

标识符和定位符分离方案研究

于士鹏

(东南大学 软件学院, 江苏 南京 210096)

摘要:目前IP地址既作为标识符又充当定位符,它的双重身份(标识符和定位符)造成了目前互联网核心路由趋向复杂。为了解决该问题,探讨了两种标识符和定位符的分离方案——LISP和HIP。LISP尽可能地保持了端系统的不变,用端系统的IP地址作为端系统的身份标识,而使用另外的路由器ID作为定位符;而HIP对现有域名空间进行扩展,通过全称域名来命名不同的主机来实现端系统标识符和定位符的分离。分析了两种方案的特点,并对它们的体系结构进行了详细的阐述,通过对这两种解决方案的对比,总结了其各自的优缺点。

关键词:标识符;定位符;LISP;HIP

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2009)07-0095-03

Study on the Locator/Identifier Separation

YU Shi-peng

(College of Software Engineering, Southeast University, Nanjing 210096, China)

Abstract: The IP address' dual statuses (identifier and locator) caused the present Internet core route trend to be complex. In order to resolve this problem, has discussed the identifier and the locator separation, and introduced two kinds in view of this question's solution, which respectively are LISP and HIP. LISP uses the host's IP address as its identifier and uses the router's ID as its locator. HIP expands the existing domain name space, and uses the global name to separate the identifier and locator. Has analyzed the architecture and the detail of the two solutions, and summed up their respective strengths and weaknesses by comparing in the end.

Key words: identifier; locator; LISP; HIP

1 标识符与定位符分离方案概述

网络地址的概念可以分为标识符(Identifier^[1])和定位符(Locator^[1])两部分。标识符是两台主机的通信会话的整个生存期内使用的位串,用于对其中一台主机相对于另一台进行标识。定位符用于对某个特定包必须交付的位置进行标识的位串。

标识符和定位符使得互联网的核心路由变得越来越复杂,通过研究者的深入研究,目前已提出了大致两类的解决方案:其中一类是在保持核心路由不变的情况下引入的机制,其典型代表是LISP^[2](Locator/ID Separation Protocol),它尽可能地保持了端系统的不变,用端系统的IP地址作为端系统的身份标识,而使用另外的路由器ID(RLOC^[2])作为定位符,并在路由器间转发报文时利用这个新的RLOC;而另一类方案HIP^[3]将现有域名空间进行扩展,通过全称域名(Fully Qualified Domain Name, FQDN)来命名不同的主机来

实现端系统标识符和定位符的分离,为了支持HI,传输层和网络层之间引入了新的一层——HIP层,HIP层完成了HI与IP地址的双射。下面将具体介绍这两种实现方案。

2 LISP

因为发送数据包的源站点将数据包的目的地址用端点标识符标记,但是此标识符并不能在Internet中全局路由的,所以目的地址需映射为一个全局路由定位符,以便于将其传递到另一个域中。LISP的提出正是解决了此问题。它基于映射(map-n-encap^[2])协议设计,它可以将Internet地址分离为终点标识符(EID^[2])和路由定位符(RLOC^[2])。终点标识符用一个唯一的空间编号来定义谁是设备;路由标识符用于描述设备是如何附在网络上的。

2.1 LISP 报头格式

经LISP封装后的IP数据包的报头的格式如图1所示,LISP其实就是在本来的报头的外部再加一个报头,这两个报头最大的不同就是其源地址和目的地址

收稿日期:2008-11-10;修回日期:2009-01-06

作者简介:于士鹏(1984-),男,硕士研究生,研究方向为网络应用;
导师:宛斌,研究员,研究方向为网络应用、无线通信。

部分,内部报头(IH)的源地址为发送数据包的源站点地址,目的地址是数据包的目的站点的地址,而外部报头(OH)的源地址为封装该数据包的 ITR(Ingress Tunnel Router^[2])的 RLOC,而目的地址部分为目的站点所在域的 ETR(Egress Tunnel Router^[2])的 RLOC。

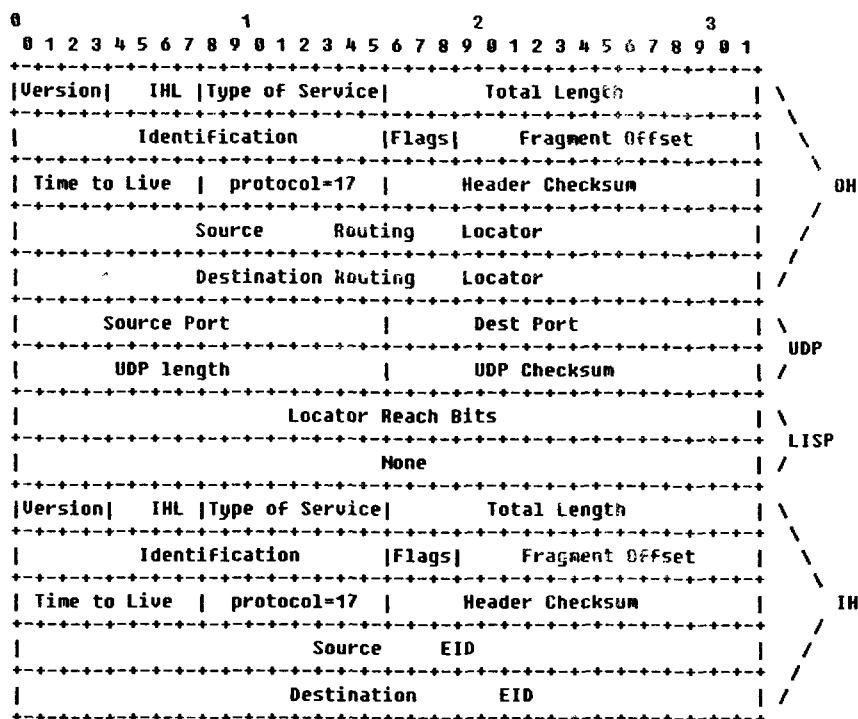


图 1 LISP 协议报头格式

2.2 LISP 的网络拓扑

为了完成从 EID 到 RLOC 的映射关系,需有一个拓扑来支撑,它就是 LISP-ALT^[2](LISP-Alternative-Topology)。这个逻辑拓扑主要用到了一些现存的技术,这其中包括 Border Gateway Protocol 和 Generic Routing Encapsulation Protocol 等。LISP-ALT 通过 BGP 和 GRE 建立了一个可完成数据探针包、映射请求包和映射应答包传递的逻辑拓扑。ALT 的路由信息由 EID 前缀和与其相关的下一跳地址组成,而 ALT 的路由器将从 ETR 处收到的或是通过配置预先得到的 EID 前缀通过 BGP^[4]进行相互之间的传递,以完成 EID 前缀的及时更新。

2.3 解析 LISP 的发送过程

处于一个支持 LISP 的域中的一台主机将要向处于另一域中的主机发送数据包时,将其 IP 地址写入报头的源地址处,将目的站点的 IP 地址写入报头的目的地址处,然后将该包发送出去。收到该数据包的本域的 ITR 将对该包进行 LISP 封装。如果 ITR 的存储器中有该 EID-to-RLOC 信息,它将目的 RLOC 写入外层报头的目的地址处,而自己的 RLOC 写入外层报头的源地址处,然后将该包发送到 Internet 中。该包

将根据目的地址处的 RLOC 到达目的域的 ETR,再由其进行解封装和发送到目的站点的工作。如果 ITR 的存储器中并不含有该 EID-to-RLOC 信息,它将首先发送一个数据探针包到映射系统中,等待对应 ETR 发送回来的 Map-Reply 包以取得所需的 EID-to-

RLOC 信息。当其收到 ETR 回复的映射信息时,再进行 LISP 封装。

3 HIP

3.1 HIP 名字空间

HIP 协议引入了新的名字空间。它将主机的地址标识和与主机通信的身份标识分离开来。这个名字空间要求任何设备都有全球范围内唯一的主机标识(HI)。主机标识是一个非对称密钥的公钥,可以由本机生成也可以由认证机构如 PKI 来生成^[5]。一个主机可以拥有多个主机标识,这些标识有些是公开的,有些是私有的,甚至是匿名的,HIP 利用这些标识就可以提供认证服务。HI 可以应用到现在的基于 IP 协议的网络中。

为了支持 HI,传输层和网络层之间引入了新的一层——HIP 层,它可以完成 HI 与 IP 地址的双射(如图 2 所示)。

HI 具有两种主要代表,一个是 full Host Identifier (HI^[3]),一个是 Host Identity Tag(HIT^[3])。HI 和 HIT 之间有细微但重要的区别。HI 指的是用来标识 Identifier 的抽象实体,具体的来说就是在标识过程中的字节位。HIT 是对 HI 的 128 位 Hash 结果值,其头两位比特的选择使其保持与 IPv6 地址空间的兼容性^[6]。

3.2 HIP 协议的层次模型

HIP 引入了一个新的命名空间 HI 来标识主机的身份,而主机的 IP 地址只标识主机在网络中的位置。在 HIP 引入了 HI 以后,由于主机的 IP 地址只代表主机在网络中的位置,而不代表主机的身份,所以 IP 地址信息只是用于报文传输过程中的路由,在传输层和应用层就不必知道主机的 IP 地址,而需感知主机的标识 HI。

由于应用层并不需要关心主机在网络中的位置信息,而更关心的是通信对端的身份,所以在 HIP 中的 IP 地址应该在被屏蔽的传输层之下;而网络层的主要功能是路由功能,主机的位置信息即主机的 IP 地址正

是网络层关注的焦点。由以上的分析,应在传输层和网络层之间加入一个 HI 层,来对上层屏蔽主机的 IP 地址和完成 HI 与 IP 之间的映射。当报文经上层送到 HI 层后,HI 层根据主机标识找到与之对应的源 IP 地址和目的地址,然后再经下层发出。报文在传输过程中路由器可以根据目的 IP 地址对主机进行路由选择。

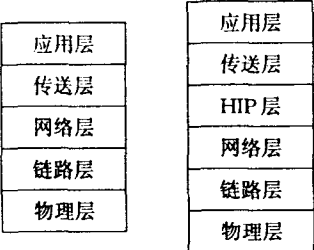


图 2 引入 HIP 层前后网络层次模型对比

3.3 HIP 包结构

所有的 HIP 数据包都是以固定的报头开始,其报头格式如图 3 所示。

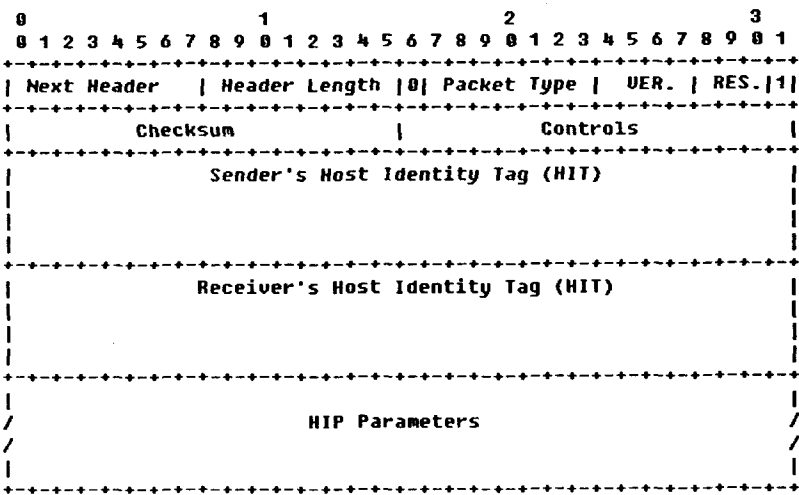


图 3 HIP 协议报头格式

Next Header 指示下一个报头的位置。
Header Length 域使用 8 比特的空间,记录的是 HIP 报头中除最前面 8 字节的其余报文的长度,当然其中也包括 HIP Parameters 部分。
Checksum 中存放校验和。源 IP 地址和目的 IP 地址被包含在校验和计算中。
Controls 是 HIP 协议的控制标志。
Packet Type 部分指出本数据包的类型。
HIP Version 部分表示 HIP 的版本号,目前的版本号为 1。
版本号后面的三比特以备将来使用,当发送 HIP 包时,该三比特将用 0 进行填充;当处理 HIP 包时,这三个比特的值也将被忽略。
HIP Parameter 域是可变长度的,用来容纳 HIP 协议的各种参数。

3.4 HIP 建立连接过程

两台主机通过一个加密的四次握手过程来建立一个双向的 IPSec SA,通过使用这种相对复杂的握手过程可有效地抵抗 QoS 攻击、中间人攻击和重放攻击^[7]。下面具体介绍一下该连接建立过程。
HIP 连接的发起者首先发送一个数据包(I1)给该连接的响应者,这个数据包主要包括发起者的 HIT,如果发起者已知响应者的 HIT,数据包中也应将其包含在内。当响应者收到 I1 后,发送一个应答数据包(R2),R2 中包含产生的 Diffie-Hellman 密钥交换算法的 DH 半会话密钥,以及它自己的公钥 HI,同时附上它自己的签名。当发起者收到该包后,他首先通过应答者的公钥检验该包是否来自于应答者,同时它产生自己的 DH 半会话密钥,结合 R 的半会话密钥计算得出 DH 会话密钥,然后由该会话密钥产生 HIP 的 SA,并使用该 SA 来认证加密数据包的信息。这些信息加上发起者的签名作为 I2 再发送给应答者。待应答者收到该包后,可得到发起者的 DH 半会话密钥,计算 DH 会话密钥和创建 HIP SA,并获得发起者的公钥,通过签名确认信息确认该包确实来自于发起者。应答者发送一个数据包 R2 用来确认发起者所发的数据包已经收到,并保护发起者免受重放攻击^[8,9]。连接建立示意图如图 4 所示。

4 结束语

LISP 和 HIP 都实现了标识符和定位符的分离,但通过比较两种方案可以发现它们各自的优缺点。LISP 没有改变现有的网络体系结构,并尽可能地保持了端系统的不变,但它是在 IPv4 的基础上实现的,而对 IPv6 没有进行考虑。

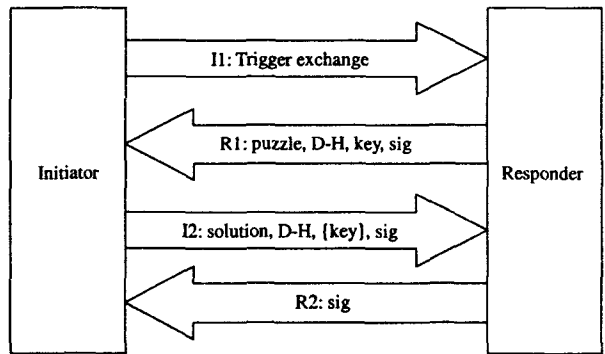


图 4 HIP 建立连接过程

(下转第 101 页)

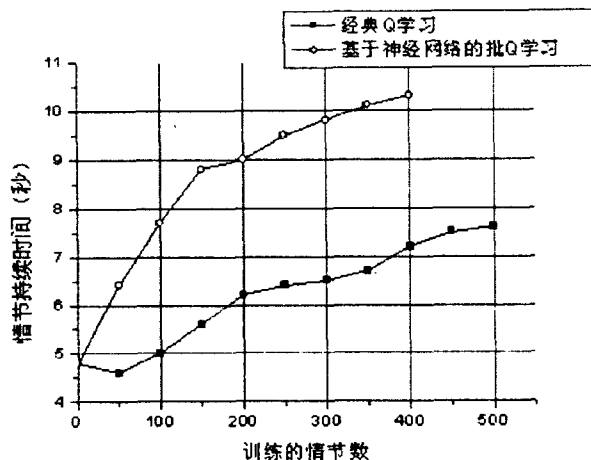


图2 500个情节的训练结果

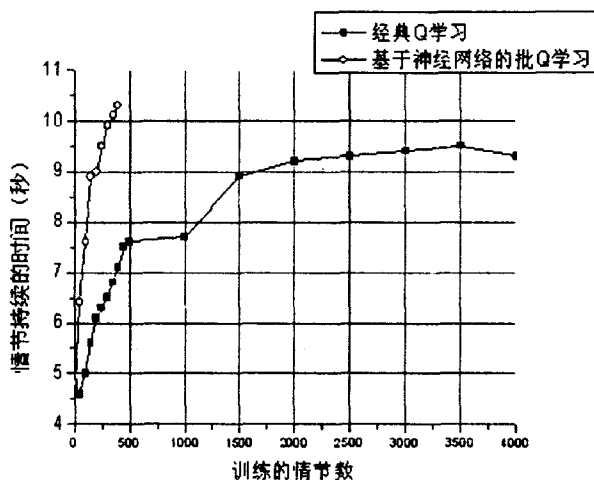


图3 40000个情节的训练结果

参考文献:

- [1] Kok J R, Vlassis N. Sparse Cooperative Q-learning[C]// Greiner R, Schuurmans D. Proc. of the 21st Int. Conf. on Machine Learning. Banff, Alberta, Canada: ACM, 2004: 481 - 488.
- [2] Stone P, Sutton R. Scaling reinforcement learning toward RoboCup soccer[C]// Pro. of the 18th International Conf on Machine Learning. Berkshires, Massachussets: ACM, 2001.
- [3] Kaelbling L P, Littman M L, Moore A W. Reinforcement learning: A survey[J]. Journal of Artificial Intelligence, 1996, 4: 237 - 285.
- [4] Sutton R S, Barto A G. Reinforcement Learning[M]. Cambridge, MA: The MIT Press, 1998.
- [5] Lin L J. Self-improving reactive agents based on reinforcement learning, planning and teaching[J]. Machine Learning, 1992, 8: 293 - 321.
- [6] Tesauro G J. TD-gammon, a self-teaching back gammon program, achieves master-level play[J]. Neural Computation, 1994, 6(2): 215 - 219.
- [7] 马勇, 李龙澍, 李学俊. 基于Q学习的Agent智能防守策略研究与应用[J]. 计算机技术与发展, 2008, 18(12): 106 - 108.
- [8] Ernst D, Geurts P, Wehenkel L. Tree-based batch mode reinforcement learning[J]. J. Mach. Learn. Res., 2005, 6: 503 - 556.
- [9] Stone P, Kuhlmann G, Taylor M E, et al. Keepaway soccer: From machine learning testbed to benchmark[C]// RoboCup - 2005: Robot Soccer World Cup IX. New York: Springer-Verlag, 2006: 93 - 105.

(上接第97页)

HIP是现有的基于IPv4和IPv6的互联网下标识符和定位符的分离方案,并在终端间进行认证和建立IPsec^[10]安全关联来提供安全保障。

虽然为了支持HI传输层和网络层之间引入了HIP层,但是IETF协议栈可以继续工作,而且原有的大多数分层网络体系结构不需改变。通过对比分析可以发现HIP是更优秀的标识符与定位符的分离方案。

参考文献:

- [1] Carpenter B, Crowcroft J, Rekhter Y. IPv4 Address Behaviour Today[S]. RFC2101. 1997.
- [2] Meyer D. The Locator/Identifier Separation Protocol[EB/OL]. 2008-02-27. <http://www.ripe.net/ripe/meeting/lisp>.
- [3] Moskowitz R, Nikander P, Henderson T. Host Identity Protocol[EB/OL]. 2007-10-30. [http://www.ietf.org/draft-](http://www.ietf.org/draft-ietf-hip-base-10.txt)

ietf-hip-base-10.txt.

- [4] 庄正松, 吴家皋, 吴清亮, 等. 互联网基本服务IPv4/IPv6过渡的研究与实现[J]. 计算机技术与发展, 2006, 16(8): 13 - 15.
- [5] 徐明伟, 吴建平. 主机标识协议研究综述[J]. 小型微型计算机系统, 2007, 28(2): 4 - 5.
- [6] 汪文勇. 下一代互联网实名访问机制研究[J]. 电子科技大学学报, 2006, 35(1): 2 - 5.
- [7] 徐剑. 主机标识协议Puzzle机制及协议实现研究[DB/OL]. 中国学位论文全文数据库, 2006.
- [8] 罗利军. 主机标识协议HIP的实现—基本通信模块[DB/OL]. 中国学位论文全文数据库, 2005.
- [9] 刘欣. 主机标识协议HIP的实现—安全模块[DB/OL]. 中国学位论文全文数据库, 2005.
- [10] 刘淑芝, 吴海涛. IPv6之后的网络安全问题分析[J]. 计算机技术与发展, 2006, 16(8): 243 - 245.