(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
2012 年 5 月 18 日 (18.05.2012)

PCT

(10) 国际公布号
WO 2012/062077 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2011/071938

(22) 国际申请日: 2011 年 3 月 17 日 (17.03.2011)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201010535847.1 2010 年 11 月 8 日 (08.11.2010) CN

(71) 申请人 (对除美国外的所有指定国): **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; 及

(75) 发明人/申请人 (仅对美国): **余万涛 (YU, Wantao)** [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)。

(74) 代理人: **北京派特恩知识产权代理事务所(普通合伙) (CHINA PAT INTELLECTUAL PROPERTY OFFICE)**; 中国北京市海淀区知春路 113 号 0717 室, Beijing 100086 (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,

[见续页]

(54) Title: MACHINE TYPE COMMUNICATION DEVICE GROUP MANAGEMENT METHOD AND SYSTEM BASED ON GENERIC BOOTSTRAPPING ARCHITECTURE

(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

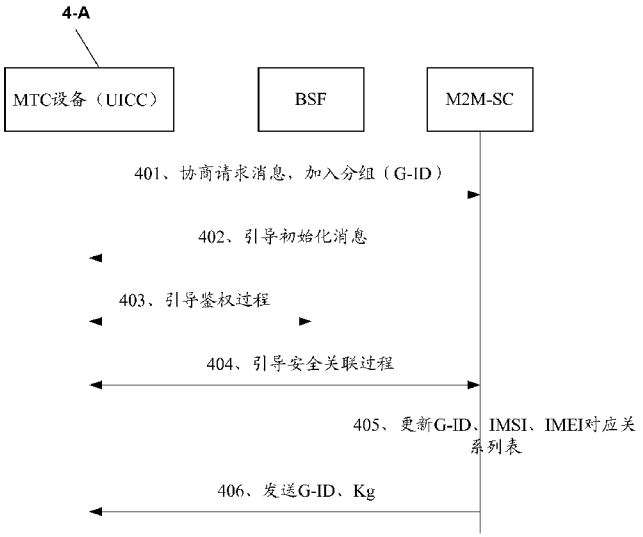

图 4 /FIG. 4

401 NEGOTIATION REQUEST MESSAGE, JOINING THE GROUP (G-ID)
402 BOOTSTRAPPING INITIALIZATION MESSAGE
403 BOOTSTRAPPING AUTHENTICATION PROCESS
404 BOOTSTRAPPING SECURITY ASSOCIATION PROCESS
405 UPDATING THE CORRESPONDING RELATIONSHIP LIST OF THE G-ID THE IMSI, AND THE IMEI
406 TRANSMITTING THE G-ID AND THE KG
4-A MTC DEVICE (UICC)

(57) Abstract: The present invention discloses a Machine Type Communication (MTC) device group management method based on Generic Bootstrapping Architecture (GBA). The method is applied in a system including the MTC device, a Bootstrapping Sever Function (BSF), and a Machine to Machine Service Center (M2M-SC). The method includes the following steps: when a first MTC device negotiates with the M2M-SC and determines to join the MTC device group with a group identifier G-ID, a first session key is established between the first MTC device and the M2M-SC via a first GBA process between the first MTC device, the BSF and the M2M-SC; the M2M-SC encrypts, with the first session key, the G-ID of the MTC device group and the group key Kg of the MTC device group and then transmits them to the first MTC device. With the present invention, a security management can be performed on group members of the MTC device group.

[见续页]

WO 2012/062077 A1

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))。

(57) 摘要:

本发明公开了一种基于通用引导架构 GBA 的机器类通信 MTC 设备分组管理方法，该方法应用于包含 MTC 设备、引导服务器功能 BSF 及机器到机器业务中心 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，通过第一 MTC 设备与 BSF 及 M2M-SC 之间的第一 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。

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

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

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。

在机器类通信中，远距离连接技术主要包括 GSM（全球移动通信系统）、GPRS（通用分组无线业务）、UMTS（通用移动电话通信系统）等；近距离连接技术主要包括 802.11b/g、蓝牙、Zigbee、RFID（射频识别）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。

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：

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；

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；

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；

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；

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。

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。

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

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。

为达到上述目的，本发明的技术方案是这样实现的:

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。

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:

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。

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;

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。

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。

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。

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。

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：

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。

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：

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。

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，

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；

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。

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，

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。

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。

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

图 1 为现有技术中 GBA 模型示意图；

图 2 为本发明中基于 GBA 的 MTC 设备分组管理系统的示意图；

图 3 为本发明创建 MTC 设备分组的流程示意图;

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

以下结合附图对本发明的技术方案作详细说明。

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。

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。

如图 3 所示，本发明创建 MTC 设备分组的流程包括:

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;

步骤 302，M2M-SC 向 MTC 设备发送引导初始化消息;

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;

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）;

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;

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；

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；

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）；

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。

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。

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。

如图 4 所示，本发明 MTC 设备加入 MTC 设备分组的流程包括：

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；

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；

步骤 402，M2M-SC 向 MTC 设备发送引导初始化消息；

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；

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）；

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；

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；

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；

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。

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。

在步骤 405 之前，MTC 设备加入 MTC 设备分组的流程还包括：

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）；

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。

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。

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。

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，

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；

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。

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 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。

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。

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。

权利要求书

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 及 M2M-SC 之间通过第一通用引导架构 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。

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 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 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，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。

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。

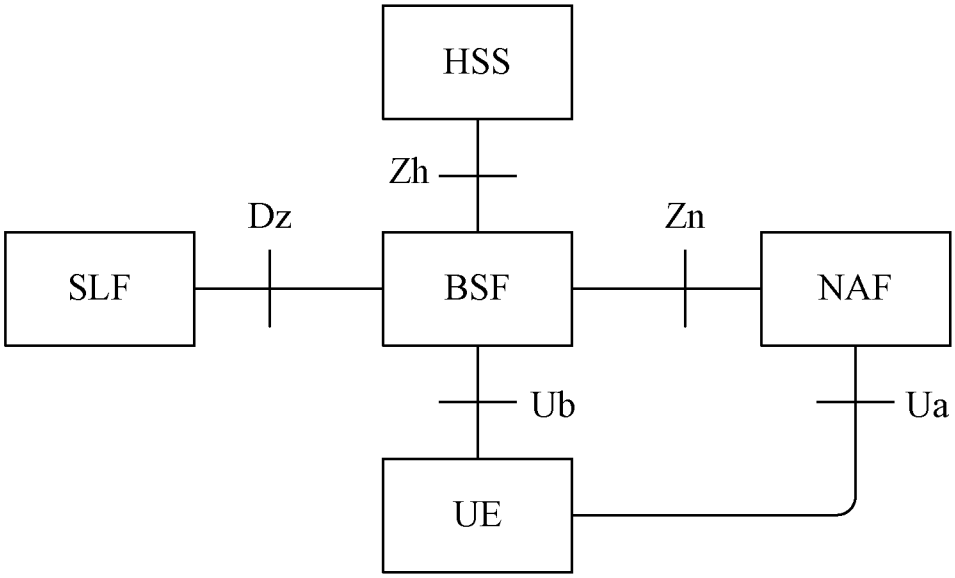

图 1

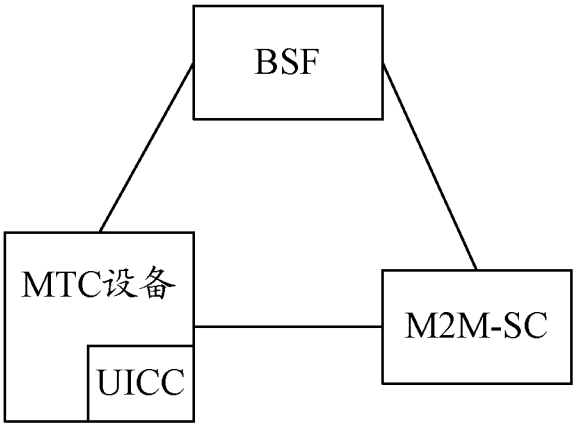

图 2

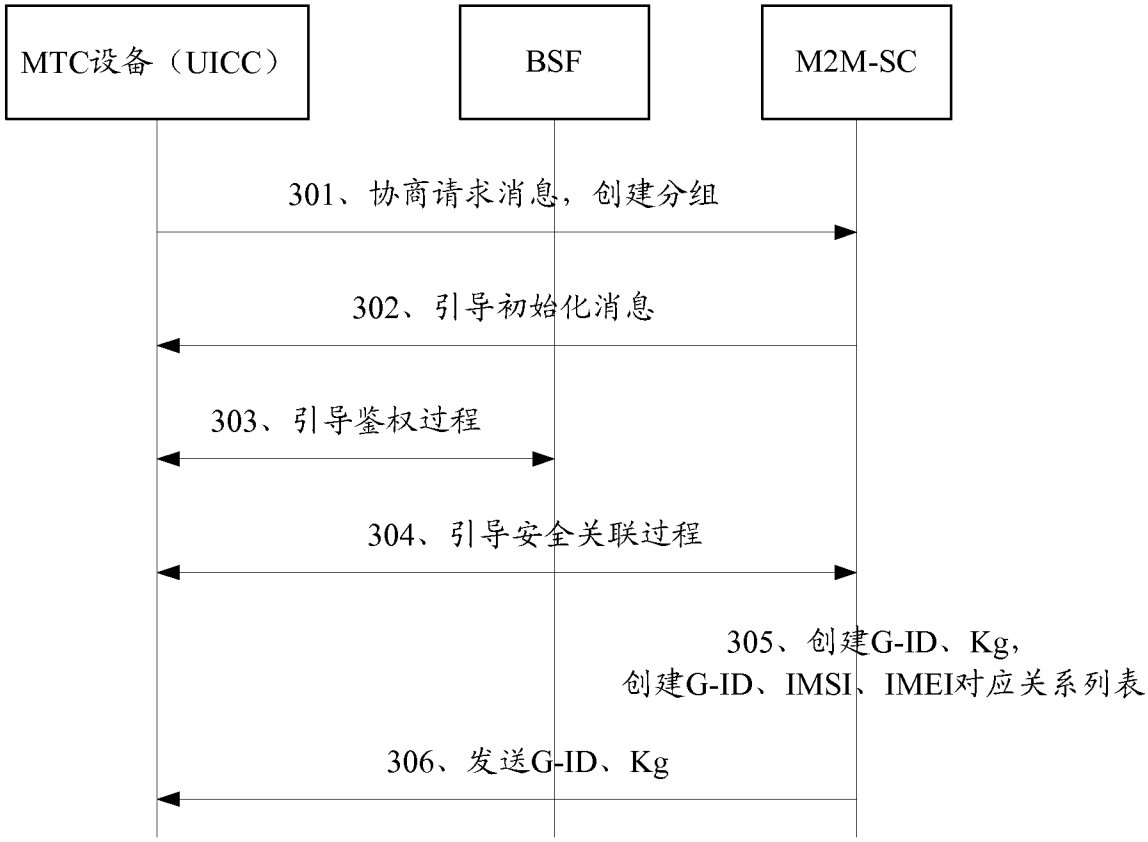
MTC设备（UICC）
BSF
M2M-SC
301、协商请求消息，创建分组
302、引导初始化消息
303、引导鉴权过程
304、引导安全关联过程
305、创建G-ID、Kg，
创建G-ID、IMSI、IMEI对应关系列表
306、发送G-ID、Kg

图 3

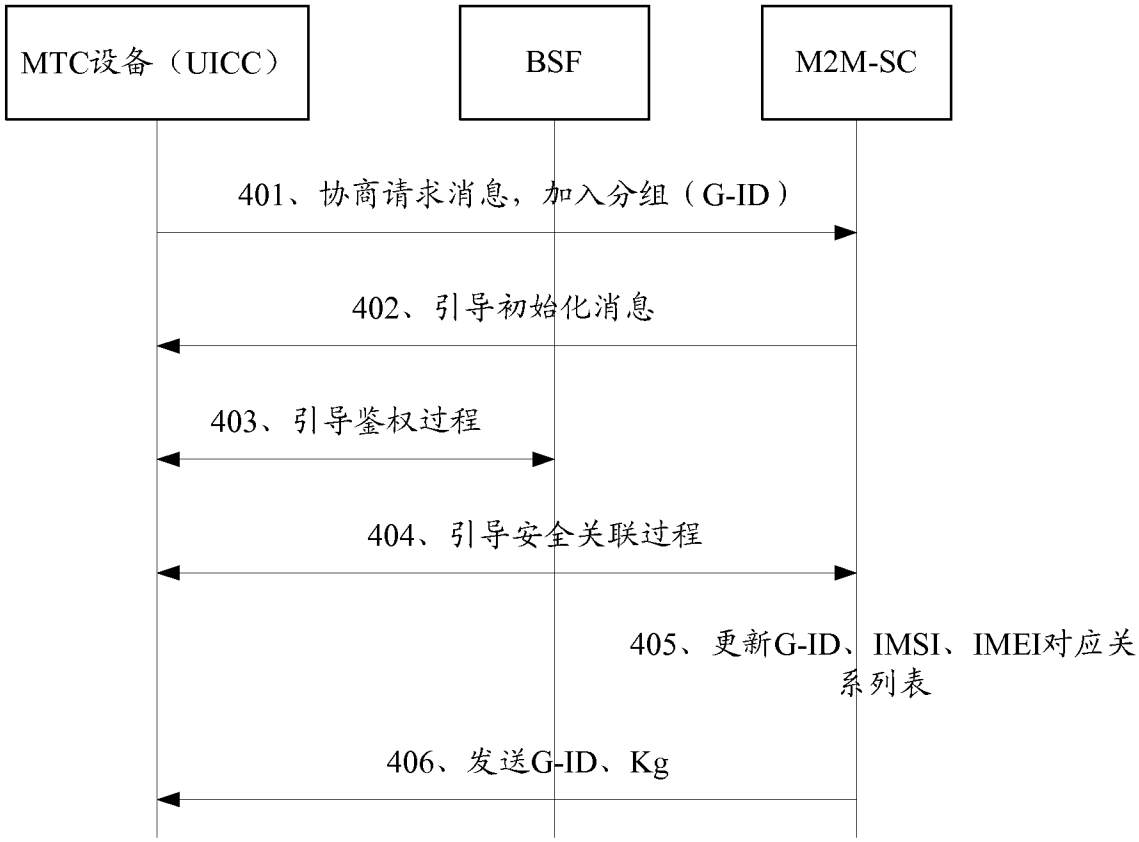
MTC设备（UICC）
BSF
M2M-SC
401、协商请求消息，加入分组（G-ID）
402、引导初始化消息
403、引导鉴权过程
404、引导安全关联过程
405、更新G-ID、IMSI、IMEI对应关系列表
406、发送G-ID、Kg

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/071938

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 H04W H04M

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,VEN,CNKI,IEEE,3GPP: MTC, M2M, ID, GBA, machine 1w to 1w machine, machine 1w type 1w communication?, group?, identity, identification?, identifier?, name?, join+, add+, registrat+, authoriz+, authenticat+, key, AKA, encrypt+, secur+, generic 1w bootstrap+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	3GPP. S1-100046: Contribution to TS 22.368 – Section 3.1 & 7.1.3 & 7.2.16.3: MTC Group. February 2010, pages 1-3	1-11
A	3GPP. TS 22.368 V10.2.0: Service Requirements for Machine-Type Communications (MTC); Stage1 (Release 10). September 2010, pages 16-17	1-11
A	ETSI. ETSI TS 102 689 V1.1.1: Machine-to-Machine Communications (M2M); M2M Service Requirements. August 2010, pages 13-14	1-11
A	3GPP. TD S2-102271: A Solution for Group Based Addressing. May 2010, pages 2-4	1-11
A	CN101523808A (ALCATEL LUCENT) 02 Sep. 2009 (02.09.2009) see the whole document	1-11

☒ 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
02 Aug. 2011 (02.08.2011)	**18 Aug. 2011 (18.08.2011)**
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 WANG, Xinyi Telephone No. (86-10)62412027

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/071938

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US20090191857A1 (NOKIA CORP et al.) 30 Jul. 2009 (30.07.2009) see the whole document	1-11
A	WO2009092115A2 (INTERDIGITAL PATENT HOLDINGS INC) 23 Jul. 2009 (23.07.2009) see the whole document	1-11

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2011/071938

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101523808A	02.09.2009	US20080091807A1	17.04.2008
		WO2008044225A2	17.04.2008
		EP2076999A2	08.07.2009
US20090191857A1	30.07.2009	WO2009095295A1	06.08.2009
		EP2248323A1	10.11.2010
WO2009092115A2	23.07.2009	JP2011510571W	31.03.2011
		KR20100113577A	21.10.2010
		EP2245829A2	03.11.2010

国际检索报告

国际申请号
PCT/CN2011/071938

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 H04W H04M

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,VEN,CNKI,IEEE,3GPP: 机器类通信,机器类型通信,通讯,机器到机器,MTC,M2M,分组,群组,标识,标记,ID,名称,加入,注册,授权,接入,密钥,加密,安全,GBA,通用引导,machine 1w to 1w machine, machine 1w type 1w communication?, group?, identity, identification?, identifier?, name?, join+, add+, registrat+, authoriz+, authenticat+, key, AKA, encrypt+, secur+, generic 1w bootstrap+

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
A	3GPP. S1-100046: Contribution to TS 22.368 – Section 3.1 & 7.1.3 & 7.2.16.3: MTC Group. 2 月 2010, 第 1-3 页	1-11
A	3GPP. TS 22.368 V10.2.0: Service Requirements for Machine-Type Communications (MTC); Stage1 (Release 10). 9 月 2010, 第 16-17 页	1-11
A	ETSI. ETSI TS 102 689 V1.1.1: Machine-to-Machine Communications (M2M); M2M Service Requirements. 8 月 2010, 第 13-14 页	1-11
A	3GPP. TD S2-102271: A Solution for Group Based Addressing. 5 月 2010, 第 2-4 页	1-11
A	CN101523808A (阿尔卡特朗讯公司) 02.9 月 2009 (02.09.2009) 参见全文	1-11

☒ 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
02.8 月 2011 (02.08.2011)	**18.8 月 2011 (18.08.2011)**
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 王心一 电话号码：(86-10) **62412027**

C(续). 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
A	US20090191857A1 (NOKIA CORP 等) 30.7 月 2009 (30.07.2009) 参见全文	1-11
A	WO2009092115A2 (INTERDIGITAL PATENT HOLDINGS INC) 23.7 月 2009 (23.07.2009) 参见全文	1-11

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2011/071938

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101523808A	02.09.2009	US20080091807A1	17.04.2008
		WO2008044225A2	17.04.2008
		EP2076999A2	08.07.2009
US20090191857A1	30.07.2009	WO2009095295A1	06.08.2009
		EP2248323A1	10.11.2010
WO2009092115A2	23.07.2009	JP2011510571W	31.03.2011
		KR20100113577A	21.10.2010
		EP2245829A2	03.11.2010