(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102469455 B
(45)授权公告日 2016.04.13

(21)申请号 201010535847.1

(22)申请日 2010.11.08

(73)专利权人 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 余万涛

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 武晨燕 周义刚

(51)Int.Cl.
H04W 12/04(2009.01)
H04W 12/06(2009.01)
H04W 24/00(2009.01)

(56)对比文件

Samsung等.Contribution to TS 22.368 - Section 3.1 & 7.1.3 & 7.2.16.3: MTC Group.《3GPP TSG-SA1 #49 S1-100046》.2010, 正文第1-3页.

SA3.Living Document on "Security Aspects of Network Improvements for Machine-Type Communication.《S3GPP TSG-SA3#60 S3-100906》.2010, 正文第1-5页.

审查员 吴欣

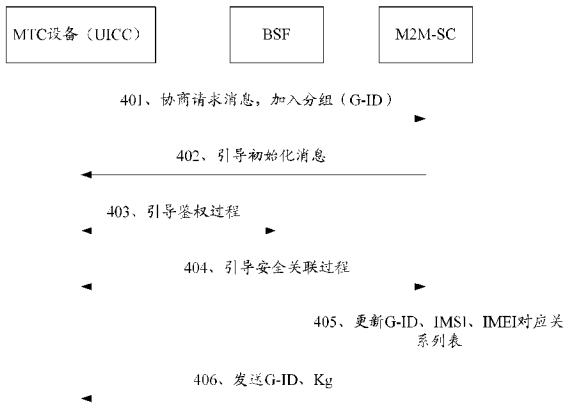
权利要求书2页 说明书6页 附图3页

(54)发明名称

基于通用引导架构的机器类通信设备分组管理方法及系统

(57)摘要

本发明公开了一种基于GBA的MTC设备分组管理方法,该方法应用于包含MTC设备、BSF及M2M-SC的系统中,该方法包括:当第一MTC设备与M2M-SC协商确定欲加入组标识为G-ID的MTC设备分组时,第一MTC设备与BSF及M2M-SC之间通过第一GBA过程,在第一MTC设备与M2M-SC之间建立第一会话密钥,M2M-SC将所述MTC设备分组的G-ID和组密钥Kg通过第一会话密钥加密后发送给第一MTC设备。采用本发明能够对MTC设备分组中的组成员进行安全管理。



CN 102469455 B

1. 一种基于通用引导架构的机器类通信设备分组管理方法，其特征在于，该方法应用于包含机器类通信 MTC 设备、引导服务器功能 BSF 及机器对机器业务中心 M2M-SC 的系统中，该方法包括：

当第一 MTC 设备与 M2M-SC 协商确定欲加入组标识为 G-ID 的 MTC 设备分组时，第一 MTC 设备与 BSF 之间进行引导鉴权过程，以确定用于第一 MTC 设备和 M2M-SC 之间通信的第一会话密钥；第一 MTC 设备与 M2M-SC 之间进行引导安全关联过程，在所述引导安全关联过程中，M2M-SC 从 BSF 获取所述第一会话密钥；

M2M-SC 将所述 MTC 设备分组的组标识 G-ID 和组密钥 Kg 通过第一会话密钥加密后发送给第一 MTC 设备；

其中，所述 G-ID 用于绑定 MTC 设备的用户身份及设备身份，组密钥 Kg 用于 MTC 设备分组的安全管理。

2. 根据权利要求 1 所述的基于通用引导架构的机器类通信设备分组管理方法，其特征在于，所述 MTC 设备分组由第二 MTC 设备创建，所述创建过程包括：

当第二 MTC 设备与 M2M-SC 协商确定欲创建所述 MTC 设备分组时，第二 MTC 设备与 BSF 及 M2M-SC 之间通过第二 GBA 过程，在第二 MTC 设备与 M2M-SC 之间建立第二会话密钥；

M2M-SC 创建所述 MTC 设备分组的组标识 G-ID 和组密钥 Kg，并将创建的 G-ID 和 Kg 通过所述第二会话密钥加密后发送给第二 MTC 设备。

3. 根据权利要求 2 所述的基于通用引导架构的机器类通信设备分组管理方法，其特征在于，在创建所述 G-ID 和 Kg 之后，所述方法还包括：M2M-SC 创建所述 G-ID 与 MTC 设备的用户身份及设备身份的对应关系列表，该对应关系列表中包含所述 G-ID 与所述第二 MTC 设备的用户身份及设备身份的对应关系；

在 M2M-SC 获取所述第一会话密钥之后，所述方法还包括：M2M-SC 更新所述对应关系列表。

4. 根据权利要求 3 所述的基于通用引导架构的机器类通信设备分组管理方法，其特征在于，在更新所述对应关系列表之前，所述方法还包括：M2M-SC 向第二 MTC 设备发送第一 MTC 设备的加入请求，第二 MTC 设备根据收到的加入请求决定允许第一 MTC 设备加入后，将决定结果返回给 M2M-SC，M2M-SC 根据决定结果，将第一 MTC 设备的用户身份及设备身份的对应关系添加到 G-ID 与 MTC 设备的用户身份及设备身份的对应关系列表中，以更新所述对应关系列表。

5. 根据权利要求 1 所述的基于通用引导架构的机器类通信设备分组管理方法，其特征在于，所述方法还包括：所述第一 MTC 设备将收到的 G-ID 和 Kg 通过所述第一会话密钥解密后存储在第一 MTC 设备中或第一 MTC 设备的通用集成电路卡 UICC 中。

6. 根据权利要求 2 所述的基于通用引导架构的机器类通信设备分组管理方法，其特征在于，所述方法还包括：所述第二 MTC 设备将收到的 G-ID 和 Kg 通过所述第二会话密钥解密后存储在第二 MTC 设备中或第二 MTC 设备的 UICC 中。

7. 根据权利要求 1 所述的基于通用引导架构的机器类通信设备分组管理方法，其特征在于，所述第一 MTC 设备与 M2M-SC 协商确定欲加入组标识为 G-ID 的 MTC 设备分组的过程包括：

第一 MTC 设备向 M2M-SC 发送协商请求消息，该协商请求消息中携带有加入组标识为

G-ID 的 MTC 设备分组的请求；

M2M-SC 向第一 MTC 设备发送引导初始化消息。

8. 根据权利要求 2 所述的基于通用引导架构的机器类通信设备分组管理方法，其特征在于，所述第二 MTC 设备与 M2M-SC 协商确定欲创建 MTC 设备分组的过程包括：

第二 MTC 设备向 M2M-SC 发送协商请求消息，该协商请求消息中携带有创建 MTC 设备分组的请求；

M2M-SC 向第二 MTC 设备发送引导初始化消息。

9. 一种基于通用引导架构的机器类通信设备分组管理系统，其特征在于，该系统包括：第一 MTC 设备、BSF 及 M2M-SC；其中，

第一 MTC 设备，用于与 M2M-SC 协商确定欲加入组标识为 G-ID 的 MTC 设备分组时，与 BSF 之间进行引导鉴权过程，以确定用于第一 MTC 设备和 M2M-SC 之间通信的第一会话密钥；

M2M-SC，用于与 M2M-SC 之间进行引导安全关联过程，在所述引导安全关联过程中，从 BSF 获取所述第一会话密钥；还用于将所述 MTC 设备分组的组标识 G-ID 和组密钥 Kg 通过第一会话密钥加密后发送给第一 MTC 设备；其中，所述 G-ID 用于绑定 MTC 设备的用户身份及设备身份，组密钥 Kg 用于 MTC 设备分组的安全管理。

10. 根据权利要求 9 所述的基于通用引导架构的机器类通信设备分组管理系统，其特征在于，所述系统还包括：创建所述 MTC 设备分组的第二 MTC 设备；其中，

第二 MTC 设备，用于与 M2M-SC 协商确定欲创建所述 MTC 设备分组时，与 BSF 及 M2M-SC 之间通过第二 GBA 过程，在第二 MTC 设备与 M2M-SC 之间建立第二会话密钥；

M2M-SC，还用于创建所述 MTC 设备分组的组标识 G-ID 和组密钥 Kg，并将创建的 G-ID 和 Kg 通过所述第二会话密钥加密后发送给第二 MTC 设备。

11. 根据权利要求 10 所述的基于通用引导架构的机器类通信设备分组管理系统，其特征在于，所述 M2M-SC，还用于在创建所述 G-ID 和 Kg 之后，创建所述 G-ID 与 MTC 设备的用户身份及设备身份的对应关系列表，该对应关系列表中包含所述 G-ID 与所述第二 MTC 设备的用户身份及设备身份的对应关系；还用于在获取所述第一会话密钥之后，更新所述对应关系列表。

基于通用引导架构的机器类通信设备分组管理方法及系统

技术领域

[0001] 本发明涉及移动通信系统和MTC(Machine Type Communication,机器类通信）技术,尤其涉及一种基于通用引导架构的MTC设备分组管理方法及系统。

背景技术

[0002] 机器类通信是指应用无线通信技术,实现机器与机器、机器与人之间的数据通信和交流的一系列技术及其组合的总称。M2M(在3GPP里称MTC)涉及两个层面:第一个是机器本身,在嵌入式领域称为智能设备;第二个是机器和机器之间的连接,通过网络将机器连接在一起。MTC的应用范围非常广泛,例如智能测量、远程监控、跟踪、医疗等,这使得人类生活更加智能化。与传统的人与人之间的通信相比,MTC设备数量众多、应用领域广泛,因此具有巨大的市场前景。

[0003] 在机器类通信中,远距离连接技术主要包括全球移动通信系统(GSM)、通用分组无线业务(GPRS)、通用移动电话通信系统(UMTS)等;近距离连接技术主要包括802.11b/g、蓝牙、Zigbee、射频识别(RFID)等。由于MTC整合了无线通信技术和信息技术,且可用于双向通信,如远距离收集信息、设置参数并发送指令,因此能够实现不同的应用方案,如安全监测、自动售货、货物跟踪等。由此可见,几乎所有日常生活中涉及到的设备都有可能成为潜在的服务对象。

[0004] GBA(Generic Bootstrapping Architecture,通用引导架构）定义了一种在终端和服务器之间通用的密钥协商机制。如图1所示,GBA模型中的主要网元有:

[0005] 1)UE(用户设备）:UE是终端设备和(U)SIM卡的总称;这里的终端可以是插卡的移动终端（如移动电话),也可以是插卡的固定终端（如机顶盒）;本文中,(U)SIM卡指SIM卡或USIM(全球用户识别模块）卡;

[0006] 2)NAF(Network Application Function,网络应用功能）:即应用服务器,用于实现应用的业务逻辑功能,在完成对终端的认证后为终端提供业务服务;

[0007] 3)BSF(Bootstrapping Server Function,引导服务器功能）:BSF是GBA的核心网元,BSF和UE通过AKA(Authentication and Key Agreement,认证与密钥协商）协议实现认证,并协商出后续用于UE和NAF之间通信的会话密钥,此外,BSF能够根据本地策略设定会话密钥的生命期;

[0008] 4)HSS(Home Subscriber System,归属签约系统）:存储终端(U)SIM卡中的鉴权数据,如SIM(用户识别模块）卡中的Ki等;

[0009] 5)SLF(Subscriber Locator Function,签约位置功能）:BSF通过查询SLF获得存储相关用户数据的HSS的名称。在单一HSS环境中并不需要SLF;另外,当BSF配置成使用预先指定的HSS时,也不需要SLF。

[0010] 在移动通信系统中引入MTC设备后,由于MTC设备数量众多,为了降低网络负载,节省网络资源,需要对MTC设备以组的方式进行管理优化,这样,MTC设备就可以按组的方式进行控制、管理及计费等,从而适应运营商的需求。目前,提出了MTC设备可以按照所在

区域是否相同、或者是否具有相同的MTC特征、或者是否属于相同的MTC用户进行分组。另外，在对MTC设备进行分组后，需要对组信息进行安全保护，否则，一个攻击者可能伪装成组成员获得组信息。

[0011] 目前虽然提出了MTC设备按区域、MTC特征或MTC用户进行分组的建议，但是还没有基于这些建议的具体实现方案，因此如何实现MTC设备分组，并对MTC设备分组中的MTC设备进行安全管理是需要解决的问题。

发明内容

[0012] 有鉴于此，本发明的主要目的在于提供一种基于GBA的MTC设备分组管理方法及系统，能够对MTC设备分组中的MTC设备进行安全管理。

[0013] 为达到上述目的，本发明的技术方案是这样实现的：

[0014] 一种基于GBA的MTC设备分组管理方法，该方法应用于包含MTC设备、BSF及M2M-SC的系统中，该方法包括：

[0015] 当第一MTC设备与M2M-SC协商确定欲加入组标识为G-ID的MTC设备分组时，第一MTC设备与BSF及M2M-SC之间通过第一GBA过程，在第一MTC设备与M2M-SC之间建立第一会话密钥；

[0016] M2M-SC将所述MTC设备分组的组标识G-ID和组密钥Kg通过第一会话密钥加密后发送给第一MTC设备。

[0017] 进一步地，所述MTC设备分组由第二MTC设备创建，所述创建过程包括：

[0018] 当第二MTC设备与M2M-SC协商确定欲创建所述MTC设备分组时，第二MTC设备与BSF及M2M-SC之间通过第二GBA过程，在第二MTC设备与M2M-SC之间建立第二会话密钥；

[0019] M2M-SC创建所述MTC设备分组的组标识G-ID和组密钥Kg，并将创建的G-ID和Kg通过所述第二会话密钥加密后发送给第二MTC设备。

[0020] 进一步地，在创建所述G-ID和Kg之后，所述方法还包括：M2M-SC创建所述G-ID与MTC设备的用户身份及设备身份的对应关系列表，该对应关系列表中包含所述G-ID与所述第二MTC设备的用户身份及设备身份的对应关系；

[0021] 在M2M-SC获取所述第一会话密钥之后，所述方法还包括：M2M-SC更新所述对应关系列表。

[0022] 进一步地，在更新所述对应关系列表之前，所述方法还包括：M2M-SC向第二MTC设备发送第一MTC设备的加入请求，第二MTC设备根据收到的加入请求决定允许第一MTC设备加入后，将决定结果返回给M2M-SC，M2M-SC根据决定结果，将第一MTC设备的用户身份及设备身份的对应关系添加到G-ID与MTC设备的用户身份及设备身份的对应关系列表中，以更新所述对应关系列表。

[0023] 进一步地，所述方法还包括：所述第一MTC设备将收到的G-ID和Kg通过所述第一会话密钥解密后存储在第一MTC设备中或第一MTC设备的通用集成电路卡UICC中。

[0024] 进一步地，所述方法还包括：所述第二MTC设备将收到的G-ID和Kg通过所述第二会话密钥解密后存储在第二MTC设备中或第二MTC设备的UICC中。

[0025] 进一步地，所述第一MTC设备与M2M-SC协商确定欲加入组标识为G-ID的MTC设备分组的过程包括：

[0026] 第一 MTC 设备向 M2M-SC 发送协商请求消息，该协商请求消息中携带有加入组标识为 G-ID 的 MTC 设备分组的请求；

[0027] M2M-SC 向第一 MTC 设备发送引导初始化消息。

[0028] 进一步地，所述第二 MTC 设备与 M2M-SC 协商确定欲创建 MTC 设备分组的过程包括：

[0029] 第二 MTC 设备向 M2M-SC 发送协商请求消息，该协商请求消息中携带有创建 MTC 设备分组的请求；

[0030] M2M-SC 向第二 MTC 设备发送引导初始化消息。

[0031] 一种基于 GBA 的设备分组管理系统，其特征在于，该系统包括：第一 MTC 设备、BSF 及 M2M-SC；其中，

[0032] 第一 MTC 设备，用于与 M2M-SC 协商确定欲加入组标识为 G-ID 的 MTC 设备分组时，与 BSF 及 M2M-SC 之间通过第一 GBA 过程，在第一 MTC 设备与 M2M-SC 之间建立第一会话密钥；

[0033] M2M-SC，用于将所述 MTC 设备分组的组标识 G-ID 和组密钥 Kg 通过第一会话密钥加密后发送给第一 MTC 设备。

[0034] 进一步地，所述系统还包括：创建所述 MTC 设备分组的第二 MTC 设备；其中，

[0035] 第二 MTC 设备，用于与 M2M-SC 协商确定欲创建所述 MTC 设备分组时，与 BSF 及 M2M-SC 之间通过第二 GBA 过程，在第二 MTC 设备与 M2M-SC 之间建立第二会话密钥；

[0036] M2M-SC，还用于创建所述 MTC 设备分组的组标识 G-ID 和组密钥 Kg，并将创建的 G-ID 和 Kg 通过所述第二会话密钥加密后发送给第二 MTC 设备。

[0037] 进一步地，所述 M2M-SC，还用于在创建所述 G-ID 和 Kg 之后，创建所述 G-ID 与 MTC 设备的用户身份及设备身份的对应关系列表，该对应关系列表中包含所述 G-ID 与所述第二 MTC 设备的用户身份及设备身份的对应关系；还用于在获取所述第一会话密钥之后，更新所述对应关系列表。

[0038] 由以上技术方案可以看出，本发明提出了一种切实可行的 MTC 设备分组方法，并且由于 M2M-SC 与 MTC 设备分组中的组成员各自拥有与 MTC 设备分组唯一对应的 G-ID 和 Kg，因此能够对 MTC 设备分组中的组成员进行安全管理；即使一个攻击者伪装成组成员，由于其无法获得 Kg，因此也就无法获得组信息。

附图说明

[0039] 图 1 为现有技术中 GBA 模型示意图；

[0040] 图 2 为本发明中基于 GBA 的 MTC 设备分组管理系统的示意图；

[0041] 图 3 为本发明创建 MTC 设备分组的流程示意图；

[0042] 图 4 为本发明 MTC 设备加入 MTC 设备分组的流程示意图。

具体实施方式

[0043] 以下结合附图对本发明的技术方案作详细说明。

[0044] 本发明基于 GBA 的 MTC 设备分组管理方法应用于如图 2 所示的系统，该系统包括 MTC 设备、BSF 及 M2M-SC(Machine to Machine Service Center，M2M 业务中心)。本

发明中，MTC 设备指移动通信网络中用于机器到机器通信的设备，且该 MTC 设备安装有 UICC(Universal Integrated Circuit Card，通用集成电路卡）；M2M-SC 具有网络应用功能 (NAF)、组成员管理功能等。

[0045] 基于 GBA 的 MTC 设备分组管理方法包括创建 MTC 设备分组及 MTC 设备加入 MTC 设备分组两个方面。

[0046] 如图 3 所示，本发明创建 MTC 设备分组的流程包括：

[0047] 步骤 301，MTC 设备向 M2M-SC 发送协商请求消息，该协商请求消息中携带有创建 MTC 设备分组的请求；

[0048] 步骤 302，M2M-SC 向 MTC 设备发送引导初始化消息；

[0049] 步骤 301-302 主要涉及的是 MTC 设备与 M2M-SC 协商确定欲创建 MTC 设备分组；

[0050] 步骤 303，MTC 设备与 BSF 之间进行引导鉴权过程，通过该引导鉴权过程，MTC 设备和 BSF 确定后续用于该 MTC 设备和 M2M-SC 之间通信的会话密钥（如 Ks-NAF）；

[0051] 步骤 304，MTC 设备与 M2M-SC 之间进行引导安全关联过程，在该引导安全关联过程中，M2M-SC 从 BSF 获取与 MTC 设备通信的会话密钥，即步骤 303 中确定的会话密钥；

[0052] 步骤 303-304 主要涉及的是 MTC 设备与 BSF 及 M2M-SC 之间通过 GBA 过程，在 MTC 设备与 M2M-SC 之间建立会话密钥；

[0053] 步骤 305，在 M2M-SC 获取会话密钥后，M2M-SC 根据创建 MTC 设备分组的请求信息，创建一个 G-ID(Group Identifier，组标识）和组密钥 Kg，并创建一个 G-ID 与 MTC 设备的用户身份（如 IMSI，国际移动用户识别码）及设备身份（如 IMEI，国际移动设备识别码）的对应关系列表，该对应关系列表一开始只包含 G-ID 与创建分组的 MTC 设备的用户身份及设备身份的对应关系，且该对应关系列表由 M2M-SC 管理和维护；

[0054] 其中，G-ID 用于绑定 MTC 设备的用户身份及设备身份，组密钥 Kg 用于 MTC 设备分组的安全管理；G-ID 是唯一的，可以作为 MTC 设备与 M2M-SC 之间协议的组密钥身份（即 G-ID 与 Kg 一一对应的）；

[0055] 步骤 306，M2M-SC 将创建的 G-ID 和 Kg 通过步骤 304 获取的会话密钥加密后发送给 MTC 设备。

[0056] MTC 设备用步骤 303 中确定的会话密钥对 G-ID 和 Kg 解密后再进行存储。如果上述引导过程（步骤 301-304）采用的是 GBA-ME，即引导过程在移动设备 (ME) 上进行，则可将 G-ID 和 Kg 存储在 MTC 设备中；如果上述引导过程采用的是 GBA-U，即引导过程在 UICC 上进行，则可将 G-ID 和 Kg 存储在 MTC 设备的 UICC 中。引导过程的具体细节可以参考现有的相关协议，在此不做详细描述。

[0057] 由上述流程可以看出，当一个 MTC 设备分组的 G-ID 创建后，一个基于该 G-ID 的 MTC 设备分组也就确定了。

[0058] 如图 4 所示，本发明 MTC 设备加入 MTC 设备分组的流程包括：

[0059] 步骤 401，MTC 设备向 M2M-SC 发送协商请求消息，该协商请求消息中携带有加入组标识为 G-ID 的 MTC 设备分组的请求；

[0060] 这里，MTC 设备如何获取 MTC 设备分组的 G-ID 不是本发明的重点，在此不做描述；

[0061] 步骤 402，M2M-SC 向 MTC 设备发送引导初始化消息；

[0062] 步骤 401-402 主要涉及的是 MTC 设备与 M2M-SC 协商确定欲加入 MTC 设备分组；

[0063] 步骤 403，MTC 设备与 BSF 之间进行引导鉴权过程，通过该引导鉴权过程，MTC 设备和 BSF 确定后续用于该 MTC 设备和 M2M-SC 之间通信的会话密钥（如 Ks-NAF）；

[0064] 步骤 404，MTC 设备与 M2M-SC 之间进行引导安全关联过程，在该引导安全关联过程中，M2M-SC 从 BSF 获取与 MTC 设备通信的会话密钥，即步骤 403 中确定的会话密钥；

[0065] 步骤 403-404 主要涉及的是 MTC 设备与 BSF 及 M2M-SC 之间通过 GBA 过程，在 MTC 设备与 M2M-SC 之间建立会话密钥；

[0066] 步骤 405，在 M2M-SC 获取会话密钥后，M2M-SC 根据加入 MTC 设备分组的请求信息，更新 G-ID 与 MTC 设备的用户身份及设备身份的对应关系列表，即在已有的对应关系列表中增加 G-ID 与新加入的 MTC 设备的用户身份（如 IMSI）及设备身份（如 IMEI）的对应关系；

[0067] 步骤 406，M2M-SC 将该 MTC 设备分组的 G-ID 和 Kg 通过步骤 404 获取的会话密钥加密后发送给 MTC 设备。

[0068] MTC 设备用步骤 403 中确定的会话密钥对 G-ID 和 Kg 解密后再进行存储。如果上述引导过程（步骤 401-404）采用的是 GBA-ME，则可将 G-ID 和 Kg 存储在 MTC 设备中；如果上述引导过程采用的是 GBA-U，则可将 G-ID 和 Kg 存储在 MTC 设备的 UICC 中。引导过程的具体细节可以参考现有的相关协议，在此不做详细描述。

[0069] 在步骤 405 之前，MTC 设备加入 MTC 设备分组的流程还包括：

[0070] M2M-SC 向创建 MTC 设备分组的 MTC 设备发送欲加入的 MTC 设备的加入请求，加入请求中携带有欲加入的 MTC 设备的信息（如身份标识）；

[0071] 创建 MTC 设备分组的 MTC 设备根据加入请求中欲加入的 MTC 设备的信息，决定是否允许其加入，并将决定结果返回给 M2M-SC，M2M-SC 根据决定结果启动或终止加入过程。

[0072] 在本发明中，一个 MTC 设备可以创建多个 MTC 设备分组，或者仅可以创建一个 MTC 设备分组。一个 MTC 设备可以加入多个 MTC 设备分组，或者仅可以加入一个 MTC 设备分组。一个 MTC 设备在加入一个 MTC 设备分组后，还可以创建新的 MTC 设备分组。一个 MTC 设备在创建一个 MTC 设备分组后，还可以加入其他的 MTC 设备分组。

[0073] 另外，如果不需要对 MTC 设备进行分组管理，则 MTC 设备按照通常的 GBA 过程完成 MTC 设备与 M2M-SC 之间的认证。

[0074] 为实现上述方法，本发明还提供了一种基于 GBA 的 MTC 设备分组管理系统，该系统包括：第一 MTC 设备、BSF 及 M2M-SC；其中，

[0075] 第一 MTC 设备，用于与 M2M-SC 协商确定欲加入组标识为 G-ID 的 MTC 设备分组时，与 BSF 及 M2M-SC 之间通过第一 GBA 过程，在第一 MTC 设备与 M2M-SC 之间建立第一会话密钥；

[0076] M2M-SC，用于将所述 MTC 设备分组的组标识 G-ID 和组密钥 Kg 通过第一会话密钥加密后发送给第一 MTC 设备。

[0077] 所述系统还包括：创建所述 MTC 设备分组的第二 MTC 设备；其中，

[0078] 第二 MTC 设备，用于与 M2M-SC 协商确定欲创建所述 MTC 设备分组时，与 BSF 及 M2M-SC 之间通过第二 GBA 过程，在第二 MTC 设备与 M2M-SC 之间建立第二会话密钥；

[0079] M2M-SC，还用于创建所述 G-ID 和 Kg，并将创建的 G-ID 和 Kg 通过所述第二会话密钥加密后发送给第二 MTC 设备。

[0080] 所述 M2M-SC，还用于在创建所述 G-ID 和 Kg 之后，创建所述 G-ID 与 MTC 设备的用

户身份及设备身份的对应关系列表，该对应关系列表中包含所述G-ID与所述第二MTC设备的用户身份及设备身份的对应关系；还用于在获取所述第一会话密钥之后，更新所述对应关系列表。

[0081] 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。

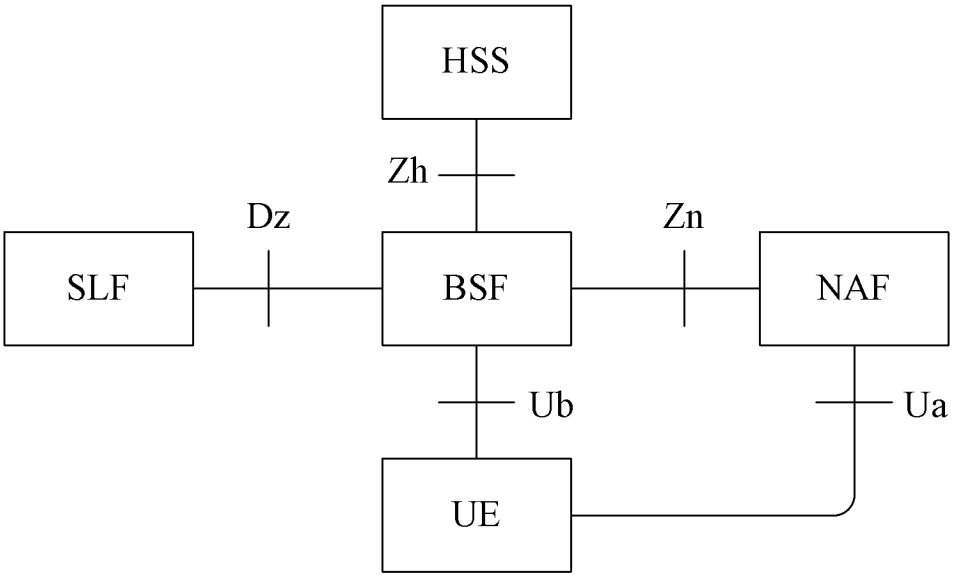


图 1

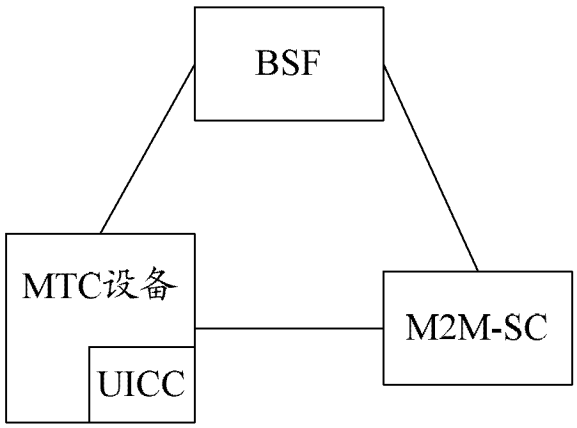


图 2

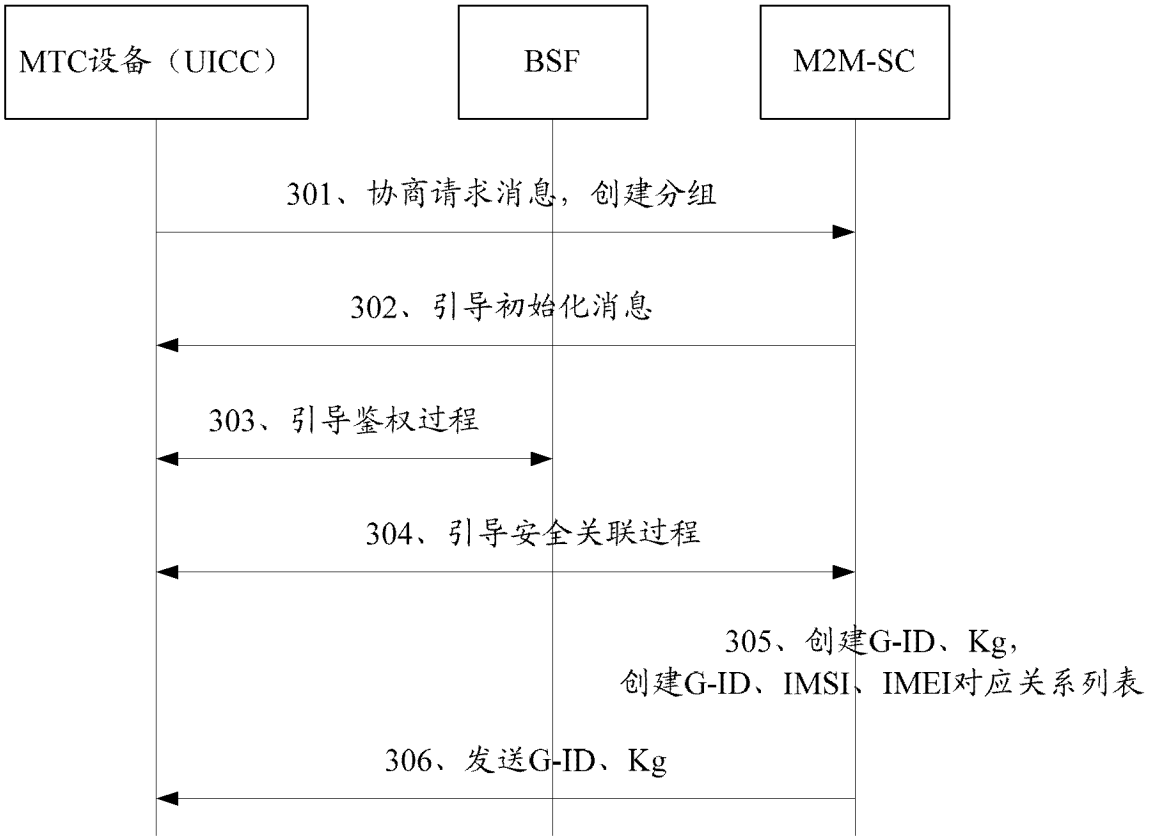

MTC设备（UICC）
BSF
M2M-SC
301、协商请求消息，创建分组
302、引导初始化消息
303、引导鉴权过程
304、引导安全关联过程
305、创建G-ID、Kg，
创建G-ID、IMSI、IMEI对应关系列表
306、发送G-ID、Kg

图 3

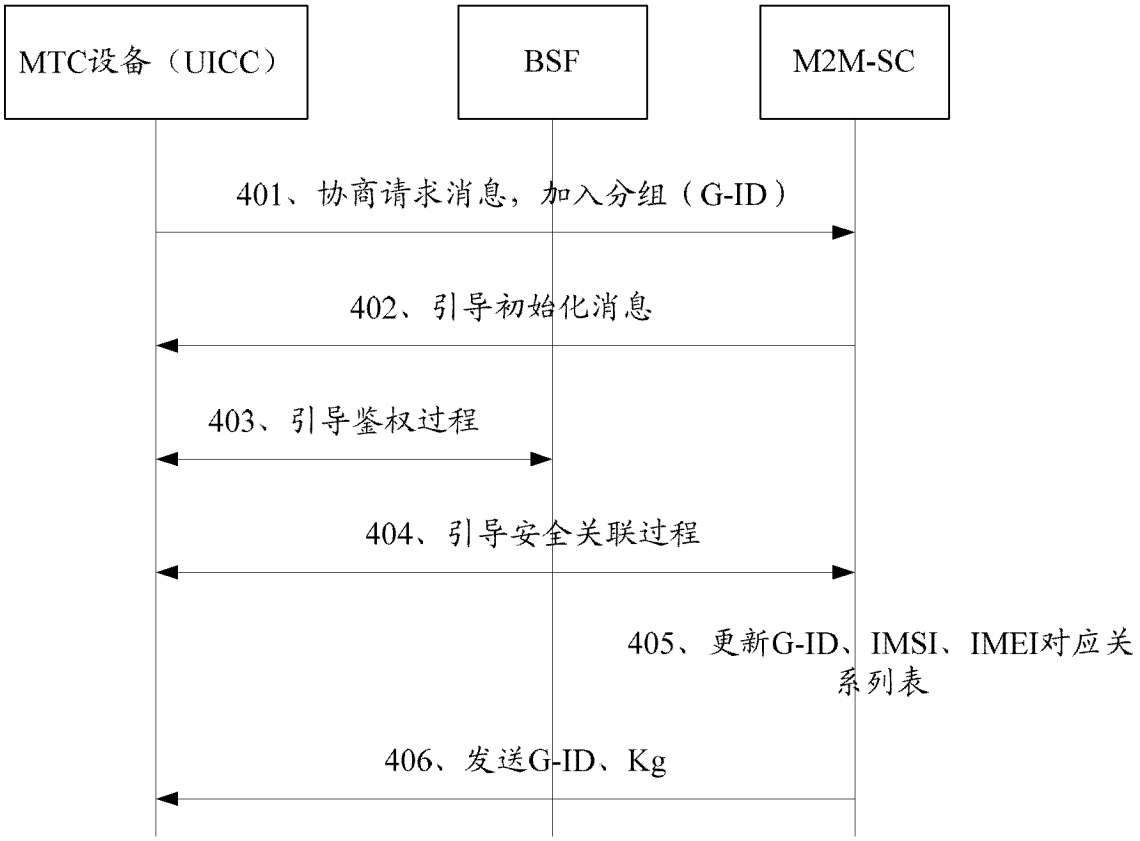

MTC设备（UICC）
BSF
M2M-SC
401、协商请求消息，加入分组（G-ID）
402、引导初始化消息
403、引导鉴权过程
404、引导安全关联过程
405、更新G-ID、IMSI、IMEI对应关系列表
406、发送G-ID、Kg

图 4