新体系结构下的一种移动通信解决方案*)

李秀芹[1,2]　兰巨龙[1]

(解放军信息工程大学 NDSC 研究所　郑州 450002)[1]　(华北水利水电学院信息工程学院　郑州 450011)[2]

摘　要　当今互联网在安全性和移动性方面存在着严重问题，应提出一种新的机制加以克服。现基于终端的身份与位置分离的设计思想，从全新的角度考虑问题，提出一种基于一体化网络的移动通信解决方案。

关键词　移动通信，AID，RID，一体化网络

Mobile Communication Solution Based on New Network Architecture

LI Xiu-qin[1,2]　LAN Ju-long[1]

(Institute of NDSC, Information Engineering University of PLA, Zhengzhou 450002, China)[1]

(Department of Information Engineering, North China University of Water Conservancy and Electric Power, Zhengzhou 450011, China)[2]

Abstract　To overcome the serious shortcomings of current Internet on aspects of the mobility and safety, a new mechanism should be proposed. According to the thought of the namespace improvement solutions that the identity and the position of a user separate mutually, this paper considered the problem from the all new angle and put forward a mobile communication solution based on the universal network.

Keywords　Mobile communication, Accessing identifier, Switching-routing identifier, Universal network

1　引言

当今互联网由于通信过程中始终使用唯一源 IP 地址和目的 IP 地址，在安全性和移动性方面存在着严重问题，应提出一种新的机制加以克服。虽然有很多研究人员对主机移动性及安全性问题进行了广泛而深入的研究，也提出了不少解决方案(如 SCTP, MIPV6)，但都没能很好地解决这些问题[1,2]；基于标识和位置分离的 LIN6, HIP, LNAI, FARA，虽然都能解决主机移动问题，但都是通过引入新的名字空间来弥补现有名字空间的不足。LIN6 协议在原有 IP 协议的基础上增加了标识转换、位置信息查询等功能，需要对网络的 DNS 服务器进行升级，同时需映射代理管理位置信息，对 IPV6 协议增加、改动较多；HIP 和 LNAI 虽然只需在端系统上实现，但由于引入了新的传输层标识，需要对所有的现有主机软件进行改动，部署代价也比较大。总体来说，都要求改变终端协议栈才能支持移动性[3-8]。FARA[9] 实际上是一种重新设计 Internet 体系结构的思想，把应用实体和网络层转发机制相分离，其新的体系结构不仅具有主机标识和位置标识分离的功能，还支持终端系统的认证。但 FARA 模型是非常抽象的，其中的通信实体并没有一个全局标识，需要带外的机制来寻找通信实体的位置，这在实际应用中并不容易做到。

而基于接入标识 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，既符合身份与位置分离的设计思想，也不需要对种类繁多的各种终端进行协议的修改[10]。

目前，各种移动、传感网络技术发展迅速，相应的移动网络和传感器网络等已逐渐形成。在一体化网络的设计过程中，必须考虑将各种固定、移动、传感网络等进行统一接入，使各种不同类型网络之间能够进行通信。一体化网络吸取现有各种信息网络在理论与技术上优点，摒弃它们各自的不足，最终达到在同一种网络下为各种不同服务提供良好支持的目的。

2　新体系架构

新的一体化网络由“服务层”和“网通层”两层次组成。“网通层”完成网络一体化，“服务层”实现服务普适化。这两层模型结合在一起，构成了一体化网络与普适服务体系的基础理论框架。图 1 为一体化网络体系结构模型。

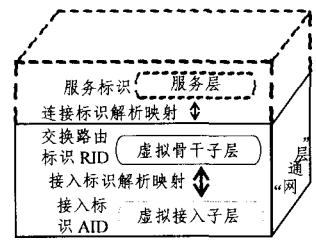

图 1　一体化网络体系结构模型

2.1　网通层

“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的通信平台。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

*)基金项目：国家 973 计划项目资助(课题编号：2007CB307102)。**李秀芹**　副教授，博士生，主要研究方向为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，主要研究方向为宽带信息网路由交换技术。

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，这方便了移动性的解决，上层应用层通信采用的接入标识不变，即使移动也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分析用户的身份，保证了用户的隐私性；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。

2.2 各功能实体

名字服务器 NS：完成应用级用户名 HN 与 AID 的双向解析；AID→用户归属服务器标识的单向解析。

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。

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。当 AS 上没有 AID-RID 映射时，MS 查询该映射关系。如果 MS 内有相应的映射关系，证明该主机通过 HS 的认证已经接入到网内。反之，如果 MS 内没有来查询的映射关系说明拥有该 AID 的主机还没有接入到网内，其它用户没法与之通信。

当 AS 为某个接入标识分配了（AID-RID）映射关系，通过映射关系更新消息向 MS 汇报这对新分配的映射关系。当 MS 收到映射关系更新消息后，则在数据库中记录映射关系，并向发送该消息的 AS 发送映射关系更新响应消息。通知其已经记录了最新的映射关系。

当 AS 收到 MS 发送的映射关系更新响应消息后，确定 MS 已收到该条（AID-RID）映射关系，如果 AS 在发送映射关系更新消息一段时间后未收到映射关系更新响应消息，则需要重新发送映射关系更新消息。

接入服务器 AS：一个域内接入服务器 AS 可有多个。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。

如果一个 AS 收到一个数据包，同时目标 RID 就是该 AS 所管辖的，将目标 RID 映射后得到的目的 AID 所代表的终端目前不在该 AS 覆盖区域内，或该 AS 的本地映射表中根本就没有数据包内的目标 RID，则该 AS 向源端 AS 发送 ERROR 消息。AS 收到 ERROR 消息表明本 AS 所存储的通信对端（AID-RID）映射错误，需要重新向映射服务器去查询。

当一个 AS 为其覆盖区域内的终端分配了（AID-RID）映射关系，如果该终端正在（将要）与一个或多个通信对端通信，这时 AS 需要向映射服务器查询通信对端的映射关系和所在 AS，这时触发该 AS 向其所有的通信对端所在的 AS 发送 UPDATE 消息，其中携带（AID-RID）映射关系及所在 AS 标识。AS 收到 UPDATE 消息后要及时更新通信对端映射表。

名字之间的关系如图 2 所示。

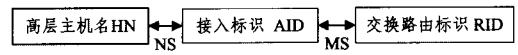

图 2 名字之间的关系

3 移动通信解决方案

由于终端并不知道自己所处的网络在什么位置，网络给用户提供的服务就是使终端感觉不到自己移动带来服务上的差别。它如果和其他终端正在通信或移动到其它 AS 下后再和其他终端建立通信，都要求通信的不中断或通信正常快速地建立。

当 MN1 移动到 AS-1'后，作为终端 MN1 它并不管自己接入在哪个 AS 下，仍像正常情况下一样，向通信对端直接发起通信。但这时是 AS-1'接收到了来自终端 MN1 的数据包，AS-1'会得知终端 MN1 不是它管辖的终端，然后强制触发终端 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和查询得到对端的映射关系之后，并不能直接用 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。

解决方案是提出了一种新的消息：UPDATE 消息。在 AS-1'已经有了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 接收到这个消息之后要更新对端映射表，存下终端 MN1 最新分配的映射关系。之后，把 UPDATE 响应消息返回给 AS-2。响应消息如是确认消息，告诉 AS-2 现在它已经有了终端 MN1 的映射关系，通告其发送数据包；如是 ERROR 消息，报告 AS-2 终端 MN1 要通信的对端 MN2 不在 AS-2 管辖范围内。当两端都确定找到最新的映射关系后，AS-1'和 AS-2 才用 RID 通信。

3.1 移动通信中使用的消息格式

移动通信中使用的消息报头格式如图 3 所示。

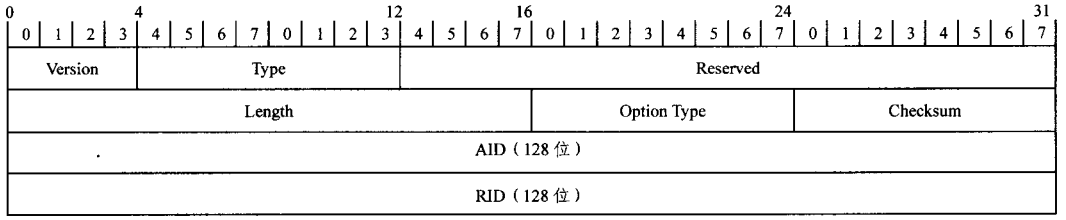

图 3 消息格式

Veision：协议版本。

Type：消息的类型。如 0＝查询消息，1＝查询响应消息，2＝报告消息，3＝报告响应消息。

Reserved：保留位。传送数据时全填 0。

Length：消息长度。

Option Type：结果类型。如在查询响应消息格式中：0 表示映射服务器上没有查到结果，内容为空；1 表示返回对交换路由标识的查询结果，2 表示返回对接入标识的查询结果。

Checksum:校验和。

AID:要查询的映射关系中的接入标识。

RID:要查询的映射关系中的交换路由标识。

3.2 域内移动通信

终端 MN1 由 AS-1 移动 AS-1',具体的通信流程如图 4 所示。

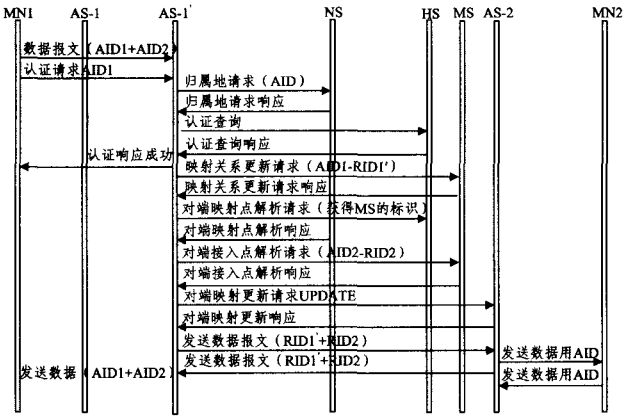

图 4 域内移动通信流程

1)端 MN1 由 AS-1 移到 AS-1'接入网络。2)终端 MN1 以自己的接入标识 AID1 为源标识,以通信对端 MN2 的接入标识 AID2 为目的标识,向 AS-1'发送数据包。3) AS-1'发现终端 MN1 不是自己管辖的用户,强制触发其发送认证请求;通过 NS 查询获得用户归属的服务器 HS 标识。4)终端 MN1 向 AS-1'发送认证请求消息;AS-1'向 HS 发送认证查询消息,HS 返回查询。5)AS-1'返回终端,MN1 认证请求消息。如果通过认证,就能允许其接入网络;反之,则认定终端 MN1 是非法用户,不允许其接入网络。6)如认证通过,AS-1'为终端 MN1 的接入标识 AID1 分配交换路由标识 RID1',形成映射关系 AID1-RID1',并存入本地映射表中。7)AS-1'向映射服务器 MS 报告这个最新的映射关系。8)如果 AS-1'不知道对端 MN2 的映射关系,则要去映射服务器查询。9)映射服务器返回查询消息,AS-1'发送将查询得到的终端 MN2 的映射关系 AID2-RID2 存入对端映射表中。10)AS-1'向 AS-2 发送 UPDATE 消息,AS-2 将 UPDATE 消息中携带的终端 MN1 的映射关系存入自己的对端映射表中。11)AS-2 向 AS-1'响应 UPDATE 消息。12)AS-1'将数据包的源和目的接入标识替换为交换路由标识,并转发出去。13)AS-2 收到数据包后也进行交换路由标识到接入标识的替换,并将数据包向接入网中的终端 MN2 转发出去,最后终端 MN2 收到终端 MN1 的数据包。

结束语 针对下一代通信网络的移动性、安全性,基于终端的身份与位置分离的设计思想,本文从全新的角度考虑问题,提出一种基于一体化网络的移动通信解决方案,对于我们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也将具有重要的借鉴意义。

但本方案只是通过对现有移动通信技术和新体系结构研究的基础提出的一种设想,对于该方案的具体实现还有待进一步深入研究。尽管如此,通过对这些新的设计技术的研究,我们相信这些非常新颖的设计思路将会影响人们解决类似问题的方法,对于移动通信问题的解决也有着非常重要的现实意义。

参 考 文 献

[1] Stewart R, Xie Q. Stream Control Transmission Protocol[S]. IETF, RFC 2960, October 2000

[2] Johnson D, Perkins C, Arkko J. Mobility support in IPv6[EB/OL]. http://www.ietf.org/rfc/rfc3775, 2004

[3] Teraoka F, Ishiyama M, Kunishii M, et al. LIN6: A Solution to Mobility and Multi-homing in IPv6[R]. internet draft-teraokaipng-lin6-01.txt (work in progress), 2001

[4] Ishiyama M, Kunishii M, Teraoka F. An analysis of mobility handling in LIN6[EB/OL]. http://www.lin6.net/papers/wpmc.pdf, 2001

[5] Moskowitz R, Nikander P. Host identity protocol architecture [EB/OL]. http://www.ietf.org/ internet-drafts/draft-ietf-hip-arch-02.txt, January 2004

[6] Nikander P, Arkko J, Henderson T. End-host mobility and multi-homing with the host identity protocol[EB/OL]. http://www.ietf.org/ internet-drafts/draft-ietf-hip-mm-01.txt, February 2005

[7] Nikander P, Ylitalo J, Wall J. Integrating Security, Mobility, and Multi-homing in a HIP Way[C]// Proceedings of Network and Distributed Systems Security Symposium (NDSS'03). San Diego, CA, US: Internet Society, February 2003: 87-99

[8] Balakrishnan H, Lakshminarayanan K, Ratnasamy S. A layered naming architecture for the Internet[C]// Proc. of the ACM SIGCOMM 2004. 2004: 343-352

[9] Clark D, Braden R. FARA: Reorganizing the Addressing Architecture[A]. ACM SIGCOMM[C], Germany, 2003: 313-321

[10] Yumiba H, Imai K, Yabusaki M. IP-based IMT Network Platform[J]. IEEE Pers. Commun., 2001, 8: 18-23

(上接第 89 页)

展性。3)基于收藏夹的缓存分类技术。

参 考 文 献

[1] Rodriguez P, Spanner C, Biersack E W. Analysis of Web Caching Architectures: Hierarchical and Distributed Caching. IEEE/ACM Transactions on Networking, 2001, 9(4): 404-419

[2] Li Wen-syan, Hsiung Wang-pin, Po O, et al. Challenges and Practices in Deploying Web Acceleration Solutions for Distributed Enterprise Systems// WWW2004. New York, 2004

[3] 贺琛,陈肇雄,黄河燕. Web 缓存技术综述. 小型微型计算机系统,2004,25(5):36-842

[4] Padmanabhan V N, Sripanidkulchai K. The Case for Cooperative Networking// IPTPS 2002. Cambridge, 2002

[5] Wang Xiao-yu, Ng Wee-siong, Ooi Beng-Chin, et al. Buddyweb: A P2P-based Collaborative Web Caching System// Networking 2002 Workshops. Pisa, Italy, 2002

[6] 黄桂敏,杨明福,王学光. 分散型Web缓存模型. 计算机工程,2004,29(17):29-30

[7] Watts D, Strogatz S. Collective dynamics of small-world networks. Nature, 1998: 393-440

[8] Webtraces. http://www.web-caching.com/traces-logs.html

[9] Kalogeraki V, Gunopulos D, Zeinalipour-Yazti D. A Local Search Mechanism for Peer-to-Peer Networks// CIKM. McLean USA, 2002