实施例 2 中基于短信的方式防止用户仿冒的方式一起应用，或者只应用本发明实施例中基于位置信息防止用户仿冒的方法。

具体的，参见图 5，包括如下步骤：

S321、获取终端在 WLAN 中的位置信息以及终端在移动蜂窝网（如 2G、3G 等网络）中的位置信息；

此步骤可以在认证过程当中，信息获取通过位置匹配单元来进行获取，位置匹配单元也可以基于现网中的 Portal 服务器或 AAA 服务器，或者也可以是一个单独的设备，其功能与 MAC 比对单元相独立。

具体的，位置匹配单元获取终端在 WLAN 网络中的位置信息通过如下方式获取：

位置匹配单元通过 Portal 协议或者 Radius/Diameter 协议从无线接入服务器（如 AC 或 BRAS）获取终端在 WLAN 网络中的位置信息，包括 AP 标识或 AP 位置信息。

同时，本发明实施例中 MAC 比对单元还可以携带用于指示“本次认证是否为 MAC 认证”的标识，以作为位置匹配单元是否进行位置匹配操作的依据，当该标识指示本次认证为 MAC 认证时，位置匹配单元后续进行位置匹配操作；否则，不进行位置匹配操作。

位置匹配单元获取终端在移动蜂窝网中的位置信息通过如下方式获取：

位置匹配单元通过 MAP（Mobile Application Part）接口的 ATI（Any Time Interrogation）消息向位置归属寄存器 HLR（Home Location Register）发送获取用户信息的请求，HLR 通过 MAP 接口的 PSI（Provide Subscriber Information）消息向 MSC 发送获取用户信息的请求，MSC 通过 PSI 寻呼获取终端的用户信息，通过 PSI 寻呼获取的用户信息当中包括益区及具体的小区信息；

或者，位置匹配单元通过 MAP 接口的 SRI（Send Routing Information）消息向 HLR 获取用户路由信息，获取位置区信息，但没有具体的小区信息。

其中，上述 MAP 接口、ATI 消息、PSI 消息、SRI 消息都为 3GPP 协议定义的消息，本领域技术人员可以根据 3GPP 协议来实现相应的操作。

S322、根据预先配置的 WLAN 部署的位置信息与移动蜂窝网部署的位置信息的对应关系对获取到的终端在 WLAN 中的位置信息与终端在移动蜂窝网中的位置信息进行匹配，判断是否满足预先配置的 WLAN 部署的位置信息与移动蜂窝网部署的位置信息的对应关系，以判断用户是否为仿冒用户。

具体的，如果不满足对应关系，则判定用户为仿冒用户，并采用针对此判定结果所定义的执行策略（如回退到 Portal 认证）；如果满足对应关系，则判定用户为正常用户，并采用针对此判定结果所定义的执行策略（如正常接入）。

例如，针对一个地区 A，假设部署了 3 个 WLAN 的 AP，分别为 AP1、AP2、AP3；同时，地区 A 部署了 2 个小区，具体为小区 1，小区 2，假设 WLAN 部署的位置信息与移动蜂窝网部署的位置信息的对应关系为 AP1、AP2 与小区 1 对应，AP3 与小区 2 对应。这些网络部署的信息都是预先知道的，可以事先配置好对应关系。当获取到的用户在 WLAN 中的位置信息为 AP1，获取到的用户在移动蜂窝网中的位置信息为小区 1 时，则这种对应关系满足预先配置的关系，可以认为用户是正常的用户；否则，如果用户在 WLAN 中的位置信息为非 AP1、AP2 的其他 AP（如 AP3、AP5），则判定用户为仿冒用户，并且可以执行回退到 Portal 认证，用户下线，清除 MAC 比对单元中保存的 MAC 地址表项等操作。

需要说明的是，当 S322 条件不满足时判定用户为仿冒用户只是一种大概率的事件，实际应用当中也有可能出现用户更换终端而导致的一些误判，因此，可以结合实际情况在满足条件下采用合适的策略，这里并不限定。这些策略都可以认为是基于“判定用户为仿冒用户”判定结果下的策略的等同实现方式。

实施例 4

参见图 6，本发明实施例基于上述各实施例提供了一种 WLAN 认证装置 50，具体包括：

获取模块 51，用于当终端接入无线局域网 WLAN 时，获取该终端的介质访问控制 MAC 地址；

认证模块 52，用于预设的 MAC 地址对通过获取模块 501 获取的终端的 MAC 地址进行比对，并完成 WLAN 认证；或者，所述认证模块 502 用于根据所述终端首次接入 WLAN 时获取的终端 MAC 地址与用户名和密码的对应关系查找该终端 MAC 地址对应的用户名和密码，将查找到的用户名和密码发送给认证中心，以使认证中心对所述终端进行 WLAN 认证。

其中，MAC 地址的获取方法在上述实施例 1、2 中已经具体介绍，这里不再赘述。

本发明实施例还包括：

对应关系建立模块 53，所述对应关系建立模块包括接收单元 531 和建立单元 532；

所述接收单元用于接收无线接入服务器发送的终端的 MAC 地址，并接收所述终端发送的用户名和密码，其中，所述无线接入服务器包括宽带远程接入服务器 BRAS，或者存取控制器 AC，或者无线接入点 AP；

所述建立单元用于根据所述终端的 MAC 地址，建立所述终端的 MAC 地址与用户名和密码的对应关系。

本实施例还包括：

短信判断模块 54，用于通知短信中心向终端下发短信提醒消息，并通过所述短信中心返回的认证确认消息判断用户是否为仿冒用户。

本实施例还包括：

位置获取模块 55，用于获取终端在 WLAN 中的位置信息以及终端在移动蜂窝网中的位置信息；

位置判断模块 56，用于根据预先配置的 WLAN 部署的位置信息与移动蜂窝网部署的位置信息的对应关系对获取到的终端在 WLAN 中的位置信息与终端在移动蜂窝网中的位置信息进行匹配，判断是否满足预先配置的 WLAN 部署的位置信息与移动蜂窝网部署的位置信

息的对应关系，以判断用户是否为仿冒用户。

其中，所述位置获取模块包括：

WLAN 位置获取模块 551，用于通过 Portal 协议或者半径 Radius 协议或者直径 Diameter 协议从无线接入服务器获取终端在 WLAN 中的位置信息，所述终端在在 WLAN 中的位置信息包括 AP 标识或 AP 位置信息；

移动蜂窝网位置获取模块 552，用于通过 MAP 接口的 ATI 消息向位置归属寄存器 HLR 发送获取用户信息的请求，使得所述 HLR 收到请求后通过 MAP 接口的 PSI 消息向移动交换中心 MSC 发送获取用户信息的请求，使得所述 MSC 收到所述 HLR 发送的请求后通过 PSI 寻呼获取终端的用户信息，所述终端的用户信息中包括位置区及小区位置信息；根据所述用户信息中包括的位置区及小区位置信息获取终端在移动蜂窝网中的位置信息；或者通过 MAP 接口的 SRI 消息向所述 HLR 获取用户路由信息，所述用户路由信息包括位置区信息，根据所述路由信息中的位置区信息获取终端在移动蜂窝网中的位置信息。

本发明实施例中，获取模块 51，认证模块 52，对应关系建立模块 53，短信判断模块 54 可以认为是前面实施例中的 MAC 比对单元中的几个模块。位置获取模块 55，位置判断模块 56 可以认为是前面实施例中的位置匹配单元中的几个模块。如前面实施例所述，这几个模块可以位于同一个实体网元（如 Portal 服务器，或者 AAA 服务器），也可以以单独的设备形式存在，考虑到尽量不改变现有网络的技术架构，本发明实施例可以将这些功能模块通过现有的网元设备（如 Portal 服务器）实现。

参见图 7，为本发明实施例基于现有 Portal 服务器或 AAA 服务器实现的硬件结构示意图，包括 CPU、存储器、通信接口等单元。其中，CPU 用于执行上述功能模块相关的代码（如图 6 中，CPU 用于执行 MAC 比对单元，位置匹配单元相关的功能代码）。在实际硬件设计过程当中，CPU 也可以采用其他具有类似处理功能的处理设备实现，如 DSP、FPGA 等处理器。存储器用于存储 CPU 运行过程当中的一些临时数据或其他需要保存的数据，通信接口用于提供与其他设备（如终端、认证中心等）交互的接口，这些技术都为本领域技术人员所熟知的技术，在此不再详述。

本实施例提供的装置，通过在网络侧保存终端 MAC 地址与用户名和密码的对应关系，下次用户接入的时候，能够在预设的终端 MAC 地址与用户名和密码的对应关系中查找所述终端的 MAC 地址对应的用户名和密码，网络侧用终端 MAC 地址索引到用户名和密码作为认证凭证，免除了用户的重复输入，方便用户使用。另外，本实施例不改动终端，只在网络侧优化流程，易部署，现网所有手机都能受益，适用性非常广。

以上实施例提供的技术方案中的全部或部分内容可以通过软件编程实现，其软件程序存储在可读取的存储介质中，存储介质例如：计算机中的硬盘、光盘或软盘。

以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权利要求

1、一种基于 MAC 地址的 WLAN 认证方法，其特征在于，所述方法包括：

当终端接入无线局域网 WLAN 时，获取所述终端的介质访问控制 MAC 地址；

根据预设的 MAC 地址对获取的到所述终端的 MAC 地址进行比对，并完成 WLAN 认证；

或者，根据所述终端首次接入 WLAN 时获取的终端 MAC 地址与用户名和密码的对应关系查找所述终端 MAC 地址对应的用户名和密码，将查找到的用户名和密码发送给认证中心，以使认证中心对所述终端进行 WLAN 认证。

2、如权利要求 1 所述的方法，其特征在于，还包括：

当采用所述根据所述终端首次接入 WLAN 时获取的终端 MAC 地址与用户名和密码的对应关系查找该终端的 MAC 地址，将查找到的终端 MAC 地址对应的用户名和密码发送给认证中心，以使认证中心进行 WLAN 认证的方法进行认证时，在所述终端首次接入无线局域网 WLAN 时，接收所述终端发送的用户名和密码；其中，所述无线接入服务器包括宽带远程接入服务器 BRAS，或者存取控制器 AC，或者无线接入点 AP；

根据获取的所述终端的 MAC 地址以及所述终端的的用户名和密码，建立所述终端的 MAC 地址与用户名和密码的对应关系。

3、如权利要求 2 所述的方法，其特征在于，还包括：

预设终端的 MAC 地址与用户名和密码的对应关系的老化时间；

当保存的终端的 MAC 地址与用户名和密码的对应关系存在的时间超过老化时间时，删除所述终端的 MAC 地址与用户名和密码的对应关系。

4、如权利要求 1 所述的方法，其特征在于，所述获取所述终端的介质访问控制 MAC 地址，具体包括：

接收无线接入服务器通过半径 Radius 协议或者直径 Diameter 协议或者 Portal 协议传递的终端的 MAC 地址，其中，所述无线接入服务器传递的终端的 MAC 地址根据终端发来的 HTTP 请求的 MAC 层报文获得。

5、如权利要求 2 所述的方法，其特征在于，还包括：

当接收到 HTTP 请求时，根据所述 HTTP 请求报文头中的用户代理（User-Agent）判断终端类型，并根据终端类型采用不同的认证策略。

6、如权利要求 1 所述的方法，其特征在于，完成 MAC 比对后，还包括：

通知短信中心向终端下发短信提醒消息，并通过所述终端返回的认证确认消息判断用户是否为仿冒用户。

7、如权利要求 6 所述的方法，其特征在于，所述方法还包括，当用户为仿冒用户时，对用户进行下线处理，并清除所述终端的 MAC 地址与用户名和密码的对应关系。

8、如权利要求 6-7 任一所述的方法，其特征在于，还包括：

携带用于指示“本次认证是否为 MAC 认证”的标识，作为是否进行短信确认流程的依据，当该标识指示本次认证为 MAC 认证时，则通知短信中心向终端下发短信提醒消息，并通过所述终端返回的认证确认消息判断用户是否为仿冒用户；否则，不通知短信中心下发短信消息。

9、如权利要求 1 所述的方法，其特征在于，还包括：

获取终端在 WLAN 中的位置信息以及终端在移动蜂窝网中的位置信息；

根据预先配置的 WLAN 部署的位置信息与移动蜂窝网部署的位置信息的对应关系对获取到的终端在 WLAN 中的位置信息与终端在移动蜂窝网中的位置信息进行匹配，判断是否满足预先配置的 WLAN 部署的位置信息与移动蜂窝网部署的位置信息的对应关系，以判断用户是否为仿冒用户。

10、如权利要求 9 所述的方法，其特征在于，所述获取终端在 WLAN 中的位置信息以及终端在移动蜂窝网中的位置信息包括：

通过 Portal 协议或者半径 Radius 协议或者直径 Diameter 协议从无线接入服务器获取终端在 WLAN 中的位置信息，所述终端在在 WLAN 中的位置信息包括 AP 标识或 AP 位置信息；

通过 MAP 接口的 ATI 消息向位置归属寄存器 HLR 发送获取用户信息的请求，使得所述 HLR 收到请求后通过 MAP 接口的 PSI 消息向移动交换中心 MSC 发送获取用户信息的请求，使得所述 MSC 收到所述 HLR 发送的请求后通过 PSI 寻呼获取终端的用户信息，所述终端的用户信息中包括位置区及小区位置信息；根据所述用户信息中包括的位置区及小区位置信息获取终端在移动蜂窝网中的位置信息；或者通过 MAP 接口的 SRI 消息向所述 HLR 获取用户路由信息，所述用户路由信息包括位置区信息，根据所述路由信息中的位置区信息获取终端在移动蜂窝网中的位置信息。

11、如权利要求 9-10 任一所述的方法，其特征在于，还包括：

携带用于指示“本次认证是否为 MAC 认证”的标识，以作为位置匹配单元是否进行位置匹配操作的依据，当该标识指示本次认证为 MAC 认证时，位置匹配单元后续进行位置匹配操作；否则，不进行位置匹配操作；

所述位置匹配操作包括如权利要求 9 所述的操作。

12、一种基于 MAC 地址的 WLAN 认证装置，其特征在于，所述装置包括，

获取模块，用于当终端接入无线局域网 WLAN 时，获取该终端的介质访问控制 MAC 地址；

认证模块，用于预设的 MAC 地址对通过获取模块 501 获取的终端的 MAC 地址进行比对，并完成 WLAN 认证；或者，所述认证模块 502 用于根据所述终端首次接入 WLAN 时获取的终端 MAC 地址与用户名和密码的对应关系查找该终端 MAC 地址对应的用户名和密码，将查找到的用户名和密码发送给认证中心，以使认证中心对所述终端进行 WLAN 认证。

13、如权利要求 12 所述的装置，其特征在于，所述装置还包括对应关系建立模块，所述对应关系建立模块包括接收单元和建立单元；

所述接收单元用于接收无线接入服务器发送的终端的 MAC 地址，并接收所述终端发送的用户名和密码，其中，所述无线接入服务器包括宽带远程接入服务器 BRAS，或者存取控制器 AC，或者无线接入点 AP；

所述建立单元用于根据所述终端的 MAC 地址，建立所述终端的 MAC 地址与用户名和密码的对应关系。

14、如权利要求 12 所述的装置，其特征在于，所述装置还包括短信判断模块，用于通知短信中心向终端下发短信提醒消息，并通过所述短信中心返回的认证确认消息判断用户是否为仿冒用户。

15、如权利要求 12 所述的装置，其特征在于，还包括：

位置获取模块，用于获取终端在 WLAN 中的位置信息以及终端在移动蜂窝网中的位置信息；

位置判断模块，用于根据预先配置的 WLAN 部署的位置信息与移动蜂窝网部署的位置信息的对应关系对获取到的终端在 WLAN 中的位置信息与终端在移动蜂窝网中的位置信息进行匹配，判断是否满足预先配置的 WLAN 部署的位置信息与移动蜂窝网部署的位置信息的对应关系，以判断用户是否为仿冒用户。

16、如权利要求 15 所述的装置，其特征在于：

所述位置获取模块包括：

WLAN 位置获取模块，用于通过 Portal 协议或者半径 Radius 协议或者直径 Diameter 协议从无线接入服务器获取终端在 WLAN 中的位置信息，所述终端在在 WLAN 中的位置信息包括 AP 标识或 AP 位置信息；

移动蜂窝网位置获取模块，用于通过 MAP 接口的 ATI 消息向位置归属寄存器 HLR

发送获取用户信息的请求，使得所述 HLR 收到请求后通过 MAP 接口的 PSI 消息向移动交换中心 MSC 发送获取用户信息的请求，使得所述 MSC 收到所述 HLR 发送的请求后通过 PSI 寻呼获取终端的用户信息，所述终端的用户信息中包括位置区及小区位置信息；根据所述用户信息中包括的位置区及小区位置信息获取终端在移动蜂窝网中的位置信息；或者通过 MAP 接口的 SRI 消息向所述 HLR 获取用户路由信息，所述用户路由信息包括位置区信息，根据所述路由信息中的位置区信息获取终端在移动蜂窝网中的位置信息。

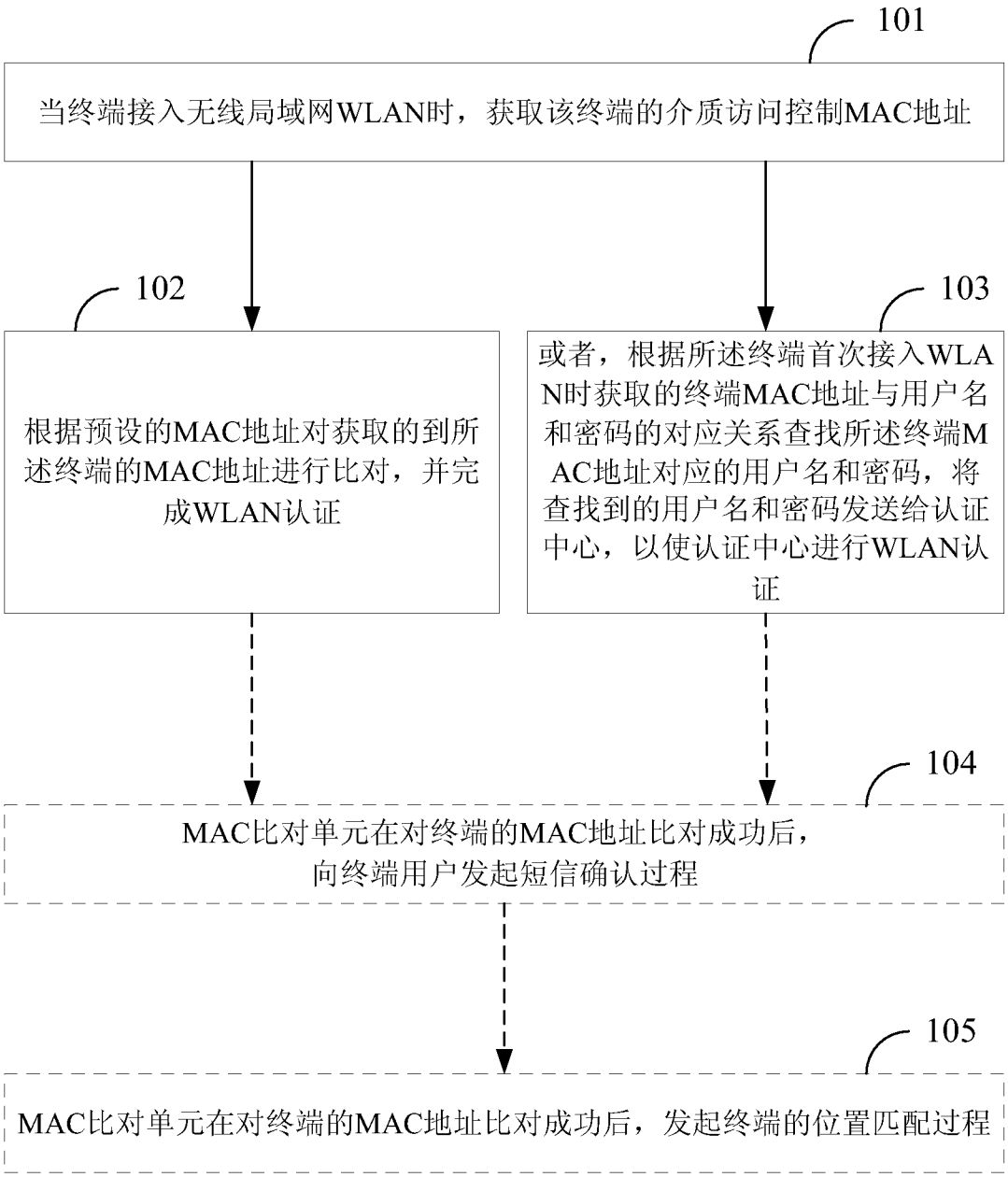

101
当终端接入无线局域网WLAN时，获取该终端的介质访问控制MAC地址
102
根据预设的MAC地址对获取的到所述终端的MAC地址进行比对，并完成WLAN认证
103
或者，根据所述终端首次接入WLAN时获取的终端MAC地址与用户名和密码的对应关系查找所述终端MAC地址对应的用户名和密码，将查找到的用户名和密码发送给认证中心，以使认证中心进行WLAN认证
104
MAC比对单元在对终端的MAC地址比对成功后，向终端用户发起短信确认过程
105
MAC比对单元在对终端的MAC地址比对成功后，发起终端的位置匹配过程

图 1

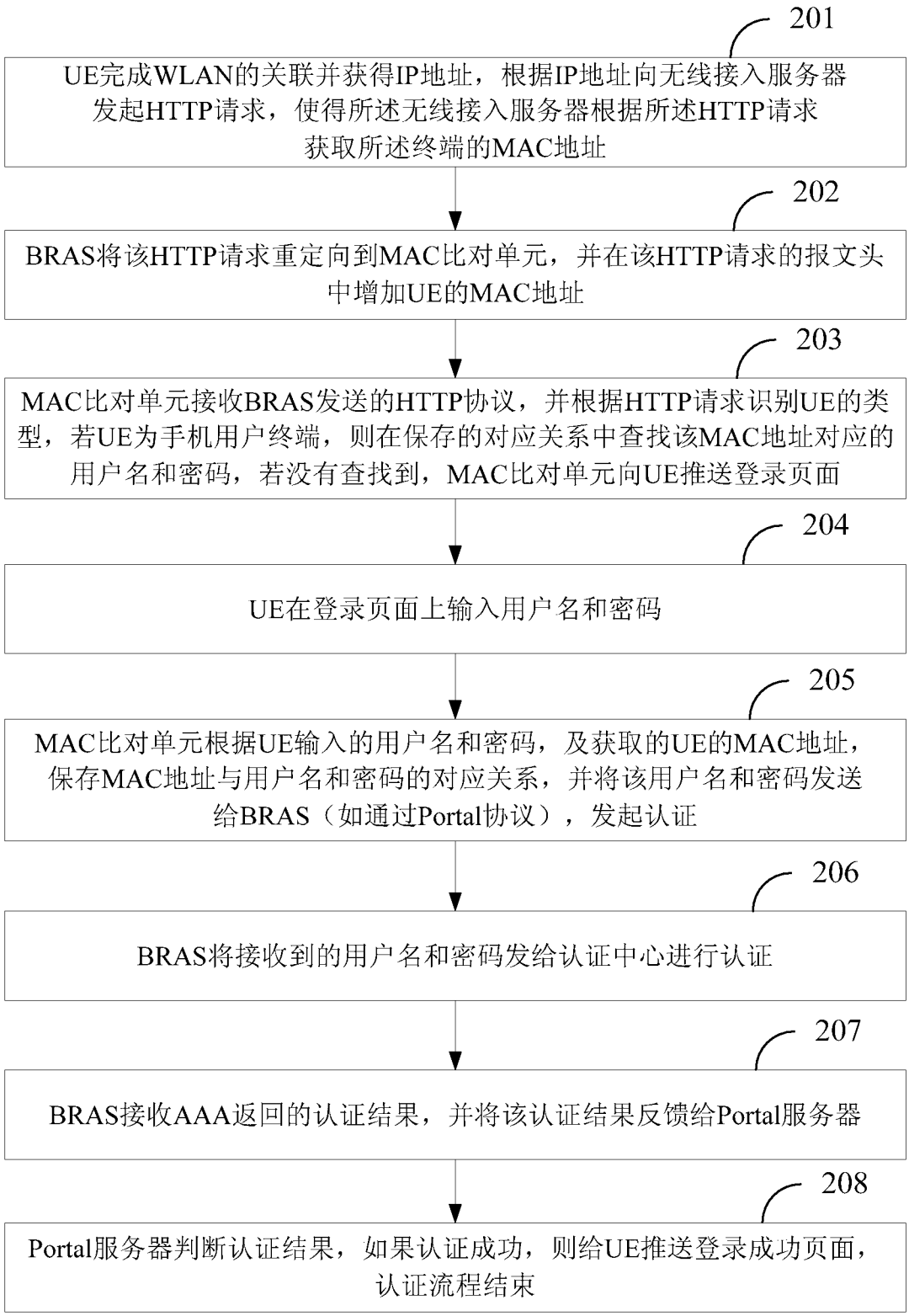

201
UE完成WLAN的关联并获得IP地址，根据IP地址向无线接入服务器发起HTTP请求，使得所述无线接入服务器根据所述HTTP请求获取所述终端的MAC地址
202
BRAS将该HTTP请求重定向到MAC比对单元，并在该HTTP请求的报文头中增加UE的MAC地址
203
MAC比对单元接收BRAS发送的HTTP协议，并根据HTTP请求识别UE的类型，若UE为手机用户终端，则在保存的对应关系中查找该MAC地址对应的用户名和密码，若没有查找到，MAC比对单元向UE推送登录页面
204
UE在登录页面上输入用户名和密码
205
MAC比对单元根据UE输入的用户名和密码，及获取的UE的MAC地址，保存MAC地址与用户名和密码的对应关系，并将该用户名和密码发送给BRAS（如通过Portal协议），发起认证
206
BRAS将接收到的用户名和密码发给认证中心进行认证
207
BRAS接收AAA返回的认证结果，并将该认证结果反馈给Portal服务器
208
Portal服务器判断认证结果，如果认证成功，则给UE推送登录成功页面，认证流程结束

图 2


301
手机用户终端基于Web浏览器完成WLAN的关联并获得IP地址，根据IP地址向BRAS发起HTTP请求
302
BRAS将该HTTP请求重定向到MAC比对单元，并在该HTTP请求的报文头中增加UE的MAC地址
303
MAC比对单元接收BRAS发送的HTTP协议，并根据HTTP请求识别UE的类型，若UE为手机用户终端，则在预设的或终端首次接入时获取的对应关系中查找MAC地址对应的用户名和密码，并将查找到的用户名和密码发送给BRAS
304
BRAS将用户名和密码发送给AAA，以使AAA进行WLAN认证
305
AAA进行WLAN认证，并向BRAS返回认证结果
306
BRAS接收AAA返回的认证结果，并将该认证结果反馈给MAC比对单元
307
MAC比对单元判断认证结果，如果认证成功，通知短信中心向UE下发短信提醒消息
308
短信中心向UE下发短信提醒消息
309
UE根据收到的短信提醒消息，向短信中心返回认证确认消息
310
短信中心根据接收到的认证确认消息通知MAC比对单元
311
MAC比对单元给UE推送登录成功页面，认证流程结束

图 3

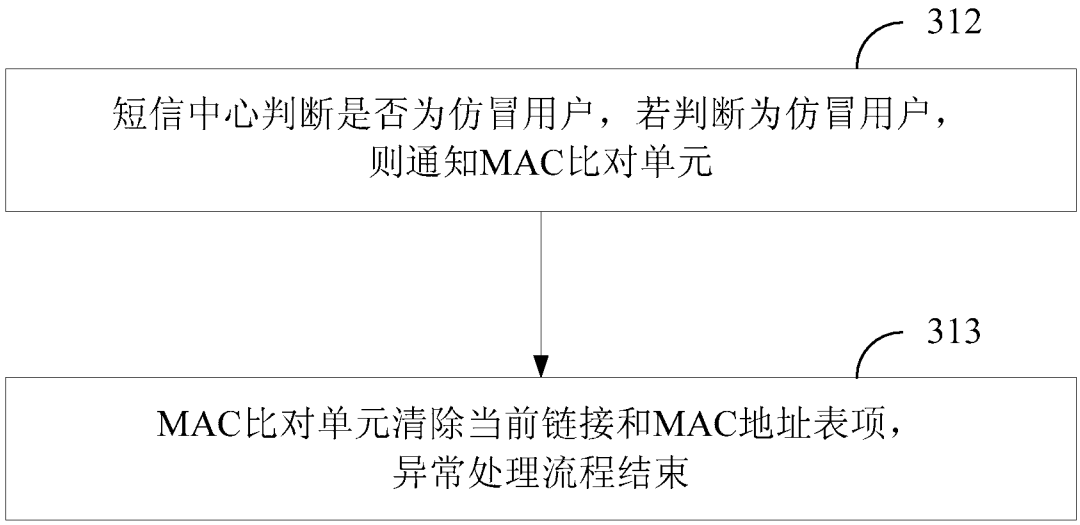

312
短信中心判断是否为仿冒用户，若判断为仿冒用户，则通知MAC比对单元
313
MAC比对单元清除当前链接和MAC地址表项，异常处理流程结束

图 4

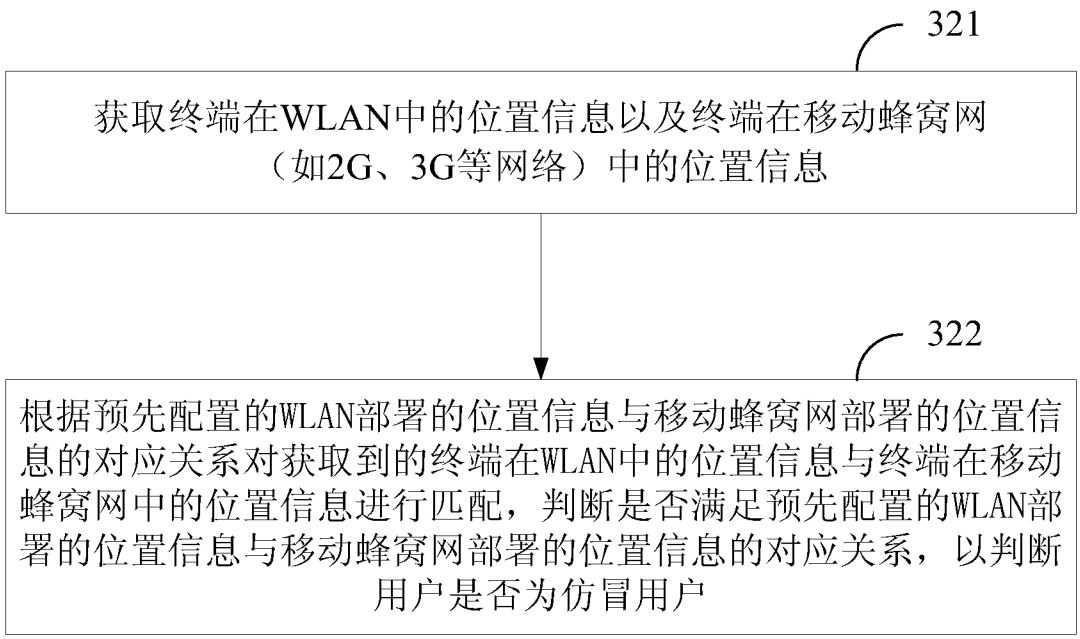

321
获取终端在WLAN中的位置信息以及终端在移动蜂窝网（如2G、3G等网络）中的位置信息
322
根据预先配置的WLAN部署的位置信息与移动蜂窝网部署的位置信息的对应关系对获取到的终端在WLAN中的位置信息与终端在移动蜂窝网中的位置信息进行匹配，判断是否满足预先配置的WLAN部署的位置信息与移动蜂窝网部署的位置信息的对应关系，以判断用户是否为仿冒用户

图 5

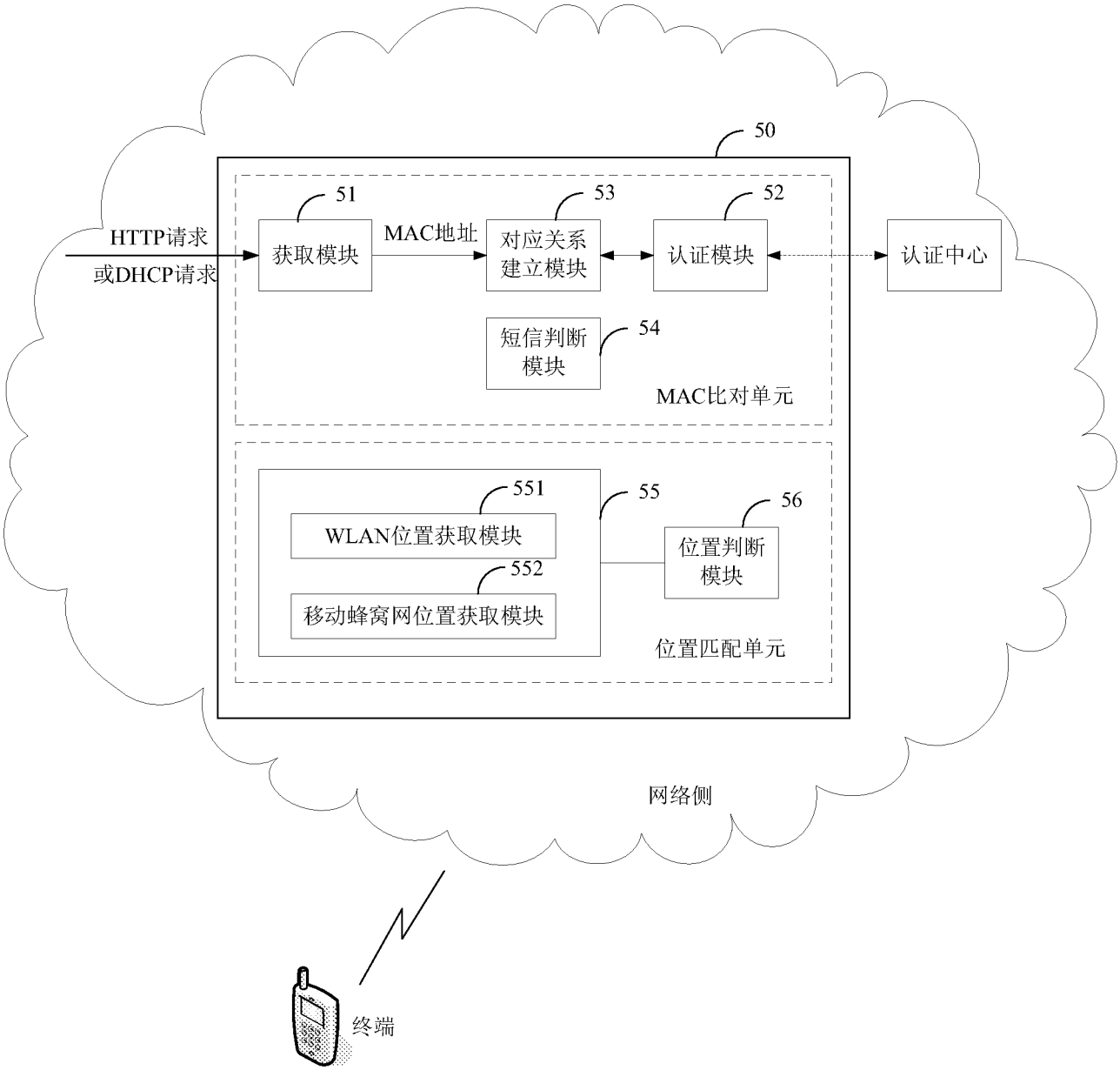

50
51
53
52
HTTP请求
或DHCP请求
获取模块
MAC地址
对应关系
建立模块
认证模块
认证中心
短信判断
模块
54
MAC比对单元
551
55
56
WLAN位置获取模块
位置判断
模块
552
移动蜂窝网位置获取模块
位置匹配单元
网络侧
终端

图 6

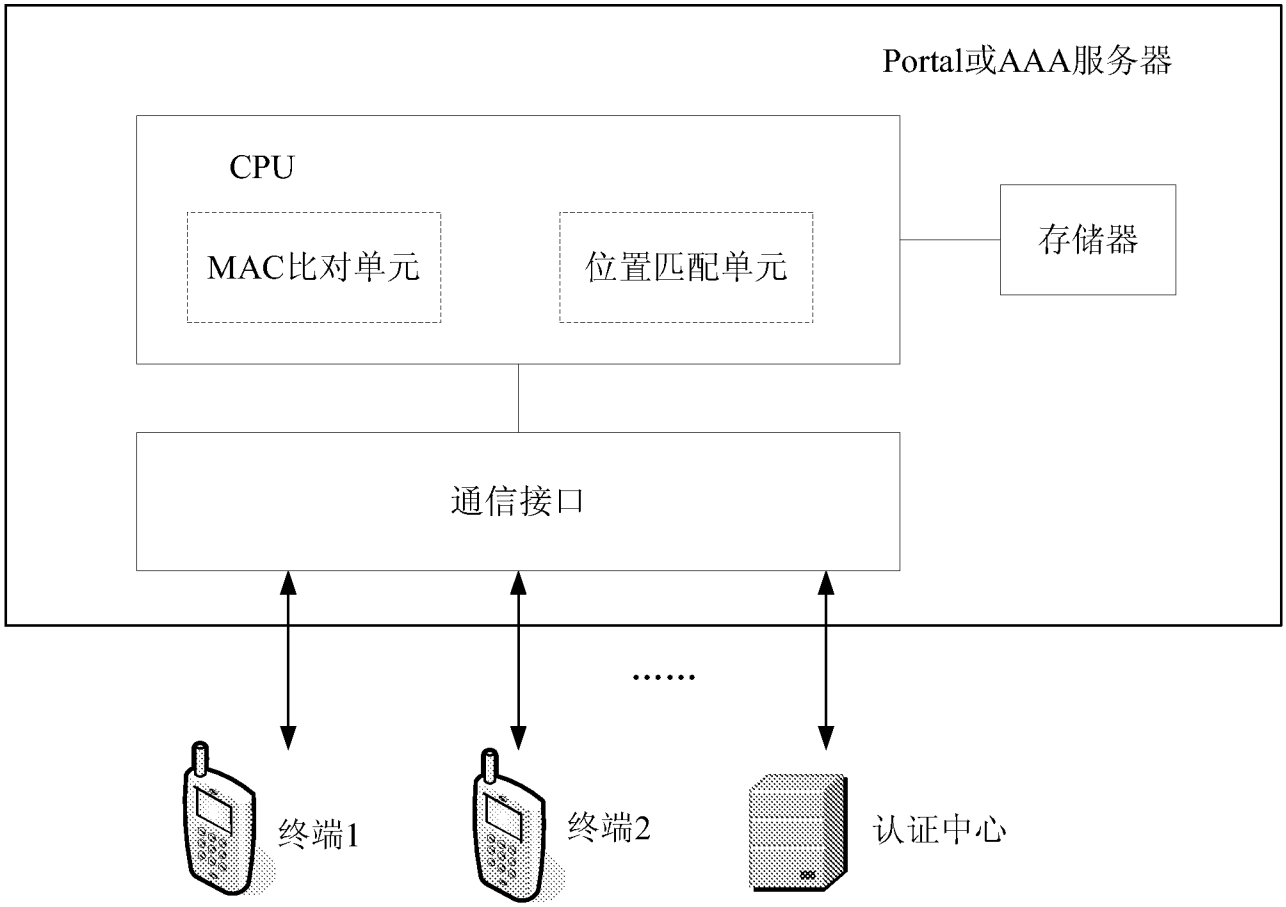


图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/075754

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/32(2006.01)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)

IPC: H04Q; H04B; H04M; 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)

DWPI, CPRS, CNKI: wlan, mac, address, user w name, password, ip, interface, sms, short w message, location, local w area w network, lan

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1842000A (HUAWEI TECHNOLOGIES CO LTD) 04 Oct. 2006 (04. 10. 2006) Page 6 paragraphs 7-8, page 7 paragraph 8 of the description	1, 4, 6, 12, 14
Y		4
A		2-3, 5, 7-11, 13, 15-16
X	CN101651548A (CHINA TELECOM CORP LTD) 17 Feb. 2010 (17.02.2010) Page 6 paragraph 2 and paragraphs 5-6 of the description, claim 1	1, 6, 12, 14
Y		4
A		2-3, 5, 7-11, 13, 15-16
A	CN102143353A (HON HAI PRECISION IND CO LTD et al.) 03 Aug. 2011 (03.08.2011) The whole document	1-10

☐ 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
25 Feb. 2012(25.02.2012)	**22 Mar. 2012 (22.03.2012)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer WANG, Ju Telephone No. (86-10)62411392

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2011/075754

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1842000A	04. 10. 2006	None	
CN101651548A	17.02.2010	None	
CN102143353A	03.08.2011	US2011187872A1	04.08.2011

国际检索报告

国际申请号
PCT/CN2011/075754

A. 主题的分类

H04L9/32(2006.01)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)

IPC：H04Q; H04B; H04M; 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）)

DWPI: wlan, mac, address, user w name, password, ip, interface, sms, short w message, location, local w area w network, lan

CPRS, CNKI:无线局域网,WLAN, MAC, 地址, 用户名, 密码, 认证, IP, 接口, 短信, 短消息, 老化, 位置, 失效

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
X	CN1842000A (华为技术有限公司) 04.10 月 2006 (04. 10. 2006) 说明书第 6 页第 7-8 段、第 7 页第 8 段	1，4，6，12，14
Y		4
A		2-3，5，7-11，13，15-16
X	CN101651548A (中国电信股份有限公司) 17.2 月 2010 (17.02.2010) 说明书第 6 页第 2、5-6 段、权利要求 1	1，6，12，14
Y		4
A		2-3，5，7-11，13，15-16
A	CN102143353A (鸿海精密工业股份有限公司等) 03.8 月 2011 (03.08.2011）	1-10

☐ 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
25.2 月 2012(25.02.2012)	**22.3 月 2012 (22.03.2012)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 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 王菊 电话号码：(86-10) **62411392**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2011/075754

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1842000A	04. 10. 2006	无	
CN101651548A	17.02.2010	无	
CN102143353A	03.08.2011	US2011187872A1	04.08.2011