(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
2011 年 10 月 20 日 (20.10.2011)

PCT

(10) 国际公布号
WO 2011/127810 A1

(51) 国际专利分类号:
H04W 12/06 (2009.01)

(21) 国际申请号: PCT/CN2011/072651

(22) 国际申请日: 2011 年 4 月 12 日 (12.04.2011)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201010149674.X 2010 年 4 月 12 日 (12.04.2010) 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总部办公楼, Guangdong 518129 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **张丽佳 (ZHANG, Li-jia)** [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)。 **许怡娴 (XU, Yixian)** [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)。 **黄迎新 (HUANG, Yingxin)** [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)。 **刘晓寒 (LIU, Xiaohan)** [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)。 **劳伦斯·梅里奥 (LAURENCE, Meriau)** [FR/CN]; 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, 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))。

(54) **Title**: METHOD AND APPARATUS FOR AUTHENTICATING COMMUNICATION DEVICES

(54) **发明名称** : 对通信设备进行认证的方法和装置

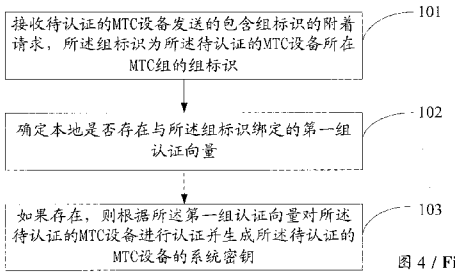

图 4 / **Fig. 4**

101 AN ATTACHING REQUEST, WHICH CONTAINS A GROUP IDENTIFIER AND IS TRANSMITTED BY A MACHINE TYPE COMMUNICATION (MTC) DEVICE TO BE AUTHENTICATED, IS RECEIVED, WHEREIN THE GROUP IDENTIFIER IS THE GROUP IDENTIFIER OF AN MTC GROUP TO WHICH THE MTC DEVICE BELONGS

102 WHETHER A FIRST GROUP OF AUTHENTICATION VECTORS BOUND WITH THE GROUP IDENTIFIER EXISTS IN THE LOCAL IS DETERMINED

103 IF YES, ACCORDING TO THE FIRST GROUP OF AUTHENTICATION VECTORS, THE MTC DEVICE TO BE AUTHENTICATED IS AUTHENTICATED AND A SYSTEM KEY FOR THE MTC DEVICE TO BE AUTHENTICATED IS GENERATED

(57) **Abstract**: A method and an apparatus for authenticating communication devices are disclosed in the embodiments of the present invention. The method includes: an attaching request, which contains a group identifier and is transmitted by a Machine Type Communication (MTC) device to be authenticated, is received, wherein the group identifier is the group identifier of an MTC group to which the MTC device belongs; whether a first group of authentication vectors bound with the group identifier exists in the local is determined, wherein the first group of authentication vectors are the authentication vectors used for authenticating MTC devices of the MTC group; if yes, according to the first group of authentication vectors, the MTC device to be authenticated is authenticated and a system key for the MTC device to be authenticated is generated. The technical solutions provided by the present invention can be applied to the technical field for authenticating MTC devices.

[见续页]

WO 2011/127810 A1

(57) **摘要**:

本发明实施例公开一种对通信设备进行认证的方法和装置，其中，所述方法包括：接收待认证的 MTC 设备发送的包含组标识的附着请求，所述组标识为所述待认证的 MTC 设备所在 MTC 组的组标识；确定本地是否存在与所述组标识绑定的第一组认证向量，所述第一组认证向量为用于认证所述 MTC 组内 MTC 设备的认证向量；如果存在，则根据所述第一组认证向量，对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥。本发明提供的技术方案可以应用在对 MTC 设备进行认证的技术领域中。

对通信设备进行认证的方法和装置

本申请要求于 2010 年 4 月 12 日提交中国专利局、申请号为 201010149674.X、发明名称为“对通信设备进行认证的方法和装置”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

本发明涉及无线通信领域，尤其涉及一种对通信设备进行认证的方法和装置。

背景技术

机器类通信（Machine Type Communication, MTC）设备需要与网络侧进行相互认证后才能与网络侧进行通信。在第三代合作伙伴计划（3rd Generation Partnership Project, 3GPP）标准中对 MTC 设备的分布提出了一种基于组的特性，即一些具有相同地理位置，或者具有相同特性，或者属于相同用户的 MTC 设备可以作为一组。一组 MTC 设备可以直接接入网络，也可以通过网关接入网络。

现有技术中，每个 MTC 设备都有一个国际移动用户身份标识（International Mobile Subscriber Identity, IMSI），这个身份标识 IMSI 是唯一的。在与网络侧进行相互认证的过程中，网络侧根据 MTC 设备唯一的 IMSI 对应的基本密钥 K，生成认证向量（Authentication Vector, AV），根据该 AV 完成 MTC 设备和网络侧之间的相互认证。不同的 MTC 设备利用不同的 IMSI 对应的不同的基本密钥 K，生成不同的认证向量 AV 来完成所述相互认证。

由于 MTC 设备数量巨大，如果采用现有的认证方法，当大量 MTC 设备在短时间内接入网络时，认证过程中产生的信令流量会迅速增大，造成网络拥塞。

发明内容

本发明的实施例提供一种对通信设备进行认证的方法和装置，能够在大量 MTC 设备在短时间内接入网络的情况下，也能对每个 MTC 设备进行有效认证。

为达到上述目的，本发明的实施例采用如下技术方案:

一种对 MTC 设备进行认证的方法，包括:

接收待认证的 MTC 设备发送的包含组标识的附着请求，所述组标识为所述待认证的 MTC 设备所在 MTC 组的组标识;

确定本地是否存在与所述组标识绑定的第一组认证向量;

如果存在，则根据所述第一组认证向量，对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥。

一种对 MTC 设备进行认证的方法，包括:

MTC 组内的主 MTC 设备与网络侧进行认证成功后，

接收所述 MTC 组内第二 MTC 设备发送的附着请求;

对所述第二 MTC 设备进行认证，并使用所述主 MTC 设备与网络侧进行认证过程中产生的组认证向量为所述第二 MTC 设备生成系统密钥;

将所述系统密钥发送给所述第二 MTC 设备。

一种对 MTC 设备进行认证的方法，包括:

MTC 组内的主 MTC 设备向网络侧发送附着请求，其中，所述附着请求中包含所述 MTC 组的组标识和所述 MTC 组内其它待认证的 MTC 设备的设备特征;

所述主 MTC 设备与所述网络侧进行认证，并使用组认证向量和所述其它待认证的 MTC 设备的设备特征为所述其它待认证的 MTC 设备生成系统密钥，其中，所述组认证向量为所述主 MTC 设备与所述网络侧进行认证的过程中产生的;

所述主 MTC 设备对所述其它待认证的 MTC 设备进行认证成功后，将所述系统密钥发送给所述其它待认证的 MTC 设备。

一种网络侧实体，包括:

第一接收单元，用于接收待认证的 MTC 设备发送的包含组标识的附着请求，所述组标识为所述待认证的 MTC 设备所在 MTC 组的组标识;

第一认证单元，当存在与由所述第一接收单元接收的组标识绑定的第一组认证向量时，用于根据所述第一组认证向量，对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥。

一种对 MTC 设备进行认证的设备，包括:

第三接收单元，用于在所述设备与网络侧进行认证成功后，接收所述设备所在的 MTC 组内第二 MTC 设备发送的附着请求;

第四认证单元，用于对所述第二 MTC 设备进行认证，并使用所述设备与网络侧进行认证过程中产生的组认证向量为所述第二 MTC 设备生成系统密钥;

第二发送单元，用于将由所述第四认证单元生成的系统密钥发送给所述第二 MTC 设备。

一种对 MTC 设备进行认证的设备，包括:

第三发送单元，用于向网络侧发送附着请求，其中，所述附着请求中包含所述设备所在 MTC 组的组标识和所述 MTC 组内待认证的 MTC 设备的设备特征;

第五认证单元，用于所述设备与所述网络侧进行相互认证，并使用组认证向量和所述待认证的 MTC 设备的设备特征为所述待认证的 MTC 设备生成系统密钥，其中，所述组认证向量为所述设备与所述网络侧进行认证的过程中产生的;

第四发送单元，在所述设备对所述待认证的 MTC 设备进行认证成功后，用于将由所述第五认证单元生成的系统密钥发送给所述待认证的 MTC

设备。

本发明实施例提供的对MTC设备进行认证的方法和装置，通过一个MTC组所共有的组标识来获取组认证向量，并通过组认证向量对组内待认证的MTC设备进行认证，或者，通过组认证向量为组内认证过的MTC设备生成系统密钥，避免了在认证或者生成系统密钥的过程中，需要为不同的MTC设备生成不同的认证向量的问题，使得信令流量大大减小，即使在大量MTC设备在短时间内接入网络的情况下，也不会造成网络拥塞。本发明的实施例提供的对MTC设备进行认证的方法和装置，在大量MTC设备在短时间内接入网络的情况下，也能够对每个MTC设备进行有效认证。

附图说明

图 1 为基于组的 MTC 设备接入网络的场景一;

图 2 为基于组的 MTC 设备接入网络的场景二;

图 3 为基于组的 MTC 设备接入网络的场景三;

图 4 为本发明实施例一提供的对 MTC 设备进行认证的方法流程图;

图 5 为本发明实施例一应用于 UMTS 网络中的流程示意图;

图 6 为本发明实施例一应用于 LTE 网络中的流程示意图;

图 7 为本发明实施例二提供的对 MTC 设备进行认证的方法流程图;

图 8 为本发明实施例二应用于 UMTS 网络中的流程示意图;

图 9 为本发明实施例二应用于 LTE 网络中的流程示意图;

图 10 为本发明实施例三提供的对 MTC 设备进行认证的方法流程图;

图 11 为本发明实施例三应用于 UMTS 网络中的流程示意图;

图 12 为本发明实施例三应用于 LTE 网络中的流程示意图;

图 13 为本发明实施例四提供的对 MTC 设备进行认证的方法流程图;

图 14 为本发明实施例四应用于 UMTS 网络中的流程示意图;

图 15 为本发明实施例四应用于 LTE 网络中的流程示意图;

图 16 为本发明实施例提供的网络侧实体结构示意图一;

图 17 为本发明实施例提供的网络侧实体结构示意图二;

图 18 为本发明实施例提供的网络侧实体结构示意图三;

图 19 为本发明实施例提供的网络侧实体结构示意图中第一认证单元 1302 的结构示意图;

图 20 为本发明实施例提供的对 MTC 设备进行认证的设备结构示意图一;

图 21 为本发明实施例提供的对 MTC 设备进行认证的设备结构示意图二;

图 22 为本发明实施例提供的对 MTC 设备进行认证的设备中第四认证单元 1402 的结构示意图;

图 23 为本发明实施例提供的对 MTC 设备进行认证的设备结构示意图三;

图 24 为本发明另一个实施例提供的对 MTC 设备进行认证的设备结构示意图;

图25为本发明另一个实施例提供的网络侧实体的结构示意图。

具体实施方式

图 1、图 2 和图 3 所示的是本发明实施例所基于的 MTC 组的三种可能的场景，其中，标号 1 为 MTC 设备，标号 2 为 MTC 网关。在图 1 中，一组 MTC 设备 1 直接接入 3GPP 网络，网络架构中不需要 MTC 网关，每个 MTC 设备需要和网络进行互鉴权后才可以进行通信。在图 2 中，一组 MTC 设备通过 MTC 网关 2 连接到 3GPP 网络，但是网络侧能够识别网关下的每一个 MTC 设备。即从网络侧来看，MTC 网关相当于一个普通的 MTC 设备，具有普通的 MTC 设备所具有的所有功能; 从组内的每一个 MTC 设备来看，MTC 网关提供了组内其它 MTC 设备的外接通道。每个 MTC 设备和 MTC

网关都需要通过认证后才能够与网络侧进行通信。在图 3 中，一组 MTC 设备通过 MTC 网关 2 连接到 3GPP 网络，但是网络侧只能识别 MTC 网关，而不能识别网关下的 MTC 设备。MTC 网关需要和网络进行互鉴权后才可以进行通信。上述 MTC 网关 2 可以为一个具备网关功能的 MTC 设备。

为了解决现有技术中在大量 MTC 设备接入网络的情况下，由于信令流量增加而造成的网络拥塞的问题，本发明实施例提供一种对通信设备进行认证的方法和装置。

如图 4 所示，本发明实施例一提供的对 MTC 设备进行认证的方法，包括:

步骤 101，接收待认证的 MTC 设备发送的包含组标识的附着请求，所述组标识为所述待认证的 MTC 设备所在 MTC 组的组标识;

在本实施例中，所述待认证的 MTC 设备为一个 MTC 组内需要与网络进行通讯的 MTC 设备，在接入网络之前，需要与网络进行相互认证并生成系统密钥。本实施例对每个 MTC 组都设置一个组标识，这个组标识是唯一的，可以用 Group IMSI 来表示，不同的 MTC 组有不同的 Group IMSI。

步骤 102，确定本地是否存在与所述组标识绑定的第一组认证向量;

在本实施例中，所述组认证向量是指用于认证 MTC 组内的 MTC 设备的认证向量，该 MTC 组内的多个待认证的 MTC 设备可共用该组认证向量进行认证。所述第一组认证向量是由 MTC 组内第一个接入网络的 MTC 设备在与网络相互认证过程中产生的，将此第一组认证向量与所述组标识绑定，以便于属于同一个 MTC 组的另一个 MTC 设备需要接入网络时，能快速地找到该组认证向量，而不需要重新生成。上述第一个接入网络的 MTC 设备指：在当前该 MTC 组中没有 MTC 设备接入上述网络的情况下，首个向该网络发送附着请求的 MTC 设备。

步骤 103，如果存在，则根据所述第一组认证向量，对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥。

在本实施例中，所述待认证的 MTC 设备的系统密钥包括网络侧密钥和设备侧密钥。

本发明实施例提供的对 MTC 设备进行认证的方法，通过一个 MTC 组所共有的组标识来获取组认证向量，并通过这个组认证向量对组内待认证的 MTC 设备进行认证并生成系统密钥，避免了在认证和生成系统密钥的过程中，需要为不同的 MTC 设备生成不同的认证向量的问题，使得信令流量大大减小，即使在大量 MTC 设备在短时间内接入网络的情况下，也不会造成网络拥塞。同时，共用一个组标识也解决了由于 MTC 设备数量巨大而造成的 15 位的 IMSI 不够用的问题。本发明的实施例提供的对 MTC 设备进行认证的方法，在大量 MTC 设备在短时间内接入网络的情况下，也能够对每个 MTC 设备进行有效认证。

进一步地，在步骤 102 中，如果确定本地不存在与所述组标识绑定的第一组认证向量，还需要获取该第一组认证向量，具体包括以下步骤：

步骤 1021，根据所述组标识从服务器获取所述第一组认证向量；

在本实施例中，所述服务器为网络侧的特定服务器。例如，在通用移动通信系统（Universal Mobile Telecommunication System, UMTS）网络中，所述服务器为归属位置寄存器（Home Location Register, HLR）；在长期演进(Long Term Evolution, LTE)网络中，所述服务器为归属用户系统（Home Subscriber System, HSS）。

步骤 1022，建立所述组标识和所述获取的第一组认证向量之间的绑定关系；

在本实施例中，建立绑定关系的目的是使得获取到的第一组认证向量能够直接用来对同一个 MTC 组中的其它 MTC 设备进行认证和生成系统密钥，而不需要每次重新获取。

进一步地，步骤 101 中所接收到的附着请求中还可以包含第二设备特征。设备特征能够在 MTC 组内唯一标识该 MTC 组内的 MTC 设备。上述

第二设备特征是用于标识上述待认证的 MTC 设备的参数; 所述第二设备特征可以是所述待认证的 MTC 设备的位置参数, 也可以是其它能够唯一标识所述待认证的 MTC 设备的参数。当附着请求中包含所述第二设备特征时, 在确定本地存在第一组认证向量之后, 还包括以下步骤:

确定所述第二设备特征与本地存储的第一设备特征是否相同, 其中, 所述第一设备特征为 MTC 组内第一个接入网络的 MTC 设备的设备特征, 它与组标识和第一组认证向量共同绑定在一起; 第二设备特征为组内其他 MTC 设备的设备特征。当第二设备特征与本地存储的第一设备特征不相同, 即待认证的 MTC 设备不是所述第一个接入网络的 MTC 设备时, 根据第一组认证向量, 对待认证的 MTC 设备进行认证并生成待认证的 MTC 设备的系统密钥; 当第二设备特征与本地存储的第一设备特征相同, 即待认证的 MTC 设备是所述第一个接入网络的 MTC 设备时, 根据组标识重新获取组认证向量, 并把重新获取的组认证向量称为第二组认证向量, 由于每次获取组认证向量时所用的随机数不一样, 所以第二组认证向量与第一组认证向量也是不一样的。然后, 建立组标识、第二设备特征和获取的第二组认证向量之间的绑定关系, 并根据第二组认证向量和第二设备特征生成的期待响应数, 根据该期待响应数对待认证的 MTC 设备进行认证; 并根据第二组认证向量和第二设备特征生成待认证的 MTC 设备的系统密钥。

为了使本领域技术人员能够更清楚地理解本发明实施例一提供的技术方案, 下面通过具体的应用场景, 对实施例一提供的技术方案进行详细说明。

如图 5 所示, 本发明实施例一提供的对 MTC 设备进行认证的方法, 可以应用于图 1 所示的场景一中。本实施例中, 一组 MTC 设备共同使用一个身份标识 Group IMSI 和该身份标识对应的基本密钥 K; 组内第一个 MTC 设备接入网络时, 和网络之间进行相互认证, 并生成系统密钥; 其它 MTC 设备接入网络时, 重用第一个 MTC 设备所获取的组认证向量与网络进行相

互认证并生成系统密钥。上述第一个 MTC 设备指：在当前该 MTC 组中没有 MTC 设备接入上述网络的情况下，首个向该网络发送附着请求的 MTC 设备。在 UMTS 网络中，该方法包括以下步骤：

步骤 201，第一个 MTC 设备向拜访位置寄存器（Visited Location Register, VLR）发送附着请求，该附着请求中含有组内设备共同的身份标识 Group IMSI、第一个 MTC 设备的设备特征 device position 1、和时间戳 time stamp 1，此时间戳是基于发送所述附着请求的时间生成的。其中，device position 表示每个设备在 MTC 设备组中所处的位置，用来作为每个设备的设备特征。该设备特征可以由拥有这一组 MTC 设备的用户指定，在注册阶段告知运营商，或者，由这一组 MTC 设备中的某个特定设备在注册时告知运营商这一组 MTC 设备的信息，由运营商为每个 MTC 设备分配设备特征。当然，还可以选用其它的特征作为设备特征，此处不一一列举。

步骤 202，VLR 接收到第一个 MTC 设备的附着请求后，检查是否存在此 Group IMSI 和组认证向量的绑定关系，即确认是否存在与此 Group IMSI 绑定的认证向量。

由于是第一个 MTC 设备，所以不存在此绑定关系，需要获取新的组认证向量。

步骤 203，VLR 向归属位置寄存器（Home Location Register, HLR）发送认证向量请求，该请求中含有 Group IMSI;

步骤 204，HLR 根据 Group IMSI 找到对应的基本密钥 K，生成组认证向量 AV=(RAND, XRES, CK, IK, AUTH)，其中，RAND 表示随机数，XRES 表示期待响应数，CK 表示加密密钥，IK 表示完整性密钥，AUTH 表示认证标记。需要说明的是，HLR 可以生成一个 AV，也可以生成一组 AV 发送给 VLR，VLR 可以重复使用一个 AV 或者循环使用一组 AV 对 MTC 设备进行认证;

步骤 205，HLR 将 AV 和预先定义的功能函数 F 发送给 VLR。

需要说明的是，所述功能函数 F 也可以直接配置在 VLR 中，用于后续步骤中计算系统密钥、设备期待响应数等参数。

步骤 206，VLR 存储 AV 和功能函数 F，并将此 AV 和第一个 MTC 设备的设备特征 device position 1、组内设备共同的身份标识 Group IMSI 建立绑定关系；然后，利用功能函数 F 计算第一个 MTC 设备的期待响应数 XRES device 1= F(device position 1, time stamp 1, XRES)，其中，device position 1 为在步骤 202 中接收到的参数，XRES 为组认证向量 AV 中的参数；

步骤 207，VLR 向第一个 MTC 设备发送组认证信息，所述组认证信息是从 AV 中获取的参数，其中含有随机数 RAND 和认证标记 AUTH；

步骤 208，第一个 MTC 设备接收到所述组认证信息后，检查认证标记 AUTH，若正确，则完成所述第一个 MTC 设备对网络侧的认证。并计算出第一个 MTC 设备的响应数 RES device 1=F(device position 1, time stamp 1, RES)、第一个 MTC 设备的加密密钥 CK device 1=F(device position 1, time stamp 1, CK)和第一个 MTC 设备的完整性密钥 IK device 1=F(device position 1, time stamp 1, IK)；

步骤209，第一个MTC设备将含有RES device 1的设备认证信息发送给VLR；

步骤210，VLR检查XRES device 1与接收到的RES device 1是否相等，如果相等，则接受第一个MTC设备的附着请求，完成网络对第一个MTC设备的认证，并计算出网络侧的密钥CK device 1= F(device position 1, time stamp 1, CK)和IK device 1= F(device position 1, time stamp 1, IK)；

步骤211，VLR向第一个MTC设备发送接受其附着请求的消息，完成第一个MTC设备和网络之间的相互认证；

步骤212，第二个MTC设备向VLR发送附着请求，消息中含有device position2、time stamp 2和Group IMSI；

步骤213，VLR收到第二个MTC设备的附着请求后，检查是否存在此

Group-IMSI和AV的绑定关系，如果不存在，则向HLR请求新的AV；如果存在，则检查附着请求中的device position 2是否跟与Group-IMSI、AV的绑定的device position相同，如果不相同，则利用现有的AV对第二个MTC设备进行认证，如果相同，则向HLR请求新的AV。

此步骤中，由于是第二个 MTC 设备，所以不需要申请新的 AV，直接利用第一个 MTC 设备申请的 AV 进行认证，并生成系统密钥。方法与对第一个 MTC 设备认证的方法相同，此处不再赘述。

上述对第二个 MTC 设备的认证方法，仅以第二个接入网络的 MTC 设备为例进行说明，但该方法并不局限于对当前 MTC 组内第二个发送附着请求的 MTC 设备的认证，该方法适用于该 MTC 组内除第一个 MTC 设备外所有后续发送附着请求的 MTC 设备。

需要说明的是，除了时间戳 time stamp 外，也可以使用其它参数，如随机数 RAND 来生成系统密钥。VLR 执行的部分功能（如利用函数 F 计算 XRES device、CK device 和 IK device，以及检查 Group IMSI 和 AV 的绑定关系等）也可以在 HLR 中执行。当第一个接入网络的 MTC 设备关机、而其他 MTC 设备仍需要和网络侧进行通信时，需要 VLR 保存第一个接入网络的 MTC 设备的关机记录，以保证第一个接入网络的 MTC 设备在关机的情况下可以使其他的 MTC 设备获得新的 AV。

如图6所示，上述方法也可以应用在长期演进(Long Term Evolution, LTE)网络中，不同之处在于，UMTS网络中的VLR对应LTE网络中的移动管理实体（Mobility Management Entity, MME）, UMTS网络中的HLR对应LTE网络中的归属用户系统（Home Subscriber System, HSS），该方法包括:

步骤301，第一个MTC设备向MME发送附着请求，该附着请求中含有组内设备共同的身份标识Group IMSI、第一个MTC设备的设备特征device position 1、和时间戳time stamp 1，此时间戳是基于发送所述附着请求的时

间生成的;

步骤 302，MME 接收到第一个 MTC 设备的附着请求后，检查是否存在此 Group IMSI 和认证向量 AV 的绑定关系，即确认是否存在与此 Group IMSI 绑定的认证向量。由于是第一个 MTC 设备，所以不存在此绑定关系，需要获取新的认证向量 AV;

步骤303，MME向归属用户系统（Home Subscriber System, HSS）发送认证向量请求，该请求中含有Group IMSI;

步骤304，HSS根据Group IMSI找到对应的K，生成认证向量AV=(RAND, AUTH, XRES, K_{ASME})，HSS可以生成一个AV，也可以生成一组AV发送给MME，MME可以重复使用一个AV或者循环使用一组AV对MTC设备进行认证;

步骤305，HSS将AV和预先定义的功能函数F发送给MME。需要说明的是，所述功能函数F也可以直接配置在MME中;

步骤306，MME存储AV和功能函数F，并将此AV和第一个MTC设备的设备特征device position 1、组设备共同的身份标识Group IMSI建立绑定关系；然后，利用功能函数F计算第一个MTC设备的期待响应数XRES device 1= F(device position 1, time stamp 1, XRES);

步骤307，MME向第一个MTC设备发送组认证信息，所述组认证信息中含有随机数RAND和认证标记AUTH;

步骤308，第一个MTC设备接收到所述组认证信息后，检查认证标记AUTH，若正确，则完成所述第一个MTC设备对网络侧的认证。并计算出第一个MTC设备的响应数RES device 1=F(device position 1, time stamp 1, RES)和参数K_{ASME} device 1=F(Device position 1, time stamp 1, K_{ASME});

步骤309，第一个MTC设备将含有RES device 1的设备认证信息发送给MME;

步骤310，MME检查XRES device 1与接收到的RES device 1是否相等，

如果相等，则接受第一个MTC设备的附着请求，完成网络对第一个MTC设备的认证，并计算出网络侧K_{ASME} device 1=F(Device position 1, time stamp 1, K_{ASME});

步骤311，MME向第一个MTC设备发送接受其附着请求的消息，完成第一个MTC设备和网络之间的相互认证;

步骤312，第二个MTC设备向MME发送附着请求，消息中含有device position2、time stamp 2和Group IMSI;

步骤313，MME收到第二个MTC设备的附着请求后，检查是否存在此Group-IMSI和AV的绑定关系，如果不存在，则向HSS请求新的AV；如果存在，则检查附着请求中的device position 2是否跟与Group-IMSI、AV的绑定的device position相同，如果不相同，则利用现有的AV对第二个MTC设备进行认证，如果相同，则向HSS请求新的AV。

此步骤中，由于是第二个 MTC 设备，所以不需要申请新的 AV，直接利用第一个 MTC 设备申请的 AV 进行认证，并生成系统密钥。方法与对第一个 MTC 设备认证的方法相同，此处不再赘述。

上述对第二个 MTC 设备的认证方法，仅以第二个接入网络的 MTC 设备为例进行说明，但该方法并不局限于对当前 MTC 组内第二个发送附着请求的 MTC 设备的认证，该方法适用于该 MTC 组内除第一个 MTC 设备外所有后续发送附着请求的 MTC 设备。

需要说明的是，除了时间戳 time stamp 外，也可以使用其它参数，如随机数 RAND 来生成系统密钥。MME 执行的部分功能（如利用函数 F 计算 XRES device、K_{ASME} device 等）也可以在 HSS 中执行。当第一个接入网络的 MTC 设备关机、而其他 MTC 设备仍需要和网络侧进行通信时，需要 MME 保存第一个接入网络的 MTC 设备的关机记录，以保证第一个接入网络的 MTC 设备在关机的情况下可以使其他的 MTC 设备获得新的 AV。

本发明实施例提供的对 MTC 设备进行认证的方法，通过一个 MTC 组

所共有的组标识来获取组认证向量，并通过这个组认证向量对组内待认证的 MTC 设备进行认证并生成系统密钥，避免了在认证和生成系统密钥的过程中，需要为不同的 MTC 设备生成不同的认证向量的问题，使得信令流量大大减小，即使在大量 MTC 设备在短时间内接入网络的情况下，也不会造成网络拥塞。同时，共用一个组标识也解决了由于 MTC 设备数量巨大而造成的 15 位的 IMSI 不够用的问题。本发明的实施例提供的对 MTC 设备进行认证的方法，在大量 MTC 设备在短时间内接入网络的情况下，也能够对每个 MTC 设备进行有效认证。

如图 7 所示，本发明实施例二提供的对 MTC 设备进行认证的方法，包括:

步骤 401，MTC 组内的主 MTC 设备与网络侧进行认证成功后，接收所述 MTC 组内第二 MTC 设备发送的附着请求;

在本实施例中，所述主 MTC 设备可以是一个 MTC 组内的网关，也可以是一个指定的 MTC 设备，由该主 MTC 设备先与网络侧进行相互认证后，再由该主 MTC 设备对组内其它待认证的 MTC 设备进行认证。

步骤 402，对所述第二 MTC 设备进行认证，并使用所述主 MTC 设备与网络侧进行认证过程中产生的组认证向量为所述第二 MTC 设备生成系统密钥;

在本实施例中，所述第二 MTC 设备为组内除了主 MTC 设备以外的任一 MTC 设备；通过重用组认证向量来为第二 MTC 设备生成系统密钥。

步骤 403，将所述系统密钥发送给所述第二 MTC 设备。

本实施例中，系统密钥包括网络侧密钥和设备侧密钥，主 MTC 设备向第二 MTC 设备发送的是第二 MTC 设备的设备侧密钥。

本发明实施例提供的对 MTC 设备进行认证的方法，首先由一个 MTC 组内的主 MTC 设备与网络侧进行相互认证，并利用它们相互认证过程中产

生的组认证向量为组内其它认证通过的 MTC 设备生成系统密钥，避免了现有技术中，需要使用不同的认证向量为不同的 MTC 设备生成系统密钥的问题。本实施例提供的方法，使得信令流量大大减小，即使在大量 MTC 设备在短时间内接入网络的情况下，也不会造成网络拥塞。

进一步地，在组内主 MTC 设备与网络侧进行认证成功之后，将它们在认证过程中生成的组认证向量与组标识建立绑定关系，以便组内其它 MTC 设备要进行认证而向主 MTC 设备发送包含组标识和该 MTC 设备的设备特征（称为第二 MTC 设备的设备特征）的附着请求时，可以快速地根据组标识找到组认证向量，并使用该组认证向量和该 MTC 设备的设备特征为该 MTC 设备生成系统密钥。

为了使本领域技术人员能够更清楚地理解本发明实施例二提供的技术方案，下面通过具体的应用场景，对实施例二提供的技术方案进行详细说明。

如图 8 所示，本发明实施例二提供的对 MTC 设备进行认证的方法，可以应用于图 2 和图 3 所示的场景二和场景三中。本实施例中，一组 MTC 设备共同使用一个身份标识 Group IMSI 和对应的基本密钥 K；组内 MTC 网关接入网络时，和网络之间进行相互认证，并生成系统密钥；MTC 网关负责对组内其它 MTC 设备进行认证，通过重用由 MTC 网关获取的 AV 生成密钥，分配给其他 MTC 设备。在 UMTS 网络中，该方法包括以下步骤：

步骤 501，MTC 网关向 VLR 发送附着请求，该请求中含有组设备共同的身份标识 Group IMSI、MTC 网关的设备特征 device position、和时间戳 time stamp，此时间戳是基于发送所述附着请求的时间生成的；

步骤 502，VLR 向 HLR 发送认证向量 AV 请求，该请求中含有 Group IMSI；

步骤 503，HLR 根据 Group IMSI 找到对应的 K，生成认证向量 AV=(RAND, XRES, CK, IK, AUTH)，其中，RAND 表示随机数，XRES 表

示期待响应数，CK 表示加密密钥，IK 表示完整性密钥，AUTH 表示认证标记;

步骤 504，HLR 将 AV 和预先定义的功能函数 F 发送给 VLR。需要说明的是，所述功能函数 F 也可以直接配置在 VLR 中，用于后续步骤中计算系统密钥、设备期待响应数等参数;

步骤 505，VLR 存储 AV 和功能函数 F，并将此 AV 和 MTC 网关的设备特征 device position、组内设备共同的身份标识 Group IMSI 建立绑定关系；然后，利用功能函数 F 计算 MTC 网关的期待响应数 XRES device = F(device position, time stamp, XRES)，其中，device position 为在步骤 502 中接收到的参数，XRES 为组认证向量 AV 中的参数;

步骤 506，VLR 向 MTC 网关发送组认证信息，所述组认证信息中含有随机数 RAND 和认证标记 AUTH;

步骤 507，MTC 网关接收到所述组认证信息后，检查认证标记 AUTH，若正确，则完成所述 MTC 网关对网络侧的认证。并计算出 MTC 网关的响应数 RES device =F(device position, time stamp, RES)、MTC 网关的加密密钥 CK device =F(device position , time stamp , CK)和 MTC 网关的完整性密钥 IK device =F(device position , time stamp , IK);

步骤508，MTC网关将含有RES device 的设备认证信息发送给VLR;

步骤509，VLR检查XRES device 与接收到的RES device 是否相等，如果相等，则接受MTC网关的附着请求，完成网络对MTC网关的认证，并计算出网络侧的密钥CK device = F(device position , time stamp, CK)和IK device = F(device position , time stamp, IK);

步骤510，VLR向MTC网关发送接受其附着请求的消息，完成MTC网关和网络之间的相互认证;

步骤511，组内其它MTC设备向MTC网关发送附着请求，消息中含有该MTC设备的device position 2、time stamp 2和Group IMSI;

步骤 512，MTC 网关收到组内其它 MTC 设备的附着请求后，对该 MTC 设备进行认证；

步骤 513，如果 MTC 网关对所述 MTC 设备认证通过，则 MTC 网关向 VLR 发送所述 MTC 设备的附着请求，该附着请求中含有 Group IMSI，time stamp2 和 device position 2；

步骤 514，VLR 根据 Group IMSI 找到在步骤 505 中接收的 AV，并计算出网络侧的密钥 CK device 2=F(device position 2, time stamp 2, CK), IK device 2=F(device position 2, time stamp 2, IK)；

步骤 515，MTC 网关根据所述 MTC 设备的设备特征 device position 2 计算出设备侧的密钥 CK device 2=F(device position 2, time stamp 2, CK), IK device 2=F(device position 2, time stamp 2, IK)；

步骤 516，MTC 网关将生成的设备侧密钥 CK device 2 和 IK device 2 分发给所述 MTC 设备。

需要说明的是，上述 MTC 网关也可以是一组 MTC 设备中的主设备，它首先进行认证接入网络。除了时间戳 time stamp 外，也可以使用其它参数，如随机数 RAND 来生成系统密钥。

如图9所示，上述方法也可以应用在LTE网络中，不同之处在于，UMTS网络中的VLR对应LTE网络中的MME, UMTS网络中的HLR对应LTE网络中HSS,具体的实现方法如下所述：

步骤 601，MTC 网关向 MME 发送附着请求，该请求中含有组设备共同的身份标识 Group IMSI、MTC 网关的设备特征 device position、和时间戳 time stamp，此时间戳是基于发送所述附着请求的时间生成的；

步骤 602，MME 向 HSS 发送认证向量 AV 请求，该请求中含有 Group IMSI；

步骤 603，HSS 根据 Group IMSI 找到对应的 K，生成认证向量 AV=(RAND, AUTH, XRES, K_{ASME})；

步骤 604，HSS 将 AV 和预先定义的功能函数 F 发送给 MME;

步骤 605，MME 存储 AV 和功能函数 F，并将此 AV 和 MTC 网关的设备特征 device position、组设备共同的身份标识 Group IMSI 建立绑定关系；然后，利用功能函数 F 计算 MTC 网关的期待响应数 XRES device = F(device position, time stamp, XRES);

步骤 606，MME 向 MTC 网关发送组认证信息，所述组认证信息中含有随机数 RAND 和认证标记 AUTH;

步骤607，MTC网关接收到所述组认证信息后，检查认证标记AUTH，若正确，则完成所述MTC网关对网络侧的认证。并计算出MTC网关的响应数 RES device =F(device position, time stamp, RES) 和参数 K_{ASM} device=F(Device position, time stamp, K_{ASME});

步骤608，MTC网关将含有RES device 的设备认证信息发送给MME;

步骤609，MME检查XRES device 与接收到的RES device 是否相等，如果相等，则接受MTC网关的附着请求，完成网络对MTC网关的认证，并计算出网络侧 K_{ASME} device =F(Device position, time stamp, K_{ASME});

步骤610，MME向MTC网关发送接受其附着请求的消息，完成MTC网关和网络之间的相互认证;

步骤611，组内其它MTC设备向MTC网关发送附着请求，消息中含有该MTC设备的device position 2、time stamp 2和Group IMSI;

步骤612，MTC网关收到组内其它MTC设备的附着请求后，对该MTC设备进行认证;

步骤 613，如果 MTC 网关对所述 MTC 设备认证通过，则 MTC 网关向 MME 发送所述 MTC 设备的附着请求，该附着请求中含有 Group IMSI 和 device position 2;

步骤614，MME根据Group IMSI找到在步骤605中接收的AV，并计算出网络侧的 K_{ASME} device 2 =F(Device position 2, time stamp 2, K_{ASME});

步骤615，MTC网关根据所述MTC设备的设备特征device position 2计算出设备侧的K_{ASME} device 2 =F(Device position 2, time stamp 2, K_{ASME});

步骤616，MTC网关将生成的设备侧的K_{ASME} device 2分发给所述MTC设备。

需要说明的是，上述 MTC 网关也可以是一组 MTC 设备中的主设备，它首先进行认证接入网络。除了时间戳 time stamp 外，也可以使用其它参数，如随机数 RAND 来生成系统密钥。

本发明实施例提供的对 MTC 设备进行认证的方法，首先由一个 MTC 组内的主 MTC 设备与网络侧进行相互认证，并利用它们相互认证过程中产生的组认证向量为组内其它认证通过的 MTC 设备生成系统密钥，避免了现有技术中，需要使用不同的认证向量为不同的 MTC 设备生成系统密钥的问题。本实施例提供的方法，使得信令流量大大减小，即使在大量 MTC 设备在短时间内接入网络的情况下，也不会造成网络拥塞。

如图 10 所示，本发明实施例三提供的对 MTC 设备进行认证的方法，包括:

步骤 701，MTC 组内的主 MTC 设备向网络侧发送附着请求，其中，所述附着请求中包含所述 MTC 组的组标识和所述 MTC 组内其它待认证的 MTC 设备的设备特征;

在本实施例中，MTC 组内其它待认证的 MTC 设备可以为一个或者多个，主 MTC 设备起到了批量处理的作用，不同的 MTC 设备对应相同的组标识和不同的设备特征。在后续生成系统密钥的过程中，针对不同的 MTC 设备会根据各自不同的设备特征生成不同的系统密钥，即保证了系统的安全性，也提高了处理效率。

步骤 702，所述主 MTC 设备与所述网络侧进行认证，并使用组认证向量和所述其它待认证的 MTC 设备的设备特征为所述其它待认证的 MTC 设

备生成系统密钥，其中，所述组认证向量为所述主 MTC 设备与所述网络侧进行认证的过程中产生的；

步骤 703，所述主 MTC 设备对所述其它待认证的 MTC 设备进行认证成功后，将所述系统密钥发送给所述其它待认证的 MTC 设备。

本实施例中，系统密钥包括网络侧密钥和设备侧密钥，主 MTC 设备向待认证的 MTC 设备发送的是它们的设备侧密钥。

本发明实施例提供的对 MTC 设备进行认证的方法，通过一个 MTC 组所共有的组标识来获取组认证向量，并通过这个组认证向量为组内所有待认证的 MTC 设备生成系统密钥，并将生成的系统密钥分发给这些 MTC 设备，避免了现有技术中，需要使用不同的认证向量为不同的 MTC 设备生成系统密钥，从而产生巨大的信令流量的问题。本实施例提供的方法，使得信令流量大大减小，即使在大量 MTC 设备在短时间内接入网络的情况下，也不会造成网络拥塞。同时，共用一个组标识也解决了由于 MTC 设备数量巨大而造成的 15 位的 IMSI 不够用的问题。

为了使本领域技术人员能够更清楚地理解本发明实施例三提供的技术方案，下面通过具体的应用场景，对实施例三提供的技术方案进行详细说明。

如图 11 所示，本发明实施例三提供的对 MTC 设备进行认证的方法，应用于图 2 和图 3 所示的场景二和场景三中。本实施例中，一组 MTC 设备共同使用一个身份标识 Group IMSI 和对应的基本密钥 K；组内 MTC 网关接入网络时，和网络之间进行相互认证，并一次性将组内其它待认证的 MTC 设备的设备特征发送给网络侧，重用认证向量 AV 为组内其它 MTC 设备生成系统密钥；MTC 网关负责对组内其它 MTC 设备进行认证，并给组内其它 MTC 设备分配密钥。在 UMTS 网络中，该方法包括以下步骤：

步骤 801，MTC 网关向 VLR 发送附着请求，该请求中含有组设备共同的身份标识 Group IMSI、时间戳 time stamp 和组内每个 MTC 设备的设备特

征 device position 1，device position 2，device position 3……所述时间戳是基于发送所述附着请求的时间生成的;

步骤 802，VLR 向 HLR 发送认证向量 AV 请求，该请求中含有 Group IMSI 和组内每个 MTC 设备的设备特征 device position 1，device position 2，device position 3……用 device position n 来表示;

步骤 803，HLR 根据 Group IMSI 找到对应的 K，生成认证向量 AV=(RAND, XRES, CK, IK, AUTH)，其中，RAND 表示随机数，XRES 表示期待响应数，CK 表示加密密钥，IK 表示完整性密钥，AUTH 表示认证标记。并利用组内每个设备的设备特征 device position n 计算出每个设备的网络侧加密密钥 CK device n=F(device position n, time stamp, CK)和网络侧完整性密钥 IK device n=F(device position n, time stamp, IK);

步骤 804，HLR 将 AV、预先定义的功能函数 F 和每个 MTC 设备网络侧的加密密钥 CK device 和完整性密钥 IK device 发送给 VLR。当然，所述功能函数 F 也可以直接配置在 VLR 中;

步骤805，VLR存储AV、功能函数F和每个设备网络侧的加密密钥CK device和完整性密钥IK device;

步骤 806，VLR 向 MTC 网关发送组认证信息，所述组认证信息中含有随机数 RAND 和认证标记 AUTH;

步骤807，MTC网关接收到所述组认证信息后，检查认证标记AUTH，若正确，则完成所述MTC网关对网络侧的认证，并计算出响应数RES、加密密钥CK和完整性密钥IK;

步骤808，MTC网关将含有RES的设备认证信息发送给VLR;

步骤809，VLR检查XRES 与接收到的RES是否相等，如果相等，则接受MTC网关的附着请求，完成网络对MTC网关的认证;

步骤810，VLR向MTC网关发送接受其附着请求的消息，完成MTC网关和网络之间的相互认证;

步骤811，MTC网关根据步骤807中计算出的CK、IK和每个MTC设备的设备特征device position n计算出每个MTC设备的加密密钥CK device n=F(device position n, time stamp, CK)，IK device n=F(device position n, time stamp, IK);

步骤812，MTC网关对组内的每个MTC设备进行认证;

步骤813，如果认证成功，MTC网关将在步骤811中计算出的CK device n和IK device n分发给相应的MTC设备。

需要说明的是，上述 MTC 网关也可以是一组 MTC 设备中的主设备，它首先进行认证接入网络。除了时间戳 time stamp 外，也可以使用其它参数，如随机数 RAND 来生成系统密钥。

如图12所示，上述方法也可以应用在LTE网络中，不同之处在于，UMTS网络中的VLR对应LTE网络中的MME, UMTS网络中的HLR对应LTE网络中的HSS,具体的实现方法如下所述:

步骤 901，MTC 网关向 MME 发送附着请求，该请求中含有组设备共同的身份标识 Group IMSI、时间戳 time stamp 和组内每个 MTC 设备的设备特征 device position 1，device position 2，device position 3……所述时间戳是基于发送所述附着请求的时间生成的;

步骤 902，MME 向 HSS 发送认证向量 AV 请求，该请求中含有 Group IMSI 和组内每个 MTC 设备的设备特征 device position 1，device position 2，device position 3……用 device position n 来表示;

步骤 903，HSS 根据 Group IMSI 找到对应的 K，生成认证向量 AV=(RAND, AUTH, XRES, K_{ASME})，并利用组内每个设备的设备特征 device position n 计算出每个设备的网络侧的 K_{ASME} device n= F(Device position n, time stamp, K_{ASME});

步骤 904，HSS 将 AV、预先定义的功能函数 F 和每个 MTC 设备网络侧的 K_{ASME} device 发送给 MME;

步骤 905，MME 存储 AV、功能函数 F 和每个设备网络侧的 K_{ASME} device;

步骤 906，MME 向 MTC 网关发送组认证信息，所述组认证信息中含有随机数 RAND 和认证标记 AUTH;

步骤 907，MTC 网关接收到所述组认证信息后，检查认证标记 AUTH，若正确，则完成所述 MTC 网关对网络侧的认证，并计算出响应数 RES 和设备侧的 K_{ASME}；

步骤 908，MTC 网关将含有 RES 的设备认证信息发送给 MME;

步骤 909，MME 检查 XRES 与接收到的 RES 是否相等，如果相等，则接受 MTC 网关的附着请求，完成网络对 MTC 网关的认证;

步骤 910，MME 向 MTC 网关发送接受其附着请求的消息，完成 MTC 网关和网络之间的相互认证;

步骤 911，MTC 网关根据步骤 907 中计算出的 K_{ASME} 和每个 MTC 设备的设备特征 device position n 计算出每个 MTC 设备的 K_{ASME} device n=F(device position n, time stamp, K_{ASME});

步骤 912，MTC 网关对组内的每个 MTC 设备进行认证;

步骤 913，如果认证成功，MTC 网关将在步骤 911 中计算出的 K_{ASME} device n 分发给相应的 MTC 设备。

需要说明的是，上述 MTC 网关也可以是一组 MTC 设备中的主设备，它首先进行认证接入网络。除了时间戳 time stamp 外，也可以使用其它参数，如随机数 RAND 来生成系统密钥。

本发明实施例提供的对 MTC 设备进行认证的方法，通过一个 MTC 组所共有的组标识来获取组认证向量，并通过这个组认证向量一次性为组内其它待认证的 MTC 设备生成系统密钥，并将生成的系统密钥分发给这些 MTC 设备，避免了现有技术中，需要使用不同的认证向量为不同的 MTC

设备生成系统密钥，从而产生巨大的信令流量的问题。本实施例提供的方法，使得信令流量大大减小，即使在大量 MTC 设备在短时间内接入网络的情况下，也不会造成网络拥塞。同时，共用一个组标识也解决了由于 MTC 设备数量巨大而造成的 15 位的 IMSI 不够用的问题。

如图 13 所示，本发明实施例四提供的对 MTC 设备进行认证的方法，包括:

步骤 1001，接收包含组标识和设备特征的附着请求，所述组标识为待认证的 MTC 设备所在 MTC 组的组标识，所述设备特征为所述待认证的 MTC 设备的设备特征;

步骤 1002，根据所述组标识和所述设备特征获取所述待认证的 MTC 设备的认证向量;

步骤 1003，根据所述认证向量和所述设备特征对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥。

本发明实施例提供的对 MTC 设备进行认证的方法，通过共用一个组标识来获取认证向量，解决了由于 MTC 设备数量巨大而造成的 15 位 IMSI 不够用的问题。同时，针对不同的 MTC 设备就会根据不同的设备特征生成不同的系统密钥，既保证了系统安全性，也提高了处理效率。本发明的实施例提供的对 MTC 设备进行认证的方法，能够在大量 MTC 设备在短时间内接入网络的情况下，也能对每个 MTC 设备进行有效认证。

为了使本领域技术人员能够更清楚地理解本发明实施例四提供的技术方案，下面通过具体的应用场景，对实施例四提供的技术方案进行详细说明。

如图 14 所示，本发明实施例四提供的对 MTC 设备进行认证的方法，可以应用于图 1 所示的场景一中。本实施例中，一组 MTC 设备共同使用一个身份标识 Group IMSI，基于份标识 Group IMSI 和设备特征 device position 对应不同的基本密钥 K; 组内每个 MTC 设备通过 Group IMSI 和设备特征

device position 接入网络，基于不同的 K 对每个 MTC 设备进行认证并生成系统密钥。在 UMTS 网络中，该方法包括以下步骤:

步骤 1101，MTC 设备向 VLR 发送附着请求，该附着请求中含有组设备共同的身份标识 Group IMSI 和该 MTC 设备的设备特征 device position;

步骤 1102，VLR 向 HLR 发送认证向量 AV 请求，该请求中含有 Group IMSI 和 device position;

步骤 1103，HLR 根据 Group IMSI 和 device position 找到对应的基本密钥 K,并利用预先定义的功能函数 F 生成 AV=(RAND, XRES device, CK, IK, AUTH)，其中，XRES device=F(device position, XRES);

步骤 1104，HLR 将 AV 和预先定义的功能函数 F 发送给 VLR。需要说明的是，所述功能函数 F 也可以直接配置在 VLR 中;

步骤 1105，VLR 存储 AV 和功能函数 F;

步骤 1106，VLR 向所述 MTC 设备发送认证信息，所述认证信息中含有随机数 RAND 和认证标记 AUTH;

步骤 1107，所述 MTC 设备接收到所述认证信息后，检查认证标记 AUTH，若正确，则完成对所述 MTC 设备对网络侧的认证。并计算出该 MTC 设备的响应数 RES device =F(device position ， RES)、MTC 设备的加密密钥 CK device =F(device position , CK)和 MTC 设备的完整性密钥 IK device =F(device position , IK);

步骤1108，所述MTC设备将含有RES device 的设备认证信息发送给 VLR;

步骤1109，VLR检查XRES device 与接收到的RES device 是否相等，如果相等，则接受所述MTC设备的附着请求，完成网络对所述MTC设备的认证，并计算出网络侧的密钥CK device = F(device position , CK)和IK device = F(device position , IK);

步骤1110，VLR向所述MTC设备发送接受其附着请求的消息，完成所述

MTC设备和网络之间的相互认证。

如图15所示，上述方法也可以应用在LTE网络中，不同之处在于，UMTS网络中的VLR对应LTE网络中的MME, UMTS网络中的HLR对应LTE网络中的HSS,具体的实现方法如下所述：

步骤1201，MTC设备向MME发送附着请求，该附着请求中含有组设备共同的身份标识Group IMSI和该MTC设备的设备特征device position;

步骤1202，MME向HSS发送认证向量AV请求，该请求中含有Group IMSI和device position;

步骤1203，HSS根据Group IMSI和device position找到对应的基本密钥K，并利用预先定义的功能函数F生成AV=(RAND, AUTH, XRES device, K_{ASME})，其中，XRES device=F(device position, XRES);

步骤1204，HSS将AV和预先定义的功能函数F发送给MME。需要说明的是，所述功能函数F也可以直接配置在MME中；

步骤1205，MME存储AV和功能函数F;

步骤1206，MME向所述MTC设备发送认证信息，所述认证信息中含有随机数RAND和认证标记AUTH;

步骤1207，所述MTC设备接收到所述认证信息后，检查认证标记AUTH，若正确，则完成对所述MTC设备对网络侧的认证。并计算出该MTC设备的响应数RES device =F(device position ，RES)、MTC设备的 K_{ASME} device =F(device position, K_{ASME});

步骤1208，所述MTC设备将含有RES device 的设备认证信息发送给MME;

步骤1209，MME检查XRES device 与接收到的RES device 是否相等，如果相等，则接受所述MTC设备的附着请求，完成网络对所述MTC设备的认证，并计算出网络侧的 K_{ASME} device =F(device position, K_{ASME});

步骤1210，MME向所述MTC设备发送接受其附着请求的消息，完成所述MTC设备和网络之间的相互认证。

本发明实施例提供的对 MTC 设备进行认证的方法，通过共用一个组标识来获取认证向量，解决了由于 MTC 设备数量巨大而造成的 15 位 IMSI 不够用的问题。同时，针对不同的 MTC 设备就会根据不同的设备特征生成不同的系统密钥，既保证了系统安全性，也提高了处理效率。本发明的实施例提供的对 MTC 设备进行认证的方法，能够在大量 MTC 设备在短时间内接入网络的情况下，也能对每个 MTC 设备进行有效认证。

如图 16 所示，本发明实施例还提供一种网络侧实体，包括:

第一接收单元 1301，用于接收待认证的 MTC 设备发送的包含组标识的附着请求，所述组标识为所述待认证的 MTC 设备所在 MTC 组的组标识;

第一认证单元 1302，当存在与由所述第一接收单元 1301 接收的组标识绑定的第一组认证向量时，用于根据所述第一组认证向量，对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥。

进一步地，如图 17 所示，所述网络侧实体还包括:

第一获取单元 1303，当所述第一组认证向量不存在时，用于根据由所述第一接收单元 1301 接收的组标识从服务器获取所述第一组认证向量;

第一建立单元 1304，用于建立由所述第一接收单元 1301 接收的组标识和由所述第一获取单元 1303 获取的第一组认证向量之间的绑定关系;

第二认证单元 1305，用于根据由所述第一获取单元 1303 获取的第一组认证向量对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥。

进一步地，如图 18 所示，所述网络侧实体还包括:

判断单元 1306，当由所述第一接收单元 1301 接收的附着请求中还包括用于标识所述待认证的 MTC 设备的第二设备特征时，用于判断所述第二设备特征与本地存储的第一设备特征是否相同，其中，所述第一设备特征为

与所述组标识和第一组认证向量共同绑定的设备特征。

进一步地，如图 18 所示，所述网络侧实体还包括:

第二获取单元 1307，当所述待认证的 MTC 设备的第二设备特征与本地存储的第一设备特征相同时，用于根据由所述第一接收单元 1301 接收的组标识获取用于认证所述 MTC 组内 MTC 设备的第二组认证向量;

第二建立单元 1308，用于建立由所述第一接收单元 1301 接收的组标识、第二设备特征和由所述第二获取单元 1307 获取的第二组认证向量之间的绑定关系;

第三认证单元 1309，用于根据由所述第二获取单元 1307 获取的第二组认证向量和由所述第一接收单元 1301 接收的第二设备特征生成的期待响应数，根据所述期待响应对所述待认证的 MTC 设备进行认证；并根据由所述第二获取单元 1307 获取的第二组认证向量和由所述第一接收单元 1301 接收的第二设备特征生成所述待认证的 MTC 设备的系统密钥。

如图 19 所示，所述第一认证单元 1302 包括:

第一生成单元 13021，用于根据所述第一组认证向量和由所述第一接收单元 1301 接收的第二设备特征生成期待响应数;

第一发送单元 13022，用于向所述待认证的 MTC 设备发送组认证信息，以使得所述待认证的 MTC 设备根据所述组认证信息对网络进行认证并根据所述第二设备特征生成设备侧密钥，所述组认证信息是所述第一组认证向量中的信息;

第二接收单元 13023，用于接收由所述待认证的 MTC 设备根据所述第二设备特征生成的响应数;

第一认证子单元 13024，用于根据由所述第二接收单元 13023 接收的响应数和由所述第一生成单元 13021 生成的期待响应数对所述待认证的 MTC 设备进行认证;

第二生成单元 13025，用于根据所述第一组认证向量和由所述第一接收

单元 1301 接收的第二设备特征生成网络侧密钥。

以上各个单元的具体实现方法可以参见步骤 201~213 或者步骤 301~313 所述的方法部分，此处不再赘述。

本发明实施例提供的网络侧实体，通过一个 MTC 组所共有的组标识来获取组认证向量，并通过这个组认证向量对组内所有待认证的 MTC 设备进行认证并生成系统密钥，避免了在认证和生成系统密钥的过程中，需要为不同的 MTC 设备生成不同的认证向量的问题，使得信令流量大大减小，即使在大量 MTC 设备在短时间内接入网络的情况下，也不会造成网络拥塞。同时，共用一个组标识也解决了由于 MTC 设备数量巨大而造成的 15 位的 IMSI 不够用的问题。本发明的实施例提供的网络侧实体，在大量 MTC 设备在短时间内接入网络的情况下，也能够对每个 MTC 设备进行有效认证。

如图 20 所示，本发明实施例还提供一种对 MTC 设备进行认证的设备，包括:

第三接收单元 1401，用于在所述设备与网络侧进行认证成功后，接收所述设备所在的 MTC 组内第二 MTC 设备发送的附着请求;

第四认证单元 1402，用于对所述第二 MTC 设备进行认证，并使用所述设备与网络侧进行认证过程中产生的组认证向量为所述第二 MTC 设备生成系统密钥;

第二发送单元 1403，用于将由所述第四认证单元 1402 生成的系统密钥发送给所述第二 MTC 设备。

进一步地，如图 21 所示，所述对 MTC 设备进行认证的设备还包括:

第三建立单元 1404，用于在所述设备与网络侧进行认证成功之后，建立所述组认证向量和所述 MTC 组的组标识之间的绑定关系。

进一步地，如图 22 所示，所述第四认证单元 1402 包括:

第三获取单元 14021，用于获取与由所述第三接收单元 1401 接收的组标识绑定的所述组认证向量;

第三生成单元 14022，用于使用由所述第三获取单元 14021 获取的组认证向量和由所述第三接收单元 1401 接收的第二 MTC 设备的设备特征为所述第二 MTC 设备生成系统密钥。

进一步地，如图 23 所示，所述对 MTC 设备进行认证的设备还包括：

转发单元 1405，用于向所述网络侧转发由所述第三接收单元 1401 接收的附着请求，以使得所述网络侧使用所述组认证向量和所述第二 MTC 设备的设备特征为所述第二 MTC 设备生成所述系统密钥。

以上各单元的具体实现方式可以参见步骤 501~516 或者步骤 601~616 所述的方法部分，此处不再赘述。

本发明实施例提供的对 MTC 设备进行认证的设备，首先由一个 MTC 组内的主 MTC 设备与网络侧进行相互认证，并利用它们相互认证过程中产生的组认证向量为组内其它认证通过的 MTC 设备生成系统密钥，避免了现有技术中，需要使用不同的认证向量为不同的 MTC 设备生成系统密钥的问题。本实施例提供的设备，使得信令流量大大减小，即使在大量 MTC 设备在短时间内接入网络的情况下，也不会造成网络拥塞。

如图 24 所示，本发明实施例还提供一种对 MTC 设备进行认证的设备，包括：

第三发送单元 1501，用于向网络侧发送附着请求，其中，所述附着请求中包含所述设备所在 MTC 组的组标识和所述 MTC 组内待认证的 MTC 设备的设备特征；

第五认证单元 1502，用于所述设备与所述网络侧进行相互认证，并使用组认证向量和所述待认证的 MTC 设备的设备特征为所述待认证的 MTC 设备生成系统密钥，其中，所述组认证向量为所述设备与所述网络侧进行认证的过程中产生的；

第四发送单元 1503，在所述设备对所述待认证的 MTC 设备进行认证成功后，用于将由所述第五认证单元 1502 生成的系统密钥发送给所述待认

证的 MTC 设备。

进一步地，所述对 MTC 设备进行认证的设备还包括:

第四生成单元 1504，用于当由所述第三发送单元 1501 发送的附着请求中包含所述设备的设备特征时，根据所述设备的设备特征生成所述设备的系统密钥。

以上各单元的具体实现方式可以参见步骤 801~813 或者步骤 901~913 所述的方法部分，此处不再赘述。

本发明实施例提供的对 MTC 设备进行认证的设备，通过一个 MTC 组所共有的组标识来获取组认证向量，并通过这个组认证向量为组内所有待认证的 MTC 设备生成系统密钥，并将生成的系统密钥分发给这些 MTC 设备，避免了现有技术中，需要使用不同的认证向量为不同的 MTC 设备生成系统密钥，从而产生巨大的信令流量的问题。本实施例提供的设备，使得信令流量大大减小，即使在大量 MTC 设备在短时间内接入网络的情况下，也不会造成网络拥塞。同时，共用一个组标识也解决了由于 MTC 设备数量巨大而造成的 15 位的 IMSI 不够用的问题。

如图 25 所示，本发明实施例还提供一种网络侧实体，包括:

第四接收单元 1601，用于接收包含组标识和设备特征的附着请求，所述组标识为待认证的 MTC 设备所在 MTC 组的组标识，所述设备特征为所述待认证的 MTC 设备的设备特征;

第四获取单元 1602，用于根据由所述第四接收单元 1601 接收的组标识和所述设备特征获取所述待认证的 MTC 设备的认证向量;

第六认证单元 1603，用于根据由所述第四获取单元 1602 获取的认证向量和由所述第四接收单元接收 1601 接收的设备特征对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥。

以上各单元的具体实现方式可以参见步骤 1101~1110 或者步骤 1201~1210 所述的方法部分，此处不再赘述。

本发明实施例提供网络侧实体，通过共用一个组标识来获取认证向量，解决了由于 MTC 设备数量巨大而造成的 15 位 IMSI 不够用的问题。同时，针对不同的 MTC 设备就会根据不同的设备特征生成不同的系统密钥，既保证了系统安全性，也提高了处理效率。本发明的实施例提供网络侧实体，能够在大量 MTC 设备在短时间内接入网络的情况下，也能对每个 MTC 设备进行有效认证。

本发明提供的技术方案可以应用在对 MTC 设备进行认证的技术领域中。

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步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于计算机可读存储介质中，如 ROM/RAM、磁碟或光盘等。

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所述以权利要求的保护范围为准。

权利要求

1、一种对机器类通信 MTC 设备进行认证的方法，其特征在于，包括:

接收待认证的 MTC 设备发送的包含组标识的附着请求，所述组标识为所述待认证的 MTC 设备所在 MTC 组的组标识;

确定本地是否存在与所述组标识绑定的第一组认证向量，所述第一组认证向量为用于认证所述 MTC 组内 MTC 设备的认证向量;

如果存在与所述组标识绑定的第一组认证向量，则根据所述第一组认证向量，对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥。

2、根据权利要求 1 所述的方法，其特征在于，所述方法还包括:

如果所述第一组认证向量不存在，则

根据所述组标识从服务器获取所述第一组认证向量;

建立所述组标识和所述获取的第一组认证向量之间的绑定关系;

根据所述第一组认证向量，对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥。

3、根据权利要求 2 所述的方法，其特征在于，

所述方法应用于通用移动通信系统 UMTS 网络中，所述方法由所述 UMTS 网络中的拜访位置寄存器 VLR 执行，所述服务器为所述 UMTS 网络中的归属位置寄存器 HLR; 或者，

所述方法应用于长期演进 LTE 网络中，所述方法由所述 LTE 网络中的移动管理实体 MME 执行，所述服务器为所述 LTE 网络中的归属用户系统 HSS。

4、根据权利要求 1-3 中任意一项所述的方法，其特征在于，所述 MTC 组内的每个 MTC 设备具有设备特征，所述设备特征用于在 MTC 组内唯一标识所述 MTC 设备;

所述附着请求中还包括用于标识所述待认证的 MTC 设备的第二设备特征;

所述确定本地存在与所述组标识绑定的第一组认证向量之后，还包括:

确定所述第二设备特征与本地存储的第一设备特征是否相同，其中，所述第一设备特征为与所述组标识和第一组认证向量共同绑定的设备特征;

如果所述第二设备特征与本地存储的第一设备特征不相同，则执行所述根据所述第一组认证向量对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥的步骤。

5、根据权利要求 4 所述的方法，其特征在于，所述方法还包括:

如果所述待认证的 MTC 设备的第二设备特征与本地存储的第一设备特征相同，则

根据所述组标识获取用于认证所述 MTC 组内 MTC 设备的第二组认证向量;

建立所述组标识、所述第二设备特征和所述获取的第二组认证向量之间的绑定关系;

根据由所述获取的第二组认证向量和所述第二设备特征生成的期待响应数对所述待认证的 MTC 设备进行认证，并生成所述待认证的 MTC 设备的系统密钥。

6、根据权利要求 4 或 5 所述的方法，其特征在于，所述根据所述第一组认证向量,对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥，包括:

根据所述第一组认证向量和所述第二设备特征生成期待响应数;

向所述待认证的 MTC 设备发送组认证信息,以使得所述待认证的 MTC 设备根据所述组认证信息对网络进行认证并根据所述第二设备特征生成设备侧密钥，所述组认证信息是所述第一组认证向量中的信息;

接收由所述待认证的 MTC 设备根据所述第二设备特征生成的响应数;

根据所述响应数和所述期待响应数对所述待认证的 MTC 设备进行认证;

根据所述第一组认证向量和所述第二设备特征生成网络侧密钥。

7、一种对 MTC 设备进行认证的方法，其特征在于，包括:

MTC 组内的主 MTC 设备与网络侧进行认证成功后，接收所述 MTC 组内第二 MTC 设备发送的附着请求，其中，所述主 MTC 设备与网络侧进行认证过程中产生的认证向量作为所述 MTC 组的组认证向量;

所述主 MTC 设备对所述第二 MTC 设备进行认证，并使用所述组认证向量为所述第二 MTC 设备生成系统密钥;

所述主 MTC 设备将所述系统密钥发送给所述第二 MTC 设备。

8、根据权利要求 7 所述的方法，其特征在于，MTC 组内的主 MTC 设备与网络侧进行认证成功后，还包括:

建立所述组认证向量和所述 MTC 组的组标识之间的绑定关系;

所述接收第二 MTC 设备发送的附着请求，包括:

接收所述第二 MTC 设备发送的包含所述组标识和所述第二 MTC 设备的设备特征的附着请求;

所述使用所述主 MTC 设备与网络侧进行认证过程中产生的组认证向量为所述第二 MTC 设备生成系统密钥，包括:

获取与所述附着请求中携带的组标识绑定的所述组认证向量;

使用所述组认证向量和所述第二 MTC 设备的设备特征为所述第二 MTC 设备生成系统密钥。

9、根据权利要求 8 所述的方法，其特征在于，所述接收所述第二 MTC 设备发送的包含所述组标识和所述第二 MTC 设备的设备特征的附着请求之后，还包括:

向所述网络侧转发所述附着请求，以使得所述网络侧使用所述组认证

向量和所述第二 MTC 设备的设备特征为所述第二 MTC 设备生成所述系统密钥。

10、一种对 MTC 设备进行认证的方法，其特征在于，包括:

MTC 组内的主 MTC 设备向网络侧发送附着请求，其中，所述附着请求中包含所述 MTC 组的组标识和所述 MTC 组内其它待认证的 MTC 设备的设备特征;

所述主 MTC 设备与所述网络侧进行认证，并使用所述认证过程中产生的组认证向量和所述其它待认证的 MTC 设备的设备特征为所述其它待认证的 MTC 设备生成系统密钥;

所述主 MTC 设备对所述其它待认证的 MTC 设备进行认证成功后，将所述系统密钥发送给所述其它待认证的 MTC 设备。

11、根据权利要求 10 所述的方法，其特征在于，所述附着请求中还包含所述主 MTC 设备的设备特征;

所述主 MTC 设备与所述网络侧进行认证，包括:

所述主 MTC 设备根据所述主 MTC 设备的设备特征与所述网络侧进行认证，并生成所述主 MTC 设备的系统密钥。

12、一种网络侧实体，其特征在于，包括:

第一接收单元，用于接收待认证的 MTC 设备发送的包含组标识的附着请求，所述组标识为所述待认证的 MTC 设备所在 MTC 组的组标识;

第一认证单元，当存在与由所述第一接收单元接收的组标识绑定的第一组认证向量时，用于根据所述第一组认证向量，对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥。

13、根据权利要求 12 所述的网络侧实体，其特征在于，所述实体还包括:

第一获取单元，当所述第一组认证向量不存在时，用于根据由所述第一接收单元接收的组标识从服务器获取所述第一组认证向量;

第一建立单元，用于建立由所述第一接收单元接收的组标识和由所述第一获取单元获取的第一组认证向量之间的绑定关系；

第二认证单元，用于根据由所述第一获取单元获取的第一组认证向量对所述待认证的 MTC 设备进行认证并生成所述待认证的 MTC 设备的系统密钥。

14、根据权利要求 12 或 13 所述的网络侧实体，其特征在于，所述实体还包括：

判断单元，当由所述第一接收单元接收的附着请求中还包括用于标识所述待认证的 MTC 设备的第二设备特征时，用于判断所述第二设备特征与本地存储的第一设备特征是否相同，其中，所述第一设备特征为与所述组标识和第一组认证向量共同绑定的设备特征。

15、根据权利要求 14 所述的网络侧实体，其特征在于，所述实体还包括：

第二获取单元，当所述待认证的 MTC 设备的第二设备特征与本地存储的第一设备特征相同时，用于根据由所述第一接收单元接收的组标识获取用于认证所述 MTC 组内 MTC 设备的第二组认证向量；

第二建立单元，用于建立由所述第一接收单元接收的组标识、第二设备特征和由所述第二获取单元获取的第二组认证向量之间的绑定关系；

第三认证单元，用于根据由所述第二获取单元获取的第二组认证向量和由所述第一接收单元接收的第二设备特征生成的期待响应数，根据所述期待响应数对所述待认证的 MTC 设备进行认证；生成所述待认证的 MTC 设备的系统密钥。

16、根据权利要求 14 或 15 所述的网络侧实体，其特征在于，所述第一认证单元包括：

第一生成单元，用于根据所述第一组认证向量和由所述第一接收单元接收的第二设备特征生成期待响应数；

第一发送单元，用于向所述待认证的 MTC 设备发送组认证信息，以使得所述待认证的 MTC 设备根据所述组认证信息对网络进行认证并根据所述第二设备特征生成设备侧密钥，所述组认证信息是所述第一组认证向量中的信息；

第二接收单元，用于接收由所述待认证的 MTC 设备根据所述第二设备特征生成的响应数；

第一认证子单元，用于根据由所述第二接收单元接收的响应数和由所述第一生成单元生成的期待响应数对所述待认证的 MTC 设备进行认证；

第二生成单元，用于根据所述第一组认证向量和由所述第一接收单元接收的第二设备特征生成网络侧密钥。

17、根据权利要求 12-16 中任意一项所述的网络侧实体，其特征在于所述网络侧实体为通用移动通信系统 UMTS 网络中的拜访位置寄存器 VLR，或者长期演进 LTE 网络中的移动管理实体 MME。

18、一种对 MTC 设备进行认证的设备，其特征在于，包括：

第三接收单元，用于在所述设备与网络侧进行认证成功后，接收所述设备所在的 MTC 组内第二 MTC 设备发送的附着请求；

第四认证单元，用于对所述第二 MTC 设备进行认证，并使用所述设备与网络侧进行认证过程中产生的组认证向量为所述第二 MTC 设备生成系统密钥；

第二发送单元，用于将由所述第四认证单元生成的系统密钥发送给所述第二 MTC 设备。

19、根据权利要求 18 所述的设备，其特征在于，所述设备还包括：

第三建立单元，用于在所述设备与网络侧进行认证成功之后，建立所述组认证向量和所述 MTC 组的组标识之间的绑定关系。

20、根据权利要求 19 所述的设备，其特征在于，当所述第三接收单元接收的附着请求中包含所述组标识和所述第二 MTC 设备的设备特征时，所

述第四认证单元包括:

第三获取单元，用于获取与由所述第三接收单元接收的组标识绑定的所述组认证向量;

第三生成单元，用于使用由所述第三获取单元获取的组认证向量和由所述第三接收单元接收的第二 MTC 设备的设备特征为所述第二 MTC 设备生成系统密钥。

21、根据权利要求 20 所述的设备，其特征在于，所述设备还包括:

转发单元，用于向所述网络侧转发由所述第三接收单元接收的附着请求，以使得所述网络侧使用所述组认证向量和所述第二 MTC 设备的设备特征为所述第二 MTC 设备生成所述系统密钥。

22、一种对 MTC 设备进行认证的设备，其特征在于，包括:

第三发送单元，用于向网络侧发送附着请求，其中，所述附着请求中包含所述设备所在 MTC 组的组标识和所述 MTC 组内待认证的 MTC 设备的设备特征;

第五认证单元，用于所述设备与所述网络侧进行相互认证，并使用组认证向量和所述待认证的 MTC 设备的设备特征为所述待认证的 MTC 设备生成系统密钥，其中，所述组认证向量为所述设备与所述网络侧进行认证的过程中产生的;

第四发送单元，在所述设备对所述待认证的 MTC 设备进行认证成功后，用于将由所述第五认证单元生成的系统密钥发送给所述待认证的 MTC 设备。

23、根据权利要求 22 所述的设备，其特征在于，所述设备还包括:

第四生成单元，用于当由所述第三发送单元发送的附着请求中包含所述设备的设备特征时，根据所述设备的设备特征生成所述设备的系统密钥。

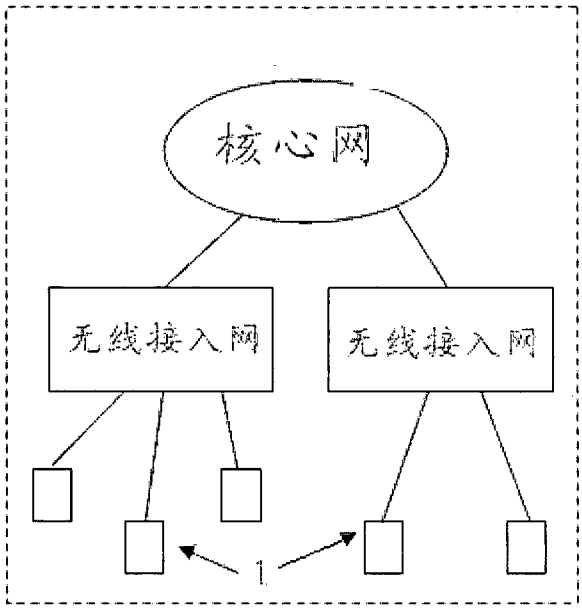

图 1

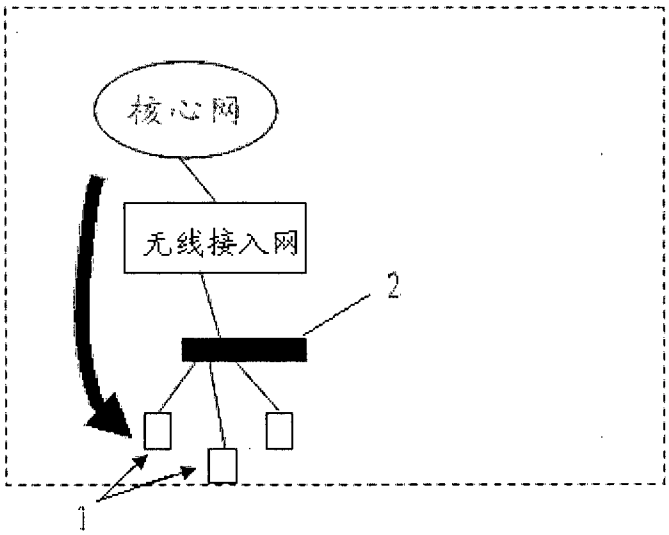

图 2

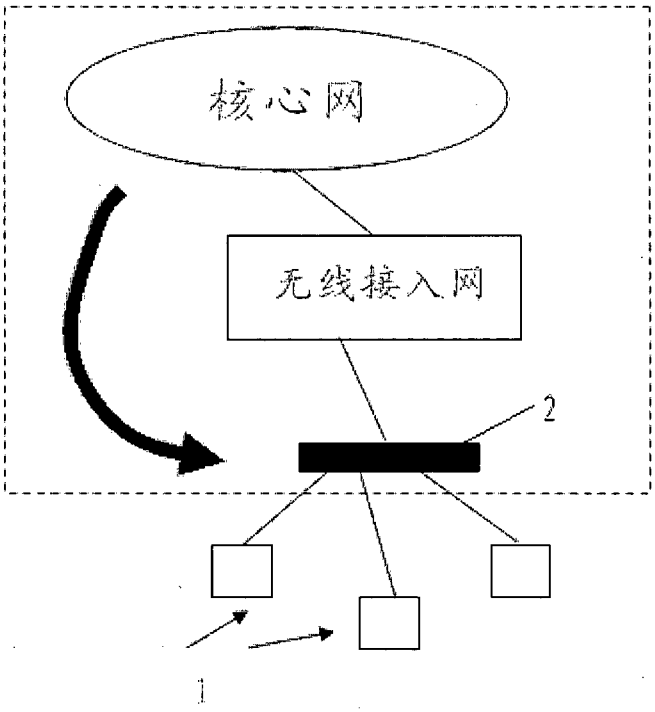
核心网
无线接入网
2
1

图 3

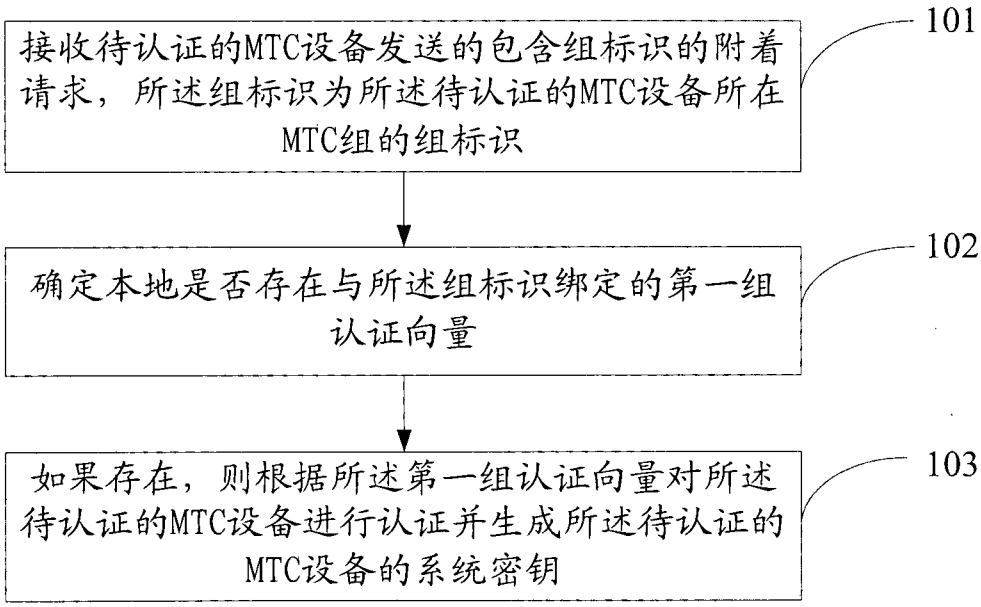
接收待认证的MTC设备发送的包含组标识的附着请求，所述组标识为所述待认证的MTC设备所在MTC组的组标识
101
确定本地是否存在与所述组标识绑定的第一组认证向量
102
如果存在，则根据所述第一组认证向量对所述待认证的MTC设备进行认证并生成所述待认证的MTC设备的系统密钥
103

图 4

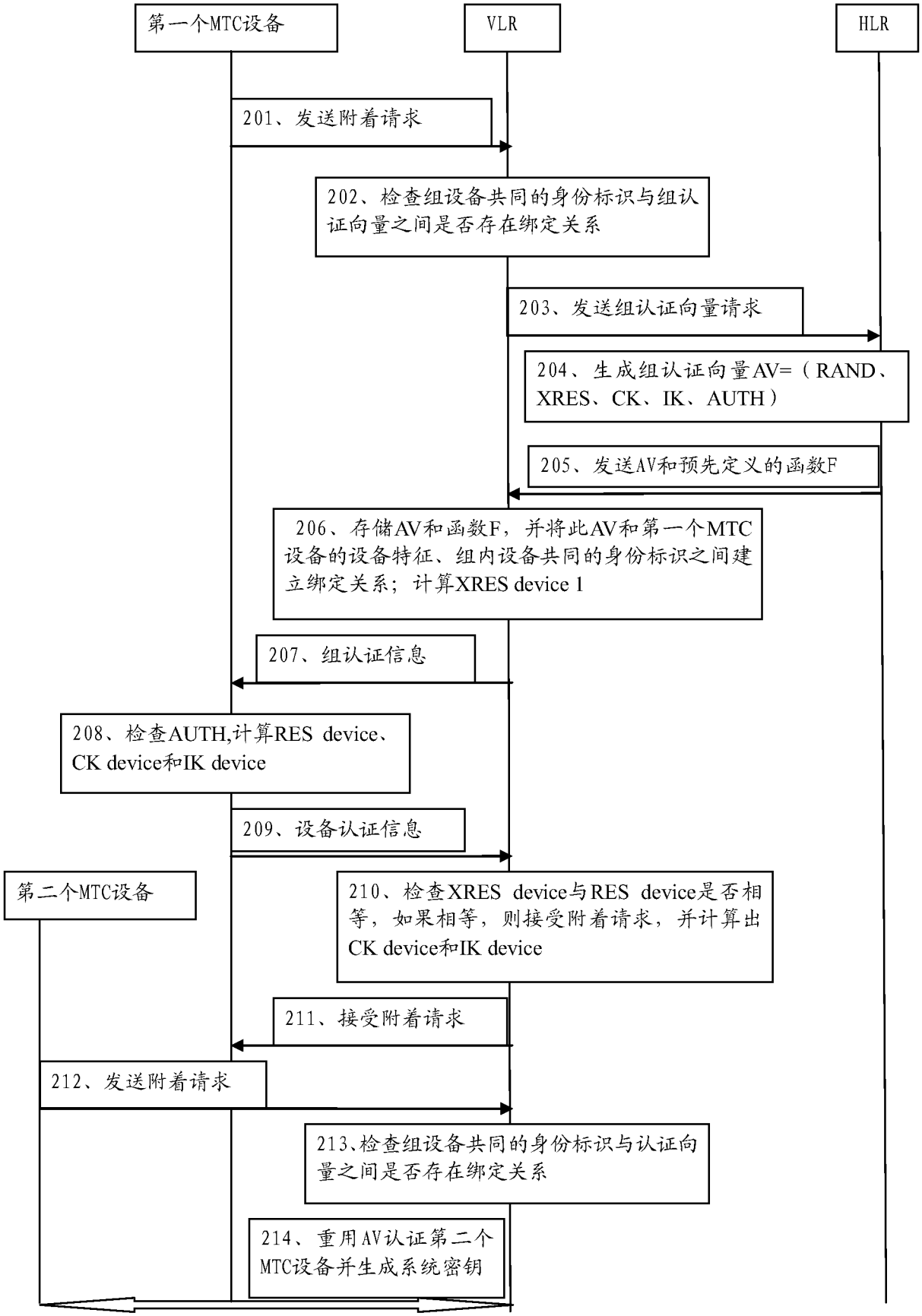
第一个MTC设备
VLR
HLR
201、发送附着请求
202、检查组设备共同的身份标识与组认证向量之间是否存在绑定关系
203、发送组认证向量请求
204、生成组认证向量AV=（RAND、XRES、CK、IK、AUTH）
205、发送AV和预先定义的函数F
206、存储AV和函数F，并将此AV和第一个MTC设备的设备特征、组内设备共同的身份标识之间建立绑定关系；计算XRES device 1
207、组认证信息
208、检查AUTH,计算RES device、CK device和IK device
209、设备认证信息
第二个MTC设备
210、检查XRES device与RES device是否相等，如果相等，则接受附着请求，并计算出CK device和IK device
211、接受附着请求
212、发送附着请求
213、检查组设备共同的身份标识与认证向量之间是否存在绑定关系
214、重用AV认证第二个MTC设备并生成系统密钥

图 5

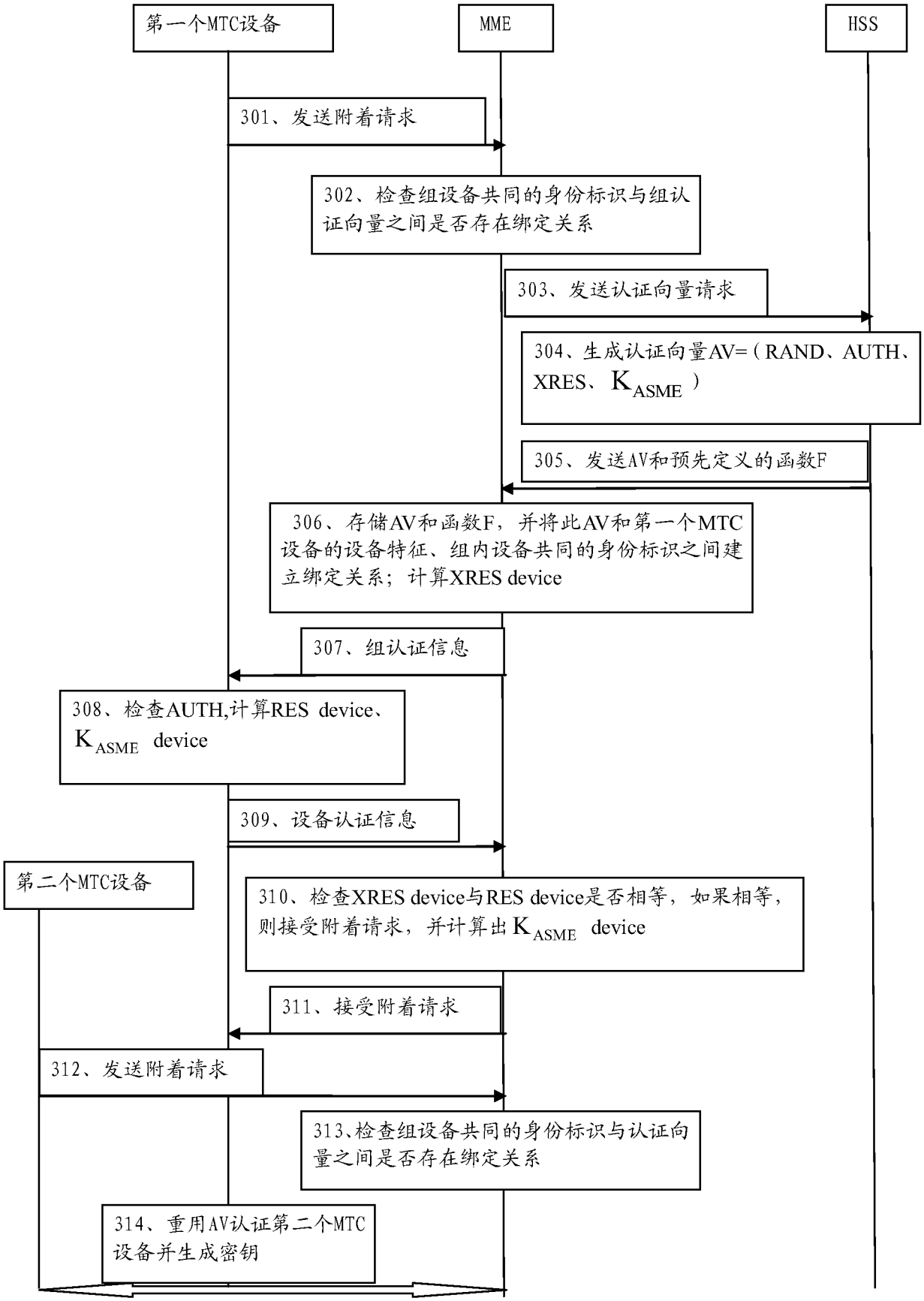
第一个MTC设备
MME
HSS
301、发送附着请求
302、检查组设备共同的身份标识与组认证向量之间是否存在绑定关系
303、发送认证向量请求
304、生成认证向量AV=（RAND、AUTH、XRES、K_{ASME}）
305、发送AV和预先定义的函数F
306、存储AV和函数F，并将此AV和第一个MTC设备的设备特征、组内设备共同的身份标识之间建立绑定关系；计算XRES device
307、组认证信息
308、检查AUTH,计算RES device、K_{ASME} device
309、设备认证信息
第二个MTC设备
310、检查XRES device与RES device是否相等，如果相等，则接受附着请求，并计算出K_{ASME} device
311、接受附着请求
312、发送附着请求
313、检查组设备共同的身份标识与认证向量之间是否存在绑定关系
314、重用AV认证第二个MTC设备并生成密钥

图 6

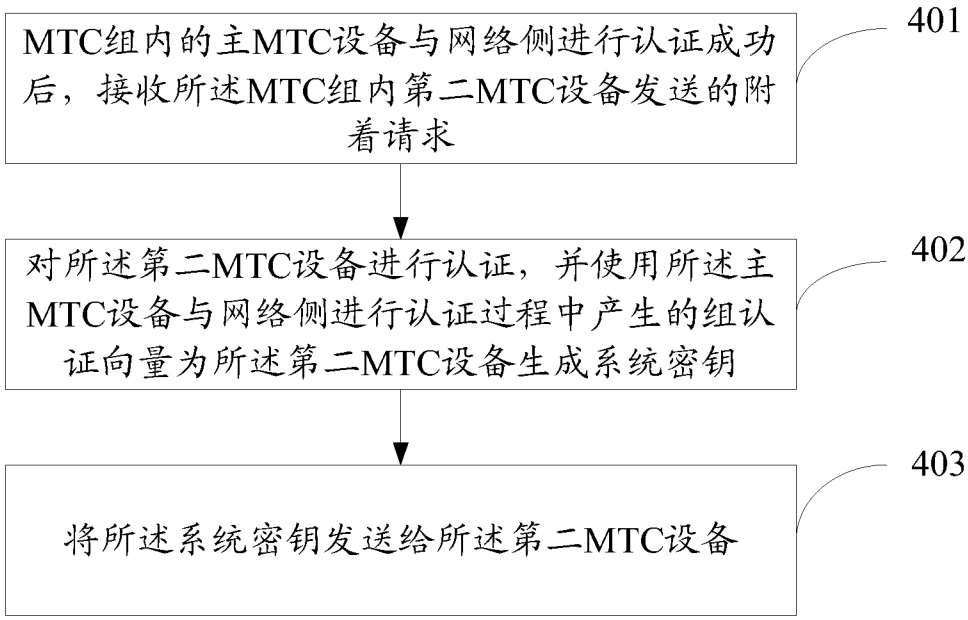
MTC组内的主MTC设备与网络侧进行认证成功后，接收所述MTC组内第二MTC设备发送的附着请求
401
对所述第二MTC设备进行认证，并使用所述主MTC设备与网络侧进行认证过程中产生的组认证向量为所述第二MTC设备生成系统密钥
402
将所述系统密钥发送给所述第二MTC设备
403

图 7

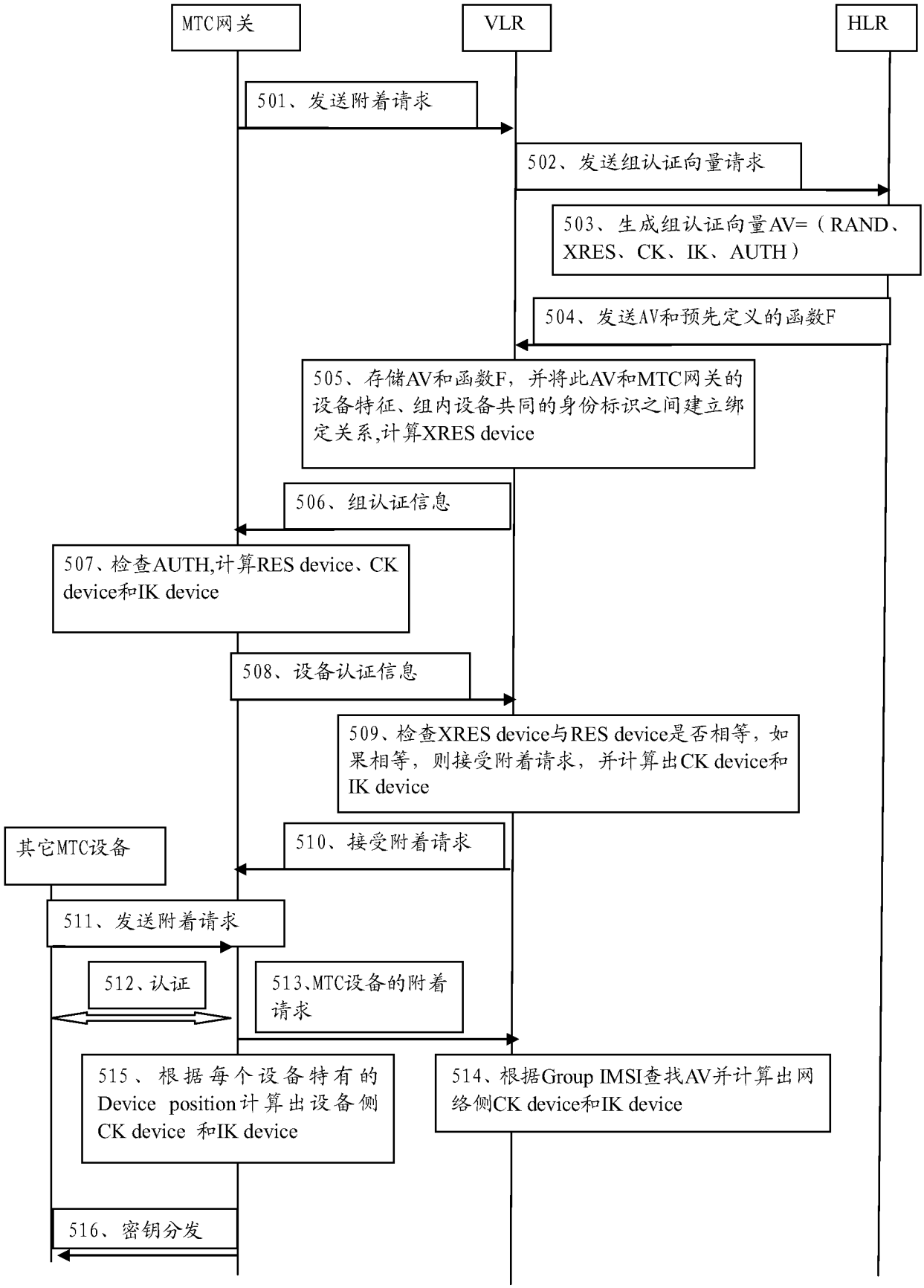
MTC网关
VLR
HLR
501、发送附着请求
502、发送组认证向量请求
503、生成组认证向量AV=（RAND、XRES、CK、IK、AUTH）
504、发送AV和预先定义的函数F
505、存储AV和函数F，并将此AV和MTC网关的设备特征、组内设备共同的身份标识之间建立绑定关系,计算XRES device
506、组认证信息
507、检查AUTH,计算RES device、CK device和IK device
508、设备认证信息
509、检查XRES device与RES device是否相等，如果相等，则接受附着请求，并计算出CK device和IK device
其它MTC设备
510、接受附着请求
511、发送附着请求
512、认证
513、MTC设备的附着请求
515、根据每个设备特有的Device position计算出设备侧CK device 和IK device
514、根据Group IMSI查找AV并计算出网络侧CK device和IK device
516、密钥分发

图 8

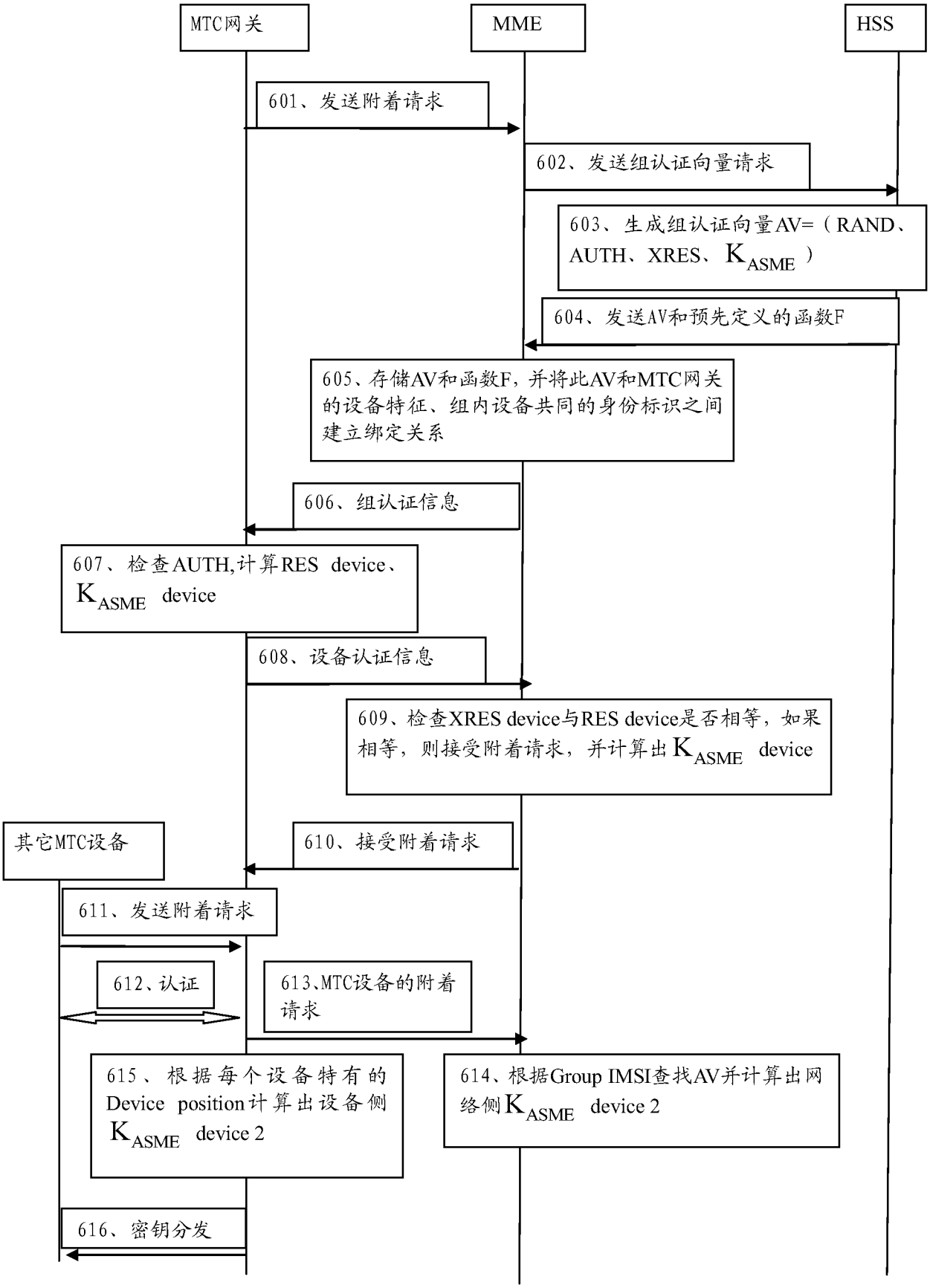
MTC网关
MME
HSS
601、发送附着请求
602、发送组认证向量请求
603、生成组认证向量AV=（RAND、AUTH、XRES、K_{ASME}）
604、发送AV和预先定义的函数F
605、存储AV和函数F，并将此AV和MTC网关的设备特征、组内设备共同的身份标识之间建立绑定关系
606、组认证信息
607、检查AUTH,计算RES device、K_{ASME} device
608、设备认证信息
609、检查XRES device与RES device是否相等，如果相等，则接受附着请求，并计算出K_{ASME} device
其它MTC设备
610、接受附着请求
611、发送附着请求
612、认证
613、MTC设备的附着请求
615、根据每个设备特有的Device position计算出设备侧K_{ASME} device 2
614、根据Group IMSI查找AV并计算出网络侧K_{ASME} device 2
616、密钥分发

图 9


MTC组内的主MTC设备向网络侧发送附着请求，其中，所述附着请求中包含所述MTC组的组标识和所述MTC组内其它待认证的MTC设备的设备特征
701
所述主MTC设备与所述网络侧进行认证，并使用组认证向量和所述其它待认证的MTC设备的设备特征为所述其它待认证的MTC设备生成系统密钥
702
所述主MTC设备对所述其它待认证的MTC设备进行认证成功后，将所述系统密钥发送给所述其它待认证的MTC设备
703

图 10

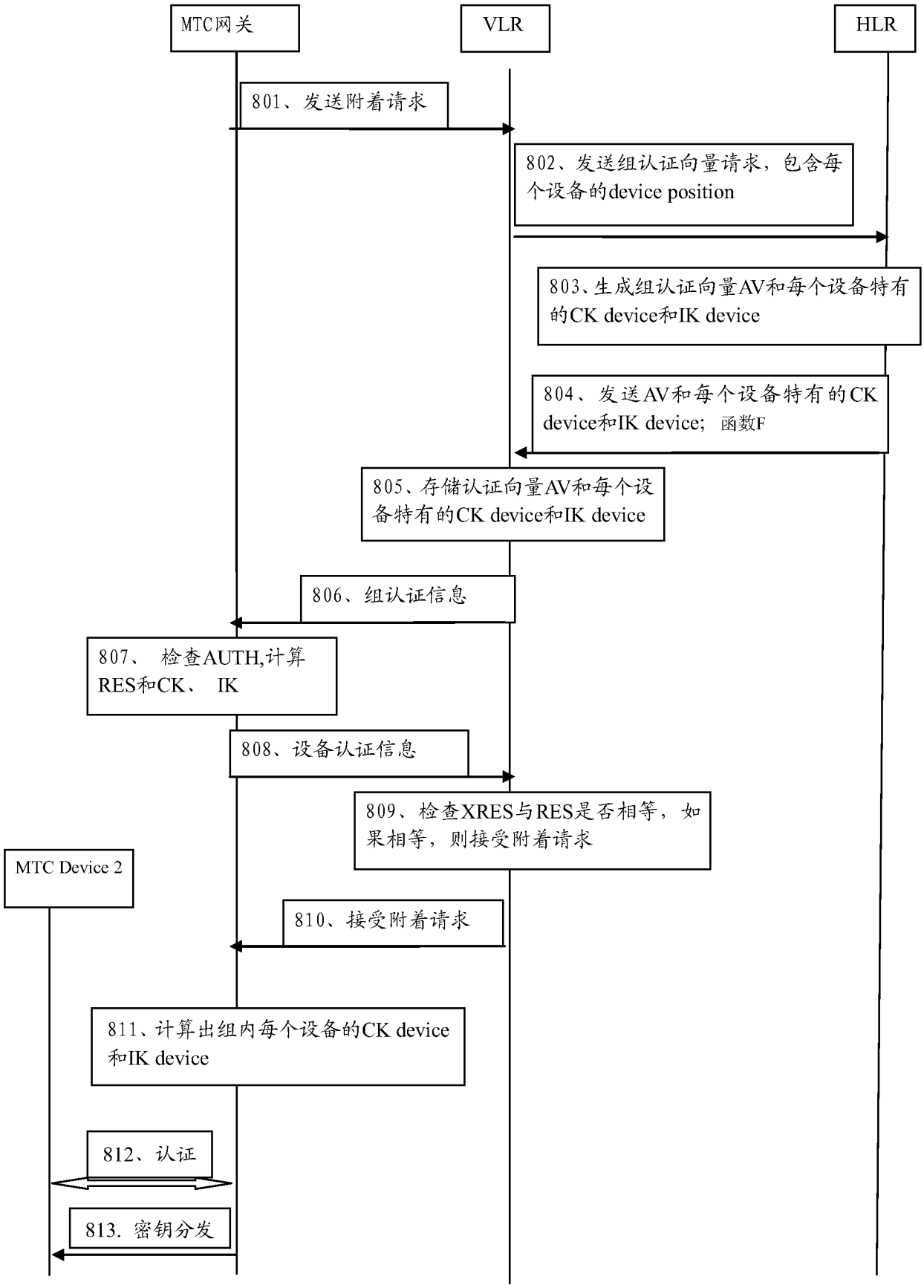
MTC网关
VLR
HLR
801、发送附着请求
802、发送组认证向量请求，包含每个设备的device position
803、生成组认证向量AV和每个设备特有的CK device和IK device
804、发送AV和每个设备特有的CK device和IK device；函数F
805、存储认证向量AV和每个设备特有的CK device和IK device
806、组认证信息
807、检查AUTH,计算RES和CK、IK
808、设备认证信息
809、检查XRES与RES是否相等，如果相等，则接受附着请求
MTC Device 2
810、接受附着请求
811、计算出组内每个设备的CK device和IK device
812、认证
813. 密钥分发

图 11

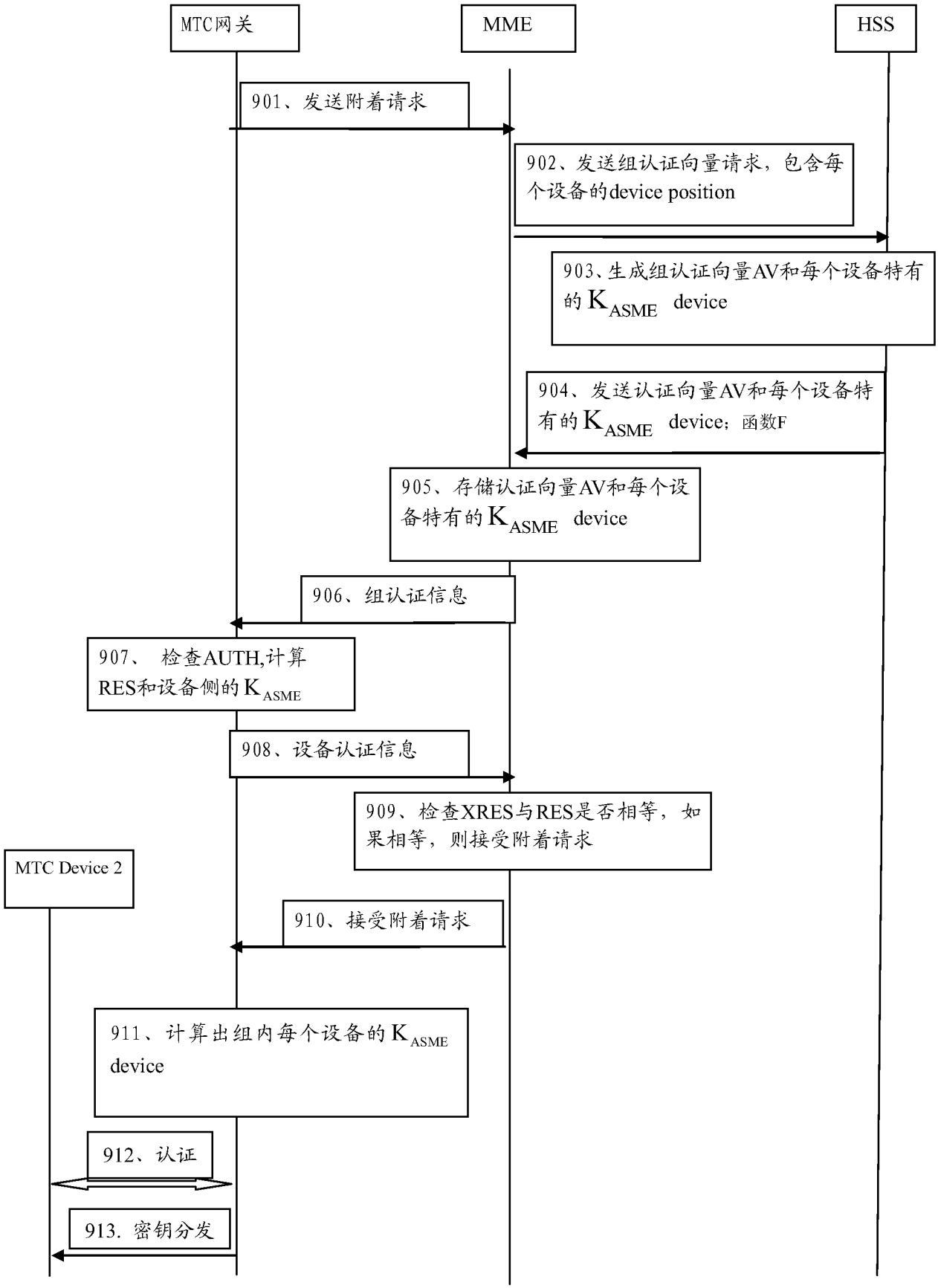
MTC网关
MME
HSS
901、发送附着请求
902、发送组认证向量请求，包含每个设备的device position
903、生成组认证向量AV和每个设备特有的K_{ASME} device
904、发送认证向量AV和每个设备特有的K_{ASME} device；函数F
905、存储认证向量AV和每个设备特有的K_{ASME} device
906、组认证信息
907、 检查AUTH,计算RES和设备侧的K_{ASME}
908、设备认证信息
909、检查XRES与RES是否相等，如果相等，则接受附着请求
MTC Device 2
910、接受附着请求
911、计算出组内每个设备的K_{ASME} device
912、认证
913. 密钥分发

图 12

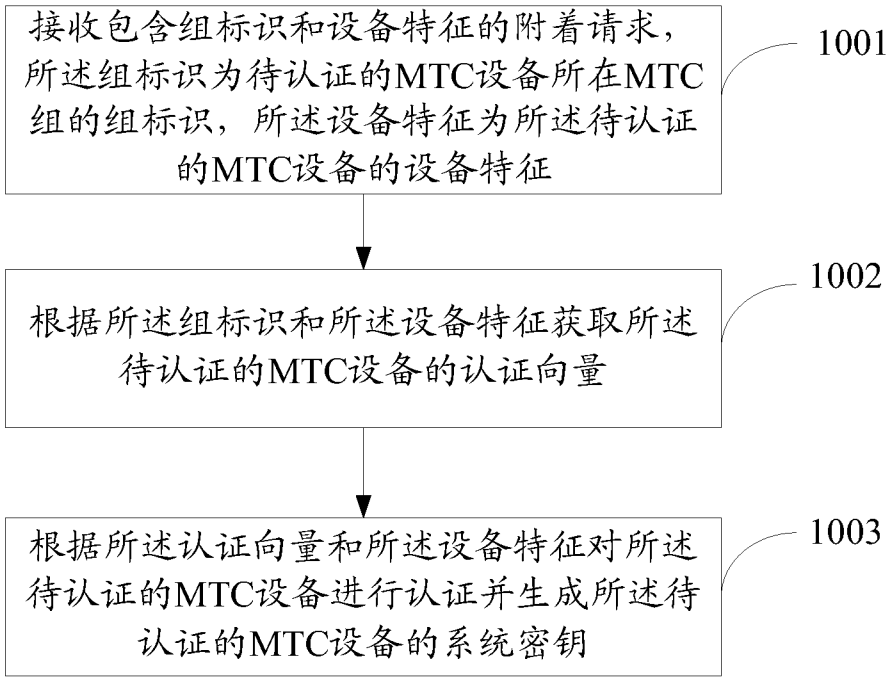
接收包含组标识和设备特征的附着请求，所述组标识为待认证的MTC设备所在MTC组的组标识，所述设备特征为所述待认证的MTC设备的设备特征
1001
根据所述组标识和所述设备特征获取所述待认证的MTC设备的认证向量
1002
根据所述认证向量和所述设备特征对所述待认证的MTC设备进行认证并生成所述待认证的MTC设备的系统密钥
1003

图 13

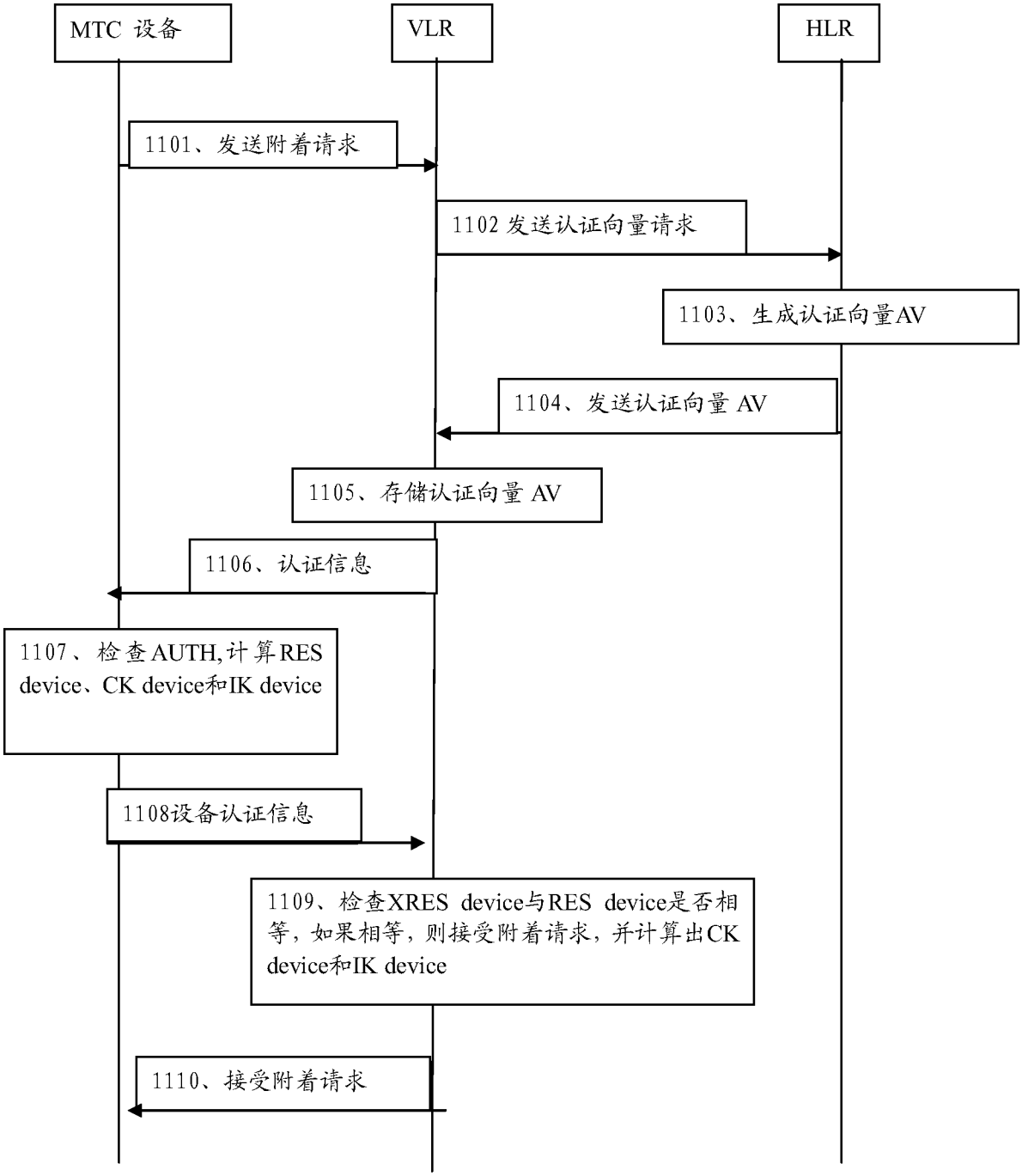
MTC 设备
VLR
HLR
1101、发送附着请求
1102 发送认证向量请求
1103、生成认证向量AV
1104、发送认证向量 AV
1105、存储认证向量 AV
1106、认证信息
1107、检查AUTH,计算RES device、CK device和IK device
1108设备认证信息
1109、检查XRES device与RES device是否相等，如果相等，则接受附着请求，并计算出CK device和IK device
1110、接受附着请求

图 14

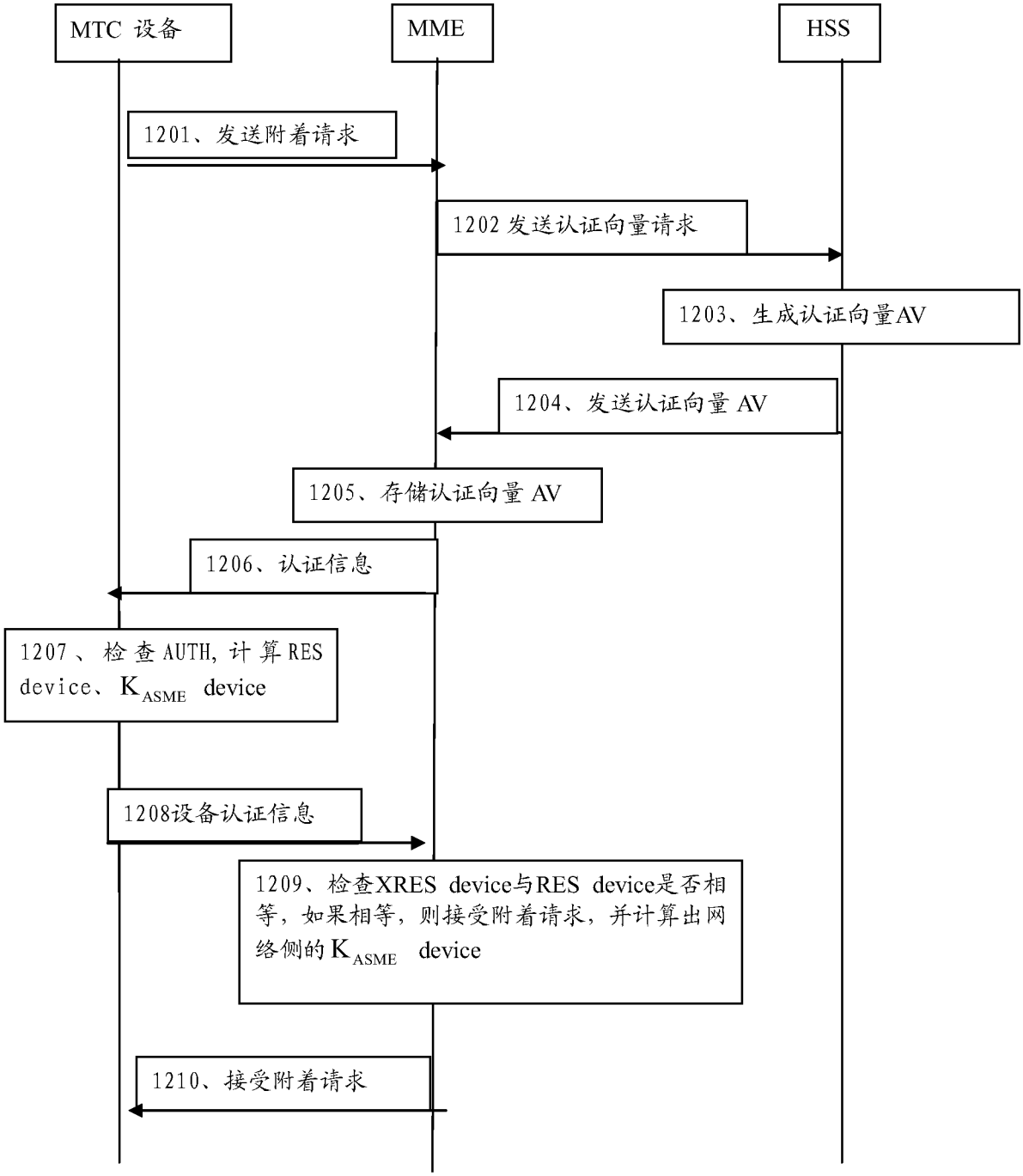
MTC 设备
MME
HSS
1201、发送附着请求
1202 发送认证向量请求
1203、生成认证向量AV
1204、发送认证向量 AV
1205、存储认证向量 AV
1206、认证信息
1207、检查 AUTH, 计算 RES device、K_{ASME} device
1208设备认证信息
1209、检查XRES device与RES device是否相等，如果相等，则接受附着请求，并计算出网络侧的K_{ASME} device
1210、接受附着请求

图 15

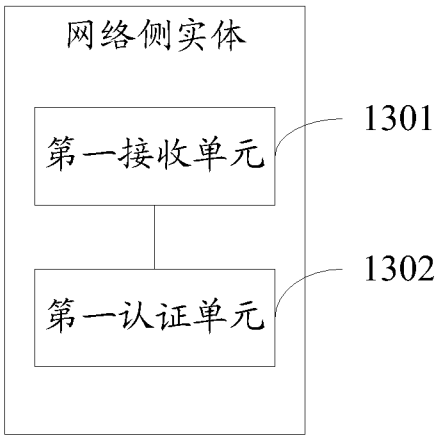
网络侧实体
第一接收单元
1301
第一认证单元
1302

图 16

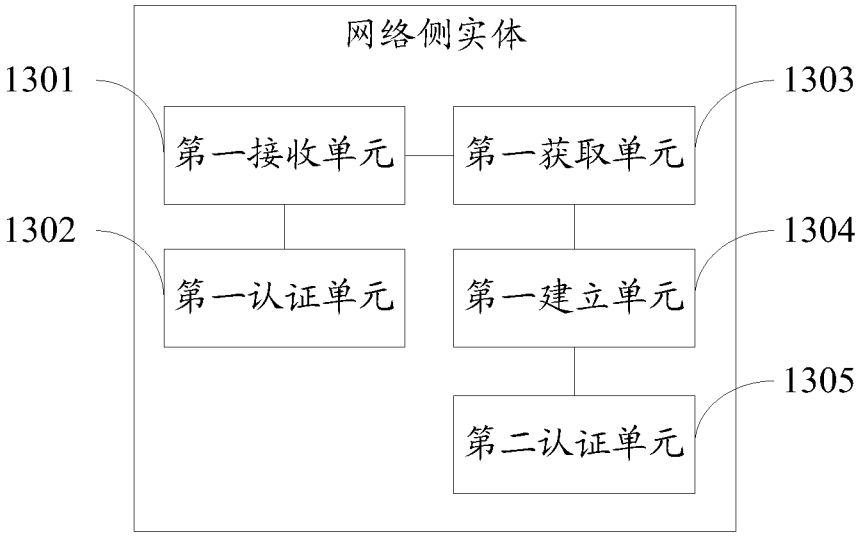
网络侧实体
1301
第一接收单元
1303
第一获取单元
1302
第一认证单元
1304
第一建立单元
1305
第二认证单元

图 17

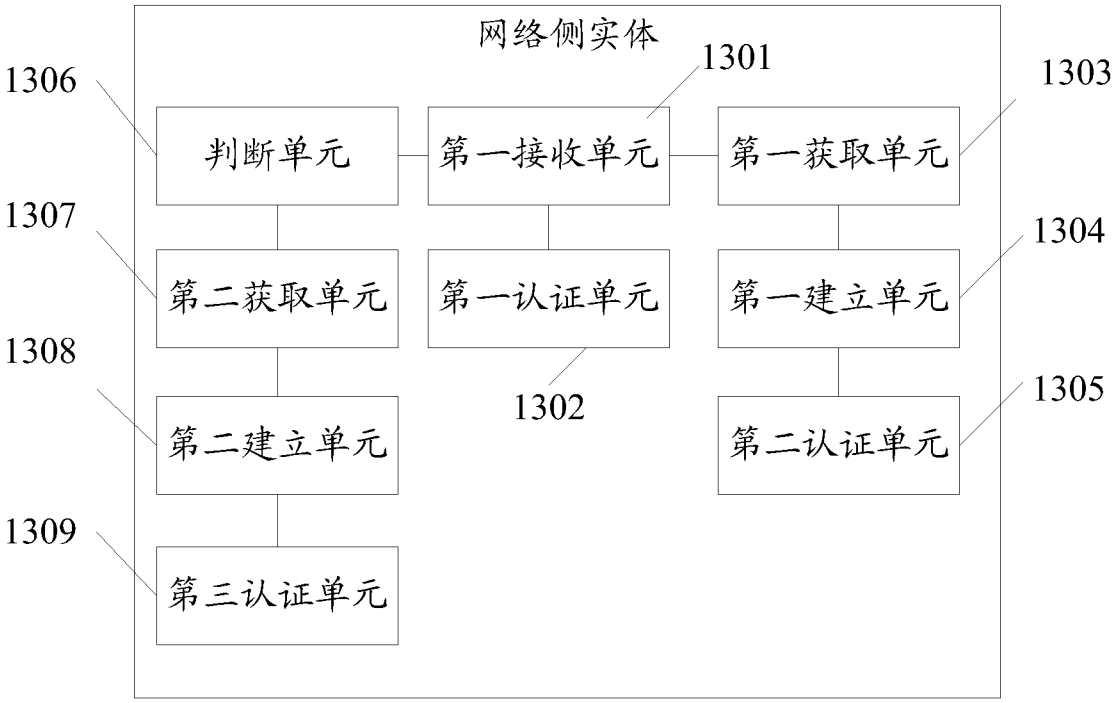
网络侧实体
1301
1303
1306
判断单元
第一接收单元
第一获取单元
1307
1304
第二获取单元
第一认证单元
第一建立单元
1308
1302
1305
第二建立单元
第二认证单元
1309
第三认证单元

图 18

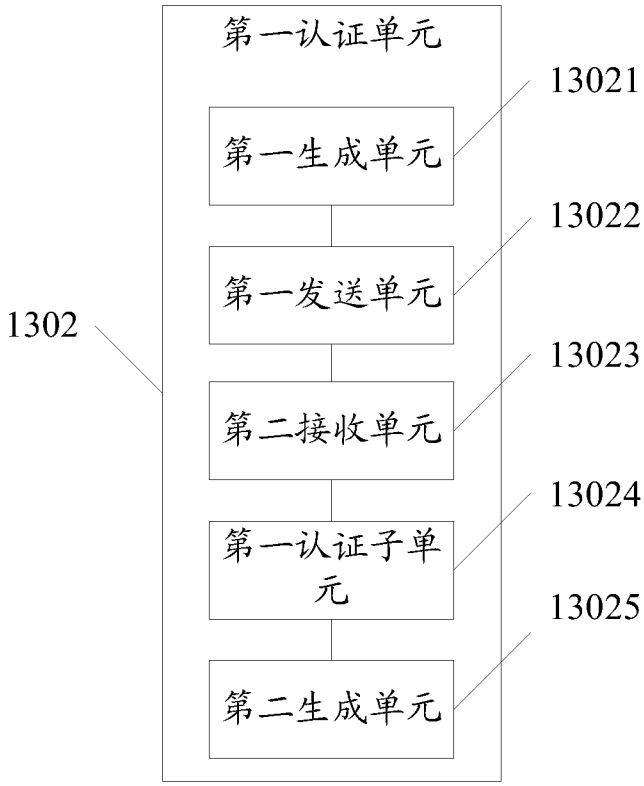
第一认证单元
13021
第一生成单元
13022
第一发送单元
1302
13023
第二接收单元
13024
第一认证子单元
13025
第二生成单元

图 19

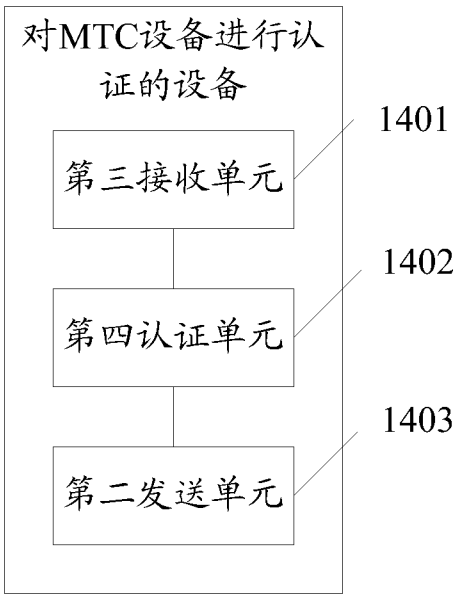
对MTC设备进行认证的设备
第三接收单元
第四认证单元
第二发送单元
1401
1402
1403

图 20

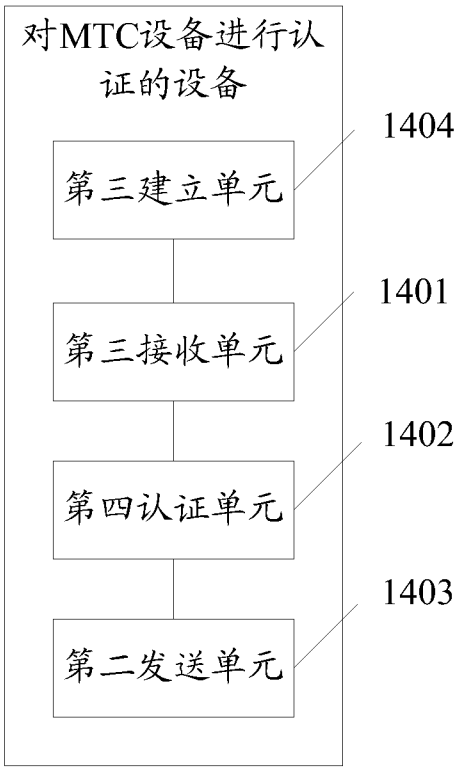
对MTC设备进行认证的设备
第三建立单元
第三接收单元
第四认证单元
第二发送单元
1404
1401
1402
1403

图 21

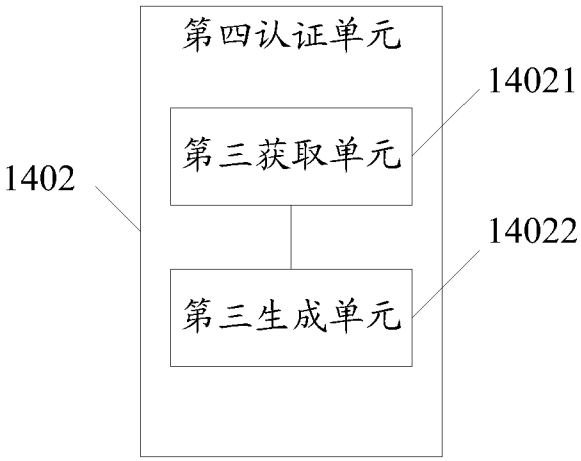
第四认证单元
14021
第三获取单元
1402
14022
第三生成单元

图 22

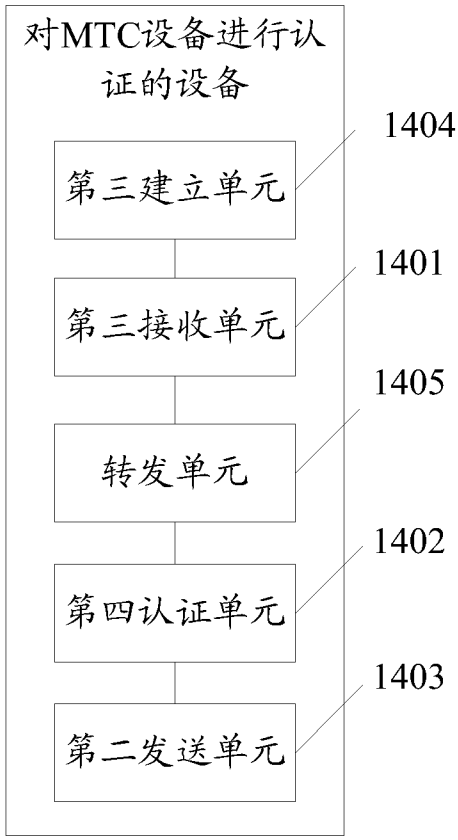
对MTC设备进行认证的设备
1404
第三建立单元
1401
第三接收单元
1405
转发单元
1402
第四认证单元
1403
第二发送单元

图 23

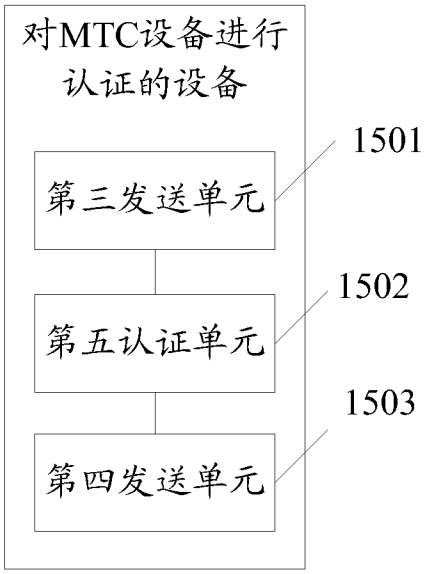
对MTC设备进行认证的设备
第三发送单元
1501
第五认证单元
1502
第四发送单元
1503

图 24

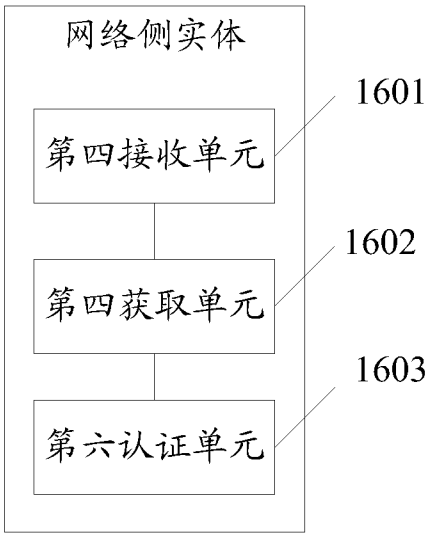
网络侧实体
第四接收单元
1601
第四获取单元
1602
第六认证单元
1603

图 25

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/072651

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; H04Q; 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)

CPRSABS, CNTXT, CNKI, VEN: group, cluster, ID, identi+, machine, MTC, communication, M2M, M2ME, authenticat+, validat+, authoriz+, vector, key, bound, bind+, correspond+, associat+, relat+, correlat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN101640887A (SHANGHAI HUAWEI TECHNOLOGIES CO LTD) 03 Feb. 2010(03.02.2010) the description page 1 paragraph 3-page 3 paragraph 1, figure 1	22-23
Y	ditto	1-3, 7, 10-13, 17-19
Y	CN101511082A (CHINA MOBILE COMMUNICATION CORP ET AL) 19 Aug. 2009(19.08.2009) the description page 1 paragraph 4-page 3 paragraph 1	1-3, 12-13, 17
Y	CN1691603A (LENOVO BEIJING CO LTD) 02 Nov. 2005(02.11.2005) the description page 4 line 7-page 9 line 12	7, 10-11, 18-19
A	WO2009095295A1 (NOKIA SIEMENS NETWORKS OY) 06 Aug. 2009(06.08.2009) the whole document	1-23

☐ 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
20 Jun. 2011(20.06.2011)	**21 Jul. 2011 (21.07.2011)**
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 LI, Meili Telephone No. (86-10)62411247

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2011/072651

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101640887A	03.02.2010	WO2010012201A1	04.02.2010
CN101511082A	19.08.2009	CN101511082B	05.01.2011
CN1691603A	02.11.2005	EP1758304B1	13.04.2011
		DE602005027458D1	26.05.2011
		KR100799222B1	29.01.2008
		KR20070014162A	31.01.2007
		JP2008500607T	10.01.2008
		N100340084C	26.09.2007
		US2007223398A1	27.09.2007
		WO2005107162A1	10.11.2005
		EP1758304A1	28.02.2007
WO2009095295A1	06.08.2009	EP2248323A1	10.11.2010
		US2009191857A1	30.07.2009

国际检索报告

国际申请号
PCT/CN2011/072651

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; H04Q; 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）)

CPRSABS, CNTXT, CNKI, VEN: 组,群,标识,标志,识别,机器,通信,认证,验证,鉴权,授权,向量,密钥,绑定,相应,对应,映射,group, cluster, ID, identi+, machine, MTC, communication, M2M, M2ME, authenticat+, validat+, authoriz+, vector, key, bound, bind+, correspond+, associat+, relat+, correlat+

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	CN101640887A（上海华为技术有限公司） 03.2 月 2010(03.02.2010) 说明书第 1 页第 3 段-第 3 页第 1 段，图 1	22-23
Y	同上	1-3, 7, 10-13, 17-19
Y	CN101511082A（中国移动通信集团公司等）19.8 月 2009(19.08.2009) 说明书第 1 页第 4 段-第 3 页第 1 段	1-3, 12-13, 17
Y	CN1691603A（联想（北京）有限公司） 02.11 月 2005(02.11.2005) 说明书第 4 页第 7 行-第 9 页第 12 行	7, 10-11, 18-19
A	WO2009095295A1（NOKIA SIEMENS NETWORKS OY） 06.8 月 2009(06.08.2009) 全文	1-23

☐ 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
20.6 月 2011(20.06.2011)	**21.7 月 2011 (21.07.2011)**
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 **李美丽** 电话号码：(86-10) **62411247**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2011/072651

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101640887A	03.02.2010	WO2010012201A1	04.02.2010
CN101511082A	19.08.2009	CN101511082B	05.01.2011
CN1691603A	02.11.2005	EP1758304B1	13.04.2011
		DE602005027458D1	26.05.2011
		KR100799222B1	29.01.2008
		KR20070014162A	31.01.2007
		JP2008500607T	10.01.2008
		N100340084C	26.09.2007
		US2007223398A1	27.09.2007
		WO2005107162A1	10.11.2005
		EP1758304A1	28.02.2007
WO2009095295A1	06.08.2009	EP2248323A1	10.11.2010
		US2009191857A1	30.07.2009