(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
2011 年 4 月 14 日 (14.04.2011)

PCT

(10) 国际公布号
WO 2011/041967 A1

(51) 国际专利分类号:
H04W 12/00 (2009.01)

(21) 国际申请号: PCT/CN2010/076378

(22) 国际申请日: 2010 年 8 月 26 日 (26.08.2010)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200910205328.6 2009 年 10 月 10 日 (10.10.2009) 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): **吴强 (WU, Qiang)** [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)。 **黄兵 (HUANG, Bing)** [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)。 **姚春波 (YAO, Chunbo)** [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, 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。

[见续页]

(54) **Title**: METHOD FOR ANONYMOUS COMMUNICATION, METHOD FOR REGISTRATION, METHOD AND SYSTEM FOR TRASMITTING AND RECEIVING INFORMATION

(54) **发明名称** : 匿名通信的方法、注册方法、信息收发方法及系统

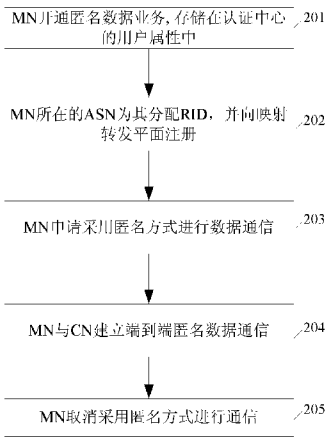

图 2 / FIG. 2

201 THE MN ACTIVATES AN ANONYMOUS DATA SERVICE, WHICH IS STORED IN THE USER ATTRIBUTE OF THE AUTHENTICATION CENTER
202 THE ASN OF THE MN ALLOCATES THE RID FOR THE MN, AND TRANSFERS THE PLANE REGISTRATION TO THE MAPPING
203 THE MN REQUESTS TO IMPLEMENT DATA COMMUNICATION IN ANONYMOUS WAY
204 THE MN ESTABLISHES AN END-TO-END ANONYMOUS DATA COMMUNICATION WITH CN
205 THE MN CANCELS IMPLEMENTING COMMUNICATION IN ANONYMOUS WAY

(57) **Abstract**: A method and system for anonymous communication are disclosed in the present invention, which are applied in identity and position separation based network architecture, the method includes: on receipt of an anonymous communication request sent from a terminal, the network allocates an anonymous identity for the terminal, and records the terminal state as anonymous communication state; when the terminal is in the anonymous communication state, on receipt of datagram sent from the terminal, the access network gateway equipment of the terminal replaces the source access identity in the datagram with the anonymous identity; and on receipt of the datagram sent to the terminal, the access network gateway equipment of the terminal replaces the anonymous identity in the datagram with the access identity of the terminal. With the present invention, an anonymous space is provided on the basis of real-name trusting domain, so as to meet the requirement of anonymous services development.

(57) **摘要**:

[见续页]

WO 2011/041967 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, 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, PT, RO, 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))。

本发明公开了一种匿名通信的方法及系统，应用于身份标识和位置分离架构网络，该方法包括：所述网络接收到终端发起的匿名通信请求后，为所述终端分配匿名身份标识，并将所述终端的状态记录为匿名通信状态；当所述终端处于匿名通信状态下时，所述终端所在的接入网关设备在收到所述终端发出的数据报文时，将所述数据报文中的源接入标识替换为所述匿名身份标识；在收到发往所述终端的数据报文时，将所述发往所述终端的数据报文中的匿名身份标识替换为所述终端的接入标识。本发明在构建了一个实名制信任域的基础上，提供一个匿名制的空间，以满足匿名业务开展的需要。

匿名通信的方法、注册方法、信息收发方法及系统

技术领域

本发明涉及通信技术领域，尤其涉及一种匿名通信的方法、注册方法、信息收发方法及系统。

背景技术

现有因特网广泛使用的传输控制协议/互联网络协议（Transmission Control Protocol/Internet Protocol，TCP/IP）中 IP 地址具有双重功能，既作为网络层的通信终端主机网络接口在网络拓扑中的位置标识，又作为传输层主机网络接口的身份标识。TCP/IP 设计之初并未考虑主机移动的情况。但是，当主机移动越来越普遍时，这种 IP 地址的语义过载缺陷日益明显。当主机的 IP 地址发生变化时，不仅路由要发生变化，通信终端主机的身份标识也发生变化，这样会导致路由负载越来越重，而且主机标识的变化会导致应用和连接的中断。身份标识和位置分离问题提出的目的是为了解决 IP 地址的语义过载和路由负载严重等问题，将 IP 地址的双重功能进行分离，实现对移动性、多家乡性、IP 地址动态重分配、减轻路由负载及下一代互联网中不同网络区域之间的互访等问题的支持。

现有技术中有关身份标识和位置分离的解决方案主要有两种，一种是基于主机的实现，另一种是基于路由器的实现，每种实现中又有相关的多种技术进行支持.基于主机的现有的主要协议是主机标识协议（Host Identity Protocol，简称 HIP），基于路由的现有主要协议是地址身份分离协议（Locator/ID Separation Protocol，简称 LISP）等。

HIP 是一种主机移动性关联协议，HIP 将 IP 地址分离为端标识与位置标识。HIP 的基本思想是在第三层网络层和第四层传输层之间引入了 3.5 层的主机标识层（Host Identity Layer，简称 HIL），即在域名空间和 IP 地址空间之间引入了主机标识（Host Identity，简称 HI）空间。主机标识层将原来紧密耦合的传输层和网络层分开，IP 地址不再扮演标识主机的角色，其只负责数据包的路由转发，即仅用作定位符，主机名称由主机标识符来表示。HIL 在逻

辑上位于网络层与传输层之间，传输层使用传输层标识符，由主机标识符层完成数据包中的主机标识符和 IP 地址转换。网络层对于传输层是屏蔽的，网络层的任何变化（例如，在通信过程中主机 IP 地址的变化）不会影响传输层链路，除非服务质量发生变化。

基于 HIP 协议的传输层的连接建立在主机标识之上，IP 地址只用于网络层路由，而不再用于标识主机身份。HIP 的关键思想就是断开网络层和传输层的紧密耦合，使应用层和传输层的连接不受 IP 地址变化的影响。当 IP 地址在一个连接中变化时，HI 保持不变，由此保证了连接的不中断。在支持 HIP 的主机中，IP 地址只是用于路由和寻址功能，而 HI 则用来标识一个连接所对应的终端主机，代替连接套接字中所使用的 IP 地址。

LISP 重用了路由技术，对现有的路由拓扑结构有了一定的改变，结合现有的传送网，利用最小的改造优化了现有的路由传送技术。

主机使用 IP 地址，在 LISP 系统中称为端标识（Endpoint Identifiers，EID）来跟踪 socket（套接字）、建立连接、发送和接收数据包。

路由器基于 IP 目的地址 RLOCs（Routing Locators，路由地址）传递数据包。

在 LISP 系统中引入了隧道路由，在发起主机包时封装 LISP 并且在最终传递到目的地前对数据包进行解封装。在 LISP 数据包中“外层报头”的 IP 地址是 RLOCs。在两个网络的主机之间进行端到端的包交换过程中，ITR（Ingress Tunnel Router，入口隧道路由器）为每个包封装一个新 LISP 头，在出口通道路由剥去新头。ITR 执行 EID-to-RLOC 查找以确定到 ETR（Egress Tunnel Router，出口隧道路由器）的路由路径，ETR 以 RLOC 作为它的一个地址。

LISP 为基于网络的协议，只影响网络部分，更确切的是只影响现有 Internet backbone（骨干网络）部分，不影响现有网络的接入层和用户主机，对主机是完全透明的。

在上述现有的身份标识和位置分离的解决方案中，都必须以用户的身份

标识查找对应的位置标识。该身份标识必须是通信节点的真实身份，身份标识必须在通讯节点之间传递，否则无法确定通讯节点的位置标识，无法建立通信节点间的联系。

出于安全性和业务特点的考虑，现有 Internet 网大量的应用业务以匿名方式开展，而现有身份标识和位置分离的解决方案无法满足以匿名方式的业务开展的需要。

发明内容

本发明要解决的技术问题是提供一种匿名通信的方法、注册方法、信息收发方法及系统，在身份标识和位置分离架构下构建实名制信任域的基础上，提供一个匿名制的空间，以满足匿名方式业务开展的需要。

为了解决上述问题，本发明提供了一种匿名通信的方法，应用于身份标识和位置分离架构网络，包括:

所述网络接收到终端发起的匿名通信请求后，为所述终端分配匿名身份标识，并将所述终端的状态记录为匿名通信状态;

当所述终端处于匿名通信状态下时，所述终端所在的接入网关设备在收到所述终端发出的数据报文时，将所述数据报文中的源接入标识替换为所述匿名身份标识；在收到发往所述终端的数据报文时，将所述发往所述终端的数据报文中的匿名身份标识替换为所述终端的接入标识。

所述为所述终端分配匿名身份标识的步骤中，由所述网络中的映射服务器、或所述终端所在的接入网关设备为所述终端分配所述匿名身份标识。

所述终端所在的接入网关设备为所述终端分配所述匿名身份标识的步骤还包括：将分配的所述匿名身份标识向所述映射服务器进行登记。

将所述终端的状态记录为匿名通信状态的步骤之前，所述方法还包括:

所述终端所在的接入网关设备在接收到所述匿名通信请求时，向认证中心发起鉴权流程，在确认所述终端具备匿名通信业务权限后，将所述终端记录为匿名通信状态。

所述方法还包括:

所述终端所在的接入网关设备在接收到所述终端的取消匿名通信请求后，将所述终端的状态由匿名通信状态改变为正常通信状态。

所述方法还包括:

所述终端所在的接入网关设备将所述终端的状态由匿名通信状态改变为正常通信状态后，在进行所述终端的数据报文的收发时，取消所述匿名身份标识的替换。

所述终端发起的所述匿名通信请求中携带时间段信息;

所述终端所在的接入网关设备在接收到所述匿名通信请求时，将所述终端的状态记录为匿名通信状态的步骤还包括:

根据所述匿名通信请求中的所述时间段信息设置匿名通信定时器；并在所述定时器到达定时周期后将所述终端的状态由匿名通信状态改变为正常通信状态。

本发明还提供了一种数据报文的转发方法，包括:

源端节点向目的节点发送数据报文，所述数据报文中包含目的地址和第一源地址;

源端接入节点接收到所述数据报文时，将所述数据报文中包含的所述第一源地址替换成为所述终端分配的第二源地址，并根据所述目的地址将所述数据报文转发至目的接入节点；以及

所述目的接入节点收到所述数据报文中后转发给所述目的节点。

所述方法还包括：所述目的节点收到所述数据报文后，以所述第二源地址作为目的地址向所述源端节点回应数据报文;

所述目的接入节点根据所述第二源地址将所述数据报文转发至所述源端接入节点;

所述源端节点收到所述回应数据报文后，将所述回应数据报文中包含的所述第二源地址替换成对应的所述第一源地址，转发给所述源端节点。

所述方法应用于身份标识与位置分离架构网络，所述第一源地址为所述终端的接入标识。

本发明还提供了一种匿名通信的注册方法，应用于身份标识与位置标识分离的架构网络中，所述架构网络至少包括第一节点、认证中心、第一接入节点及第一分配节点，其中，所述第一节点分配有一实际身份标识，包括:

第一节点经由第一接入节点向认证中心发送匿名通信请求;

所述认证中心接收所述匿名通信请求并判断所述第一节点是否具备匿名通信权限;

在第一节点具备匿名通信权限的情况下，所述第一接入节点向第一分配节点发送匿名身份标识分配请求，第一分配节点为第一节点分配一匿名身份标识，并保存该第一节点匿名身份标识与第一节点实际身份标识的对应关系，或第一节点的匿名身份标识与第一节点实际身份标识以及位置标识的对应关系。

所述方法还包括第一分配节点记录第一节点处于匿名通信状态，并将所述匿名身份标识发送至第一接入节点。

所述方法还包括:

所述匿名请求中包括时间段信息;

所述第一接入节点收到所述匿名请求时，根据所述时间段信息设置匿名通信定时器；并在所述定时器到达定时周期后将所述终端的状态由匿名通信状态改变为正常通信状态。

所述匿名身份标识自一预定用于匿名身份标识的标识群组中选择，或自一预定群组中选择。

本发明还提供了另一种匿名通信的注册方法，应用于身份标识与位置标识分离的架构网络中，所述架构网络至少包括有第一节点、第一接入节点及第一存储节点，其中，所述第一节点分配有一实际身份标识，包括:

第一节点经由第一接入节点向认证中心发送匿名通信请求;

所述认证中心接收所述匿名通信请求并判断所述第一节点是否具备匿名通信权限;

在第一节点具备匿名通信权限的情况下，所述第一接入节点为第一节点分配一匿名身份标识，同时向第一存储节点登记该第一节点匿名身份标识与

第一节点实际身份标识的对应关系，或第一节点的匿名身份标识与第一节点实际身份标识以及位置标识的对应关系。

所述方法还包括第一接入节点记录第一节点处于匿名通信状态。

所述方法还包括:

所述匿名请求中包括时间段信息;

所述第一接入节点收到所述匿名请求时，根据所述时间段信息设置匿名通信定时器；并在所述定时器到达定时周期后将所述终端的状态由匿名通信状态改变为正常通信状态。

本发明还提供了一种信息的发送方法，包括:

第一节点经由第一节点归属地的第一接入节点发送一信息至第二节点，所述信息至少包括有第一节点第一标识及第二节点第一标识；以及

第一节点归属地的第一接入节点替换第一节点第一标识为第一节点更新后第一标识后，采用第一节点第二标识及第二节点第二标识封装所述第一节点更新后的第一标识及第二节点第一标识，并发送至第二节点归属地的第二接入节点，并经由该第二节点归属地的第二接入节点解封后发送该信息至第二节点。

第一标识为身份标识，第二标识为位置标识，所述第一节点更新后的第一标识和/或第一节点第二标识及第二节点第二标识为第一接入节点本地获取，或自第一接入节点外的另一节点获取。

所述方法还包括，在第一接入节点接收所述信息时，还包括一判断所述信息发送是否触发替换程序的步骤。

本发明还提供了一种用以实现信息收发的系统，应用于身份与位置分离的架构网络中，包括:

接收单元，其设置为：接收第一节点发送至第二节点的信息，其中，所述信息至少包括有所述第一节点及第二节点的身份标识;

更新单元，其设置为：更新第一节点的身份标识为一匿名的身份标识;以及

封装单元，其设置为：封装第一节点和第二节点的位置标识在所述匿名身份标识及第二节点的身份标识外，以供身份与位置分离架构网络实现路由转发以发送信息至第二节点；

所述接收单元还设置为：在接收第二节点发送至第一节点的信息时，更新匿名的身份标识为第一节点的身份标识，并转发信息至第一节点。

本发明还提供了另一种用以实现信息收发的系统，应用于身份与位置分离的架构网络中，所述系统包括有第一系统及第二系统，其中，

第一系统包括：

第一收发单元，其设置为：接收第一节点发送至第二节点的第一信息，其中，所述第一信息包括有第一节点和第二节点的身份标识；接收第二系统第二收发单元发送的第二信息，其中，第二信息包括有第一节点的匿名身份标识及第二节点的身份标识；以及

第一替换单元，其设置为：在第一节点向第二节点发送第一信息时，更新第一节点的身份标识为匿名身份标识；以及在第二节点发送第二信息至第一节点时，更新匿名身份标识为第一节点的身份标识；

第二系统包括：

第二收发单元，其设置为：接收第一信息并转发至第一节点；向第一节点转发自第二节点的第二信息，其中，第二信息包括有第一节点的匿名身份标识及第二节点的身份标识。

在第一节点发送第一信息至第二节点时，第一节点的匿名身份标识用以标识信息的发送方，第二节点的身份标识用以标识信息的接收方，在第二节点发送第二信息至第一节点时，第一节点的匿名身份标识用以标识信息的接收方，第二节点的身份标识用以标识信息的发送方。

与现有技术相比，上述实施方案至少具有如下有益效果：提出一种身份标识和位置分离架构下匿名通信的解决方案，可以实现在构建了一个实名制信任域的基础上，提供一个匿名制的空间，以满足匿名业务开展的需要，在身份标识和位置分离架构下，实名制信任域由网络信用保证，匿名制空间由

网络根据业务授权开展业务。

附图概述

图 1 是基于身份位置分离架构的网络拓扑示意图;

图 2 是本发明实施例的匿名通信流程;

图 3 是终端用户登录接入流程;

图 4 本发明实施案例一的终端用户发起匿名通信信令流程;

图 5 是本发明实施案例一的建立端到端匿名通信流程;

图 6 是本发明实施案例一的终端用户取消匿名通信信令流程;

图 7 是本发明实施案例二的终端用户发起匿名通信信令流程。

本发明的较佳实施方式

本发明的核心思想是：在身份标识和位置分离架构下，由接入网关设备和/或映射服务器为启动匿名业务的用户终端分配一个用于匿名的身份识别 AID，在数据报文转发时使用该 AID 替换该用户的真实身份识别，以实现与通信对端的匿名通信。

下面结合附图及具体实施例对本发明作进一步详细描述。

基于网络的身份标识和位置分离架构有多种，图 1 为本发明实施例的身份标识和位置分离架构的网络拓扑示意图，其中示出了与本发明相关的系统架构的关键网元/功能实体。

如图 1 中所示，本实施例所述的基于身份位置分离架构（以下称本架构）中，将网络划分为接入网和骨干网，接入网位于骨干网的边缘，负责所有终端的接入。骨干网负责不同通过接入网接入的终端的路由。接入服务节点（Access Service Node，简称 ASN）位于骨干网和接入网的分界点，与接入网接口，与骨干网接口。ASN 用于为终端提供接入服务、维护用户连接以及转发用户数据等。接入网与骨干网在拓扑关系上没有重叠。

本架构网络中有两种标识类型，接入标识（Access Identifier，简称 AID）

和路由标识（Routing-Location Identifier，简称 RID）。其中 AID 是为网络中每个用户终端分配的唯一的身份标识，在接入层使用，且在用户终端的移动过程中始终保持不变；本架构网络内部的用户终端间使用 AID 标识对端，用户终端间只需使用对端的 AID 进行通信。

参见图 1，在优选实施例中，骨干网在组网时分为两个平面：映射转发平面，广义转发平面。

广义转发平面的主要功能是根据数据报文中的路由标识 RID 进行选路和转发数据报文。广义转发平面内的数据路由转发行为与传统 IP 网络一致。

映射转发平面的主要功能是保存移动节点身份位置的映射信息（即 RID-AID 之间的映射信息）、处理移动节点的登记注册流程、处理通信对端的位置查询流程，以及路由并转发以接入标识 AID 为目的地址的数据报文。

参见图 1，本实施例的基于网络的身份标识和位置分离架构中，涉及的主要网元和功能实体如下：

用户终端：本架构中，接入的用户终端可以是移动节点、固定节点及游牧节点中的一种或多种。

接入网：用于为用户终端提供二层（物理层和链路层）接入服务。接入网可以是基站系统，如基站子系统（Base Station Subsystem，BSS），无线接入网（Radio Access Network，RAN），演进的节点 B（evolved Node B，eNodeB）等，也可以是数字用户线（Digital Subscriber Line，xDSL）、无线访问接入点（Access Point，AP）等。

ASN：维护终端与骨干网的连接关系，为终端分配 RID，处理切换流程，处理登记注册流程，计费/鉴权，维护/查询通讯对端的 AID-RID 映射关系，封装、路由并转发送达终端或终端发出的数据报文。

ASN 收到终端发来的数据报文时，根据报文中的 CN 的 AID 在本地查找其对应的 RID：如果查到对应的 AID-RID 映射条目，则在数据报文中以 RID 替换 AID 的方式、或者以封装 RID 的方式将数据报文转发到骨干网；如果没有查到对应的 AID-RID 映射条目，则向 ILR 发出查询流程，以获取 AID-RID 映射表条目，然后在相关数据报文中以 RID 替换 AID 的方式、或者以封装

RID 的方式将数据报文转发出去；或是在向 ILR 发出查询的同时将数据报文转发到骨干网进行路由转发，在收到 ILR 返回的 CN 的 AID-RID 映射关系后，在本地缓存保存 CN 的 AID-RID 映射；

ASN 在收到网络发往终端的数据报文时，剥离外层的 RID 封装后，发给终端。

通用路由器（Common Router，CR）：路由并转发以 RID 格式为源地址/目的地址的数据报文。

认证中心：负责记录本架构网络的用户属性，包括用户类别、鉴权信息、用户服务等级等信息，产生用于鉴权、完整性保护和加密的用户安全信息，在用户接入时进行合法性认证和授权。认证中心支持本架构网络与用户间的双向鉴权。

身份位置寄存器（Identity Location Register，ILR）/分组转发功能（Packet Transfer Function，PTF）实体：ILR 和 PTF 实体可以为同一实体上的两个功能模块，位于骨干网的映射转发平面中。

ILR 负责维护/保存基于网络的身份标识和位置分离架构中用户的 AID-RID 映射关系，实现登记注册功能，处理通信对端的位置查询流程。具体地，当终端（Mobile Node，简称 MN）开机或者发生位置变化时，将通过所在的 ASN 向 ILR 发起注册过程，这样 ILR 中就保存了 MN 的实时 AID-RID 的映射关系。

PTF 实体在收到 ASN 送达的数据报文后，由 PTF 实体根据目的 AID 路由并转发。映射转发平面内 PTF 实体节点向 ILR 查到目的 AID-RID 的映射关系后，在数据报文头部封装查到的 RID 信息并转发到广义转发平面内路由到通信对端所在的 ASN。

在上述架构中，有效合法存续期间的终端的接入标识（AID）始终保持不变。路由标识（RID）标示终端当前所在的 ASN 位置。根据业务需要，ASN 可以为一个终端分配专用的一个或多个 RID 并注册登记到映射转发平面中的 ILR/PTF 实体；ASN 也可为多个终端分配相同的 RID。终端接入网络时，通

过认证中心鉴权保证用户身份的真实性，ILR 保存了各接入终端的 AID-RID 映射信息。接入网部分采用 AID 区别不同终端，广义交换平面采用 RID 路由数据报文。建立端到端的通信过程需要通过 AID 查找对应的 RID。端到端通信过程中，需要将本端的 AID 作为源端地址在数据报文中携带到通信对端。通信对端能够从数据报文携带的源端地址获得源端身份。

本架构网络通过对用户身份的鉴权，以网络信用保证了用户身份的真实可靠，在网络中构建了一个信任域。网络对用户身份的鉴权方法根据不同的网络体制可采用不同的方法，可以对用户接入标识 AID 直接鉴权；也可以对网络中标识用户的其他类型的用户识别（例如国际移动用户识别（International Mobile Subscriber Identification Number，IMSI）、网络用户识别（Network Access Identifier，NAI）等）进行鉴权，网络设备将保存该用户识别与 AID 之间的对应关系。

现有接入网 RAN 部分能够保证二层连接安全性，保证终端接入网络时数据报文不被篡改。例如：码分多址（Code Division Multiple Access，CDMA）无线接入采用码分多址方式，非对称数字用户环路（Asymmetric Digital Subscriber Line，ADSL）采用专线或 VLAN 隔离方式，GSM 采用频分多址方式。所有的终端都是通过鉴权认证的有效合法用户。终端在接入网络时，将建立终端与网络的 ASN 间的点到点连接关系。ASN 将终端的 AID 绑定在终端与 ASN 间的端到端用户连接上，如果从该用户连接上发出报文的源地址与该用户的 AID 不匹配，ASN 将丢弃数据报文，这样，能够保证本架构中终端的 AID 不被仿冒和更改。

ASN，以及从源端 ASN 到目的端 ASN 之间的通信设备如 ILR/PTF，CR，认证中心等，由网络运营和管理方提供，由网络信用保证数据报文传输的安全性，保证数据报文真实可靠。

从而，基于身份位置分离架构将能够在网络中以网络信用构建一个信任域，保证进行数据通信的两端身份的真实可靠。

出于安全性和业务特点的考虑，现有 Internet 网大量的应用业务以匿名方式开展，这就需要在网络信用担保的信任域中，提供一个匿名制的空间，以满足业务开展的需要。

以下将结合上述身份标识和位置分离架构下的若干实施案例对本发明如何提供匿名制的空间的具体实施方案进行详细说明。本实施例中，是以基于网络的身份标识和位置分离架构为例进行说明，但本发明技术方案所基于的架构网络还可以是基于 LISP 及其他多种身份标识和位置分离架构。

实施案例一

在身份标识和位置分离架构下，实名制信任域由网络信用保证，匿名制空间由网络根据设置的业务授权开展。如图 2 所示，其具体实现流程如下:

步骤 201. MN 发起登录请求，请求接入本架构网络，认证中心对 MN 进行合法性认证和授权，记录的用户属性，如果 MN 在本架构网络开通了匿名数据业务，则存储在 MN 的用户属性中;

MN 接入本架构网络的流程如图 3 所示，其中 MN 的合法性认证及鉴权等可采用现有流程，并且，本架构网络中支持双向认证，即 MN 还可以对网络的合法性进行认证。

步骤 202. MN 接入本架构网络，MN 所在的 ASN 为其分配 RID，并向归属 ILR 注册映射关系，ILR 将保存 MN 的 AID-RID 映射信息;

步骤 203. MN 申请数据通信采用匿名方式;

图 4 所示为终端用户发起匿名通信的流程示意图，具体包括:

MN 通过其所在的 ASN 发起匿名通信请求;

认证中心确认 MN 具备匿名通信业务权限后，向 ASN 发出确认;（该步骤根据运营需要为可选步骤。）

MN 所在的 ASN 向归属 ILR 发起匿名 AID 分配请求，归属 ILR 收到该请求消息后，记录 MN 为匿名通信状态，并为 MN 分配一个新的接入标识 AID 作为匿名 AID，归属 ILR 可以从专用于匿名 AID 的号段中选取，也可以从号段中选取一个空闲的 AID; 并将该匿名 AID 保存在归属 ILR 存储的 MN 的记录中，例如记录对应关系: AID-匿名 AID-RID;

归属 ILR 向 ASN 发出匿名通信响应消息，携带匿名 AID 的信息，例如 AID-匿名 AID 的对应关系，ASN 收到该消息后，从消息中读取匿名 AID 的信息，保存在 MN 对应的数据区中，并记录 MN 为匿名通信状态，在匿名通信状态期间，MN 与其所有通信对端的通信均采用匿名方式;

ASN 向 MN 发出匿名通信确认消息。

步骤 204. MN 与 CN 建立端到端匿名数据通信;

如图 5 所示，MN 与 CN 建立端到端匿名通信的流程如下:

MN 与 CN 建立端到端通信，在 MN 与源 ASN 之间的接口上，收发的数据报文格式为:（源 AID，目的 AID），即源地址目的地址分别为双方用户的身份识别。MN 所在的 ASN 判断该用户匿名数据业务有效后，将发出的数据报文中的源 AID 替换为匿名 AID,并查找对应的源 RID/目的 RID 并封装在数据报文中，通过骨干网发往 CN 所在的 ASN;

其中，在源 ASN 与目的 ASN 之间的接口上传送的数据报文格式为:（源 RID，匿名 AID，目的 RID，目的 AID）。

CN 所在的目的 ASN 收到数据报文后，剥离 RID 封装，将数据报文发往 CN，数据报文格式为（匿名 AID，目的 AID）;

CN 所在的 ASN 收到 CN 回应的数据报文，数据报文格式为:（源 AID，匿名 AID），即源地址为 CN 的 AID，目的地址为匿名 AID;

CN 所在的 ASN 将数据报文增加 RID 封装，封装后的数据报文格式为:（源 RID，源 AID，目的 RID，匿名 AID），通过骨干网将数据报文发往 MN 所在的 ASN;

MN 所在的 ASN 收到 CN 发出的数据报文后，剥离 RID 封装，并将数据报文中的匿名 AID 替换为 MN 的 AID，发送给 MN。

由上述流程可见，在 MN 与 CN 的通信期间，CN 看到的 MN 的身份识别是匿名 AID，而不是接入 AID。

步骤 205. MN 取消匿名通信方式。

图 6 为终端用户取消匿名通信的流程示意图，具体流程如下:

MN 发起取消匿名数据通信请求;

认证中心确认 MN 具备匿名通信业务权限后，向 ASN 发出确认；（该步骤根据运营需要为可选步骤。）

ASN 删除 MN 数据区中的 AID-匿名 AID 对应关系，将 MN 的匿名通信状态改为正常通信状态;

ASN 向归属 ILR 发起取消匿名 AID 对应关系流程，ILR 将删除 MN 的 AID-匿名 AID-RID 的对应关系，保存 MN 的 AID-RID 映射关系，并将 MN 的匿名通信状态改为正常通信状态，向 ASN 发送取消匿名通信响应消息;

ASN 向 MN 发送取消匿名通信响应消息。

后续 ASN 在进行 MN 的数据报文收发时，将不再进行 AID 与匿名 AID 的替换。

实施案例二

本实施案例与实施案例一的流程基本相同，二者的主要区别在于，本实施例中，作为上述匿名 AID 分配流程的替代步骤，如图 7 所示，也可以由 ASN 按以下流程自行完成匿名 AID 的分配流程:

MN 通过其所在的 ASN 发起匿名通信请求;

认证中心确认 MN 具备匿名通信业务权限后，向 ASN 发出确认；（该步骤根据运营需要为可选步骤。）

MN 所在的 ASN 收到鉴权认证中心匿名业务权限确认后，ASN 为 MN 分配匿名 AID，保存在 MN 对应的数据区中，并记录 MN 为匿名通信状态;

ASN 向归属 ILR 发起匿名 AID 登记流程，归属 ILR 将保存 MN 的 AID-匿名 AID-RID 的对应关系，并记录 MN 为匿名通信状态;

此处，归属 ILR 保存匿名 AID 的对应关系后，后续 CN 向 MN 发送数据报文时，可以根据 MN 的匿名 AID 查询到 MN 的 RID。

ASN 向 MN 发送匿名通信确认消息。

后续 MN 进行数据通信的过程中，ASN 如果判断出 MN 处于匿名通信状

态，则在进行MN的数据报文收发时，将负责进行AID与匿名AID的替换。

实施案例三

本实施案例与前述实施案例的流程基本相同，其主要区别在于：前述案例中，MN 通过发起匿名通信请求申请匿名通信方式，后续需要取消匿名通信方式时，MN通过发起取消匿名通信请求取消通信匿名方式。

而在本实施案例中（未图示），MN 申请匿名通信方式时，在发起匿名通信请求中，携带时间段信息，表示在该时间段内，MN 处于匿名通信状态中；ASN收到该匿名通信请求时，设置匿名通信定时器，在匿名通信定时器到时前，ASN将进入如前述实施案例所述的匿名通信处理流程。

本实施案例中，MN 将无需发起取消匿名通信的流程，匿名通信定时器到时即可取消本次匿名方式通信，MN由匿名通信状态改变为正常通信状态。

由上可知，本发明提出了一种身份标识和位置分离架构下匿名通信的方法，基于本发明的身份标识和位置分离架构下的匿名通信方法，可以实现在构建实名制信任域的基础上，提供一个匿名制的空间，以满足业务开展的需要。在身份标识和位置分离框架下，实名制信任域由网络信用保证，匿名制空间由网络根据业务授权开展业务。

本发明实施例中还提供了一种数据报文的转发方法，包括:

源端节点向目的节点发送数据报文，所述数据报文中包含目的地址和第一源地址;

源端接入节点接收到所述数据报文时，将其中包含的所述第一源地址替换成为所述终端分配的第二源地址，并根据所述目的地址将所述数据报文转发至目的接入节点;

所述目的接入节点收到所述数据报文中后转发给所述目的节点。

进一步地，所述目的节点收到所述数据报文后，以所述第二源地址作为

目的地址向所述源端节点回应数据报文;

所述目的接入节点根据所述第二源地址将所述数据报文转发至所述源端接入节点;

所述源端节点收到所述数据报文后，将其中包含的所述第二源地址替换成对应的所述第一源地址，转发给所述源端节点。

进一步地，所述方法应用于身份标识与位置分离架构网络，所述第一源地址为所述终端的接入标识。

此外，本发明实施例中还提供了一种匿名通信的注册方法，应用于身份标识与位置标识分离的架构网络中，所述架构网络至少包括有第一节点、认证中心、第一接入节点及第一分配节点，其中，所述第一节点分配有一实际身份标识，包括:

第一节点经由第一接入节点向认证中心发送匿名通信请求;

所述认证中心接收所述匿名通信请求并判断所述第一节点是否具备匿名通信权限;

在第一节点具备匿名通信权限的情况下，所述第一接入节点向第一分配节点发送匿名身份标识分配请求，第一分配节点为第一节点分配一匿名身份标识，并保存该第一节点匿名身份标识与第一节点实际身份标识的对应关系，或第一节点的匿名身份标识与第一节点实际身份标识以及位置标识的对应关系。

进一步地，所述方法还包括第一分配节点记录第一节点处于匿名通信状态，并将所述匿名身份标识发送至第一接入节点。

进一步地，所述匿名身份标识自一预定用于匿名身份标识的标识群组中选择，或自一预定群组中选择。

本发明实施例中还提供了另一种匿名通信的注册方法，应用于身份标识与位置标识分离的架构网络中，所述架构网络至少包括有第一节点、第一接入节点及第一存储节点，其中，所述第一节点分配有一实际身份标识，包括:

第一节点经由第一接入节点向认证中心发送匿名通信请求;

所述认证中心接收所述匿名通信请求并判断所述第一节点是否具备匿名通信权限;

在第一节点具备匿名通信权限的情况下，所述第一接入节点为第一节点分配一匿名身份标识，同时向第一存储节点登记该第一节点匿名身份标识与第一节点实际身份标识的对应关系，或第一节点的匿名身份标识与第一节点实际身份标识以及位置标识的对应关系。

进一步地，所述方法还包括第一接入节点记录第一节点处于匿名通信状态。

此外，本发明实施例还提供了一种信息的发送方法，包括:

第一节点经由第一节点归属地的第一接入节点发送一信息至第二节点，所述信息至少包括有第一节点第一标识及第二节点第一标识;

第一节点归属地的第一接入节点替换第一节点第一标识为第一节点更新后第一标识后，采用第一节点第二标识及第二节点第二标识封装所述第一节点更新后的第一标识及第二节点第一标识，并发送至第二节点归属地的第二接入节点，并经由该第二节点归属地的第二接入节点解封后发送该信息至第二节点。

进一步地，第一标识为身份标识，第二标识为位置标识，所述第一节点更新后的第一标识和/或第一节点第二标识及第二节点第二标识为第一接入节点本地获取，或自第一接入节点外的另一节点获取。

进一步地，所述方法还包括，在第一接入节点接收所述信息时，还包括一判断所述信息发送是否触发替换程序的步骤。

本发明实施例中还提供了一种用以实现信息收发的系统，应用于身份与位置分离的架构网络中，包括:

接收单元，用以接收第一节点发送至第二节点的信息，其中所述信息至少包括有所述第一节点及第二节点的身份标识;

更新单元，用以更新第一节点的身份标识为一匿名的身份标识；

封装单元，用以封装第一节点和第二节点的位置标识在所述匿名身份标识及第二节点的身份标识外，以供身份与位置分离架构网络实现路由转发以发送信息至第二节点；其中，

所述接收单元还用以在接收第二节点发送至第一节点的信息时，更新匿名的身份标识为第一节点的身份标识，并转发信息至第一节点。

本发明实施例中还提供了另一种用以实现信息收发的系统，应用于身份与位置分离的架构网络中，其特征在于：所述系统包括有第一系统及第二系统，其中，

第一系统包括：

第一收发单元，用以接收第一节点发送至第二节点的第一信息，其中，所述第一信息包括有第一节点和第二节点的身份标识；及，用以接收第二系统第二收发单元发送的第二信息，其中，第二信息包括有第一节点的匿名身份标识及第二节点的身份标识；

第一替换单元，用以在第一节点向第二节点发送第一信息时，更新第一节点的身份标识为匿名身份标识，以及在第二节点发送第二信息至第一节点时，更新匿名身份标识为第一节点的身份标识；

第二系统包括：

第二收发单元，用以接收第一信息并转发至第一节点；及用以向第一节点转发自第二节点的第二信息，其中，第二信息包括有第一节点的匿名身份标识及第二节点的身份标识。

进一步地，在第一节点发送第一信息至第二节点时，第一节点的匿名身份标识用以标识信息的发送方，第二节点的身份标识用以标识信息的接收方，在第二节点发送第二信息至第一节点时，第一节点的匿名身份标识用以标识信息的接收方，第二节点的身份标识用以标识信息的发送方。

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，所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。本发明不限制于任何特定形式的硬件和软件的结合。

工业实用性

本发明提出一种身份标识和位置分离架构下匿名通信的解决方案，可以实现在构建了一个实名制信任域的基础上，提供一个匿名制的空间，以满足匿名业务开展的需要，在身份标识和位置分离架构下，实名制信任域由网络信用保证，匿名制空间由网络根据业务授权开展业务。

权 利 要 求 书

1、一种匿名通信的方法，应用于身份标识和位置分离架构网络，该方法包括:

所述网络接收到终端发起的匿名通信请求后，为所述终端分配匿名身份标识，并将所述终端的状态记录为匿名通信状态;

当所述终端处于匿名通信状态下时，所述终端所在的接入网关设备在收到所述终端发出的数据报文时，将所述数据报文中的源接入标识替换为所述匿名身份标识；在收到发往所述终端的数据报文时，将所述发往所述终端的数据报文中的匿名身份标识替换为所述终端的接入标识。

2、如权利要求 1 所述的方法，其中，

所述为所述终端分配匿名身份标识的步骤中，由所述网络中的映射服务器、或所述终端所在的接入网关设备为所述终端分配所述匿名身份标识。

3、如权利要求 2 所述的方法，其中，

所述终端所在的接入网关设备为所述终端分配所述匿名身份标识的步骤还包括：将分配的所述匿名身份标识向所述映射服务器进行登记。

4、如权利要求 1、2 或 3 所述的方法，其中，将所述终端的状态记录为匿名通信状态的步骤之前，所述方法还包括:

所述终端所在的接入网关设备在接收到所述匿名通信请求时，向认证中心发起鉴权流程，在确认所述终端具备匿名通信业务权限后，将所述终端记录为匿名通信状态。

5、如权利要求 4 所述的方法，所述方法还包括:

所述终端所在的接入网关设备在接收到所述终端的取消匿名通信请求后，将所述终端的状态由匿名通信状态改变为正常通信状态。

6、如权利要求 5 所述的方法，所述方法还包括:

所述终端所在的接入网关设备将所述终端的状态由匿名通信状态改变为正常通信状态后，在进行所述终端的数据报文的收发时，取消所述匿名身份标识的替换。

7、如权利要求 1 所述的方法，其中，

所述终端发起的所述匿名通信请求中携带时间段信息;

所述终端所在的接入网关设备在接收到所述匿名通信请求时，将所述终端的状态记录为匿名通信状态的步骤还包括:

根据所述匿名通信请求中的所述时间段信息设置匿名通信定时器；并在所述定时器到达定时周期后将所述终端的状态由匿名通信状态改变为正常通信状态。

8、一种数据报文的转发方法，所述方法包括:

源端节点向目的节点发送数据报文，所述数据报文中包含目的地址和第一源地址;

源端接入节点接收到所述数据报文时，将所述数据报文中包含的所述第一源地址替换成为所述终端分配的第二源地址，并根据所述目的地址将所述数据报文转发至目的接入节点；以及

所述目的接入节点收到所述数据报文中后转发给所述目的节点。

9、如权利要求 8 所述的方法，所述方法还包括:

所述目的节点收到所述数据报文后，以所述第二源地址作为目的地址向所述源端节点回应数据报文;

所述目的接入节点根据所述第二源地址将所述回应数据报文转发至所述源端接入节点；以及

所述源端节点收到所述回应数据报文后，将所述回应数据报文中包含的所述第二源地址替换成对应的所述第一源地址，转发给所述源端节点。

10、如权利要求 8 或 9 所述的方法，其中，

所述方法应用于身份标识与位置分离架构网络，所述第一源地址为所述终端的接入标识。

11、一种匿名通信的注册方法，应用于身份标识与位置标识分离的架构网络中，所述架构网络至少包括第一节点、认证中心、第一接入节点及第一分配节点，其中，所述第一节点分配有一实际身份标识，其特征在于，所述

方法包括:

第一节点经由第一接入节点向认证中心发送匿名通信请求;

所述认证中心接收所述匿名通信请求并判断所述第一节点是否具备匿名通信权限; 以及

在第一节点具备匿名通信权限的情况下, 所述第一接入节点向第一分配节点发送匿名身份标识分配请求, 第一分配节点为第一节点分配一匿名身份标识, 并保存该第一节点匿名身份标识与第一节点实际身份标识的对应关系, 或第一节点的匿名身份标识与第一节点实际身份标识以及位置标识的对应关系。

12、如权利要求 11 所述的方法, 所述方法还包括: 第一分配节点记录第一节点处于匿名通信状态, 并将所述匿名身份标识发送至第一接入节点。

13、如权利要求 12 所述的方法, 所述方法还包括:

所述匿名请求中包括时间段信息;

所述第一接入节点收到所述匿名请求时, 根据所述时间段信息设置匿名通信定时器; 并在所述定时器到达定时周期后将所述终端的状态由匿名通信状态改变为正常通信状态。

14、如权利要求 11、12 或 13 所述的方法, 其中, 所述匿名身份标识自一预定用于匿名身份标识的标识群组中选择, 或自一预定群组中选择。

15、一种匿名通信的注册方法, 应用于身份标识与位置标识分离的架构网络中, 所述架构网络至少包括有第一节点、第一接入节点及第一存储节点, 其中, 所述第一节点分配有一实际身份标识, 其特征在于, 该方法包括:

第一节点经由第一接入节点向认证中心发送匿名通信请求;

所述认证中心接收所述匿名通信请求并判断所述第一节点是否具备匿名通信权限; 以及

在第一节点具备匿名通信权限的情况下, 所述第一接入节点为第一节点分配一匿名身份标识, 同时向第一存储节点登记该第一节点匿名身份标识与第一节点实际身份标识的对应关系, 或第一节点的匿名身份标识与第一节点实际身份标识以及位置标识的对应关系。

16、如权利要求 15 所述的方法，所述方法还包括：第一接入节点记录第一节点处于匿名通信状态。

17、如权利要求 16 所述的方法，所述方法还包括：

所述匿名请求中包括时间段信息；

所述第一接入节点收到所述匿名请求时，根据所述时间段信息设置匿名通信定时器；并在所述定时器到达定时周期后将所述终端的状态由匿名通信状态改变为正常通信状态。

18、一种信息的发送方法，该方法包括：

第一节点经由第一节点归属地的第一接入节点发送一信息至第二节点，所述信息至少包括有第一节点第一标识及第二节点第一标识；以及

第一节点归属地的第一接入节点替换第一节点第一标识为第一节点更新后第一标识后，采用第一节点第二标识及第二节点第二标识封装所述第一节点更新后的第一标识及第二节点第一标识，并发送至第二节点归属地的第二接入节点，并经由该第二节点归属地的第二接入节点解封后发送该信息至第二节点。

19、如权利要求 18 所述的方法，其中，第一标识为身份标识，第二标识为位置标识，所述第一节点更新后的第一标识和/或第一节点第二标识及第二节点第二标识为第一接入节点本地获取，或自第一接入节点外的另一节点获取。

20、如权利要求 18 或 19 所述的方法，所述方法还包括，在第一接入节点接收所述信息时，判断所述信息发送是否触发替换程序的步骤。

21、一种用以实现信息收发的系统，应用于身份与位置分离的架构网络中，所述系统包括：

接收单元，其设置为：接收第一节点发送至第二节点的信息，其中，所述信息至少包括有所述第一节点及第二节点的身份标识；

更新单元，其设置为：更新第一节点的身份标识为一匿名的身份标识；以及

封装单元，其设置为：封装第一节点和第二节点的位置标识在所述匿名

身份标识及第二节点的身份标识外，以供身份与位置分离架构网络实现路由转发以发送信息至第二节点；

所述接收单元还设置为：在接收第二节点发送至第一节点的信息时，更新匿名的身份标识为第一节点的身份标识，并转发信息至第一节点。

22、一种用以实现信息收发的系统，应用于身份与位置分离的架构网络中，所述系统包括有第一系统及第二系统，其中，

第一系统包括：

第一收发单元，其设置为：接收第一节点发送至第二节点的第一信息，其中，所述第一信息包括有第一节点和第二节点的身份标识；接收第二系统第二收发单元发送的第二信息，其中，第二信息包括有第一节点的匿名身份标识及第二节点的身份标识；以及

第一替换单元，其设置为：在第一节点向第二节点发送第一信息时，更新第一节点的身份标识为匿名身份标识；以及在第二节点发送第二信息至第一节点时，更新匿名身份标识为第一节点的身份标识；

第二系统包括：

第二收发单元，其设置为：接收第一信息并转发至第一节点；向第一节点转发自第二节点的第二信息，其中，第二信息包括有第一节点的匿名身份标识及第二节点的身份标识。

23、如权利要求 22 所述的系统，其中，

在第一节点发送第一信息至第二节点时，第一节点的匿名身份标识用以标识信息的发送方，第二节点的身份标识用以标识信息的接收方，在第二节点发送第二信息至第一节点时，第一节点的匿名身份标识用以标识信息的接收方，第二节点的身份标识用以标识信息的发送方。

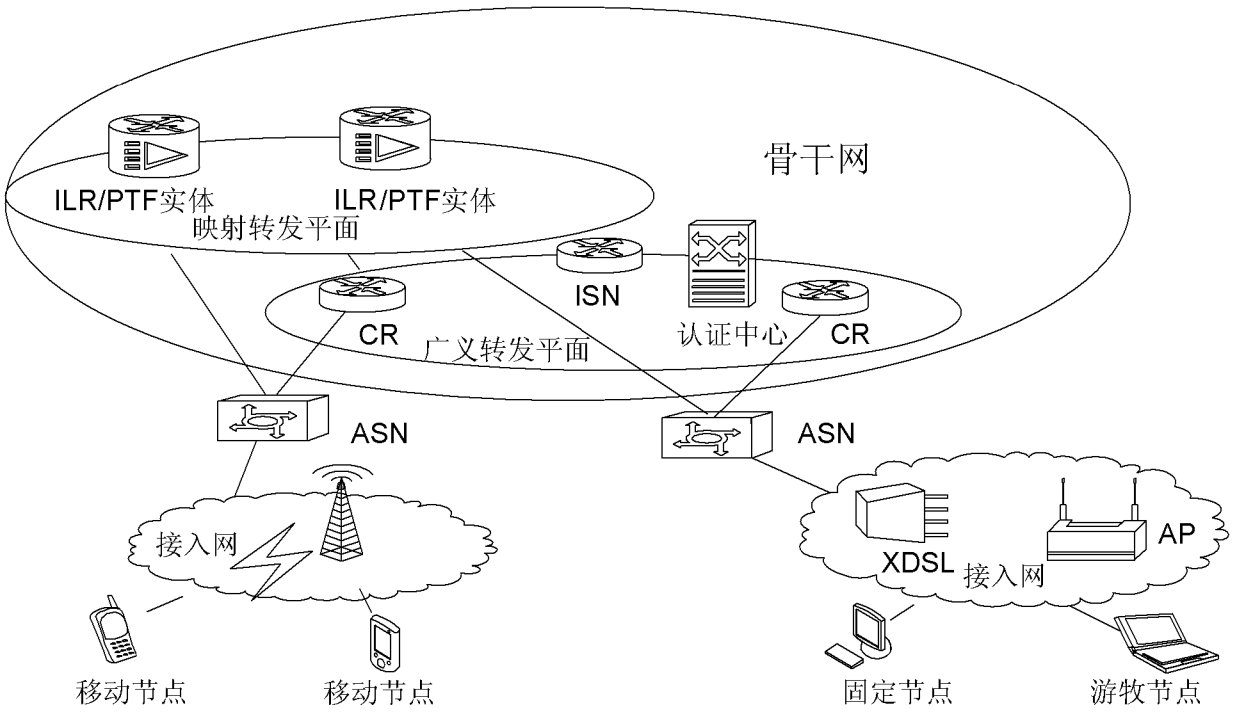
骨干网
ILR/PTF实体
ILR/PTF实体
映射转发平面
ISN
CR
广义转发平面
认证中心
CR
ASN
ASN
接入网
XDSL
接入网
AP
移动节点
移动节点
固定节点
游牧节点

图 1

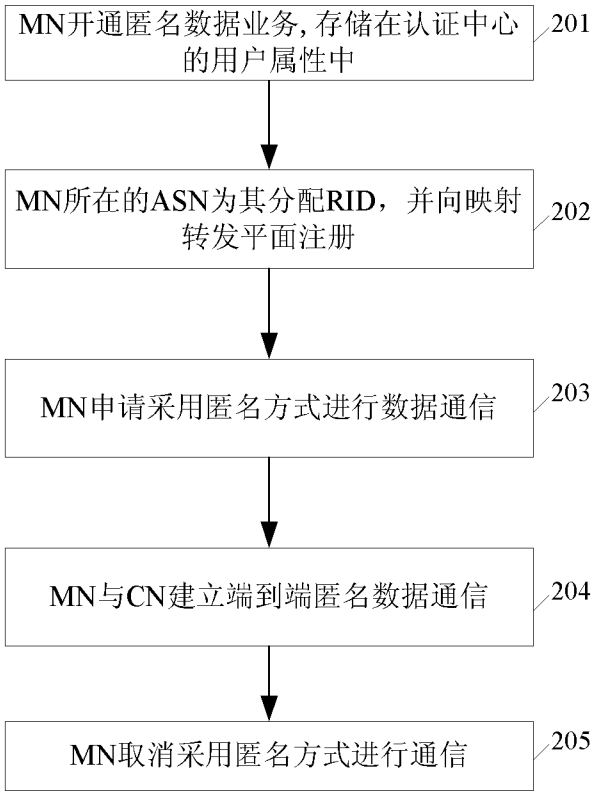
MN开通匿名数据业务，存储在认证中心的用户属性中
201
MN所在的ASN为其分配RID，并向映射转发平面注册
202
MN申请采用匿名方式进行数据通信
203
MN与CN建立端到端匿名数据通信
204
MN取消采用匿名方式进行通信
205

图 2

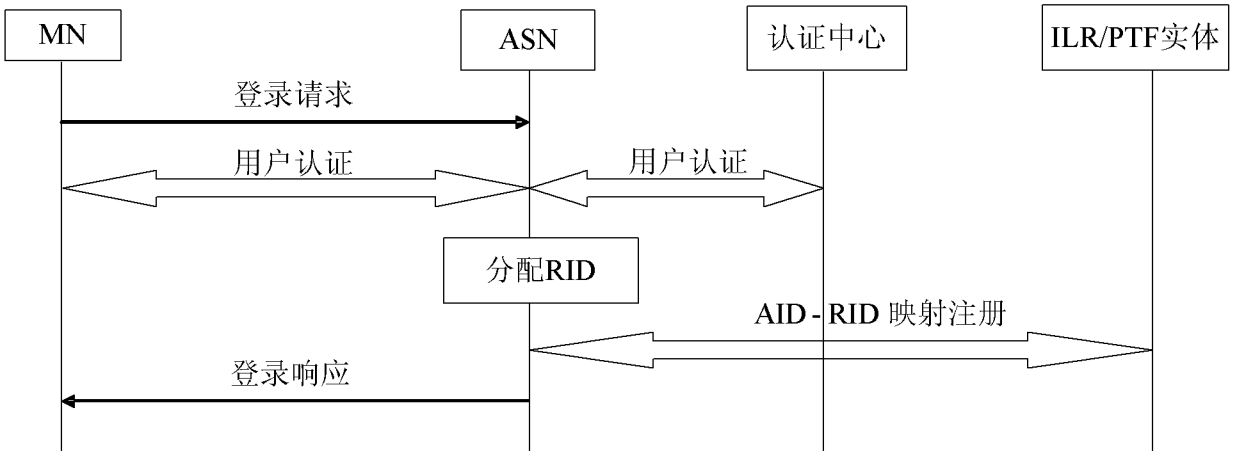
MN
ASN
认证中心
ILR/PTF实体
登录请求
用户认证
用户认证
分配RID
AID - RID 映射注册
登录响应

图 3

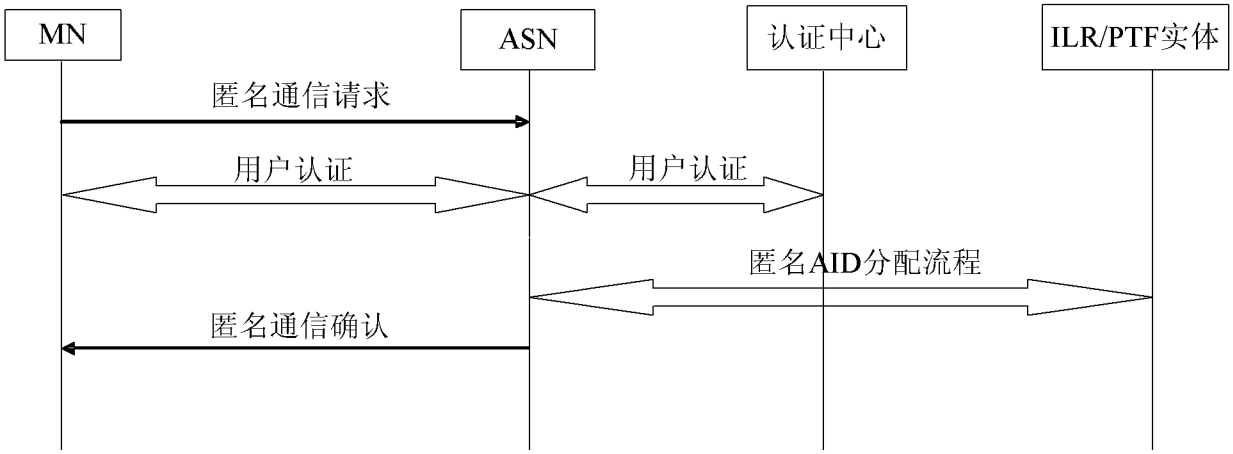
MN
ASN
认证中心
ILR/PTF实体
匿名通信请求
用户认证
用户认证
匿名AID分配流程
匿名通信确认

图 4

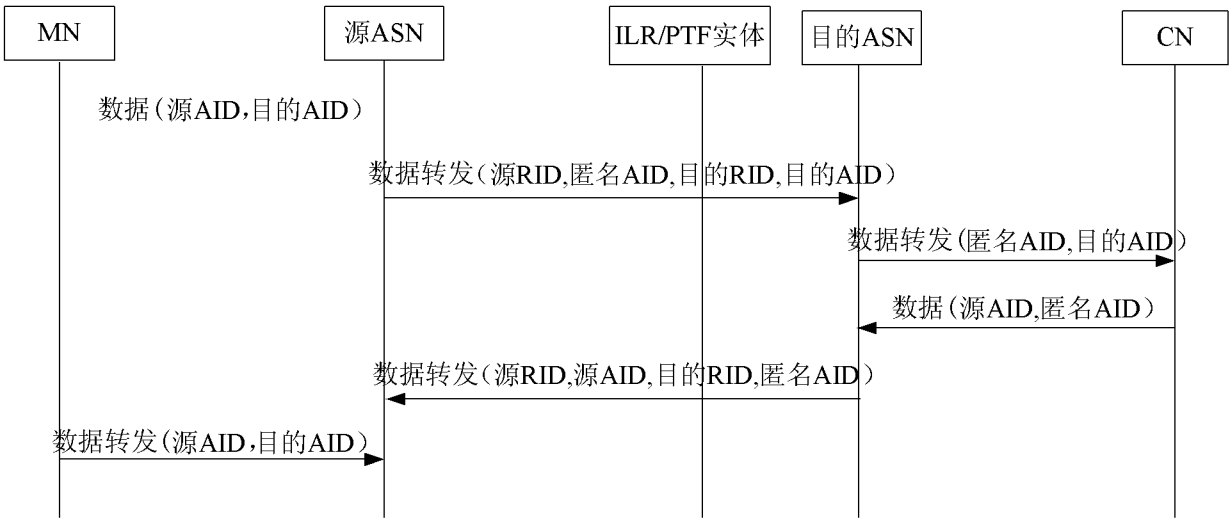
MN
源ASN
ILR/PTF实体
目的ASN
CN
数据（源AID,目的AID）
数据转发（源RID,匿名AID,目的RID,目的AID）
数据转发（匿名AID,目的AID）
数据（源AID,匿名AID）
数据转发（源RID,源AID,目的RID,匿名AID）
数据转发（源AID,目的AID）

图 5

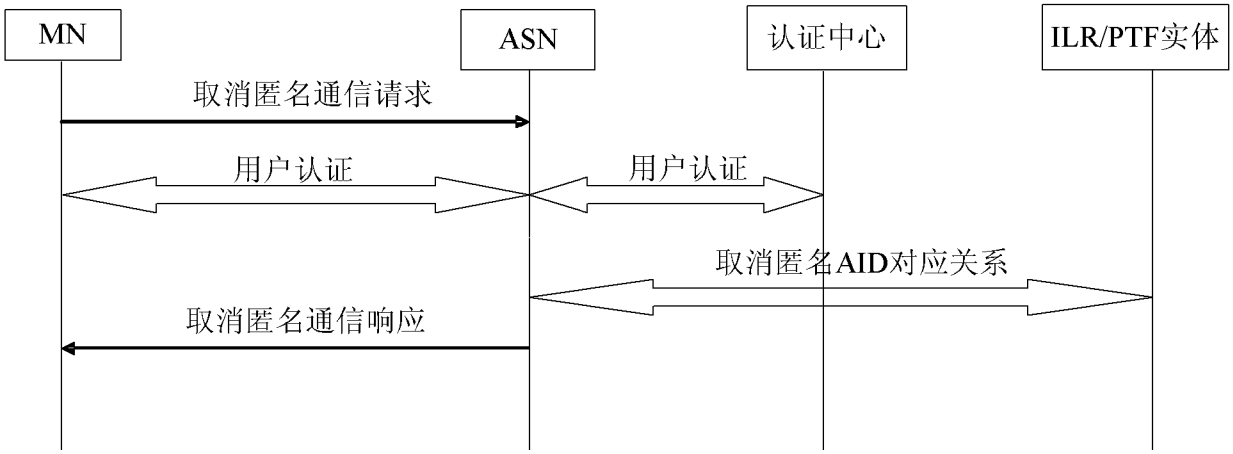
MN
ASN
认证中心
ILR/PTF实体
取消匿名通信请求
用户认证
用户认证
取消匿名AID对应关系
取消匿名通信响应

图 6

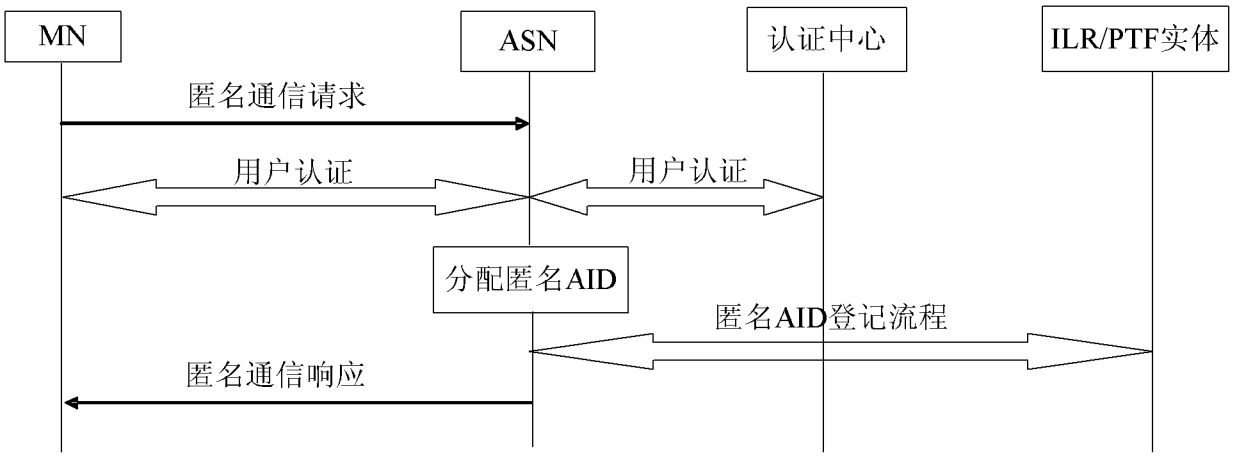
MN
ASN
认证中心
ILR/PTF实体
匿名通信请求
用户认证
用户认证
分配匿名AID
匿名AID登记流程
匿名通信响应

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2010/076378

A. CLASSIFICATION OF SUBJECT MATTER

H04W12/00 (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)

IPC: H04Q7, H04W, 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)

WPI, EPODOC, CPRSABS, CNKI: information, data, message, datagram, transfer, transmi+, anonym+, hid+, identi+, address, position, location, map+, node, conver+, replac+, encapsulat+, de-encapsulat+, source, destination, regist+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN101262416A (HUAWEI TECHNOLOGIES CO LTD) 10 Sept. 2008(10.09.2008) Claims 1, 6, 7, page 2 lines 15-24, page 6 lines 3-5, page 9 lines 13-27 of the description	8, 9, 18-20
A		1-7, 10-17, 21-23
A	CN101400054A (HUAWEI TECHNOLOGIES CO LTD) 01 Apr. 2009(01.04.2009) Pages 2-4 of the description	1-23
A	US7324517B1 (CISCO TECHNOLOGY INC) 29 Jan. 2008(29.01.2008) Pages 2-6 of the description	1-23

☐ 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
11 Nov. 2010 (11.11.2010)	**09 Dec. 2010 (09.12.2010)**
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 HAO, Yue Telephone No. (86-10)62411999

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2010/076378

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101262416A	10.09.2008	NONE	
CN101400054A	01.04.2009	NONE	
US7324517B1	29.01.2008	NONE	

国际检索报告

国际申请号
PCT/CN2010/076378

A. 主题的分类

H04W12/00 (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)

IPC: H04Q7, H04W, 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, CNKI: 信息，数据，报文，转发，发送，匿名，隐藏，状态，身份，标识，地址，位置，分离，映射，节点，替换，代替，替代，恢复，封装，解封，源，目的，注册，登记

WPI, EPODOC: information, data, message, datagram, transfer, transmi+, anonym+, hid+, identi+, address, position, location, map+, node, conver+, replac+, encapsulat+, de-encapsulat+, source, destination, regist+

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	CN101262416A (华为技术有限公司) 10.9 月 2008(10.09.2008) 权利要求 1，6，7，说明书第 2 页第 15-24 行，第 6 页 3-5 行，第 9 页第 13-27 行	8，9，18-20
A		1-7，10-17，21-23
A	CN101400054A(华为技术有限公司) 01.4 月 2009(01.04.2009) 说明书第 2 页-第 4 页	1-23
A	US7324517B1(思科技术公司) 29.1 月 2008(29.01.2008) 说明书第 2 页-第 6 页	1-23

☐ 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
11.11 月 2010(11.11.2010)	**09.12 月 2010 (09.12.2010)**
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 **郝悦** 电话号码：(86-10) **62411999**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2010/076378

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101262416A	10.09.2008	无	
CN101400054A	01.04.2009	无	
US7324517B1	29.01.2008	无	