

(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
2013 年 10 月 17 日 (17.10.2013)



(10) 国际公布号
WO 2013/152740 A1

- (51) 国际专利分类号:
H04W 12/06 (2009.01)
- (21) 国际申请号: PCT/CN2013/074156
- (22) 国际申请日: 2013 年 4 月 12 日 (12.04.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210106342.2 2012 年 4 月 12 日 (12.04.2012) CN
- (71) 申请人: 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: 张冬梅 (ZHANG, Dongmei); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 熊春山 (XIONG, Chunshan); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 陈璟 (CHEN, Jing); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

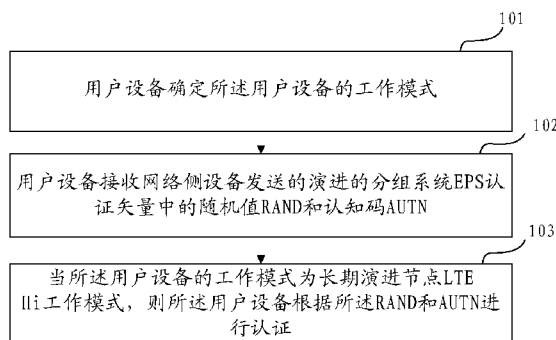
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME,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

(54) Title: AUTHENTICATION METHOD, DEVICE AND SYSTEM FOR USER EQUIPMENT

(54) 发明名称: 用户设备的认证方法、装置及系统



101 A USER EQUIPMENT DETERMINES AN OPERATING MODE OF THE USER EQUIPMENT

102 THE USER EQUIPMENT RECEIVES A RANDOM VALUE RAND AND A COGNITIVE CODE AUTN IN AN EVOLVED PACKET SYSTEM (EPS) AUTHENTICATION VECTOR SENT BY A NETWORK SIDE DEVICE

103 WHEN THE OPERATING MODE OF THE USER EQUIPMENT IS A LONG-TERM EVOLVED NODE LTE HI OPERATING MODE, THE USER EQUIPMENT PERFORMS AUTHENTICATION BASED ON THE RAND AND THE AUTN

图 1 /Fig. 1

(57) Abstract: Disclose are an authentication method, device and system for a user equipment. The method comprises: first, a user equipment receiving a random value RAND and a cognitive code AUTN in an evolved packet system (EPS) authentication vector sent by a network side device; when an operating mode of the user equipment is a long-term evolved node LTE Hi operating mode, the user equipment performing authentication based on the RAND and the AUTN. In the authentication process, the user equipment ignores a verification result of a separation bit of an authentication management field (AMF) in the AUTN; or, the user equipment does not verify the separation bit of the AMF. The present invention is applicable to the field of communication systems.

(57) 摘要:

[见续页]



本发明实施例公开了一种用户设备的认证方法、装置及系统，所述方法包括：首先用户设备接收网络侧设备发送的演进的分组系统 EPS 认证矢量中的随机值 RAND 和认知码 AUTN；当所述用户设备的工作模式为长期演进节点 LTE Hi 工作模式，则所述用户设备根据所述 RAND 和 AUTN 进行认证，其中，在所述认证过程中，所述用户设备忽略对所述 AUTN 中认证管理域 AMF 的分离比特位进行校验的校验结果；或者，所述用户设备不对所述 AMF 的分离比特位进行校验。本发明适用于通信系统领域。

用户设备的认证方法、装置及系统

本申请要求于 2012 年 4 月 12 日提交中国专利局、申请号为 201210106342.2、发明名称为“用户设备的认证方法、装置及系统”的中国专利申请优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本发明涉及通信系统领域，特别涉及一种用户设备的认证方法、装置及系统。

10 背景技术

LTE Hi (Long Term Evolution Hi, 长期演进节点) 技术是新引入的一套基于现有移动网络，面向固定、低速移动场景的通信技术。LTE Hi 接入节点的协议栈和 LTE (Long Term Evolution, 长期演进) 接入节点相同，由于空口使用 LTE 技术时，节点 Hi 可能比 LTE 网络更早布置，所以当 Hi 节点比 LTE 网络
15 更早布置时，只能通过现有的 3G(3rd-generation, 第三代移动通信业务) 网络接入。这种场景下，在一个适配网关 LTE Hi GW (GateWay, 网关) 里，提供虚拟 EPC(Evolved Packet Core, 移动核心网演进) 核心网功能，所以从安全角度看，可以认为有一个虚拟的 MME (Mobility Management Entity 移动性管理实体) 存在。LTE Hi UE (User Equipment, 用户设备) 和 LTE UE 一样，接入时可能
20 触发认证过程，对于 3G 的 HLR (Home Location Register 归属位置寄存器) 来说，由于这是一个普通的 3G 认证，网络侧会将认证矢量中的 AMF 的分离比特位设置为 0。而对于 LTE Hi UE 来说，它会认为这是一个 EPS (Evolved Packet System 演进的分组系统) AKA (Authentication and Key Agreement 认证及密钥协商) 认证，所以会按照 EPS AKA 的处理认证过程对各个参量进行
25 校验，从而会通过检测认证矢量中的 AMF 的分离比特位是否为 1，来判断 EPS AKA 的处理认证过程是否成功。由于对于 3G 的 HLR，AMF 的分离比特位设

-2-

置为 0，进而导致了在 3G 的 HLR 条件下，UE 无法通过 EPS AKA 的验证，从而不能正常入网的问题。

发明内容

5 本发明实施例提供一种用户设备的认证方法、装置及系统，在不修改认证服务器 HLR 的处理逻辑下，解决了在 3G 的 HLR 条件下，UE 无法通过 EPS AKA 的验证，从而不能正常入网的问题。

本发明实施例采用的技术方案为：

一种用户设备的认证方法，包括：

10 用户设备接收网络侧设备发送的演进的分组系统 EPS 认证矢量中的随机值 RAND 和认知码 AUTN；

当所述用户设备的工作模式为长期演进节点 LTE Hi 工作模式，则所述用户设备根据所述 RAND 和 AUTN 进行认证，其中，在所述认证过程中，所述用户设备忽略对所述 AUTN 中认证管理域 AMF 的分离比特位进行校验的校验
15 结果；或者，所述用户设备不对所述 AMF 的分离比特位进行校验。

一种用户设备的认证装置，包括：

接收单元，用于接收网络侧设备发送的演进的分组系统 EPS 认证矢量中的随机值 RAND 和认知码 AUTN；

20 认证单元，用于当工作模式为长期演进节点 LTE Hi 工作模式，则根据所述 RAND 和 AUTN 进行认证，其中，在所述认证过程中，忽略对所述 AUTN 中认证管理域 AMF 的分离比特位进行校验的校验结果；或者，不对所述 AMF 的分离比特位进行校验。

另一种用户设备的认证方法，包括：

网络侧设备获取通用移动通信系统 UMTS 认证矢量；

25 当用户设备的工作模式为长期演进节点 LTE Hi 工作模式时，所述网络侧

—3—

设备根据所述 UMTS 认证矢量，获取分组系统 EPS 认证矢量；

所述网络侧设备向所述用户设备发送所述 EPS 认证矢量中的随机值 RAND 和认知码 AUTN，以使得所述用户设备根据所述 RAND 和所述 AUTN 进行认证。

5 另一种用户设备的认证装置，包括：

获取单元，用于获取通用移动通信系统 UMTS 认证矢量；

所述获取单元，还用于当用户设备的工作模式为长期演进节点 LTE Hi 工作模式时，根据所述 UMTS 认证矢量，获取分组系统 EPS 认证矢量；

10 发送单元，用于向所述用户设备发送所述 EPS 认证矢量中的随机值 RAND 和认知码 AUTN，以使得所述用户设备根据所述 RAND 和所述 AUTN 进行认证。

一种用户设备的认证系统，包括：用户设备，认证服务器 HLR 和网络侧设备 MME；

15 所述 HLR，用于接收到网络侧设备发送的认证请求信息后，向所述网络侧设备发送携带有通用移动通信系统 UMTS 认证矢量的认证响应请求响应信息。

20 本发明实施例提供的用户设备的认证方法、装置及系统，首先用户设备接收网络侧设备发送的演进的分组系统 EPS 认证矢量中的随机值 RAND 和认知码 AUTN；当所述用户设备的工作模式为长期演进节点 LTE Hi 工作模式，则所述用户设备根据所述 RAND 和 AUTN 进行认证，其中，在所述认证过程中，所述用户设备忽略对所述 AUTN 中认证管理域 AMF 的分离比特位进行校验的校验结果；或者，所述用户设备不对所述 AMF 的分离比特位进行校验。通过现有技术在进行用户设备认证时，由于对于 3G 的认证服务器 HLR，AMF 的分离比特位设置为 0，进而导致了在 3G 的 HLR 条件下，用户设备 UE 无法通
25 过 EPS AKA 的验证，从而造成用户设备不能正常入网的问题。而本发明实施

-4-

例，通过忽略或不进行 AMF 的分离比特位的验证，实现了在不修改认证服务器 HLR 的处理逻辑下，UE 可以正常地进行 EPS AKA 的验证，解决了由于用户设备无法通过 EPS AKA 的验证，从而不能正常入网的问题。

5 附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其它的附图。

- 10 图 1 为本发明实施例提供的一种用户设备的认证方法流程图；
图 2 为本发明实施例提供的一种用户设备的认证装置结构示意图；
图 3 为本发明实施例提供的另一种用户设备的认证方法流程图；
图 4 为本发明实施例提供的另一种用户设备的认证装置结构示意图；
图 5 为本发明实施例提供的一种用户设备的认证系统结构示意图。

15

具体实施方式

- 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。
- 20

为使本发明技术方案的优点更加清楚，下面结合附图和实施例对本发明作详细说明。

本实施例提供一种用户设备的认证方法，如图1所示，所述方法包括：

101、用户设备确定所述用户设备的工作模式。

其中，所述用户设备可以通过无线接入点接入网络，所述无线接入节点可以为长期演进节点LTE Hi。

可选地，所述用户设备可以根据所述无线接入节点的类型，确定所述用户设备对应的工作模式，所述无线接入节点的类型为所述网络侧设备通过附着接收信息或跟踪区域更新信息或安全模式完成信息指示的，或无线接入节点的类型为与所述无线接入节点对应的小区通过广播消息指示的。

其中，所述网络设备可以为移动性管理实体MME或者具有所述MME功能的设备，在此不作限定。

具体地，可以通过在所述信息中增加无线接入节点的指示信元来指示所述无线接入节点的类型。

可选地，所述用户设备可以根据所述无线接入节点的载波频率确定所述用户设备对应的工作模式。

具体地，由于不同的载波频率对应着特定的接入节点类型，所以用户设备可以根据载波频率确定与载波频率对应的接入节点类型，从而判断出所述用户设备的工作模式。

可选地，所述用户设备根据所述用户设备的功能信息确定所述用户设备的工作模式。

其中，所述功能信息可以为所述用户设备的版本，或所述用户设备进行工作的功能模块儿信息，在此不作限定。

可选地，所述用户设备可以通过判断当前的工作模式是否支持预设功能，确定所述用户设备的工作模式。

具体地，例如，当所述用户设备判断出当前工作模式支持256正交振幅键

控QAM时, 所述用户设备就可以获取到当前的工作模式为LTE Hi工作模式。

可选地, 所述用户设备根据与工作模式对应的用户设备标识, 获取与所述用户设备对应的工作模式。

其中, 所述用户设备标识可以是用户在所述工作模式下使用的USIM对应的
5 的全球移动用户标识IMSI。

102、用户设备接收网络侧设备发送的演进的分组系统EPS认证矢量中的随机值RAND和认知码AUTN。

其中, 所述演进的分组系统EPS认证矢量包括所述RAND、所述AUTN、密
钥KASME和期望的响应值RES, 所述EPS认证矢量为所述网络侧设备根据认证
10 服务器HLR发送的通用移动通信系统UMTS认证矢量获取的, 所述KASME为所
述网络侧设备根据所述UMTS认证矢量中的加密密钥CK以及完整性保护密钥
IK获取的。

进一步地, 当所述用户设备的工作模式为LTE UE工作模式时, 采用现有的EPS AKA进行用户设备的认证。

15 103、当所述用户设备的工作模式为长期演进节点LTE Hi工作模式, 则所述用户设备根据所述RAND和AUTN进行认证。

其中, 在所述认证过程中, 所述用户设备忽略对所述AUTN中认证管理域AMF的分离比特位进行校验的校验结果; 或者, 所述用户设备不对所述AMF的分离比特位进行校验。

20 具体地, 所述用户设备判断所述AUTN中的消息认证码MAC和序列号SQN是否均与所述用户设备的MAC和SQN相同; 当所述AUTN中的所述MAC和所述SQN与所述用户设备的所述MAC和所述SQN均相同时, 所述用户设备向所

述网络侧设备发送验证成功消息。

其中，所述验证成功消息携带文本文档RES。进一步地，所述网络侧设备对所述用户设备进行认证。

本实施例提供一种用户设备的认证装置，如图2所示，所述装置的实体可以
5 以为用户设备，所述装置包括：接收单元21、认证单元22、确定单元23。

接收单元21，用于接收网络侧设备发送的演进的分组系统EPS认证矢量中的随机值RAND和认知码AUTN。

认证单元22，用于当工作模式为长期演进节点LTE Hi工作模式，则根据所述接收单元21接收的所述RAND和AUTN进行认证，其中，在所述认证过程中，
10 忽略对所述AUTN中认证管理域AMF的分离比特位进行校验的校验结果；或者，不对所述AMF的分离比特位进行校验。

所述认证单元22具体可以包括：判断模块2201、发送模块2202。

判断模块2201，可以用于判断所述AUTN中的消息认证码MAC和序列号SQN是否均与所述用户设备的MAC和SQN相同；

15 发送模块2202，可以用于当所述判断模块2201判断出所述AUTN中的所述MAC和所述SQN与所述用户设备的所述MAC和所述SQN均相同时，向所述网络侧设备发送验证成功消息。

确定单元23，用于确定工作模式。

所述确定单元23具体可以包括：第一确定模块2301、第二确定模块2302、
20 第三确定模块2303、第四确定模块2304、第五确定模块2305。

第一确定模块2301，可以用于根据无线接入节点的类型确定所述工作模式。

第二确定模块2302,可以用于根据无线接入节点的载波频率确定所述工作模式。

第三确定模块2303,可以用于根据功能信息确定所述工作模式。

5 第四确定模块2304,可以用于通过判断当前的工作模式是否支持预设功能,确定所述工作模式。

第五确定模块2305,可以用于根据与工作模式对应的用户设备标识,确定所述工作模式。

本实施例提供另一种用户设备的认证方法,如图3所示,所述方法包括:

301、网络侧设备获取通用移动通信系统UMTS认证矢量。

10 其中,所述网络侧设备可以为移动性管理实体MME或者具有MME功能的设备,在此不作限定。所述UMTS包括随机值RAND、认知码AUTN、加密密钥CK、完整性保护密钥IK和期望的响应值RES。

所述步骤301之前,还包括所述网络侧设备通过附着接收信息或跟踪区域更新信息或安全模式完成信息指示所述用户设备对应的无线接入节点的类型,
15 以使得所述用户设备获取所述用户设备对应的工作模式。

302、当用户设备的工作模式为长期演进节点LTE Hi工作模式时,所述网络侧设备根据所述UMTS认证矢量,获取分组系统EPS认证矢量。

其中,所述EPS认证矢量包括所述RAND、所述AUTN、密钥KASME和期望的响应值RES,所述KASME为所述网络侧设备根据所述UMTS认证矢量中的
20 所述CK和所述IK获取的。

具体地,根据公式 $KASME = KDF(CK || IK, (FC, SN\ id, SQN \oplus AK, \text{length of } SN\ id, \text{length of } SQN \oplus AK))$ 将所述UMTS认证矢量转化为分组系统EPS认证

矢量。

其中，所述 KDF 为密钥推演函数，FC 为区分值，SN ID 为服务网络标识，AK 为匿名密钥。

303、所述网络侧设备向所述用户设备发送所述EPS认证矢量中的随机值
5 RAND和认知码AUTN，以使得所述用户设备根据所述RAND和所述AUTN进行认证。

本实施例提供另一种用户设备的认证装置，如图4所示，所述装置的实体可以为移动性管理实体MME，所述装置包括：获取单元41、发送单元42、指示单元43。

10 获取单元41，用于获取通用移动通信系统UMTS认证矢量。

所述获取单元41，还可以用于当用户设备的工作模式为长期演进节点LTE Hi工作模式时，根据所述UMTS认证矢量，获取分组系统EPS认证矢量。

其中，所述UMTS包括随机值RAND、认知码AUTN、加密密钥CK、完整性保护密钥IK和期望的响应值RES；所述EPS认证矢量包括所述RAND、所述
15 AUTN、密钥KASME和期望的响应值RES，所述KASME为所述网络侧设备根据所述UMTS认证矢量中的所述CK和所述IK获取的。

发送单元42，用于向所述用户设备发送所述获取单元41获取的所述EPS认证矢量中的随机值RAND和认知码AUTN，以使得所述用户设备根据所述RAND和所述AUTN进行认证。

20 指示单元43，用于通过附着接收信息或跟踪区域更新信息或安全模式完成信息指示所述用户设备对应的无线接入节点的类型，以使得所述用户设备确定所述用户设备的工作模式。

本实施例提供一种用户设备的认证系统，如图5所示，所述系统包括：用户设备51、认证服务器HLR52、网络侧设备53。

所述HLR52，用于接收到网络侧设备53发送的认证请求信息后，向所述网络侧设备发送携带有通用移动通信系统UMTS认证矢量的认证响应请求响应信息。

本发明实施例提供的用户设备的认证方法、装置及系统，首先用户设备接收网络侧设备发送的演进的分组系统EPS认证矢量中的随机值RAND和认知码AUTN；当所述用户设备的工作模式为长期演进节点LTE Hi工作模式，则所述用户设备根据所述RAND和AUTN进行认证，其中，在所述认证过程中，所述用户设备忽略对所述AUTN中认证管理域AMF的分离比特位进行校验的校验结果；或者，所述用户设备不对所述AMF的分离比特位进行校验。通过现有技术在进行用户设备认证时，由于对于3G的认证服务器HLR，AMF的分离比特位设置为0，进而导致了在3G的HLR条件下，用户设备UE无法通过EPS AKA的验证，从而造成用户设备不能正常入网的问题。而本发明实施例，通过忽略或不进行AMF的分离比特位的验证，实现了在不修改认证服务器HLR的处理逻辑下，UE可以正常地进行EPS AKA的验证，解决了由于用户设备无法通过EPS AKA的验证，从而不能正常入网的问题。

本发明实施例提供的用户设备的认证装置可以实现上述提供的方法实施例，具体功能实现请参见方法实施例中的说明，在此不再赘述。本发明实施例提供的用户设备的认证方法、装置及系统可以适用于通信系统领域，但不仅限于此。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，

是可以通过计算机程序来指令相关的硬件来完成,所述的程序可存储于一计算机可读取存储介质中,该程序在执行时,可包括如上述各方法的实施例的流程。其中,所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory, ROM)或随机存储记忆体(Random Access Memory, RAM)等。

- 5 以上所述,仅为本发明的具体实施方式,但本发明的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,可轻易想到的变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应该以权利要求的保护范围为准。

权 利 要 求

1、一种用户设备的认证方法，其特征在于，包括：

用户设备接收网络侧设备发送的演进的分组系统EPS认证矢量中的随机值RAND和认知码AUTN；

5 当所述用户设备的工作模式为长期演进节点LTE Hi工作模式，则所述用户设备根据所述RAND和AUTN进行认证，其中，在所述认证过程中，所述用户设备忽略对所述AUTN中认证管理域AMF的分离比特位进行校验的校验结果；或者，所述用户设备不对所述AMF的分离比特位进行校验。

2、根据权利要求1所述的所述的用户设备的认证方法，其特征在于，所述方法还
10 包括：

所述用户设备确定所述用户设备的工作模式。

3、根据权利要求2所述的所述的用户设备的认证方法，其特征在于，所述用户设备确定所述用户设备的工作模式包括：

所述用户设备根据无线接入节点的类型确定所述用户设备的工作模式；

15 所述用户设备根据无线接入节点的载波频率确定所述用户设备的工作模式；

所述用户设备根据所述用户设备的功能信息确定所述用户设备的工作模式；

20 所述用户设备通过判断当前的工作模式是否支持预设功能，确定所述用户设备的工作模式；或

所述用户设备根据与工作模式对应的用户设备标识，确定所述用户设备的工作模式。

4、根据权利要求3所述的用户设备的认证方法，其特征在于，

所述无线接入节点的类型为所述网络侧设备通过附着接收信息或跟踪区域更新信息或安全模式完成信息指示的；或

所述无线接入节点的类型为与所述无线接入节点对应的小区通过广播消

5 息指示的。

5、根据权利要求1至4中任意一项所述的用户设备的认证方法，其特征在于，所述用户设备根据所述RAND和AUTN进行认证包括：

所述用户设备判断所述AUTN中的消息认证码MAC和序列号SQN是否均与所述用户设备的MAC和SQN相同；

10 当所述AUTN中的所述MAC和所述SQN与所述用户设备的所述MAC和所述SQN均相同时，所述用户设备向所述网络侧设备发送验证成功消息。

6、一种用户设备的认证装置，其特征在于，包括：

接收单元，用于接收网络侧设备发送的演进的分组系统EPS认证矢量中的随机值RAND和认证码AUTN；

15 认证单元，用于当工作模式为长期演进节点LTE Hi工作模式，则根据所述接收单元接收的所述RAND和AUTN进行认证，其中，在所述认证过程中，忽略对所述AUTN中认证管理域AMF的分离比特位进行校验的校验结果；或者，不对所述AMF的分离比特位进行校验。

7、根据权利要求6所述的用户设备的认证装置，其特征在于，还包括：

20 确定单元，用于确定工作模式。

8、根据权利要求7所述的用户设备的认证装置，其特征在于，所述确定单元包括：

—14—

第一确定模块，用于根据无线接入节点的类型确定所述工作模式；

第二确定模块，用于根据无线接入节点的载波频率确定所述工作模式；

第三确定模块，用于根据功能信息确定所述工作模式；

第四确定模块，用于通过判断当前的工作模式是否支持预设功能，确定所

5 述工作模式；

第五确定模块，用于根据与工作模式对应的用户设备标识，确定所述工作模式。

9、根据权利要求8所述的用户设备的认证装置，其特征在于，

所述无线接入节点的类型为所述网络侧设备通过附着接收信息或跟踪区
10 域更新信息或安全模式完成信息指示的；或

所述无线接入节点的类型为与所述无线接入节点对应的小区通过广播消息指示的。

10、根据权利要求5至9中任意一项所述的用户设备的认证装置，其特征在于，所述认证单元包括：

15 判断模块，用于判断所述AUTN中的消息认证码MAC和序列号SQN是否均与所述用户设备的MAC和SQN相同；

发送模块，用于当所述判断模块判断出所述AUTN中的所述MAC和所述SQN与所述用户设备的所述MAC和所述SQN均相同时，向所述网络侧设备发送验证成功消息。

20 11、一种用户设备的认证方法，其特征在于，包括：

网络侧设备获取通用移动通信系统UMTS认证矢量；

当用户设备的工作模式为长期演进节点LTE Hi工作模式时，所述网络侧设

备根据所述UMTS认证矢量，获取分组系统EPS认证矢量；

所述网络侧设备向所述用户设备发送所述EPS认证矢量中的随机值RAND和认知码AUTN，以使得所述用户设备根据所述RAND和所述AUTN进行认证。

12、根据权利要求11所述的用户设备的认证方法，其特征在于，所述UMTS
5 包括随机值RAND、认知码AUTN、加密密钥CK、完整性保护密钥IK和期望的响应值RES；

所述EPS认证矢量包括所述RAND、所述AUTN、密钥KASME和期望的响应值RES，所述KASME为所述网络侧设备根据所述UMTS认证矢量中的所述CK和所述IK获取的。

10 13、根据权利要求11所述的用户设备的认证方法，其特征在于，在所述网络侧设备获取通用移动通信系统UMTS认证矢量之前，所述方法还包括：

所述网络侧设备通过附着接收信息或跟踪区域更新信息或安全模式完成信息指示所述用户设备对应的无线接入节点的类型，以使得所述用户设备确定所述用户设备的工作模式。

15 14、一种用户设备的认证装置，其特征在于，包括：

获取单元，用于获取通用移动通信系统UMTS认证矢量；

所述获取单元，还用于当用户设备的工作模式为长期演进节点LTE Hi工作模式时，根据所述UMTS认证矢量，获取分组系统EPS认证矢量；

发送单元，用于向所述用户设备发送所述获取单元获取的所述EPS认证矢
20 量中的随机值RAND和认知码AUTN，以使得所述用户设备根据所述RAND和所述AUTN进行认证。

15、根据权利要求14所述的用户设备的认证装置，其特征在于，所述UMTS

-16-

包括随机值RAND、认知码AUTN、加密密钥CK、完整性保护密钥IK和期望的响应值RES;

所述EPS认证矢量包括所述RAND、所述AUTN、密钥KASME和期望的响应值RES, 所述KASME为所述网络侧设备根据所述UMTS认证矢量中的所述

5 CK和所述IK获取的。

16、根据权利要求14所述的用户设备的认证装置, 其特征在于, 还包括:

指示单元, 用于通过附着接收信息或跟踪区域更新信息或安全模式完成信息指示所述用户设备对应的无线接入节点的类型, 以使得所述用户设备确定所述用户设备的工作模式。

10 17、一种用户设备的认证系统, 其特征在于, 包括: 权利要求6至10中任一项所述的用户设备的认证装置、认证服务器HLR和权利要求14至16中任一项所述的用户设备的认证装置;

所述HLR, 用于接收到网络侧设备发送的认证请求信息后, 向所述网络侧设备发送携带有通用移动通信系统UMTS认证矢量的认证响应请求响应信
15 息。

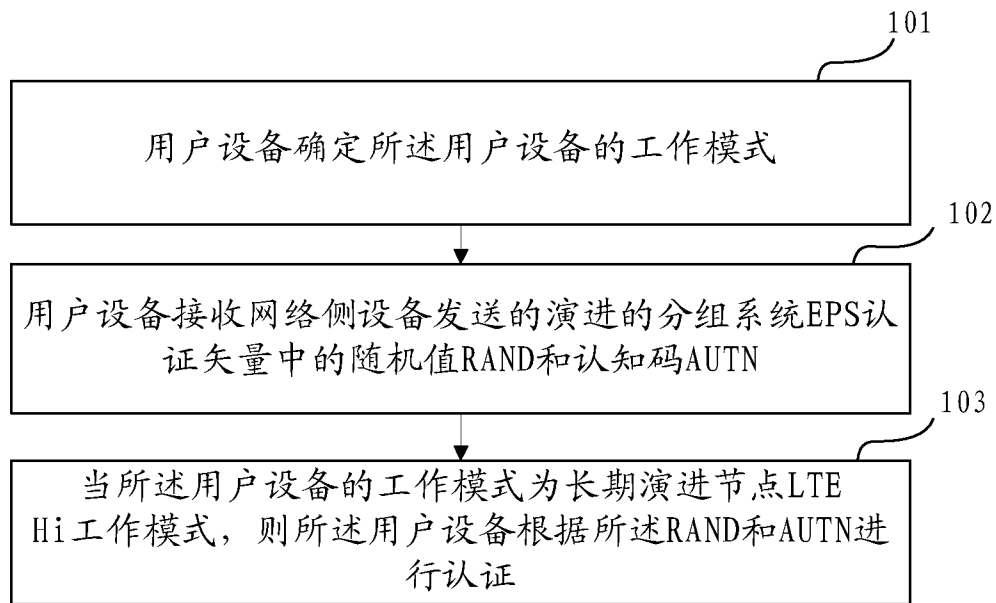


图 1

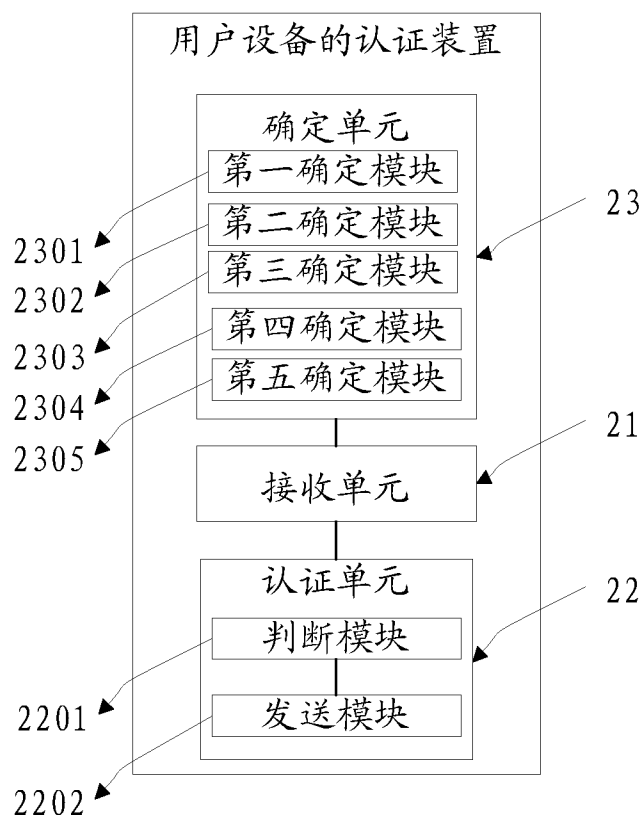


图 2

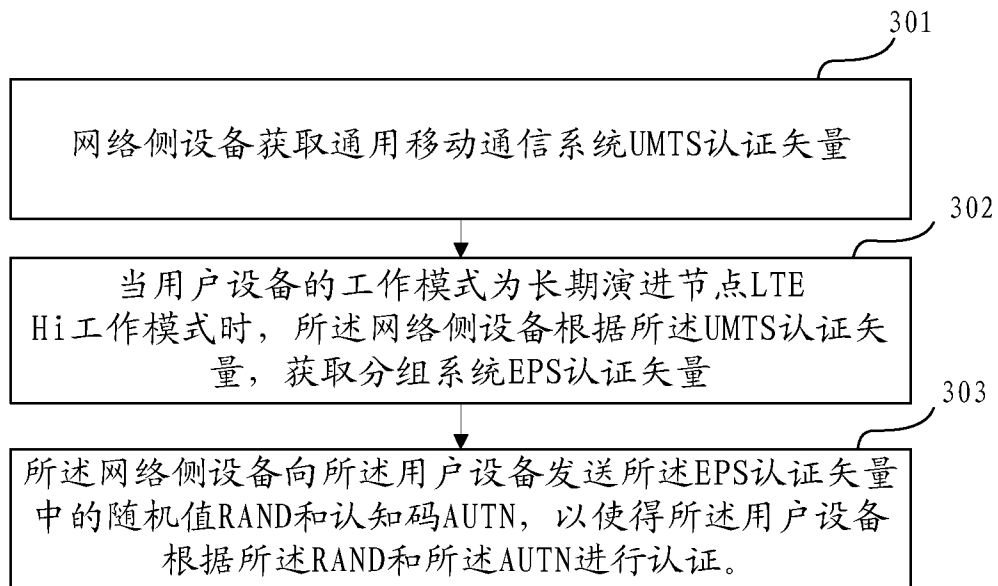


图 3

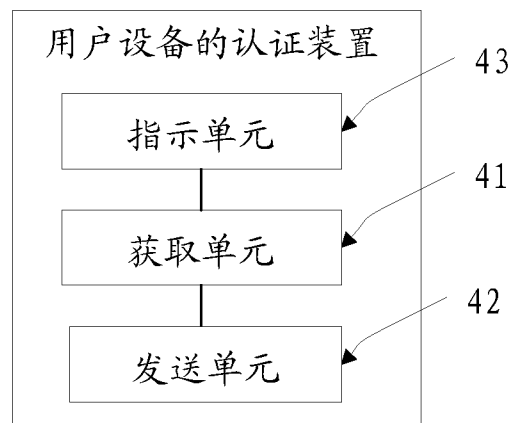


图 4

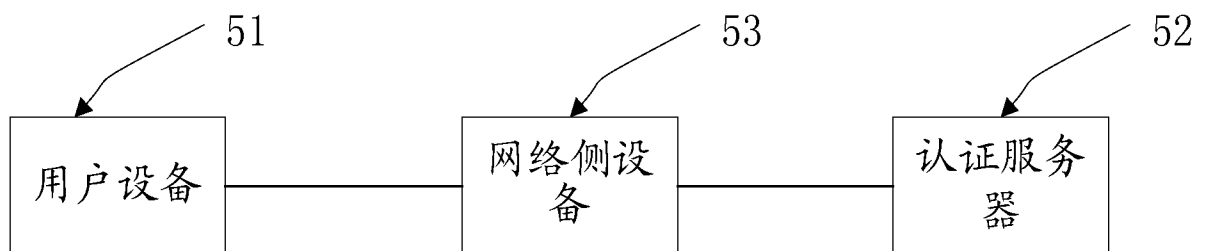


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/074156

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06 (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; H04L 9/-

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, USTXT, CNTXT, WOTXT, 3GPP: authentication, random, cognition code, test, authentication, evolution, LTE, Hi, EPS, packet?, vector, RAND, AUTN, KASME, RES, AMF, separation, bit, check???

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	3 rd GENERATION PARTNERSHIP PROJECT, 3GPP TS 33.401: Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security, architecture (Release 11), http://www.3gpp.org/ftp/Specs/html-info/33401.htm , 16 March 2012 (16.03.2012), pages 19-21	1-4, 6-9, 11, 13-14, 16
Y		5, 10, 12, 15, 17
Y	CN 102083064 A (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.), 01 June 2011 (01.06.2011), description, paragraphs [0002]-[0005] and [0037]-[0055], and figures 1-2 and 4-7	5, 10, 12, 15, 17
A	CN 101827364 A (LG ELECTRONICS INC.), 08 September 20 10 (08.09.2010), the whole document	1-17
A	WO 2009/121407 A1 (NOKIA SIEMENS NETWORKS OY et al.), 08 October 2009 (08.10.2009), the whole document	1-17

☐ 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 May 2013 (08.05.2013)

Date of mailing of the international search report
23 May 2013 (23.05.2013)

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
CHENG, Qian
Telephone No.: (86-10) **62413377**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2013/074156

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102083064 A	01.06.2011	None	
CN 101827364 A	08.09.2010	EP 2227049 A1	08.09.2010
		US 2010/0227591 A1	09.09.2010
		KR 20100100641 A	15.09.2010
WO 2009/121407 A1	08.10.2009	EP 2258126 A1	08.12.2010
		US 2011/0004762 A1	06.01.2011
		CN 101983517 A	02.03.2011
		DK 2258126 T3	15.10.2012
		ES 2393577 T3	26.12.2012

国际检索报告

国际申请号
PCT/CN2013/074156

A. 主题的分类

H04W 12/06 (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; H04L 9/-

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, USTXT, CNTXT, WOTXT, 3GPP:鉴权, 认证, 演进, 分组, 矢量, 随机, 认知码, 分离, 比特, 校验, 检验, authentication, evolution, LTE, Hi, EPS, packet?, vector, RAND, AUTN, KASME, RES, AMF, separation, bit, check???

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	3 rd GENERATION PARTNERSHIP PROJECT, 3GPP TS 33.401: Technical Specification Group Services and System Aspects; 3GPP System Architecture	1-4,6-9,11,13-14,16
Y	Evolution(SAE); Security architecture(Release 11), http://www.3gpp.org/ftp/Specs/html-info/33401.htm , 16. 3 月 2012(16.03.2012), 第 19 至 21 页	5,10,12,15,17
Y	CN 102083064A(大唐移动通信设备有限公司) 01. 6 月 2011(01.06.2011), 说明书第[0002]-[0005], [0037]-[0055]段, 附图 1-2, 4-7	5,10,12,15,17
A	CN 101827364A(LG 电子株式会社) 08. 9 月 2010(08.09.2010), 全文	1-17
A	WO 2009/121407A1(NOKIA SIEMENS NETWORKS OY 等) 08. 10 月 2009(08.10.2009), 全文	1-17

☐ 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. 5 月 2013(08.05.2013)

国际检索报告邮寄日期

23.5 月 2013 (23.05.2013)

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

成谦

电话号码: (86-10) **62413377**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/074156

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 102083064A	01.06.2011	无	
CN 101827364A	08.09.2010	EP 2227049A1	08.09.2010
		US 2010/0227591A1	09.09.2010
		KR 20100100641A	15.09.2010
WO 2009/121407A1	08.10.2009	EP 2258126A1	08.12.2010
		US 2011/0004762A1	06.01.2011
		CN 101983517A	02.03.2011
		DK 2258126T3	15.10.2012
		ES 2393577T3	26.12.2012