(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 12 月 19 日 (19.12.2013)

WIPO | PCT

(10) 国际公布号
WO 2013/185709 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2013/080490

(22) 国际申请日: 2013 年 7 月 31 日 (31.07.2013)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201210335631.X 2012 年 9 月 12 日 (12.09.2012) CN

(71) 申请人: **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: **谢仕云 (XIE, Shiyun)**; 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中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **曹岚健 (CAO, Lanjian)**; 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中兴通讯股份有限公司转交, 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, 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, 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, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title**: CALL AUTHENTICATION METHOD, DEVICE, AND SYSTEM

(54) **发明名称** : 一种呼叫认证方法、设备和系统

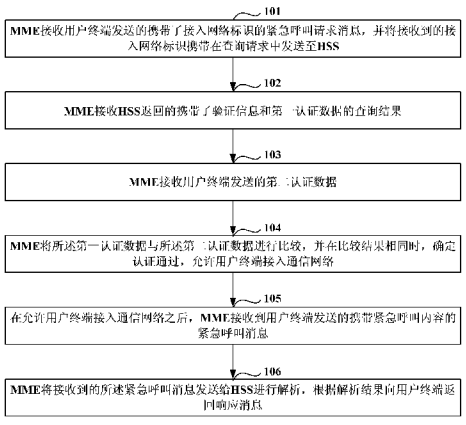

图 2 / Fig. 2

101 An MME receives an emergency call request message carrying an access network identifier and sent by a user terminal, carries the access network identifier in a query request, and sends the inquiry request to an HSS

102 The MME receives a query result carrying verification information and first authentication data and returned by the HSS

103 The MME receives second authentication data sent by the user terminal

104 The MME compares the first authentication data with the second authentication data, when a comparison is the same, determines that authentication is passed, and allows the user terminal to access a communication network

105 After allowing the user terminal to access the communication network, the MME receives an emergency call message carrying emergency call content and sent by the user terminal

106 The MME sends the received emergency call message to the HSS for being parsed, and returns a response message to the user terminal according to a parsing result

(57) **Abstract**: A call authentication method, device, and system. The method comprises: an MME receiving an emergency call request message carrying an access network identifier and sent by a user terminal, carrying the access network identifier in a query request, and sending the inquiry request to an HSS; the MME receiving a query result carrying verification information and first authentication data and returned by the HSS; the MME receiving second authentication data sent by the user terminal; and the MME comparing the first authentication data with the second authentication data, when a comparison is the same, determining that authentication is passed, and allowing the user terminal to access a communication network. In embodiments of the present invention, an illegal user terminal is prevented from maliciously using the communication network by using an emergency call manner, thereby improving the security of an emergency call and ensuring the security of application of the communication network.

(57) **摘要**: 一种呼叫认证方法、设备和系统。所述方法包括：MME 接收用户终端发送的携带了接入网络标识的紧急呼叫请求消息，并将所述接入网络标识携带在查询请求中发送至 HSS；所述 MME 接收所述 HSS 返回的携带了验证信息和第一认证数据的查询结果；所述 MME 接收所述用户终端发送的第二认证数据；以及所述 MME 将第一认证数据与第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许用户终端接入通信网络。本发明实施例中，避免了非法的用户终端利用紧急呼叫方式恶意使用通信网络，提高了紧急呼叫的安全性，保证了通信网络的应用的安全性。

WO 2013/185709 A1

根据细则 4.17 的声明:

— 关于申请人有权申请并被授予专利(细则 4.17(ii))

— 发明人资格(细则 4.17(iv))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

— 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。

一种呼叫认证方法、设备和系统

技术领域

本发明涉及无线通信领域，尤其涉及一种呼叫认证方法、设备和系统。

背景技术

紧急呼叫是移动通信系统中一种特有的语音业务，允许移动用户在移动终端处于受限呼叫或者未插入用户识别模块(Subscriber Identity Module，SIM)卡的情况下，通过所处位置覆盖的移动通信网络，呼叫运营商提供的紧急呼叫中心，例如，120中心、119火警等，其中，将移动终端处于受限呼叫或者未插入SIM卡的情况称之为紧急附着情况。

在相关技术中，移动终端在紧急附着的情况下向网络侧发出紧急呼叫，网络侧通常可以忽略移动终端的国际移动用户标识（International Mobile Subscriber Identity，IMSI），允许移动终端接入核心网。此时，移动终端需要将其国际移动设备标识（International Mobile Equipment Identity，IMEI）发送至网络侧；网络侧在接收到的移动终端的IMEI时，将IMEI作为移动终端紧急接入核心网的标识信息。如图1所示，图1为用户利用移动终端通过移动通信网络发出紧急呼叫的流程图，包括如下步骤:

第一步、移动终端（即，用户设备（User Equipment，UE））与所处位置的基站（即，演进型节点B（Evolved Node B，eNodeB））建立无线资源控制（Radio Resource Control，RRC）连接。

第二步、UE向eNodeB发送请求消息，所述请求消息中包含了呼叫类型和接入网络标识，其中，所述呼叫类型为紧急呼叫类型。

所述接入网络标识可以是UE保存的全球唯一临时标识(Globally Unique Temporary Identity，GUTI）或者分组临时移动用户标识（Packet Temporary Mobile Subscriber Identity，P-TMSI），可以是UE的IMSI，还可以是UE的IMEI。

第三步、eNodeB为所述UE选择一个移动管理实体(Mobile Management

Entity，MME），并将接收到的请求消息转发给 MME。

第四步、MME 判断自身是否具有响应紧急呼叫的能力，当确定具有响应紧急呼叫的能力时，判断接收到的请求消息中携带的 UE 的接入网络标识，执行第五步；当确定不具有响应紧急呼叫的能力时，返回拒绝响应消息。

第五步、MME 在确定所述请求消息中携带的接入网络标识为 GUTI 或者 P-TMSI 时，请求 UE 上报 IMSI，并在接收到的 UE 上报的 IMSI 时，响应请求消息，允许接入网络。

第六步、MME 在确定所述请求消息中携带的接入网络标识为 IMEI 时，将接收到的 IMEI 发送至设备识别寄存器（Equipment Identity Register，EIR）进行确认，并在确认通过时，响应请求消息，允许接入网络。

由于在通信系统中，MME 响应终端的紧急呼叫请求时，确定 UE 上报的接入网络标识为 IMEI 后，MME 仅对所述 IMEI 是否被列入黑名单进行确认，并在确认所述 IMEI 没有被列入黑名单时，允许 UE 接入核心网。

这样不仅将导致不法者利用紧急呼叫这一方式进入核心网，对核心网进行恶意攻击，增加了通信网络的不安全因素，而且由于在紧急呼叫中 UE 和网络侧没有建立安全的通信链路，导致通信中占用的空口资源得不到安全保护，使得紧急呼叫中的一些信息被窃取或者篡改，使得紧急呼叫的安全性较差。

发明内容

本发明实施例提供了一种呼叫认证方法、设备和系统，解决相关技术中当用户终端在紧急附着的情况下向网络侧发送紧急呼叫请求时，网络侧并不对发起呼叫的用户终端进行安全认证，导致紧急呼叫的安全性较差的问题。

本发明实施例提供了一种呼叫认证方法，包括:

移动管理实体（MME）接收用户终端发送的携带了接入网络标识的紧急呼叫请求消息，并将所述接入网络标识携带在查询请求中发送至归属签约用户服务器（HSS）；

所述 MME 接收所述 HSS 返回的携带了验证信息和第一认证数据的查询

结果，其中，所述第一认证数据是所述 HSS 将查找的安全密钥和随机产生的验证信息进行计算得到的；所述安全密钥包括设备密钥；所述设备密钥是所述 HSS 根据本地存储的接入网络标识与设备密钥之间的对应关系确定；

所述 MME 接收所述用户终端发送的第二认证数据，其中，所述第二认证数据是所述用户终端在接收所述 MME 发送的验证信息后，利用本地存储的安全密钥和所述验证信息进行计算得到的；以及

所述 MME 将所述第一认证数据与所述第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许所述用户终端接入通信网络。

可选地，所述方法还包括：在允许所述用户终端接入所述通信网络之后，

所述 MME 接收到所述用户终端发送的携带紧急呼叫内容的紧急呼叫消息，其中，所述紧急呼叫内容是所述用户终端利用所述安全密钥进行加密后得到的；以及

所述 MME 将接收到的所述紧急呼叫消息发送给所述 HSS 进行解析，根据解析结果向所述用户终端返回响应消息。

可选地，所述方法还包括：所述 MME 在接收到所述紧急呼叫请求消息之后，向所述 HSS 发送所述查询请求之前，

所述 MME 根据所述用户终端的接入网络标识与紧急呼叫请求次数之间的对应关系，查找所述用户终端在设定时长内向所述 MME 发送紧急呼叫请求的次数；

所述 MME 判断查找到的紧急呼叫请求次数是否大于设定阈值，若是，则拒绝响应所述用户终端的紧急呼叫请求；若否，则执行向所述 HSS 发送所述查询请求的操作。

可选地，所述 MME 接收用户终端发送的第二认证数据的步骤包括：

所述 MME 接收在所述用户终端接收到所述 MME 发送的验证信息时，利用本地存储的安全密钥对接收到的验证信息进行计算得到的第二认证数据。

可选地，所述 MME 将所述第一认证数据与所述第二认证数据进行比较的步骤包括：

所述 MME 判断接收到的第一认证数据与第二认证数据是否相同，若相同，则执行认证通过，允许接入网络的操作；若不相同，则执行认证不通过，拒绝接入网络的操作。

本发明实施例还提供了一种呼叫认证方法，包括:

归属签约用户服务器（HSS）接收移动管理实体（MME）发送的查询请求，其中，所述查询请求中包含了接入网络标识，所述接入网络标识是用户终端向所述 MME 发送紧急呼叫请求消息时携带的;

所述 HSS 根据本地存储的接入网络标识与设备密钥之间的对应关系，确定所述查询请求中包含的接入网络标识对应的设备密钥，并利用包含所述设备密钥的安全密钥和随机产生的验证信息进行计算得到第一认证数据；以及

所述 HSS 将随机产生的验证信息与得到的第一认证数据作为查询结果发送给所述 MME，使得所述 MME 将得到的第一认证数据与接收到的所述用户终端发送的第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许所述用户终端接入通信网络。

可选地，所述接入网络标识为所述用户终端的国际移动设备标识(IMEI);

所述本地存储的接入网络标识与设备密钥之间的对应关系包括:

所述 HSS 本地存储的所述用户终端的 IMEI 与所述设备密钥之间的对应关系。

本发明实施例还提供了一种呼叫认证设备，包括:

第一接收模块，其设置成：接收用户终端发送的携带了接入网络标识的紧急呼叫请求消息，并将所述接入网络标识携带在查询请求中发送至归属签约用户服务器（HSS）；

第二接收模块，其设置成：接收所述 HSS 返回的携带了验证信息和第一认证数据的查询结果，其中，所述第一认证数据是所述 HSS 将查找的安全密钥和随机产生的验证信息进行计算得到的；所述安全密钥包含设备密钥；所述设备密钥是所述 HSS 根据本地存储的接入网络标识与设备密钥之间的对应关系确定;

第三接收模块，其设置成：接收所述用户终端发送的第二认证数据，其

中，所述第二认证数据是所述用户终端在接收移动管理实体（MME）发送的验证信息后，利用本地存储的安全密钥对所述验证信息进行计算得到的；以及

比较模块，其设置成：将所述第一认证数据与所述第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许所述用户终端接入通信网络。

可选地，所述设备还包括：

第四接收模块，其设置成：在允许所述用户终端接入所述通信网络之后，接收到所述用户终端发送的携带紧急呼叫内容的紧急呼叫消息，其中，所述紧急呼叫内容是所述用户终端利用所述安全密钥进行加密后得到的；

消息处理模块，其设置成：将接收到的所述紧急呼叫消息发送给所述 HSS 进行解析，根据解析结果向所述用户终端返回响应消息。

可选地，所述紧急呼叫请求消息中携带了所述用户终端的接入网络标识；

所述设备还包括：呼叫次数确定模块和呼叫判断模块，其中：

所述呼叫次数确定模块设置成：将接收到的所述接入网络标识携带在所述查询请求中发送至所述 HSS 之前，根据所述用户终端的接入网络标识与紧急呼叫请求次数之间的对应关系，查找所述用户终端在设定时长内发送紧急呼叫请求的次数；

所述呼叫判断模块设置成：判断查找到的紧急呼叫请求次数是否大于设定阈值，若是，则拒绝响应所述用户终端的紧急呼叫请求；若否，则执行将接收到的所述接入网络标识携带在所述查询请求中发送至所述 HSS 的操作。

可选地，所述比较模块是设置成以如下方式将所述第一认证数据与所述第二认证数据进行比较：

判断接收到的所述第一认证数据与所述第二认证数据是否相同，若相同，则执行认证通过，允许接入网络的操作；若不相同，则执行认证不通过，拒绝接入网络的操作。

本发明实施例还提供了一种归属签约用户服务器（HSS），包括：

接收模块，其设置成：接收移动管理实体（MME）发送的查询请求，其中，所述查询请求中包含了接入网络标识，所述接入网络标识是用户终端向

所述 MME 发送紧急呼叫请求消息时携带的;

第一认证数据计算模块，其设置成：根据本地存储的接入网络标识与设备密钥之间的对应关系，确定所述查询请求中包含的接入网络标识对应的设备密钥，并利用包含所述设备密钥的安全密钥和随机产生的验证信息进行计算得到第一认证数据；以及

发送模块，其设置成：将所述随机产生的验证信息与得到的所述第一认证数据作为查询结果发送给所述 MME，使得所述 MME 将得到的所述第一认证数据与接收到的所述用户终端发送的第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许所述用户终端接入通信网络。

可选地，所述接入网络标识为所述用户终端的国际移动设备标识(IMEI);

所述第一认证数据计算模块还设置成：存储所述用户终端的 IMEI 与所述设备密钥之间的对应关系。

本发明实施例还提供了一种呼叫认证系统，包括：移动管理实体 MME、用户终端和归属签约用户服务器（HSS）；其中，

所述 MME 设置成：接收用户终端发送的紧急呼叫请求消息，并将包含了所述紧急呼叫请求消息中携带的接入网络标识的查询请求发送至所述 HSS；接收所述 HSS 返回的携带了验证信息和第一认证数据的查询结果，以及所述用户终端发送的第二认证数据；将所述第一认证数据与所述第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许所述用户终端接入通信网络；在允许所述用户终端接入所述通信网络之后，接收到所述用户终端发送的携带紧急呼叫内容的紧急呼叫消息，其中，所述紧急呼叫内容是所述用户终端利用安全密钥进行加密后得到的；以及将接收到的所述紧急呼叫消息发送给所述 HSS 进行解析，根据解析结果向所述用户终端返回响应消息;

所述用户终端设置成：发送所述携带了接入网络标识的紧急呼叫请求消息至所述 MME；发送所述第二认证数据至所述 MME；以及在允许接入所述通信网络之后，向所述 MME 发送所述携带紧急呼叫内容的紧急呼叫消息，其中，所述紧急呼叫内容是利用所述安全密钥进行加密后得到的；以及

所述 HSS 设置成：接收所述 MME 发送的所述携带了接入网络标识的查询请求，并根据本地存储的接入网络标识与设备密钥之间的对应关系，确定所述查询请求中包含的接入网络标识对应的设备密钥，并利用包含所述设备密钥的安全密钥和随机产生的验证信息进行计算得到所述第一认证数据发送至所述 MME；以及在允许所述用户终端接入所述通信网络之后，接收并解析所述 MME 发送的所述携带紧急呼叫内容的紧急呼叫消息。

可选地，所述用户终端还设置成：在所述用户终端接收到所述 MME 发送的验证信息时，利用本地存储的安全密钥对接收到的验证信息进行计算得到所述第二认证数据。

本发明实施例中，通过在用户终端本地和 HSS 本地分别存储了用户终端的 IMEI 与设备密钥之间的对应关系，避免了非法的用户终端利用紧急呼叫方式恶意使用通信网络，提高了紧急呼叫的安全性，保证了通信网络的应用的安全性。

附图概述

图 1 为用户利用移动终端通过移动通信网络发出紧急呼叫的流程图；

图 2 为本发明实施例一的一种呼叫认证方法的流程图；

图 3 为本发明实施例二的一种呼叫认证设备的结构示意图；

图 4 为本发明实施例三的一种 HSS 的结构示意图；

图 5 为本发明实施例四的一种呼叫认证系统的结构图。

本发明的较佳实施方式

本发明实施例公开了一种呼叫认证方法、设备和系统，通过在用户终端本地和 HSS 本地分别存储了用户终端的 IMEI 与设备密钥之间的对应关系，在用户终端向 MME 发送紧急呼叫请求消息时，MME 从 HSS 处获取包含设备密钥的安全密钥，并和随机验证信息进行运算得到的第一认证数据，以及接收到用户终端发送的根据本地存储的安全密钥和接收到的验证消息计算得

到的第二认证数据，并将第一认证数据与第二认证数据进行比较，在比较结果相同时，确定认证通过，允许用户终端接入通信网络，这样避免了非法的用户终端利用紧急呼叫方式恶意使用通信网络，提高了紧急呼叫的安全性，保证了通信网络的应用的安全性。

需要说明的是，在本发明实施例的方案中，网络侧和用户终端中设置了对称的设备密钥，用于网络侧对用户终端进行认证。所述设备密钥和用户终端的 IMEI 相关联，网络侧将用户终端的 IMEI 与设备密钥之间的对应关系、以及设备密钥存放在 HSS 中，网络侧仅能通过查询获取利用设备密钥进行计算的运算结果，并不能直接获取设备密钥；合法的用户终端将自身的设备密钥存储在安全组件中，也仅能通过查询获取利用设备密钥进行计算的运算结果，并不能直接获取设备密钥。其中，设备密钥与 IMEI 是一一对应关系，每一个设备密钥对应唯一一个 IMEI。

本发明各实施例中涉及的安全密钥不管是在网络侧还是用户终端，都是根据设定的计算方法，利用存储的设备密钥、参数信息和用户终端的接入网络标识信息进行计算得到的，网络侧和用户终端具有加密和解密的功能，保证信令传输过程中的安全性，以及使得利用的空口资源得到保护。

下面结合说明书附图对本发明各实施例进行详细描述。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

实施例一

如图 2 所示，为本发明实施例一的一种呼叫认证方法的流程图，所述方法包括如下步骤:

步骤 101、MME 接收用户终端发送的携带了接入网络标识的紧急呼叫请求消息，并将所述接入网络标识携带在查询请求中发送至 HSS。

其中，所述接入网络标识是用户终端的 IMEI。

在步骤 101 中，当用户终端处于呼叫受限或者未插入 SIM 卡/USIM（Universal Subscriber Identity Module，通用用户识别模块）卡，且需要发起紧急呼叫请求时，用户终端将自身 IMEI 作为接入网络标识携带在紧急呼叫请

求消息中发送给 MME。

可选地，MME 在接收到用户发送的紧急呼叫请求消息时，指示用户终端上报接入网络标识，以便于对用户终端的识别。

当 MME 接收到的用户终端上报的接入网络标识是 GUIT 或者 P_TMSI 时，指示用户终端上报用户终端的 IMSI；当 MME 接收到用户终端上报的接入网络标识是 IMSI，指示用户终端上报用户终端的 IMEI。

需要说明的是，当用户终端处于未插入 SIM 卡状态时，是没有 IMSI 的，只能向 MME 提供 IMEI。

可选地，MME 在接收到紧急呼叫请求消息之后，向 HSS 发送查询请求之前，所述方法还包括:

首先，MME 根据用户终端的接入网络标识与紧急呼叫请求次数之间的对应关系，查找所述用户终端在设定时长内向 MME 发送紧急呼叫请求的次数;

其中，MME 自身存在一个用于计算用户终端发出紧急呼叫次数的计数器，每当用户终端发送一次紧急呼叫请求消息，MME 就将针对该用户终端的紧急呼叫次数增加一，并记录时间、以及用户终端的接入网络标识和紧急呼叫次数之间的对应关系;

其次，MME 判断查找到的呼叫请求次数是否大于设定阈值，若是，则拒绝响应用户终端的紧急呼叫请求；若否，则执行向 HSS 发送查询请求的操作;

其中，设定阈值是为了限定单位时间内一个用户终端向 MME 发送紧急呼叫请求的次数，一般根据实际需要确定，这里不做限定。

步骤 102、MME 接收 HSS 返回的携带了验证信息和第一认证数据的查询结果。

其中，所述第一认证数据是 HSS 将查找的安全密钥和随机产生的验证信息进行计算得到的，其中，安全密钥中包含设备密钥，所述设备密钥是 HSS 根据本地存储的接入网络标识与设备密钥之间的对应关系确定。

在步骤 102 中，MME 将接收到的紧急呼叫请求消息中携带的接入网络标识包含在查询请求中发送给 HSS。

HSS 在接收到 MME 发送的查询请求后，执行以下操作步骤:

第一步、根据本地存储的接入网络标识与设备密钥之间的对应关系，确定查询请求中包含的接入网络标识对应的设备密钥。

第二步、利用包含该设备密钥的安全密钥和随机产生的验证信息进行计算得到第一认证数据。

需要说明的是，计算的方式可以是利用设定的算法，也可以是按照 3GPP（the 3rd Generation Partnership Project，第三代合作伙伴项目）协议中的协议规则进行计算，这里不做限定。

第三步、将随机产生的验证信息与得到的第一认证数据作为查询结果发送给 MME。

其中，所述验证信息可以是 3GPP 格式的验证信息，例如，RAND；所述第一认证数据为 device-challenge；所述查询结果为 RAND||device-challenge，还可以是其他形式的信息，根据实际需要进行确定，这里不做限定。

步骤 103、MME 接收用户终端发送的第二认证数据。

其中，所述第二认证数据是用户终端在接收 MME 发送的验证信息后，利用本地存储的安全密钥和所述验证信息进行计算得到的。

在步骤 103 中，MME 接收到 HSS 返回的查询结果，该查询结果中包含了随机验证信息，MME 将该随机验证信息发送给用户终端。

用户终端在接收到该验证信息后，执行以下操作步骤：

第一步、确定自身的 IMEI 对应的设备密钥。

第二步、利用包含确定的设备密钥的安全密钥对接收到的验证信息进行计算得到第二认证数据。

第三步、将得到的第二认证数据发送给 MME。

步骤 104、MME 将所述第一认证数据与所述第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许用户终端接入通信网络。

在步骤 104 中，MME 判断接收到的第一认证数据与第二认证数据是否相同，若相同，则执行认证通过，允许接入网络的操作；若不相同，则执行认证不通过，拒绝接入网络的操作。

步骤 105、在允许用户终端接入通信网络之后，MME 接收到用户终端发送的携带紧急呼叫内容的紧急呼叫消息，其中，所述紧急呼叫内容是用户终端利用安全密钥进行加密后得到的。

为了保证用户终端发送的紧急呼叫消息不被篡改，在用户终端向 MME 发送紧急呼叫消息时，对携带的紧急呼叫内容进行加密操作，这样保证了传输消息的安全性。

步骤 106、MME 将接收到的所述紧急呼叫消息发送给 HSS 进行解析，根据解析结果向用户终端返回响应消息。

由于 HSS 存储了设备密钥，而安全密钥是利用设备密钥确定的，因此，MME 在接收到加密的紧急呼叫消息时，需要通过 HSS 对接收到加密的紧急呼叫消息进行解密操作。

在本发明实施例一的方案中，通过在用户终端本地和 HSS 本地分别存储了用户终端的 IMEI 与设备密钥之间的对应关系，在用户终端向 MME 发送紧急呼叫请求消息时，MME 从 HSS 处获取包含设备密钥的安全密钥，并和随机验证信息进行运算得到的第一认证数据，以及接收到用户终端发送的根据本地存储的安全密钥和接收到的验证消息计算得到的第二认证数据，并将第一认证数据与第二认证数据进行比较，在比较结果相同时，确定认证通过，允许用户终端接入通信网络，这样避免了非法的用户终端利用紧急呼叫方式恶意使用通信网络，提高了紧急呼叫的安全性，保证了通信网络的应用的安全性。

实施例二

如图 3 所示，为本实施例二的一种呼叫认证设备的结构示意图，所述设备包括：第一接收模块 11、第二接收模块 12、第三接收模块 13 和比较模块 14，其中：

第一接收模块 11 设置成：接收用户终端发送的携带了接入网络标识的紧急呼叫请求消息，并将所述接入网络标识携带在查询请求中发送至 HSS;

第二接收模块 12 设置成：接收 HSS 返回的携带了验证信息和第一认证数据的查询结果，其中，所述第一认证数据是 HSS 将查找的安全密钥和产生

的验证信息进行计算得到的，安全密钥中包含了设备密钥，所述设备密钥是HSS根据本地存储的接入网络标识与设备密钥之间的对应关系确定;

第三接收模块13设置成：接收用户终端发送的第二认证数据，其中，所述第二认证数据是用户终端在接收MME发送的验证信息后，利用本地存储的安全密钥对所述验证信息进行计算得到的；以及

比较模块14设置成：将所述第一认证数据与所述第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许用户终端接入通信网络。

可选地，所述设备还包括：第四接收模块15和消息处理模块16，其中：

第四接收模块15设置成：在允许用户终端接入通信网络之后，接收到用户终端发送的携带紧急呼叫内容的紧急呼叫消息，其中，所述紧急呼叫内容是用户终端利用安全密钥进行加密后得到的;

消息处理模块16设置成：将接收到的所述紧急呼叫消息发送给HSS进行解析，根据解析结果向用户终端返回响应消息。

其中，所述紧急呼叫请求消息中携带了用户终端的接入网络标识。

所述设备还包括：呼叫次数确定模块17和呼叫判断模块18，其中：

呼叫次数确定模块17设置成：将所述接入网络标识携带在查询请求中发送至HSS之前，根据用户终端的接入网络标识与紧急呼叫请求次数之间的对应关系，查找所述用户终端在设定时长内发送紧急呼叫请求的次数;

呼叫判断模块18设置成：判断查找到的紧急呼叫请求次数是否大于设定阈值，若是，则拒绝响应用户终端的紧急呼叫请求；若否，则执行将所述接入网络标识携带在查询请求中发送至HSS的操作。

所述比较模块14是设置成以如下方式将所述第一认证数据与所述第二认证数据进行比较：判断接收到的第一认证数据与第二认证数据是否相同，若相同，则执行认证通过，允许接入网络的操作；若不相同，则执行认证不通过，拒绝接入网络的操作。

实施例三

如图4所示，为本实施例三的一种HSS的结构示意图，所述HSS包括：接收模块21、第一认证数据计算模块22和发送模块23，其中：

接收模块 21 设置成：接收 MME 发送的查询请求，其中，所述查询请求中包含了接入网络标识，所述接入网络标识是用户终端向 MME 发送紧急呼叫请求消息时携带的；

第一认证数据计算模块 22 设置成：根据本地存储的接入网络标识与设备密钥之间的对应关系，确定查询请求中包含的接入网络标识对应的设备密钥，并利用包含该设备密钥的安全密钥和随机产生的验证信息进行计算得到第一认证数据；以及

发送模块 23 设置成：将随机产生的验证信息与得到的第一认证数据作为查询结果发送给 MME，使得 MME 将得到的第一认证数据与接收到的用户终端发送的第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许用户终端接入通信网络。

可选地，所述接入网络标识为用户终端的 IMEI；

所述第一认证数据计算模块 22 还设置成：存储用户终端的 IMEI 与设备密钥之间的对应关系。

实施例四：

如图 5 所示，为本实施例四的一种呼叫认证系统的结构图，所述系统包括：MME31、用户终端 32 和 HSS33，其中：

MME31 设置成：接收用户终端 32 发送的紧急呼叫请求消息，并将包含了所述紧急呼叫请求消息中携带的接入网络标识的查询请求发送至 HSS33；接收 HSS33 返回的携带了验证信息和第一认证数据的查询结果，以及用户终端 32 发送的第二认证数据；将所述第一认证数据与所述第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许用户终端 32 接入通信网络；在允许用户终端 32 接入通信网络之后，接收到用户终端 32 发送的携带紧急呼叫内容的紧急呼叫消息，其中，所述紧急呼叫内容是用户终端 32 利用安全密钥进行加密后得到的；以及将接收到的所述紧急呼叫消息发送给 HSS33 进行解析，根据解析结果向用户终端 32 返回响应消息；

用户终端 32 设置成：发送携带了接入网络标识的紧急呼叫请求消息至 MME31；发送第二认证数据至 MME31；以及在允许接入通信网络之后，向

MME31 发送携带紧急呼叫内容的紧急呼叫消息，其中，所述紧急呼叫内容是利用安全密钥进行加密后得到的；以及

HSS33 设置成：接收 MME31 发送的携带了接入网络标识的查询请求，并根据本地存储的接入网络标识与设备密钥之间的对应关系，确定查询请求中包含的接入网络标识对应的设备密钥，并利用包含该设备密钥的安全密钥和随机产生的验证信息进行计算得到第一认证数据发送至 MME31，以及在允许用户终端 32 接入通信网络之后，接收并解析 MME31 发送的携带紧急呼叫内容的紧急呼叫消息。

可选地，所述用户终端 32 还设置成：在用户终端接 32 收到 MME31 发送的验证信息时，利用本地存储的安全密钥对接收到的验证信息进行计算得到第二认证数据。

本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块/单元可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本发明实施例不限制于任何特定形式的硬件和软件的结合。

显然，本领域的技术人员可以对本发明实施例进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明实施例的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

工业实用性

本发明实施例中，通过在用户终端本地和 HSS 本地分别存储了用户终端的 IMEI 与设备密钥之间的对应关系，避免了非法的用户终端利用紧急呼叫方式恶意使用通信网络，提高了紧急呼叫的安全性，保证了通信网络的应用的安全性。

权 利 要 求 书

1、一种呼叫认证方法，包括:

移动管理实体（MME）接收用户终端发送的携带了接入网络标识的紧急呼叫请求消息，并将所述接入网络标识携带在查询请求中发送至归属签约用户服务器（HSS）；

所述 MME 接收所述 HSS 返回的携带了验证信息和第一认证数据的查询结果，其中，所述第一认证数据是所述 HSS 将查找的安全密钥和随机产生的验证信息进行计算得到的；所述安全密钥包含设备密钥；所述设备密钥是所述 HSS 根据本地存储的接入网络标识与设备密钥之间的对应关系确定;

所述 MME 接收所述用户终端发送的第二认证数据，其中，所述第二认证数据是所述用户终端在接收所述 MME 发送的验证信息后，利用本地存储的安全密钥和所述验证信息进行计算得到的；以及

所述 MME 将所述第一认证数据与所述第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许所述用户终端接入通信网络。

2、如权利要求 1 所述的方法，还包括：在允许所述用户终端接入所述通信网络之后，

所述 MME 接收到所述用户终端发送的携带紧急呼叫内容的紧急呼叫消息，其中，所述紧急呼叫内容是所述用户终端利用所述安全密钥进行加密后得到的；以及

所述 MME 将接收到的所述紧急呼叫消息发送给所述 HSS 进行解析，根据解析结果向所述用户终端返回响应消息。

3、如权利要求 1 所述的方法，所述方法还包括：所述 MME 在接收到所述紧急呼叫请求消息之后，向所述 HSS 发送所述查询请求之前，

所述 MME 根据所述用户终端的接入网络标识与紧急呼叫请求次数之间的对应关系，查找所述用户终端在设定时长内向所述 MME 发送紧急呼叫请求的次数;

所述 MME 判断查找到的紧急呼叫请求次数是否大于设定阈值，若是，则拒绝响应所述用户终端的紧急呼叫请求；若否，则执行向所述 HSS 发送所

述查询请求的操作。

4、如权利要求 1 所述的方法，其中，所述 MME 接收用户终端发送的第二认证数据的步骤包括:

所述 MME 接收在所述用户终端接收到所述 MME 发送的验证信息时，利用本地存储的安全密钥对接收到的验证信息进行计算得到的第二认证数据。

5、如权利要求 1~4 任一所述的方法，其中，所述 MME 将所述第一认证数据与所述第二认证数据进行比较的步骤包括:

所述 MME 判断接收到的第一认证数据与第二认证数据是否相同，若相同，则执行认证通过，允许接入网络的操作；若不相同，则执行认证不通过，拒绝接入网络的操作。

6、一种呼叫认证方法，包括:

归属签约用户服务器（HSS）接收移动管理实体（MME）发送的查询请求，其中，所述查询请求中包含了接入网络标识，所述接入网络标识是用户终端向所述 MME 发送紧急呼叫请求消息时携带的;

所述 HSS 根据本地存储的接入网络标识与设备密钥之间的对应关系，确定所述查询请求中包含的接入网络标识对应的设备密钥，并利用包含所述设备密钥的安全密钥和随机产生的验证信息进行计算得到第一认证数据；以及

所述 HSS 将随机产生的验证信息与得到的第一认证数据作为查询结果发送给所述 MME，使得所述 MME 将得到的第一认证数据与接收到的所述用户终端发送的第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许所述用户终端接入通信网络。

7、如权利要求 6 所述的方法，其中，所述接入网络标识为所述用户终端的国际移动设备标识（IMEI）;

所述本地存储的接入网络标识与设备密钥之间的对应关系包括:

所述 HSS 本地存储的所述用户终端的 IMEI 与所述设备密钥之间的对应关系。

8、一种呼叫认证设备，包括:

第一接收模块，其设置成：接收用户终端发送的携带了接入网络标识的紧急呼叫请求消息，并将所述接入网络标识携带在查询请求中发送至归属签约用户服务器（HSS）；

第二接收模块，其设置成：接收所述HSS返回的携带了验证信息和第一认证数据的查询结果，其中，所述第一认证数据是所述HSS将查找的安全密钥和随机产生的验证信息进行计算得到的；所述安全密钥包含设备密钥；所述设备密钥是所述HSS根据本地存储的接入网络标识与设备密钥之间的对应关系确定；

第三接收模块，其设置成：接收所述用户终端发送的第二认证数据，其中，所述第二认证数据是所述用户终端在接收移动管理实体（MME）发送的验证信息后，利用本地存储的安全密钥对所述验证信息进行计算得到的；以及

比较模块，其设置成：将所述第一认证数据与所述第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许所述用户终端接入通信网络。

9、如权利要求8所述的设备，其中，所述设备还包括：

第四接收模块，其设置成：在允许所述用户终端接入所述通信网络之后，接收到所述用户终端发送的携带紧急呼叫内容的紧急呼叫消息，其中，所述紧急呼叫内容是所述用户终端利用所述安全密钥进行加密后得到的；

消息处理模块，其设置成：将接收到的所述紧急呼叫消息发送给所述HSS进行解析，根据解析结果向所述用户终端返回响应消息。

10、如权利要求8所述的设备，其中， 所述紧急呼叫请求消息中携带了所述用户终端的接入网络标识；

所述设备还包括：呼叫次数确定模块和呼叫判断模块，其中：

所述呼叫次数确定模块设置成：将接收到的所述接入网络标识携带在所述查询请求中发送至所述HSS之前，根据所述用户终端的接入网络标识与紧急呼叫请求次数之间的对应关系，查找所述用户终端在设定时长内发送紧急呼叫请求的次数；

所述呼叫判断模块设置成：判断查找到的紧急呼叫请求次数是否大于设

定阈值，若是，则拒绝响应所述用户终端的紧急呼叫请求；若否，则执行将接收到的所述接入网络标识携带在所述查询请求中发送至所述 HSS 的操作。

11、如权利要求 8 所述的设备，其中，所述比较模块是设置成以如下方式将所述第一认证数据与所述第二认证数据进行比较：

判断接收到的所述第一认证数据与所述第二认证数据是否相同，若相同，则执行认证通过，允许接入网络的操作；若不相同，则执行认证不通过，拒绝接入网络的操作。

12、一种归属签约用户服务器（HSS），包括：

接收模块，其设置成：接收移动管理实体（MME）发送的查询请求，其中，所述查询请求中包含了接入网络标识，所述接入网络标识是用户终端向所述 MME 发送紧急呼叫请求消息时携带的；

第一认证数据计算模块，其设置成：根据本地存储的接入网络标识与设备密钥之间的对应关系，确定所述查询请求中包含的接入网络标识对应的设备密钥，并利用包含所述设备密钥的安全密钥和随机产生的验证信息进行计算得到第一认证数据；以及

发送模块，其设置成：将所述随机产生的验证信息与得到的所述第一认证数据作为查询结果发送给所述 MME，使得所述 MME 将得到的所述第一认证数据与接收到的所述用户终端发送的第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许所述用户终端接入通信网络。

13、如权利要求 12 所述的 HSS，其中，所述接入网络标识为所述用户终端的国际移动设备标识（IMEI）；

所述第一认证数据计算模块还设置成：存储所述用户终端的 IMEI 与所述设备密钥之间的对应关系。

14、一种呼叫认证系统，包括：移动管理实体（MME）、用户终端和归属签约用户服务器（HSS）；其中，

所述 MME 设置成：接收用户终端发送的紧急呼叫请求消息，并将包含了所述紧急呼叫请求消息中携带的接入网络标识的查询请求发送至所述 HSS；接收所述 HSS 返回的携带了验证信息和第一认证数据的查询结果，以

及所述用户终端发送的第二认证数据；将所述第一认证数据与所述第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许所述用户终端接入通信网络；在允许所述用户终端接入所述通信网络之后，接收到所述用户终端发送的携带紧急呼叫内容的紧急呼叫消息，其中，所述紧急呼叫内容是所述用户终端利用安全密钥进行加密后得到的；以及将接收到的所述紧急呼叫消息发送给所述 HSS 进行解析，根据解析结果向所述用户终端返回响应消息；

所述用户终端设置成：发送所述携带了接入网络标识的紧急呼叫请求消息至所述 MME；发送所述第二认证数据至所述 MME；以及在允许接入所述通信网络之后，向所述 MME 发送所述携带紧急呼叫内容的紧急呼叫消息，其中，所述紧急呼叫内容是利用所述安全密钥进行加密后得到的；以及

所述 HSS 设置成：接收所述 MME 发送的所述携带了接入网络标识的查询请求，并根据本地存储的接入网络标识与设备密钥之间的对应关系，确定所述查询请求中包含的接入网络标识对应的设备密钥，并利用包含所述设备密钥的安全密钥和随机产生的验证信息进行计算得到所述第一认证数据发送至所述 MME；以及在允许所述用户终端接入所述通信网络之后，接收并解析所述 MME 发送的所述携带紧急呼叫内容的紧急呼叫消息。

15、如权利要求 14 所述的系统，其中，

所述用户终端还设置成：在所述用户终端接收到所述 MME 发送的验证信息时，利用本地存储的安全密钥对接收到的验证信息进行计算得到所述第二认证数据。

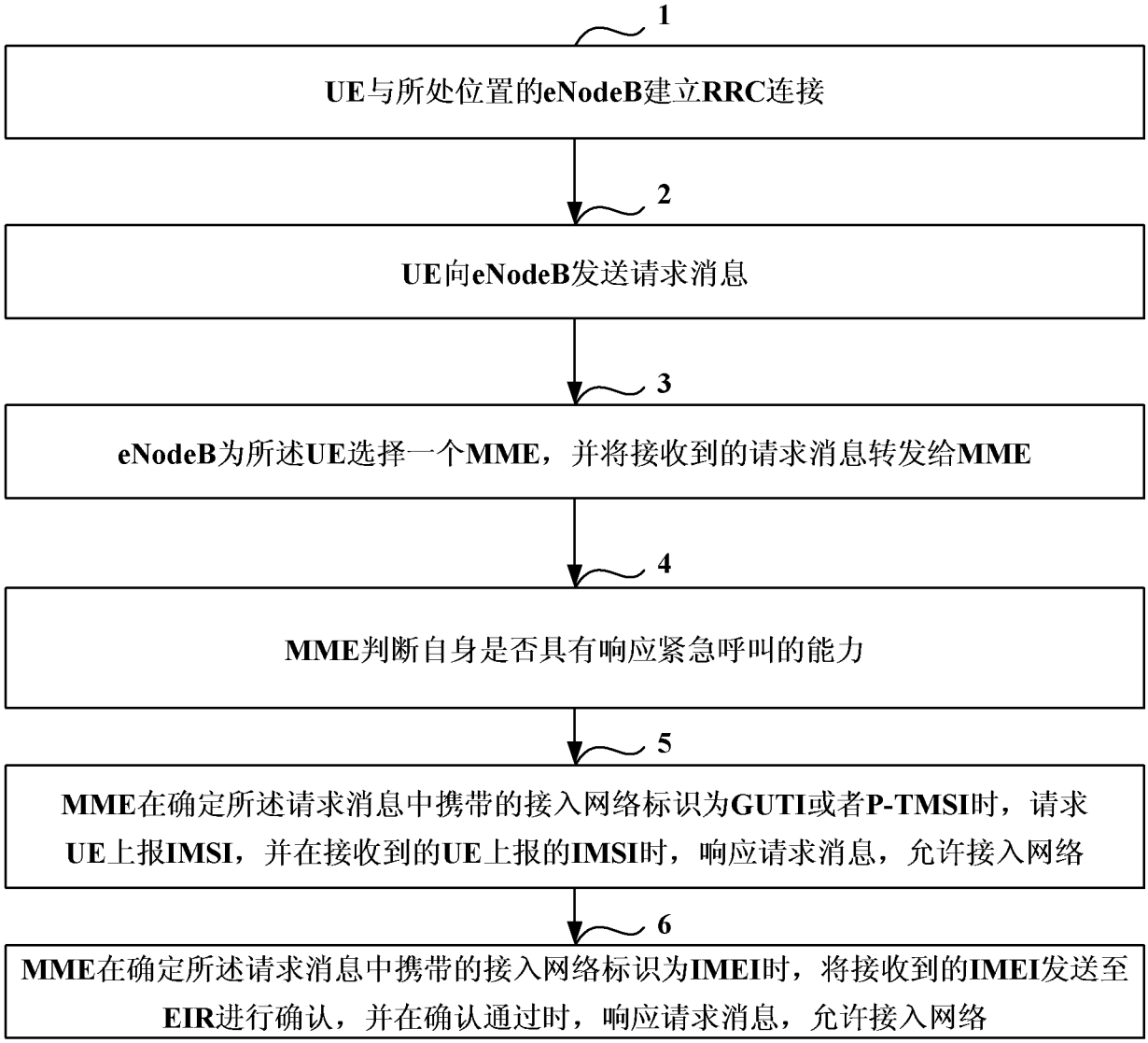
1
UE与所处位置的eNodeB建立RRC连接
2
UE向eNodeB发送请求消息
3
eNodeB为所述UE选择一个MME，并将接收到的请求消息转发给MME
4
MME判断自身是否具有响应紧急呼叫的能力
5
MME在确定所述请求消息中携带的接入网络标识为GUTI或者P-TMSI时，请求UE上报IMSI，并在接收到的UE上报的IMSI时，响应请求消息，允许接入网络
6
MME在确定所述请求消息中携带的接入网络标识为IMEI时，将接收到的IMEI发送至EIR进行确认，并在确认通过时，响应请求消息，允许接入网络

图 1

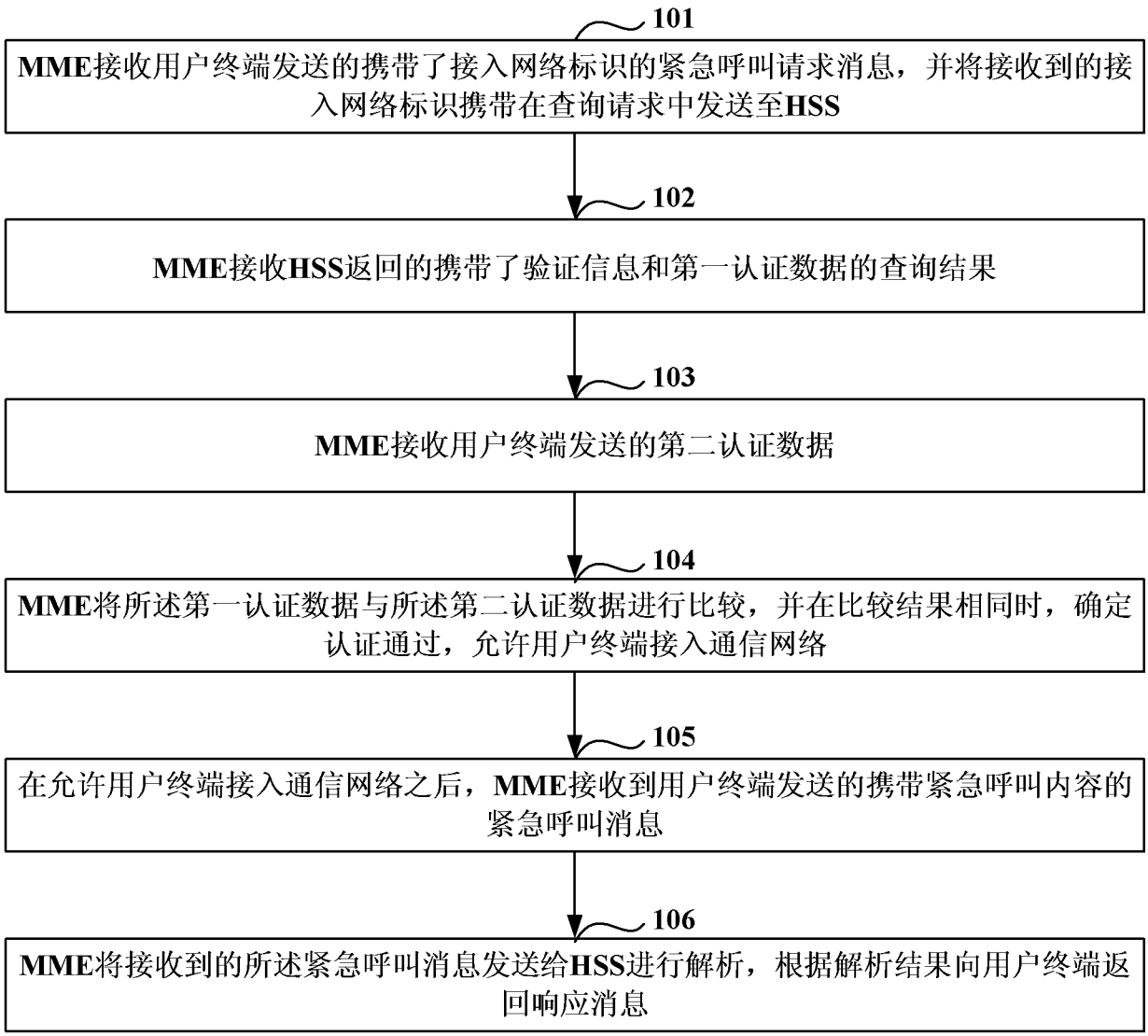
101
MME接收用户终端发送的携带了接入网络标识的紧急呼叫请求消息，并将接收到的接入网络标识携带在查询请求中发送至HSS
102
MME接收HSS返回的携带了验证信息和第一认证数据的查询结果
103
MME接收用户终端发送的第二认证数据
104
MME将所述第一认证数据与所述第二认证数据进行比较，并在比较结果相同时，确定认证通过，允许用户终端接入通信网络
105
在允许用户终端接入通信网络之后，MME接收到用户终端发送的携带紧急呼叫内容的紧急呼叫消息
106
MME将接收到的所述紧急呼叫消息发送给HSS进行解析，根据解析结果向用户终端返回响应消息

图 2

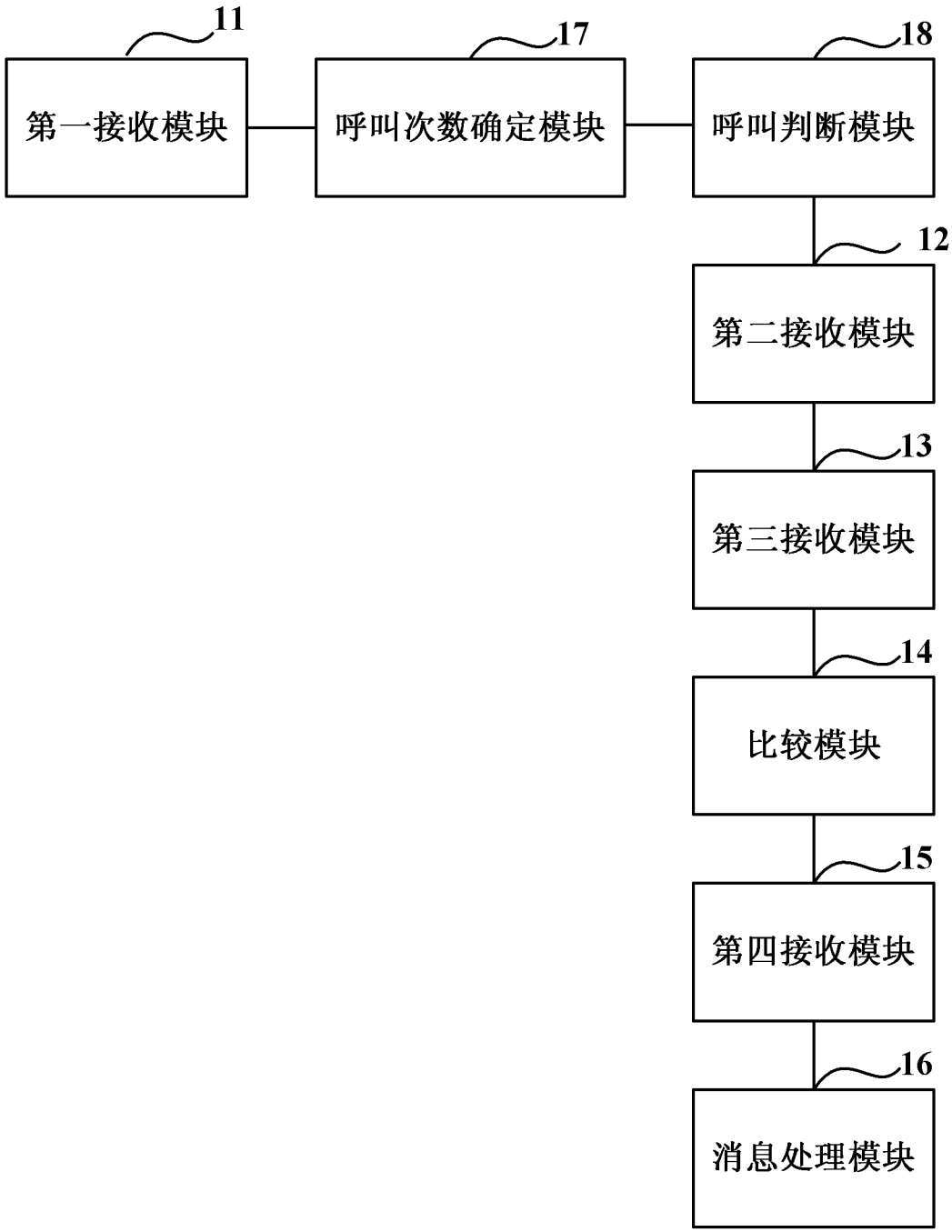
11
第一接收模块
17
呼叫次数确定模块
18
呼叫判断模块
12
第二接收模块
13
第三接收模块
14
比较模块
15
第四接收模块
16
消息处理模块

图 3

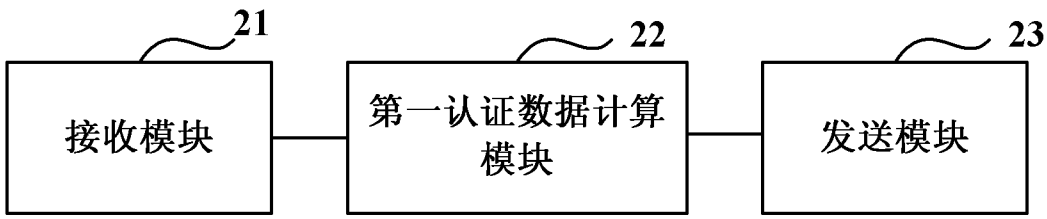
21
接收模块
22
第一认证数据计算模块
23
发送模块

图 4

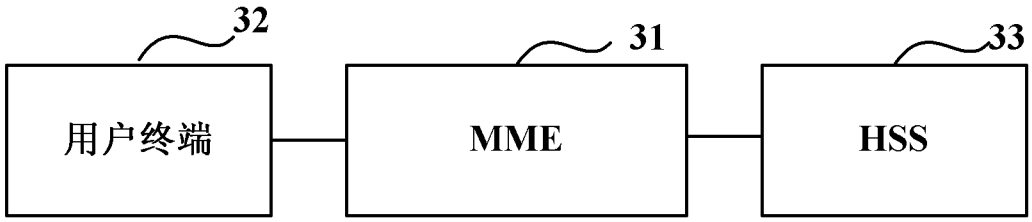

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/080490

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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

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)

CNKI, CNPAT, WPI, EPODOC: emergency, call, authenticat+, second, compare???, MME, HSS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102396203 A (ALCATEL LUCENT USA INC.) 28 March 2012 (28.03.2012) description, paragraphs [0019] to [0075] and figures 1 to 5	1-15
A	CN 102025685 A (HUAWEI TECHNOLOGIES CO., LTD.) 20 April 2011 (20.04.2011) the whole document	1-15
A	CN 102055744 A (ZTE CORP.) 11 May 2011 (11.05.2011) the whole document	1-15
A	US 2007211867 A1 (POLK, James M) 13 September 2007 (13.09.2007) the whole document	1-15

☐ 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
17 October 2013 (17.10.2013)	07 September 2013 (07.09.2013)

Name and mailing address of the ISA	Authorized officer
State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	ZHANG, Jian Telephone No. (86-10) 61648103

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/080490

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102396203 A	28.03.2012	WO 2010120674 A2	21.10.2010
		US 2010266107 A1	21.10.2010
		KR 20110135969 A	20.12.2011
		EP 2420037 A2	22.02.2012
		JP 2012524469 A	11.10.2012
CN 102025685 A	20.04.2011	WO 2011032515 A1	24.03.2011
		US 2011072488 A1	24.03.2011
		EP 2472928 A1	04.07.2012
CN 102055744 A	11.05.2011	None	
US 2007211867 A1	13.09.2007	None	

国际检索报告

国际申请号 **PCT/CN2013/080490**

A. 主题的分类

H04L 29/06 (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

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）)

CNKI, CNPAT, WPI, EPODOC:紧急呼叫, 认证, 第二, 二次, 比较, 移动管理实体,归属签约用户服务器

emergency,call,authenticat+, second, compar???, MME, HSS

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	CN 102396203 A (阿尔卡特朗讯公司) 28.3 月 2012(28.03.2012) 说明书第[0019]段到第[0075]段，附图 1-5	1-15
A	CN 102025685 A (华为技术有限公司) 20.4 月 2011(20.04.2011) 全文	1-15
A	CN 102055744 A (中兴通讯股份有限公司) 11.5 月 2011(11.05.2011) 全文	1-15
A	US 2007211867 A1 (POLK, James M.等)13.9 月 2007(13.09.2007) 全文	1-15

☐ 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
17.10 月 2013(17.10.2013)	**07.11 月 2013 (07.11.2013)**
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 张建 电话号码：(86-10) **61648103**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2013/080490

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 102396203 A	28.03.2012	WO 2010120674 A2	21.10.2010
		US 2010266107 A1	21.10.2010
		KR 20110135969 A	20.12.2011
		EP 2420037 A2	22.02.2012
		JP 2012524469 A	11.10.2012
CN 102025685 A	20.04.2011	WO 2011032515A1	24.03.2011
		US 2011072488 A1	24.03.2011
		EP 2472928A1	04.07.2012
CN 102055744 A	11.05.2011	无	
US 2007211867 A1	13.09.2007	无	