(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
2009 年7 月23 日 (23.07.2009)

PCT

(10) 国际公布号
WO 2009/089773 A1

(51) 国际专利分类号:
H04W 12/08 (2009.01)

(21) 国际申请号: PCT/CN2009/070035

(22) 国际申请日: 2009 年1 月5 日 (05.01.2009)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200810055741.4
2008 年1 月8 日 (08.01.2008) CN

(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基地总部办公楼, Guangdong 518129 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): 梁文亮(LIANG, Wenliang) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。 张伟(ZHANG, Wei) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。 顾亮(GU, Liang) [CN/CN]; 中国广东省深圳市龙岗区坂田华为基地总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京挺立专利事务所(BEIJING TINGLI PATENT AGENCY); 中国北京市西城区宣武门西大街129号金隅大厦804、805、806室, Beijing 100031 (CN)。

[见续页]

(54) **Title:** MULTI-HOST ACCESS AUTHENTICATION METHOD AND SYSTEM FOR WIMAX NETWORK

(54) **发明名称:** WiMAX网络的多主机接入认证方法及系统

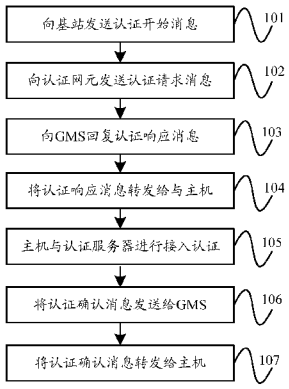

图 3 / Fig 3

101 THE AUTHENTICATION START MESSAGE IS SENT TO THE BASE STATION
102 THE AUTHENTICATION REQUEST MESSAGE IS SENT TO THE AUTHENTICATION NETWORK ELEMENT
103 THE AUTHENTICATION RESPONSE MESSAGE IS RETURNED TO THE GMS
104 THE AUTHENTICATION RESPONSE MESSAG IS TRANSMITTED TO THE HOST
105 THE HOST PERFORMS ACCESS AUTHENTICATION WITH THE AUTHENTICATION SERVER
106 THE AUTHENTICATION CONFIRMATION MESSAGE IS SENT TO THE GMS
107 THE AUTHENTICATION CONFIRMATION MESSAGE IS TRANSMITTED TO THE HOST

(57) Abstract: A multi-host access authentication method and system for WiMAX network, the method includes that: after an access request message from a host is received, a label information of the host which is carried in an authentication start message is sent to an authentication network element; according to the received label information carried in an authentication response message which is from the authentication network element, the authentication response message is transmitted to the host corresponding to the label information, in order to the host performs access authentication with an authentication server after it receives the authentication response message, and the authentication server sends an authentication result to the authentication network element; and the authentication result sent by the authentication network element is received. The system includes a node of network element, a base station, a NAS, and an authentication server. Application of the present invention enables the node of network element to acquire the authentication result of the host, and decide whether an authorization port will be opened or closed according to the authentication result, application of the present invention also can avoid the lawless access of a lawless user, and improve the security of the system.

[见续页]

WO 2009/089773 A1

(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, 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, 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, SE, SI, SK, 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。

(57) 摘要：

本发明涉及一种 WiMAX 网络的多主机接入认证方法及系统，其中方法包括：接收到来自于一主机的接入请求消息后，将所述主机的标识信息携带于认证开始消息中发送给认证网元；根据接收到的来自于所述认证网元的认证响应消息中携带的所述标识信息，将所述认证响应消息转发给与所述标识信息相应的主机，以供所述主机接收到所述认证响应消息后，与认证服务器进行接入认证，并由所述认证服务器将认证结果发送给所述认证网元；接收所述认证网元发送的所述认证结果。系统包括：网元节点、基站、NAS 和认证服务器。通过本发明，使网元节点获知了主机的认证结果，根据该认证结果，网元节点可以决定是否开启或封闭授权端口，避免了非法用户的非法接入，提高了系统的安全性。

WiMAX 网络的多主机接入认证方法及系统

本申请要求于 2008 年 1 月 8 日提交中国专利局，申请号为 200810055741.4，发明名称为“WiMAX 网络的多主机接入认证方法及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及通信技术领域，尤其涉及一种微波接入全球互通（Worldwide Interoperability Microwave Access，简称：WiMAX）网络的多主机接入认证方法及系统。

背景技术

WiMAX 系统是一种互联网无线接入系统。随着因特网业务的蓬勃发展和无线网络的广泛应用，现有的 WiMAX 系统在组网形态上可以分为多主机（Multi-Host）场景和非多主机场景。

如图 1 所示，为非多主机场景的接入认证信令流程图。其中，请求方（Supplicant）移动台（Mobile Station，简称：MS）在空口上将可扩展认证协议（Extensible Authentication Protocol，简称：EAP）消息承载在私钥管理（Privacy Key Management，简称：PKM）v2 协议消息上；接入服务网络（Access Service Network，简称：ASN）内部的基站（Base Station，简称：BS）和网关（GateWay，简称：GW）之间将 EAP 消息承载在认证延迟（Auth. Relay）协议消息上；ASN 和连接服务网络（Connective Service Network，简称：CSN）之间则将 EAP 消息承载在 RADIUS 消息中。其中，PKMv2 是 802.16e 协议中定义的一套私钥管理协议版本 2，用于空中接口上的密钥安全联盟管理，以及承载 EAP 数据；认证延迟协议则是 WiMAX 接入网定义的一套承载 EAP 数据的协议。局域网可扩展认证协议（Extensible

Authentication Protocol over LAN，简称：EAPoL）是一种局域网上的认证承载协议，主要用于通过太网数据包封装 EAP 数据。

在非多主机场景中，进行 WiMAX 网络接入过程选择时，不同 ASN 会广播其所连接的网络服务提供商（Network Service Provider，简称：NSP）信息，包括直接相连的 NSP 以及可以通过漫游协议到达的 NSP。然后，由移动台根据自己的签约信息选择一个 ASN/NAP 进行接入，在接入认证消息中的网络接入标识（Network Access Identifier，简称：NAI）上给出网络选择的结果。

多主机场景是 WiMAX 系统的另一种组网形态，它可以在不同地点，例如在机场、咖啡吧或火车上利用多主机形式进行布局。如图 2 所示，为多主机场景下的 WiMAX 系统组网结构示意图。其中，ASN 由一个或多个无线基站和接入服务网络网关（Access Service Network GateWay，简称：ASN-GW）组成，ASN 作为一个逻辑实体，管理 IEEE 802.16 空中接口，为 WiMAX 用户提供无线接入；CSN 由计费服务器，例如认证授权计费（Authentication Authorization and Accounting，简称：AAA）服务器、家乡代理（Home Agent，简称：HA）和 IP 多媒体子系统（Internet Protocol Multimedia Subsystem，简称：IMS）核心组成，用于提供 IP 连接、服务和管理。

由于无线高保真（Wireless Fidelity，简称：WiFi）接入方式和以太网接入方式的价格优势，以及市场的高占有率，在布局的最末端可以使用 WiFi 和以太网进行接入，主机（HOST）和网关移动台（Gateway MS，简称：GMS）之间可以采用 WiMAX 接入方式进行连接。GMS 和 ASN 之间的连接可以采用 WiMAX 无线连接。GMS 可以在 HOST 接入之前就接入 ASN/CSN 网络；也可以在 HOST 接入之后再接入 ASN/CSN 网络。

现有技术的缺陷在于：现有 WiMAX 系统在多主机场景下对主机进行接入认证时，是把 EAP 消息作为空中接口上的数据进行发送的，这对于 BS/GMS 都是透明的。因此，BS 和 GMS 都并不知道 HOST 认证的结果。而在某些场景中，GMS 是需要知道 HOST 认证结果的，

例如，GMS 需要根据 HOST 的认证结果决定是否要开启或封闭端口，以避免非法用户的非法接入。

发明内容

本发明要解决的问题是：提供一种在对主机进行接入认证时，能够使 GMS 获知认证结果的 WiMAX 网络的多主机接入认证方法及系统。

为了解决上述问题，本发明的一个实施例提供了一种 WiMAX 网络的多主机接入认证方法，其中包括：

接收到来自于一主机的接入请求消息后，将所述主机的标识信息携带于认证开始消息中发送给认证网元；

根据接收到的来自于所述认证网元的认证响应消息中携带的所述标识信息，将所述认证响应消息转发给与所述标识信息相应的主机，以供所述主机接收到所述认证响应消息后，与认证服务器进行接入认证，并由所述认证服务器将认证结果发送给所述认证网元；

接收所述认证网元发送的所述认证结果。

为了解决上述问题，本发明的另一个实施例是提供了一种网元节点，包括：

第一网元模块，用于当接收到来自于一主机的接入请求消息后，将所述主机的标识信息携带于认证开始消息中进行发送；

第二网元模块，用于根据接收到的第一认证响应消息中携带的标识信息，将所述认证响应消息转发给与所述标识信息相应的主机。

为了解决上述问题，本发明的另一个实施例提供了一种 WiMAX 网络的多主机接入认证系统，包括网元节点、基站、NAS 和认证服务器，其中：

所述网元节点包括：

第一网元模块，用于当接收到来自于一主机的接入请求消息后，将所述主机的标识信息携带于认证开始消息中进行发送；

第二网元模块，用于根据接收到的第一认证响应消息中携带的标识信息，将所述认证响应消息转发给与所述标识信息相应的主机；

所述基站包括：

第一基站模块，用于当接收到来自于网元节点的认证开始消息后发出第一认证请求消息；

第二基站模块，用于将接收到的第一认证响应消息发送给所述网元节点；

所述 NAS 包括：

第一网络模块，用于当接收到来自于基站的所述第一认证请求消息后，回复第一认证响应消息；

第二网络模块，用于将来自于认证服务器的第一认证确认消息通过所述基站发送给所述网元节点；

所述认证服务器包括：

第一认证模块，用于当所述主机接收到所述第一认证响应消息后，与该主机进行接入认证；

第二认证模块，用于将第一认证模块的认证结果携带于第一认证确认消息中发送给所述 NAS。

通过本发明，使网元节点获知了主机的认证结果，根据该认证结果，网元节点可以决定是否开启或封闭授权端口，避免了非法用户的非法接入，提高了系统的安全性。

为了解决上述问题，本发明的另一个实施例还提供了一种 WiMAX 网络的多主机接入认证系统，包括主机、网元节点、认证网元和认证服务器，其中：

所述主机，用于向所述网元节点发送接入请求消息；

所述网元节点，用于接收到来自于一主机的接入请求消息后，将所述主机的标识信息携带于认证开始消息中发送给认证网元；根据接收到的来自于所述认证网元的认证响应消息中携带的所述标识信息，将所述认证响应消息转发给与所述标识信息相应的主机，以供所述主机接收到所述认证响应消息后，与认证服务器进行接入认证，并由所

述认证服务器将认证结果发送给所述认证网元；接收所述认证网元发送的所述认证结果；

所述认证网元，用于接收来自所述网元节点的认证开始消息后，向所述网元节点回复认证响应消息；

所述认证服务器，用于与所述主机进行接入认证，并将认证结果发送给所述认证网元。

下面通过附图和实施例，对本发明的技术方案做进一步的详细描述。

附图说明

图 1 为现有的非多主机场景下的 WiMAX 系统的接入认证信令流程图；

图 2 为现有的多主机场景下的 WiMAX 系统组网结构示意图；

图 3 为本发明方法实施例 1 所述的 WiMAX 网络的多主机接入认证方法的流程图；

图 4A 为本发明方法实施例 2 所述的 WiMAX 网络的多主机接入认证方法的流程图；

图 4B 为本发明方法实施例 2 所述的 WiMAX 网络的多主机接入认证方法的信令图；

图 5A 为本发明方法实施例 3 所述的 WiMAX 网络的多主机接入认证方法的流程图；

图 5B 为本发明方法实施例 3 所述的 WiMAX 网络的多主机接入认证方法的信令图；

图 5C 为本发明方法实施例 3 所述的 WiMAX 网络的多主机接入认证方法的另一信令图；

图 5D 为本发明方法实施例 3 所述的隧道建立过程的信令图；

图 5E 为本发明方法实施例 3 所述的隧道建立过程的数据面协议栈说明图；

图 6 为本发明系统实施例 1 所述的 WiMAX 网络的多主机接入认

证系统的结构示意图;

图 7 为本发明系统实施例 2 所述的 WiMAX 网络的多主机接入认证系统的结构示意图;

图 8 为本发明系统实施例 2 所述的另一种 WiMAX 网络的多主机接入认证系统的结构示意图。

具体实施方式

方法实施例 1

本实施例提供了一种 WiMAX 网络的多主机接入认证方法，如图 3 所示，包括:

步骤 101，网元节点接收到来自于一主机的接入请求消息后，将该主机的标识信息携带于认证开始消息中发送给网络侧的基站（Base Station，简称：BS）。

此处首先需要说明的是，上述网元节点具体可以为 GMS 等具有网关接入功能或类似功能的节点。为了叙述方便，在本实施例及以下各实施例中，仅以 GMS 为例进行说明，对于其他类型的网元节点，其相应的方法或结构与 GMS 的情况类似，此处不再赘述。

其中，上述主机是指在多主机场景下 WiMAX 系统中的某一主机。具体地，在请求接入认证时，主机可发送 EAPoL/EAP-START 信令作为接入请求消息，GMS 检测到所述 EAPoL/EAP-START 信令为 EAPoL 格式的数据包后，可以将该 EAPoL/EAP-START 信令转换为 PKMv2/EAP-START 信令，并将该主机的标识信息携带于该 PKMv2/EAP-START 信令中发送给基站，其中，标识信息可以为与主机的媒体访问控制（Media Access Control，简称：MAC）地址相关联的信息。

步骤 102，所述基站接收到所述认证开始消息后向认证网元发送认证请求消息。

其中，认证网元是指用于对主机进行认证的网元，可以根据

WiMAX 的具体网络架构而有所不同。例如，可以为网络中专门用于对主机进行认证的网络认证服务器（Network Authentication Server，简称：NAS），或者也可以为与一个后端网络连接的远程宽带接入服务器（Broadband Remote Access Server，简称：BRAS）。

步骤 103，所述认证网元向所述 GMS 回复认证响应消息。

具体地，可以先将认证响应消息回复给所述基站，再由所述基站将该认证响应消息封装为相应的信令格式后转发给所述 GMS。

步骤 104，GMS 根据所述认证响应消息中携带的标识信息，将该认证响应消息转发给与所述标识信息相应的主机。

具体地，可以先将该认证响应消息转换为相应的信令格式后再转发给所述主机。

步骤 105，所述主机接收到所述认证响应消息后，与认证服务器进行接入认证，并由所述认证服务器将认证结果携带于认证确认消息中发送给所述认证网元。

步骤 106，所述认证网元将所述认证确认消息通过所述基站发送给所述 GMS。

在主机认证过程中，在上行方向上，将认证请求经由认证网元进行信令格式转换后发送给认证服务器；在下行方向上，将认证确认消息经由认证网元进行信令格式转换后发送给 GMS。

步骤 107，另外，所述 GMS 当需要时还可以根据所述认证确认消息中携带的标识信息，将该认证确认消息转发给与所述标识信息相应的主机。

通过本实施例所述方法，网元节点获知了主机的认证结果，根据该认证结果，网元节点可以决定是否开启或封闭授权端口，避免了非法用户的非法接入，提高了系统的安全性。

方法实施例 2

本实施例提供了一种当 WiMAX 网络中的认证网元为 NAS 时的多主机接入认证方法，如图 4A 所示，包括：

步骤 201，GMS 接收到来自于一主机的接入请求消息后，将该主

机的标识信息携带于认证开始消息中发送给基站。

其中，上述主机是指在多主机场景下 WiMAX 系统中的某一主机。具体地，在请求接入认证时，主机可发送 EAPoL/EAP-START 信令作为接入请求消息，GMS 检测到所述 EAPoL/EAP-START 信令为 EAPoL 格式的数据包后，可以将该 EAPoL/EAP-START 信令转换为 PKMv2/EAP-START 信令，并将该主机的标识信息携带于该 PKMv2/EAP-START 信令中发送给基站。

步骤 202，所述基站接收到所述认证开始消息后向 NAS 发送第一认证请求消息。

其中，在多主机场景中，GMS 作为第一个认证控制点；因此，此时的 NAS 实际上发挥了接入网上的 AAA 代理的作用，同时也可能具有一些控制功能。具体地，NAS 可以为预先为所述 BS 配置好的一个默认的 NAS，所述 BS 下的接入终端都使用该 NAS。

具体地，所述第一认证请求消息可以为 AR-EAP-START 信令。

步骤 203，所述 NAS 向所述 GMS 回复第一认证响应消息。

具体地，可以先向所述基站回复 AR-EAP-Transfer/Identity-Req 信令；再由所述基站将所述 AR-EAP-Transfer/Identity-Req 信令封装为 PKM-RSP/EAP Transfer 信令后转发给所述 GMS。

步骤 204，GMS 根据所述第一认证响应消息中携带的标识信息，将该第一认证响应消息转发给与所述标识信息相应的主机。

具体地，可以将接收到的所述 PKM-RSP/EAP Transfer 信令转换为 EAPoL-Request 信令后发送给所述主机。

步骤 205，所述主机接收到所述第一认证响应消息后，与认证服务器进行接入认证，并由所述认证服务器将认证结果携带于第一认证确认消息中发送给所述 NAS。

具体地，在主机认证过程中，认证数据包中包括上述第一认证确认消息，该认证数据包经由 NAS 进行信令格式转换后发送给认证服务器。其中的信令格式转换包括从 R4/R6 信令 AR-EAP-Transfer 转换成 R3 接口上的基于 IP 的 RADIUS 或者 DIAMETER 等认证协议。

步骤 206，所述 NAS 将所述第一认证确认消息通过所述基站发送给所述 GMS。

具体地，NAS 将 R3 接口上的基于 IP 的 RADIUS 或者 DIAMETER 等认证协议的认证数据包，转换成 R4/R6 信令发送给基站，然后通过基站在空中接口上将上述认证数据包封装为 PKM 消息发送给 GMS。

步骤 207，另外，所述 GMS 当需要时还可以根据所述第一认证确认消息中携带的标识信息，将该第一认证确认消息转发给与所述标识信息相应的主机。如图 4B 所示，为本实施例所述方法的信令图。

通过本实施例所述方法，对主机进行了接入认证，并且使 GMS 获知了该主机的认证结果，根据该认证结果，GMS 可以决定是否开启或封闭授权端口，避免了非法用户的非法接入，提高了系统的安全性。

方法实施例 3

本实施例提供了一种当 WiMAX 网络中的认证网元为 BRAS 时的多主机接入认证方法，如图 5A 所示，包括:

步骤 301，GMS 接收到来自于一主机的接入请求消息后，将该主机的标识信息携带于认证开始消息中发送给基站。

步骤 302，所述基站接收到所述认证开始消息后向 BRAS 发送第二认证请求消息。

具体地，发送第二认证请求消息可以有多种形式，例如可以如图 5B 所示，先由所述基站将所述认证开始消息转换为 EAPoL 格式的第二认证请求消息后发送给所述 BRAS。其中，第二认证请求消息可以为 EAPoL-START 信令。此处需要说明的是，进行消息格式的转换时，也可以将所述认证开始消息先发送给 NAS，再由 NAS 将该认证开始消息转换为 EAPoL 格式的第二认证请求消息后发送给所述 BRAS。

或者，也可以如图 5C 所示，与所述 BRAS 建立以太网上点对点协议（PPP over Ethernet，简称: PPPoE）会话连接后，将第二认证请求消息转发给所述 BRAS。此时，第二认证请求消息可以为 EAPoPPP（EAP over Point to Point Protocol，基于点对点协议的 EAP）-START

信令。

步骤 303，所述 BRAS 向所述 GMS 回复第二认证响应消息。

具体地，在图 5B 所示信令流程中，第二认证响应消息可以为 EAPoL-Request/Identity 信令；在图 5C 所示信令流程中，第二认证响应消息可以为 EAPoPPP-Request/Identity 信令。

步骤 304，GMS 根据所述第二认证响应消息中携带的标识信息，将该第二认证响应消息转发给与所述标识信息相应的主机。

具体地，可以将接收到的所述 PKM-RSP/EAP Transfer 信令转换为 EAPoL-Request 信令后发送给所述主机。

步骤 305，所述主机接收到所述第二认证响应消息后，与认证服务器进行接入认证，并由所述认证服务器将认证结果携带于第二认证确认消息中发送给所述 BRAS。

具体地，在主机认证过程中，认证数据包中包括上述第二认证确认消息，该认证数据包经由 BRAS 进行信令格式转换后发送给认证服务器。其中，信令格式转换包括：从 EAPoL 或者 EAPoPPP 信令转换成 R3 接口（BRAS 和 AAA 之间的接口）上的基于 IP 的 RADIUS 或者 DIAMETER 等认证协议；或者在相反方向上，R3 接口上的基于 IP 的 RADIUS 或者 DIAMETER 等认证协议的认证数据包，转换成 EAPoL 或者 EAPoPPP 信令发送给基站，然后通过基站在空中接口上封装为 PKM 消息发送给 GMS。

此处需要特别指出的是，为了进一步提高数据传输的效率，当认证通过时，即可以开始隧道建立过程。具体包括建立所述 BRAS 与 HA 之间的隧道及所述 HA 与 ASN 之间的隧道。其中，BRAS 与 HA 之间的隧道可以为移动 IP（Mobile IP，简称：MIP）隧道；HA 与 ASN 之间的隧道可以为代理移动 IP（Proxy Mobile IP，简称：PMIP）隧道。隧道建立后，再将认证结果通知所述主机，当主机得到认证通过的结果后，可以直接利用已建立的隧道进行以太网数据包的传输。具体地，主机可以先将以太网数据包发送到 GMS；由 GMS 通过空中接口的以太网会聚子层（Ethernet Convergence Sublayer，简称：Eth-CS）发送

到外部代理（Foreign Agent，简称 FA）；FA 进行 MIP 数据的封装，进而转发给 HA，最后由 HA 封装转发给 BRAS。

具体的隧道建立过程如信令图 5D 所示，主要包括以下步骤：当认证服务器得到认证成功结果后，通知 HA 建立到 BRAS 的隧道以及 HA 建立 MIP 隧道所需要的密钥信息，并且还将认证成功结果返回给 ASN；当 ASN 中的 NAS 收到认证服务器返回的认证成功结果后，发送 MIP 请求（简称：MIP-RRQ），建立 PMIP 隧道。其具体的数据面协议栈如图 5E 所示。

步骤 306，所述 BRAS 将所述第二认证确认消息通过所述基站发送给所述 GMS。

步骤 307，另外，所述 GMS 当需要时还可以根据所述第二认证确认消息中携带的标识信息，将该第二认证确认消息转发给与所述标识信息相应的主机。

另外，如果在上述步骤的执行过程中，主机还把网络层配置的信息告知了 ASN，则 ASN 可以继续代理主机完成点对点协议（Point-to-Point Protocol，简称：PPP）的网络核心协议（Network Core Protocol，简称：NCP）过程，然后把结果告知主机；或者主机利用建立起来的 PPP 信道，通过动态主机配置协议（Dynamic Host Configuration Protocol，简称：DHCP）等形式进行高层配置信息的获取。

通过本实施例所述方法，通过 BRAS 对主机进行了接入认证，并且使 GMS 获知了该主机的认证结果，根据该认证结果，GMS 可以决定是否开启或封闭授权端口，避免了非法用户的非法接入，提高了系统的安全性。

系统实施例 1

本实施例提供了一种 WiMAX 网络的多主机接入认证系统，如图 6 所示，包括网元节点 10、基站 20、NAS30 和认证服务器 40，其中：网元节点 10 包括第一网元模块 11 和第二网元模块 12；所述基站 20 包括第一基站模块 21 和第二基站模块 22；所述 NAS30 包括第一网

络模块 31 和第二网络模块 32；所述认证服务器 40 包括第一认证模块 41 和第一认证模块 42。其中，网元节点 10 具体可以为 GMS 等具有网关接入功能或类似功能的节点。其工作原理如下：

网元节点 10 的第一网元模块 11 当接收到来自于一主机的接入请求消息后，将该主机的标识信息携带于认证开始消息中进行发送；基站 20 中的第一基站模块 21 当接收到来自于网元节点 10 的认证开始消息后发出第一认证请求消息；NAS30 的第一网络模块 31 当接收到来自于基站 20 发出的所述第一认证请求消息后，回复第一认证响应消息；基站 20 中的第二基站模块 22 将接收到的来自于 NAS30 的第一认证响应消息发送给网元节点 10；网元节点 10 的第二网元模块 12 根据接收到的来自于基站 20 第一认证响应消息中携带的标识信息，将该第一认证响应消息转发给与所述标识信息相应的主机；

当所述主机接收到所述第一认证响应消息后，与认证服务器 40 的第一认证模块 41 进行接入认证；认证服务器 40 的第二认证模块 42 将第一认证模块 41 的认证结果携带于第一认证确认消息中发送给 NAS30；NAS30 的第二网络模块 32 将来自于认证服务器 40 的第一认证确认消息通过 20 基站发送给网元节点 10。

通过本实施例所述系统，通过 NAS 对主机进行了接入认证，并且使 GMS 获知了该主机的认证结果，根据该认证结果，GMS 可以决定是否开启或封闭授权端口，避免了非法用户的非法接入，提高了系统的安全性。

系统实施例 2

本实施例在系统实施例 1 的基础上进行了改进，提供了另一种 WiMAX 网络的多主机接入认证系统，如图 7 所示，其中除了包括系统实施例 1 所述各模块以外，还包括 BRAS50，该 BRAS50 中包括第一远程模块 51 和第二远程模块 52；另外，基站 20 中还包括：第三基站模块 23。其工作原理如下：

基站 20 的第三基站模块 23 接收到来自于网元节点 10 的认证开始消息后，将该认证开始消息转换为 EAPoL 格式的第二认证请求消

息，并发送给 BRAS50；BRAS50 中的第一远程模块 51 当接收到来自于基站 20 的第二认证请求消息后，向基站 20 回复第二认证响应消息。

基站 20 中的第二基站模块 22 将接收到的来自于 BRAS50 的第二认证响应消息发送给网元节点 10；网元节点 10 的第二网元模块 12 根据接收到的来自于基站 20 第二认证响应消息中携带的标识信息，将该第二认证响应消息转发给与所述标识信息相应的主机；

当所述主机接收到所述第二认证响应消息后，与认证服务器 40 的第一认证模块 41 进行接入认证；认证服务器 40 的第二认证模块 42 将第一认证模块 41 的认证结果携带于第二认证确认消息中发送给 BRAS50；BRAS50 的第二远程模块 52 将来自于认证服务器的第二认证确认消息通过基站 20 发送给网元节点 10。

上述 NAS 和 BRAS 在物理层面上可以同时存在，在实际实现本发明实施例提供的方法时，可以选择其中的一个来实现认证网元的功能。

另外，如图 8 所示，本实施中所述的 WiMAX 网络的多主机接入认证系统中还可以进一步包括 HA60，用于当所述认证服务器将认证结果携带于第二认证确认消息中发送给所述 BRAS 之后，与所述 BRAS 建立隧道，具体地，可以建立 MIP 隧道；并与所述 NAS 所在的 ASN 建立隧道，具体地，可以建立 PMIP 隧道，以进一步提高数据传输的效率。

通过本实施例所述系统，通过 BRAS 对主机进行了接入认证，并且使 GMS 获知了该主机的认证结果，根据该认证结果，GMS 可以决定是否开启或封闭授权端口，避免了非法用户的非法接入，提高了系统的安全性。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以

软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述的方法。

以上公开的仅为本发明的几个具体实施例，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

权利要求

1、一种微波接入全球互通 WiMAX 网络的多主机接入认证方法，其特征在于，包括:

接收到来自于一主机的接入请求消息后，将所述主机的标识信息携带于认证开始消息中发送给认证网元;

根据接收到的来自于所述认证网元的认证响应消息中携带的所述标识信息，将所述认证响应消息转发给与所述标识信息相应的主机，以供所述主机接收到所述认证响应消息后，与认证服务器进行接入认证，并由所述认证服务器将认证结果发送给所述认证网元;

接收所述认证网元发送的所述认证结果。

2、根据权利要求 1 所述的 WiMAX 网络的多主机接入认证方法，其特征在于，将所述主机的标识信息携带于认证开始消息中发送给认证网元包括:

所述网络侧中的基站接收到所述认证开始消息后向认证网元发送认证请求消息;

所述认证请求消息携带所述主机的标识信息。

3、根据权利要求 2 所述的 WiMAX 网络的多主机接入认证方法，其特征在于，所述认证网元为网络认证服务器 NAS，所述基站向所述认证网元发送认证请求消息包括: 向所述 NAS 发送第一认证请求消息。

4、根据权利要求 2 所述的 WiMAX 网络的多主机接入认证方法，其特征在于，所述认证网元为远程宽带接入服务器 BRAS，所述基站向所述认证网元发送认证请求消息包括: 向所述 BRAS 发送第二认证请求消息。

5、根据权利要求 4 所述的 WiMAX 网络的多主机接入认证方法，其特征在于，所述基站向 BRAS 发送第二认证请求消息包括: 将所述认证开始消息转换为局域网可扩展认证协议 EAPoL 格式的第二认证请求消息后发送给所述 BRAS。

6、根据权利要求 4 所述的 WiMAX 网络的多主机接入认证方法，其特征在于，所述基站向 BRAS 发送第二认证请求消息包括:

将所述认证开始消息发送给 NAS;

所述 NAS 将所述认证开始消息转换为 EAPoL 格式的第二认证请求消息后发送给所述 BRAS。

7、根据权利要求 4 所述的 WiMAX 网络的多主机接入认证方法，其特征在于，所述基站向 BRAS 发送第二认证请求消息包括: 与所述 BRAS 建立以太网上点对点协议 PPPoE 会话连接后，将第二认证请求消息转发给所述 BRAS。

8、根据权利要求 6 所述的 WiMAX 网络的多主机接入认证方法，其特征在于，当所述认证网元为 BRAS 时，所述认证服务器将认证结果发送给所述认证网元，包括:

认证服务器将携带所述认证结果的认证确认消息发送给所述 BRAS; 所述方法还包括:

在所述 BRAS 与家乡代理 HA 之间建立隧道;

在所述 HA 与所述 NAS 所在的 ASN 之间建立隧道。

9、根据权利要求 1 所述的 WiMAX 网络的多主机接入认证方法，其特征在于，在所述主机与所述认证服务器的认证过程中，所述认证网元对携带有所述认证结果的认证数据包进行信令格式转换。

10、根据权利要求 1 所述的 WiMAX 网络的多主机接入认证方法，其特征在于，所述接收所述认证网元发送的所述认证结果之后，还包括: 根据携带所述认证结果的认证确认消息中的标识信息，将该认证确认消息转发给与所述标识信息相应的主机。

11、一种网元节点，其特征在于，包括:

第一网元模块，用于当接收到来自于一主机的接入请求消息后，将所述主机的标识信息携带于认证开始消息中进行发送;

第二网元模块，用于根据接收到的第一认证响应消息中携带的标识信息，将所述认证响应消息转发给与所述标识信息相应的主机。

12、一种 WiMAX 网络的多主机接入认证系统，包括网元节点、

基站、NAS 和认证服务器，其特征在于:

所述网元节点包括:

第一网元模块，用于当接收到来自于一主机的接入请求消息后，将所述主机的标识信息携带于认证开始消息中进行发送;

第二网元模块，用于根据接收到的第一认证响应消息中携带的标识信息，将所述认证响应消息转发给与所述标识信息相应的主机;

所述基站包括:

第一基站模块，用于当接收到来自于网元节点的认证开始消息后发出第一认证请求消息;

第二基站模块，用于将接收到的第一认证响应消息发送给所述网元节点;

所述 NAS 包括:

第一网络模块，用于当接收到来自于基站的所述第一认证请求消息后，回复第一认证响应消息;

第二网络模块，用于将来自于认证服务器的第一认证确认消息通过所述基站发送给所述网元节点;

所述认证服务器包括:

第一认证模块，用于当所述主机接收到所述第一认证响应消息后，与该主机进行接入认证;

第二认证模块，用于将第一认证模块的认证结果携带于第一认证确认消息中发送给所述 NAS。

13、根据权利要求 12 所述的 WiMAX 网络的多主机接入认证系统，其特征在于，还包括 BRAS，

所述基站还包括:

第三基站模块，用于将来自于网元节点的所述认证开始消息转换为 EAPoL 格式的第二认证请求消息后发送给所述 BRAS;

所述 BRAS 包括:

第一远程模块，用于当接收到来自于基站的第二认证请求消息后，回复第二认证响应消息;

第二远程模块，用于将来自于认证服务器的第二认证确认消息通过所述基站发送给所述网元节点。

14、根据权利要求 13 所述的 WiMAX 网络的多主机接入认证系统，其特征在于，所述基站还包括：第四基站模块，用于与所述 BRAS 建立 PPPoE 会话连接。

15、根据权利要求 14 所述的 WiMAX 网络的多主机接入认证系统，其特征在于，还包括：HA，用于与所述 BRAS 建立隧道；并与所述 NAS 所在的 ASN 建立隧道。

16、一种 WiMAX 网络的多主机接入认证系统，包括主机、网元节点、认证网元和认证服务器，其特征在于：

所述主机，用于向所述网元节点发送接入请求消息；

所述网元节点，用于接收到来自于一主机的接入请求消息后，将所述主机的标识信息携带于认证开始消息中发送给认证网元；根据接收到的来自于所述认证网元的认证响应消息中携带的所述标识信息，将所述认证响应消息转发给与所述标识信息相应的主机，以供所述主机接收到所述认证响应消息后，与认证服务器进行接入认证，并由所述认证服务器将认证结果发送给所述认证网元；接收所述认证网元发送的所述认证结果；

所述认证网元，用于接收来自所述网元节点的认证开始消息后，向所述网元节点回复认证响应消息；

所述认证服务器，用于与所述主机进行接入认证，并将认证结果发送给所述认证网元。

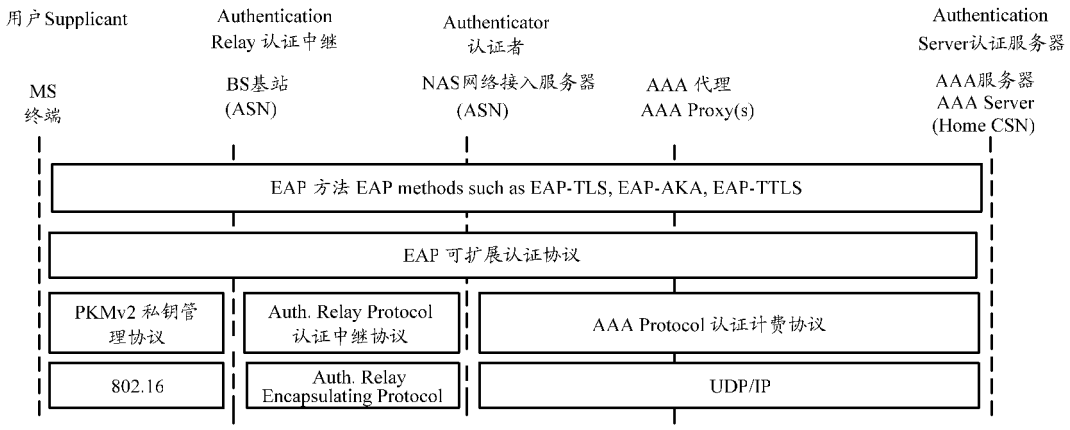
用户 Supplicant
Authentication Relay 认证中继
Authenticator 认证者
Authentication Server认证服务器
MS 终端
BS基站 (ASN)
NAS网络接入服务器 (ASN)
AAA 代理 AAA Proxy(s)
AAA服务器 AAA Server (Home CSN)
EAP 方法 EAP methods such as EAP-TLS, EAP-AKA, EAP-TTLS
EAP 可扩展认证协议
PKMv2 私钥管理协议
Auth. Relay Protocol 认证中继协议
AAA Protocol 认证计费协议
802.16
Auth. Relay Encapsulating Protocol
UDP/IP

图 1

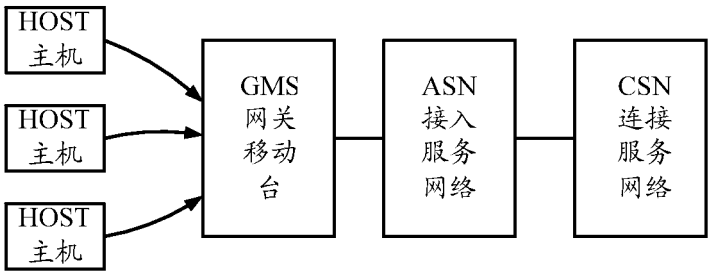
HOST 主机
HOST 主机
HOST 主机
GMS 网关 移动 台
ASN 接入 服务 网络
CSN 连接 服务 网络

图 2

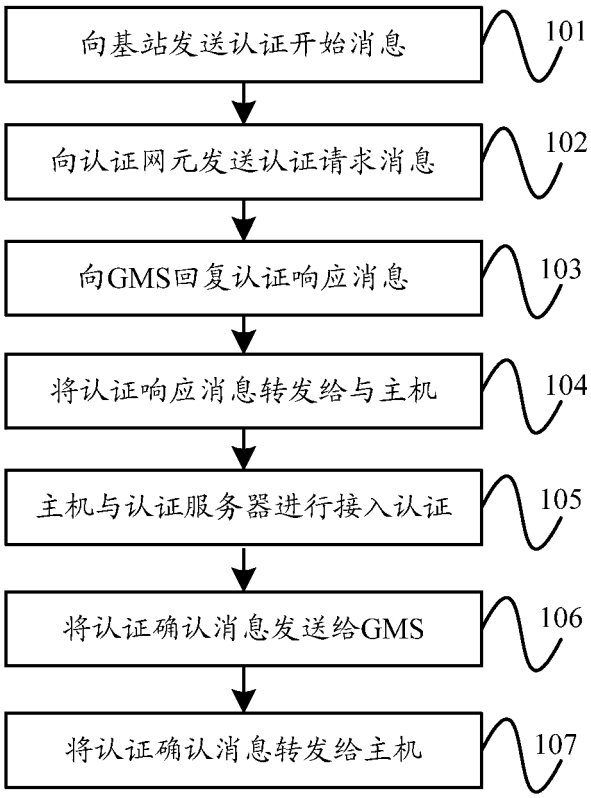
向基站发送认证开始消息
101
向认证网元发送认证请求消息
102
向GMS回复认证响应消息
103
将认证响应消息转发给与主机
104
主机与认证服务器进行接入认证
105
将认证确认消息发送给GMS
106
将认证确认消息转发给主机
107

图 3

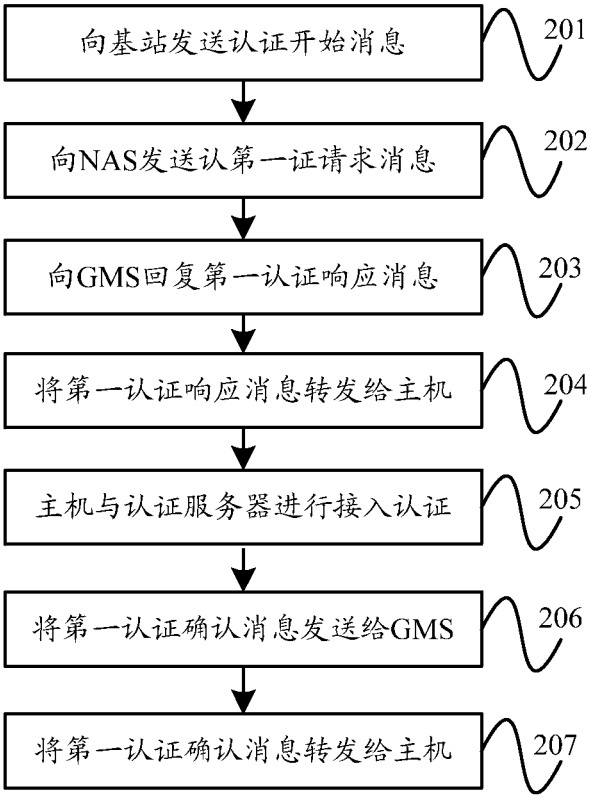
向基站发送认证开始消息
201
向NAS发送认第一证请求消息
202
向GMS回复第一认证响应消息
203
将第一认证响应消息转发给主机
204
主机与认证服务器进行接入认证
205
将第一认证确认消息发送给GMS
206
将第一认证确认消息转发给主机
207

图 4A

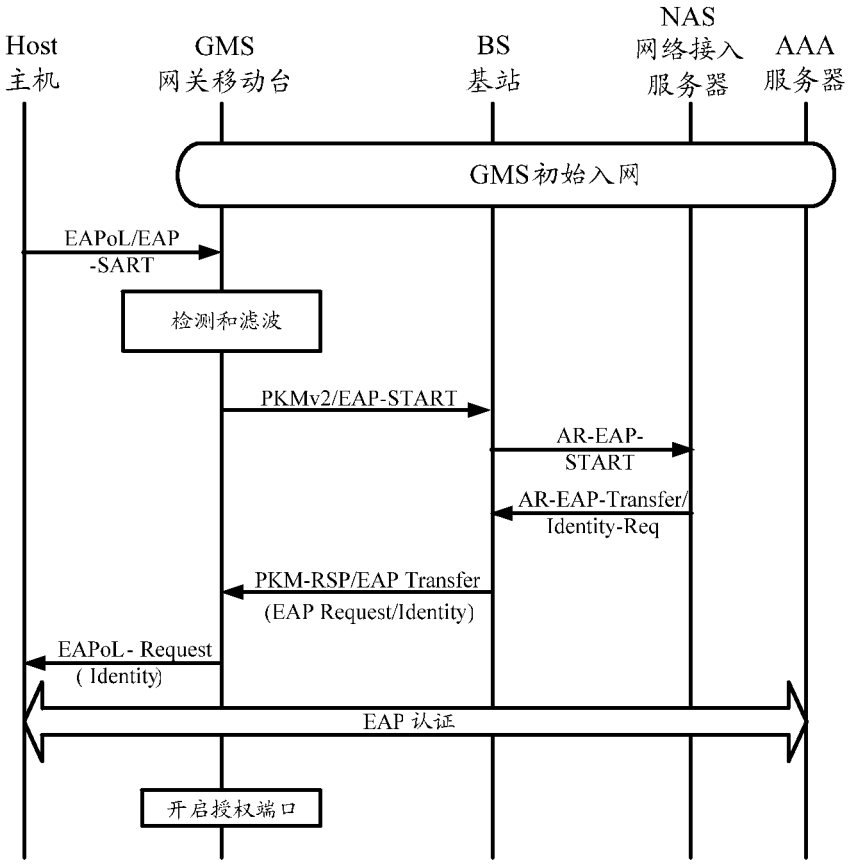
Host
主机
GMS
网关移动台
BS
基站
NAS
网络接入
服务器
AAA
服务器
GMS初始入网
EAPoL/EAP
-SART
检测和滤波
PKMv2/EAP-START
AR-EAP-
START
AR-EAP-Transfer/
Identity-Req
PKM-RSP/EAP Transfer
(EAP Request/Identity)
EAPoL- Request
(Identity)
EAP 认证
开启授权端口

图 4B

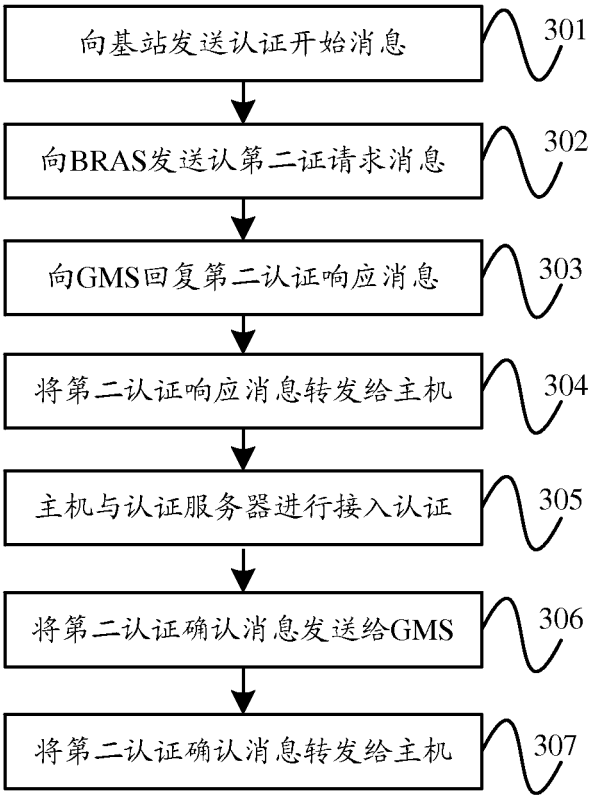
向基站发送认证开始消息
301
向BRAS发送认第二证请求消息
302
向GMS回复第二认证响应消息
303
将第二认证响应消息转发给主机
304
主机与认证服务器进行接入认证
305
将第二认证确认消息发送给GMS
306
将第二认证确认消息转发给主机
307

图 5A

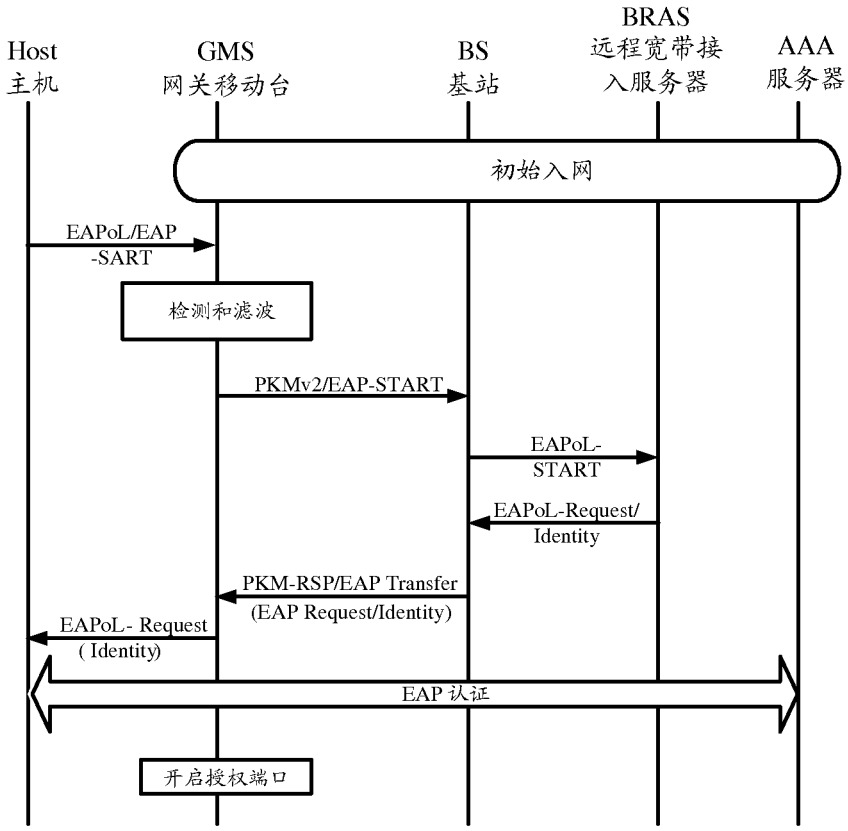
Host
主机
GMS
网关移动台
BS
基站
BRAS
远程宽带接入服务器
AAA
服务器
初始入网
EAPoL/EAP-SART
检测和滤波
PKMv2/EAP-START
EAPoL-START
EAPoL-Request/Identity
PKM-RSP/EAP Transfer
(EAP Request/Identity)
EAPoL- Request
(Identity)
EAP 认证
开启授权端口

图 5B

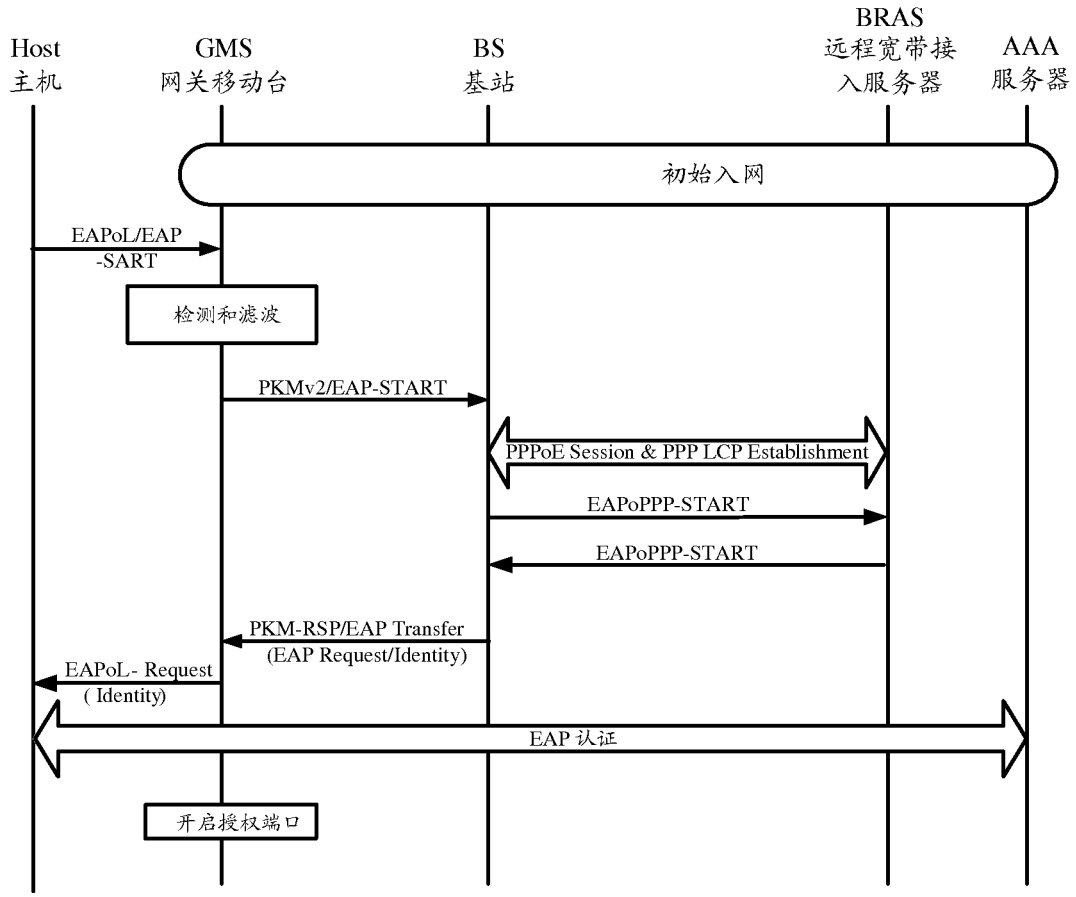
Host
主机
GMS
网关移动台
BS
基站
BRAS
远程宽带接入服务器
AAA
服务器
初始入网
EAPoL/EAP -SART
检测和滤波
PKMv2/EAP-START
PPPoE Session & PPP LCP Establishment
EAPoPPP-START
EAPoPPP-START
PKM-RSP/EAP Transfer
(EAP Request/Identity)
EAPoL- Request
(Identity)
EAP 认证
开启授权端口

图 5C

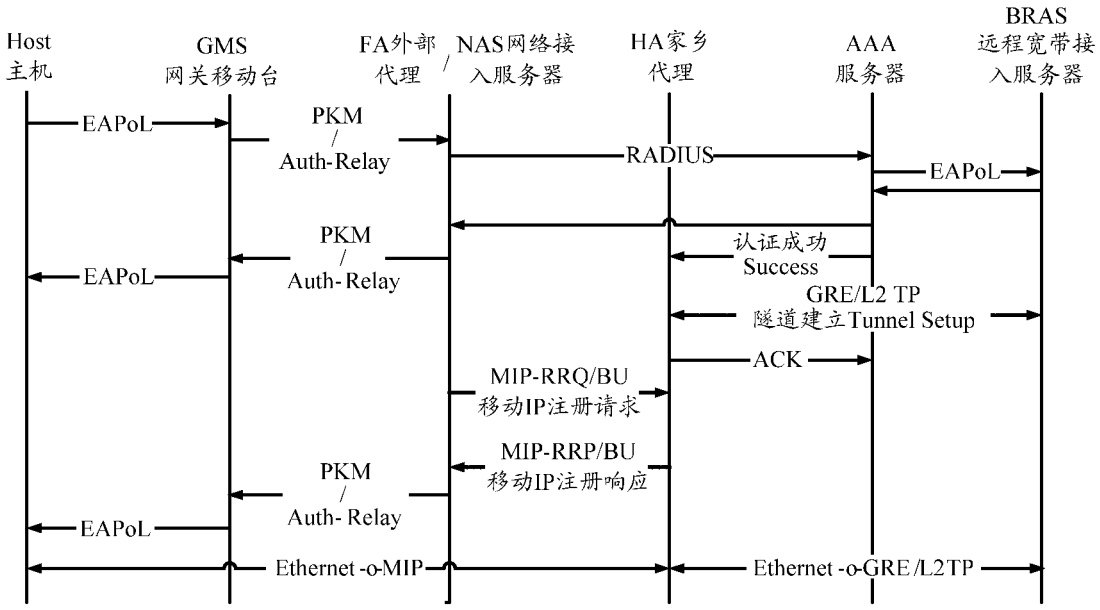
Host
主机
GMS
网关移动台
FA外部代理
NAS网络接入服务器
HA家乡代理
AAA服务器
BRAS
远程宽带接入服务器
EAPoL
PKM
/
Auth-Relay
RADIUS
EAPoL
PKM
/
Auth-Relay
认证成功
Success
EAPoL
GRE/L2 TP
隧道建立Tunnel Setup
ACK
MIP-RRQ/BU
移动IP注册请求
MIP-RRP/BU
移动IP注册响应
PKM
/
Auth-Relay
EAPoL
Ethernet -o-MIP
Ethernet -o-GRE /L2TP

图 5D

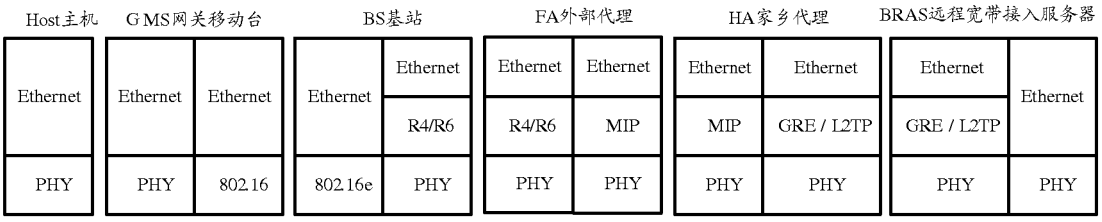
Host主机
GMS网关移动台
BS基站
FA外部代理
HA家乡代理
BRAS远程宽带接入服务器
Ethernet
Ethernet
Ethernet
Ethernet
R4/R6
Ethernet
Ethernet
R4/R6
MIP
Ethernet
Ethernet
MIP
GRE / L2TP
Ethernet
Ethernet
GRE / L2TP
PHY
PHY
802.16
802.16e
PHY
PHY
PHY
PHY
PHY
PHY

图 5E

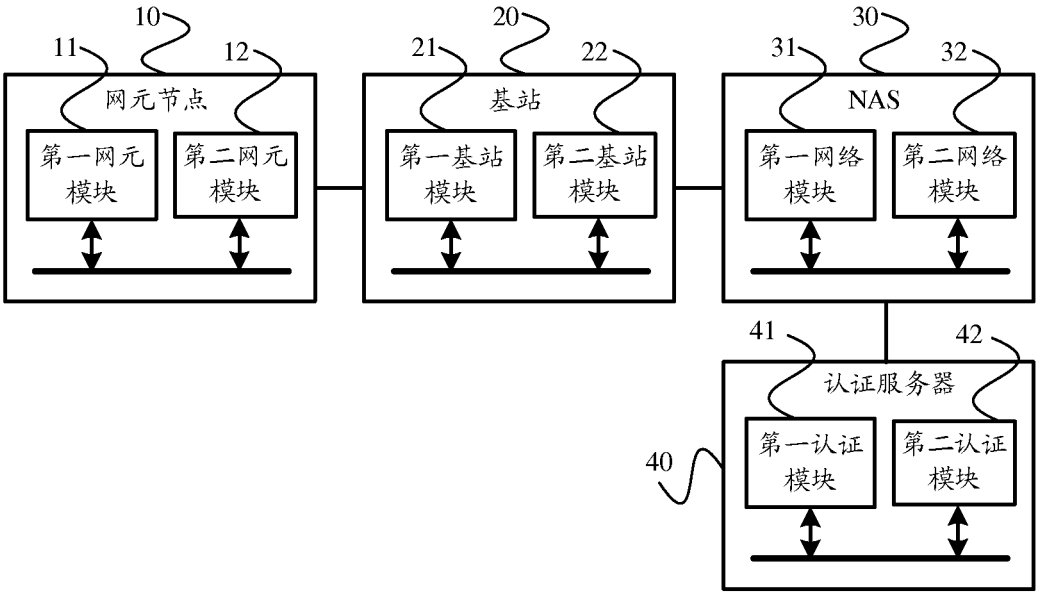
10
11
12
网元节点
第一网元模块
第二网元模块
20
21
22
基站
第一基站模块
第二基站模块
30
31
32
NAS
第一网络模块
第二网络模块
41
42
认证服务器
第一认证模块
第二认证模块
40

图 6

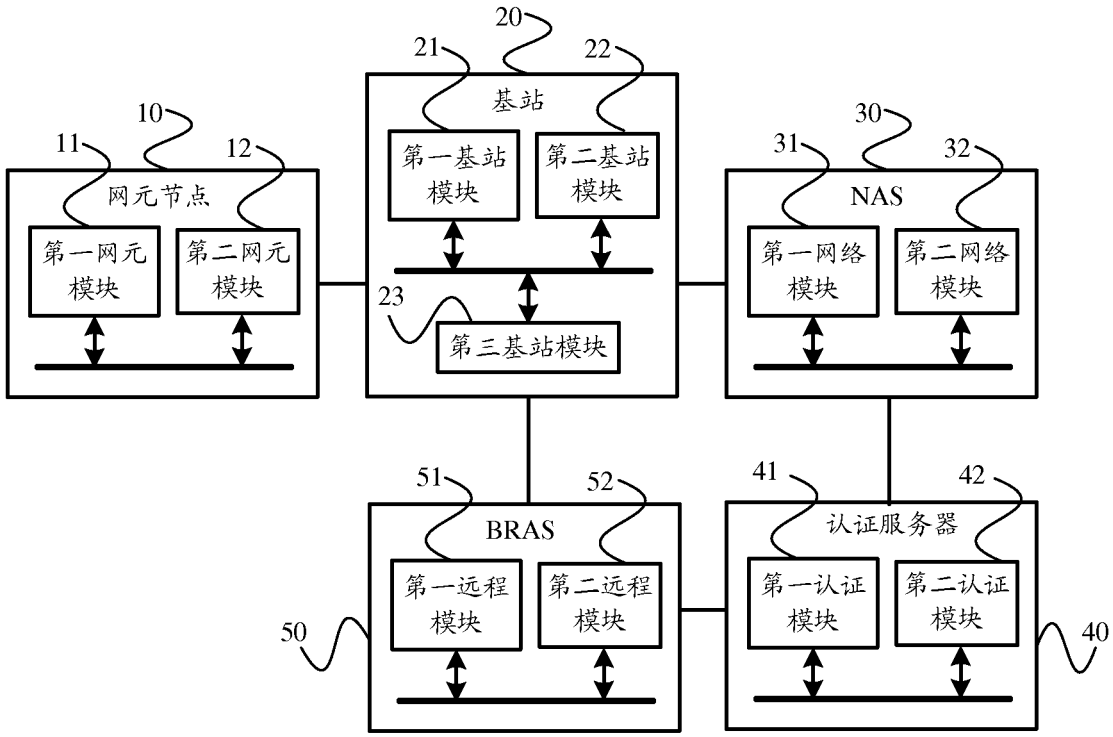
20
21
22
基站
第一基站模块
第二基站模块
23
第三基站模块
10
11
12
网元节点
第一网元模块
第二网元模块
30
31
32
NAS
第一网络模块
第二网络模块
51
52
BRAS
第一远程模块
第二远程模块
50
41
42
认证服务器
第一认证模块
第二认证模块
40

图 7

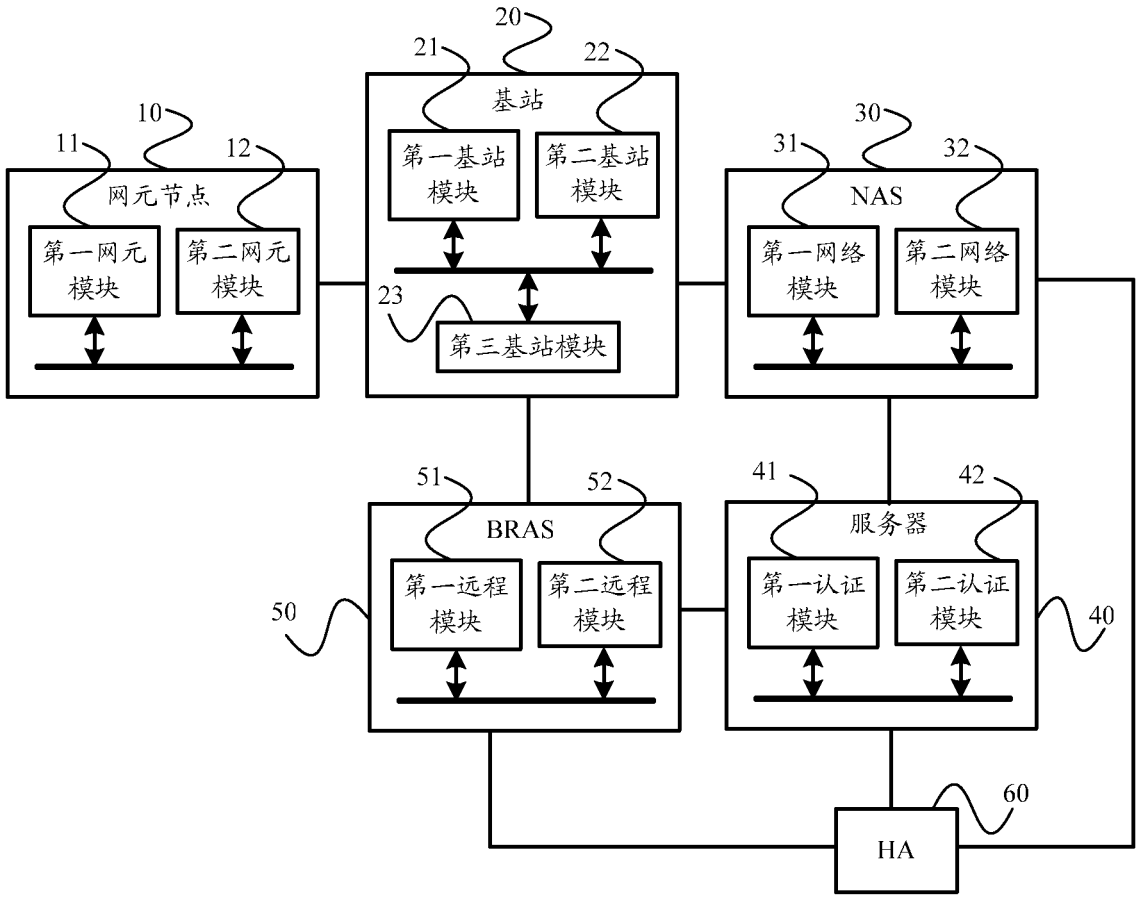
20
21
22
基站
第一基站模块
第二基站模块
23
第三基站模块
10
11
12
网元节点
第一网元模块
第二网元模块
30
31
32
NAS
第一网络模块
第二网络模块
51
52
BRAS
第一远程模块
第二远程模块
50
41
42
服务器
第一认证模块
第二认证模块
40
60
HA

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/070035

A. CLASSIFICATION OF SUBJECT MATTER

H04W12/08(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: H04B, 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)

CNPAT,CNKI,WPI,EPODOC,PAJ: wimax, access+, authenticat+, certificat+, request+, require+, ask+, respon+, answer+, report+, notif+, return+, feedback+, server, host, multi+, net+.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN1972505A (HUAWEI TECHNOLOGIES CO., LTD.) 30 May 2007 (30.05.2007) the description page 8 lines 5-25, fig. 4	1-16
Y	CN1486029A (HUAWEI TECHNOLOGIES CO., LTD.) 31 Mar. 2004 (31.03.2004) the description page 3 lines 1-9	1-16
A	CN1455551A(UNIV DONGHUA) 12 Nov. 2003 (12.11.2003) The whole document	1-16

☐ 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
31 Mar. 2009 (31.03.2009)	**09 Apr. 2009 (09.04.2009)**
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 JIN Xi Telephone No. (86-10)62411334

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2009/070035

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1972505A	30.05.2007	None	
CN1486029A	31.03.2004	CN1243434C	22.02.2006
CN1455551A	12.11.2003	None	

国际检索报告

国际申请号
PCT/CN2009/070035

A. 主题的分类

H04W12/08(2009.01)i

按照国际专利分类表(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: H04B, 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） CNPAT,CNKI,WPI,EPODOC,PAJ: ＷＩＭＡＸ,接入,认证,鉴权,请求,要求,响应,报告,反馈,回送,回传,服务器,多主机,网元, access+, authenticat+, certificat+, request+, require+, ask+, respon+, answer+, report+, notif+, return+, feedback+, server, host, multi+, net+.

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
Y	CN1972505A(华为技术有限公司)30.5 月 2007（30.05.2007） 说明书第 8 页第 5-25 行，图 4	1-16
Y	CN1486029A(华为技术有限公司)31.3 月 2004（31.03.2004） 说明书第 3 页第 1-9 行	1-16
A	CN1455551A(东华大学) 12.11 月 2003（12.11.2003） 全文	1-16

☐ 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

"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
31. 3 月 2009（31.03.2009）	**09.4 月 2009 (09.04.2009)**
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 金曦 电话号码：(86-10) **62411334**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2009/070035

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1972505A	30.05.2007	无	
CN1486029A	31.03.2004	CN1243434C	22.02.2006
CN1455551A	12.11.2003	无	