(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 11 月 18 日 (18.11.2010)

PCT

(10) 国际公布号
WO 2010/130121 A1

(51) 国际专利分类号:
H04L 12/46 (2006.01)

(21) 国际申请号: PCT/CN2009/074143

(22) 国际申请日: 2009 年 9 月 23 日 (23.09.2009)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200910140445.9 2009 年 5 月 15 日 (15.05.2009) 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): **梁洁辉 (LIANG, Jiehui)** [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)。 **施元庆 (SHI, Yuanqing)** [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)。 **刘家兵 (LIU, Jiabing)** [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): ARIPO (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,

[见续页]

(54) **Title**: METHOD AND SYSTEM FOR ACCESSING 3RD GENERATION NETWORK

(54) **发明名称** : 一种第三代网络的接入方法及系统

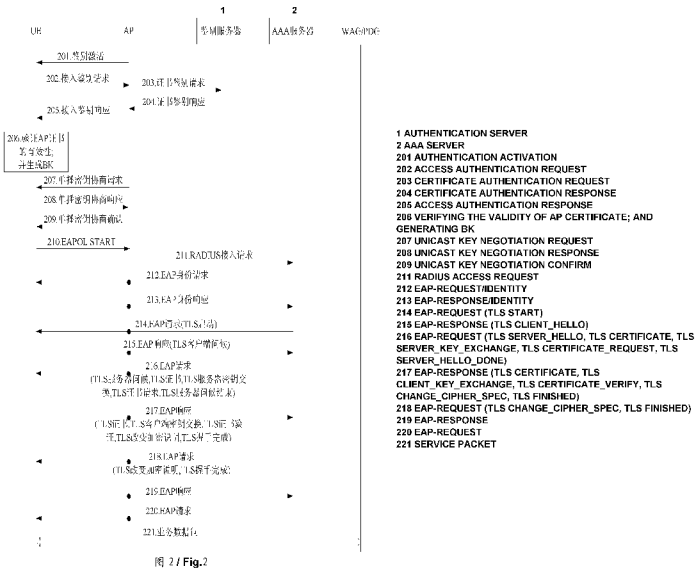

图 2 / Fig.2

(57) **Abstract**: The present invention provides a method and system for accessing the 3rd generation (3G) network. The method includes the following steps: a terminal accesses Wireless Local Area Networks (WLAN) through WLAN Authentication Privacy Infrastructure (WAPI) protocol, and through the Access Point (AP) of the WLAN, notifies the Authentication Authorization Accounting (AAA) server of the 3G network about that the terminal is prepared to access the 3G network; the AAA server obtains the identity information of the terminal through the AP, and performs the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) negotiation procedure with the terminal through the AP after judging that the terminal is a subscribed terminal of the 3G network according to the identity information; after the EAP-TLS negotiation procedure is finished, the terminal accesses the 3G network. The system includes the AP of the WLAN and the AAA server of the 3G network. The present invention reduces the unnecessary processes, such as message exchange, certificate verification and signature verification, and improves the efficiency of the system.

(57) **摘要**:

[见续页]

WO 2010/130121 A1

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))。

本发明提供一种第三代网络的接入方法及系统，所述方法包括：终端采用无线局域网认证和保密基础结构 WAPI 协议接入无线局域网，通过无线局域网的接入点 AP 通知第三代 3G 网络的认证授权和审计 AAA 服务器所述终端准备接入 3G 网络；所述 AAA 服务器通过 AP 获取所述终端的身份信息，并根据所述身份信息判定所述终端为 3G 网络的签约终端后，通过 AP 与所述终端进行可扩展认证协议-传输层安全 EAP-TLS 协商过程；所述 EAP-TLS 协商过程完成后，所述终端接入 3G 网络。所述系统包括：无线局域网的 AP 和 3G 网络的 AAA 服务器。本发明减少了不必要的消息交互、证书验证和签名验证等处理，提高了系统的效率。

一种第三代网络的接入方法及系统

技术领域

本发明涉及通信领域，尤其涉及一种第三代（3rd Generation，3G）网络的接入方法及系统。

背景技术

为了应对无线局域网 IEEE(Institute of Electrical and Electronics Engineers，电气和电子工程师协会） 802.11 的安全机制 WEP（Wried Equivalent Privacy，有线等效隐私）和 WPA（Wi-Fi Protected Access，无线保真保护访问）存在的安全隐患，提出了 WAPI（WLAN Authentication Privacy Infrastructure，无线局域网认证和保密基础结构）安全协议。该协议实现了 ASUE（鉴别请求实体，设置在终端中）和 AE（鉴别器实体，设置在接入点中）的对等认证，确保了无线局域网（WLAN）的链路层安全。

WAPI 安全协议支持两种格式的证书: GBW(国家标准物质)证书和 X.509 v3 证书。X.509 v3 证书支持多种扩展属性/字段，包括: 密钥标识符、密钥用法、扩展密钥用法、CRL（Certificate Revocation List，证书吊销列表）分布点、证书策略、证书机构策略映射、证书主体别名、颁发者别名和证书主体目录属性。

如图 1 所示，无线局域网终端（简称终端）完成接入认证后，如果无线局域网与因特网相连，则终端可以通过无线局域网访问因特网；但对于 3G(3rd Generation，第三代）网络，终端还必须经过 3G 网络的 AAA（Authentication Authorization Accounting，认证授权和审计）服务器的接入认证，才能访问电路业务和分组业务等 3G 网络资源。

AAA 服务器负责对具备 IP（Internet Protocol，因特网协议）能力的终端进行接入认证，检索存储在 HSS（Home Subscriber Server，归属用户服务器）中的用户信息，判断当前用户是否合法，维护 WLAN 接入的连续性，提供 WLAN 的漫游功能，生成用户接入 3G 网络的账单，并报告给用户。如果 3G

网络应用 QoS（Quality of Service，服务质量）机制，那么 AAA 服务器还需实现授权和存储无线局域网的 QoS 配置，并将其映射到作为接入网的无线局域网中。

现有技术中，3G 网络的 AAA 服务器采用 EAP-SIM（Extensible Authentication Protocol-Subscriber Identification Module，可扩展认证协议-用户识别模块）和 EAP-AKA（Extensible Authentication Protocol-Authentication and Key Agreement，可扩展认证协议-认证和密钥协商）对采用 IEEE 802.11i 作为安全机制的无线局域网终端进行接入认证。这两种认证机制需要终端具备读取 UICC（Universal Integrated Circuit Card，通用集成电路卡）的能力，这就限制了无线局域网终端用户必须使用多模终端下才能享受 3G 网络服务。而对于采用 WAPI 安全机制而不具备读取 UICC 能力的 WLAN 终端，3GPP（3rd Generation Partnership Project，第三代合作伙伴计划）组织目前尚未提出如何接入到 3G 网络的技术方案。

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 3G 网络的接入方法及系统，使采用 WAPI 安全机制而不具备读取 UICC 能力的 WLAN 终端可以安全地接入 3G 网络。

本发明提供一种第三代网络的接入方法，该方法包括:

终端采用无线局域网认证和保密基础结构 WAPI 协议接入无线局域网后，通过无线局域网的接入点 AP 通知第三代 3G 网络的认证授权和审计 AAA 服务器该终端准备接入 3G 网络;

AAA 服务器通过 AP 获取所述终端的身份信息，并根据所述身份信息判定所述终端为 3G 网络的签约终端后，通过 AP 与所述终端进行可扩展认证协议-传输层安全 EAP-TLS 协商过程;

EAP-TLS 协商过程完成后，所述终端接入 3G 网络。

此外，通知 AAA 服务器该终端准备接入 3G 网络的所述步骤包括:

所述终端向 AP 发送局域网可扩展认证协议的开始分组;

接收到所述开始分组后，AP 向 AAA 服务器发送远程用户拨入认证系统 RADIUS 协议的接入请求分组，以通知 AAA 服务器有终端准备接入 3G 网络。

此外，获取所述终端的身份信息的所述步骤包括:

AAA 服务器通过 AP 向所述终端发送可扩展认证协议的身份请求消息;

接收到所述身份请求消息后，所述终端将所述身份信息包含在可扩展认证协议的身份响应消息中，通过 AP 发送给 AAA 服务器。

此外，所述身份信息是记录在所述终端的终端证书中的: 3G 网络中与所述终端的终端证书绑定的初始会话协议帐号、或所述终端的国际移动用户识别码。

此外，所述 EAP-TLS 协商过程包括如下步骤:

AAA 服务器通过 AP 向所述终端发送包含 TLS 启动消息的 EAP 请求分组，以启动 EAP-TLS 协商过程;

所述终端通过 AP 向 AAA 服务器发送包含 TLS 客户端问候消息的 EAP 响应分组; 所述 TLS 客户端问候消息中包含所述终端的能力信息;

AAA 服务器通过 AP 向所述终端发送包含 TLS 服务器问候消息、TLS 服务器密钥交换消息的 EAP 请求分组; 所述 TLS 服务器问候消息中包含 AAA 服务器根据所述终端的能力信息选择的密钥套件和压缩算法; TLS 服务器密钥交换消息中包含 AAA 服务器侧的密钥交换参数;

所述终端向 AAA 服务器发送包含 TLS 客户端密钥交换消息的 EAP 响应分组; 所述 TLS 客户端密钥交换消息中包含终端侧的密钥交换参数。

此外，AAA 服务器通过 AP 向所述终端发送的、包含 TLS 服务器问候消息和 TLS 服务器密钥交换消息的所述 EAP 请求分组中还包含: TLS 证书消息和 TLS 证书请求消息; 所述 TLS 证书消息中包含 AAA 服务器证书; 所述 TLS 证书请求消息用于指示所述终端提供终端证书;

所述终端向 AAA 服务器发送包含 TLS 客户端密钥交换消息的 EAP 响应分组的所述步骤还包括: 所述终端接收到所述 TLS 证书消息和 TLS 证书请求消息，对 TLS 证书消息中包含的 AAA 服务器证书进行验证，并根据所述 TLS 证书请求消息在其发送的所述 EAP 响应分组中携带 TLS 证书消息; 所述 TLS

证书消息中包含终端证书;

进行可扩展认证协议-传输层安全 EAP-TLS 协商过程的所述步骤在所述终端向 AAA 服务器发送包含 TLS 客户端密钥交换消息的 EAP 响应分组之后还包括: AAA 服务器对接收到的所述 TLS 证书消息中包含的所述终端证书进行验证。

本发明还提供一种第三代网络的接入系统，用于对无线局域网终端进行 3G 网络的接入认证; 该系统包含: 无线局域网的 AP 和 3G 网络的 AAA 服务器，其中:

所述 AP 设置成采用 WAPI 协议对所述终端进行无线局域网的接入认证，并在终端接入无线局域网之后，向所述 AAA 服务器发送所述终端准备接入 3G 网络的通知消息;

所述 AAA 服务器设置成通过所述 AP 获取所述终端的身份信息，并根据所述身份信息判定所述终端是 3G 网络的签约终端后，通过所述 AP 与所述终端进行 EAP-TLS 协商过程; 并在 EAP-TLS 协商过程完成后，允许所述终端接入 3G 网络。

此外，所述 AP 设置成采用如下方式通知所述 AAA 服务器所述终端准备接入 3G 网络:

接收到所述终端发送的局域网可扩展认证协议的开始分组后，所述 AP 向所述 AAA 服务器发送 RADIUS 协议的接入请求分组，以通知所述 AAA 服务器有终端准备接入 3G 网络。

此外，所述 AAA 服务器设置成采用如下方式获取所述终端的身份信息:

所述 AAA 服务器通过所述 AP 向所述终端发送可扩展认证协议的身份请求消息;

接收到所述身份请求消息后，所述终端将所述身份信息包含在可扩展认证协议的身份响应消息中，通过所述 AP 发送给所述 AAA 服务器。

此外，所述身份信息是记录在所述终端的终端证书中的: 3G 网络中与所述终端的终端证书绑定的初始会话协议帐号、或所述终端的国际移动用户识别码。

综上所述，本发明通过将 WAPI 的终端证书作为接入 3G 网络的凭证，使得 WLAN 终端在签约后，使用同一证书即可同时安全地接入 WLAN 和 3G 网络，极大地方便了用户。

此外，本发明对 AAA 服务器侧的接入认证方法进行了优化，即 AAA 服务器先通过 AP 获取终端身份信息，并根据终端身份信息对终端进行初步的鉴别（判断终端是否是签约终端）后，再与终端进行 EAP-TLS 协商，避免了与没有在 3G 网络中签约的 WLAN 终端发起 EAP-TLS 协商，减少了不必要的消息交互、证书验证和签名验证等处理，提高了系统的效率。

附图概述

图 1 WLAN 终端接入 3G 网络示意图；

图 2 是本发明实施例 WLAN 终端接入 3G 网络的方法流程图；

图 3 是本发明实施例 3G 网络的接入系统结构示意图。

本发明的较佳实施方式

本发明的核心思想是，终端采用 WAPI 协议接入无线局域网后，通过无线局域网的 AP 通知 3G 网络的 AAA 服务器该终端准备接入 3G 网络；AAA 服务器通过 AP 获取终端的 3G 接入身份信息，并判定该终端为 3G 网络的签约终端后发起 EAP-TLS（Extensible Authentication Protocol-Transport Layer Security，可扩展认证协议-传输层安全）协商过程；终端与 AAA 服务器通过 EAP-TLS 协商过程完成 3G 网络的证书鉴别（即接入认证）和密钥交换，主要包括:

（1）终端和 AAA 服务器之间通过 TLS 客户端问候消息/TLS 服务器问候消息的交互完成了双方能力参数（主要包括密钥套件和压缩算法）的协商；

（2）终端和 AAA 服务器之间通过 TLS 证书消息交换双方的证书（可选）；

（3）终端和 AAA 服务器之间通过 TLS 客户端密钥交换消息/TLS 服务器密钥交换消息完成密钥参数的交换和密钥的协商。

下面将结合附图和实施例对本发明进行详细描述。

图 2 是本发明实施例 WLAN 终端接入 3G 网络的方法流程图，如图 2 所示，该方法包括如下步骤:

201: 当 WLAN 终端（简称终端或 UE）关联或重新关联至 AP 时，AP 向终端发送鉴别激活分组;

鉴别激活分组中包含: AP 证书和 AP 信任的鉴别服务器标识。

202: 终端收到鉴别激活分组后，保存 AP 证书，根据 AP 信任的鉴别服务器标识选择 AP 信任的鉴别服务器所颁发的终端证书，生成 ECDH（椭圆曲线密码体制的 Diffie-Hellman（戴菲-赫曼））交换所使用的临时密钥对（包括: 临时公钥 px、临时私钥 sx），向 AP 发送接入鉴别请求分组;

接入鉴别请求分组中包含: 终端证书、终端的临时公钥 px 以及终端的签名等参数。

203: AP 收到接入鉴别请求分组后，验证终端的签名是否正确: 如果终端的签名正确，则向鉴别服务器发送证书鉴别请求分组; 否则丢弃该接入鉴别请求分组，本流程结束;

证书鉴别请求分组中包含: AP 证书和终端证书。

204: 鉴别服务器收到证书鉴别请求分组后，对 AP 证书和终端证书进行验证，并将证书验证结果以及鉴别服务器的签名包含在证书鉴别响应分组中发送给 AP。

205: AP 收到证书鉴别响应分组后，根据其中包含的证书验证结果及鉴别服务器的签名检查终端的证书是否有效，如果终端证书无效，则丢弃证书鉴别响应分组，本流程结束; 如果终端证书有效，则生成用于 ECDH 交换的临时密钥对（包括: 临时公钥 py、临时私钥 sy），使用 AP 的临时私钥 sy 和终端的临时公钥 px 进行 ECDH 运算，得到基密钥 BK，并向终端发送接入鉴别响应分组。

接入鉴别响应分组中包含: 证书验证结果、鉴别服务器的签名、AP 的临时公钥 py 和 AP 的签名。

206: 终端收到接入鉴别响应分组后，根据证书验证结果、鉴别服务器的

签名以及AP的签名检查AP证书是否有效：如果AP证书无效，则丢弃接入鉴别响应分组，本流程结束；否则使用终端的临时私钥sx和AP的临时公钥py进行ECDH运算，得到基密钥BK。

需要注意的是，根据ECDH原理，AP和终端生成的基密钥BK相同。

经过步骤201～206的交互，终端和AP完成了证书鉴别过程，并在证书鉴别过程中协商出了基密钥BK；在后续步骤中，终端和AP将使用基密钥BK协商生成单播会话密钥。

207：AP向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：AP生成的随机数N_1等参数。

208：接收到单播密钥协商请求分组后，终端生成随机数N_2；使用基密钥BK、随机数N_1和随机数N_2计算生成单播会话密钥；并向AP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随机数N_2等参数。

209：AP接收到单播密钥协商响应分组后，使用基密钥BK、随机数N_1和随机数N_2计算生成单播会话密钥，并向终端发送单播密钥协商确认分组，结束单播密钥的协商过程。

至此，终端和AP完成了WAPI协议的证书鉴别过程和单播会话密钥协商过程，终端成功接入无线局域网。在以下步骤中，终端将采用EAP-TLS协商过程接入3G网络，在此过程中，终端与AP之间通过EAPoL协议封装EAP-TLS消息，WLAN接入网络与3G AAA之间通过RADIUS（Remote Authentication Dial-In User Service，远程用户拨入认证系统）协议封装EAP-TLS消息，并且终端与AP之间可以使用上述单播密钥协商过程中协商得到的单播会话密钥进行链路层的加密。

210：当终端准备接入3G网络时，首先向AP发送EAPoL（EAP Over LAN，局域网可扩展认证协议）的START（开始）分组，通知AP该终端准备接入3G网络。

211：AP收到终端发送的EAPoL START（开始）分组后，将其封装成RADIUS协议的接入请求分组，发送给3G网络的AAA服务器，通知AAA

服务器有终端要接入 3G 网络。

212: 接收到上述接入请求分组后，AAA 服务器通过 AP 向终端发送 EAP（Extensible Authentication Protocol，可扩展认证协议）身份请求（EAP-Request/Identity）消息，以获取终端的身份信息。

213: 终端收到 EAP 身份请求消息后，将终端证书的主体别名字段中记录的身份信息包含在 EAP 身份响应（EAP-Response/Identity）消息中通过 AP 发送给 AAA 服务器;

上述主体别名字段中记录的身份信息可以是在 3G 网络中与终端证书绑定的 SIP（Session Initial Protocol，初始会话协议）账号或 IMSI（International Mobile Subscriber Identifier，国际移动用户识别码）等信息。

214: AAA 服务器收到 EAP 身份响应消息后，根据该消息中携带的终端身份信息判断该终端是否已签约（即是否为 3G 网络的签约终端），如果未签约，则本流程结束；如果终端已签约，则通过 AP 向终端发送包含 TLS 启动（TLS Start）消息的 EAP 请求分组，开始进行 TLS 协商过程。

AAA 服务器可以在本地存储的用户签约信息或存储在 HSS 中的用户签约信息中检索上述消息中携带的终端身份信息，并根据检索的结果判断对应终端是否已签约。

215: 终端开始正常的 TLS 握手过程，向服务器发送包含 TLS 客户端问候（TLS client_hello）消息的 EAP 响应分组;

TLS 客户问候消息中包含终端的 TLS 能力信息，具体包含: TLS 版本号、会话标识、初始随机数、客户端支持的密钥套件和压缩算法等参数。

216: AAA 服务器通过 AP 向终端发送包含 TLS 服务器问候（TLS server_hello）消息、TLS 证书（TLS certificate）消息、TLS 服务器密钥交换（TLS server_key_exchange）消息、TLS 证书请求（TLS certificate_request）消息和 TLS 服务器问候结束（TLS server_hello_done）消息的 EAP 请求分组;

其中:

TLS 服务器问候消息中包含: AAA 服务器根据终端的能力信息，从终端支持的密钥套件和压缩算法中选择的 AAA 服务器支持的密钥套件和压缩算

法等信息;

TLS 证书消息中包含 AAA 服务器证书;

TLS 服务器密钥交换消息中包含 AAA 服务器侧的密钥交换参数;

TLS 证书请求消息用于指示终端提供证书;

TLS 服务器问候结束消息用于表示本阶段的服务器握手过程结束，AAA 服务器开始等待终端的应答。

217: 终端接收到上述 EAP 请求分组后，验证 TLS 证书消息中包含的 AAA 服务器证书，验证通过后，通过 AP 向 AAA 服务器发送包含 TLS 证书（TLS certificate）消息、TLS 客户端密钥交换（TLS client_key_exchange）消息、TLS 证书验证（TLS certificate_verify）消息、TLS 改变加密说明（TLS change_cipher_spec）消息和 TLS 握手完成（TLS finished）消息的 EAP 响应分组；其中:

TLS 证书消息中包含终端证书;

TLS 客户端密钥交换消息中包含终端侧的密钥交换参数;

TLS 证书验证消息中包含终端的签名信息，防止非授权终端仿冒该终端接入 3G 网络;

TLS 改变加密说明消息用于通知 AAA 服务器开始启用新的密钥套件和压缩算法;

TLS 握手完成消息用于表示终端已完成本阶段的 TLS 握手协议。

218: 接收到上述 EAP 响应分组后，AAA 服务器验证其中包含的终端证书和终端的签名；如果验证失败，则丢弃该分组，本流程结束；如果验证通过，则通过 AP 向终端发送包含 TLS 改变加密说明（TLS change_cipher_spec）消息和 TLS 握手完成（TLS finished）消息的 EAP 请求分组；其中:

TLS 改变加密说明消息用于通知终端开始启用新的密钥套件和压缩算法;

TLS 握手完成消息用于表示 AAA 服务器已完成本阶段的 TLS 握手协议。

219: 终端向 AAA 服务器发送 EAP 响应分组，指示已完成 TLS 协商。

220: AAA 服务器发送 EAP 成功（EAP-SUCCESS）消息，表明完成对终端的证书鉴别（即接入认证）并协商出会话密钥，允许终端接入 3G 网络。

221: 接收到 EAP 成功消息后，终端获知接入认证成功，因此通过 WAG（Wireless Access Gateway，无线接入网关）/PDG（Packet Data Gateway，分组数据网关）使用 3G 网络的资源，发起音频、视频等 3G 业务。

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）根据 WAPI 协议，除了在步骤 201～205 所示的证书鉴别过程中进行 BK 的协商外，终端和 AP 也可以使用预共享密钥（PSK）直接导出 BK。

（二）根据 WAPI 协议，AP 在接收到包含终端证书的接入鉴别请求后，也可以在本地进行证书的验证，因此步骤 203～204 可省略；同样，终端也无需使用鉴别服务器的证书验证结果，而在本地对 AP 证书进行验证。

（三）在步骤 211 中，AP 接收到终端发送的 EAPoL START（开始）分组后，获知终端准备接入 3G 网络，也就是获知终端与 AAA 服务器的后续消息交互是用于 3G 网络的接入认证和密钥协商，因此 AP 可以不对后续的 EAP-TLS 协商过程中的 EAP-TLS 消息进行链路层加密，终端也无需对 EAP-TLS 消息进行链路层加密。

图 3 是本发明实施例 3G 网络的接入系统结构示意图，该系统用于对无线局域网终端（简称终端）进行 3G 网络的接入认证；该系统包含：无线局域网的 AP、无线局域网的鉴别服务器和 3G 网络的 AAA 服务器，其中:

AP 和鉴别服务器用于采用 WAPI 协议对终端进行无线局域网的接入认证，在终端接入无线局域网之后，AP 向 AAA 服务器发送终端准备接入 3G 网络的通知消息;

AAA 服务器用于通过 AP 获取终端的身份信息，并根据所述身份信息判定终端是 3G 网络的签约终端后，通过 AP 与终端进行 EAP-TLS 协商过程；并在 EAP-TLS 协商过程完成后，允许终端接入 3G 网络。

上述身份信息是记录在终端证书中的: 3G 网络中与该终端证书绑定的初始会话协议帐号、或该终端的国际移动用户识别码。

AP 可以采用如下方式通知 AAA 服务器终端准备接入 3G 网络：接收到

终端发送的局域网可扩展认证协议的开始分组后，AP 向 AAA 服务器发送 RADIUS 协议的接入请求分组，以通知 AAA 服务器有终端准备接入 3G 网络。

AAA 服务器可以采用如下方式获取终端的身份信息：AAA 服务器通过 AP 向终端发送可扩展认证协议的身份请求消息；接收到该消息后，终端将身份信息包含在可扩展认证协议的身份响应消息中，通过 AP 发送给 AAA 服务器。

上述系统中包含的其它网元、各网元的详细功能、以及各网元间的连接关系（消息交互关系）详见上述对图 2 所示的方法的描述部分。

工业实用性

本发明对 AAA 服务器侧的接入认证方法进行了优化，即 AAA 服务器先通过 AP 获取终端身份信息，并根据终端身份信息对终端进行初步的鉴别（判断终端是否是签约终端）后，再与终端进行 EAP-TLS 协商，避免了与没有在 3G 网络中签约的 WLAN 终端发起 EAP-TLS 协商，减少了不必要的消息交互、证书验证和签名验证等处理，提高了系统的效率。

权 利 要 求 书

1、一种第三代网络的接入方法，该方法包括:

终端采用无线局域网认证和保密基础结构 WAPI 协议接入无线局域网，通过无线局域网的接入点 AP 通知第三代 3G 网络的认证授权和审计 AAA 服务器所述终端准备接入 3G 网络;

所述 AAA 服务器通过 AP 获取所述终端的身份信息，并根据所述身份信息判定所述终端为 3G 网络的签约终端后，通过 AP 与所述终端进行可扩展认证协议-传输层安全 EAP-TLS 协商过程;

所述 EAP-TLS 协商过程完成后，所述终端接入 3G 网络。

2、如权利要求 1 所述的方法，其中，通过无线局域网的接入点 AP 通知第三代 3G 网络的认证授权和审计 AAA 服务器所述终端准备接入 3G 网络的所述步骤包括:

所述终端向 AP 发送局域网可扩展认证协议的开始分组;

所述 AP 接收所述开始分组，向 AAA 服务器发送远程用户拨入认证系统 RADIUS 协议的接入请求分组，以通知所述 AAA 服务器有终端准备接入 3G 网络。

3、如权利要求 1 或 2 所述的方法，其中，所述 AAA 服务器通过 AP 获取所述终端的身份信息的所述步骤包括:

AAA 服务器通过 AP 向所述终端发送可扩展认证协议的身份请求消息;

所述终端接收所述身份请求消息，将所述身份信息包含在可扩展认证协议的身份响应消息中，通过 AP 发送给所述 AAA 服务器。

4、如权利要求 1 所述的方法，其中，

所述身份信息是记录在所述终端的终端证书中的以下信息之一:

3G 网络中与所述终端的终端证书绑定的初始会话协议帐号; 或

所述终端的国际移动用户识别码。

5、如权利要求 1 所述的方法，其中， 进行可扩展认证协议-传输层安全 EAP-TLS 协商过程的所述步骤包括:

AAA 服务器通过 AP 向所述终端发送包含 TLS 启动消息的 EAP 请求分组，以启动 EAP-TLS 协商过程;

所述终端通过 AP 向 AAA 服务器发送包含 TLS 客户端问候消息的 EAP 响应分组，所述 TLS 客户端问候消息中包含所述终端的能力信息;

AAA服务器通过AP向所述终端发送包含TLS服务器问候消息和TLS服务器密钥交换消息的 EAP 请求分组，所述 TLS 服务器问候消息中包含 AAA 服务器根据所述终端的能力信息选择的密钥套件和压缩算法，所述 TLS 服务器密钥交换消息中包含 AAA 服务器侧的密钥交换参数; 以及

所述终端向 AAA 服务器发送包含 TLS 客户端密钥交换消息的 EAP 响应分组，所述 TLS 客户端密钥交换消息中包含终端侧的密钥交换参数。

6、如权利要求 5 所述的方法，其中，

AAA服务器通过AP向所述终端发送的、包含TLS服务器问候消息和TLS服务器密钥交换消息的 EAP 请求分组中还包含: TLS 证书消息和 TLS 证书请求消息，所述 TLS 证书消息中包含 AAA 服务器证书，所述 TLS 证书请求消息用于指示所述终端提供终端证书;

所述终端向 AAA 服务器发送包含 TLS 客户端密钥交换消息的 EAP 响应分组的所述步骤还包括:

所述终端接收到所述 TLS 证书消息和 TLS 证书请求消息，对所接收到的 TLS 证书消息中包含的 AAA 服务器证书进行验证，并根据所接收到的 TLS 证书请求消息在所发送的 EAP 响应分组中携带 TLS 证书消息，所携带的 TLS 证书消息中包含终端证书;

进行可扩展认证协议-传输层安全 EAP-TLS 协商过程的所述步骤在所述终端向 AAA 服务器发送包含 TLS 客户端密钥交换消息的 EAP 响应分组之后还包括:

AAA 服务器对接收到的 TLS 证书消息中包含的终端证书进行验证。

7、一种第三代网络的接入系统，该系统包括: 无线局域网的 AP 和 3G 网络的 AAA 服务器，其中:

所述 AP 设置成采用 WAPI 协议对终端进行无线局域网的接入认证，并

在终端接入无线局域网之后，向所述 AAA 服务器发送有终端准备接入 3G 网络的通知消息;

所述 AAA 服务器设置成通过所述 AP 获取终端的身份信息，根据所述身份信息判定所述终端是 3G 网络的签约终端后，通过所述 AP 与所述终端进行 EAP-TLS 协商过程，并在 EAP-TLS 协商过程完成后，允许所述终端接入 3G 网络。

8、如权利要求 7 所述的系统，其中，

所述 AP 设置成采用如下方式通知所述 AAA 服务器有终端准备接入 3G 网络:

所述 AP 接收终端发送的局域网可扩展认证协议的开始分组，向所述 AAA 服务器发送 RADIUS 协议的接入请求分组，以通知所述 AAA 服务器有终端准备接入 3G 网络。

9、如权利要求 7 或 8 所述的系统，其中，

所述 AAA 服务器设置成采用如下方式获取终端的身份信息:

所述 AAA 服务器通过所述 AP 向终端发送可扩展认证协议的身份请求消息;

所述终端接收所述身份请求消息，将所述身份信息包含在可扩展认证协议的身份响应消息中，通过所述 AP 发送给所述 AAA 服务器。

10、如权利要求 9 所述的系统，其中，

所述终端的身份信息是记录在终端的终端证书中的以下信息之一:

3G 网络中与终端的终端证书绑定的初始会话协议帐号; 或

终端的国际移动用户识别码。

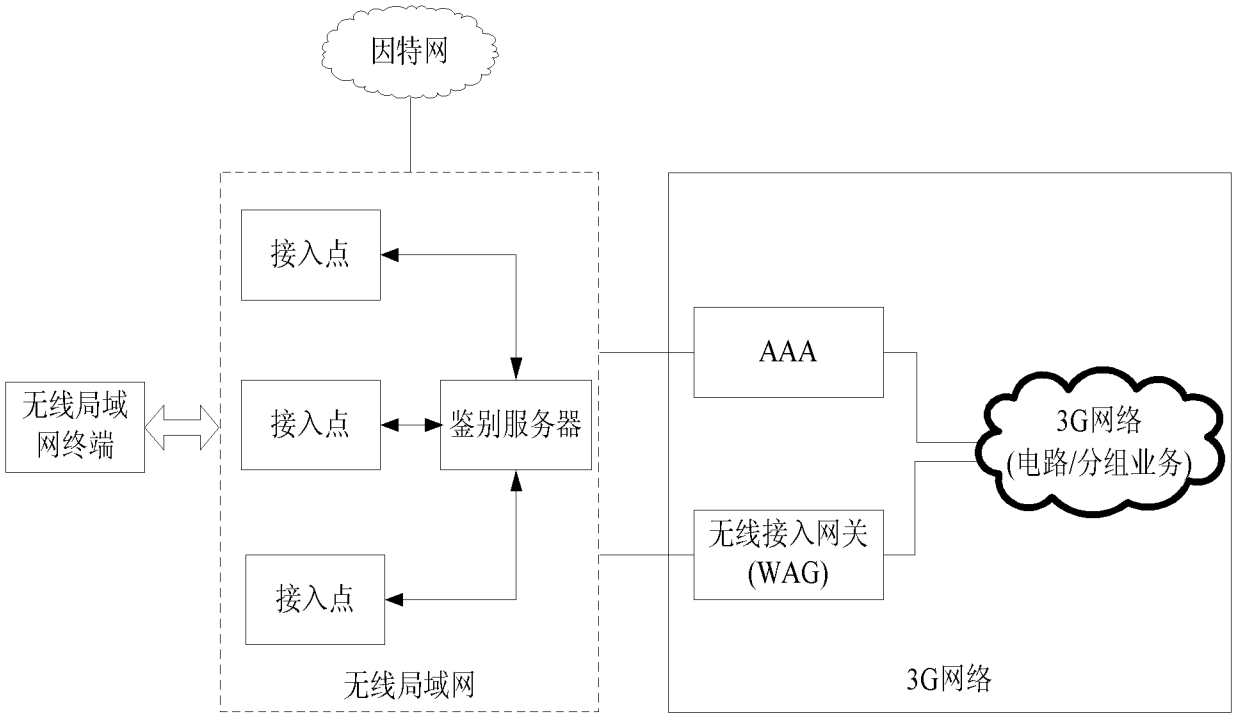
因特网
接入点
接入点
接入点
鉴别服务器
无线局域网终端
无线局域网
AAA
无线接入网关(WAG)
3G网络(电路/分组业务)
3G网络

图 1


UE
AP
鉴别服务器
AAA服务器
WAG/PDG
201.鉴别激活
202.接入鉴别请求
203.证书鉴别请求
204.证书鉴别响应
205.接入鉴别响应
206.验证AP证书的有效性;并生成BK
207.单播密钥协商请求
208.单播密钥协商响应
209.单播密钥协商确认
210.EAPOL START
211.RADIUS接入请求
212.EAP身份请求
213.EAP身份响应
214.EAP请求(TLS启动)
215.EAP响应(TLS客户端问候)
216.EAP请求
(TLS服务器问候,TLS证书,TLS服务器密钥交换,TLS证书请求,TLS服务器问候结束)
217.EAP响应
(TLS证书,TLS客户端密钥交换,TLS证书验证,TLS改变加密说明,TLS握手完成)
218.EAP请求
(TLS改变加密说明,TLS握手完成)
219.EAP响应
220.EAP请求
221.业务数据包

图 2

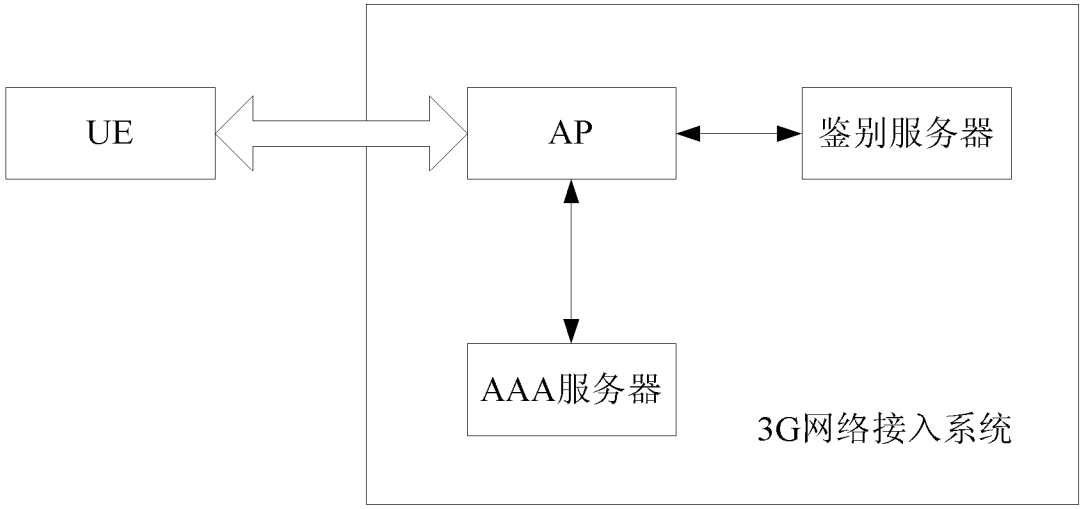

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/074143

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/46 (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: H04L; H04Q; 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) WPI, EPODC, CNPAT, 3GPP, IETF: WLAN, access point, AP, authenticate, privacy, authority, accounting, identity, EAP, TLS, negotiate, AAA, 3G

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	P. Funk et al., Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0), RFC 5281, Aug. 2008, abstract, sections 4, 15	1-10
A	3GPP TSG SA, Wireless Local Area Network (WLAN) interworking security (Release 8), 3GPP TS 33.234 V8.1.0, Mar. 2008, section 6.1	1-10
A	CN101079786A (HUAWEI TECHNOLOGIES CO., LTD.) 28 Nov. 2007 (28.11.2007) the whole document	1-10
A	CN101013940A (XIAN ELECTRONICS SCI & TECHNOLOGY UNIVERSITY) 08 Aug. 2007 (08.08.2007) the whole document	1-10
A	CN101056177A(TSINGHUA UNIVERSITY) 17 Oct. 2007 (17.10.2007) 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
16 Jan. 2010 (16.01.2010)	**25 Feb. 2010 (25.02.2010)**
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 YAN, Yan Telephone No. (86-10)62413129

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2009/074143

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101079786A	28.11.2007	NONE	
CN101013940A	08.08.2007	NONE	
CN101056177A	17.10.2007	NONE	

国际检索报告

国际申请号
PCT/CN2009/074143

A. 主题的分类

H04L 12/46 (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: H04L; H04Q; 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）) WPI, EPODC, CNPAT, 3GPP, IETF: 无线局域网，接入点，认证，保密，授权，计费，审计，身份，可扩展认证协议，传输层安全，协商，第三代，WLAN, access point，AP，authenticate，privacy，authority，accounting，identity，EAP，TLS，negotiate，AAA，3G

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	P.Funk et al., Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0), RFC 5281, 8 月 2008, 摘要，第 4、15 节	1-10
A	3GPP TSG SA, Wireless Local Area Network (WLAN) interworking security (Release 8), 3GPP TS 33.234 V8.1.0, 3 月 2008，第 6.1 节	1-10
A	CN101079786A (华为技术有限公司) 28.11 月 2007 (28.11.2007) 全文	1-10
A	CN101013940A (西安电子科技大学) 08.8 月 2007 (08.08.2007) 全文	1-10
A	CN101056177A(清华大学) 17.10 月 2007 (17.10.2007) 全文	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
16.1 月 2010 (16.01.2010)	**25.2 月 2010 (25.02.2010)**
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 阎岩 电话号码：(86-10) **62413129**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2009/074143

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101079786A	28.11.2007	无	
CN101013940A	08.08.2007	无	
CN101056177A	17.10.2007	无	