(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 11 月 29 日 (29.11.2012)

WIPO | PCT

(10) 国际公布号
WO 2012/159356 A1

(51) 国际专利分类号:
H04W 12/04 (2009.01)

(21) 国际申请号: PCT/CN2011/077808

(22) 国际申请日: 2011 年 7 月 29 日 (29.07.2011)

(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): **王锐 (WANG, Rui)** [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)。 **刘晟 (LIU, Sheng)** [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)。 **杜颖钢 (DU, Yinggang)** [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: **深圳市深佳知识产权代理事务所（普通合伙） (SHENPAT INTELLECTUAL PROPERTY AGENCY)**; 中国广东省深圳市国贸大厦 15 楼西座 1521 室, Guangdong 518014 (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, 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))。

[见续页]

(54) Title: METHOD, APPARATUS AND SYSTEM FOR SIMPLIFYING WIRELESS LOCAL AREA NETWORK AUTHENTICATION

(54) 发明名称 : 一种简化无线局域网认证的方法、装置及系统

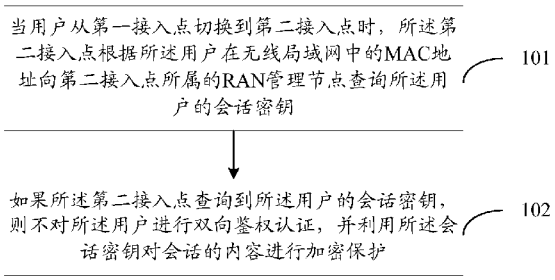

图 1 / Fig. 1

101 When a user switches from a first access point to a second access point, the second access point asks the RAN management node to which the second access point belongs about the session key of the user according to the MAC address of the user on the wireless local area network
102 If the second access point finds the session key of the user, bidirectional authentication of the user will not be carried out and the session key will be used for encrypting the session content for protection

(57) **Abstract**: Provided is a method for simplifying a wireless local area network authentication, a method, apparatus and system for storing a session key. The method for simplifying wireless local area network authentication comprises: a first access point, after successfully completing bidirectional authentication with a user, sending a session key of the user and the media access control (MAC) address of the user on a wireless local area network to a wireless radio access network (RAN) management node for storage; when the user switches from the first access point to a second access point, the second access point asks the RAN management node to which the second access point belongs about the session key of the user according to the MAC address of the user on the wireless local area network (101); and if the second access point finds the session key of the user, bidirectional authentication of the user will not be carried out and the session key will be used for encrypting the session content for protection (102). By means of the present invention, the number of times bidirectional authentication is performed is reduced, and both the delay in accessing access points on the wireless local area network and the load on authentication servers in the core network are reduced.

(57) 摘要:

[见续页]

WO 2012/159356 A1

— 在修改权利要求的期限届满之前进行，在收到该修改后将重新公布(细则 48.2(h))。

— 根据申请人的请求，在条约第 21 条(2)(a)所规定的期限届满之前进行。

提供一种简化无线局域网认证的方法、会话密钥存储方法、装置及系统。所述简化无线局域网认证的方法包括：第一接入点在与用户进行双向鉴权认证成功后，将用户的会话密钥及用户在无线局域网中的媒体接入控制层（MAC）地址发送给无线蜂窝网络接入网（RAN）管理节点存储；当用户从第一接入点切换到第二接入点时，所述第二接入点根据所述用户在无线局域网中的 MAC 地址向第二接入点所属的 RAN 管理节点查询所述用户的会话密钥（101）；如果所述第二接入点查询到所述用户的会话密钥，则不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护（102）。利用本发明，减少了重新进行双向鉴权的次数，降低了无线局域网中的接入点的接入时延和核心网中认证服务器的负担。

一种简化无线局域网认证的方法、装置及系统

技术领域

本发明涉及通信技术领域，特别涉及一种简化无线局域网认证的方法、装置及系统。

背景技术

随着人们对无线通信需求的不断增加，现有的无线蜂窝网络的带宽将很难为满足未来的需求。虽然无线蜂窝技术正在不断的演进，但是由于频谱本身的约束，其吞吐量在未来的提升将比较有限。为了解决无线通信的带宽瓶颈，把无线蜂窝技术和 WLAN 技术相互融合。

目前，无线蜂窝网络和 WLAN 融合有多种方案。

一种融合的技术方案为：WLAN 的 AP 通过某个逻辑链路连接到无线蜂窝网络接入网(RAN)的某个管理节点中，并且受该管理节点的管理；该管理节点对接收到的数据进行转发。当用户从一个 AP 的覆盖范围进入另一个 AP 的覆盖范围时，用户需要通过 AAA 服务器重新进行认证。这样会给 AAA 服务器带来很大的通信负担，同时也给用户接入带来较大的时延。

另一种融合的技术方案为：在 IWLAN 体系中为用户接入 WLAN AP 进行认证过程。其中，IWLAN 是另一种 WLAN 与无线蜂窝网络的融合框架。在 IWLAN 的框架下面，WLAN 的 AP 和无线蜂窝网络 RAN 侧的节点是没有直接的逻辑连接，用户设备上的 UMTS 空口和 WLAN 空口是采用的认证协议分别为 UMTS-AKA 和 EAP-AKA。

在对现有技术的研究和实践过程中，本发明的发明人发现，现有的实现方式中，当用户从一个 AP 的覆盖范围进入另一个 AP 的覆盖范围时，用户需要重新进行认证。这样会给 AAA 服务器带来很大的通信负担，同时也给用户接入带来较大的时延。

发明内容

有鉴于此，本发明实施例提供一种简化无线局域网认证的方法、会话密钥存储方法、装置及系统，以解决在用户发生 AP 切换时，减少用户重新进行双

向鉴权的次数，降低了 WLAN AP 的接入时延。

本发明实施例提供一种简化无线局域网认证的方法，所述方法包括:

当用户从第一接入点切换到第二接入点时，所述第二接入点根据所述用户在无线局域网中的媒体接入控制层 MAC 地址向所述第二接入点所属的 RAN 管理节点查询所述用户的会话密钥;

如果所述第二接入点查询到所述用户的会话密钥，则不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护。

相应的，本发明实施例还提供一种会话密钥存储方法，所述方法包括:

无线蜂窝网络接入网RAN管理节点接收到至少一个接入点发送的用户认证信息，所述用户认证信息包括: 第一会话密钥及用户在无线局域网中的媒体接入控制层MAC地址;

RAN管理节点保存和维护所述用户的认证信息。

相应的，本发明实施例提供一种简化无线局域网认证的装置，与无线蜂窝网络接入网RAN管理节点进行数据交互，所述装置包括:

第一查询单元，用于在用户从第一接入点切换到该简化无线局域网认证的装置时，根据用户在无线局域网中的媒体接入控制层MAC地址向所述装置所属的RAN管理节点查询所述用户的会话密钥;

加密单元，用于所述第一查询单元查询到所述用户的会话密钥，则不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护。

本发明实施例还提供一种会话密钥存储装置，所述装置包括:

接收单元，用于接收到至少一个接入点发送的用户认证信息，所述用户认证信息包括: 第一会话密钥及用户在无线局域网中的媒体接入控制层MAC地址;

存储单元，用于保存和维护所述用户的认证信息。

相应的，本发明实施例提供一种简化无线局域网认证系统，所述系统包括: 第一接入点，第二接入点，以及第一接入点和第二接入点所属的无线蜂窝网络接入网RAN管理节点，其中，

所述第一接入点，用于在与用户进行双向鉴权认证成功后，将用户的会话密钥及用户在无线局域网中的媒体接入控制层MAC地址发送给所述RAN管

理节点；

所述RAN管理节点，用于接收第一接入点发送的用户的会话密钥及用户在无线局域网中的MAC地址，并存储和维护所述用户的认证信息；

所述第二接入点，用于在用户从第一接入点切换到第二接入点时，根据所述用户的MAC地址从所述RAN管理节点中查询所述用户的会话密钥；并在查询到所述用户的会话密钥时，不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护。

本发明实施例还提供一种简化无线局域网认证系统，所述系统包括：第一接入点，及其所属的第一无线蜂窝网络接入网RAN管理节点，第二接入点及所属的第二RAN管理节点，其中，

所述第一接入点，用于在与用户进行双向鉴权认证成功后，将用户的会话密钥及用户在无线局域网中的媒体接入控制层MAC地址发送给所述第一RAN管理节点；

所述第一RAN管理节点，用于接收第一接入点发送的用户的会话密钥及用户在无线局域网中的MAC地址，并存储和维护所述用户的会话密钥及用户在无线局域网中的MAC地址；以及在用户从第一接入点切换到第二接入点时，将所述用户的会话密钥及用户在无线局域网中的MAC地址发送给第二RAN管理节点；

所述第二RAN管理节点，用于接收所述第一RAN管理节点发送的所述用户的会话密钥及用户在无线局域网中的MAC地址，并存储和维护所述用户的会话密钥及用户在无线局域网中的MAC地址；

所述第一接入点，用于在用户从第一接入点切换到第二接入点时，根据所述用户的MAC地址从所述RAN管理节点中查询所述用户的会话密钥；并在查询到所述用户的会话密钥时，不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护。

由上述技术方案可知，本发明实施例利用管理WLAN AP的RAN管理节点进行MSK的共享，使得当用户进入新的AP覆盖范围时不需要重新进行双向鉴权而直接进行数据通信，从而减少了需要重新进行双向鉴权的次数，降低了WLAN AP的接入时延，和核心网中认证服务器的负担。

附图说明

图 1 为本发明实施例提供的一种简化无线局域网认证的方法的流程图;

图 2 为本发明实施例提供的一种会话密钥存储方法的流程图;

图 3 为本发明实施例提供的一种简化无线局域网认证的方法的应用场景的示意图;

图 4 为本发明实施例中源 RNC 向目标 RNC 切换的 Relocation Required 的消息示意图;

图 5 为本发明实施例中源 RNC 向目标 eNodeB 切换的 Relocation Required 的消息示意图;

图 6 为本发明实施例提供的一种简化无线局域网认证的装置的结构示意图;

图 6A 为本发明实施例提供的另一种简化无线局域网认证的装置的结构示意图;

图 7 为本发明实施例提供的一种会话密钥存储装置的结构示意图;

图 7A 为本发明实施例提供的第二种会话密钥存储装置的结构示意图;

图 7B 为本发明实施例提供的第三种会话密钥存储装置的结构示意图;

图 7C 为本发明实施例提供的第四种会话密钥存储装置的结构示意图;

图 8 为本发明实施例一种简化无线局域网认证系统的结构示意图;

图 9 为本发明实施例一种简化无线局域网认证系统的结构示意图。

具体实施方式

为了使本技术领域的人员更好地理解本发明实施例的方案，下面结合附图和实施方式对本发明实施例作进一步的详细说明。

请参阅图1，为本发明实施例提供一种简化无线局域网认证的方法的流程图，在该实施例中，接入点（AP，Access Point）为无线局域网中的AP，即WLAN AP，所述方法包括:

步骤101: 当用户从第一接入点切换到第二接入点时，所述第二接入点根据所述用户在无线局域网中的MAC地址向第二接入点所属的RAN管理节点查询所述用户的会话密钥;

步骤102: 如果所述第二接入点查询到所述用户的会话密钥，则不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护。

在步骤101之前，所述方法还可以包括：第一接入点在与用户进行双向鉴权认证成功后，将用户的会话密钥及用户在无线局域网中的媒体接入控制层MAC地址发送给所属的无线蜂窝网络接入网RAN管理节点存储。

也就是说，该步骤为基础条件，即第一接入点（即源接入点）将用户的会话密钥及用户在无线局域网中的媒体接入控制层MAC地址发RAN管理节点存储为基础条件，在后需用户发送接入点切换时，执行步骤102和步骤103。

在该实施例中，第一接入点和第二接入点属于同一个RAN管理节点管理，也就是说，用户切换到同一个RAN管理节点下的新接入点。

在该实施例中，第一接入点（即源接入点）需要在与用户进行双向鉴权认证成功后，先将用户的会话密钥及用户在无线局域网中的媒体接入控制层MAC地址发送给无线蜂窝网络接入网RAN管理节点存储；以便于在用户发生接入点切换时，新的接入点能直接从RAN管理节点获取该用户的会话密钥，简化在用户接入点发生切换时，简化新的接入点与该用户的双向鉴权认证过程。

在上述实施例中，如果所述第二接入点没有查询到所述用户的会话密钥，则与所述用户进行双向鉴权认证；具体可以采用EAP-AKA协议通过AAA服务器对用户进行双向鉴权认证。其中，在认证的过程中，AAA服务器扮演EAP-AKA协议中的EAP-server的角色，第二接入点扮演EAP-AKA协议中Authenticator的角色；其认证过程为：AAA服务器向HLR获取鉴权向量（Authentication Vector），AAA服务器根据鉴权向量计算密钥MK，并且根据MK计算会话密钥MSK。AAA服务器向第二接入点发送所述用户对应的MSK。第二接入点将利用MSK对无线通信的数据进行完整性检查和加密。

在所述第二接入点与所述用户双向鉴权认证成功后，所述第二接入点将所述用户的认证信息发送给RAN管理节点存储，其中，所述述用户的认证信息包括：第二用户的MSK及用户在无线局域网中的MAC地址。

优选的，当所述第一接入点与第二接入点所属的RAN管理节点不同时，在所述第二接入点根据所述用户在无线局域网中的MAC地址向所述第二接入点所属的RAN管理节点查询所述用户的会话密钥之前，所述方法还可以包括：第二接入点所属的RAN管理节点接收到第一接入点所属的RAN管理节点发送的所述用户的会话密钥及用户在无线局域网中的MAC地址。或者；

当所述第一接入点与第二接入点所属的RAN管理节点不同时，在用户从

第一接入点切换到第二接入点时，所述方法还可以包括：第二接入点所属的RAN管理节点接收到第一接入点所属的RAN管理节点发送的所述用户的会话密钥及用户在无线局域网中的MAC地址；第二接入点根据所述用户在无线局域网中的MAC地址向所属的RAN管理节点查询所述用户的会话密钥。

也就是说，第一接入点所属的RAN管理节点将所述用户的会话密钥及用户在无线局域网中的MAC地址发送给所述第二接入点所属的RAN管理节点；其中，第一接入点所属的RAN管理节点可以通过核心网将用户的会话密钥及用户在MAC地址发送给所述第二接入点所属的RAN管理节点；所述第二接入点向所属的RAN管理节点查询所述用户的会话密；

如果所述第二接入点查询到所述用户的会话密钥，则不与所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护；

如果所述第二接入点没有查询到所述用户的会话密钥，则与所述用户进行双向鉴权认证；

在所述第二接入点与所述用户双向鉴权认证成功后，所述第二接入点将所述用户的认证信息发送给RAN管理节点存储，所述述用户的认证信息包括：用户的会话密钥及用户在无线局域网中的MAC地址。

在上述实施例中，所述RAN可以为通用移动通信系统陆地无线接入网UTRAN中的无线网络控制器RNC；或者为增强型UTRAN（E-UTRAN中）的演进基站eNodeB；

所述第一接入点所属的RAN管理节点将所述用户的会话密钥及用户的MAC地址发送给所述第二接入点所属的RAN管理节点具体包括：

第一接入点所属的RNC通过核心网将所述用户的会话密钥及用户在MAC地址发送给所述第二接入点所属的RNC或者eNodeB；或者，第一接入点所属的eNodeB通过核心网将所述用户的会话密钥及用户在MAC地址发送给所述第二接入点所属的eNodeB或者RNC；或者

第二接入点所属的RNC或者eNodeB通过核心网接收到第一接入点所属的RNC发送的所述用户的会话密钥及用户在在无线局域网中的MAC地址发；或者，第二接入点所属的RNC或者eNodeB通过核心网接收到第一接入点所属的eNodeB发送的所述用户的会话密钥及用户在在无线局域网中的MAC地址。

本发明实施例利用管理WLAN AP的RAN管理节点进行MSK的共享，使得

当用户进入新的AP覆盖范围时不需要重新进行双向鉴权而直接进行数据通信，从而减少了需要重新进行双向鉴权的次数，降低了WLAN AP的接入时延，和核心网中认证服务器的负担。

还请参阅图2，本发明实施例提供的一种会话密钥存储方法的流程图，在该实施例中，接入点AP为无线局域网中的AP，所述方法包括:

步骤201: 无线蜂窝网络接入网RAN管理节点接收到至少一个接入点发送的用户认证信息，所述用户认证信息包括: 第一会话密钥及用户在无线局域网中的媒体接入控制层MAC地址;

步骤202: RAN管理节点保存和维护所述用户的认证信息。

优选的，在上述实施例中，RAN管理节点还提供查询接口，便于接入点查询用户的会话密钥，所述方法还可以包括:

所述RAN管理节点接收至少一个接入点发送的查询会话密钥请求，其中，所述查询会话密钥请求包括用户在无线局域网中的MAC地址；所述RAN管理节点根据所述MAC地址进行查询，得到用户的第一会话密钥；所述RAN管理节点向所述接入点反馈查询到的会话密钥响应，所述会话密钥响应中包括用户的第一会话密钥。

优选的，为了便于会话密钥MSK随用户的RAN管理节点的迁移而迁移，即当用户从RAN管理节点下的第一接入点切换到目标RAN管理节点下的第二接入点时，所述方法还可以包括: 所述RAN管理节点将所述用户的会话密钥及用户在无线局域网中的MAC地址发送给目标RAN管理节点，以便于在第一接入点切换到第二接入点时，所述第二接入点从所述目标RAN管理节点获取用户的第一会话密钥。

优选的，为了便于更新会话密钥，RAN管理节点还提供密钥更新接口，所述方法还可以包括: 所述RAN管理节点接收到至少一个接入点发送的所述用户的第二会话密钥（新会话密钥），并将所述第一会话密钥更新为第二会话密钥，用户第二会话密钥替换第一会话密钥。

本发明利用管理WLAN AP的RAN管理节点进行MSK密钥的共享，使得当用户进入新的AP覆盖范围时不需要重新进行双向鉴权而直接进行数据通信。本发明提供了MSK在RAN管理节点共享的方法，以及MSK密钥随用户的RAN管理节点的迁移而迁移的方法。

为了便于本领域技术人员的理解，下面以具体的实施例来说明。

实施例一

请参阅图3，为本发明实施例提供的一种简化无线局域网认证的方法的应用场景的示意图，具体包括：若干个WLAN AP31、多个RAN管理节点32和其他若干个RAN节点33，其中，若干个WLAN AP通过某逻辑链路连接到无线蜂窝网络接入网RAN侧的某个RAN管理节点上，由该RAN管理节点管理上下行数据通过该管理节点进行分流和汇聚。该RAN管理节点也可能还管理其他的RAN节点。

用户同时支持无线蜂窝网络接入网和WLAN的通信协议，并且在使用WLAN通信时可以保持无线蜂窝网络接入网侧的通信连接。用户通过无线蜂窝网络接入网连接的RAN管理节点必须和通过WLAN协议连接的RAN管理节点一致。

WLAN AP采用EAP-AKA协议通过AAA服务器对用户进行双向鉴权认证。AP和AAA服务器分别对应EAP-AKA协议中的Authenticator和EAP server。因此，当一个用户关联到一个WLAN AP，并且该AP和用户间采用EAP-AKA协议双向鉴权认证成功后，该AP将获得AAA服务器发送的该用户的MSK，并将所述MSK发送给RAN管理节点存储。

也就是说，MSK将在RAN管理节点中共享，具体包括:

在AP通过AAA服务器第一次与用户双向鉴权认证成功后，AP向RAN管理节点发送该用户认证信息，所述认证信息包括MSK，以及该用户在无线局域网中的媒体接入控制层MAC地址，但不限于此，还可以适应性包括其他的参数，本实施例不作限制。

当AP收到AAA服务器发送的该用户的新MSK时（该新MSK用于用户重新发起鉴权或者发起快速重鉴权等），AP需要向RAN管理节点更新对应的MSK，即将新的MSK发送给RAN管理节点；RAN管理节点对接收到的MSK和该用户在无线局域网中的媒体接入控制层MAC地址的二元组进行保存与维护。

当用户发生AP切换（比如从第一接入点切换到第二接入点）时，所述实施例一包括两种情况:

一种情况是：用户在同一个RAN管理节点下的不同AP间切换，即用户切换到同一个RAN管理节点下的新AP，具体为:

该新AP用所述用户的MAC地址向RAN管理节点查询用户的MSK; 如果获得MSK，则不需要对该用户进行双向鉴权，同时利用该MSK对通信内容进行保护；否则，新AP认为需要对该用户进行双向鉴权认证，其双向鉴权认证过程详见上述，在此不再赘述。

另一种情况是：用户在不同RAN管理节点下的不同AP间的切换，即用户切换到不同RAN管理节点的新AP（意味着用户已经在无线蜂窝网络侧进行RAN管理节点的切换），具体为：

当用户在无线蜂窝网络侧进行RAN管理节点切换的时候，源RAN管理节点需要把该用户对应的MSK和WLAN MAC地址传输给目标RAN管理节点。

当所述用户关联到所述新AP后，所述新AP用所述用户的WLAN MAC地址向RAN管理节点查询MSK；如果获得MSK，则不需要对该用户进行双向鉴权，同时利用该MSK对通信内容进行保护；否则，需要对该用户进行双向鉴权；其双向鉴权认证过程详见上述，在此不再赘述。

实施例二

本发明提供的实施例二是实施例一的一个特例。本实施例应用于所述无线蜂窝网络接入网RAN为通用移动通信系统-陆地无线接入网（UTRAN，Universal Mobile Telecommunications System-Terrestrial Radio Access Network）时的情况，具体而言：

所述RAN为UTRAN；所述RAN管理节点为UTRAN中的无线网络控制器RNC；受所述RAN管理节点管理的其他RAN节点为基站NodeB。

本实施例二的应用场景为：

用户从源RNC（源RAN管理节点）进入目标RNC或者目标eNodeB（目标RAN管理节点）时，按照协议，源RNC将向核心网发送“迁移请求Relocation Required”类型的无线接入网络应用部分RANAP消息。此“Relocation Required”类型消息中的“源节点到目标节点的透明容器信息元素（即Source To Target Transparent Container”IE数据）将被直接传输给目标RNC或者目标eNodeB: 其中，所述IE数据就是一些信息元素，他是由源RNC产生的。

如图4所示，为本发明实施例中源RNC向目标RNC切换的Relocation Required的消息示意图；图中所示，当目标RAN管理节点是RNC时，“Source To Target Transparent Container”IE数据需要包含源RNC到目标RNC的透明容器”

信息元素，即“Source RNC To Target RNC Transparent Container”IE;

如图5所示，为本发明实施例中源RNC向目标eNodeB切换的Relocation Required的消息示意图；图中所示，

当目标管理节点是eNodeB时，“Source To Target Transparent Container”IE需要包含源eNodeB到目标eNodeB的透明容器”信息元素，即“Source eNodeB To Target eNodeB Transparent Container”IE。

“Source RNC To Target RNC Transparent Container” IE和“Source eNodeB To Target eNodeB Transparent Container” IE都包含无线资源控制容器（RRC-Container）和扩展信息元素（iE-Extensions）两个子字段。对RRC-Container和iE-Extensions数据的解释是可以自定义的，因此，本实施例可以利用RRC-Container和iE-Extensions来携带自定义的信息，，比如，可以将会话密钥和MAC地址填充带这两个字段中，而不修改现有的无线标准。

本实施例二的具体过程包括:

当用户在同一个RNC的不同AP间切换时，其具体的实现过程详见施例一中对应的实现过程。

当用户从一个RNC的AP切换到其他RNC（或者一个eNodeB）的AP时，将实施例一中所描述的“源RAN管理节点需要把该用户对应的MSK和WLAN MAC地址传输给目标RAN管理节点”可以具体细化为:

用户的MSK和WLAN MAC地址可以写入“Relocation Required”消息“Source To Target Transparent Container”IE中的RRC-Container或iE-Extensions字段，从而从源RNC传输到目标RNC或者目标eNodeB。

源RNC和目标RNC（或者目标eNodeB）按照一个预先约定的格式对RRC-Container或iE-Extensions进行编码，从而保证能够成功进行用户的MSK和WLAN MAC地址的加密传输。

实施例三

本实施例三也是实施例一的另一个特例。本实施例应用于当所述无线蜂窝网络采用LTE协议时的情况，具体而言:

所述RAN为E-UTRAN; 所述RAN管理节点为eNodeB; eNodeB没有管理其他RAN节点;

用户从源eNodeB（源RAN管理节点）进入目标RNC或者目标eNodeB（目

标RAN管理节点)时，按照协议，源eNodeB将向核心网发送“切换请求Handover Required”类型的接口应用协议S1AP消息。此“Handover Required”类型消息中的“Source To Target Transparent Container” IE数据将被直接传输给目标RNC或者目标eNodeB:

当目标管理节点是RNC时，“Source To Target Transparent Container”IE需要包含“Source RNC To Target RNC Transparent Container”IE;

当目标管理节点是eNodeB时，“Source To Target Transparent Container”IE需要包含“Source eNodeB To Target eNodeB Transparent Container”IE。

同实施例二相同，“Source RNC To Target RNC Transparent Container”IE和“Source eNodeB To Target eNodeB Transparent Container”IE都包含RRC-Container和iE-Extensions两个子字段。本实施例中，对RRC-Container和iE-Extensions数据的解释是可以自定义的，因此可以利用RRC-Container和iE-Extensions来携带自定义的信息，比如，可以将会话密钥和MAC地址填充带这两个字段中，而不修改现有的无线标准。

本实施例的具体实现过程包括:

当用户在同一个eNodeB的不同AP间切换时，其实现步骤同实施例一中相对应的步骤一致，具体详见上述，在此不再赘述。

当用户从一个eNodeB的AP切换到其他eNodeB（或者一个RNC）的AP时，实施例一中所描述的“源RAN管理节点需要把该用户对应的MSK和WLAN MAC地址传输给目标RAN管理节点”具体可以细化为:

用户的MSK和WLAN MAC地址可以写入“Handover Required”消息“Source To Target Transparent Container” IE中的RRC-Container或iE-Extensions字段，从而从源eNodeB传输到目标RNC或者目标eNodeB。

源eNodeB和目标eNodeB（或者目标RNC）按照一个预先约定的格式对RRC-Container或iE-Extensions进行编码，从而保证能够成功进行用户的MSK和WLAN MAC地址的加密传输。

本发明实施例针对EAP-AKA协议进行，设计了密钥在管理节点间共享的方法以及简化无线局域网认证的方法，从而减少了当用户进行AP切换时需要重新进行双向鉴权的次数，降低了WLAN AP的接入时延和核心网中认证服务器的负担。

基于上述实施例的实现过程，本发明实施例提供一种简化无线局域网认证的装置，其结构示意图如图6所示，所述装置与无线蜂窝网络接入网RAN管理节点进行数据交互，所述RAN理节点存储用户与第一接入点进行双向鉴权认证成功的会话密钥，及用户在无线局域网中的媒体接入控制层MAC地址；所述装置包括：第一查询单元61和加密单元62，其中，

所述第一查询单元61，用于在用户从第一接入点切换到该简化无线局域网认证的装置时，根据用户在无线局域网中的媒体接入控制层MAC地址向所述装置所属的RAN管理节点查询所述用户的会话密钥；所述加密单元62，用于所述第一查询单元查询到所述用户的会话密钥，则不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护。

优选的，所述装置还可以包括：鉴权认证单元63和发送单元64，其中，鉴权认证单元63，用于在所述第一查询单元没有查询到所述用户的会话密钥时，则该鉴权认证单元与所述用户进行双向鉴权认证；发送单元64，用于在该鉴权认证单元与所述用户进行双向鉴权认证成功后，将所述用户的认证信息发送给RAN管理节点存储，所述用户的认证信息包括：用户的会话密钥及用户在无线局域网中的MAC地址；具体详见图6A，图6A为本发明实施例提供的另一种简化无线局域网认证的装置的结构示意图。

所述装置中各个单元的功能和作用的实现过程，详见上述方法中对应的实现过程，在此不再赘述。

相应的，本发明实施例还一种会话密钥存储装置，其结构示意图如图7所示，所述装置包括：接收单元71和存储单元72，其中，所述接收单元71，用于接收到至少一个接入点发送的用户认证信息，所述用户认证信息包括：第一会话密钥及用户在无线局域网中的媒体接入控制层MAC地址；所述存储单元72，用于保存和维护所述用户的认证信息。

优选的，所述装置还可以包括：查询单元73，用于在接收到至少一个接入点发送的携带用户在无线局域网中的MAC地址的查询会话密钥请求时，根据所述MAC地址从所述存储单元查询对应的第一会话密钥；反馈单元74，与查询单元73连接，用于向所述接入点反馈会话密钥响应，所述会话密钥响应包括用户的第一会话密钥；具体详见图7A，图7A为本发明实施例提供的第二种会话密钥存储装置的结构示意图。

优选的，在上述所有实施例的基础上，所述装置还可以包括：密钥更新单元75，用于在接收到至少一个接入点发送的所述用户的第二会话密钥，将将存储单元72中的所述第一会话密钥更新为第二会话密钥；具体详见图7B，图7B为本发明实施例提供的第三种会话密钥存储装置的结构示意图，即图7B在图7A的基础上增加了密钥更新单元75，当然，在图7的基础上也可以增加密钥更新单元75，本实施例只是以其中一种为例，不限于此。

优选，在上述所有实施例的基础上，当用户从RAN管理节点下的第一接入点切换到目标RAN管理节点下的第二接入点时，所述装置还可以包括:

发送单元76，与存储单元72连接，用于将所述用户的会话密钥及用户在无线局域网中的MAC地址发送给目标RAN管理节点，以便于在第一接入点切换到第二接入点时，所述第二接入点从所述目标RAN管理节点获取用户的会话密钥；具体详见图7C，图7C为本发明实施例提供的第四种会话密钥存储装置的结构示意图；即图7 C在图7B的基础上增加了发送单元76，当然，在图7、图A或图7B的基础上也可以增加发送单元76，本实施例只是以其中一种为例，并不限于此。

所述装置中各个单元的功能和作用的实现过程，详见上述方法中对应的实现过程，在此不再赘述。

相应的，本发明实施例还提供一种简化无线局域网认证系统，其结构示意图详见图8，所述系统包括：第一接入点81，第二接入点82，以及第一接入点和第二接入点所属的无线蜂窝网络接入网RAN管理节点83，其中，

所述第一接入点81，用于在与用户进行双向鉴权认证成功后，将用户的会话密钥及用户在无线局域网中的媒体接入控制层MAC地址发送给所述RAN管理节点;

所述RAN管理节点83，用于接收第一接入点发送的用户的会话密钥及用户在无线局域网中的MAC地址，并存储和维护所述用户的认证信息;

所述第二接入点82，用于在用户从第一接入点切换到第二接入点时，根据所述用户的MAC地址从所述RAN管理节点中查询所述用户的会话密钥；并在查询到所述用户的会话密钥时，不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护。

其中，所述RAN管理节点83包括会话密钥存储装置，所述第二接入点包

括简化无线局域网认证的装置，所述会话密钥存储装置和简化无线局域网认证的装置的功能和作用如上述所示，在此不再赘述。

相应的，本发明实施例还提供另一种简化无线局域网认证系统，其结构示意图详见图9，所述系统包括：第一接入点91，及其所属的第一无线蜂窝网络接入网RAN管理节点92，第二接入点93及所属的第二RAN管理节点94，其中，

所述第一接入点91，用于在与用户进行双向鉴权认证成功后，将用户的会话密钥及用户在无线局域网中的媒体接入控制层MAC地址发送给所述第一RAN管理节点；

所述第一RAN管理节点92，用于接收第一接入点发送的用户的会话密钥及用户在无线局域网中的MAC地址，并存储和维护所述用户的会话密钥及用户在无线局域网中的MAC地址；以及在用户从第一接入点切换到第二接入点时，将所述用户的会话密钥及用户在无线局域网中的MAC地址发送给第二RAN管理节点；

所述第二RAN管理节点94，用于接收所述第一RAN管理节点发送的所述用户的会话密钥及用户在无线局域网中的MAC地址，并存储和维护所述用户的会话密钥及用户在无线局域网中的MAC地址；

所述第一接入点93，用于在用户从第一接入点切换到第二接入点时，根据所述用户的MAC地址从所述RAN管理节点中查询所述用户的会话密钥；并在查询到所述用户的会话密钥时，不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护。

其中，所述第一RAN管理节点和第二RAN管理节点分别包括会话密钥存储装置，所述第二接入点和第二接入点分别包括简化无线局域网认证的装置，所述会话密钥存储装置和简化无线局域网认证的装置的功能和作用如上述所示，在此不再赘述。

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以通过硬件实现，也可以可借助软件加必要的通用硬件平台的方式来实现。基于这样的理解，本发明的技术方案可以以软件产品的形式体现出来，该软件产品可以保存在一个非易失性保存介质（例如，可以是只读存储器（ROM），U盘，移动硬盘，随机存取存储器（RAM）、磁碟或者光盘等各

种可以存储程序代码的介质等)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。

在本申请所提供的几个实施例中，应该理解到，所揭露装置和方法，在没有超过本申请的精神和范围内，可以通过其他的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述模块的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个模块或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。

显然，本领域的技术人员应该明白，上述的本发明的各单元或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，或者将它们分别制作成各个集成电路模块，或者将它们中的多个单元或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。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，均包含在本发明的保护范围内。

权 利 要 求

1、一种简化无线局域网认证的方法，其特征在于，所述方法包括:

当用户从第一接入点切换到第二接入点时，所述第二接入点根据所述用户在无线局域网中的媒体接入控制层MAC地址向所述第二接入点所属的RAN管理节点查询所述用户的会话密钥;

如果所述第二接入点查询到所述用户的会话密钥，则不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护。

2、根据权利要求1所述的方法，其特征在于，还包括:

如果所述第二接入点没有查询到所述用户的会话密钥，则与所述用户进行双向鉴权认证;

在所述第二接入点与所述用户双向鉴权认证成功后，所述第二接入点将所述用户的认证信息发送给RAN管理节点存储，所述述用户的认证信息包括:用户的会话密钥及用户在无线局域网中的MAC地址。

3、根据权利要求1或2所述的方法，其特征在于，当所述第一接入点与第二接入点所属的RAN管理节点不同时,在所述第二接入点根据所述用户在无线局域网中的MAC地址向所述第二接入点所属的RAN管理节点查询所述用户的会话密钥之前，还包括:

第二接入点所属的RAN管理节点接收到第一接入点所属的RAN管理节点发送的所述用户的会话密钥及用户在无线局域网中的MAC地址。

4、根据权利要求2或3所述的方法，其特征在于，所述与用户进行双向鉴权认证具体为:采用EAP-AKA协议通过AAA服务器对用户进行双向鉴权认证。

5、根据权利要求1至4任一项所述的方法，其特征在于，所述RAN为通用移动通信系统陆地无线接入网UTRAN中的无线网络控制器RNC; 或者为增强型UTRAN中的演进基站eNodeB。

6、根据权利要求5所述的方法，其特征在于，所述第二接入点所属的RAN管理节点接收到第一接入点所属的RAN管理节点发送的所述用户的会话密钥及用户在无线局域网中的MAC地址具体包括:

第二接入点所属的RNC或者eNodeB通过核心网接收到第一接入点所属的RNC发送的所述用户的会话密钥及用户在在无线局域网中的MAC地址发; 或

者

第二接入点所属的RNC或者eNodeB通过核心网接收到第一接入点所属的eNodeB发送的所述用户的会话密钥及用户在在无线局域网中的MAC地址。

7、一种会话密钥存储方法，其特征在于，包括:

无线蜂窝网络接入网RAN管理节点接收到至少一个接入点发送的用户认证信息，所述用户认证信息包括: 第一会话密钥及用户在无线局域网中的媒体接入控制层MAC地址;

RAN管理节点保存和维护所述用户的认证信息。

8、根据权利要求7所述的方法，其特征在于，还包括:

所述RAN管理节点接收至少一个接入点发送的查询会话密钥请求，所述查询会话密钥请求包括: 用户在无线局域网中的MAC地址;

所述RAN管理节点根据所述MAC地址进行查询，得到用户的第一会话密钥;

所述RAN管理节点向所述接入点反馈查询到的会话密钥响应，所述会话密钥响应包括用户的第一会话密钥。

9、根据权利要求7或8所述的方法，其特征在于，当用户从RAN管理节点下的第一接入点切换到目标RAN管理节点下的第二接入点时，所述方法还包括:

所述RAN管理节点将所述用户的会话密钥及用户在无线局域网中的MAC地址发送给目标RAN管理节点，以便于在第一接入点切换到第二接入点时，所述第二接入点从所述目标RAN管理节点获取用户的第一会话密钥。

10、根据权利要求7或8所述的方法，其特征在于，还包括:

所述RAN管理节点接收到至少一个接入点发送的所述用户的第二会话密钥;

所述RAN管理节点将所述第一会话密钥更新为第二会话密钥。

11、一种简化无线局域网认证的装置，与无线蜂窝网络接入网RAN管理节点进行数据交互，其特征在于，所述装置包括:

第一查询单元，用于在用户从第一接入点切换到该简化无线局域网认证的装置时，根据用户在无线局域网中的媒体接入控制层MAC地址向所述装置所属的RAN管理节点查询所述用户的会话密钥;

加密单元，用于所述第一查询单元查询到所述用户的会话密钥，则不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护。

12、根据权利要求11所述的装置，其特征在于，还包括:

鉴权认证单元，用于在所述第一查询单元没有查询到所述用户的会话密钥时，则与所述用户进行双向鉴权认证;

发送单元，用于在与所述用户进行双向鉴权认证成功后，将所述用户的认证信息发送给RAN管理节点存储，所述用户的认证信息包括: 用户的会话密钥及用户在无线局域网中的MAC地址。

13、一种会话密钥存储装置，其特征在于，包括:

接收单元，用于接收到至少一个接入点发送的用户认证信息，所述用户认证信息包括: 第一会话密钥及用户在无线局域网中的媒体接入控制层MAC地址;

存储单元，用于保存和维护所述用户的认证信息。

14、根据权利要求13所述的装置，其特征在于，还包括:

查询单元，用于在接收到至少一个接入点发送的携带用户在无线局域网中MAC地址的查询会话密钥请求时，根据所述MAC地址从所述存储单元中查询到对应的第一会话密钥;

反馈单元，用于向所述接入点反馈会话密钥响应，所述会话密钥响应包括用户的第一会话密钥。

15、根据权利要求13或14所述的装置，其特征在于，还包括:

密钥更新单元，用于在接收到至少一个接入点发送的所述用户的第二会话密钥，将所述第一会话密钥更新为第二会话密钥。

16、根据权利要求13至15任一项所述的装置，其特征在于，当用户从RAN管理节点下的第一接入点切换到目标RAN管理节点下的第二接入点时，所述装置还包括:

发送单元，用于将所述用户的会话密钥及用户在无线局域网中的MAC地址发送给目标RAN管理节点，以便于在第一接入点切换到第二接入点时，所述第二接入点从所述目标RAN管理节点获取用户的会话密钥。

17、一种简化无线局域网认证系统，其特征在于，包括: 第一接入点，

第二接入点，以及第一接入点和第二接入点所属的无线蜂窝网络接入网RAN管理节点，其中，

所述第一接入点，用于在与用户进行双向鉴权认证成功后，将用户的会话密钥及用户在无线局域网中的媒体接入控制层MAC地址发送给所述RAN管理节点；

所述RAN管理节点，用于接收第一接入点发送的用户的会话密钥及用户在无线局域网中的MAC地址，并存储和维护所述用户的认证信息；

所述第二接入点，用于在用户从第一接入点切换到第二接入点时，根据所述用户的MAC地址从所述RAN管理节点中查询所述用户的会话密钥；并在查询到所述用户的会话密钥时，不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护。

18、一种简化无线局域网认证系统，其特征在于，包括：第一接入点，及其所属的第一无线蜂窝网络接入网RAN管理节点，第二接入点及所属的第二RAN管理节点，其中，

所述第一接入点，用于在与用户进行双向鉴权认证成功后，将用户的会话密钥及用户在无线局域网中的媒体接入控制层MAC地址发送给所述第一RAN管理节点；

所述第一RAN管理节点，用于接收第一接入点发送的用户的会话密钥及用户在无线局域网中的MAC地址，并存储和维护所述用户的会话密钥及用户在无线局域网中的MAC地址；以及在用户从第一接入点切换到第二接入点时，将所述用户的会话密钥及用户在无线局域网中的MAC地址发送给第二RAN管理节点；

所述第二RAN管理节点，用于接收所述第一RAN管理节点发送的所述用户的会话密钥及用户在无线局域网中的MAC地址，并存储和维护所述用户的会话密钥及用户在无线局域网中的MAC地址；

所述第一接入点，用于在用户从第一接入点切换到第二接入点时，根据所述用户的MAC地址从所述RAN管理节点中查询所述用户的会话密钥；并在查询到所述用户的会话密钥时，不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护。

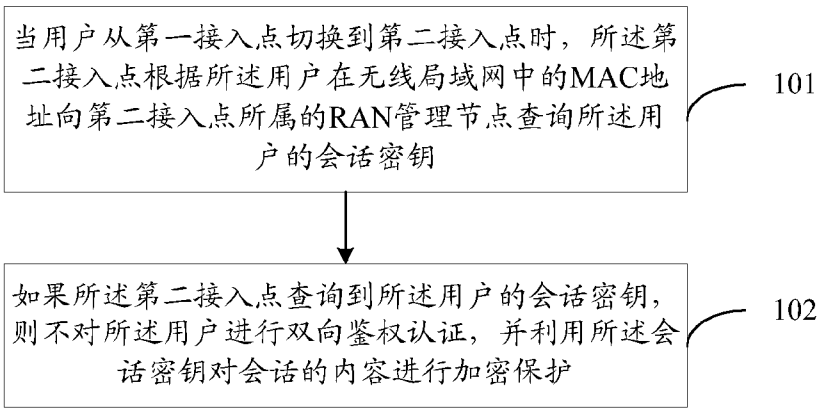
当用户从第一接入点切换到第二接入点时，所述第二接入点根据所述用户在无线局域网中的MAC地址向第二接入点所属的RAN管理节点查询所述用户的会话密钥
101
如果所述第二接入点查询到所述用户的会话密钥，则不对所述用户进行双向鉴权认证，并利用所述会话密钥对会话的内容进行加密保护
102

图 1

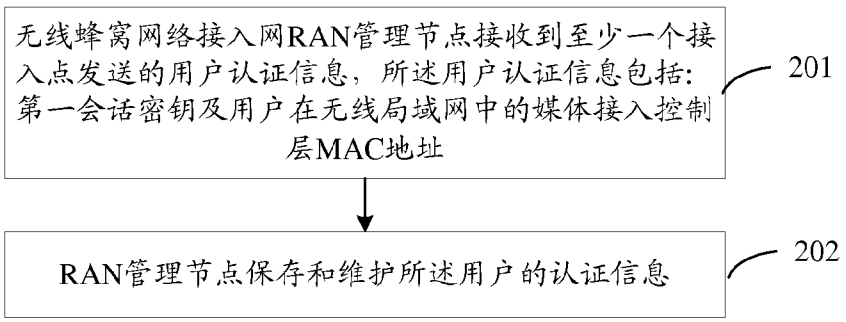
无线蜂窝网络接入网RAN管理节点接收到至少一个接入点发送的用户认证信息，所述用户认证信息包括：第一会话密钥及用户在无线局域网中的媒体接入控制层MAC地址
201
RAN管理节点保存和维护所述用户的认证信息
202

图2

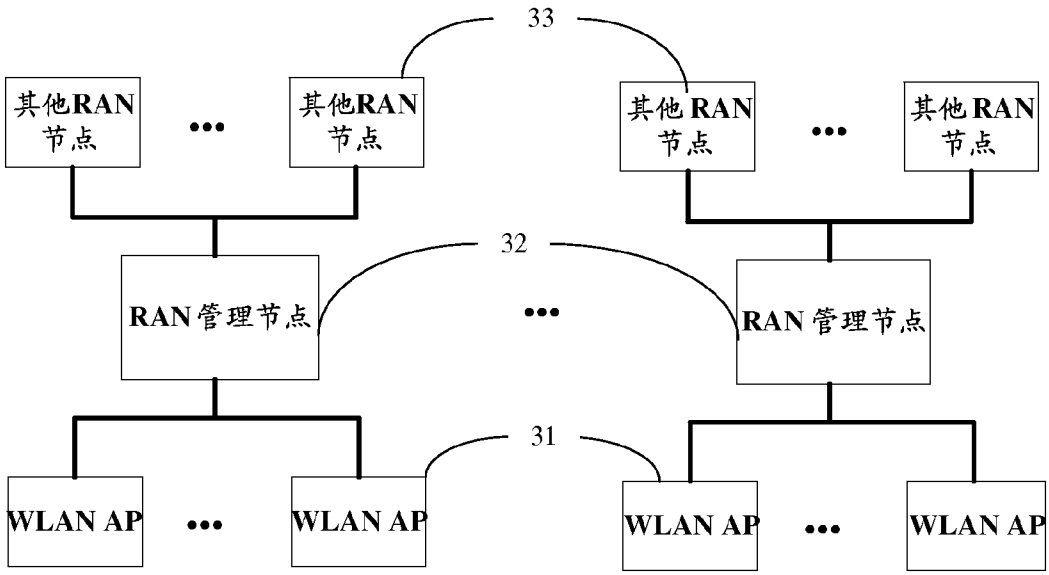
33
其他RAN节点
其他RAN节点
其他RAN节点
其他RAN节点
32
RAN管理节点
RAN管理节点
31
WLAN AP
WLAN AP
WLAN AP
WLAN AP

图3

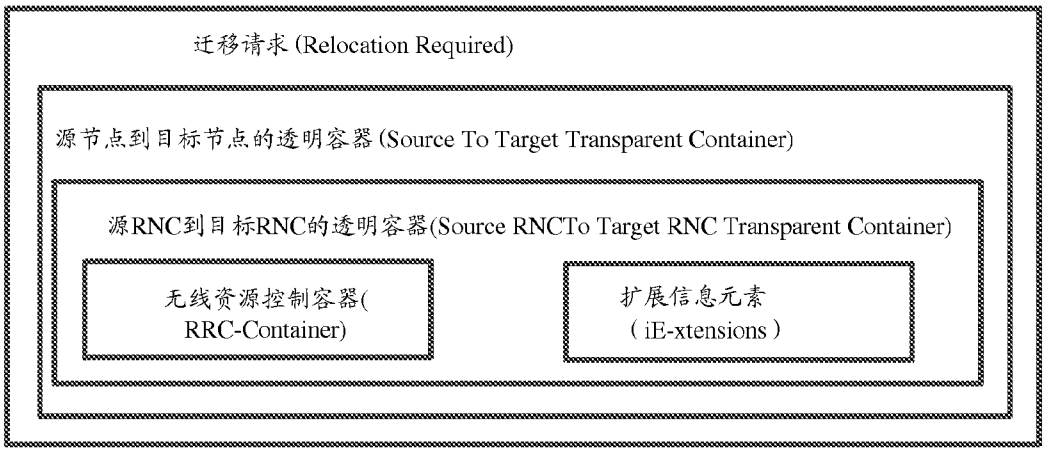
迁移请求 (Relocation Required)
源节点到目标节点的透明容器 (Source To Target Transparent Container)
源RNC到目标RNC的透明容器(Source RNCTo Target RNC Transparent Container)
无线资源控制容器(
RRC-Container)
扩展信息元素
(iE-xtensions)

图4

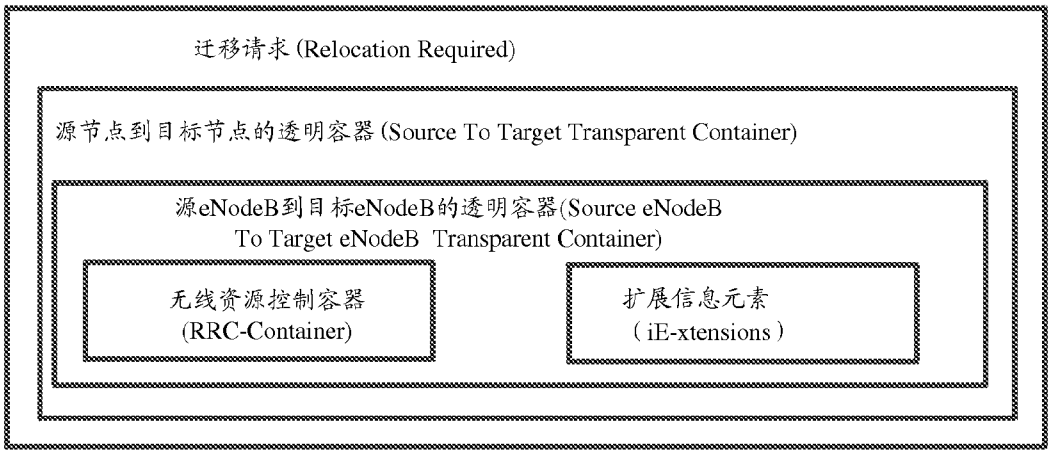
迁移请求 (Relocation Required)
源节点到目标节点的透明容器 (Source To Target Transparent Container)
源eNodeB到目标eNodeB的透明容器(Source eNodeB
To Target eNodeB Transparent Container)
无线资源控制容器
(RRC-Container)
扩展信息元素
(iE-xtensions)

图5

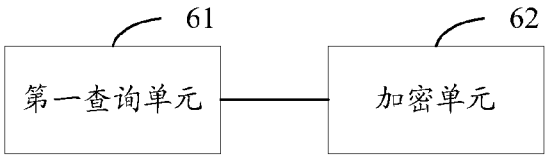
61
62
第一查询单元
加密单元

图6

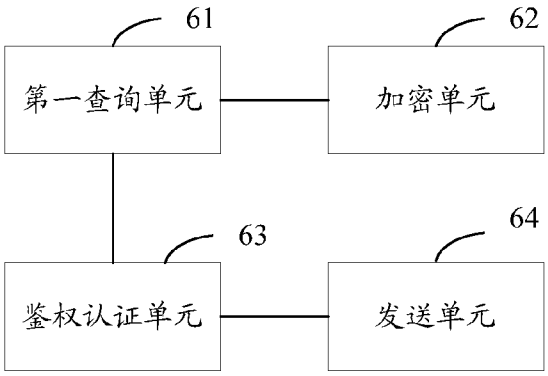

图6A

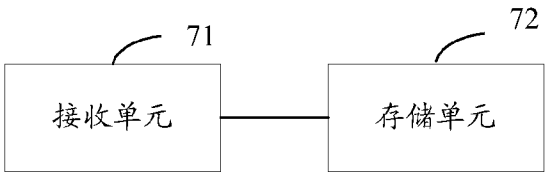

图7

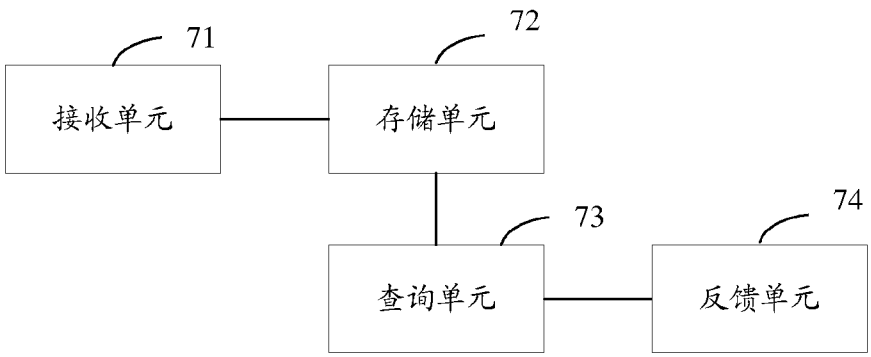

图7A

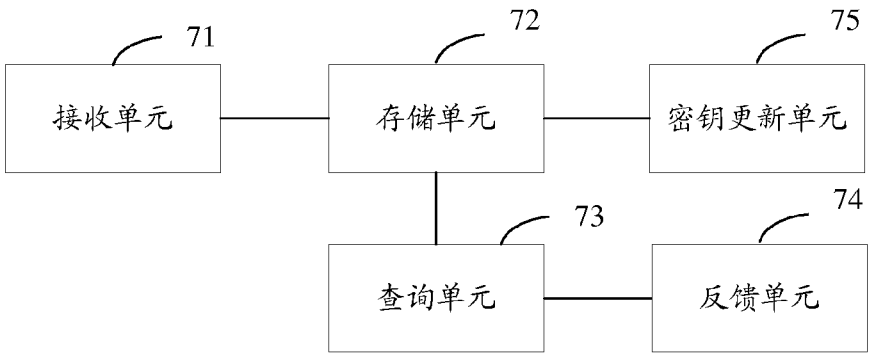

图7B

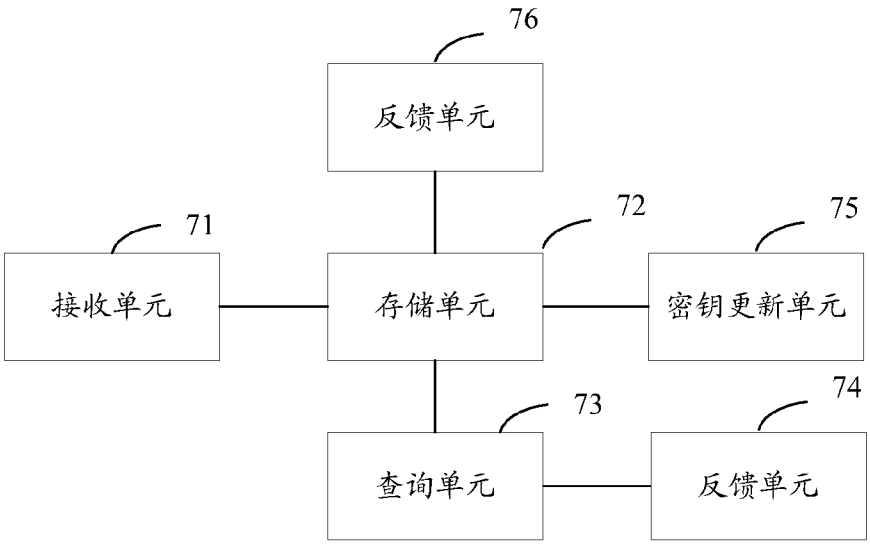
76
反馈单元
71
72
75
接收单元
存储单元
密钥更新单元
73
74
查询单元
反馈单元

图7C

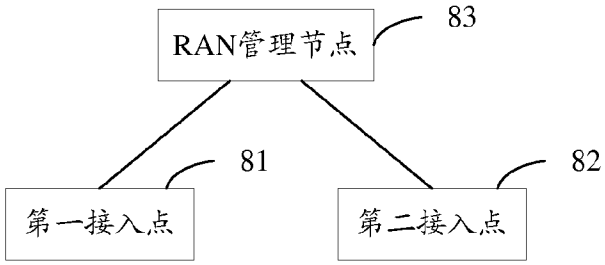
RAN管理节点
83
81
82
第一接入点
第二接入点

图8

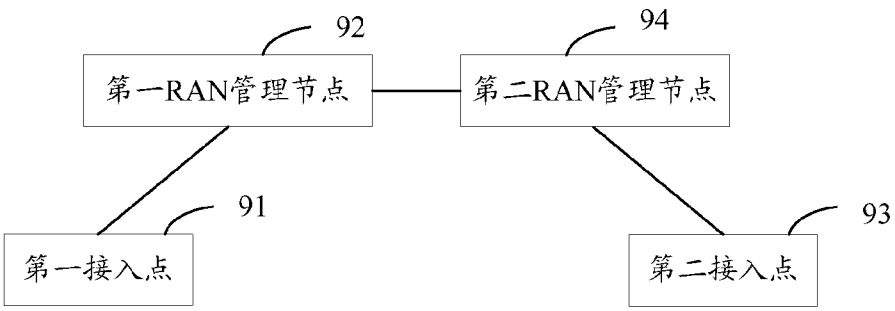
92
94
第一RAN管理节点
第二RAN管理节点
91
93
第一接入点
第二接入点

图9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/077808

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04 (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 12/-, H04L 29/-, H04L 12/-

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)

CPRSABS, CNABS, CNTXT, DWPI, SIPOABS: access, media access control layer, access w point, AP, switch+, mov+, transfer+, authenticat+, search+, code, key, password, MAC, address

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101079891 A (TSINGHUA UNIVERSITY), 28 November 2007 (28.11.2007), description, page 4, 6th line from the bottom to page 6, line 3, and figures 1 and 2	1-18
A	CN 101902722 A (ZTE CORP. et al.), 01 December 2010 (01.12.2010), the whole document	1-18
A	CN 101702802 A (ZTE CORP.), 05 May 2010 (05.05.2010), the whole document	1-18

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

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

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 March 2012 (21.03.2012)	**03 May 2012 (03.05.2012)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **XU, Jiaying** Telephone No.: (86-10) **62411370**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2011/077808

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101079891 A	28.11.2007	CN 101079891 B	15.12.2010
CN 101902722 A	01.12.2010	None	
CN 101702802 A	05.05.2010	WO 2010145273 A1	23.12.2010

国际检索报告

国际申请号
PCT/CN2011/077808

A. 主题的分类

H04W12/04（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：H04W12/-，H04L29/-，H04L12/-

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）)

CPRSABS，CNABS，CNTXT，DWPI，SIPOABS：接入点，AP，切换，进入，移动，鉴权，认证，查询，密钥，密码，媒体接入控制层，MAC，地址，access w point，AP，switch+，mov+，transfer+，authenticat+，search +，code，key，password，MAC，address

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	CN101079891A（清华大学）28.11 月 2007（28.11.2007） 说明书第 4 页倒数第 6 行至第 6 页第 3 行，附图 1 和 2	1-18
A	CN101902722A（中兴通讯股份有限公司等）01.12 月 2010（01.12.2010）全文	1-18
A	CN101702802A（中兴通讯股份有限公司）05.5 月 2010（05.05.2010）全文	1-18

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

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

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

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

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

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

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
21.3 月 2012 (21.03.2012)	**03.5 月 2012 (03.05.2012)**
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 徐佳颖 电话号码：(86-10) **62411370**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2011/077808

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101079891A	28.11.2007	CN101079891B	15.12.2010
CN101902722A	01.12.2010	无	
CN101702802A	05.05.2010	WO2010145273A1	23.12.2010