

WO 2010/148609 A1

(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
2010 年 12 月 29 日 (29.12.2010)(10) 国际公布号
WO 2010/148609 A1

(51) 国际专利分类号:

H04W 12/08 (2009.01)

(21) 国际申请号:

PCT/CN2009/075505

(22) 国际申请日:

2009 年 12 月 11 日 (11.12.2009)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

200910148675.X 2009 年 6 月 25 日 (25.06.2009) CN

(71) 申请人(对除美国外的所有指定国): 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: 及

(75) 发明人/申请人(仅对美国): 高滨 (GAO, Bin) [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)。

(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, 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, 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): ARIP (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: ACCESS METHOD AND SYSTEM FOR CELLULAR MOBILE COMMUNICATION NETWORK

(54) 发明名称: 一种蜂窝移动通信网络的接入方法和系统

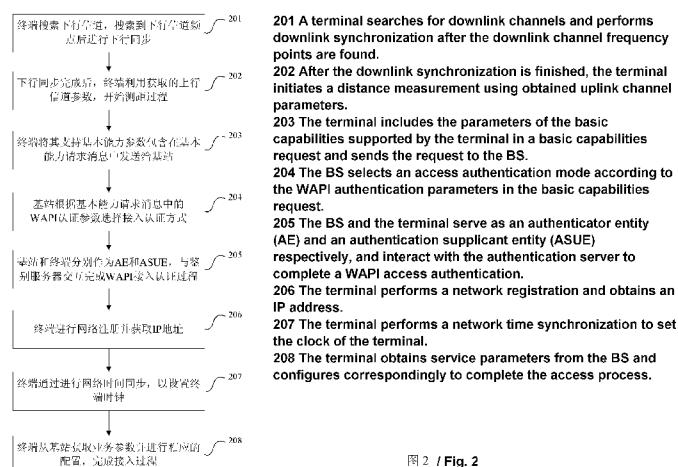


图 2 / Fig. 2

(57) Abstract: An access method and a system for cellular mobile communication networks are provided. The method includes the following steps: after a terminal finishes a distance measurement with the BS, the terminal performs a basic capabilities negotiation with the BS. After the basic capabilities negotiation is finished, the BS performs a WLAN Authentication and Privacy Infrastructure (WAPI) access authentication with the terminal. After the access authentication is finished, the terminal performs the subsequent access process to access the cellular mobile communication network. The WAPI access authentication includes the following steps: the terminal sends the BS an access authentication request packet, which includes the certificate of the terminal and the signature of the terminal. After receiving the access authentication request packet, the BS authenticates the signature of the terminal. After a successful signature authentication, the BS includes the certificate of the terminal in a certificate authentication request packet and sends the packet to an authentication server for authentication. After a successful authentication of the certificate of the terminal, the BS sends the terminal an access authentication response packet and negotiates with the terminal for a unicast session key.

[见续页]

**本国际公布：**

- 包括国际检索报告(条约第 21 条(3))。

(57) 摘要：

一种蜂窝移动通信网络的接入方法和系统，该方法包括：终端与基站完成测距过程后，与基站进行基本能力协商，基本能力协商过程完成后，基站与终端执行 WAPI 接入认证过程；接入认证过程完成后，终端执行后续的接入流程，接入到蜂窝移动通信网络；所述 WAPI 接入认证过程包括：终端向基站发送接入鉴别请求分组，该分组中包含：终端的证书及终端的签名；接收到接入鉴别请求分组后，基站对终端的签名进行认证，签名认证成功后，基站将终端的证书包含在证书鉴别请求分组中发送给鉴别服务器进行验证；终端的证书验证成功后，基站向终端发送接入鉴别响应分组，并与终端协商得到单播会话密钥。

一种蜂窝移动通信网络的接入方法和系统

技术领域

本发明涉及通信领域，尤其涉及一种蜂窝移动通信网络的接入方法和系
5 统。

背景技术

WAPI (WLAN Authentication Privacy Infrastructure, 无线局域网鉴别与保
密基础结构) 是一种应用于无线局域网 (Wireless Local Area Networks, 简称
10 WLAN) 系统的接入认证协议。 WAPI 将基于三元对等鉴别的访问控制方法
应用于无线局域网领域，保障了合法移动终端 (Mobile Terminal, 简称为 MT)
通过合法的接入点 (Access Point, 简称为 AP) 接入网络，并实现移动终端和
接入点间的保密通信。

基于 WAPI 协议的 WLAN 安全网络由： ASUE (Authentication Supplicant
15 Entity, 鉴别请求者实体，通常驻留在移动终端中) 、 AE (Authenticator Entity,
鉴别器实体，通常驻留在接入点中) 和 ASE (Authentication Service Entity,
鉴别服务实体，通常驻留在鉴别服务器中) 三个实体组成，利用公开密码体
系完成移动终端和接入点间的双向认证，在认证过程中移动终端和 AP 采用
20 椭圆曲线密码算法协商出会话密钥，并对通信过程中的数据采用国家密码主
管部门指定的加密算法完成加密，安全性极高。同时， WAPI 还支持在通信
过程中经过一定时间间隔后或传输了一定数量的数据包后，更新会话密钥，
极大地提高了数据传输的安全性。

根据 WAPI 协议，鉴别服务器 (AS) 负责证书的颁发、验证与吊销等处
理，移动终端 (MT) 与无线接入点 (AP) 上都安装有 AS 颁发的公钥证书，
25 作为自己的数字身份凭证。当移动终端关联至 AP 后，在使用或访问网络之
前必须通过鉴别服务器进行双方的身份验证，根据验证的结果，持有合法证
书的移动终端才能接入持有合法证书的 AP, 也就是说才能通过 AP 访问网络。
这样不仅可以防止非法移动终端接入 AP 访问网络并占用网络资源，而且还能
以防止移动终端接入非法 AP 而造成信息泄漏。

下一代基于 IP (Internet Protocol, 因特网协议) 的蜂窝移动通信网络系统，如 WiMAX (Worldwide Interoperability for Microwave Access, 微波接入全球互操作性认证)，LTE (Long Term Evolution, 长期演进) 等系统中，接入认证由在 IP 网侧单独设置的一台或一组 AAA (Authentication Authorization 5 Accounting, 鉴权授权计费) 服务器来完成，AAA 服务器可以对终端进行单向认证，或基于 EAP (Extensible Authentication Protocol, 扩展认证协议) 与终端进行双向认证。

目前，有许多运营商同时拥有基于 IP 的蜂窝移动通信网络系统和无线局域网系统，由于需要针对不同的系统采用不同的认证机制，运营商需要部署 10 不同类型的鉴别服务器，增加了运营商的硬件成本，同时也不利于网络融合、业务融合以及网络和业务的整体管理。

同时，随着双模终端的普及，如果能够采用相同的接入认证机制接入蜂窝无线通信系统和无线局域网系统，就可以在双模终端中设置单一的接入认证模块，以降低双模终端的软硬件成本，且更易于实现在不同的接入网络之 15 间的切换。

将 WAPI 作为蜂窝移动通信网络系统和无线局域网系统的统一认证机制是满足运营商和用户的上述需求的一种可行方案。但是，现有技术中还没有在基于 IP 的蜂窝无线通信系统中实现 WAPI 的技术方案。

20 发明内容

本发明所要解决的技术问题是，克服现有技术的不足，提供一种蜂窝移动通信网络的接入方法和系统，以在基于 IP 的蜂窝无线通信系统中实现 WAPI 接入认证。

为了解决上述问题，本发明提供一种蜂窝移动通信网络的接入方法，该 25 方法包括：

终端与基站完成测距过程后，与基站进行基本能力协商，基本能力协商过程完成后，基站与终端执行无线局域网鉴别与保密基础结构 WAPI 接入认证过程；接入认证过程完成后，终端执行后续的接入流程，接入到蜂窝移动

通信网络；

所述 WAPI 接入认证过程包括：

终端向基站发送接入鉴别请求分组，该分组中包含：终端的证书及终端的签名；

5 接收到接入鉴别请求分组后，基站对终端的签名进行认证，签名认证成功后，基站将终端的证书包含在证书鉴别请求分组中发送给鉴别服务器进行验证；

终端的证书验证成功后，基站向终端发送接入鉴别响应分组，并与终端进行单播会话密钥协商得到单播会话密钥。

10 进一步地，所述证书鉴别请求分组中还包含基站的证书；

所述 WAPI 接入过程还包括：

鉴别服务器还对所述基站的证书进行验证，并将证书验证结果和鉴别服务器的签名通过基站发送给终端；

15 终端根据证书验证结果和鉴别服务器的签名判断对基站的证书是否验证成功。

进一步地，所述方法还具有以下特征：

发送所述接入鉴别请求分组前，终端还生成用于椭圆曲线密码体制的戴菲-赫曼 ECDH 交换的临时公钥 px 和临时私钥 sx，并将所述 px 包含在所述接入鉴别请求分组中发送给基站；

20 对所述终端的证书验证成功后，基站还生成用于 ECDH 交换的临时私钥 sy 和临时公钥 py，使用所述 px 和 sy 进行 ECDH 计算，生成基密钥 BK，并将所述 py 包含在所述接入鉴别响应分组中发送给终端；

终端接收到所述接入鉴别响应分组后，使用所述 py 和 sx 进行 ECDH 计算，生成基密钥 BK；

25 终端和基站使用所述基密钥 BK 进行单播会话密钥协商得到所述单播会话密钥。

进一步地，终端和基站采用如下方式进行所述基本能力协商：

终端向基站发送基本能力请求消息，该消息中包含终端是否支持 WAPI 接入认证的信息；

基站根据基本能力请求消息中包含的所述信息判断是否启动与终端的所述 WAPI 接入认证过程。

5 进一步地，基站与终端采用如下方式进行单播会话密钥协商得到单播会话密钥：

基站生成随机数 N_1 和用于 ECDH 交换的临时私钥 sy 和临时公钥 py ，并向终端发送单播密钥协商请求分组，该分组中包含所述 N_1 和 py ；

10 接收到所述单播密钥协商请求分组后，终端生成随机数 N_2 和用于 ECDH 交换的临时私钥 sx 和临时公钥 px ，对 py 和 sx 进行 ECDH 计算，得到基密钥 BK ，使用基密钥 BK 、所述 N_1 和 N_2 生成所述单播会话密钥；

终端向基站发送单播密钥协商响应分组，该分组中包含所述 N_2 和 px ；

接收到所述单播密钥协商响应分组后，基站对 px 和 sy 进行 ECDH 计算，得到基密钥 BK ，使用基密钥 BK 、所述 N_1 和 N_2 生成所述单播会话密钥。

15 本发明还提供一种支持蜂窝移动通信网络接入的基站，所述基站设置成：与终端完成测距过程后，与所述终端进行基本能力协商；

在基本能力协商过程完成后，接收所述终端发送的接入鉴别请求分组，该分组中包含：终端的证书及终端的签名；

20 在接收到所述接入鉴别请求分组后，对所述终端的签名进行认证，签名认证成功后，将终端的证书包含在证书鉴别请求分组中发送给鉴别服务器进行验证；

在鉴别服务器对终端的证书验证成功后，向终端发送接入鉴别响应分组，并与终端进行单播会话密钥协商；以及

25 在单播会话密钥协商完成后，与终端交互，完成后续的接入流程，使终端接入到蜂窝移动通信网络。

进一步地，所述基站还可设置成：在鉴别服务器对所述终端的证书验证

成功后，生成用于 ECDH 交换的临时私钥 sy 和临时公钥 py ，使用所述 px 和 sy 进行 ECDH 计算，生成基密钥 BK ，并将所述 py 包含在所述接入鉴别响应分组中发送给所述终端。

进一步地，所述基站还可设置成：根据基本能力协商过程中所述终端发送的基本能力请求消息中包含的用于标识所述终端是否支持 WAPI 接入认证的信息来判断是否启动与所述终端的所述 WAPI 接入认证过程。
5

本发明还提供一种支持蜂窝移动通信网络接入的终端，所述终端设置成：

在与基站完成测距过程后，与基站进行基本能力协商；

在基本能力协商过程完成后，向所述基站发送接入鉴别请求分组，该分
10 组中包含：终端的证书及终端的签名；

在鉴别服务器对所述终端的证书验证成功后，接收基站向所述终端发送的接入鉴别响应分组，并与所述基站进行单播会话密钥协商；以及

在单播会话密钥协商完成后，与基站交互，完成后续的接入流程，接入
到蜂窝移动通信网络。

15 进一步地，所述终端还可设置成：发送所述接入鉴别请求分组前，生成用于椭圆曲线密码体制的戴菲-赫曼 ECDH 交换的临时公钥 px 和临时私钥 sx ，并将所述 px 包含在所述接入鉴别请求分组中发送给所述基站；以及接收到所
述接入鉴别响应分组后，使用所述 py 和 sx 进行 ECDH 计算，得到基密钥 BK ；

本发明还提供一种支持蜂窝移动通信网络接入的鉴别服务器，所述鉴别
20 服务器设置成：对终端的证书进行验证，以及对基站的证书进行验证，并将对基站的证书的验证结果和鉴别服务器的签名通过基站发送给终端。

本发明还提供一种蜂窝移动通信网络的接入系统，该系统包含：如上所述的基站、如上所述的终端、及如上所述的鉴别服务器，其中：

所述基站与所述终端设置成采用如下方式进行单播会话密钥协商得到单
25 播会话密钥：

所述基站生成随机数 N_1 和用于 ECDH 交换的临时私钥 sy 和临时公钥 py ，

并向所述终端发送单播密钥协商请求分组，该分组中包含所述 N_1 和 py ；

接收到所述单播密钥协商请求分组后，所述终端生成随机数 N_2 和用于 ECDH 交换的临时私钥 sx 和临时公钥 px ，对 py 和 sx 进行 ECDH 计算，得到基密钥 BK ，使用基密钥 BK 、所述 N_1 和 N_2 生成所述单播会话密钥；

5 所述终端向基站发送单播密钥协商响应分组，该分组中包含所述 N_2 和 px ；

接收到所述单播密钥协商响应分组后，所述基站对 px 和 sy 进行 ECDH 计算，得到基密钥 BK ，使用基密钥 BK 、所述 N_1 和 N_2 生成所述单播会话密钥。

10 综上所述，本发明将基站作为 WAPI 协议中的 AE，蜂窝移动通信终端作为 WAPI 协议中的 ASUE，在蜂窝移动通信网络系统中实现了基于 WAPI 的接入认证，降低了运营商的运营和管理成本。

附图概述

15 图 1 是统一采用 WAPI 作为接入认证协议的蜂窝移动通信网络系统和无线局域网系统的结构示意图；

图 2 是本发明实施例 LTE 网络的接入方法流程图；

图 3 是 LTE 终端与基站和鉴别服务器交互完成 WAPI 接入认证的方法流程图。

20

本发明的较佳实施方式

本发明的核心思想是，将基站作为 WAPI 协议中的 AE，蜂窝移动通信终端作为 WAPI 协议中的 ASUE，在蜂窝移动通信网络系统中实现基于 WAPI 的接入认证。

25 此外，为了保持兼容性，需要在蜂窝移动通信网络系统中保留原有的接入认证方式，因此，基站需要判断终端是否支持 WAPI 协议，并根据判断结果启动相应的接入认证方式。

下面将结合附图和实施例对本发明进行详细描述。

图 1 是统一采用 WAPI 作为接入认证协议的蜂窝移动通信网络系统和无线局域网系统的结构示意图；如图 1 所示，蜂窝移动通信网络系统中采用 WAPI 作为接入认证协议时，蜂窝移动通信网络系统可以和无线局域网系统共用相同的鉴别服务器。

5 以下将对蜂窝移动通信网络系统中终端接入网络的过程中，终端、基站和鉴别服务器的功能，以及相互之间的消息交互关系进行详细描述。无线局域网系统中终端接入网络的过程与现有技术相同，本文从略。

图 2 是本发明实施例 LTE 网络的接入方法流程图，具体包括如下步骤：

201：LTE 终端搜索下行信道，搜索到下行信道频点后进行下行同步；

10 202：下行同步完成后，LTE 终端利用获取的上行信道参数，开始测距过程；

203：LTE 终端根据测距获得的信息，将其支持基本能力参数包含在基本能力请求消息（SS Basic Capability Request，简称为 SBC-REQ）中发送给基站，以启动基本能力协商过程；

15 如果 LTE 终端同时支持 EAP 和 WAPI，上述基本能力参数中包含 WAPI 认证参数和 EAP 认证参数。

WAPI 认证参数中包含：LTE 终端支持的 WAI (WLAN Authentication Infrastructure，无线局域网鉴别基础结构) 鉴别和密钥管理方式、LTE 终端支持的单播加密算法等，具体描述如下：

20 WAI 鉴别和密钥管理方式分为以下两种：WAI 证书鉴别和密钥管理方式，WAI 预共享密钥鉴别和密钥管理方式；

其中，如果采用 WAI 证书鉴别和密钥管理方式，LTE 终端需要向基站提供数字证书，与基站和鉴别服务器交互完成证书鉴别过程，并在证书鉴别过程中协商基密钥（BK）；如果采用 WAI 预共享密钥鉴别和密钥管理方式，25 LTE 终端无需进行证书鉴别过程，基密钥由 LTE 终端和基站的预共享密钥直接导出。

单播加密算法包含了 LTE 终端支持的一种或多种单播加密算法；例如 SMS4 算法等；

鉴别服务器列表字段包含了 LTE 终端所支持（信任）的鉴别服务器的标识。

204: 基站接收到基本能力请求消息后，判断其中是否包含 WAPI 认证参数：

- 5 如果基本能力请求消息中未包含 WAPI 认证参数，基站获知该 LTE 终端不支持 WAPI，因此向 LTE 终端返回包含 EAP 认证参数的基本能力应答消息（SS Basic Capability Response，简称为 SBC-RSP），并在后续步骤中采用现有技术中的 EAP 认证方式对 LTE 终端进行认证，并完成后续的接入过程，本流程结束；
- 10 如果基本能力请求消息中包含 WAPI 认证参数，则基站判断其是否支持终端提供的 WAPI 认证参数，如果不支持，则向 LTE 终端返回包含 EAP 认证参数的基本能力应答消息（SBC-RSP），并在后续步骤中采用现有技术中的 EAP 认证方式对 LTE 终端进行认证，并完成后续的接入过程，本流程结束；如果基站支持终端提供的 WAPI 认证参数，则向 LTE 终端返回包含基站最终选定的 WAPI 认证参数（包括基站选定的 WAI 鉴别和密钥管理方式、单播加密算法）的基本能力应答消息（SBC-RSP），并在后续步骤中采用 WAPI 接入认证方式对 LTE 终端进行接入认证。

20 基站支持终端提供的 WAPI 认证参数是指：基站支持终端提供的 WAPI 认证参数中包含的一种或多种鉴别和密钥管理方式；且基站支持终端提供的 WAPI 认证参数中包含的一种或多种单播加密算法；且基站可以将后续的证书鉴别请求转发到 LTE 终端信任的鉴别服务器。

25 需要注意的是，虽然 WAPI 协议中包含 WAI 预共享密钥鉴别和密钥管理方式，但该方式的安全性较差，且需要在基站中预先配置每一终端的预共享密钥，因此基站通常不支持这种鉴别和密钥管理方式。也就是说，如果终端提供的 WAPI 认证参数中不包含 WAI 证书密钥鉴别和密钥管理方式时，基站通常会选择 EAP 认证方式与 LTE 终端完成接入认证。

205: 如果 LTE 终端支持 WAPI 接入认证方式，且基站支持终端提供的 WAPI 认证参数，则基站和 LTE 终端分别作为 WAPI 协议中的 AE 和 ASUE，与鉴别服务器交互完成 WAPI 接入认证过程；

WAPI 接入认证过程的具体步骤如图 3 所示，将在下文中详细描述。

206: 完成 WAPI 接入认证后，LTE 终端进行网络注册，然后启动 DHCP (Dynamic Host Configuration Protocol, 动态主机配置协议) 过程以获取 IP 地址；

5 207: LTE 终端通过 DHCP 过程获取到 IP 地址、网关、DNS (Domain Name System, 域名系统) 等网络层设置后，尝试进行网络时间同步，以设置终端时钟；

208: LTE 终端从基站获取业务参数并进行相应的配置，完成接入过程。

图 3 是 LTE 终端与基站和鉴别服务器交互完成 WAPI 接入认证的方法流程图，WAPI 接入认证方法包括：证书鉴别过程（步骤 301 ~ 309）和单播密钥协商过程（步骤 310 ~ 314）两部分，具体包括如下步骤：

301: 基站向 LTE 终端发送鉴别激活分组，发起证书鉴别过程；

鉴别激活分组中可以包含：基站的证书等字段。

302: 接收到鉴别激活分组后，LTE 终端保存基站的证书，并产生用于 ECDH (椭圆曲线密码体制的 Diffie-Hellman (戴菲-赫曼) 交换) 交换的临时私钥 sx 和临时公钥 px；

303: LTE 终端生成接入鉴别请求分组，并发送给基站；

接入鉴别请求分组中包含：临时公钥 px、LTE 终端的证书等字段，以及 LTE 终端对上述字段的签名值。

20 304: 接收到接入鉴别请求分组后，基站对 LTE 终端的签名进行验证（使用 LTE 终端证书中包含的公钥），若签名验证失败，则丢弃该分组；否则基站生成证书鉴别请求分组，并将其通过 RNC (Radio Network Controller, 无线网络控制器) 和 IP 网络发送给 LTE 终端和基站都信任的鉴别服务器；

证书鉴别请求分组中包含：LTE 终端的证书和基站的证书。

25 305: 鉴别服务器对 LTE 终端的证书和基站的证书进行验证；

306: 鉴别服务器根据对 LTE 终端的证书和基站的证书的验证结果，构造证书鉴别响应分组，并且附加鉴别服务器的签名后将证书鉴别响应分组通

过 IP 网络和 RNC 发送给基站；

307：基站验证鉴别服务器的签名，签名验证成功后，进一步验证对 LTE 终端的证书的验证结果，验证成功后，执行以下操作：

307a：生成用于 ECDH 交换的临时私钥 sy 和临时公钥 py；

5 307b：使用 LTE 终端发送的临时公钥 px 和本地生成的临时私钥 sy 进行 ECDH 计算，生成基密钥 BK。

308：基站向 LTE 终端发送接入鉴别响应分组；

接入鉴别响应分组中包含：临时公钥 py，证书验证结果，鉴别服务器签名，以及基站对上述字段的签名。

10 309：接收到接入鉴别响应分组后，LTE 终端验证鉴别服务器和基站签名以及证书验证结果，如果签名正确，并且鉴别服务器对基站的证书验证成功，则 LTE 终端使用临时公钥 py 和临时私钥 sx 进行 ECDH 计算生成 BK。

需要注意的是，根据 ECDH 的原理，LTE 终端和基站生成的 BK 相同。

15 至此，LTE 终端和基站完成了 WAPI 的证书鉴别过程，并在此过程中协商出了基密钥 BK；此后，LTE 终端和基站可以使用 BK 进行单播密钥协商，生成单播会话密钥，具体包括如下步骤：

310：基站向 LTE 终端发送单播密钥协商请求分组；

单播密钥协商请求分组中包含：BKID 和 N₁ 等参数，其中：

BKID 为基站和 LTE 终端先前协商得到基密钥 BK 的标识符；

20 N₁ 为基站生成的随机数。

311：接收到单播密钥协商请求分组后，LTE 终端生成随机数 N₂，然后计算：

Key=KD-HMAC-SHA256(BK,N₁||N₂||String)；其中：

25 BK 为上述 BKID 所标识的基密钥；KD-HMAC-SHA256 为基于 SHA256 算法的 HMAC (Hashed Message Authentication Code, 散列信息认证码) 算法，也就是一种带密钥 (以 BK 为密钥) 的 HASH (哈希) 算法；String 为一预先设置的字符串；“||”表示字符串连接操作，“||N₁||N₂||String”为

KD-HMAC-SHA256 算法所使用的字符参数。

计算得到 Key 后，LTE 终端将其中的一部分（例如，前 16 个字节）作为单播会话密钥 USK。图 1 中以 T(•) 表示从 Key 中提取（或称为截取）部分字符串的操作。

5 312：LTE 终端向基站发送单播密钥协商响应分组；

单播密钥协商响应分组中包含：BKID、随机数 N₂ 等参数。

313：基站接收到单播密钥协商响应分组后计算：

Key=KD-HMAC-SHA256(BK, ||N₁||N₂||String)，并从中提取 USK。

314：基站向 LTE 终端发送单播密钥协商确认分组，结束单播密钥的协

10 商流程。

至此，基站和 LTE 终端完成了 WAPI 证书鉴别和单播密钥协商过程。

由上可知，基站采用上述方式对 LTE 终端进行接入认证时，鉴别服务器可以同时为蜂窝移动通信网络系统和无线局域网系统提供服务，降低了运营商的运营成本。

15 需要注意的是，除了 LTE 以外，本发明的上述接入认证方法还适用于其它蜂窝移动通信网络系统。

根据本发明的基本原理，上述实施例还可以有多种变换方式，例如：

(一) 考虑到蜂窝移动通信网络系统与无线局域网系统的不同，在系统中设置非法基站（假冒基站）的可能性较小，因此，终端可以不对基站进行证书鉴别；即：步骤 301 中的鉴别激活分组中可以不包含基站的证书；步骤 20 304 中的证书鉴别请求分组中可以不包含基站的证书；步骤 305 中也无需对基站的证书进行验证；步骤 308 中的接入鉴别响应分组中也可以不包含证书验证结果。

(二) 在上述实施例中，基站通过终端发送的基本能力请求消息中包含的 WAPI 认证参数判断终端是否支持 WAPI；在本发明的其它实施例中，终端可以在基本能力请求消息中添加一个标识（可以成为 WAPI 标识）来告知基站其是否支持 WAPI，在这种情况下，基站和终端采用默认的 WAPI 参数（例如，采用 WAI 证书鉴别和密钥管理方式和 SMS4 单播加密算法）进行

WAPI 接入认证及后续的数据加解密；或者当基本能力协商完成后，基站直接向终端发送鉴别激活分组，并设置定时器，若定时器超时时未接收到终端发送的接入鉴别请求分组，则认为终端不支持 WAPI，进而与终端进行 EAP 接入认证。

5 (三) 在上述实施例中，基站和终端在 WAPI 的证书鉴别过程中交换了 ECDH 临时公钥，并协商生成了基密钥 BK，这样做的优点在于减少了消息的交互；

10 在本发明的其他实施例中，可以在 WAPI 的证书鉴别过程中仅完成证书的交换和验证，证书验证成功后再进行 ECDH 临时公钥的交换，并协商生成基密钥 BK。例如：

在步骤 310 的单播密钥协商请求分组中携带随机数 N_1 和基站的临时公钥 py ，以及上述字段的签名值；

15 在步骤 311 中，终端生成随机数 N_2 、临时公钥 px 和临时私钥 sx ，并使用 py 和 sx 进行 ECDH 计算，生成基密钥 BK ，然后使用基密钥 BK 和随机数 N_1 和 N_2 生成单播会话密钥 USK ；

在步骤 312 中，终端将临时公钥 px 和随机数 N_2 一起包含在单播密钥协商响应分组中发送给基站；

在步骤 313 中，基站先使用 px 和 sy 生成 BK ，然后再使用基密钥 BK 和随机数 N_1 和 N_2 生成单播会话密钥 USK 。

20

工业实用性

本发明将基站作为 WAPI 协议中的 AE，蜂窝移动通信终端作为 WAPI 协议中的 ASUE，在蜂窝移动通信网络系统中实现了基于 WAPI 的接入认证，降低了运营商的运营和管理成本。

权利要求书

1、一种蜂窝移动通信网络的接入方法，其包括：

5 终端与基站完成测距过程后，与基站进行基本能力协商，基本能力协商过程完成后，基站与终端执行无线局域网鉴别与保密基础结构 WAPI 接入认证过程；接入认证过程完成后，终端执行后续的接入流程，接入到蜂窝移动通信网络；

所述 WAPI 接入认证过程包括：

10 终端向基站发送接入鉴别请求分组，该分组中包含：终端的证书及终端的签名；

15 接收到接入鉴别请求分组后，基站对终端的签名进行认证，签名认证成功后，基站将终端的证书包含在证书鉴别请求分组中发送给鉴别服务器进行验证；

终端的证书验证成功后，基站向终端发送接入鉴别响应分组，并与终端进行单播会话密钥协商得到单播会话密钥。

20 2、如权利要求 1 所述的方法，其中，

所述证书鉴别请求分组中还包含基站的证书；

所述 WAPI 接入过程还包括：

鉴别服务器对所述基站的证书进行验证，并将证书验证结果和鉴别服务器的签名通过基站发送给终端；

25 终端根据所述证书验证结果和鉴别服务器的签名判断对基站的证书是否验证成功。

3、如权利要求 1 所述的方法，其中，

所述 WAPI 接入认证过程在终端向基站发送接入鉴别请求分组的步骤之前，还包括：终端生成用于椭圆曲线密码体制的戴菲-赫曼 ECDH 交换的临时公钥 px 和临时私钥 sx；

所述接入鉴别请求分组还包括所述 px；

所述 WAPI 接入认证过程在终端的证书验证成功的步骤之后还包括：基站生成用于 ECDH 交换的临时私钥 sy 和临时公钥 py，使用所述 px 和 sy 进行 ECDH 计算，得到基密钥 BK；

所述接入鉴别响应分组包括所述 py；

5 所述 WAPI 接入认证过程还包括：终端接收到所述接入鉴别响应分组后，使用所述 py 和 sx 进行 ECDH 计算，得到所述基密钥 BK；

与终端进行单播会话密钥协商的步骤中，终端和基站使用所述基密钥 BK 协商得到所述单播会话密钥。

4、如权利要求 1 所述的方法，其中，

10 与基站进行基本能力协商的步骤包括：

终端向基站发送基本能力请求消息，该消息中包含终端是否支持 WAPI 接入认证的信息；

基站根据基本能力请求消息中包含的所述信息判断是否启动与终端的所述 WAPI 接入认证过程。

15 5、如权利要求 1 所述的方法，其中，

与终端进行单播密钥协商得到单播会话密钥的步骤包括：

基站生成随机数 N₁ 和用于 ECDH 交换的临时私钥 sy 和临时公钥 py，并向终端发送单播密钥协商请求分组，该分组中包含所述 N₁ 和 py；

接收到所述单播密钥协商请求分组后，终端生成随机数 N₂ 和用于 ECDH 20 交换的临时私钥 sx 和临时公钥 px，对 py 和 sx 进行 ECDH 计算，得到基密钥 BK，使用所得到的基密钥 BK、所述 N₁ 和 N₂ 生成所述单播会话密钥；

终端向基站发送单播密钥协商响应分组，该分组中包含所述 N₂ 和 px；

接收到所述单播密钥协商响应分组后，基站对 px 和 sy 进行 ECDH 计算，25 得到所述基密钥 BK，使用所述基密钥 BK、所述 N₁ 和 N₂ 生成所述单播会话密钥。

6、一种支持蜂窝移动通信网络接入的基站，所述基站设置成：

与终端完成测距过程后，与所述终端进行基本能力协商；

在基本能力协商过程完成后，接收所述终端发送的接入鉴别请求分组，该分组中包含：终端的证书及终端的签名；

在接收到所述接入鉴别请求分组后，对所述终端的签名进行认证，签名
5 认证成功后，将终端的证书包含在证书鉴别请求分组中发送给鉴别服务器进
行验证；

在鉴别服务器对终端的证书验证成功后，向终端发送接入鉴别响应分组，
并与终端进行单播会话密钥协商；以及

在单播会话密钥协商完成后，与终端交互，完成后续的接入流程，使终
10 端接入到蜂窝移动通信网络。

7、如权利要求 6 所述的基站，其中，

所述基站还设置成：在鉴别服务器对所述终端的证书验证成功后，生成
用于 ECDH 交换的临时私钥 sy 和临时公钥 py，使用所述 px 和 sy 进行 ECDH
计算，得到基密钥 BK，并将所述 py 包含在所述接入鉴别响应分组中发送给
15 所述终端。

8、如权利要求 6 或 7 所述的基站，其中，

所述基站还设置成：根据基本能力协商过程中所述终端发送的基本能力
请求消息中包含的用于标识所述终端是否支持 WAPI 接入认证的信息来判断
是否启动与所述终端的所述 WAPI 接入认证过程。

20 9、一种支持蜂窝移动通信网络接入的终端，所述终端设置成：

在与基站完成测距过程后，与基站进行基本能力协商；

在基本能力协商过程完成后，向所述基站发送接入鉴别请求分组，该分
组中包含：终端的证书及终端的签名；

在鉴别服务器对所述终端的证书验证成功后，接收基站向所述终端发送
25 的接入鉴别响应分组，并与所述基站进行单播会话密钥协商；以及

在单播会话密钥协商完成后，与基站交互，完成后续的接入流程，接入到蜂窝移动通信网络。

10、如权利要求 9 所述的终端，其中，

所述终端还设置成：发送所述接入鉴别请求分组前，生成用于椭圆曲线
5 密码体制的戴菲-赫曼 ECDH 交换的临时公钥 px 和临时私钥 sx，并将所述 px
包含在所述接入鉴别请求分组中发送给所述基站；以及在接收到所述接入鉴
别响应分组后，使用所述 py 和 sx 进行 ECDH 计算，得到基密钥 BK；

11、一种支持蜂窝移动通信网络接入的鉴别服务器，

所述鉴别服务器设置成：对终端的证书进行验证，以及对基站的证书进
10 行验证，并将对基站的证书的验证结果和鉴别服务器的签名通过基站发送给
终端。

12、一种蜂窝移动通信网络的接入系统，该系统包含：如权利要求 6-8
中的任一项所述的基站，如权利要求 9-10 中任一项所述的终端，及如权利要
求 11 所述的鉴别服务器；其中，

15 所述基站与所述终端设置成采用如下方式进行单播会话密钥协商得到单
播会话密钥：

所述基站生成随机数 N_1 和用于 ECDH 交换的临时私钥 sy 和临时公钥 py，
并向所述终端发送单播密钥协商请求分组，该分组中包含所述 N_1 和 py；

接收到所述单播密钥协商请求分组后，所述终端生成随机数 N_2 和用于
20 ECDH 交换的临时私钥 sx 和临时公钥 px，对 py 和 sx 进行 ECDH 计算，得到
基密钥 BK，使用基密钥 BK、所述 N_1 和 N_2 生成所述单播会话密钥；

所述终端向基站发送单播密钥协商响应分组，该分组中包含所述 N_2 和
px；

接收到所述单播密钥协商响应分组后，所述基站对 px 和 sy 进行 ECDH
25 计算，得到基密钥 BK，使用基密钥 BK、所述 N_1 和 N_2 生成所述单播会话密
钥。

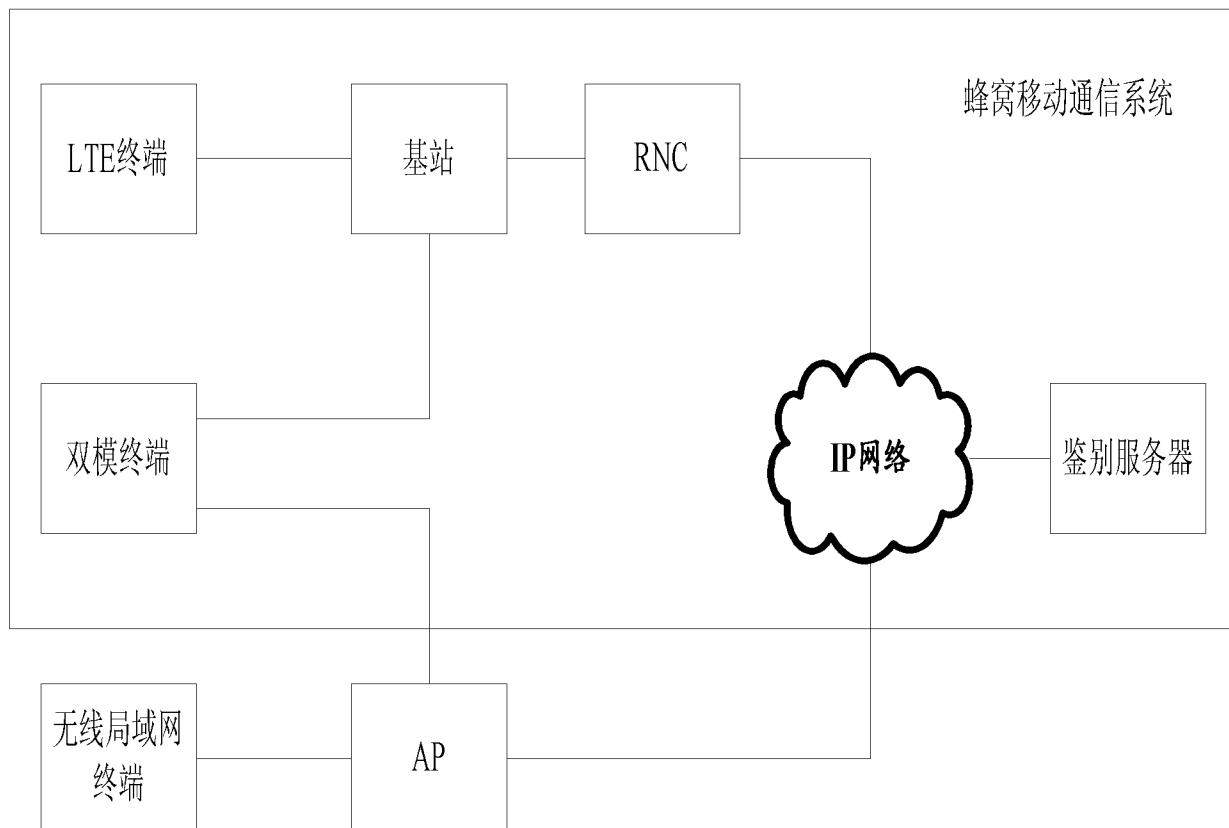


图 1 / Fig. 1

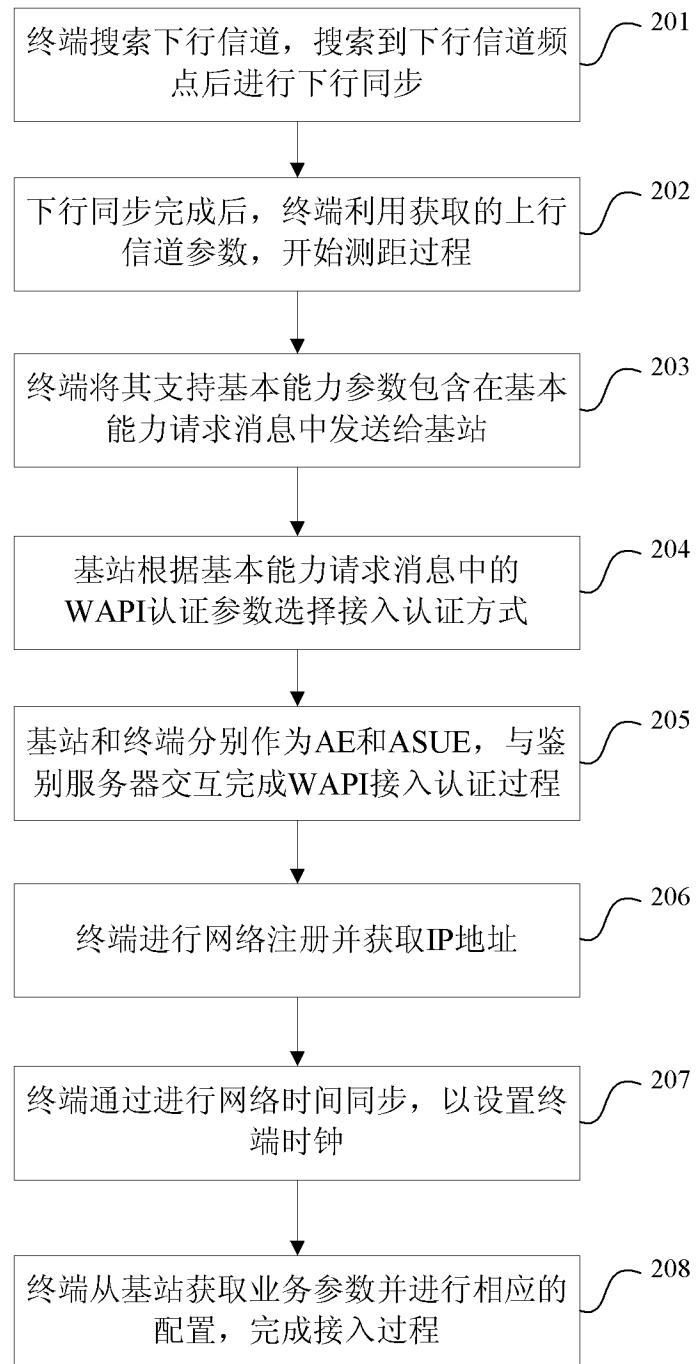


图 2 / Fig. 2

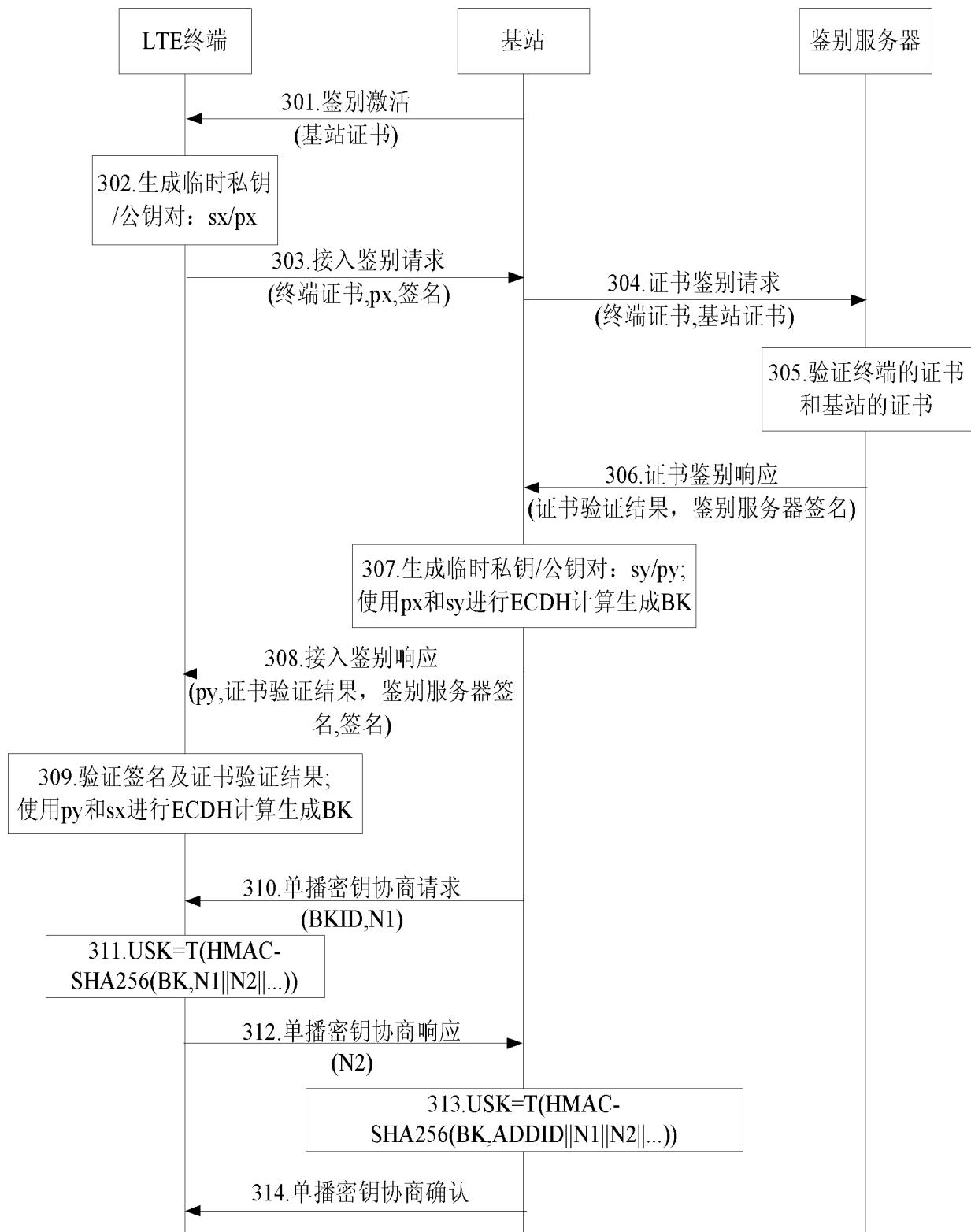


图 3 / Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2009/075505

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/08 (2009.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04W; H04Q;H04L;H04B

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, CNKLCNPAT, GOOGLE, IEEE: WAPI, BS, AP, MT, STA, MS, ASE, distance, measurement, capabilities, negotiation, authenticate, base station, access point, terminal, cellular, certificate, signature, server, service, entity, ZTE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|--|-----------------------|
| A | HUANG, Zhenhai et al. Review of WLAN Authentication and Privacy Infrastructure (WAPI) Mobile Communication May 2006, pages 31-35 | 1-12 |
| A | CN 101198181 A (INSTITUTE OF COMPUTING TECHNOLOGY, CHINESE ACADEMY OF SCIENCES) 11 June 2008 (11.06.2008) the whole document | 1-12 |
| A | CN 101272616 A (GCI SCIENCE & TECHNOLOGY CO., LTD.) 24 September 2008 (24.09.2008) the whole document | 1-12 |
| A | CN 1949709 A (XIAN XIDIAN JIETONG WIRELESS NETWORK COMMUNICATION CO., LTD.) 18 April 2007 (18.04.2007) the whole document | 1-12 |

Further documents are listed in the continuation of Box C.

See patent family annex.

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

| | |
|--|--|
| Date of the actual completion of the international search 08 March 2010(08.03.2010) | Date of mailing of the international search report 01 Apr. 2010 (01.04.2010) |
| 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 LI, Xiaoli Telephone No. (86-10)82245131 |

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2009/075505

| Patent Documents referred in the Report | Publication Date | Patent Family | Publication Date |
|---|------------------|---|--|
| CN 101198181 A | 11.06.2008 | None | |
| CN 101272616 A | 24.09.2008 | None | |
| CN 1949709 A | 18.04.2007 | WO 2008034360 A1 EP 2063567 A1 CN 100488305 C US 2010009656 A1 | 27.03.2008 27.05.2009 13.05.2009 14.01.2010 |

A. 主题的分类

H04W 12/08 (2009.01) i

按照国际专利分类(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04W; H04Q;H04L;H04B

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, GOOGLE, IEEE: 测距, 能力协商, 认证, 验证, 鉴别, 鉴权, WAPI, 基站, BS, AP, 接入点, 终端, MT, STA, MS, 蜂窝, 证书, 签名, 服务实体, 服务器, ASE, 中兴, distance, measurement, capabilities, negotiation, authenticate, base station, access point, terminal, cellular, certificate, signature, server, service, entity, ZTE

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 | 黄振海等 无线局域网鉴别与保密基础结构 WAPI 综述 移动通信 5 月 2006, 第 31-35 页 | 1-12 |
| A | CN 101198181 A (中国科学院计算技术研究所) 11.6 月 2008 (11.06.2008) 全文 | 1-12 |
| A | CN 101272616 A (广州杰赛科技股份有限公司) 24.9 月 2008 (24.09.2008) 全文 | 1-12 |
| A | CN 1949709 A (西安西电捷通无线网络通信有限公司) 18.4 月 2007 (18.04.2007) 全文 | 1-12 |

 其余文件在 C 栏的续页中列出。 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

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

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

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

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

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

“&” 同族专利的文件

国际检索实际完成的日期

08.3 月 2010(08.03.2010)

国际检索报告邮寄日期

01.4 月 2010 (01.04.2010)

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

李晓莉

电话号码: (86-10) 82245131

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2009/075505

| 检索报告中引用的专利文件 | 公布日期 | 同族专利 | 公布日期 |
|----------------|------------|---|--|
| CN 101198181 A | 11.06.2008 | 无 | |
| CN 101272616 A | 24.09.2008 | 无 | |
| CN 1949709 A | 18.04.2007 | WO 2008034360 A1 EP 2063567 A1 CN 100488305 C US 2010009656 A1 | 27.03.2008 27.05.2009 13.05.2009 14.01.2010 |