(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 6 日 (06.10.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/155112 A1

(51) 国际专利分类号:
*H04W 12/06* (2009.01)

(21) 国际申请号: PCT/CN2015/080377

(22) 国际申请日: 2015 年 5 月 29 日 (29.05.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510157337.8 2015 年 4 月 3 日 (03.04.2015) CN

(71) 申请人: **宇龙计算机通信科技（深圳）有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.)** [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(72) 发明人: **张云飞 (ZHANG, Yunfei)**; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。 **郑倩 (ZHENG, Qian)**; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。 **雷艺学 (LEI, Yixue)**; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。 **张晨璐 (ZHANG, Chenlu)**; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(74) 代理人: **广州三环专利代理有限公司 (GUANGZHOU SCIHEAD PATENT AGENT CO., LTD)**; 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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。

(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,

[见续页]

(54) Title: AUTHENTICATION METHOD FOR INTERNET OF THINGS DEVICE AND TERMINAL

(54) 发明名称 : 一种物联网设备的认证方法及终端

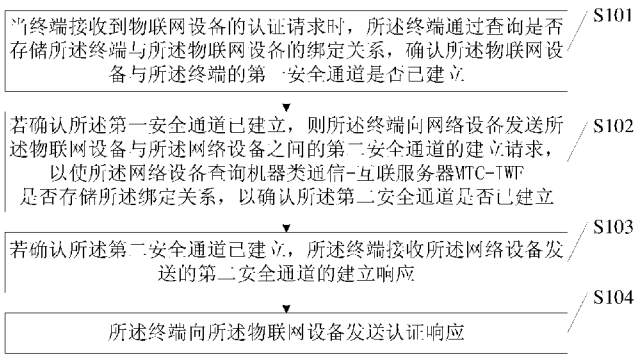


图 2

S101 WHEN A TERMINAL RECEIVES AN AUTHENTICATION REQUEST OF AN INTERNET OF THINGS DEVICE, THE TERMINAL DETERMINES WHETHER A FIRST SECURE CHANNEL BETWEEN THE INTERNET OF THINGS DEVICE AND THE TERMINAL IS ESTABLISHED BY QUERYING WHETHER A BINDING RELATIONSHIP BETWEEN THE TERMINAL AND THE INTERNET OF THINGS DEVICE IS STORED

S102 IF IT IS CONFIRMED THAT THE FIRST SECURE CHANNEL IS ESTABLISHED, THE TERMINAL SENDS AN ESTABLISHMENT REQUEST FOR A SECOND SECURE CHANNEL BETWEEN THE INTERNET OF THINGS DEVICE AND A NETWORK DEVICE TO THE NETWORK DEVICE, SO THAT THE NETWORK DEVICE QUERIES WHETHER A MACHINE TYPE COMMUNICATION-INTER-WORKING FUNCTION (MTC-IWF) STORES THE BINDING RELATIONSHIP, SO AS TO CONFIRM WHETHER THE SECOND SECURE CHANNEL IS ESTABLISHED

S103 IF IT IS CONFIRMED THAT THE SECOND SECURE CHANNEL IS ESTABLISHED, THE TERMINAL RECEIVES A SECOND SECURE CHANNEL ESTABLISHMENT RESPONSE SENT BY THE NETWORK DEVICE

S104 THE TERMINAL SENDS AN AUTHENTICATION RESPONSE TO THE INTERNET OF THINGS DEVICE

(57) **Abstract**: An authentication method for an Internet of Things device and a terminal. The method comprises: when a terminal receives an authentication request of an Internet of Things device, the terminal determines whether a first secure channel between the Internet of Things device and the terminal is established by querying whether a binding relationship between the terminal and the Internet of Things device is stored; if it is confirmed that the first secure channel is established, the terminal sends an establishment request for a second secure channel between the Internet of Things device and a network device to the network device; if it is confirmed that the second secure channel is established, the terminal receives a second secure channel establishment response sent by the network device; and the terminal sends an authentication response to the Internet of Things device. Also disclosed is a corresponding terminal. In the present invention, by binding an Internet of Things device to an intelligent terminal for a network access authentication, storage and synchronization costs of a network side background can be reduced, and the problem of insufficient Internet of Things device identification is also solved at the same time, so that the lightweight security authentication process for an Internet of Things device to access a mobile network can be realized.

(57) 摘要:

[见续页]

WO 2016/155112 A1

RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, 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))。

一种物联网设备的认证方法及终端。其中的方法包括：当终端接收到物联网设备的认证请求时，终端通过查询是否存储终端与物联网设备的绑定关系，确认物联网设备与终端的第一安全通道是否已建立；若确认第一安全通道已建立，则终端向网络设备发送物联网设备与网络设备之间的第二安全通道的建立请求；若确认第二安全通道已建立，终端接收网络设备发送的第二安全通道的建立响应；终端向物联网设备发送认证响应。还公开了相应的终端。本发明通过将物联网设备绑定智能终端进行接入网络的认证，可以减少网络侧后台的存储和同步成本，同时也解决了物联网设备标识不足的问题，从而可以实现物联网设备的接入移动网络的轻量级安全性鉴权过程。

# 一种物联网设备的认证方法及终端

本申请要求于2015年04月03日提交中国专利局，申请号为201510157337.8、发明名称为“一种物联网设备的认证方法及终端”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

本发明涉及物联网技术领域，尤其涉及一种物联网设备的认证方法及终端。

## 背景技术

伴随着物联网的快速发展，物联网设备即机器类型通信(Machine Type Communication，MTC)设备已经成为一类新的网络安全威胁，曾经出现在互联网上的攻击技术，如分布式拒绝服务(Distributed Denial of Service，DDoS)、证书盗窃等，都可能出现在物联网上，例如数以千计的烤箱对InfoWord网站发动大规模DDoS攻击，致使网站的后台服务瘫痪。一个有效的解决途径是对物联网设备展开普遍的身份认证。

在第三代合作伙伴计划(3rd Generation Partnership Project，3GPP)MTC网络架构中，物联网设备通过短信注册流程认证设备，MTC设备基于短信注册的安全架构如图1所示。为了对MTC设备的身份进行识别，防止非法的设备接入移动通信网络，后台归属用户服务器(Home Subscriber Server，HSS)/归属位置寄存器(Home Location Register，HLR)需要存储每个MTC设备的用户信息和签约数据，随着物联网技术的日趋发展和成熟，应用领域的多元化， MTC设备数量将出现爆炸性增长发展到百亿数量级，甚至比现在智能终端数量还要多几个量级，数以百亿数量级的设备数量对于后台的存储和同步是很大的成本。且MTC设备的用户标识即移动台国际用户识别码(Mobile Subscriber International

ISDN number，MSISDN)在国际标准中有16位长度限制，因此MSISDN的地址空间可能不足以支持未来海量的MTC设备。

因此，如何实现物联网设备的轻量级认证过程，是目前需要解决的问题。

## 发明内容

本发明提供了一种物联网设备的认证方法及终端，以实现物联网设备的轻量级认证。

一方面，提供了一种物联网设备的认证方法，所述方法包括:

当所述终端接收到物联网设备的认证请求时，所述终端通过查询是否存储所述终端与所述物联网设备的绑定关系，确认所述物联网设备与所述终端的第一安全通道是否已建立;

若确认所述第一安全通道已建立，则所述终端向网络设备发送所述物联网设备与所述网络设备之间的第二安全通道的建立请求，以使所述网络设备查询机器类型通信互通功能 MTC-IWF 是否存储所述绑定关系，以确认所述第二安全通道是否已建立;

若确认所述第二安全通道已建立，所述终端接收所述网络设备发送的第二安全通道的建立响应;

所述终端向所述物联网设备发送认证响应。

另一方面，提供了一种终端，包括:

确认单元，用于当接收到物联网设备的认证请求时，通过查询是否存储终端与所述物联网设备的绑定关系，确认所述物联网设备与所述终端的第一安全通道是否已建立;

第一发送单元，用于若确认所述第一安全通道已建立，则向网络设备发送所述物联网设备与所述网络设备之间的第二安全通道的建立请求，以使所述网络设备查询机器类型通信互通功能 MTC-IWF 是否存储所述绑定关系，以确认所述第二安全通道是否已建立;

接收单元，用于若确认所述第二安全通道已建立，接收所述网络设备发送的第二安全通道的建立响应;

第二发送单元，用于向所述物联网设备发送认证响应。

可见，根据本发明提供的一种物联网设备的认证方法及终端，通过将物联网设备绑定智能终端进行接入网络的认证，可以减少网络侧后台的存储和同步成本，同时也解决了物联网设备标识不足的问题，从而可以实现物联网设备的接入移动网络的轻量级安全性鉴权过程。

## 附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为现有技术中的 MTC 设备基于短信注册的安全架构示意图；

图 2 为本发明实施例提供的一种物联网设备的认证方法的流程示意图；

图 3 为本发明实施例提供的另一种物联网设备的认证方法的流程示意图；

图 4 为本发明实施例提供的 MTC 设备绑定智能终端进行认证的安全架构示意图；

图 5 为本发明实施例提供的一种终端的结构示意图；

图 6 为本发明实施例提供的另一种终端的结构示意图。

## 具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

本发明适用于物联网设备接入移动网络时的认证场景，本发明通过将物联网设备绑定智能终端进行接入网络的认证，可以减少网络侧后台的存储和同步成本，同时也解决了物联网设备标识不足的问题，从而可以实现物联网设备的接入移动网络的轻量级安全性鉴权过程。

本发明所涉及的终端可以是手机、平板电脑等可以接入网络的终端设备。

下面结合图 2-图 4，对本发明实施例提供的一种物联网设备的认证方法进行详细描述：

请参阅图 2，为本发明实施例提供的一种物联网设备的认证方法的流程示意图，该方法包括以下步骤：

步骤 S101，当终端接收到物联网设备的认证请求时，所述终端通过查询是否存储所述终端与所述物联网设备的绑定关系，确认所述物联网设备与所述终端的第一安全通道是否已建立。

物联网设备在接入移动网络之前，首先要进行认证。本实施例中由终端绑定一个或多个物联网设备，并存储终端与物联网设备的绑定关系。终端接收物联网设备的认证请求，并通过查询是否存储终端与物联网设备的绑定关系，确认物联网设备与终端的第一安全通道是否已建立；若没有存储该物联网设备与终端的绑定关系，则确认该物联网设备不能通过该终端进行安全认证。

步骤 S102，若确认所述第一安全通道已建立，则所述终端向网络设备发送所述物联网设备与所述网络设备之间的第二安全通道的建立请求，以使所述网络设备查询机器类型通信互通功能 MTC-IWF 是否存储所述绑定关系，以确认所述第二安全通道是否已建立。

若终端已确认物联网设备与终端的第一安全通道已建立，则终端向网络设备请求建立物联网设备与网络设备之间的第二安全通道，以使物联网设备真正通过接入网络的认证。终端与网络设备的通信属于现有技术，只不过在这里终端与网络设备通信的内容是确认网络设备是否允许物联网设备通过终端接入网络。进行确认的根据是在机器类型通信互通功能(Machine Type Communication-Inter Working Function，MTC-IWF)中存储的终端与物联网设备的绑定关系。若网络设备接收到第二安全通道的建立请求后，在 MTC-IWF 查询是否存储了该绑定关系，然后向终端进行响应，以确认该第二安全通道是否已建立。

在现有技术中，如图 1 所示，网络侧后台需要一一存储每个物联网设备的用户信息和签约数据，而在本实施例中，仅需根据物联网设备的标识如移动设备国际身份码(International Mobile Equipment Identity，IMEI)、终端的标识如

IMEI、全球用户识别卡(Universal Subscriber Identity Module，USIM)等建立一对一或一对多的简单的绑定关系或映射关系即可。终端与网络设备的签约认证是已经存在的。因此，可以减少网络侧后台的存储和同步成本。且由于是物联网设备绑定终端，不再受物联网设备的用户标识的长度限制，在该终端下的物联网设备可以采用任意的标识，各个终端的物联网设备的标识可以相同或不同。

步骤 S103，若确认所述第二安全通道已建立，所述终端接收所述网络设备发送的第二安全通道的建立响应。

若网络设备确认该第二安全通道已建立，终端接收网络设备发送的请求建立第二安全通道的响应消息，则确认该第二安全通道已建立。

步骤 S104，所述终端向所述物联网设备发送认证响应。

若终端确认该物联网设备的第一安全通道和第二安全通道都已经建立，则认为这是一个被许可的安全通信链路，该物联网设备也被判定为一个安全的通信设备，可以响应该物联网设备的认证请求。

根据本发明实施例提供的一种物联网设备的认证方法，通过将物联网设备绑定智能终端进行接入网络的认证，可以减少网络侧后台的存储和同步成本，同时也解决了物联网设备标识不足的问题，从而可以实现物联网设备的接入移动网络的轻量级安全性鉴权过程。

请参阅图 3，为本发明实施例提供的另一种物联网设备的认证方法的流程示意图，该方法包括以下步骤:

步骤 S201，终端建立所述终端与至少一个物联网设备的绑定关系。

本实施例中通过预置软件根据物联网设备的标识如 IMEI、终端的标识如 IMEI、全球用户识别卡(Universal Subscriber Identity Module，USIM)等建立一对一或一对多的简单的绑定关系或映射关系。如图 4 所示的本发明实施例提供的 MTC 设备绑定智能终端进行认证的安全架构示意图，智能终端与 MTC 设备 1 至 MTC 设备 N 进行绑定。

步骤 S202，所述终端存储所述绑定关系。

该终端可以在本地或者在云端等存储该绑定关系，这里不作限定。

步骤 S203，所述终端向网络设备发送绑定关系建立或更新消息，以使所述网络设备将所述绑定关系发送给所述 MTC-IWF，以使所述 MTC-IWF 建立或更新所述终端与所述物联网设备的绑定关系。

网络侧也需存储物联网设备与终端的简单的绑定关系，以作为对物联网设备接入网络进行认证的根据，绑定关系可以由 MTC-IWF 存储或管理。需要说明的是，MTC-IWF 可以是一个独立的功能实体，也可以是分散在各个网络设备中的功能模块。

如图 4 所示，该安全架构中包括两种网络设备，即：移动管理实体(Mobility Management Entity，MME)和 MTC 应用服务器(MTC Server)，MME 和 MTC 应用服务器都与 MTC-IWF 连接，终端可以通过路径 1 将绑定关系由 MME 接收、解析后转发给 MTC-IWF，也可以通过路径 2 将绑定关系由 MTC 应用服务器接收、解析后转发给 MTC-IWF。

若 MTC-IWF 中已经存在属于该终端的绑定关系表或映射表，则无需新建，只需要更新该映射表的映射关系或绑定关系即可。

步骤 S204，当所述终端接收到物联网设备的认证请求时，所述终端通过查询是否存储所述终端与所述物联网设备的绑定关系，确认所述物联网设备与所述终端的第一安全通道是否已建立。

该步骤与前述实施例的步骤 S101 相同，在此不再赘述。

步骤 S205，若确认所述第一安全通道已建立，则所述终端向所述核心网设备发送所述第二安全通道的建立请求，以使所述核心网设备查询机器类型通信互通功能 MTC-IWF 是否存储所述绑定关系，以确认所述第二安全通道是否已建立，所述建立请求为所述无线资源控制层消息或非无线资源控制层消息。

可替换的是，步骤 S205 也可以是：若确认所述第一安全通道已建立，则所述终端向机器类型通信 MTC 应用服务器发送所述第二安全通道的建立请求，以使所述 MTC 应用服务器查询机器类型通信互通功能 MTC-IWF 是否存储所述绑定关系，以确认所述第二安全通道是否已建立，所述建立请求为应用层消息。

第二安全通道的建立可以通过如图 4 的路径 1 或路径 2 进行。

作为一种实施方式，通过路径 1 建立第二安全通道，该网络设备为核心网

设备，如 MME 等，可选地，在终端与核心网设备通信之前，若终端在网络中处于断开连接状态，则先利用现有的网络鉴权机制请求接入移动网络，在网络侧同意终端的接入请求后变成连接状态。在确认终端与核心网设备之间为连接状态后，终端向核心网设备发送第二安全通道的建立请求，具体的，该建立请求可以是非接入层(Non-Access Stratum，NAS)消息或无线资源控制(Radio Resource Control，RRC)消息。MME 通过 MTC-IWF 实体识别智能终端和它的从属 MTC 设备关系是否存在，若存在，则给出同意智能终端作为中继接入网络的响应。

需要说明的是，在该实施方式中，终端与物联网设备的绑定关系对网络侧可见，从而使网络设备可以区分物联网设备从而实现分类管控和计费。

作为一种实施方式，通过路径 2 建立第二安全通道，该网络设备为 MTC 应用服务器。终端向 MTC 应用服务器发送第二安全通道的建立请求，具体的，该建立请求为应用层消息。MTC 应用服务器通过 MTC-IWF 实体识别智能终端和它的从属 MTC 设备关系是否存在，若存在，则给出同意智能终端作为中继接入网络的响应。

需要说明的是，在该实施方式中，终端与物联网设备的绑定关系对网络侧不可见，对网络侧可见的始终是智能终端，由智能终端承担所有物联网设备数据消费的流量。

步骤 S206，若确认所述第二安全通道已建立，所述终端接收所述网络设备发送的第二安全通道的建立响应。

该步骤与前述实施例的步骤 S103 相同，在此不再赘述。

步骤 S207，所述终端向所述物联网设备发送认证响应。

该步骤与前述实施例的步骤 S104 相同，在此不再赘述。

根据本发明实施例提供的一种物联网设备的认证方法，通过将物联网设备绑定智能终端进行接入网络的认证，可以减少网络侧后台的存储和同步成本，同时也解决了物联网设备标识不足的问题，从而可以实现物联网设备的接入移动网络的轻量级安全性鉴权过程。

下面结合图 5-图 6，对实现本发明实施例提供的一种物联网设备的认证方

法的终端进行详细描述:

请参阅图 5，为本发明实施例提供的一种终端的结构示意图，该终端 1000 包括:

确认单元 11，用于当终端接收到物联网设备的认证请求时，通过查询是否存储所述终端与所述物联网设备的绑定关系，确认所述物联网设备与所述终端的第一安全通道是否已建立。

物联网设备在接入移动网络之前，首先要进行认证。本实施例中由终端绑定一个或多个物联网设备，并存储终端与物联网设备的绑定关系。终端接收物联网设备的认证请求，并通过查询是否存储终端与物联网设备的绑定关系，确认物联网设备与终端的第一安全通道是否已建立; 若没有存储该物联网设备与终端的绑定关系，则确认该物联网设备不能通过该终端进行安全认证。

第一发送单元 12，用于若确认所述第一安全通道已建立，则向网络设备发送所述物联网设备与所述网络设备之间的第二安全通道的建立请求，以使所述网络设备查询机器类型通信互通功能 MTC-IWF 是否存储所述绑定关系，以确认所述第二安全通道是否已建立。

若确认单元 11 已确认物联网设备与终端的第一安全通道已建立，则第一发送单元 12 向网络设备请求建立物联网设备与网络设备之间的第二安全通道，以使物联网设备真正通过接入网络的认证。终端与网络设备的通信属于现有技术，只不过在这里终端与网络设备通信的内容是确认网络设备是否允许物联网设备通过终端接入网络。进行确认的根据是在 MTC-IWF 中存储的终端与物联网设备的绑定关系。若网络设备接收到第二安全通道的建立请求后，在 MTC-IWF 查询是否存储了该绑定关系，然后向终端进行响应，以确认该第二安全通道是否已建立。

在现有技术中，如图 1 所示，网络侧后台需要一一存储每个物联网设备的用户信息和签约数据，而在本实施例中，仅需根据物联网设备的标识如 IMEI、终端的标识如 IMEI、USIM 等建立一对一或一对多的简单的绑定关系或映射关系即可。终端与网络设备的签约认证是已经存在的。因此，可以减少网络侧后台的存储和同步成本。且由于是物联网设备绑定终端，不再受物联网设备的用户标识的长度限制，在该终端下的物联网设备可以采用任意的标识，各个终

端的物联网设备的标识可以相同或不同。

接收单元 13，用于若确认所述第二安全通道已建立，接收所述网络设备发送的第二安全通道的建立响应。

若网络设备确认该第二安全通道已建立，接收单元 13 接收网络设备发送的请求建立第二安全通道的响应消息，则确认该第二安全通道已建立。

第二发送单元 14，用于向所述物联网设备发送认证响应。

若终端确认该物联网设备的第一安全通道和第二安全通道都已经建立，则认为这是一个被许可的安全通信链路，该物联网设备也被判定为一个安全的通信设备，可以响应该物联网设备的认证请求。

根据本发明实施例提供的一种终端，通过将物联网设备绑定智能终端进行接入网络的认证，可以减少网络侧后台的存储和同步成本，同时也解决了物联网设备标识不足的问题，从而可以实现物联网设备的接入移动网络的轻量级安全性鉴权过程。

请参阅图 6，为本发明实施例提供的另一种终端的结构示意图，该终端 2000 包括:

建立单元 21，用于建立终端与至少一个物联网设备的绑定关系。

本实施例中通过预置软件根据物联网设备的标识如 IMEI、终端的标识如 IMEI、USIM 等建立一对一或一对多的简单的绑定关系或映射关系。如图 4 所示的本发明实施例提供的 MTC 设备绑定智能终端进行认证的安全架构示意图，智能终端与 MTC 设备 1 至 MTC 设备 N 进行绑定。

存储单元 22，用于存储所述绑定关系。

存储单元 22 可以在本地或者在云端等存储该绑定关系，这里不作限定。

第三发送单元 23，用于向网络设备发送绑定关系建立或更新消息，以使所述网络设备将所述绑定关系发送给所述 MTC-IWF，以使所述 MTC-IWF 建立或更新所述终端与所述物联网设备的绑定关系。

网络侧也需存储物联网设备与终端的简单的绑定关系，以作为对物联网设备接入网络进行认证的根据，绑定关系可以由 MTC-IWF 存储或管理。需要说明的是，MTC-IWF 可以是一个独立的功能实体，也可以是分散在各个网络设

备中的功能模块。

如图 4 所示，该安全架构中包括两种网络设备，即： MME 和 MTC 应用服务器，MME 和 MTC 应用服务器都与 MTC-IWF 连接，终端可以通过路径 1 将绑定关系由 MME 接收、解析后转发给 MTC-IWF，也可以通过路径 2 将绑定关系由 MTC 应用服务器接收、解析后转发给 MTC-IWF。

若 MTC-IWF 中已经存在属于该终端的绑定关系表或映射表，则无需新建，只需要更新该映射表的映射关系或绑定关系即可。

确认单元 24，用于当所述终端接收到物联网设备的认证请求时，通过查询是否存储所述终端与所述物联网设备的绑定关系，确认所述物联网设备与所述终端的第一安全通道是否已建立。

该确认单元 24 的功能与前述实施例的确认单元 11 相同，在此不再赘述。

第一发送单元 25，用于若确认所述第一安全通道已建立，则向所述核心网设备发送所述第二安全通道的建立请求，以使所述核心网设备查询机器类型通信互通功能 MTC-IWF 是否存储所述绑定关系，以确认所述第二安全通道是否已建立，所述建立请求为所述无线资源控制层消息或非无线资源控制层消息。

可替换的是，第一发送单元 25 也可以用于：若确认所述第一安全通道已建立，则向机器类型通信 MTC 应用服务器发送所述第二安全通道的建立请求，以使所述 MTC 应用服务器查询机器类型通信互通功能 MTC-IWF 是否存储所述绑定关系，以确认所述第二安全通道是否已建立，所述建立请求为应用层消息。

第二安全通道的建立可以通过如图 4 的路径 1 或路径 2 进行。

作为一种实施方式，通过路径 1 建立第二安全通道，该网络设备为核心网设备，如 MME 等，可选地，在终端与核心网设备通信之前，若终端在网络中处于断开连接状态，则先利用现有的网络鉴权机制请求接入移动网络，在网络侧同意终端的接入请求后变成连接状态。在确认终端与核心网设备之间为连接状态后，终端向核心网设备发送第二安全通道的建立请求，具体的，该建立请求可以是非接入层消息或无线资源控制(Radio Resource Control，RRC)消息。MME 通过 MTC-IWF 实体识别智能终端和它的从属 MTC 设备关系是否存在，

若存在，则给出同意智能终端作为中继接入网络的响应。

需要说明的是，在该实施方式中，终端与物联网设备的绑定关系对网络侧可见，从而使网络设备可以区分物联网设备从而实现分类管控和计费。

作为一种实施方式，通过路径 2 建立第二安全通道，该网络设备为 MTC 应用服务器。终端向 MTC 应用服务器发送第二安全通道的建立请求，具体的，该建立请求为应用层消息。MTC 应用服务器通过 MTC-IWF 实体识别智能终端和它的从属 MTC 设备关系是否存在，若存在，则给出同意智能终端作为中继接入网络的响应。

需要说明的是，在该实施方式中，终端与物联网设备的绑定关系对网络侧不可见，对网络侧可见的始终是智能终端，由智能终端承担所有物联网设备数据消费的流量。

接收单元 26，用于若确认所述第二安全通道已建立，接收所述网络设备发送的第二安全通道的建立响应。

该接收单元 26 的功能与前述实施例的接收单元 13 的功能相同，在此不再赘述。

第二发送单元 27，用于向所述物联网设备发送认证响应。

该第二发送单元 27 的功能与前述实施例的第二发送单元 14 相同，在此不再赘述。

根据本发明实施例提供的一种终端，通过将物联网设备绑定智能终端进行接入网络的认证，可以减少网络侧后台的存储和同步成本，同时也解决了物联网设备标识不足的问题，从而可以实现物联网设备的接入移动网络的轻量级安全性鉴权过程。

需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为根据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本发明可以用硬件实现，或固件实现，或它们的组合方式来实现。当使用软件实现时，可以将上述功能存储在计算机可读介质中或作为计算机可读介质上的一个或多个指令或代码进行传输。计算机可读介质包括计算机存储介质和通信介质，其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是计算机能够存取的任何可用介质。以此为例但不限于：计算机可读介质可以包括随机存取存储器(Random Access Memory，RAM)、只读存储器(Read-Only Memory，ROM)、电可擦可编程只读存储器(Electrically Erasable Programmable Read-Only Memory，EEPROM)、只读光盘(Compact Disc Read-Only Memory，CD-ROM)或其他光盘存储、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质。此外。任何连接可以适当的成为计算机可读介质。例如，如果软件是使用同轴电缆、光纤光缆、双绞线、数字用户线（Digital Subscriber Line，DSL）或者诸如红外线、无线电和微波之类的无线技术从网站、服务器或者其他远程源传输的，那么同轴电缆、光纤光缆、双绞线、DSL 或者诸如红外线、无线和微波之类的无线技术包括在所属介质的定影中。如本发明所使用的，盘（Disk）和碟（disc）包括压缩光碟（CD）、激光碟、光碟、数字通用光碟（DVD）、软盘和蓝光光碟，其中盘通常磁性的复制数据，而碟则用激光来光学的复制数据。上面的组合也应当包括在计算机可读介质的保护范围之内。

总之，以上所述仅为本发明技术方案的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

# 权 利 要 求

1、 一种物联网设备的认证方法，其特征在于，包括:

当所述终端接收到物联网设备的认证请求时，所述终端通过查询是否存储所述终端与所述物联网设备的绑定关系，确认所述物联网设备与所述终端的第一安全通道是否已建立;

若确认所述第一安全通道已建立，则所述终端向网络设备发送所述物联网设备与所述网络设备之间的第二安全通道的建立请求，以使所述网络设备查询机器类型通信互通功能 MTC-IWF 是否存储所述绑定关系，以确认所述第二安全通道是否已建立;

若确认所述第二安全通道已建立，所述终端接收所述网络设备发送的第二安全通道的建立响应;

所述终端向所述物联网设备发送认证响应。

2、如权利要求 1 所述的方法，其特征在于，所述终端接收所述物联网设备的认证请求之前，还包括:

所述终端建立所述终端与至少一个所述物联网设备的绑定关系;

所述终端存储所述绑定关系。

3、如权利要求 2 所述的方法，其特征在于，所述终端向网络设备发送所述物联网设备与所述网络设备之间的第二安全通道的建立请求之前，还包括:

所述终端向网络设备发送绑定关系建立或更新消息，以使所述网络设备将所述绑定关系发送给所述 MTC-IWF，以使所述 MTC-IWF 建立或更新所述终端与所述物联网设备的绑定关系。

4、如权利要求 1-3 任意一项所述的方法，其特征在于，所述终端向网络设备发送所述物联网设备与所述网络设备之间的第二安全通道的建立请求，包括:

所述终端向核心网设备发送所述第二安全通道的建立请求，所述建立请求

为无线资源控制层消息或非无线资源控制层消息。

5、如权利要求 1-3 任意一项所述的方法，其特征在于，所述终端向网络设备发送所述物联网设备与所述网络设备之间的第二安全通道的建立请求，包括:

所述终端向机器类型通信 MTC 应用服务器发送所述第二安全通道的建立请求，所述建立请求为应用层消息。

6、一种终端，其特征在于，包括:

确认单元，用于当接收到物联网设备的认证请求时，通过查询是否存储终端与所述物联网设备的绑定关系，确认所述物联网设备与所述终端的第一安全通道是否已建立;

第一发送单元，用于若确认所述第一安全通道已建立，则向网络设备发送所述物联网设备与所述网络设备之间的第二安全通道的建立请求，以使所述网络设备查询机器类型通信互通功能 MTC-IWF 是否存储所述绑定关系，以确认所述第二安全通道是否已建立;

接收单元，用于若确认所述第二安全通道已建立，接收所述网络设备发送的第二安全通道的建立响应;

第二发送单元，用于向所述物联网设备发送认证响应。

7、如权利要求 6 所述的终端，其特征在于，还包括:

建立单元，用于建立所述终端与至少一个所述物联网设备的绑定关系;

存储单元，用于存储所述绑定关系。

8、如权利要求 7 所述的终端，其特征在于，还包括:

第三发送单元，用于向网络设备发送绑定关系建立或更新消息，以使所述网络设备将所述绑定关系发送给所述 MTC-IWF，以使所述 MTC-IWF 建立或更新所述终端与所述物联网设备的绑定关系。

9、如权利要求 6-8 任意一项所述的终端，其特征在于，所述第一发送单元具体用于：

向核心网设备发送所述第二安全通道的建立请求，所述建立请求为无线资源控制层消息或非无线资源控制层消息。

10、如权利要求 6-8 任意一项所述的终端，其特征在于，所述第一发送单元具体用于：

向机器类型通信 MTC 应用服务器发送所述第二安全通道的建立请求，所述建立请求为应用层消息。

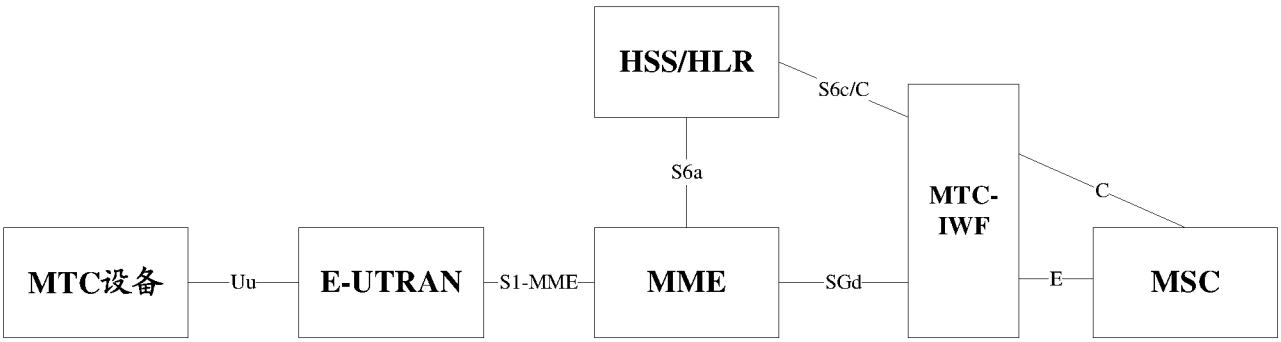
HSS/HLR
S6c/C
S6a
MTC-IWF
C
MTC设备
Uu
E-UTRAN
S1-MME
MME
SGd
E
MSC

图 1

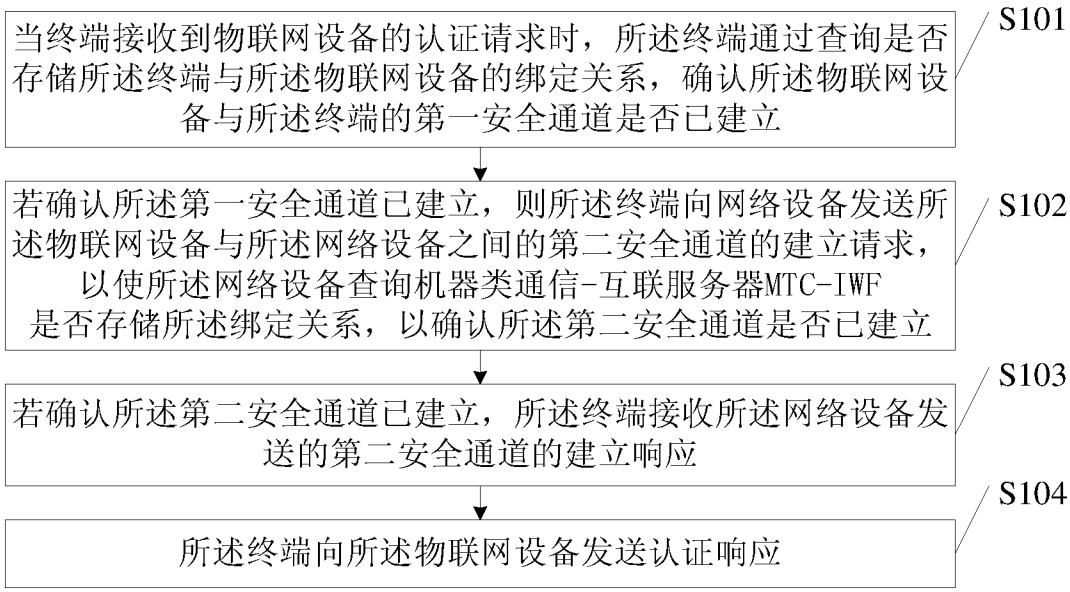
当终端接收到物联网设备的认证请求时，所述终端通过查询是否存储所述终端与所述物联网设备的绑定关系，确认所述物联网设备与所述终端的第一安全通道是否已建立
S101
若确认所述第一安全通道已建立，则所述终端向网络设备发送所述物联网设备与所述网络设备之间的第二安全通道的建立请求，以使所述网络设备查询机器类通信-互联服务器MTC-IWF是否存储所述绑定关系，以确认所述第二安全通道是否已建立
S102
若确认所述第二安全通道已建立，所述终端接收所述网络设备发送的第二安全通道的建立响应
S103
所述终端向所述物联网设备发送认证响应
S104

图 2

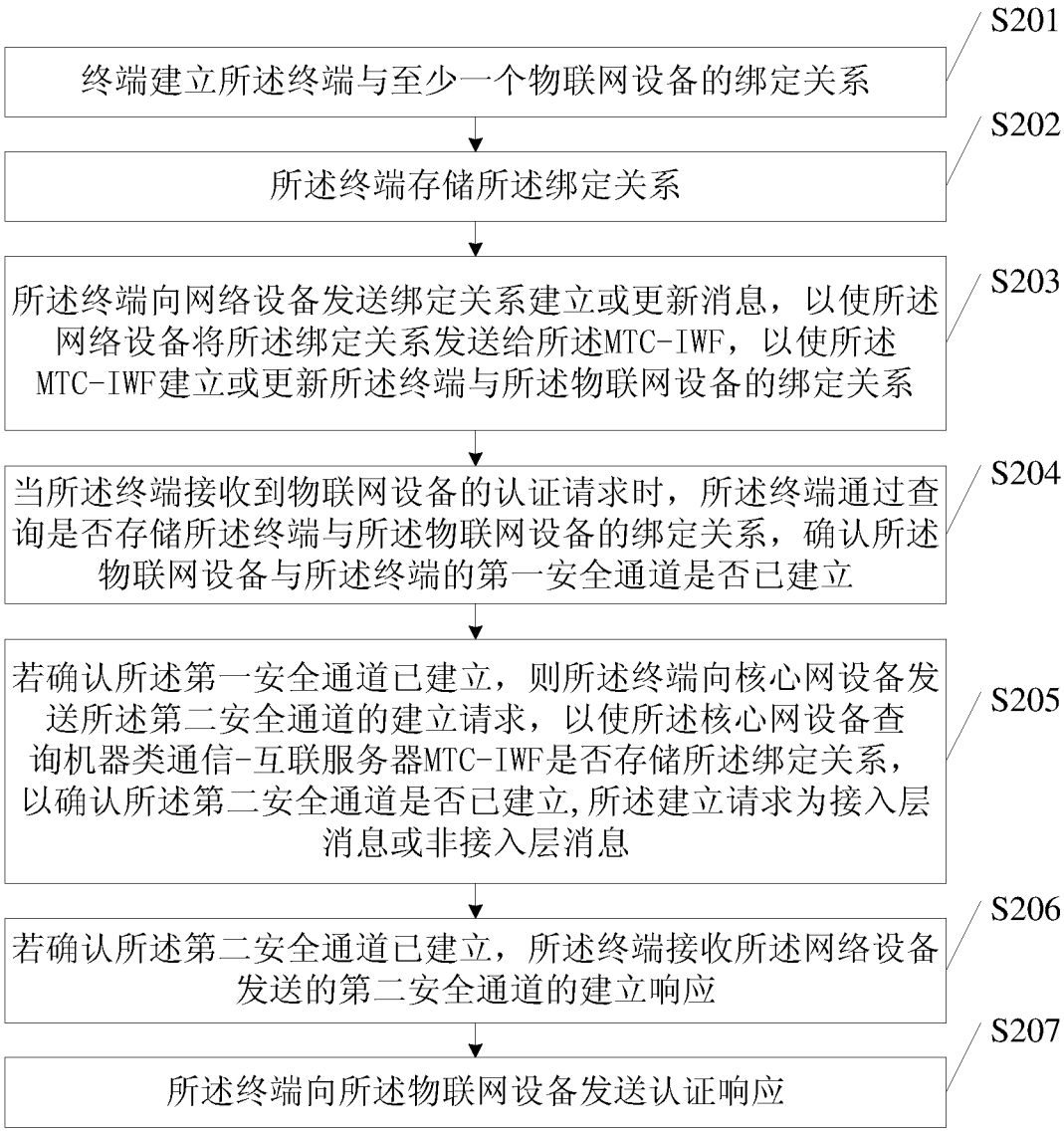
S201
终端建立所述终端与至少一个物联网设备的绑定关系
S202
所述终端存储所述绑定关系
S203
所述终端向网络设备发送绑定关系建立或更新消息，以使所述网络设备将所述绑定关系发送给所述MTC-IWF，以使所述MTC-IWF建立或更新所述终端与所述物联网设备的绑定关系
S204
当所述终端接收到物联网设备的认证请求时，所述终端通过查询是否存储所述终端与所述物联网设备的绑定关系，确认所述物联网设备与所述终端的第一安全通道是否已建立
S205
若确认所述第一安全通道已建立，则所述终端向核心网设备发送所述第二安全通道的建立请求，以使所述核心网设备查询机器类通信-互联服务器MTC-IWF是否存储所述绑定关系，以确认所述第二安全通道是否已建立,所述建立请求为接入层消息或非接入层消息
S206
若确认所述第二安全通道已建立，所述终端接收所述网络设备发送的第二安全通道的建立响应
S207
所述终端向所述物联网设备发送认证响应

图 3

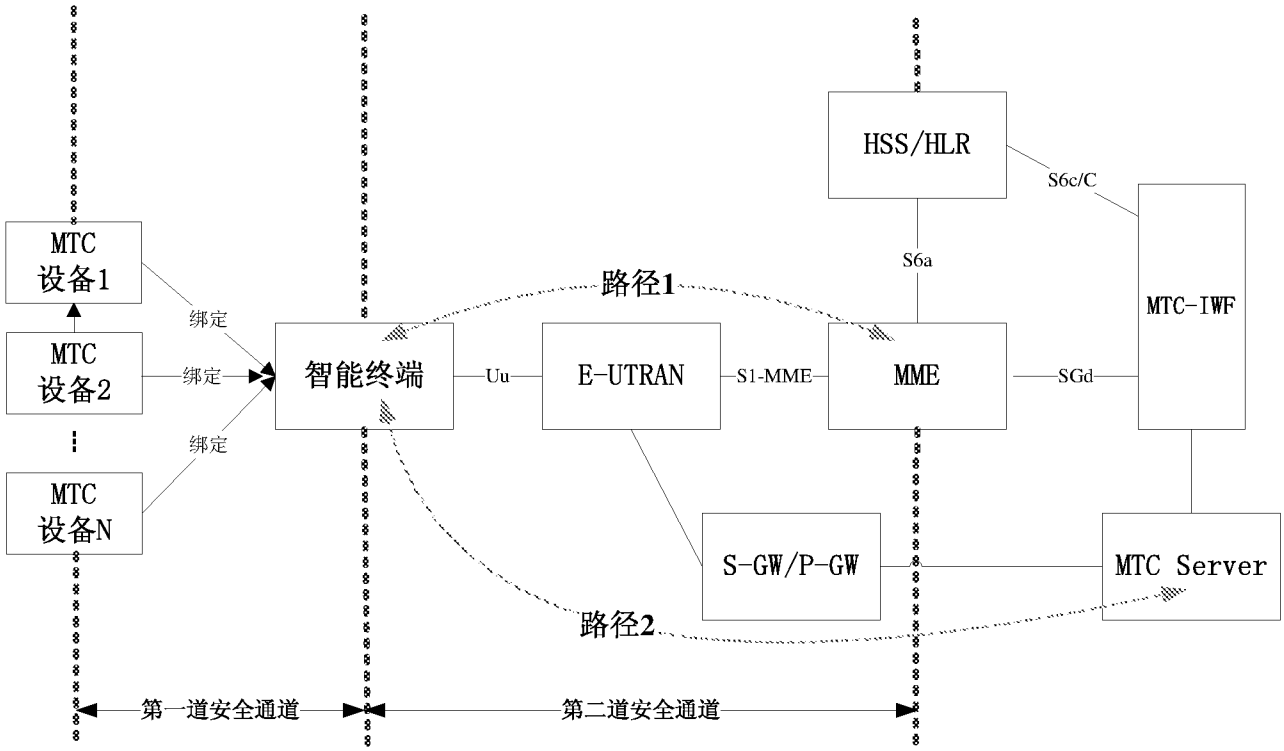
HSS/HLR
S6c/C
MTC
设备1
MTC
设备2
MTC
设备N
绑定
绑定
绑定
路径1
S6a
MTC-IWF
智能终端
Uu
E-UTRAN
S1-MME
MME
SGd
S-GW/P-GW
MTC Server
路径2
第一道安全通道
第二道安全通道

图 4

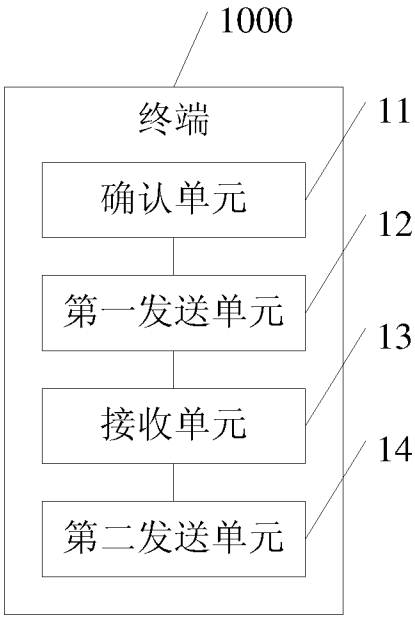
1000
终端
11
确认单元
12
第一发送单元
13
接收单元
14
第二发送单元

图 5

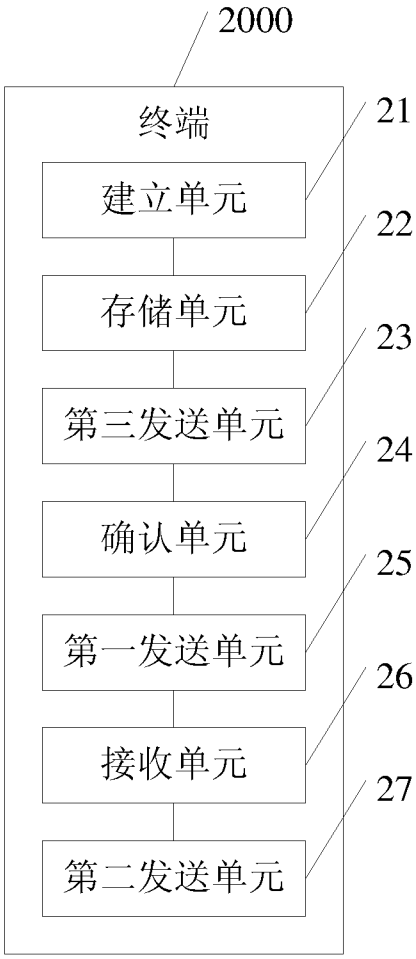
2000
终端
21
建立单元
22
存储单元
23
第三发送单元
24
确认单元
25
第一发送单元
26
接收单元
27
第二发送单元

图 6

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/CN2015/080377**

**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)

H04W, H04L, H04Q

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)

WPI, EPODOC, CNPAT, CNKI: machine type communication, internet of things, interworking function, MTC, M2M, Machine, IoT, things, authentic+, identi+, mobile, terminal, bind, associat+, IWF

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | CN 103250389 A (NEC EUROPE LTD.), 14 August 2013 (14.08.2013), description, paragraphs [0015]-[0016] and [0039] | 1-10 |
| A | CN 103107878 A (ZTE CORP.), 15 May 2013 (15.05.2013), the whole document | 1-10 |
| A | CN 102083212 A (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.), 01 June 2011 (01.06.2011), the whole document | 1-10 |
| A | US 2012284787 A1 (CLEMOT, O. et al.), 08 November 2012 (08.11.2012), the whole document | 1-10 |

☐ 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 December 2015 (19.12.2015) | **07 January 2016 (07.01.2016)** |
| Name and mailing address of the ISA/CN:<br>State Intellectual Property Office of the P. R. China<br>No. 6, Xitucheng Road, Jimenqiao<br>Haidian District, Beijing 100088, China<br>Facsimile No.: (86-10) 62019451 | Authorized officer<br>**WANG, Ming**<br>Telephone No.: (86-10) **62413679** |

# INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
**PCT/CN2015/080377**

| Patent Documents referred in the Report | Publication Date | Patent Family | Publication Date |
|---|---|---|---|
| CN 103250389 A | 14 August 2013 | KR 20130100164 A | 09 September 2013 |
| | | US 2013225130 A1 | 29 August 2013 |
| | | WO 2012126484 A1 | 27 September 2012 |
| | | EP 2601770 A1 | 12 June 2013 |
| | | JP 2014512718 A | 22 May 2014 |
| CN 103107878 A | 15 May 2013 | WO 2013071707 A1 | 23 May 2013 |
| | | US 2014302816 A1 | 09 October 2014 |
| | | EP 2744250 A1 | 18 June 2014 |
| CN 102083212 A | 01 June 2011 | WO 2011134397 A1 | 03 November 2011 |
| US 2012284787 A1 | 08 November 2012 | FR 2973909 A1 | 12 October 2012 |
| | | EP 2509025 A1 | 10 October 2012 |

# 国际检索报告

国际申请号 PCT/CN2015/080377

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)

H04W, H04L, H04Q

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）)

WPI,EPODOC,CNPAT,CNKI:机器类型通信，物联网，认证，鉴权，标识，识别，移动，终端，绑定，关联，互通功能，MTC, M2M, Machine, IoT, things, authentic+, identi+, mobile, terminal, bind, associat+, IWF

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 | CN 103250389 A (NEC欧洲有限公司) 2013年 8月 14日 (2013 - 08 - 14)<br>说明书第[0015]-[0016]段，[0039]段 | 1-10 |
| A | CN 103107878 A (中兴通讯股份有限公司) 2013年 5月 15日 (2013 - 05 - 15)<br>全文 | 1-10 |
| A | CN 102083212 A (大唐移动通信设备有限公司) 2011年 6月 1日 (2011 - 06 - 01)<br>全文 | 1-10 |
| A | US 2012284787 A1 (CLEMOT, OLIVIER 等) 2012年 11月 8日 (2012 - 11 - 08)<br>全文 | 1-10 |

☐ 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 12月 19日 | 2016年 1月 7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)<br>中国北京市海淀区蓟门桥西土城路6号 100088 | 王明 |
| 传真号 (86-10)62019451 | 电话号码 (86-10)62413679 |

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/080377

| 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 | 103250389 | A | 2013年 8月 14日 | KR | 20130100164 | A | 2013年 9月 9日 |
| | | | | US | 2013225130 | A1 | 2013年 8月 29日 |
| | | | | WO | 2012126484 | A1 | 2012年 9月 27日 |
| | | | | EP | 2601770 | A1 | 2013年 6月 12日 |
| | | | | JP | 2014512718 | A | 2014年 5月 22日 |
| CN | 103107878 | A | 2013年 5月 15日 | WO | 2013071707 | A1 | 2013年 5月 23日 |
| | | | | US | 2014302816 | A1 | 2014年 10月 9日 |
| | | | | EP | 2744250 | A1 | 2014年 6月 18日 |
| CN | 102083212 | A | 2011年 6月 1日 | WO | 2011134397 | A1 | 2011年 11月 3日 |
| US | 2012284787 | A1 | 2012年 11月 8日 | FR | 2973909 | A1 | 2012年 10月 12日 |
| | | | | EP | 2509025 | A1 | 2012年 10月 10日 |