(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
2016 年 10 月 27 日 (27.10.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/169232 A1

(51) 国际专利分类号:
H04W 12/00 (2009.01)

(21) 国际申请号: PCT/CN2015/092118

(22) 国际申请日: 2015 年 10 月 16 日 (16.10.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510196876.2 2015 年 4 月 23 日 (23.04.2015) CN

(71) 申请人: **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: **彭锦 (PENG, Jin)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **朱进国 (ZHU, Jinguo)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **游世林 (YOU, Shilin)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **林兆骥 (LIN, Zhaoji)**; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。

(74) 代理人: **北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE)**; 中国北京市海淀区学清路 8 号 B 座 1601A, Beijing 100192 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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。

[见续页]

(54) **Title**: AUTHENTICATION METHOD, APPARATUS AND SYSTEM FOR D2D SERVICE MULTICAST

(54) **发明名称** : 一种 D2D 业务组播的认证方法、装置和系统

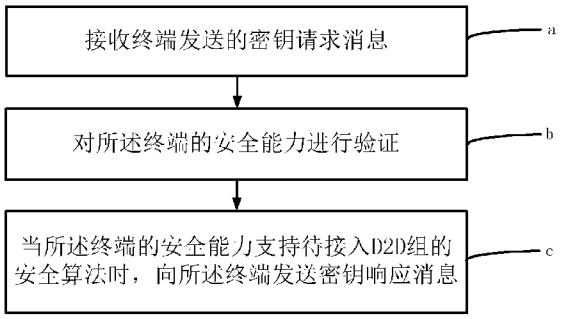

图 7

a Receiving a key request message sent by a terminal
b Verifying the security capability of the terminal
c Sending, when the security capability of the terminal supports a security algorithm to be accessed by a D2D group, a key response message to the terminal

(57) **Abstract**: Disclosed are a D2D service multicast authentication method, apparatus and system. The authentication method comprises: receiving a key request message sent by a terminal; verifying the security capability of the terminal; and when the security capability of the terminal supports a security algorithm to be accessed by a D2D group, sending a key response message to the terminal, the key response message carrying group key information about the D2D group.

(57) **摘要**: 本发明实施例公布了一种 D2D 业务组播的认证方法、装置和系统，所述的认证方法包括：接收终端发送的密钥请求消息；对所述终端的安全能力进行验证；当所述终端的安全能力支持待接入 D2D 组的安全算法时，向所述终端发送密钥响应消息，所述密钥响应消息携带所述 D2D 组的群组密钥信息。

WO 2016/169232 A1

(84) **指定国** (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则 4.17 的声明:

— 关于申请人有权申请并被授予专利(细则 4.17(ii))

— 发明人资格(细则 4.17(iv))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种 D2D 业务组播的认证方法、装置和系统

技术领域

本发明实施例涉及但不限于移动通信领域，尤其涉及一种 D2D 业务组播的认证方法、装置和系统。

背景技术

临近区域的终端利用设备到设备（Device to Device，简称为 D2D）直接通信能够给终端带来很多好处，比如更高的速率，更低的延迟以及更小的功耗，同时也极大地提高了运营商的无线资源效率，D2D 的中继（Relay）模式有利于运营商提高无线覆盖；对于应用来说利用 D2D 通讯过程中的临近信息可以开发出更加吸引人的新业务。公共安全（Public Safety）系统也可以利用 D2D 技术实现没有无线覆盖的情况下终端之间的通讯。

图 1 是相关技术中与 3GPP（3rd Generation Partnership Project，第三代合作伙伴计划）相关的 D2D Relay 架构示意图，如图 1 所示，涉及网元的功能说明如下：

远终端：也称为用户设备（User Equipment，简称为 UE），该终端处于无移动信号覆盖之内，支持通过 PC5 接口和其他终端进行 D2D 发现和通信，远终端也可以通过 Relay 节点和网络进行通信；

Relay 节点：该节点是一个终端，处于有移动信号覆盖之内，支持其他远终端通过该终端和网络通信，Relay 节点支持 Relay 发现广播，远终端通过读取该广播信息，选择合适的 Relay 节点并通过该节点和网络进行通信；

基站：为 Relay 节点提供无线覆盖，也可以为 Relay 节点进行 D2D 发现或者通信时候进行无线资源授权和分配，在进行 eMBMS（Evolved Multimedia Broadcast Multicast Service，增强型多媒体广播多播业务）广播的时候，基站通过广播进行下行数据发送，有利于节约空口资源，基站和终端或中继节点之间的空中接口为 Uu 口；

核心网：主要负责 Relay 节点的注册、分配 IP（Internet Protocol，网络互

连协议）地址以及承载建立，Relay 节点通过核心网和外部网络进行通信，基站和核心网之间接口为 S1 接口；

集群通信服务器：集群服务主要功能包括集群业务组的管理、呼叫建立、释放和管理等功能，UE 和集群通信服务器之间为 PC1 接口，UE 利用该接口向集群通信服务器发起注册，并从集群通信服务器获得业务相关信息，UE 也通过该接口向集群通信服务器发起组呼叫、请求话权等功能。

D2D 业务可以利用中继节点向远终端提供 eMBMS 组播业务，相关的流程如图 2 所示，包括:

201，远终端发现中继节点，应用向远终端提供 TMGI（Temporary Mobile Group Identity，临时移动组标识），其中所述应用安装远终端上，可以跟集群通信服务器交互;

202，远终端向中继节点发送 TMGI 监听请求消息，消息中包括 TMGI 参数;

203，中继节点向远终端回送 TMGI 监听响应消息，消息中包括 ProSe（Proximity-based Services，基于邻近的业务）层 2 组标识和 TMGI 定时器等参数;

204，中继节点监听到 TMGI 广播;

205，中继节点向远终端发送 TMGI 通知消息，消息中包括 TMGI 参数;

206，远终端可以通过中继节点的中继接收广播内容。

在以上的流程中，中继节点和远终端之间使用 D2D 组播方式进行通讯，这要求中继节点和远终端加入同一个 D2D 组播组，并获取该组的群组密钥。但是，远终端没有网络覆盖，无法跟网络交互完成加入群组和获取群组密钥的过程，因此无法提供安全的 eMBMS 业务。

发明内容

以下是对本文详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

本发明实施例提供一种 D2D 业务组播的认证方法、装置和系统，实现在 D2D 业务中中继节点向远终端进行组播的认证。

本发明实施例提供了一种设备到设备 D2D 业务组播的认证方法，包括:

接收终端发送的密钥请求消息;

对所述终端的安全能力进行验证;

当所述终端的安全能力支持待接入 D2D 组的安全算法时，向所述终端发送密钥响应消息，所述密钥响应消息携带所述 D2D 组的群组密钥信息。

可选地，所述方法还包括: 当所述终端的安全能力不支持待接入 D2D 组的安全算法时，向所述终端发送密钥响应消息，所述密钥响应消息携带失败标识和失败原因信息。

可选地，所述接收终端发送的密钥请求消息之后，所述方法还包括: 与基于邻近的业务 ProSe 密钥管理功能实体交互，获取所述 D2D 组的群组密钥信息。

可选地，所述接收终端发送的密钥请求消息之前，所述方法还包括:

接收所述终端发送的临时移动组标识 TMGI 监听请求消息;

根据所述 TMGI 监听请求消息确定是否存在与所述 TMGI 对应的 ProSe 组;

当不存在与所述 TMGI 对应的 ProSe 组时，向 ProSe 功能实体发送群组请求消息; 并接收所述 ProSe 功能实体发送群组响应消息，所述群组响应消息中携带所述 ProSe 功能实体为所述终端分配 ProSe 组信息; 向所述终端发送 TMGI 监听响应消息;

当存在与所述 TMGI 对应的 ProSe 组时，向所述终端发送 TMGI 监听响应消息。

可选地，所述向所述终端发送密钥响应消息之后，所述方法还包括: 向所述终端发送多媒体互联网密钥 MIKEY 消息，所述 MIKEY 消息用于传送密

钥数据。

可选地，其中，所述密钥请求消息包括：待接入 D2D 组标识和终端安全能力参数；或者包括临时移动组标识 TMGI 参数和终端安全能力参数；或者包括待接入 D2D 组标识、所述终端标识和终端安全能力参数。

可选地，其中，所述群组密钥信息包括：所述 D2D 组成员标识、ProSe 组密钥 PGK 标识、PGK 和待接入 D2D 组的安全算法；或者包括待接入 D2D 组标识 、所述 D2D 组成员标识、PGK 标识、PGK、待接入 D2D 组的安全算法和 TMGI 定时器参数；或者包括所述 D2D 组成员标识、ProSe 多媒体互联网密钥 PMK 标识、PMK 和待接入 D2D 组的安全算法；或者包括所述终端标识、所述 D2D 组成员标识、PGK 标识、PGK、待接入 D2D 组的安全算法。

本发明实施例还提供一种设备到设备 D2D 业务组播的认证方法，包括：

向中继节点发送密钥请求消息；

接收所述中继节点返回的密钥响应消息，所述密钥响应消息携带待接入 D2D 组的群组密钥信息。

可选地，所述向中继节点发送密钥请求消息之前，所述方法还包括：

向所述中继节点发送临时移动组标识 TMGI 监听请求消息；

接收所述中继节点返回的 TMGI 监听响应消息。

本发明实施例还提供一种设备到设备 D2D 业务组播的认证装置，设置在中继节点，包括：

第一接收模块，设置为接收终端发送的密钥请求消息；

验证模块，设置为对所述终端的安全能力进行验证；以及

第一发送模块，设置为当所述终端的安全能力支持待接入 D2D 组的安全算法时，向所述终端发送密钥响应消息，所述密钥响应消息携带所述 D2D 组的群组密钥信息。

可选地，其中，所述第一发送模块还设置为当所述终端的安全能力不支

持待接入 D2D 组的安全算法时，向所述终端发送密钥响应消息，所述密钥响应消息携带失败标识和失败原因信息。

可选地，所述装置还包括交互模块，

所述交互模块，设置为与基于邻近的业务 ProSe 密钥管理功能实体交互，获取所述 D2D 组的群组密钥信息。

可选地，所述装置还包括确定模块，

所述第一接收模块，还设置为接收所述终端发送的临时移动组标识 TMGI 监听请求消息；

所述确定模块，设置为根据所述 TMGI 监听请求消息确定是否存在与所述 TMGI 对应的 ProSe 组；

所述第一发送模块，还设置为当不存在与所述 TMGI 对应的 ProSe 组时，向 ProSe 功能实体发送群组请求消息；

所述第一接收模块，还设置为接收所述 ProSe 功能实体发送群组响应消息，所述群组响应消息中携带所述 ProSe 功能实体为所述终端分配 ProSe 组信息；

所述第一发送模块，还设置为向所述终端发送 TMGI 监听响应消息。

可选地，其中，所述第一发送模块，还设置为向所述终端发送密钥响应消息之后，向所述终端发送多媒体互联网密钥 MIKEY 消息，所述 MIKEY 消息用于传送密钥数据。

本发明实施例还提供一种设备到设备 D2D 业务组播的认证装置，设置在终端，包括：

第二发送模块，设置为向中继节点发送密钥请求消息；以及

第二接收模块，设置为接收所述中继节点返回的密钥响应消息，所述密钥响应消息携带待接入 D2D 组的群组密钥信息。

可选地，其中，所述第二发送模块，还设置为向所述中继节点发送临时移动组标识 TMGI 监听请求消息；

所述第二接收模块，还设置为接收所述中继节点返回的 TMGI 监听响应消息。

本发明实施例还提供一种设备到设备 D2D 业务组播的认证系统，包括上述的中继节点和上述的终端。

本发明实施例还提供一种计算机可读存储介质，存储有程序指令，当该程序指令被执行时可实现上述方法。

本发明实施例通过中继节点具有 ProSe 管理功能实体的功能，或者终端通过中继节点与 ProSe 密钥管理功能实体交互，向终端分配 D2D 组密钥，实现了使用 D2D 中继节点向终端提供安全的 eMBMS 组播业务。由此增强了 ProSe 系统功能和安全性。

在阅读并理解了附图和详细描述后，可以明白其他方面。

附图概述

图 1 是 D2D 业务 Relay 架构示意图；

图 2 是相关技术利用中继节点向远终端提供 eMBMS 组播业务的流程图；

图 3 是本发明应用实施例一利用中继节点向远终端提供安全的 eMBMS 组播业务的基本流程图；

图 4 是本发明应用实施例二利用中继节点向远终端提供安全的 eMBMS 组播业务，合并监听请求和密钥请求消息的流程图；

图 5 是本发明应用实施例三利用中继节点向远终端提供安全的 eMBMS 组播业务，使用 MIKEY 发送 PGK 等参数的流程图；

图 6 是本发明应用实施例四利用中继节点向远终端提供安全的 eMBMS 组播业务，ProSe 密钥管理功能实体独立设置的流程图；

图 7 是本发明实施例中继节点侧 D2D 业务组播的认证方法的流程图；

图 8 是本发明实施例终端侧 D2D 业务组播的认证方法的流程图；

图 9 本发明实施例中继节点侧 D2D 业务组播的认证装置的结构示意图；

图 10 是本发明实施例终端侧 D2D 业务组播的认证装置的结构示意图。

本发明的实施方式

下面结合附图对本发明实施例进行说明，需要说明的是，在不冲突的情况下，本申请中的实施例和实施例中的特征可以相互任意组合。

如图 7 所示，本发明实施例提供的一种设备到设备 D2D 业务组播的认证方法，应用于中继节点，包括:

Sa、接收终端发送的密钥请求消息;

Sb、对所述终端的安全能力进行验证;

Sc、当所述终端的安全能力支持待接入 D2D 组的安全算法时，向所述终端发送密钥响应消息，所述密钥响应消息携带所述 D2D 组的群组密钥信息。

Sc 中如果所述终端的安全能力不支持待接入 D2D 组的安全算法，向所述终端发送密钥响应消息，所述密钥响应消息携带失败标识和失败原因信息。

可选地，Sa 之后还包括: 与 ProSe 密钥管理功能实体交互，获取所述 D2D 组的群组密钥信息。

在 D2D 业务中中继节点向终端进行组播的认证，中继节点可具有 ProSe 密钥管理功能实体的功能，或者终端通过中继节点与 ProSe 密钥管理功能实体交互。终端向中继节点请求组密钥，用于 D2D 组播通讯。中继节点接收 eMBMS 组播，将内容转换为 D2D 组播发送。实现了使用 D2D 中继节点向远终端提供安全的 eMBMS 组播业务。由此增强了 ProSe 系统功能和安全性。

可选地，Sa 之前还包括:

接收所述终端发送的临时移动组标识 TMGI 监听请求消息;

根据所述 TMGI 监听请求消息确定是否存在与所述 TMGI 对应的 ProSe 组;

当不存在与所述 TMGI 对应的 ProSe 组时，向 ProSe 功能实体发送群组请求消息; 并接收所述 ProSe 功能实体发送群组响应消息，所述群组响应消息中携带所述 ProSe 功能实体为所述终端分配 ProSe 组信息; 向所述终端发

送 TMGI 监听响应消息;

当存在与所述 TMGI 对应的 ProSe 组时，向所述终端发送 TMGI 监听响应消息。

可选地，Sc 之后还包括：向所述终端发送多媒体互联网密钥 MIKEY 消息，所述 MIKEY 消息用于传送密钥数据。

当所述密钥请求消息包括：待接入 D2D 组标识和终端安全能力参数；所述群组密钥信息包括：所述 D2D 组成员标识、PGK（ProSe Group Key， ProSe 组密钥）标识、PGK 和待接入 D2D 组的安全算法。

当所述密钥请求消息包括临时移动组标识 TMGI 参数和终端安全能力参数；所述群组密钥信息包括待接入 D2D 组标识 、所述 D2D 组成员标识、PGK 标识、PGK、待接入 D2D 组的安全算法和 TMGI 定时器参数；或者包括所述 D2D 组成员标识、PMK（ProSe MIKEY Key，ProSe 多媒体互联网密钥）标识、PMK 和待接入 D2D 组的安全算法。

当所述密钥请求消息包括待接入 D2D 组标识、终端标识和终端安全能力参数；所述群组密钥信息包括终端标识、所述 D2D 组成员标识、PGK 标识、PGK、待接入 D2D 组的安全算法。

其中，MIKEY 消息由 RFC（Remote Function Call，远程函数调用） 3830 定义，MIKEY 消息可以在两个实体间建立安全连接，用于传送密钥等重要数据，PGK 为 ProSe 组的共享密钥，PMK 用于 MIKEY 消息加密的密钥。

如图 8 所示，本发明实施例提供的一种设备到设备 D2D 业务组播的认证方法，应用于终端，包括:

Sd、向中继节点发送密钥请求消息;

Se、接收所述中继节点返回的密钥响应消息，所述密钥响应消息携带待接入 D2D 组的群组密钥信息。

可选地，Sd 之前还包括:

向所述中继节点发送临时移动组标识 TMGI 监听请求消息;

接收所述中继节点返回的 TMGI 监听响应消息。

如图 9 所示，本发明实施例提供的一种设备到设备 D2D 业务组播的认证装置，设置在中继节点，包括:

第一接收模块 110，设置为接收终端发送的密钥请求消息;

验证模块 120，设置为对所述终端的安全能力进行验证；以及

第一发送模块 130，设置为当所述终端的安全能力支持待接入 D2D 组的安全算法时，向所述终端发送密钥响应消息，所述密钥响应消息携带所述 D2D 组的群组密钥信息。

所述第一发送模块 130 还设置为当所述终端的安全能力不支持待接入 D2D 组的安全算法时，向所述终端发送密钥响应消息，所述密钥响应消息携带失败标识和失败原因信息。

可选地，上述认证装置还包括交互模块 140，所述交互模块 140，设置为与 ProSe 密钥管理功能实体交互，获取所述 D2D 组的群组密钥信息。

可选地，上述认证装置还包括确定模块 150，

所述第一接收模块 110，还设置为接收所述终端发送的临时移动组标识 TMGI 监听请求消息;

所述确定模块 150，设置为根据所述 TMGI 监听请求消息确定是否存在与所述 TMGI 对应的 ProSe 组;

所述第一发送模块 130，还设置为当不存在与所述 TMGI 对应的 ProSe 组时，向 ProSe 功能实体发送群组请求消息;

所述第一接收模块 110，还设置为接收所述 ProSe 功能实体发送群组响应消息，所述群组响应消息中携带所述 ProSe 功能实体为所述终端分配 ProSe 组信息;

所述第一发送模块 130，还设置为向所述终端发送 TMGI 监听响应消息。

可选地，所述第一发送模块 130，还设置为向所述终端发送密钥响应消息之后，向所述终端发送多媒体互联网密钥 MIKEY 消息，所述 MIKEY 消息用于传送密钥数据。

如图 10 所示、本发明实施例提供的一种设备到设备 D2D 业务组播的认

证装置，设置在终端，包括:

第二发送模块 210，设置为向中继节点发送密钥请求消息；以及

第二接收模块 220，设置为接收所述中继节点返回的密钥响应消息，所述密钥响应消息携带待接入 D2D 组的群组密钥信息。

可选地，所述第二发送模块 210，还设置为向所述中继节点发送临时移动组标识 TMGI 监听请求消息;

所述第二接收模块 220，还设置为接收所述中继节点返回的 TMGI 监听响应消息。

本发明实施例还提供一种设备到设备 D2D 业务组播的认证系统，包括上述的中继节点和终端。

应用实施例一:

如图 3 所示，利用中继节点向远终端提供安全的 eMBMS 组播业务的基本流程如下所示:

301，远终端发现中继节点，应用向远终端提供 TMGI;

302，远终端向中继节点发送 TMGI 监听请求消息，消息中包括 TMGI 参数;

303，中继节点向远终端回送 TMGI 监听响应消息，消息中包括 ProSe 层 2 组标识和 TMGI 定时器等参数;

304，远终端向中继节点发送密钥请求消息，消息中包括 ProSe 层 2 组标识和终端安全能力等参数;

305，中继节点进行算法检查，确定远终端的安全能力是否支持组安全算法;

306，中继节点向远终端回送密钥响应消息，消息中包括组成员标识、PGK 标识、PGK 和算法等参数;

307，中继节点监听到 TMGI 广播;

308，中继节点向远终端发送 TMGI 通知消息，消息中包括 TMGI 参数;

309，远终端可以通过中继节点的中继接收广播内容。

应用实施例二:

如图 4 所示，利用中继节点向远终端提供安全的 eMBMS 组播业务，合并监听请求和密钥请求消息的流程如下所示:

401，远终端发现中继节点，应用向远终端提供 TMGI;

402，远终端向中继节点发送 TMGI 监听与密钥请求消息，消息中包括 TMGI 参数和终端安全能力等参数;

403，中继节点进行算法检查，确定远终端的安全能力是否支持组安全算法;

404，中继节点向远终端回送 TMGI 监听与密钥响应消息，消息中包括 ProSe 层 2 组标识、组成员标识、PGK 标识、PGK、算法和 TMGI 定时器等参数;

405，中继节点监听到 TMGI 广播;

406，中继节点向远终端发送 TMGI 通知消息，消息中包括 TMGI 参数;

407，远终端可以通过中继节点的中继接收广播内容。

应用实施例三:

如图 5 所示，利用中继节点向远终端提供安全的 eMBMS 组播业务，使用 MIKEY 发送 PGK 等参数的流程如下所示:

501，远终端发现中继节点，应用向远终端提供 TMGI;

502，远终端向中继节点发送 TMGI 监听请求消息，消息中包括 TMGI 参数;

503，中继节点向远终端回送 TMGI 监听响应消息，消息中包括 ProSe 层 2 组标识和 TMGI 定时器等参数;

504，远终端向中继节点发送密钥请求消息，消息中包括 ProSe 层 2 组标识和终端安全能力等参数;

505，中继节点进行算法检查，确定远终端的安全能力是否支持组安全算法；

506，中继节点向远终端回送密钥响应消息，消息中包括组成员标识、PMK标识、PMK 和算法等参数；

507，中继节点使用 MIKEY 消息向远终端发送 PGK、PGK 标识和定时器等参数；

508，中继节点监听到 TMGI 广播；

509，中继节点向远终端发送 TMGI 通知消息，消息中包括 TMGI 参数；

510，远终端可以通过中继节点的中继接收广播内容。

应用实施例四：

如图 6 所示，利用中继节点向远终端提供安全的 eMBMS 组播业务，ProSe 密钥管理功能实体独立设置的流程如下所示：

601，远终端发现中继节点，应用向远终端提供 TMGI；

602，远终端向中继节点发送 TMGI 监听请求消息，消息中包括终端标识和 TMGI 等参数；中继节点检查是否存在与该 TMGI 对应的 ProSe 组，或是否存在已分配而尚未使用的 ProSe 组，如有，则转至步骤 605；如无，则转至步骤 603；

603，可选地，中继节点向 ProSe 功能实体发送群组请求消息，消息中包括中继节点终端标识和远终端终端标识；

604，可选地，ProSe 功能实体为该中继节点和远终端分配 ProSe 群组，ProSe 密钥管理功能实体为该群组生成 PGK；ProSe 功能实体向中继节点回送群组响应消息，消息中包括 ProSe 层 2 组标识参数；

605，中继节点向远终端回送 TMGI 监听响应消息，消息中包括 ProSe 层 2 组标识和 TMGI 定时器等参数；

604，远终端向通过中继节点向 ProSe 密钥管理功能实体发送密钥请求消息，消息中包括 ProSe 层 2 组标识、终端标识和终端安全能力等参数；

605，ProSe 密钥管理功能实体进行算法检查，确定远终端的安全能力是否支持组安全算法;

606，ProSe 密钥管理功能实体通过中继节点向远终端回送密钥响应消息，消息中包括远终端的终端标识、组成员标识、PGK 标识、PGK 和算法等参数;

607，中继节点监听到 TMGI 广播;

608，中继节点向远终端发送 TMGI 通知消息，消息中包括 TMGI 参数;

609，远终端可以通过中继节点的中继接收广播内容。

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

虽然所揭示的实施方式如上，但只是为了便于理解本发明技术方案而采用的实施方式，并非用于限定本发明。

工业实用性

通过中继节点具有 ProSe 管理功能实体的功能，或者终端通过中继节点与 ProSe 密钥管理功能实体交互，向终端分配 D2D 组密钥，实现了使用 D2D 中继节点向终端提供安全的 eMBMS 组播业务。由此增强了 ProSe 系统功能和安全性。

权 利 要 求 书

1、一种设备到设备 D2D 业务组播的认证方法，包括:

接收终端发送的密钥请求消息;

对所述终端的安全能力进行验证;

当所述终端的安全能力支持待接入 D2D 组的安全算法时，向所述终端发送密钥响应消息，所述密钥响应消息携带所述 D2D 组的群组密钥信息。

2、如权利要求 1 所述的方法，所述方法还包括：当所述终端的安全能力不支持待接入 D2D 组的安全算法时，向所述终端发送密钥响应消息，所述密钥响应消息携带失败标识和失败原因信息。

3、如权利要求 1 所述的方法，所述接收终端发送的密钥请求消息之后，所述方法还包括：与基于邻近的业务 ProSe 密钥管理功能实体交互，获取所述 D2D 组的群组密钥信息。

4、如权利要求 3 所述的方法，所述接收终端发送的密钥请求消息之前，所述方法还包括:

接收所述终端发送的临时移动组标识 TMGI 监听请求消息;

根据所述 TMGI 监听请求消息确定是否存在与所述 TMGI 对应的 ProSe 组;

当不存在与所述 TMGI 对应的 ProSe 组时，向 ProSe 功能实体发送群组请求消息；并接收所述 ProSe 功能实体发送群组响应消息，所述群组响应消息中携带所述 ProSe 功能实体为所述终端分配 ProSe 组信息；向所述终端发送 TMGI 监听响应消息;

当存在与所述 TMGI 对应的 ProSe 组时，向所述终端发送 TMGI 监听响应消息。

5、如权利要求 1 所述的方法，所述向所述终端发送密钥响应消息之后，所述方法还包括：向所述终端发送多媒体互联网密钥 MIKEY 消息，所述 MIKEY 消息用于传送密钥数据。

6、如权利要求 1 所述的方法，其中：所述密钥请求消息包括：待接入

D2D 组标识和终端安全能力参数；或者包括临时移动组标识 TMGI 参数和终端安全能力参数；或者包括待接入 D2D 组标识、所述终端标识和终端安全能力参数。

7、如权利要求 1 所述的方法，其中：所述群组密钥信息包括：所述 D2D 组成员标识、ProSe 组密钥 PGK 标识、PGK 和待接入 D2D 组的安全算法；或者包括待接入 D2D 组标识 、所述 D2D 组成员标识、PGK 标识、PGK、待接入 D2D 组的安全算法和 TMGI 定时器参数；或者包括所述 D2D 组成员标识、ProSe 多媒体互联网密钥 PMK 标识、PMK 和待接入 D2D 组的安全算法；或者包括所述终端标识、所述 D2D 组成员标识、PGK 标识、PGK、待接入 D2D 组的安全算法。

8、一种设备到设备 D2D 业务组播的认证方法，包括：

向中继节点发送密钥请求消息；

接收所述中继节点返回的密钥响应消息，所述密钥响应消息携带待接入 D2D 组的群组密钥信息。

9、如权利要求 8 所述的方法，所述向中继节点发送密钥请求消息之前，所述方法还包括：

向所述中继节点发送临时移动组标识 TMGI 监听请求消息；

接收所述中继节点返回的 TMGI 监听响应消息。

10、一种设备到设备 D2D 业务组播的认证装置，其特征在于，设置在中继节点，包括：

第一接收模块，设置为接收终端发送的密钥请求消息；

验证模块，设置为对所述终端的安全能力进行验证；以及

第一发送模块，设置为当所述终端的安全能力支持待接入 D2D 组的安全算法时，向所述终端发送密钥响应消息，所述密钥响应消息携带所述 D2D 组的群组密钥信息。

11、如权利要求 10 所述的装置，其中：所述第一发送模块还设置为当所述终端的安全能力不支持待接入 D2D 组的安全算法时，向所述终端发送密钥响应消息，所述密钥响应消息携带失败标识和失败原因信息。

12、如权利要求 10 所述的装置，所述装置还包括交互模块，所述交互模块，设置为与基于邻近的业务 ProSe 密钥管理功能实体交互，获取所述 D2D 组的群组密钥信息。

13、如权利要求 12 所述的装置，所述装置还包括确定模块，

所述第一接收模块，还设置为接收所述终端发送的临时移动组标识 TMGI 监听请求消息；

所述确定模块，设置为根据所述 TMGI 监听请求消息确定是否存在与所述 TMGI 对应的 ProSe 组；

所述第一发送模块，还设置为当不存在与所述 TMGI 对应的 ProSe 组时，向 ProSe 功能实体发送群组请求消息；

所述第一接收模块，还设置为接收所述 ProSe 功能实体发送群组响应消息，所述群组响应消息中携带所述 ProSe 功能实体为所述终端分配 ProSe 组信息；

所述第一发送模块，还设置为向所述终端发送 TMGI 监听响应消息。

14、如权利要求 10 所述的装置，其中：所述第一发送模块，还设置为向所述终端发送密钥响应消息之后，向所述终端发送多媒体互联网密钥 MIKEY 消息，所述 MIKEY 消息用于传送密钥数据。

15、一种设备到设备 D2D 业务组播的认证装置，其特征在于，设置在终端，包括：

第二发送模块，设置为向中继节点发送密钥请求消息；以及

第二接收模块，设置为接收所述中继节点返回的密钥响应消息，所述密钥响应消息携带待接入 D2D 组的群组密钥信息。

16、如权利要求 15 所述的装置，其中：

所述第二发送模块，还设置为向所述中继节点发送临时移动组标识 TMGI 监听请求消息；

所述第二接收模块，还设置为接收所述中继节点返回的 TMGI 监听响应消息。

17、一种设备到设备 D2D 业务组播的认证系统，包括权利要求 10 至 14 任一所述的中继节点和权利要求 15 至 16 任一所述的终端。

18、一种计算机可读存储介质，存储有程序指令，当该程序指令被执行时可实现权利要求 1-7 任一项所述的方法。

19、一种计算机可读存储介质，存储有程序指令，当该程序指令被执行时可实现权利要求 8-9 任一项所述的方法。

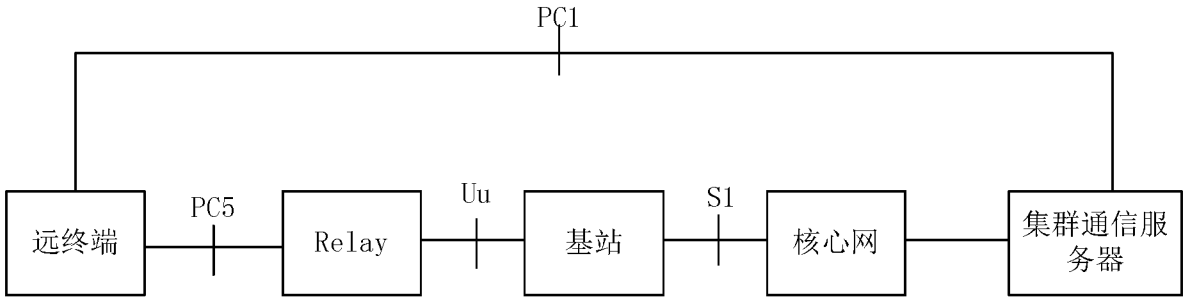
PC1
远终端
PC5
Relay
Uu
基站
S1
核心网
集群通信服务器

图 1

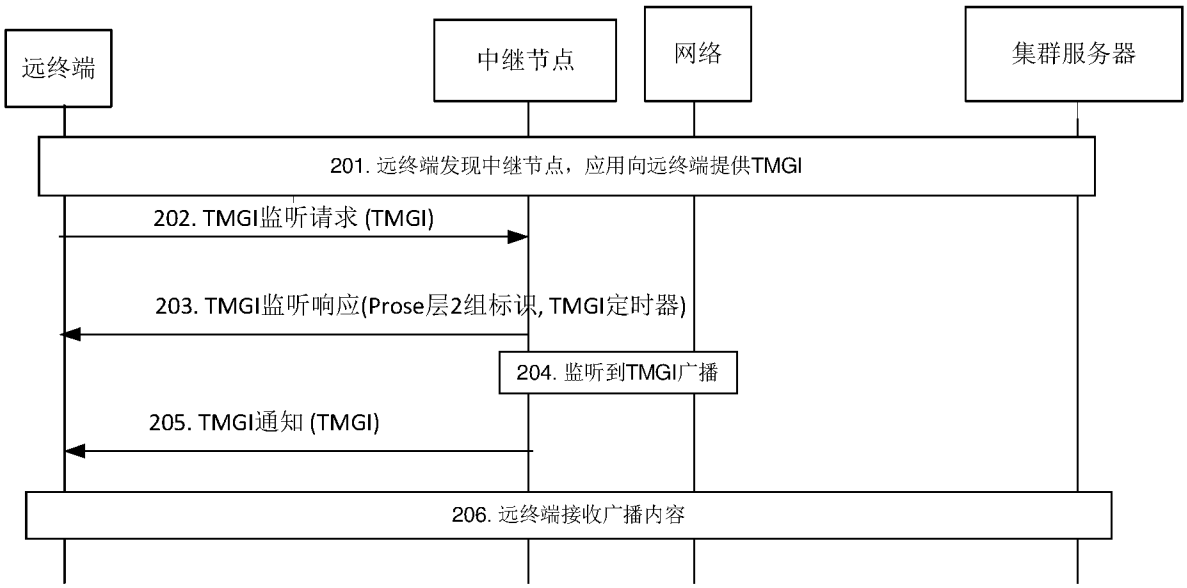
远终端
中继节点
网络
集群服务器
201. 远终端发现中继节点，应用向远终端提供TMGI
202. TMGI监听请求 (TMGI)
203. TMGI监听响应(Prose层2组标识, TMGI定时器)
204. 监听到TMGI广播
205. TMGI通知 (TMGI)
206. 远终端接收广播内容

图 2

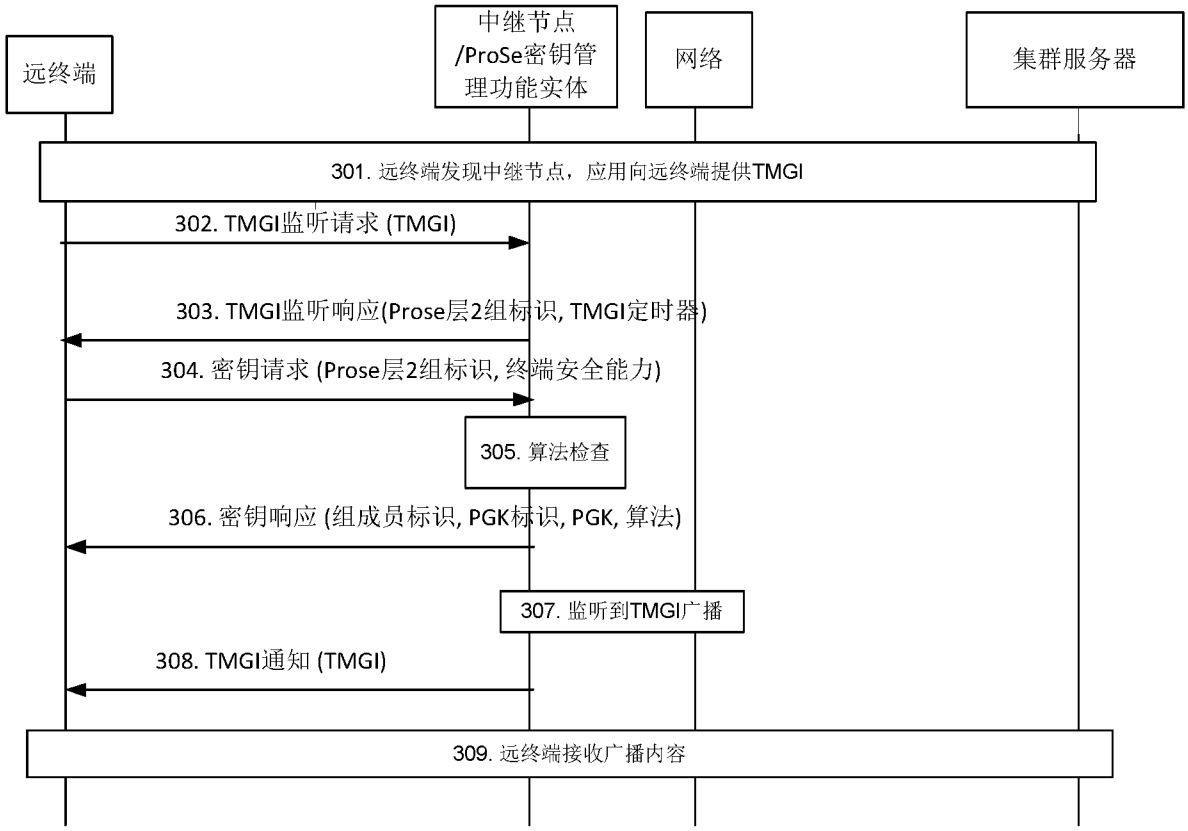
远终端
中继节点
/ProSe密钥管
理功能实体
网络
集群服务器
301. 远终端发现中继节点，应用向远终端提供TMGI
302. TMGI监听请求 (TMGI)
303. TMGI监听响应(Prose层2组标识, TMGI定时器)
304. 密钥请求 (Prose层2组标识, 终端安全能力)
305. 算法检查
306. 密钥响应 (组成员标识, PGK标识, PGK, 算法)
307. 监听到TMGI广播
308. TMGI通知 (TMGI)
309. 远终端接收广播内容

图 3

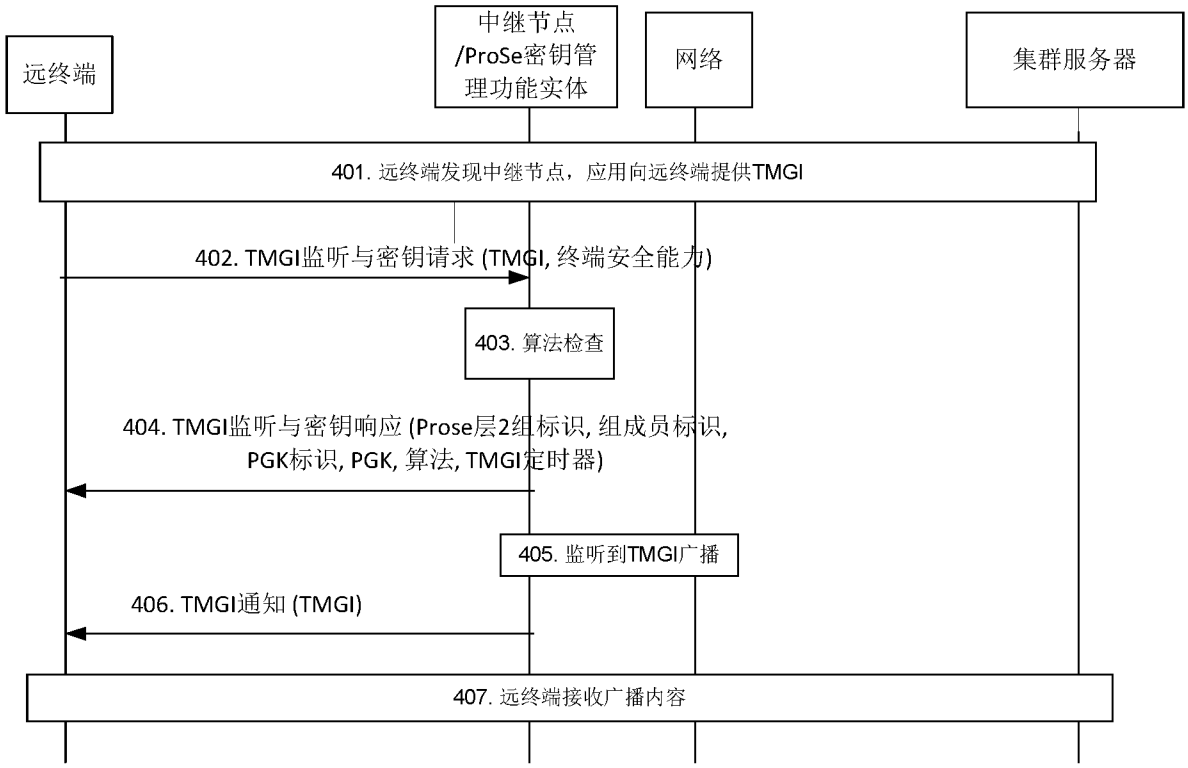
远终端
中继节点
/ProSe密钥管
理功能实体
网络
集群服务器
401. 远终端发现中继节点，应用向远终端提供TMGI
402. TMGI监听与密钥请求 (TMGI, 终端安全能力)
403. 算法检查
404. TMGI监听与密钥响应 (Prose层2组标识, 组成员标识,
PGK标识, PGK, 算法, TMGI定时器)
405. 监听到TMGI广播
406. TMGI通知 (TMGI)
407. 远终端接收广播内容

图 4

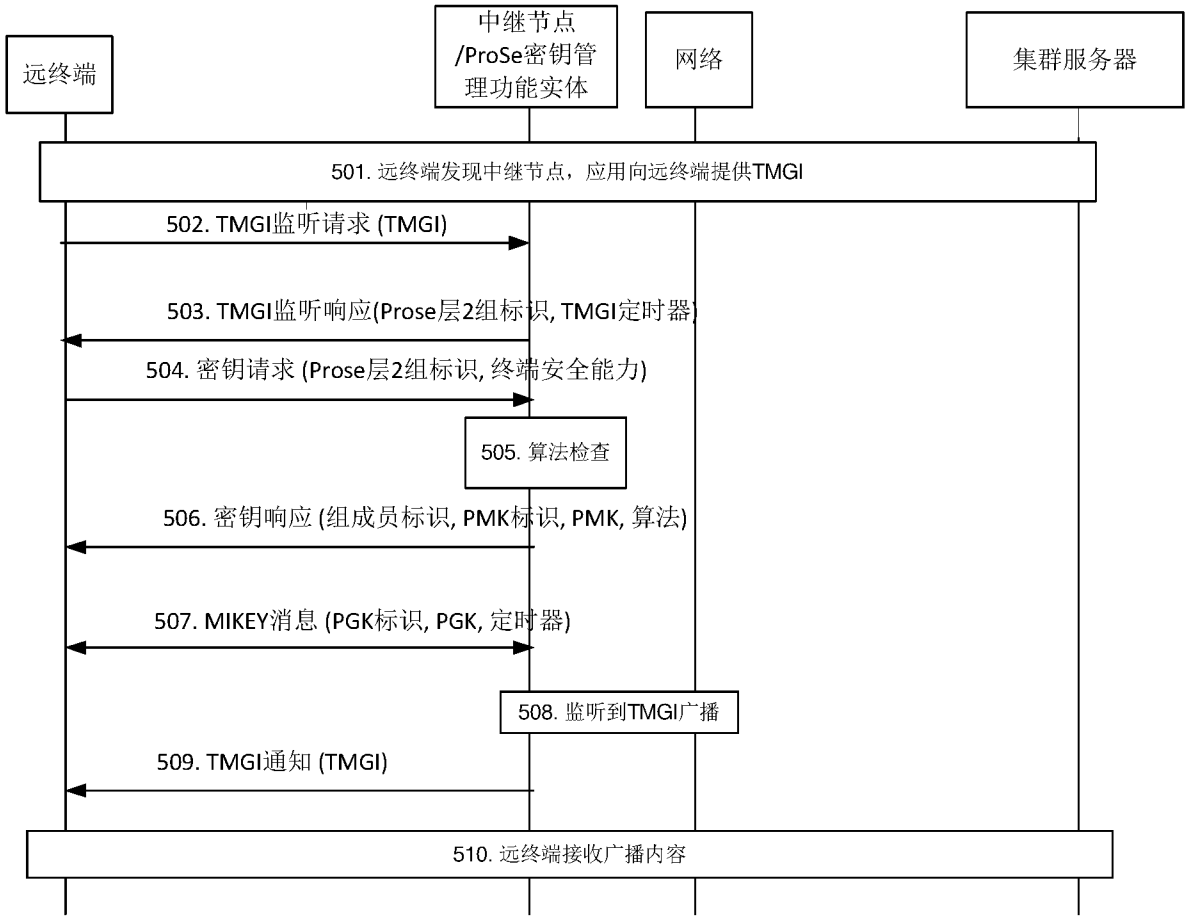
远终端
中继节点
/ProSe密钥管
理功能实体
网络
集群服务器
501. 远终端发现中继节点，应用向远终端提供TMGI
502. TMGI监听请求 (TMGI)
503. TMGI监听响应(Prose层2组标识, TMGI定时器)
504. 密钥请求 (Prose层2组标识, 终端安全能力)
505. 算法检查
506. 密钥响应 (组成员标识, PMK标识, PMK, 算法)
507. MIKEY消息 (PGK标识, PGK, 定时器)
508. 监听到TMGI广播
509. TMGI通知 (TMGI)
510. 远终端接收广播内容

图 5

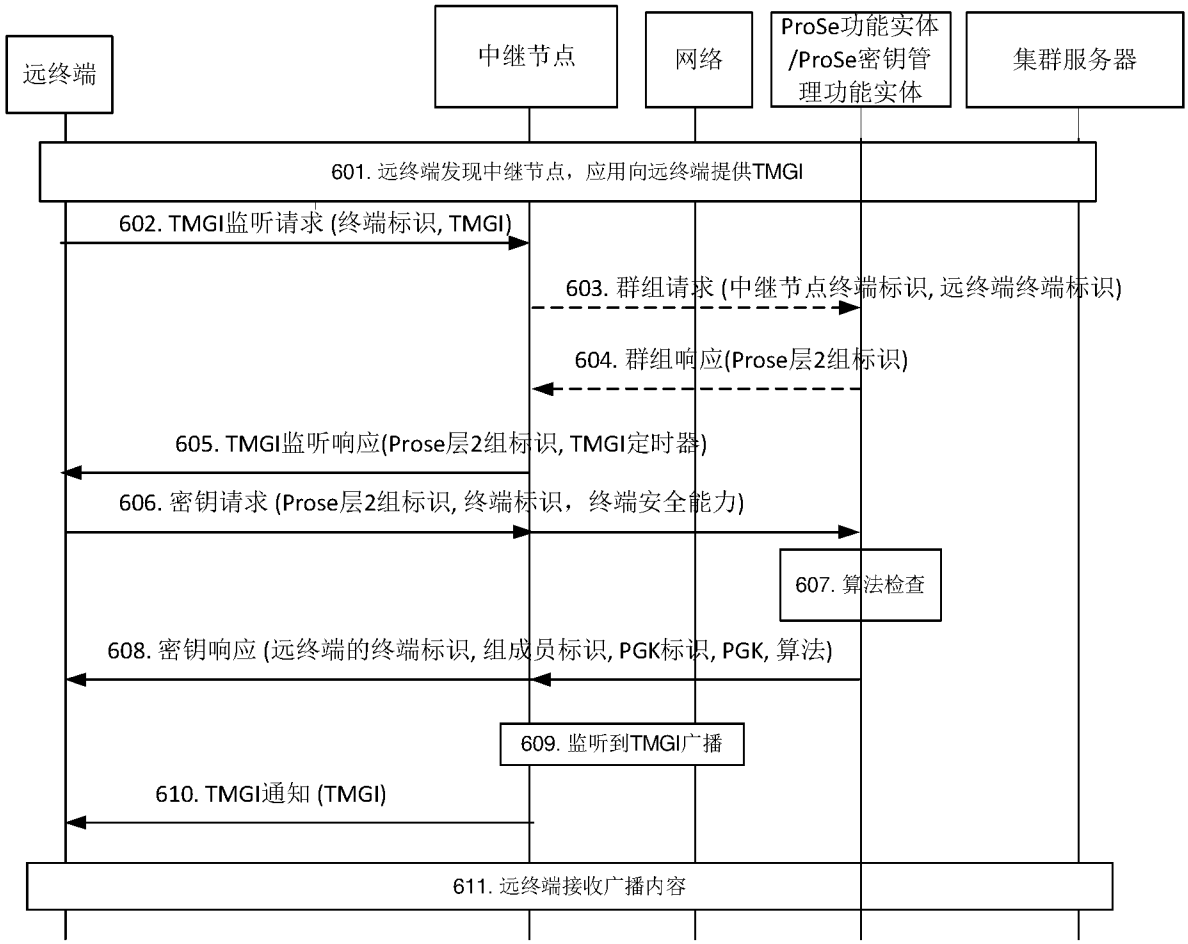
远终端
中继节点
网络
ProSe功能实体/ProSe密钥管理功能实体
集群服务器
601. 远终端发现中继节点，应用向远终端提供TMGI
602. TMGI监听请求 (终端标识, TMGI)
603. 群组请求 (中继节点终端标识, 远终端终端标识)
604. 群组响应(Prose层2组标识)
605. TMGI监听响应(Prose层2组标识, TMGI定时器)
606. 密钥请求 (Prose层2组标识, 终端标识，终端安全能力)
607. 算法检查
608. 密钥响应 (远终端的终端标识, 组成员标识, PGK标识, PGK, 算法)
609. 监听到TMGI广播
610. TMGI通知 (TMGI)
611. 远终端接收广播内容

图 6

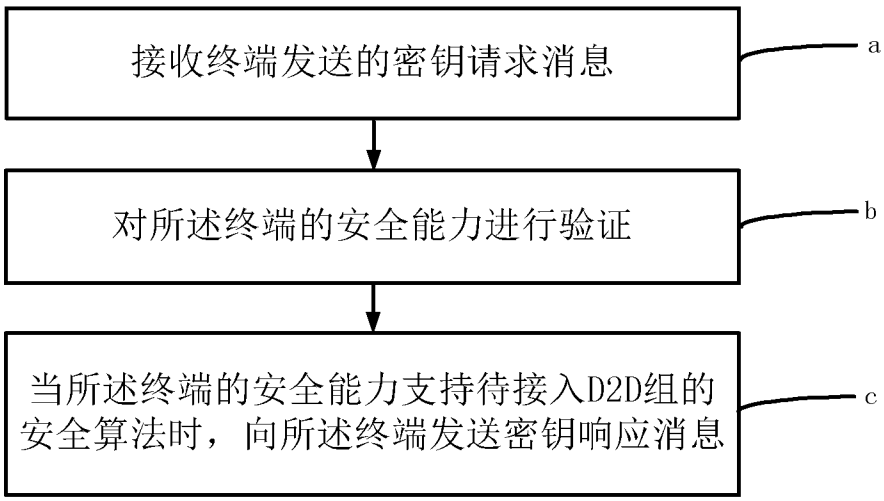
接收终端发送的密钥请求消息
a
对所述终端的安全能力进行验证
b
当所述终端的安全能力支持待接入D2D组的安全算法时，向所述终端发送密钥响应消息
c

图 7

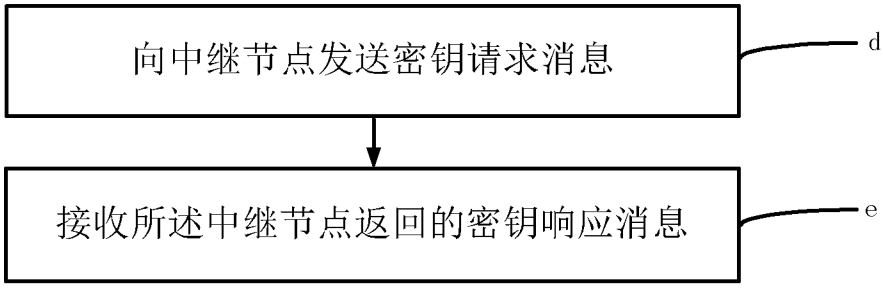
向中继节点发送密钥请求消息
d
接收所述中继节点返回的密钥响应消息
e

图 8

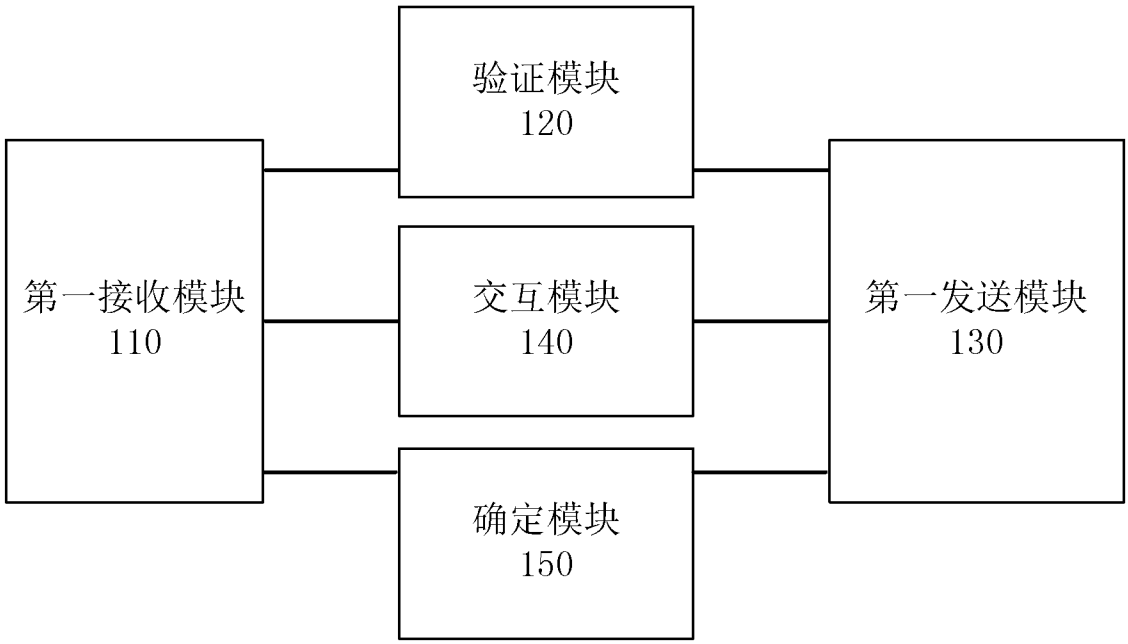
验证模块
120
第一接收模块
110
交互模块
140
第一发送模块
130
确定模块
150

图 9

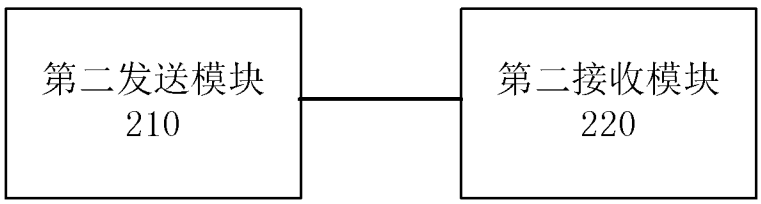
第二发送模块
210
第二接收模块
220

图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/092118

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/00 (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)

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; IEEE: relay, D2D, device, secure, key, M2M, machine, verify, group, monitor, listen

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103297961 A (ALCATEL-LUCENT SHANGHAI BELL CO., LTD.), 11 September 2013 (11.09.2013), description, paragraphs [0054]-[0095]	8, 15, 19
A	CN 103297961 A (ALCATEL-LUCENT SHANGHAI BELL CO., LTD.), 11 September 2013 (11.09.2013), description, paragraphs [0054]-[0095]	1-7, 9-14, 16-18
A	CN 103959739 A (BROADCOM CORPORATION), 30 July 2014 (30.07.2014), the whole document	1-19
A	CN 102984699 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED), 20 March 2013 (20.03.2013), the whole document	1-19
A	WO 2014126386 A1 (SAMSUNG ELECTRONICS CO., LTD.), 21 August 2014 (21.08.2014), the whole document	1-19

☐ 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
19 November 2015 (19.11.2015)	**12 January 2016 (12.01.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **GAO, Fei** Telephone No.: (86-10) **62089174**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/092118

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103297961 A	11 September 2013	None	
CN 103959739 A	30 July 2014	GB 2497745 A	26 June 2013
		DE 112012005319 T5	02 October 2014
		GB 2497745 B	05 November 2014
		WO 2013093724 A3	13 February 2014
		WO 2013093724 A2	27 June 2013
		GB 201121795 D0	01 February 2012
		US 2013160101 A1	20 June 2013
CN 102984699 A	20 March 2013	None	
WO 2014126386 A1	21 August 2014	US 2014227997 A1	14 August 2014
		KR 20140102050 A	21 August 2014

国际检索报告

国际申请号
PCT/CN2015/092118

A. 主题的分类

H04W 12/00(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)

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;IEEE:设备，relay，D2D，device，secure，中继，安全，key，密钥，验证，群组，监听，M2M，machine，verify，group，monitor，listen

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 103297961 A (上海贝尔股份有限公司) 2013年 9月 11日 (2013-09-11) 说明书第[0054]-[0095]段	8，15，19
A	CN 103297961 A (上海贝尔股份有限公司) 2013年 9月 11日 (2013-09-11) 说明书第[0054]-[0095]段	1-7，9-14，16-18
A	CN 103959739 A (美国博通公司) 2014年 7月 30日 (2014-07-30) 全文	1-19
A	CN 102984699 A (中国联合网络通信集团有限公司) 2013年 3月 20日 (2013-03-20) 全文	1-19
A	WO 2014126386 A1 (三星电子有限公司) 2014年 8月 21日 (2014-08-21) 全文	1-19

☐ 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
2015年 11月 19日	2016年 1月 12日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	高菲
传真号 (86-10)62019451	电话号码 (86-10)62089174

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/092118

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	103297961	A	2013年 9月 11日	无			
CN	103959739	A	2014年 7月 30日	GB	2497745	A	2013年 6月 26日
				DE	112012005319	T5	2014年 10月 2日
				GB	2497745	B	2014年 11月 5日
				WO	2013093724	A3	2014年 2月 13日
				WO	2013093724	A2	2013年 6月 27日
				GB	201121795	D0	2012年 2月 1日
				US	2013160101	A1	2013年 6月 20日
CN	102984699	A	2013年 3月 20日	无			
WO	2014126386	A1	2014年 8月 21日	US	2014227997	A1	2014年 8月 14日
				KR	20140102050	A	2014年 8月 21日