第 35 卷 第 5 期 计 算 机 工 程 2009 年 3 月
Vol.35 No.5 Computer Engineering March 2009
·网络与通信· 文章编号：1000—3428(2009)05—0087—04 文献标识码：A 中图分类号：TP393

基于 HIP 协议的间接通信结构设计与实现

景娜娜，程东年，胡宇祥，王浩学
(国家数字交换系统工程技术研究中心，郑州 450002)

摘 要：针对目前网络中最为棘手的移动和安全问题，提出一种基于主机身份协议的间接通信结构模型 HBIA，将用户的身份信息与位置信息相分离，引入新型接入路由器作为实现间接通信的中介。在搭建的测试环境中进行实现，测试结果表明，HBIA 能够较好地支持主机移动，并保证了其安全性。

关键词：主机身份协议；间接通信；接入路由器；移动

Design and Implementation of Indirect Communication Architecture Based on HIP Protocol

JING Na-na, CHENG Dong-nian, HU Yu-xiang, WANG Hao-xue
(National Digital Switching System Engineering and Technology Research Center, Zhengzhou 450002)

【Abstract】In order to solve the mobile and secure problems in the existing network, an indirect communication architecture model HBIA based on HIP protocol is propsed. In HBIA, the identity info and location info is separated, and new access routers are imported as the resonance of indirect communications. Then HBIA is implemented in the test environment and the result indicates this model can support the mobility of hosts and ensure the security very well.

【Key words】HIP protocol; indirect communication; access router; mobility

1 概述

现有因特网体系结构设计的思想就是为固定位置的主机提供点对点的单播通信。在这一基本服务中，发送主机知道接收者的 IP 地址，所以它可以直接进行 IP 路由并转发分组。这种点到点的通信有很多优点，但是随着 Internet 逐步发展成为一个全球性的通信基础结构，人们对通信功能的要求迅速增多，诸如组播、任播以及支持终端主机的移动等。尽管这些年很多学者、专家都在进行深入研究，试图将这些服务加入到 Internet 中，但效果都不是很理想。主要困难就在于点对点的直接通信结构假设发送者和接收者位于已知且固定的网络位置，这种假设无法满足上述几种服务的要求。而且，这种点对点的直接通信结构是具有幂率结构的无标度网络，导致其对恶意攻击和欺骗的抵御能力十分脆弱，因此安全问题也越来越严重地影响着网络提供的服务质量。

为了解决上述问题，需要提出能够综合多种服务的新的体系架构[1]，以此获得更加多样性的服务。于是，学者们开始尝试另外一个解决问题的思路，使用一种简单并且很有效的技术——间接通信技术[2]。这种方案假设在发送方和接收方之间插入一个物理的或者逻辑的“间接通信点”，用来在通信双方之间进行数据的中继。发送方通过这种“间接通信点”进行数据传输，而不是将数据直接发往终端接收主机。通过这种间接通信方式，发送方可以不用考虑接收方的具体位置，而且大大减弱了发送方和接收方紧密耦合的程度。

针对上述分析的移动和安全问题，设计了一种网络分层、功能分离、面向服务的基于 HIP 协议的间接通信结构(HIP-based Indirection Architecture, HBIA)模型。

通过 HIP 协议[3]建立一个安全的通信信道，使得基于 HIP 的数据流在 2 个互相信任的主机之间仍然能够以端对端的方式直接进行传输，实质上是通过一些中间功能实体完成通信。区别于目前网络提供的“一站式”信息直接传递方式，HBIA 模型采用的是“接力传递”方式，逻辑上分离了“基于 HIP 建立的通信通道”和“分段式的转发通道”，实现了 IP 层意义的间接通信。

2 HBIA 体系结构

HBIA 的基本思路就是允许直接的、用 IPsec 保护的端对端数据流通信，但实际上使用的是一种间接通信结构来路由 HIP 控制报文，将数据平面和控制平面相分离。其结构模型如图 1 所示。

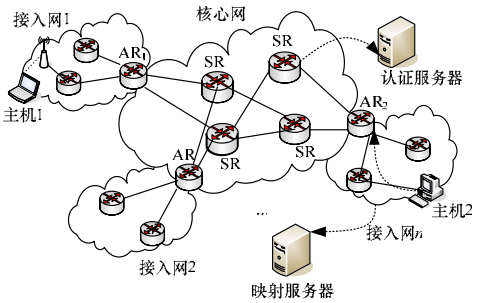

图 1 HBIA 结构模型

基金项目：国家“973”计划基金资助项目“一体化网络体系结构模型及交换路由理论与技术”(2007CB307102)
作者简介：景娜娜(1982－)，女，硕士研究生，主研方向：新一代网络体系结构；程东年，教授；胡宇祥，硕士研究生；王浩学，博士研究生
收稿日期：2008-07-14 **E-mail：**gena2004@163.com

2.1 基本定义

现有因特网的分层命名空间结构是扁平、一维的，以至于很多名字的概念与实际代表意义并不是很清晰。于是，笔者在 HBIA 通信网络中将命名空间结构变为分层的、多维命名空间，实现从以主机为中心的命名到以服务(数据)为中心的命名的转变。

HBIA 中用 HIT 表示主机身份信息；IP 地址表示主机的位置信息；LI 表示终端在本地子网内的位置；引入了接入路由器 AR[4]，负责多种异质异构子网和终端到核心网的接入工作，是实现间接通信的“ 中间功能实体 ”。在其内部维护一张本子网内的“ 用户信息采集表 ”，用以记录本网内接入该 AR 的所有用户的相关信息。

HBIA 中还引入了认证服务器 AS_{vr} 和映射射服务器 MS_{vr}。AS_{vr} 为用户提供身份认证服务；MS_{vr} 采用分布式哈希表(Distributed Hash Table, DHT)，结构互联为映射服务器网络，存储终端主机标识与网络地址标识的映射关系。

2.2 通信过程

整个通信过程包括 2 个阶段：基础网络初始化阶段和网络提供服务阶段。在初始化阶段，接入网中的各个接入路由器和本接入网的出口广义交换路由器建立连接。当基础网络初始化完成以后，通信网络就可以为用户终端提供服务。用户终端开机以后，接入某个接入路由器所辖网络，其首先完成身份认证，然后进行位置注册。用户利用已知的对方身份标识到映射服务器查询其位置，最后利用双方的位置信息建立通信连接。由网络来支持用户移动，负责由于终端移动而导致的通信连接的切换等。

2.2.1 用户私有身份认证过程

当终端用户开机以后，通过其所接入的 AR 接入通信网络。AR 将用户的私有身份 HI_{pri} 送到认证中心进行认证，如果其认证通过，则判定该用户为合法用户。

2.2.2 状态转换过程

当用户被判定为合法用户以后，AR 就为其分配一个 LI，于是该主机就可以与本网内的其他主机进行通信。而在 AR 从整个网络的角度来看，该终端处于“ 睡眠状态 ”，不需要为其提供更多的其他服务。但是，如果此主机预与本网外的其他主机进行通信，AR 一旦收到它的接入请求，就将主机的状态转换为“ 活跃状态 ”，至此主机被激活。通信结束以后，终端主机又会回到“ 睡眠状态 ”。同时接入某 AR 的终端可能会有很多，所以，采取这种方式能够降低 AR 的负担。

2.2.3 终端接入过程

当终端进入活跃状态时，AR 就要为其分配网络地址标识 IP，并在自己的“ 用户信息采集表 ”中添加“ 本地映射 ”记录 然后将该终端主机的 HIT 及其 IP 地址送到映射服务器，由 MS_{vr} 进行唯一性检测并建立“ HIT-IP ”映射表。

2.2.4 通信连接建立过程

至此，终端主机已经拥有了自己在网络中赖以通信的 IP 地址。类似于 TCP 传输需要三次握手过程来建立通信连接，在 HBIA 中，定义了终端用以建立连接的四次协商报文，分别是 I1, R1, I2 和 R2。

主机 1 首先向它自己的 AR 发送 I1 报文，触发本次通信。AR 查询“ 用户信息采集表 ”中的“ 对端映射 ”，查找主机 1 与主机 2 的映射关系；若没有找到，则无法继续转发 I1。因此，AR 将主机 2 的 HIT 发往 MS_{vr}。MS_{vr} 查找它自己的映射表，如果存在，说明主机 2 目前正处在活跃状态，可以与其通信；如果没找到，则说明主机 2 处于睡眠状态，那么 MS_{vr} 根据主机 2 的 HIT 判断其所处的子网位置及其 AR，然后 MS_{vr} 通知主机 2 的 AR，要求将其激活。同样主机 2 的 AR 为其分配一个 IP，填入“ 用户信息采集表 ”，并将“ HIT-IP ”映射关系发送给 MS_{vr}。之后映射服务器会将主机 2 的 IP 地址返回给主机 1 的 AR，由 2 个路由器之间进行报文交互。具体流程如图 2 所示，其中虚线表示当存在对应的标识映射时的直接跨越操作。

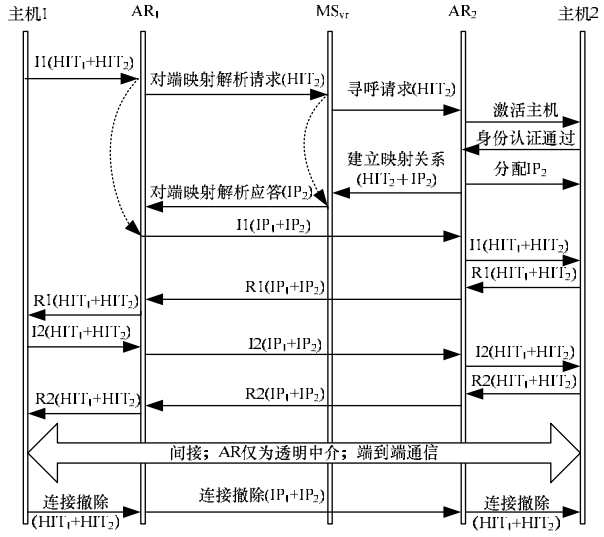

图 2 通信连接建立过程

由上面的流程图可以清晰地看到通信连接的建立过程，以及四次协商报文的报头信息，图 3 所示为四次报文所携带的数据内容。

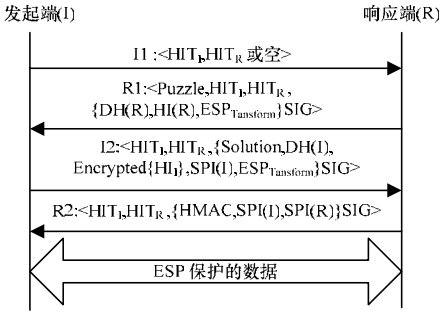

图 3 四次报文交互过程

基本交换完成后，通信双方就建立了一对安全关联。2 台主机可以通过 AR 进行 ESP 保护的端对端通信。其中，AR 仅仅是透明中介，帮助 2 台主机实现正常的间接通信。

2.2.5 通信连接拆除过程

当 2 个主机之间的数据传输完成以后，就需要拆除双方的通信连接。其中一方的 AR 在收到“ 连接撤除 ”消息后，就删除“ 对端映射 ”。同时，AR 还要通告 MS_{vr} 删除主机 1 与主机 2 的映射表项。之后，AR 将各自“ 用户信息采集表 ”中“ 本地映射 ”也删除，将主机的状态改为“ 睡眠状态 ”。至此，本次通信正式结束。

2.3 HBIA 移动性

为提高移动节点(MN)的切换性能，移动性支持主要由 HBIA 网络本身来完成，终端不参与移动切换的管理。节点移动的过程中，由于仅仅改变了节点的网络标识，而用户身份标识并没有发生变化，因此对于终端隐藏了网络拓扑位置

的变化，可以保持通信中的会话不中断。切换中映射的更新过程如图 4 所示。

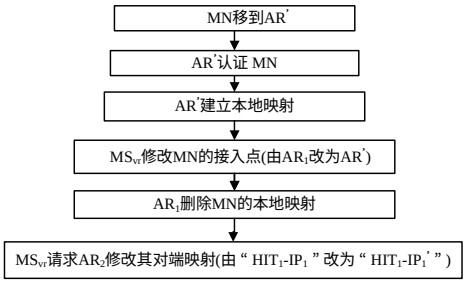

图 4　映射更新过程

2.4　HBIA 安全性

在 HBIA 中，HIT 仅仅用于表示主机的身份信息，不会在网络中出现，在网络中路由数据包的是 IP 地址。IP 的生存期也仅仅是本次通信的有效期，如果通信连接断开，那么 IP 地址就会被 AR 删除；下次需要建立通信连接时，AR 会根据网络地址标识的生成规则生成一个新的 IP。非法用户想要根据 IP 来获取主机的身份信息以及主机所在的具体位置是不能做到的。因此，终端主机的位置具有一定的隐秘性，极大地提高了安全性。而且，HBIA 采用非对称密钥算法保证了命名机制本身的安全性，在报文交互过程中引入了 Puzzle 机制避免响应端遭受 DoS 攻击。

3　HBIA 的实现

由于 HBIA 模型涉及众多的网络实体，诸如映射服务器、认证服务器等，这在现有网络环境中是很难做到的。因此，采用一种简化的 HBIA 模型进行实验，如图 5 所示。

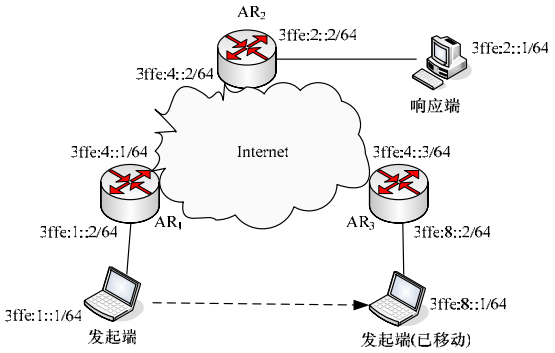

图 5　HBIA 的网络拓扑结构

该环境虽然使用了最小规模的网络设备，但是能够对 HBIA 中各种通信应用、标识的解析映射、各种终端的位置和身份隐私性等进行实验和验证。HBIA 的单向实现流程如图 6 所示。

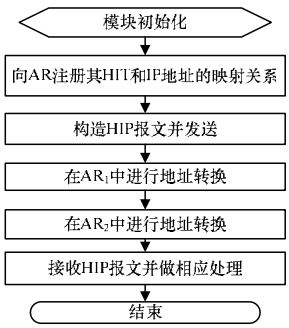

图 6　HBIA 单向实现流程

HBIA 模型是基于 HIP 协议的，并且需要 AR 作为中介来实现其间接性，因此，它的实现包括以下 2 个主要模块：

(1)主机上 HIP 协议的实现。HIP 模块主要用于实现 HIP 的协议机制，使得主机能够顺利传输 HIP 数据报。本文中 HIP 模块的实现基于 Linux 内核 2.6.10，在 IPv6 协议中支持 HIP 协议的基本功能。HIPL 的实现框图如图 7 所示。

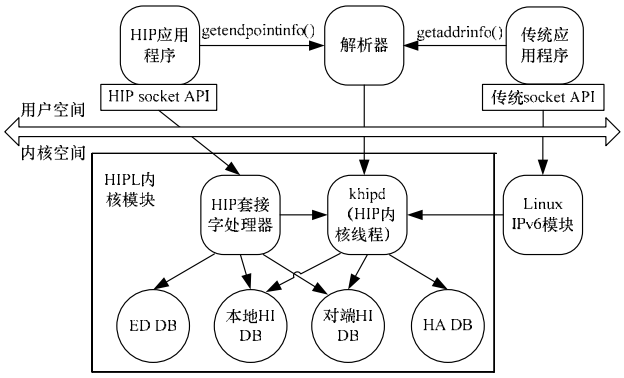

图 7　HIPL 实现框图

HIP 模块的实现主要分为 3 个部分：内核模块，接口处理模块和解析器的处理。HIP 应用程序通过已修改的 libinet6 解析器与 HIPL 内核模块进行通信，socket API 调用 HIP socket，从而将数据移到内核模块的 HIP 套接字处理器。而传统应用程序使用普通的 IPv6 socket API，只是在 IPv6 地址处使用 HIT。

(2)AR 功能的实现。AR 模块用于实现其作为“间接通信点”的功能，主要完成地址变换并转发报文。由于无法通过映射服务器查询主机 HIT 和 IP 的映射关系，因此在 AR 内增加了一个 hash 表，其中填入主机 HIT 和下一步路由的 IP 地址的映射关系，用以完成地址的查表转换。即假设 AR_1 知道对端主机所接入 AR_2 的地址。

4　HBIA 系统测试

当 HBIA 设计实现以后，笔者对其进行了一系列测试，其中包括 HBIA 通过 HIP 协议的连接建立过程、正常通信过程和主机移动性等。

4.1　测试过程

(1)数据通信

将一台主机作为发起端，即客户端，另外一台主机作为响应端，即服务器端。客户端向服务器端发送 HIP 报文，上层协议使用的是 TCP。

发起端给响应端发送数据的过程如图 8 所示。响应端的输出结果如图 9 所示。

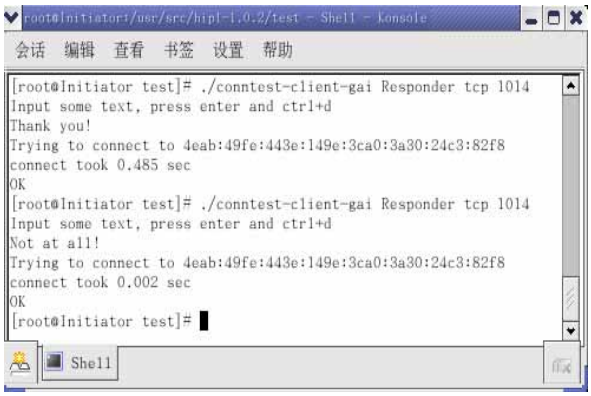

图 8　发起端数据

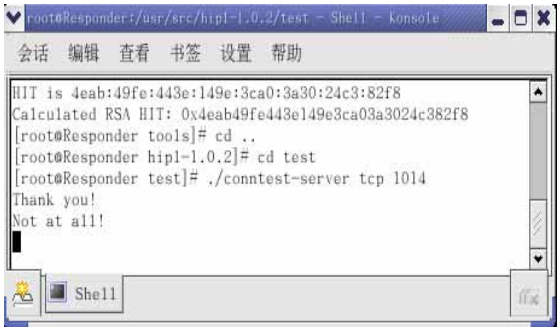

图 9　响应端数据

由此可见，发起端发送的数据都能够正常到达响应端，双方之间的通信连接已经成功建立。而且，第 2 次发送报文时不需要重新建立连接，可直接利用已有的连接过程，所以第 2 次数据传输所用的时间明显比第 1 次短很多。

(2)移动性测试

因为条件所限，所以用更改地址的方式来模拟主机移动。用来测试主机发生移动，IP 地址改变以后是否仍然可以使用原来的安全连接进行通信，而不需要重新建立安全连接。笔者在 2 台已经建立了连接的主机通信过程中，将发起端的 IP 地址由原来的 3ffe:1::1/64 变为 3ffe:8::1/64，接入的子网发生变化也就意味着其接入路由器发生了变化。然后，该主机再向响应端发送数据，结果证明 2 台主机之间的通信没有中断，数据能够正常传输。

4.2　测试数据分析

在测试过程中，笔者在发起端主机上装了抓包工具 Wireshark，其截获的报文如图 10 所示。

Wireshark 没有识别出 HIP 包，但是“ 0x63 ”化成十进制是“ 99 ”，正是 HIP 目前暂定的协议号，所以说明这是 HIP 包。如图 10 所示，前面 2 个 ICMP 报文是邻居探测消息，后面 IPv6 的 4 个报文正是 HIP 的四次协商报文：I1, R1, I2 和 R2。通信连接建立以后，通过 IPsec ESP 安全模式进行数据传输。因此，从第 7 个报文开始是加密的数据报文。在进行第 2 次传输报文时，不需要重新建立连接，因此没有四次协商报文，直接是 ESP 加密的数据报文。

当主机地址发生变化以后，数据仍然能够正确到达目的地，而且原来建立的安全连接也没有改变。因为安全连接的改变必然导致 SPI 的改变，但是根据抓包图(篇幅所限不在列出)，可以看到主机建立 SA 的 SPI 值仍然是 c9a3953b 和 82cb4a6c。因此，在主机发生移动之后，可以利用原有的安全连接进行通信。

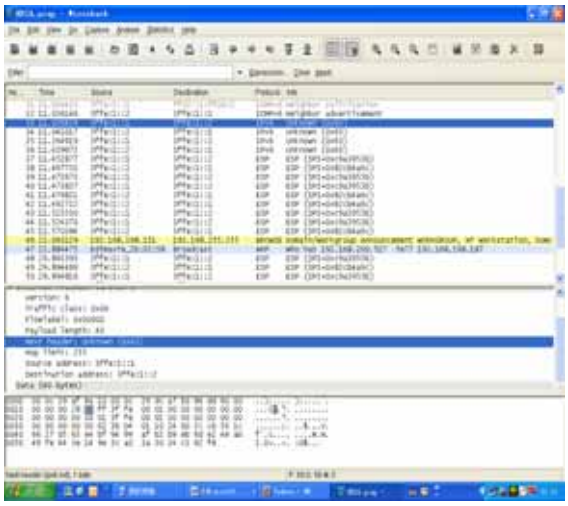

图 10　截获的 HIP 报文

5　结束语

现有网络以点对点为主的直接通信模式，严重阻碍了网络中其他功能的扩展，比如组播、任播以及终端移动等。而且现有网络是具有幂率结构的无标度网络，因此，各种安全问题时刻威胁着网络用户。针对最为棘手的移动和安全问题，提出一种基于 HIP 的间接通信结构模型 HBIA，将用户的身份信息与位置信息相分离，引入映射服务器和认证服务器提供安全保障，最主要的是引入新型的接入路由器作为实现间接通信的中介，将发送端与接收端的信息进行中转。移动问题都是由接入路由器进行处理，终端主机根本不需要参与。然后在简化的实验环境中进行了实现，测试结果表明这一模型能够很好地实现主机的移动，并保障了其安全性。

参考文献

[1] Crovella M, Kolaczyk E. FIND: Future Internet Network Design [EB/OL]. (2005-12-09). http://find.isi.edu.

[2] Stoica I, Adkins D, Shenker S, et al. Internet Indirection Infrastructure[C]//Proc. of ACM SIGCOMM’02. Pittsburgh, PA, USA: IEEE Press, 2002: 235-245.

[3] Moskowitz R. Identity Protocol (HIP) Architecture[S]. RFC 4423, 2006.

[4] 张宏科. 一种实现一体化网络服务的体系结构: 中国, 20050134579[P]. 2005.

编辑　顾逸斐

（上接第 71 页）

(4)“ 断点续传 ”技术在准确定位异常的基础上，提高了异常恢复的效率。

进一步的研究将深入到对分割粒度的控制上，可以在进一步提高交互性的基础上，设计一种更为智能的分割策略，并在研究中探索提高同步性能的新方法，期望推出交互性更好的、实用性更强的数据库同步新产品。

参考文献

[1] 蒋　敏. 基于网络隔离的异构数据库同步技术的研究与实现[D]. 杭州: 浙江大学, 2005

[2] 者　敬. 开放式异构数据库复制框架的研究与实现[D]. 北京: 中国科学院软件研究所, 2004-04.

[3] 杨　鹏. 异构数据库同步中间件技术的研究与实现[D]. 长沙: 国防科技大学, 2007-11.

[4] Ericson, IBM, Lotus, et al. SyncML Representation Protocal(Version 1.1)[Z]. (2002-02-15). http://www.syncml.org/docs/syncml_represent_ v11_20020215.pdf.

[5] Ericson, IBM, Lotus, et al. SyncML Sync Protocal(version 1.1)[Z]. (2002-02-15). http://www.syncml.org/docs/syncml_sync_protocol_v11_20020215.pdf.

编辑　索书志