第34卷 第15期 计 算 机 工 程 2008年8月
Vol.34 No.15 Computer Engineering August 2008
·网络与通信· 文章编号：1000—3428(2008)15—0097—03 文献标识码：A 中图分类号：TN929.5

基于标识支持的移动通信技术

李秀芹[1,2]，兰巨龙[1]
(1. 解放军信息工程大学国家数字交换系统工程技术研究中心，郑州 450002；2. 华北水利水电学院信息工程学院，郑州 450011)

摘 要：目前互联网在移动性和安全性方面存在缺陷，IP地址同时作为用户的身份标识和位置标识，导致语义过载。该文分析几种典型的基于身份标识和位置标识相分离的名字空间改进方案，比较其对移动性、安全性的支持，提出一种新的基于一体化网络的移动通信机制。
关键词：标识；移动通信；一体化网络

Mobility Communication Technology Based on Identity Holding

LI Xiu-qin[1,2], LAN Ju-long[1]
(1. National Digital Switching System Engineering & Technological Center, PLA Information Engineering University, Zhengzhou 450002;
2. Department of Information Engineering, North China University of Water Conservancy and Electric Power, Zhengzhou 450011)

【Abstract】There are shortcomings of current Internet on aspects of the mobility and safety, and IP address is overloaded in semantics because it is used to represent both the location and the identity of a user. This paper analyzes several typical namespace improvement solutions that the identity and the position of a user separate mutually currently, compares its mobility, safety, and puts forward a mobile communication mechanism based on the universal network.
【Key words】identity; mobile communication; universal network

1 概述

Internet的节点最初都被设计为静态[1]，随着Internet中移动设备数量的增加，其缺陷越来越明显。在传统Internet协议体系结构中，传输层使用传输层标识符<IP地址，端口>，与网络层紧密绑定。网络层使用IP地址表示节点在网络中的拓扑位置，由于网络层IP地址承担双重功能，因此在主机移动和多宿主情况下，无法提供良好服务。如果在主机移动时改变其IP地址，通信双方将无法在原始网络层通信链路上发送或接收数据而导致通信中断。

IP地址的双重功能破坏了Internet分层结构中不同层次之间尽量减少耦合的原则，网络层和传输层的紧密耦合不利于各层独立发展。

当主机因移动发生位置变化时，其IP地址相应改变，但主机身份不变。在目前解决移动问题的主要方案中，MIP用主机的家乡地址作为主机的身份标识，通过设置家乡代理来实现路由重定向，但MIP没有解决三角路由、切换延迟和潜在的安全隐患问题。虽然MIPv6允许移动设备在维护其IP地址和传输层连接的同时改变连接到网络的位置，避免了三角路由，但仍存在较大切换延迟，且MIPv6没有解决多宿主问题，容易受到拒绝服务攻击[2]。MIP和MIPv6通过对路由器的修改来解决移动问题，可部署性较差。

解决移动问题的关键在于使主机位置标识和主机身份标识相分离。为了更好地解决多宿主、IP地址动态重分配等问题，必须分离IP地址的双重功能。因此，采用身份标识和位置标识相分离的名字空间，进行基于标识、支持主机移动的技术研究具有重要意义，将有助于解决主机移动、Multi-homing, IP地址动态重分配及不同网络区域之间的互访等问题。

2 基于标识支持的移动通信技术

基于标识支持的移动通信技术对IP地址双重功能进行分离，采用身份标识和位置标识相分离的名字空间，使设备的身份标识和位置标识分离。

2.1 主机标识协议(Host Identity Protocol, HIP)

2.1.1 HIP及其对移动性的支持

HIP[3]引进一个新的加密命名空间——主机标识符(Host Identifier, HI)。HI全球唯一地标识每台连接到Internet的主机，将传输层与网络层分开，为Internet提供一个安全的主机移动多宿主方法及一个加密的主机标识命名空间，以便于对通信双方进行认证，从而实现安全、可靠的网络系统。

除HI，HIP还引进了主机标识标签(HIT)和局部标识符(LSI)。每个主机可以有多个HI，用不对称加密算法中公/私密钥对的公钥来表示，但由于不同加密算法拥有的密钥长度不一样，因此在HIP协议分组、网络套接字中不直接使用HI作为主机的标识符，而是使用主机标识符HIT，它是对HI进行单向散列(Hash)构成的128 bit位串，与IPv6地址等长。它有自校验、低冲突率的特性，实现及控制代价较小。HIP在传输层和网络层之间插入一个独立的新协议层——主机标识层(Host Identity Layer, HIL)。HIL将原来紧密耦合的传输层和网络层分开，IP地址不再作为主机名称，只负责数据包的路由转发，主机名称由HI来表示。引入HIL后的体系结

基金项目：国家“973”计划基金资助项目(2007CB307102)
作者简介：李秀芹(1967－)，女，副教授、在职博士研究生，主研方向：下一代网络体系结构，路由交换技术；兰巨龙，教授、博士生导师
收稿日期：2008-03-12 **E-mail：**lxq8228@163.com

构如图 1 所示。

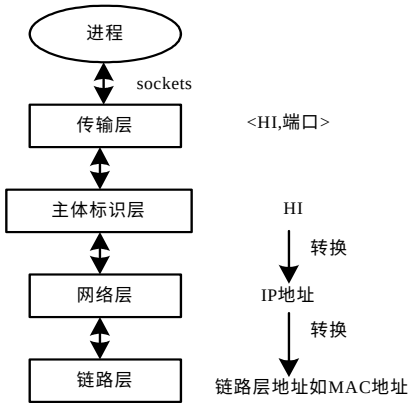

图 1　HIL 的体系结构

HIP 中的 IP 地址是非唯一分配的，一个主机标识可以对应多个 IP 地址。在 HIP 体系中，移动与多宿问题实际就是 HIT 和 IP 地址一对一和一对多的动态绑定关系。由于主机标志层的引入隔离了传输层与网络层，因此应用程序只看到一对不变的源 HIT、目的 HIT，移动与多宿对应用程序是透明的。HIP 协议从全局角度审视当前网络体系的缺陷，引入了主机标志和主机标志层，提出了一个解决主机移动、多宿问题的新思路，是 IETF 和 IRTF 研究的新热点。

2.1.2　HIP 的缺点

HIP 协议能同时解决主机移动、多宿主及系统安全性问题，其关键是对现有协议体系结构核心的修改。主机标识层将传输层和网络层分离，并用公/私钥对的公钥作为 HI 实现主机移动、多宿主及其安全性，但因为它是对 TCP/IP 核心的变动，所以在实际应用时会引发许多问题。

HIP 中主机标识层的名字空间定义很复杂，在实际使用中要维护很多对应关系，增大了管理开销和出错概率，且这些名字空间都是无结构的，查找效率较低。HIP 中没有提供从主机标识空间到 IP 地址空间的全局解析机制，且不支持组播。

2.2　PeerNet 协议

2.2.1　PeerNet 及其对移动性的支持

PeerNet[4]基于节点的身份标识和位置标识相分离的思想实现了 IP 地址双重功能的分离。PeerNet 是基于 P2P 的全新网络层协议，适用于由大量移动和固定节点组成的大型网络，这些节点使用当前 MAC 技术、采用双向链路连接，以取代 Internet 中的 IP 协议。PeerNet 采用 3 级区域网络结构，如图 2 所示。网络中所有节点都属于 3 级嵌套区域网络，且一个级别范围的网络节点共享唯一的地址前缀，L 级区域网络划分需要 L 位地址空间。

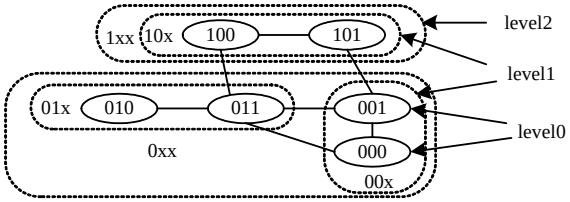

图 2　3 级区域网络结构

PeeerNet 网络中的每个节点都有一个节点标识和一个地址标识。PeerNet 中引入了 2 个新的全局名字空间，以取代现有 IP 地址空间。节点标识空间是全局的、非唯一分配的，节点标识代表节点身份，不随节点的移动而改变。PeerNet 对节点标识空间的其他性质没有进行明确定义。地址标识空间是全局的，具有固定长度及层次化结构，并且是唯一分配的。一个节点可能负责管理多个地址，但只能使用反映当前网络拓扑位置的唯一地址标识，当节点移动时，节点的地址标识随之动态改变。

PeeerNet 网络层中包括地址分配、路由和节点查找 3 个主要部分。地址组织像一个二叉树，地址分配是动态、永久不变的；动态寻址依靠节点当前的网络位置，由于地址标识完全层次化分配，因此在 PeerNet 中可以运用 P2P 网络的路由思想来组织路由；节点查找服务采用分布式机制，由节点标识查找对应的地址标识，存储找到的对应关系条目<ID,addr>。但 PeerNet 引入的是 2 个全局名字空间，因此，节点标识空间到地址标识空间的查找解析也是全局统一的。每个节点的节点标识和地址标识之间的对应关系由某个其他节点来维护。在进行通信之前，源节点只要知道目的节点的节点标识，利用查找解析机制查找到目的节点的地址标识并发送分组。由于地址标识仅用于网络层路由，因此 PeeNet 可以较好地支持主机移动。当移动节点获取新地址后，应及时进行节点标识和地址标识对应关系的更新。PeerNet 还可以支持组播和任意播。

2.2.2　PeerNet 的缺点

虽然 PeerNet 实现了对 IP 地址双重功能的分离，能较好适应未来大型网络、移动网络的发展需求，并支持主机移动，但 PeerNet 仍存在以下问题：(1)很难保证 P2P 路由表中的紧邻项也位于实际网络的紧邻位置，这对路由表的维护和路由效率都有影响；(2)由于每个节点只能使用反映当前网络拓扑的唯一地址，因此 PeerNet 不支持多宿主。

2.3　LNAI

2.3.1　LNAI 名字空间结构及对移动性的支持

LNAI[5](a Layered Naming Architecture for the Internet)对 Internet 名字空间的改进包括对 IP 地址双重功能的分离、对 DNS 的改进和对边缘网络中间件如 NATs/NAPTs 的兼容。LNAI 提出了 Internet 的 4 层名字空间结构，如图 3 所示。

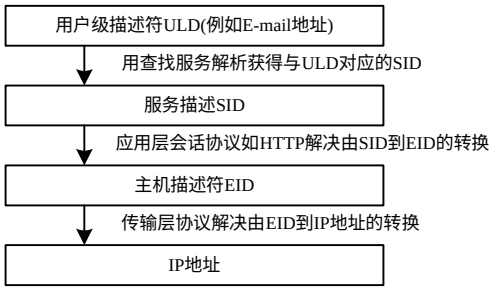

图 3　4 层名字空间结构

LNAI 采用扁平的名字空间，通过对服务和数据进行永久性的命名 SID，使它们成为 Internet 上最重要的对象；通过引入 EID，不再用 IP 地址作为主机标识，实现无缝支持主机移动和多宿主；通过各个层次的重定向功能，把边缘网络中间件整合到 Internet 体系结构。

2.3.2　存在的问题

LNAI 的部署无须改变 Internet 底层结构，但需要改变现有主机软件，包括协议和应用程序。解析这些扁平名字空间需要新的解析器，因此，LNAI 的部署代价较大。协议和应用程序的改变造成一些问题，如随着需要的增加，DHT 在引入了多个层次的名字空间后，安全问题(如 DoS 攻击)成为

LNAI 的一个较大隐患。

2.4 对比分析

现有多数改进因特网名字空间的方案改进角度不同，但都通过引入新的名字空间来弥补现有名字空间的不足。PeerNet 对因特网名字空间的改动最大,改变了核心网络的 IP 地址结构，其部署代价很大；HIP 和 LNAI 虽然只要在端系统上实现，但引入了新的传输层标识，需要改动所有现有主机软件，部署代价较大。

上述几种方案对 IP 地址的双重功能进行分离，解决 IP 地址语义过载问题。分离设备的身份标识和位置标识有利于从体系结构上解决移动、多宿主、IP 地址重分配及不同网络区域之间的通信等问题。把传输层的实体标识和网络层的实体标识分离更符合互联网的分层结构原则，使传输层和网络层可以各自独立地发展。一些方案还对网络安全性做了改进。

对因特网名字空间的改进是一项大工程，需要考虑多方面问题。现有改进方案仍存在不足，许多问题有待进一步研究。例如，对于 IP 地址双重功能的分离；在引入设备的身份标识空间后，如何设计新名字空间与 IP 地址之间的解析机制；如何与现有 DNS 协同工作。

3 基于一体化网络的移动通信机制

终端并不知道自己所处的网络位置，网络给用户提供的服务就是使终端无法感觉到自己的移动带来服务上的差别。如果它和其他终端正在通信或需要移动到其他接入路由器并和其他终端建立通信，都要求通信的不中断或正常快速地建立通信。

3.1 基于标识的一体化网络及其对移动性支持

基于接入标识 AID 与交换路由标识 RID 分离映射理论的一体化网络，使用接入标识代表终端的身份信息，使用交换路由标识代表终端的位置信息，利用网络来支持用户的移动性，符合身份与位置分离的设计思想且无须对种类繁多的各种终端进行协议修改[6]。新的一体化网络由服务层和网通层组成。网通层完成网络一体化，服务层实现服务普适化。这 2 层模型相结合，构成了一体化网络与普适服务体系的基础理论框架。

图 4 为一体化网络体系结构模型。

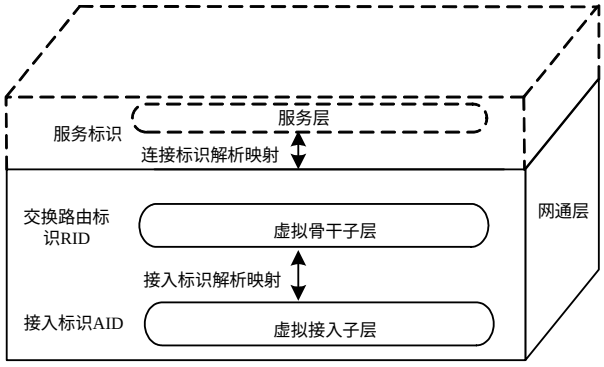

图 4 一体化网络体系结构模型

网通层又分为虚拟接入子层和虚拟骨干子层，采用基于 AID 与 RID 分离映射机制的通信方案，为语音、数据、图像等服务提供一个一体化通信平台。其核心思想是在一体化网络上分出接入层和核心层，接入层使用接入标识，核心层使用交换路由标识，在接入交换路由器上实现接入标识和交换路由标识的分离映射。虚拟接入子层引入了接入标识作为终端接入的身份标识，每个终端都具有一个或多个全球唯一的接入标识。终端的接入标识在移动中是固定不变的，有利于实现移动性。上层应用层通信采用的接入标识不变，即使移动仍不会造成用户连接的中断。虚拟骨干子层引入了交换路由标识，用于虚拟骨干子层的广义交换路由和寻路。当数据包进入虚拟骨干子层传输时，源端接入交换路由器采用内部的交换路由标识替代接入标识进行转发，到达通信对端的接入交换路由器后，数据包的交换路由标识被置换为原来的接入标识。这样，当数据包在虚拟骨干子层上传输时，其他用户不可能通过截获虚拟骨干子层的信息来分析用户身份，保护了用户隐私；也不可能通过用户身份来截获他们的信息，保证了用户信息的安全性。

3.2 移动通信机制

基于标识的一体化网络涉及的功能实体如下：

(1)名字服务器 NS。完成应用级用户名 HN 与 AID 的双向解析及 AID 到用户归属服务器标识的单向解析。

(2)用户归属服务器 HS。提供认证服务(用户与它所归属的 HS 之间)、用户身份信息(含认证需要的认证素材)、用户业务信息(用户签约信息)、用户所在的映射服务器标识。

(3)映射服务器 MS。存储接入本域的所有用户的映射关系及主机所在的 AS 标识，负责维护 AID-RID 的映射关系。在 MS 中查询 AS 上没有的 AID-RID 映射关系时，如果 MS 内有相应映射关系，则证明该主机通过 HS 的认证已接入网内；反之，则说明拥有该 AID 的主机还没有接入网内，其他用户无法与之通信。

(4)接入服务器 AS。一个域内可以有多个接入服务器 AS，AS 建立 AID-RID 映射，是虚拟接入子层和虚拟骨干子层的分界点。各名字之间的关系如图 5 所示。

图 5 名字之间的关系

当终端 MN1 移动到 AS-1’后，无论在哪个 AS 下，仍如同正常情况一样，向通信对端直接发起通信。但这时是 AS-1’接收来自终端 MN1 的数据包，AS-1’得知终端 MN1 不是它管辖的终端后，强制触发终端 MN1 发起认证请求，防止终端 MN1 是恶意用户冒充的非法终端。认证通过再分配得到自己的映射关系，查询得到对端的映射关系，此时不能直接用 RID 替换数据包中的 AID，因为对端的 AS 还不知道这个发生移动的终端 MN1 的映射关系。

解决方案是采用一种新的消息——Update 消息。在 AS-1’已经有源和目的标识映射关系后，向通信对端 AS-2 发送数据包之前，要向 AS-2 发送 Update 消息。Update 消息携带了终端 MN1 最新的映射关系，AS-2 接收到这个消息后要更新对端映射表，保存终端 MN1 最新分配的映射关系，返回给 AS-2 Update 响应消息。如果响应消息是确认消息，则通知 AS-2 现在它已经有终端 MN1 的映射关系，通告其发送数据包；如是错误消息，则通知 AS-2 终端 MN1 要通信的对端 MN2 不在 AS-2 管辖范围内。当 2 端都确定找到最新的映射关系后，AS-1’和 AS-2 才用 RID 通信。

4 结束语

本文方案对构建基于身份标识和路由标识分离机制的新型一体化网络与路由交换机制具有重要借鉴意义，但其实现有待进一步研究。

（下转第 113 页）