(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102238484 A
(43)申请公布日 2011.11.09

(21)申请号 201010153947.8

(22)申请日 2010.04.22

(71)申请人 中兴通讯股份有限公司
地址 518057 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法务部

(72)发明人 田甜 朱允文 韦银星 高峰

(74)专利代理机构 北京派特恩知识产权代理事务所(普通合伙) 11270
代理人 王黎延 迟姗

(51)Int.Cl.
H04W 4/08(2009.01)
H04W 12/04(2009.01)
H04W 12/06(2009.01)

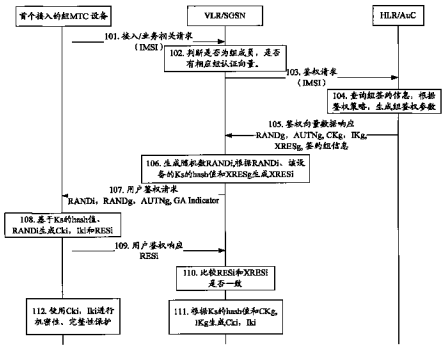
权利要求书 2 页 说明书 8 页 附图 5 页

(54)发明名称

机器对机器的通信系统中基于组的认证方法及系统

(57)摘要

本发明公开了一种机器对机器的通信系统中基于组的认证方法，包括：鉴权中心根据 MTC 设备所签约的组信息，生成组认证参数，并将组认证参数发送给接入安全管理设备；接入安全管理设备，根据生成的组认证参数，生成针对每个 MTC 设备的鉴权参数，并对该组中的 MTC 设备进行鉴权。本发明同时公开了一种机器对机器的通信系统中基于组的认证系统，包括 MTC 设备、接入安全管理设备 ASME 以及鉴权中心；鉴权中心用于根据机器类型通信 MTC 设备所签约的组信息，生成组认证参数，并将组认证参数发送给接入安全管理设备；接入安全管理设备用于根据生成的组认证参数，生成针对每个 MTC 设备的鉴权参数，并对该组中的 MTC 设备进行鉴权。本发明大大提高了对 MTC 设备的认证效率。



CN 102238484 A

1. 一种机器对机器的通信系统中基于组的认证方法，其特征在于，

鉴权中心根据机器类型通信 MTC 设备所签约的组信息，生成组认证参数，并将所述组认证参数发送给接入安全管理设备；

接入安全管理设备，根据生成的所述组认证参数，生成针对每个所述 MTC 设备的鉴权参数，并对该组中的 MTC 设备进行鉴权。

2. 根据权利要求 1 所述的方法，其特征在于，鉴权中心根据机器类型通信 MTC 设备所属的组签约信息，生成组认证参数之前：

鉴权中心预先配置 MTC 设备所属的组的组根密钥以及 MTC 设备的根密钥。

3. 根据权利要求 2 所述的方法，其特征在于，

鉴权中心根据收到的认证请求消息中携带的 MTC 设备标识，查询该 MTC 设备的签约信息，若该 MTC 设备拥有组签约，所述鉴权中心根据所述 MTC 设备所属组的组根密钥以及组标识生成相应的组认证向量；

鉴权中心根据所述 MTC 设备的根密钥及 hash 算法，生成所述 MTC 设备的根密钥的哈希值。

4. 根据权利要求 1 或 3 所述的方法，其特征在于，所述组认证参数包括：所述组认证向量、所述 MTC 设备根密钥的哈希值、所述 MTC 设备所属的签约的组及组成员信息。

5. 根据权利要求 1 所述的方法，其特征在于，

收到 MTC 设备附着请求或业务请求后，接入安全管理设备 ASME 根据所述请求消息中携带的 MTC 设备标识，查询是否已存在所述 MTC 设备所属签约的组及所述签约的组的组认证参数；若不存在，向鉴权中心发起对所述 MTC 设备的认证请求；若存在，由接入安全管理设备直接对所述 MTC 设备进行认证。

6. 根据权利要求 5 所述的方法，其特征在于，接入安全管理设备对所述 MTC 设备进行认证过程为：

所述接入安全管理设备生成随机数，根据所述组认证向量、所述 MTC 设备根密钥的哈希值、所述接入安全管理设备生成的随机数，生成针对所述 MTC 设备的认证向量，对所述 MTC 设备进行认证。

7. 一种机器对机器的通信系统中基于组的认证系统，包括 MTC 设备、接入安全管理设备 ASME 以及鉴权中心；其特征在于，

所述鉴权中心，用于根据机器类型通信 MTC 设备所签约的组信息，生成组认证参数，并将所述组认证参数发送给所述接入安全管理设备；

所述接入安全管理设备，用于根据生成的所述组认证参数，生成针对每个所述 MTC 设备的鉴权参数，并对该组中的 MTC 设备进行鉴权。

8. 根据权利要求 7 所述的系统，其特征在于，

所述鉴权中心，用于预先配置 MTC 设备所属的组的组根密钥以及 MTC 设备的根密钥；根据收到的认证请求消息中携带的 MTC 设备标识，查询该 MTC 设备的签约信息，若该 MTC 设备拥有组签约，根据所述 MTC 设备所属组的组根密钥以及组标识生成相应的组认证向量；根据所述 MTC 设备的根密钥及 hash 算法，生成所述 MTC 设备的根密钥的哈希值。

9. 根据权利要求 7 所述的系统，其特征在于，所述组认证参数包括：所述组认证向量、所述 MTC 设备根密钥的哈希值、所述 MTC 设备所属的签约的组及组成员信息。

10. 根据权利要求 7 所述的系统，其特征在于，

所述接入安全管理设备，用于收到 MTC 设备附着请求或业务请求后，根据所述请求消息中携带的 MTC 设备标识，查询是否已存在所述 MTC 设备所属签约的组及所述签约的组的组认证参数；若不存在，向鉴权中心发起对所述 MTC 设备的认证请求；若存在，对所述 MTC 设备进行认证；

所述接入安全管理设备，用于生成随机数，根据所述组认证向量、所述 MTC 设备根密钥的哈希值、所述随机数，生成针对所述 MTC 设备的认证向量，对所述 MTC 设备进行认证。

机器对机器的通信系统中基于组的认证方法及系统

技术领域

[0001] 本发明涉及机器对机器的通信系统中的认证技术，尤其涉及一种机器对机器(M2M，Machine-to-Machine)的通信系统中基于组的认证方法及系统。

背景技术

[0002] 在现有的第二代(2G，2nd Generation)和第三代(3G，3rd Generation)移动网络中，只有具有有效国际移动用户识别码(IMSI，International MobileSubscriber Identification Number)的用户才有权得到服务。

[0003] 鉴权，即识别有效国际移动用户识别码IMSI号码的过程。这是移动网络安全性管理的一部分，用来实现移动网络的保密性、数据完整性。下面简述一下通用移动通信系统(UMTS，Universal Mobile Telecommunications System)的认证和密钥协商机制(AKA，Authentication and Key Agreement)认证过程。在演进分组系统(EPS，Evolved Packet System)中EPS-AKA与UMTS-AKA本质上没有区别。具体的认证过程包括以下几个步骤：

[0004] (1)生成鉴权五元组：终端向归属位置寄存器(HLR，Home LocationRegister)/鉴权中心(AuC，The Authentication Centre)发出接入请求。从收到鉴权数据请求组后，VLR/SGSN生成相应的鉴权向量，每个向量由下列5个元素组成：随机数字RAND、期望响应XRES、密钥CK、完整性密钥IK和鉴权令牌AUTN。

[0005] (2)将鉴权五元组发送到请求的VLR/SGSN。

[0006] (3)从得到的多个五元组中选择一个，发送RAND(i)、AUTN(i)到用户。

[0007] (4)全球用户身份模块(USIM，Universal Subscriber Identity Module)卡检查AUTN(i)可否接受，例如AUTN(i)是由有效的鉴权令牌组成。

[0008] (5)终端接收到认证请求后，首先计算消息认证码XMAC，并与认证令牌AUTN中的消息认证码MAC比较，如果不同，则向SGSN/VLR发出拒绝认证消息，并放弃认证过程。同时移动台(MS，Mobile Station)验证接收到的序列号SQN是否在有效的范围内，若不在有效的范围内，MS则向SGSN/VLR发送同步失败消息，放弃认证过程。

[0009] (6)当以上验证通过以后，才产生响应RES(i)，并发送到VLR/SGSN；由VLR/SGSN比较RES(i)和XRES(i)。USIM卡同时计算CK和IK，用于在空中接口加密和完整性保护。

[0010] 但是，现有移动网络优化都是基于人对人(human-to-human)而设计的，而对于machine-to-machine、机器对人(machine-to-human)、或人对机器(human-to-machine)的应用并非最佳。

[0011] 随着M2M技术的日趋发展和成熟，M2M用途的多元化，M2M终端的数量将会出现爆炸性的增长，据估计，M2M的终端数将达到手持终端数量的两个数量级，如果每个M2M终端独立跟网络鉴权和传送数据，用户签约数据库/鉴权中心即HSS或HLR将为每个接入的机器类型通信MTC(Machine TypeCommunication)设备生成相应的鉴权向量并发送给接入安全管理实体，对现有的网络压力将会非常大，从而对M2M服务的服务质量和用户体验造成很大影响。

[0012] 当有许多 MTC 设备被部署为属于同一个 MTC 用户的 MTC 设备组，或当所有在同一个地点的 MTC 设备被分在一个组时，对于组中所有 MTC 设备的认证代价也是很高的，但也常常是不必要的。没有对组进行优化时，每一个 MTC 设备都必须单独地被认证，这样，由于系统中认证所需的信令负荷会随着认证被单独执行而增加，甚至可能造成网络拥塞。

[0013] 由于当前的第三代合作伙伴计划 (3GPP，3rd Generation Partnership Project) 的网络认证技术难以满足今后数量越来越庞大的 MTC 设备。所以需要一种优化的 MTC 设备的鉴权机制来大幅减少所需要的信令数量，尤其是降低核心网的压力。

发明内容

[0014] 有鉴于此，本发明的主要目的在于提供一种机器对机器的通信系统中基于组的认证方法及系统，提高 MTC 设备认证的效率，能够大幅减少现有网络中的信令数量，同时减轻现有网络的认证负荷。

[0015] 为达到上述目的，本发明的技术方案是这样实现的：

[0016] 一种机器对机器的通信系统中基于组的认证方法，鉴权中心根据 MTC 设备所签约的组信息，生成组认证参数，并将所述组认证参数发送给接入安全管理设备；

[0017] 接入安全管理设备，根据生成的所述组认证参数，生成针对每个所述 MTC 设备的鉴权参数，并对该组中的 MTC 设备进行鉴权。

[0018] 优选地，鉴权中心根据机器类型通信 MTC 设备所属的组签约信息，生成组认证参数之前：

[0019] 鉴权中心预先配置 MTC 设备所属的组的组根密钥以及 MTC 设备的根密钥。

[0020] 优选地，鉴权中心根据收到的认证请求消息中携带的 MTC 设备标识，查询该 MTC 设备的签约信息，若该 MTC 设备拥有组签约，所述鉴权中心根据所述 MTC 设备所属组的组根密钥以及组标识生成相应的组认证向量；

[0021] 鉴权中心根据所述 MTC 设备的根密钥及 hash 算法，生成所述 MTC 设备的根密钥的哈希值。

[0022] 优选地，所述组认证参数包括：所述组认证向量、所述 MTC 设备根密钥的哈希值、所述 MTC 设备所属的签约的组及组成员信息。

[0023] 优选地，收到 MTC 设备附着请求或业务请求后，接入安全管理设备 ASME 根据所述请求消息中携带的 MTC 设备标识，查询是否已存在所述 MTC 设备所属签约的组及所述签约的组的组认证参数；若不存在，向鉴权中心发起对所述 MTC 设备的认证请求；若存在，由接入安全管理设备直接对所述 MTC 设备进行认证。

[0024] 优选地，接入安全管理设备对所述 MTC 设备进行认证过程为：

[0025] 所述接入安全管理设备生成随机数，根据所述组认证向量、所述 MTC 设备根密钥的哈希值、所述接入安全管理设备生成的随机数，生成针对所述 MTC 设备的认证向量，对所述 MTC 设备进行认证。

[0026] 一种机器对机器的通信系统中基于组的认证系统，包括 MTC 设备、ASME 以及鉴权中心；所述鉴权中心，用于根据机器类型通信 MTC 设备所签约的组信息，生成组认证参数，并将所述组认证参数发送给所述接入安全管理设备；

[0027] 所述接入安全管理设备，用于根据生成的所述组认证参数，生成针对每个所述 MTC

设备的鉴权参数，并对该组中的 MTC 设备进行鉴权。

[0028] 优选地，所述鉴权中心，用于预先配置 MTC 设备所属的组的组根密钥以及 MTC 设备的根密钥；根据收到的认证请求消息中携带的 MTC 设备标识，查询该 MTC 设备的签约信息，若该 MTC 设备拥有组签约，根据所述 MTC 设备所属组的组根密钥以及组标识生成相应的组认证向量；根据所述 MTC 设备的根密钥及 hash 算法，生成所述 MTC 设备的根密钥的哈希值。

[0029] 优选地，所述组认证参数包括：所述组认证向量、所述 MTC 设备根密钥的哈希值、所述 MTC 设备所属的签约的组及组成员信息。

[0030] 优选地，所述接入安全管理设备，用于收到 MTC 设备附着请求或业务请求后，根据所述请求消息中携带的 MTC 设备标识，查询是否已存在所述 MTC 设备所属签约的组及所述签约的组的组认证参数；若不存在，向鉴权中心发起对所述 MTC 设备的认证请求；若存在，对所述 MTC 设备进行认证；

[0031] 所述接入安全管理设备，用于生成随机数，根据所述组认证向量、所述 MTC 设备根密钥的哈希值、所述随机数，生成针对所述 MTC 设备的认证向量，对所述 MTC 设备进行认证。

[0032] 本发明中，将共享同一组签约信息的 MTC 设备划分为一组，这样，在同一组内的 MTC 设备首次进行鉴权认证时，即 ASME 中没有有效的组认证参数时，ASME 向鉴权中心发起认证请求，鉴权中心会将相应的认证向量发送给 ASME，由 ASME 完成对 MTC 设备的鉴权认证，而当 ASME 中已经有相应的组认证参数时，该组内的 MTC 设备进行鉴权认证时，直接由该 ASME 利用相应的认证向量对属同一组内的其他 MTC 设备进行认证即可，不必再让鉴权中心参与对每一 MTC 设备的认证，这无疑提高了对 MTC 设备认证的效率，并且，分担了鉴权中心对 MTC 设备认证的负荷，节约了网络侧的处理资源，有利于提高核心网侧的业务处理效率。

附图说明

[0033] 图 1 为 UMTS 网络中一组 MTC 设备中首个接入的 MTC 设备的认证流程图；

[0034] 图 2 为 UMTS 网络中一组 MTC 设备中已有 MTC 设备进行过认证的认证流程图；

[0035] 图 3 为 LTE/SAE 的密钥架构图；

[0036] 图 4 为 EPS 网络中共享同一签约信息的组内首个 MTC 设备的认证流程图；

[0037] 图 5 为 EPS 网络中一组 MTC 设备中已有 MTC 设备进行过认证的认证流程图；

[0038] 图 6 为本发明机器对机器的通信系统中基于组的认证系统的组成结构示意图。

具体实施方式

[0039] 本发明的基本思想为：将共享同一组签约信息的 MTC 设备划分为一组，这样，在同一组内的 MTC 设备首次进行鉴权认证时，即 ASME 中没有有效的组认证参数时，ASME 向鉴权中心发起认证请求，鉴权中心会将相应的认证向量发送给 ASME，由 ASME 完成对 MTC 设备的鉴权认证，而当 ASME 中已经有相应的组认证参数时，该组内的 MTC 设备进行鉴权认证时，直接由该 ASME 利用相应的认证向量对属同一组内的其他 MTC 设备进行认证即可，不必再让鉴权中心参与对每一 MTC 设备的认证。

[0040] 为使本发明的目的、技术方案和优点更加清楚明白，以下举实施例并参照附图，对本发明进一步详细说明。

[0041] 图 1 及图 2 所示为 3G 网络中共享同一签约信息的组内 MTC 设备组认证流程，其中

网元 ASME 具体为 VLR/SGSN，用户签约数据库 / 鉴权中心具体为 HLR/AuC。在签约为一组的各 MTC 设备中预先配置组标识信息、组根密钥 Ksg 信息及 MTC 设备根密钥 Ksi 信息；在签约中心预先配置签约为一组的 MTC 设备的组根密钥信息、组中各 MTC 设备的根密钥信息以及组的签约信息。

[0042] 图 1 为 UMTS 网络中一组 MTC 设备中首个接入的 MTC 设备的认证流程图，如图 1 所示，本示例 MTC 设备认证流程具体包括以下步骤：

[0043] 步骤 101：共享同一签约信息的 MTC 设备组中的首个接入的 MTC 设备发起接入 / 业务相关请求，请求消息中包含该首个 MTC 设备的标识信息，具体的，本示例中的 MTC 设备的标识信息为 MTC 设备的 IMSI。

[0044] 步骤 102：VLR/SGSN 查询自身中是否已存在包含该 MTC 设备的签约组信息及其组认证向量。

[0045] 步骤 103：本示例中，由于当前认证的 MTC 设备为该组中的首个 MTC 设备进行的认证，因此不存在该 MTC 设备签约的组的认证参数信息。VLR/SGSN 向 HLR/AuC 发起鉴权请求，请求中携带 MTC 设备 IMSI 信息。

[0046] 步骤 104：HLR/AuC 根据 MTC 设备标识查询其签约信息，如该设备拥有组签约，根据鉴权策略，生成相应的组认证向量。具体的，组认证向量是根据相应的鉴权策略生成相应的认证向量，鉴权策略中包含一些生成相应密钥的算法，如哈希算法，还有生成认证向量的密钥生成算法等。这里，组认证向量包含组随机数 RANDg、组鉴权令牌 AUTNg、组加密密钥 CKg、组完整性密钥 IKg、组期望响应 XRESg 五元信息。这里，生成认证向量的密钥生成算法及哈希算法可以是现有的任一种算法。认证向量由组根密钥及组签约信息如组标识信息等的相关信息生成，由于其为现有技术，这里不再赘述各参数的生成方式。

[0047] 步骤 105：HLR/AuC 返回鉴权向量数据响应给 VLR/SGSN，该消息中包括组鉴权五元组：组随机数 RANDg、组鉴权令牌 AUTNg、组加密密钥 CKg、组完整性密钥 IKg、组期望响应 XRESg，同时消息中还携带有该组的签约信息，组的签约信息包括该组标识，该组所有 MTC 设备标识 IMSI。发送给 VLR/SGSN 的消息中还包括每个 MTC 设备的根密钥的哈希值 hash(Ksi)。具体的，HLR/AuC 根据设定的哈希算法计算每个 MTC 设备的根密钥的哈希值。本发明中，由鉴权中心统一生成上述 MTC 设备的根密钥的哈希值，主要是保证鉴权认证的安全性，本发明优选采用此方式。

[0048] 步骤 106：VLR/SGSN 保存 HLR/AuC 发送的组认证参数，如认证向量及相应的哈希值等，在参数中查找到该 MTC 设备对应的 hash(Ksi)，并生成随机数 RANDi，根据 hash(Ksi)、RANDi 和 XRESg 生成 XRESi。具体的，根据 MTC 设备标识即可查找出其对应的 hash(Ksi)。

[0049] 步骤 107：VLR/SGSN 发送用户鉴权请求给 MTC 设备，消息中包含 RANDi，RANDg，AUTNg 和组认证指示 GA Indicator。

[0050] 步骤 108：MTC 设备使用和 HLR/AuC 相同的哈希算法计算出自身 MTC 设备根密钥的 Ksi 的哈希值 hash(Ksi)，并基于此哈希值 hash(Ksi) 和 RANDi，利用现有密钥算法计算出的组机密性密钥 CKg、组完整性密钥 KIg 以及组期望响应 XRESg，分别计算出 MTC 设备的机密性密钥 CKi，MTC 设备的完整性密钥 IKi 和 MTC 设备的响应 RESi。

[0051] 步骤 109：MTC 设备向 VLR/SGSN 返回用户鉴权响应，该响应中包含 RESi。

[0052] 步骤 110：VLR/SGSN 比较 RESi 和 XRESi，如果一致，则通过认证，否则认证失败。

[0053] 步骤 111 :VLR/SGSN 根据 hash(Ksi) 和 RANDi，以及 CKg、KIg，分别生成 CKi，IKi，发送给无线网络控制器 (RNC，Radio Network Controller) 用于数据加密。

[0054] 步骤 112 :MTC 设备使用 CKi、IKi 对数据分别进行机密性、完整性保护。

[0055] 图 2 为 UMTS 网络中一组 MTC 设备中已有 MTC 设备进行过认证的认证流程图，如图 2 所示，本示例 MTC 设备认证流程具体包括以下步骤 :

[0056] 步骤 201 :MTC 设备发起接入 / 业务相关请求，请求消息中包含该 MTC 设备标识 (本示例中为 IMSI)。

[0057] 步骤 202 :VLR/SGSN 查询自身中是否已存在包含该 MTC 设备的签约组信息。

[0058] 步骤 203 :本示例中 VLR/SGSN 查找到拥有该 MTC 设备的相应签约组的信息及该组的组认证向量，VLR/SGSN 生成随机数 RANDi，根据 RANDi、hash(Ksi) 和 XRESg 生成 XRESi。

[0059] 步骤 204 :VLR/SGSN 发送用户鉴权请求给 MTC 设备，消息中包含 RANDi、RANDg，AUTNg 和组认证指示 GA Indicator。

[0060] 步骤 205 :MTC 设备使用和 HLR/AuC 相同的哈希算法计算出自身的 Ksi 的哈希值 hash(Ksi)，并基于此哈希值 hash(Ksi) 和 RANDi 以及用现有算法计算出组的 CKg、IKg、RESg，分别计算出 MTC 设备的 CKi、IKi 和 RESi。

[0061] 步骤 206 :MTC 设备向 VLR/SGSN 返回用户鉴权响应，该响应中包含 RESi。

[0062] 步骤 207 :VLR/SGSN 比较 RESi 和 XRESi，如果一致，通过认证。

[0063] 步骤 208 :VLR/SGSN 根据 hash(Ksi) 和 CKg，KIg 生成 CKi，IKi，发送给 RNC 用于数据加密。

[0064] 步骤 209 :MTC 设备使用 CKi，IKi 对数据进行机密性、完整性保护。

[0065] 在长期演进 (LTE，Long Term Evolution)/(SAE，SystemArchitechtureEvolution) 中，由于 eNB 处于一个不完全信任区域，因此 LTE/SAE 的安全包括两个层次 :接入层 (AS，Access Stratum) 和非接入层 (NAS，Non AccessStratum) 的安全 :

[0066] 1) 接入层 (AS) 安全 :UE 与 eNB 之间的安全，主要执行 AS 信令的加密和完整性保护，用户面 UP 的加密性保护。

[0067] 2) 非接入层 (NAS) 安全 :UE 与 MME 之间的安全，主要执行 NAS 信令的加密和完整性保护。

[0068] 图 3 为 LTE/SAE 的密钥架构图，如图 3 所示，LTE/SAE 网络的密钥层次架构中包含如下密钥 :

[0069] 1)UE 和 HSS 间共享的密钥 :

[0070] K :存储在 MTC 设备的 USIM 中和鉴权中心 AuC 的永久密钥，属组根密钥。

[0071] CK/IK :AuC 和 USIM 在 AKA 认证过程中生成的密钥对。与 UMTS 相比，CK/IK 不应离开 HSS。

[0072] 2) 管理单元 (ME，Management Element) 和 ASME 共享的中间密钥 :

[0073] K_{ASME} :UE 和 HSS 根据 CK/IK 推演得到的密钥，用于推演下层密钥。

[0074] 3)UE 与 eNB 和 MME 的共享密钥 :

[0075] K_{NASint} :UE 和 MME 根据 K_{ASME} 推演得到的密钥，用于保护 UE 和 MME 间 NAS 流量的完整性。

[0076] K_{NASenc} :UE 和 MME 根据 K_{ASME} 推演得到的密钥,用于保护 UE 和 MME 间 NAS 流量的保密性。

[0077] K_{eNB} :UE 和 MME 根据 K_{ASME} 推演得到的密钥。K_{eNB} 用于推导 AS 层密钥。

[0078] K_{UPenc} :UE 和 eNB 根据 K_{eNB} 和加密算法的标识符推演得到,用于保护 UE 和 eNB 间 UP 的保密性。

[0079] K_{RRCint} :UE 和 eNB 根据 K_{eNB} 和完整性算法的标识符推演得到,用于保护 UE 和 eNB 间 RCC 的完整性。

[0080] K_{RRCenc} :UE 和 eNB 根据 K_{eNB} 和加密算法的标识符推演得到,用于保护 UE 和 eNB 间 RCC 的保密性。

[0081] 图 4 及图 5 所示为 EPS 网络中共享同一签约信息的组内 MTC 设备认证流程,其中网元 ASME 具体为 MME,用户签约数据库 / 鉴权中心具体为 HSS。在签约为一组的各 MTC 设备中预先配置组标识信息、组根密钥 Ksg 信息及 MTC 设备根密钥 Ksi 信息 ;在签约中心预先配置签约为一组的 MTC 设备的组根密钥信息、组中各 MTC 设备的根密钥信息以及组的签约信息。

[0082] 图 4 为 EPS 网络中共享同一签约信息的组内首个 MTC 设备的认证流程图,如图 4 所示,本示例 MTC 设备认证流程具体包括以下步骤 :

[0083] 步骤 401 :接入的 MTC 设备发起接入 / 业务相关请求,请求消息中包含该用户标识 (IMSI)。

[0084] 步骤 402 :MME 查询自身中是否已存在包含该 MTC 设备的签约组信息及其组认证向量。

[0085] 步骤 403 :本示例中,由于当前认证的 MTC 设备为该组中的首个 MTC 设备进行的认证,因此不存在该 MTC 设备所属签约的组的信息。MME 发起鉴权请求,请求中携带设备标识,此例中为设备的 IMSI。

[0086] 步骤 404 :HSS 根据 MTC 设备标识查询其签约信息,如该设备拥有组签约,根据鉴权策略,生成相应的组认证向量。该实例中,MTC 设备拥有组签约,则 HSS 生成组认证向量。具体的,根据组根密钥及相应的密钥生成算法生成包含有组随机数 RANDg、组鉴权令牌 AUTNg、组密钥集识别码 $KSI_{ASME}g$、接入网元密钥 K_{ASME}、组期望响应 XRESg 的认证向量。

[0087] 步骤 405 :HSS 返回鉴权向量数据响应给 MME,该消息中包括组随机数 RANDg、组鉴权令牌 AUTNg、组密钥集识别码 $KSI_{ASME}g$、接入网元密钥 K_{ASME}、组期望响应 XRESg,组的签约信息包括该组标识,该组所有 MTC 设备标识。发送给 MME 的消息中还包括每个 MTC 设备的根密钥的哈希值 hash(Ksi) ;具体的,HSS 根据设定的哈希算法对每个 MTC 设备的根密钥计算即可。

[0088] 步骤 406 :MME 保存组认证参数,在参数中查找到该 MTC 设备对应的 hash(Ksi),生成随机数 RANDi,根据 hash(Ksi)、RANDi 以及 K_{ASME} 生成 $K_{ASME}i$、根据 hash(Ksi)、RANDi 以及 XRESg 生成 XRESi。

[0089] 步骤 407 :MME 发送用户鉴权请求给 MTC 设备,消息中包含 RANDi、RANDg、AUTNg、$KSI_{ASME}g$ 和组认证指示 GA Indicator。

[0090] 步骤 408 :MTC 设备使用和 HSS 相同的哈希算法计算出该 MTC 设备自身 MTC 设备根密钥的 Ksi 的哈希值 hash(Ksi),并基于此哈希值 hash(Ksi)、RANDi 以及利用现有算法计

算出的组响应 RESg 和 K_{ASME}，分别计算出 MTC 设备的响应 RESi、$K_{ASME}i$。。

[0091] 步骤 409 :MTC 设备向 MME 返回用户鉴权响应，该响应中包含 RESi。

[0092] 步骤 410 :MME 比较 RESi 和 XRESi，如果一致，通过认证，否则认证失败。

[0093] 步骤 411 :MME 根据 hash(Ksi)、RANDi 和 K_{ASME} 生成 $K_{ASME}i$，基于 $K_{ASME}i$ 生成 $K_{NASenc}i$、$K_{NASint}i$、$K_{eNB}i$。其中，$K_{NASenc}i$、$K_{NASint}i$ 用于保护用户和 MME 之间的 NAS 信令，$K_{eNB}i$ 下发给 eNB，eNB 基于 K_{eNBi} 生成 $K_{UPenc}i$、$K_{RRCint}i$ 和 $K_{RRCenc}i$。

[0094] 步骤 412 :MTC 设备基于 $K_{ASME}i$ 生成 $K_{NASenc}i$、$K_{NASint}i$、$K_{eNB}i$，其中，$K_{NASenc}i$、$K_{NASint}i$ 分别对数据进行机密性、完整性保护。

[0095] 图 5 为 EPS 网络中一组 MTC 设备中已有 MTC 设备进行过认证的认证流程图，如图 5 所示，本示例 MTC 设备认证流程具体包括以下步骤 :

[0096] 步骤 501 :MTC 设备发起接入 / 业务相关请求，请求消息中包含该用户标识 (IMSI)。

[0097] 步骤 502 :MME 查询自身中是否已存在包含该 MTC 设备的签约组信息。。

[0098] 步骤 503 :本示例中 MME 查找到已有该 MTC 设备所属签约组的信息及该组认证向量信息，MME 生成随机数 RANDi，根据 RANDi、hash(Ksi) 和 XRESg 生成 XRESi。

[0099] 步骤 504 :MME 发送用户鉴权请求给 MTC 设备，消息中包含 RANDi、RANDg，AUTNg、$KSI_{ASME}g$ 和组认证指示 GA Indicator。

[0100] 步骤 505 :MTC 设备使用和 HSS 相同的哈希算法计算出自己的 Ksi 的哈希值 hash(Ksi)，并基于此哈希值和 RANDi 以及用现有算法算出的 RESg 计算出 RESi。

[0101] 步骤 506 :MTC 设备向 MME 返回用户鉴权响应，该响应中包含 RESi。

[0102] 步骤 507 :MME 比较 RESi 和 XRESi，如果一致，通过认证。

[0103] 步骤 508 :MME 根据 RANDi、hash(Ksi) 和 K_{ASME} 生成 $K_{ASME}i$，基于 $K_{ASME}i$ 生成 $K_{NASenc}i$，$K_{NASint}i$，$K_{eNB}i$。其中，$K_{NASenc}i$，$K_{NASint}i$ 用户保护用户和 MME 之间的 NAS 信令，$K_{eNB}i$ 下发给 eNB，eNB 基于 $K_{eNB}i$ 生成 $K_{UPenc}i$，$K_{RRCint}i$ 和 $K_{RRCenc}i$。

[0104] 步骤 509 :MTC 设备基于 $K_{ASME}i$ 生成 $K_{NASenc}i$，$K_{NASint}i$，$K_{UPenc}i$，$K_{RRCint}i$ 和 $K_{RRCenc}i$ 对数据进行机密性、完整性保护。

[0105] 图 6 为本发明机器对机器的通信系统中基于组的认证系统的组成结构示意图，如图 6 所示，本发明机器对机器的通信系统中基于组的认证系统包括 MTC 设备 60、接入安全管理设备 61 以及鉴权中心 62，系统中还有其他网元，与现有技术中的网络结构相同，其中，所述鉴权中心 62，用于根据 MTC 设备所签约的组信息，生成组认证参数，并将所述组认证参数发送给所述接入安全管理设备 ;

[0106] 接入安全管理设备 61，用于根据生成的所述组认证参数，生成针对每个所述 MTC 设备的鉴权参数，并对该组中的 MTC 设备进行鉴权。

[0107] 进一步地，鉴权中心 62，用于预先配置 MTC 设备所属的组的组根密钥以及 MTC 设备的根密钥 ;根据收到的认证请求消息中携带的 MTC 设备标识，查询该 MTC 设备的签约信息，若该 MTC 设备拥有组签约，根据所述 MTC 设备所属组的组根密钥以及组标识生成相应的组认证向量 ;根据所述 MTC 设备的根密钥及 hash 算法，生成所述 MTC 设备的根密钥的哈希值。

[0108] 进一步地，所述组认证参数包括 :所述组认证向量、所述 MTC 设备根密钥的哈希值、所述 MTC 设备所属的签约的组及组成员信息。

[0109] 进一步地，接入安全管理设备 61，用于收到 MTC 设备附着请求或业务请求后，根据所述请求消息中携带的 MTC 设备标识，查询是否已存在所述 MTC 设备所属签约的组及所述签约的组的组认证参数；若不存在，向鉴权中心发起对所述 MTC 设备的认证请求；若存在，对所述 MTC 设备进行认证；

[0110] 进一步地，接入安全管理设备 61，用于生成随机数，根据所述组认证向量、所述 MTC 设备根密钥的哈希值、所述随机数，生成针对所述 MTC 设备的认证向量，对所述 MTC 设备进行认证。

[0111] 上述 ASME 为 VLR/SGSN，或 MME；所述鉴权中心为 HLR/AuC，或为 HSS。

[0112] 本领域技术人员应当理解，本领域技术人员应当理解，本发明的机器对机器的通信系统中基于组的认证系统是为实现前述的机器对机器的通信系统中基于组的认证方法而设计的，上述各网元的实现功能可参照前述方法的相关描述而理解。

[0113] 以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

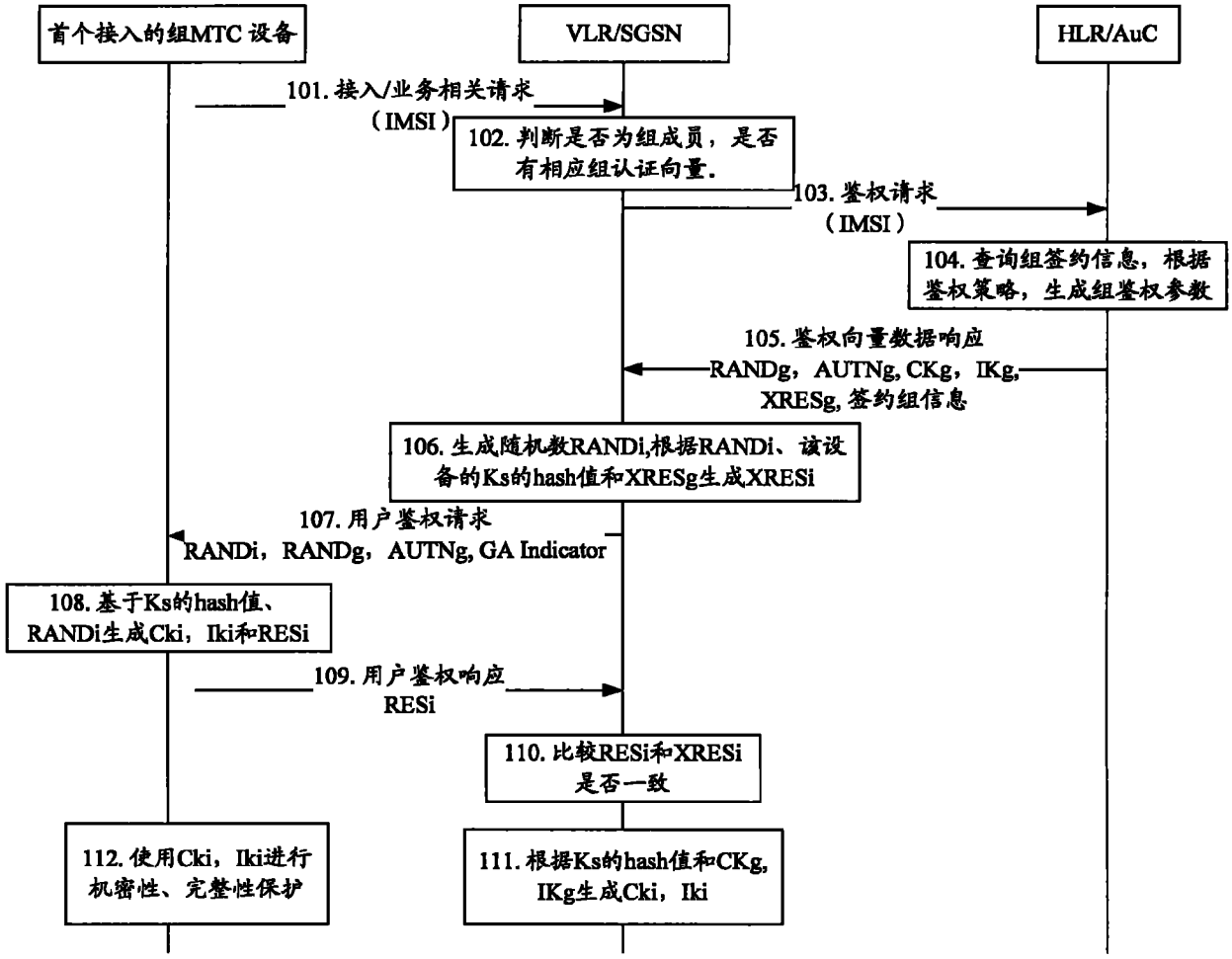

首个接入的组MTC 设备
VLR/SGSN
HLR/AuC
101. 接入/业务相关请求
（IMSI）
102. 判断是否为组成员，是否有相应组认证向量.
103. 鉴权请求
（IMSI）
104. 查询组签约信息，根据鉴权策略，生成组鉴权参数
105. 鉴权向量数据响应
RANDg，AUTNg, CKg，IKg,
XRESg, 签约组信息
106. 生成随机数RANDi,根据RANDi、该设备的Ks的hash值和XRESg生成XRESi
107. 用户鉴权请求
RANDi，RANDg，AUTNg, GA Indicator
108. 基于Ks的hash值、RANDi生成Cki，Iki和RESi
109. 用户鉴权响应
RESi
110. 比较RESi和XRESi是否一致
112. 使用Cki，Iki进行机密性、完整性保护
111. 根据Ks的hash值和CKg, IKg生成Cki，Iki

图 1

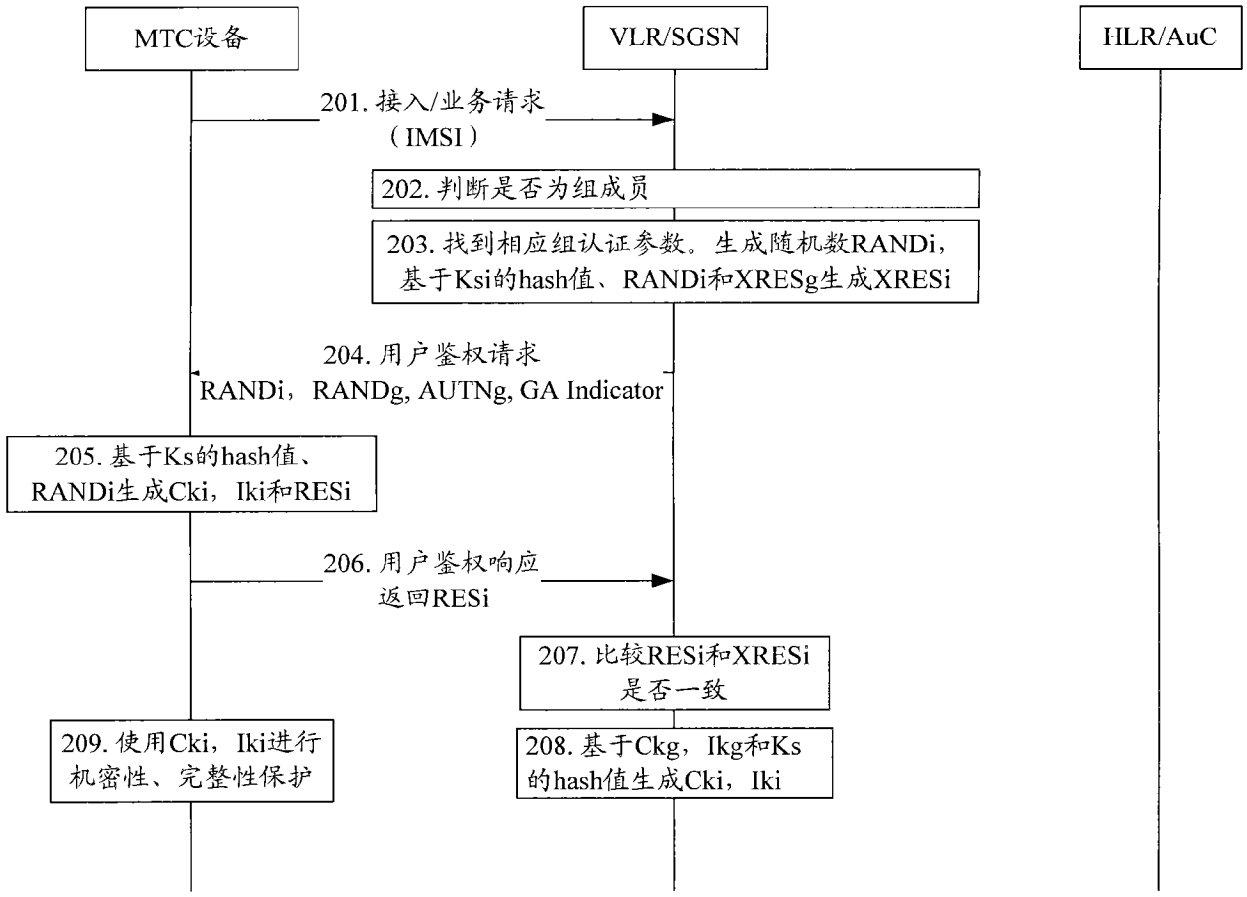

MTC设备
VLR/SGSN
HLR/AuC
201. 接入/业务请求
（IMSI）
202. 判断是否为组成员
203. 找到相应组认证参数。生成随机数RANDi，
基于Ksi的hash值、RANDi和XRESg生成XRESi
204. 用户鉴权请求
RANDi，RANDg, AUTNg, GA Indicator
205. 基于Ks的hash值、
RANDi生成Cki，Iki和RESi
206. 用户鉴权响应
返回RESi
207. 比较RESi和XRESi
是否一致
208. 基于Ckg，Ikg和Ks
的hash值生成Cki，Iki
209. 使用Cki，Iki进行
机密性、完整性保护

图 2

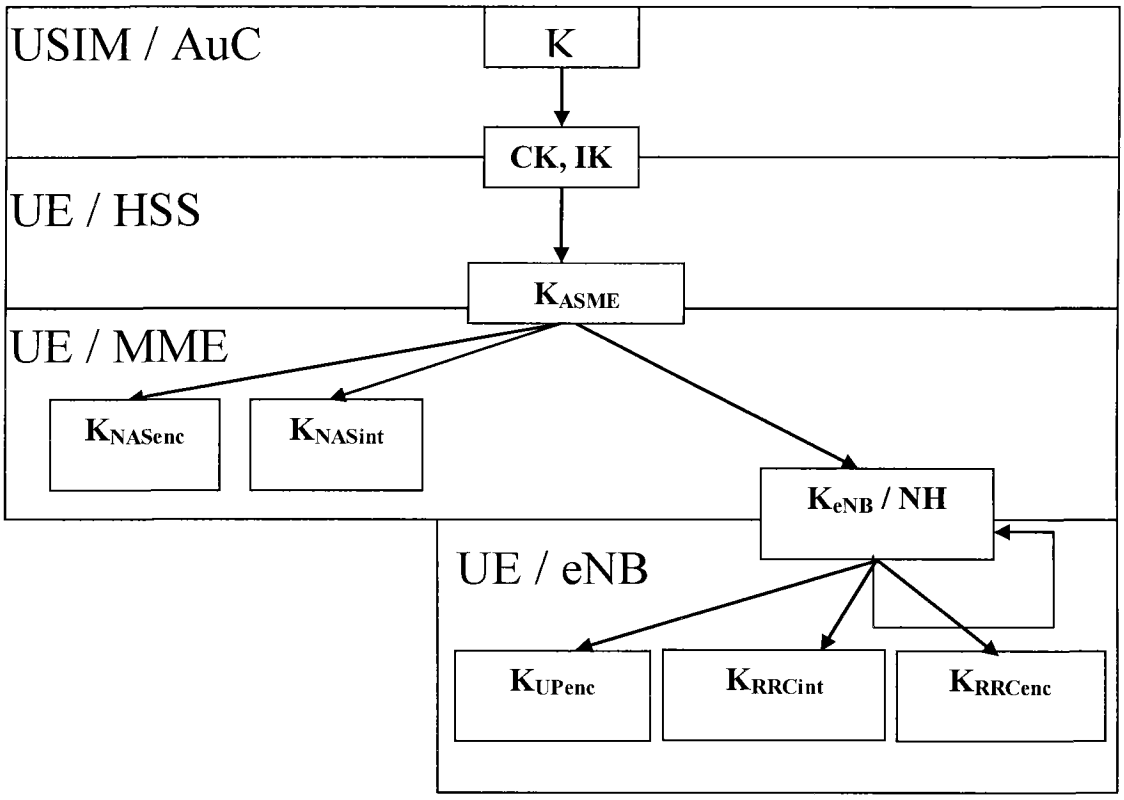

USIM / AuC
K
CK, IK
UE / HSS
KASME
UE / MME
KNASenc
KNASint
KeNB / NH
UE / eNB
KUPenc
KRRCint
KRRCenc

图 3

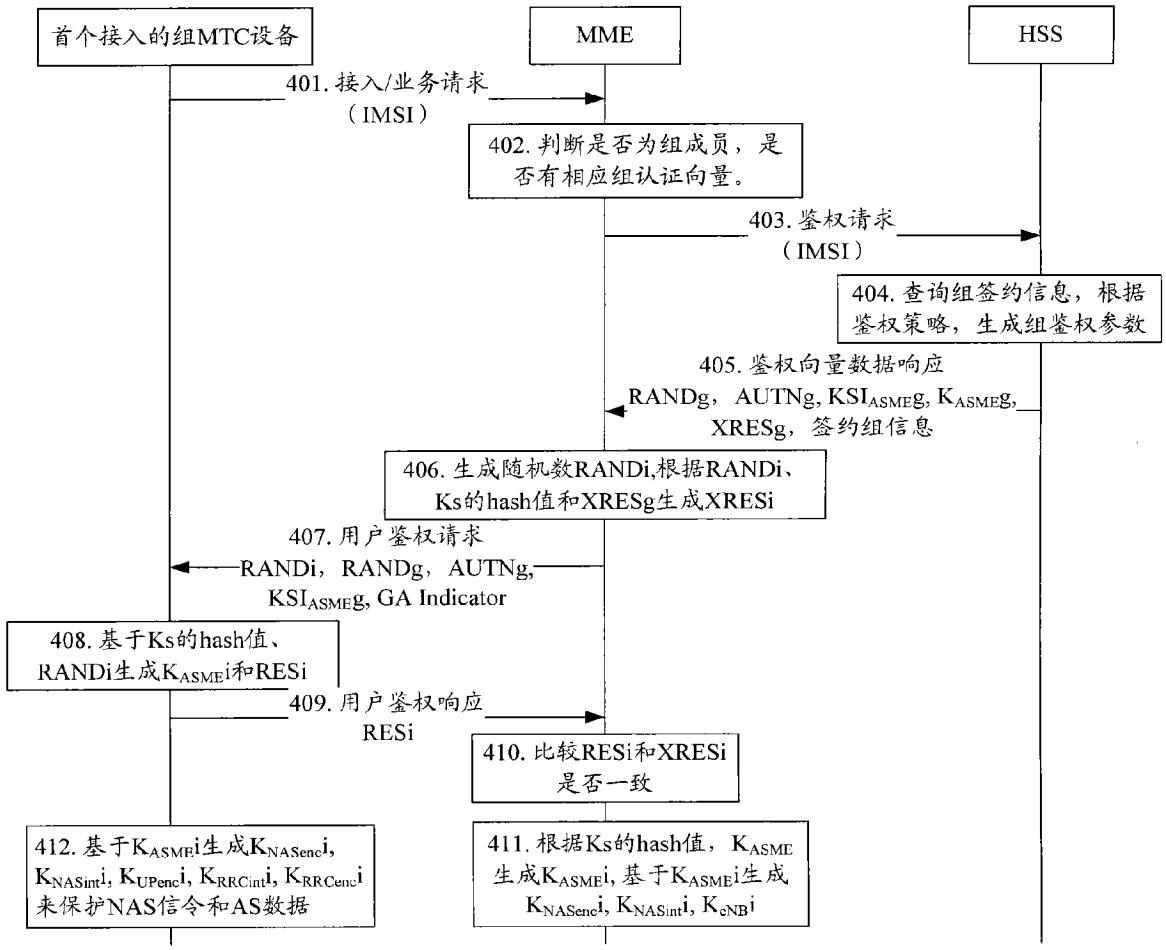

首个接入的组MTC设备
MME
HSS
401. 接入/业务请求
（IMSI）
402. 判断是否为组成员，是否有相应组认证向量。
403. 鉴权请求
（IMSI）
404. 查询组签约信息，根据鉴权策略，生成组鉴权参数
405. 鉴权向量数据响应
RANDg，AUTNg, KSIASMEg, KASMEg,
XRESg，签约组信息
406. 生成随机数RANDi,根据RANDi、Ks的hash值和XRESg生成XRESi
407. 用户鉴权请求
RANDi，RANDg，AUTNg,
KSIASMEg, GA Indicator
408. 基于Ks的hash值、RANDi生成KASMEi和RESi
409. 用户鉴权响应
RESi
410. 比较RESi和XRESi是否一致
412. 基于KASMEi生成KNASenci, KNASinti, KUPenci, KRRCinti, KRRCenci来保护NAS信令和AS数据
411. 根据Ks的hash值，KASME生成KASMEi，基于KASMEi生成KNASenci, KNASinti, KeNBi

图 4

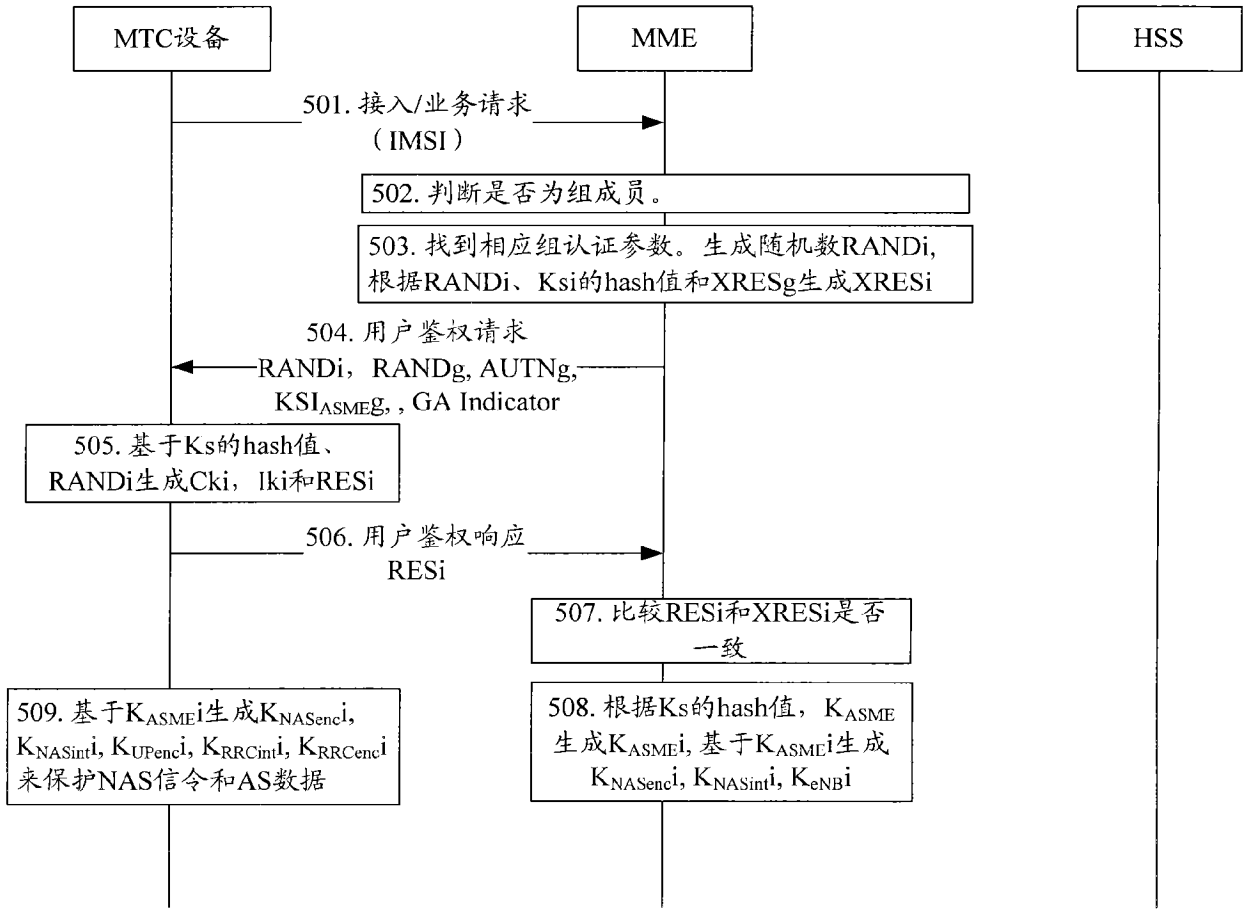

MTC设备
MME
HSS
501. 接入/业务请求
（IMSI）
502. 判断是否为组成员。
503. 找到相应组认证参数。生成随机数RANDi，
根据RANDi、Ksi的hash值和XRESg生成XRESi
504. 用户鉴权请求
RANDi，RANDg, AUTNg,
KSIASMEg, , GA Indicator
505. 基于Ks的hash值、
RANDi生成Cki，Iki和RESi
506. 用户鉴权响应
RESi
507. 比较RESi和XRESi是否
一致
509. 基于KASMEi生成KNASenci,
KNASinti, KUPenci, KRRCinti, KRRCenci
来保护NAS信令和AS数据
508. 根据Ks的hash值，KASME
生成KASMEi, 基于KASMEi生成
KNASenci, KNASinti, KeNBi

图 5

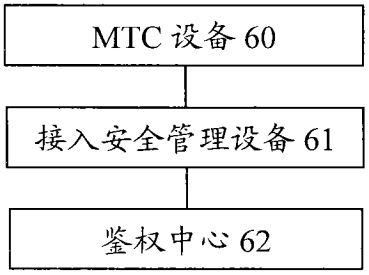

MTC 设备 60
接入安全管理设备 61
鉴权中心 62

图 6