基于 AAA 的移动 IPv6 跨管理域注册过程的研究

李永建,郑明春,张善伟,姜 永
(山东师范大学 管理学院,山东 济南 250014)

摘 要:当移动 IPv6 在商业化网络中进行部署的时候,移动节点需要 AAA 服务器进行认证、授权、计费,于是怎样使移动 IPv6 和 AAA 协议高效地融合成为人们研究的热点。文中从协议交互的角度先对具有代表性的两种方案进行了分析和研究,指出了由于在路由优化模式中采用了迂回路由过程产生了较多的信令报文和较长的时延使得整体效果不理想,最后介绍了 IETF 提出的一种优化草案,利用家乡代理(HA)和通信对端(CN)之间的 AAA 机制来替代迂回路由过程,有效地减少了信令开销和切换时延。

关键词:移动 IPv6;AAA;路由优化模式;迂回路由过程
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2007)06-0022-04

Study on Mobile IPv6 Handover Between Administrative Domains Based on AAA

LI Yong-jian, ZHENG Ming-chun, ZHANG Shan-wei, JIANG Yong
(School of Management, Shandong Normal University, Jinan 250014, China)

Abstract: When mobile IPv6 is deployed in commercial network, a mobile node needs AAA for authentication, authorization and accounting. Hence scheme which integrating AAA with mobile IPv6 has been research by people. In this paper, do some research and analysis on the two schemes and point out that the result is not satisfactory. Since route optimization mode for MIPv6 is performed using return routability procedure. At last introduce a draft proposed by IETF, which using the AAA infrastructure between the home agent and a correspondent node instead of return routability procedure. The scheme can reduce handover latency and signaling overhead.

Key words: mobile IPv6; AAA; route optimization mode; return routability procedure

0 引 言

移动 IPv6[1]提供了移动节点在 IPv6 网络中移动时保持数据通信不间断的技术,并在 2006 年被 IETF 制定成标准。但在高度商业化的社会中,用户是以付费的方式使用网络资源和享受网络服务的。特别是移动节点在不同的管理域间移动的时候,需要 AAA 服务器进行认证、授权、计费。

认证(Authentication)即确定用户的身份;授权(Authorization)即确定用户使用资源的权限;计费(Accounting)即利用统计的用户使用资源情况对用户进行计费。人们常常称认证、授权、计费为"3A"或"AAA"。但是 AAA 协议和移动 IPv6 是相互独立运行的,于是怎样使移动 IPv6 和 AAA 协议高效融合成为人们研究的课题。

收稿日期:2006-09-19
基金项目:山东省泰山学者基金资助项目
作者简介:李永建(1983-),男,山东人,硕士研究生,研究方向为网络服务质量、AAA(认证、授权、计费);郑明春,教授,硕士生导师,研究方向为计算机网络应用、网络拥塞控制等。

1 移动 IPv6 和迂回路由过程(RRP)

MIPv6 协议使移动节点(MN)在改变网络接入点时具有继续和家乡代理(HA)、通信对端(CN)保持链接的能力。在 MIPv6 中 MN 有两个地址:家乡地址(HoA)和转交地址(CoA)。HoA 在家乡网络中分配给 MN,并且在 MN 移动过程中保持不变,因此 HA 和 CN 总是能够通过 HoA 访问到 MN。CoA 是 MN 移动到外地链路时产生并使用的地址,移动节点的 HoA 和 CoA 的关联称为绑定。

在 MIPv6 中,MN 通过路由优化模式进行路由优化,直接与 CN 进行通信。路由优化模式包括迂回路由过程(RRP, Return Routability Procedure)、绑定更新和绑定应答。

MN 和 CN 执行 RRP 来证明通过移动节点的 HoA 和 CoA 均可对其进行访问,并防范各种链接劫持和拒绝服务攻击,来保证 MN 和 CN 通信时的安全[2]。其

原理是通过对 MN 和 CN 之间交换的信令进行加密来对它们之间的登记进行认证。在执行的过程中,MN 向 CN 发送两个不同的测试数据包。其中一个通过家乡代理发送,另一个直接发送给 CN。在路由优化模式中通信双方共同计算一个共享密钥,通过该共享密钥对绑定更新和绑定应答进行认证。路由优化模式如图 1 所示。

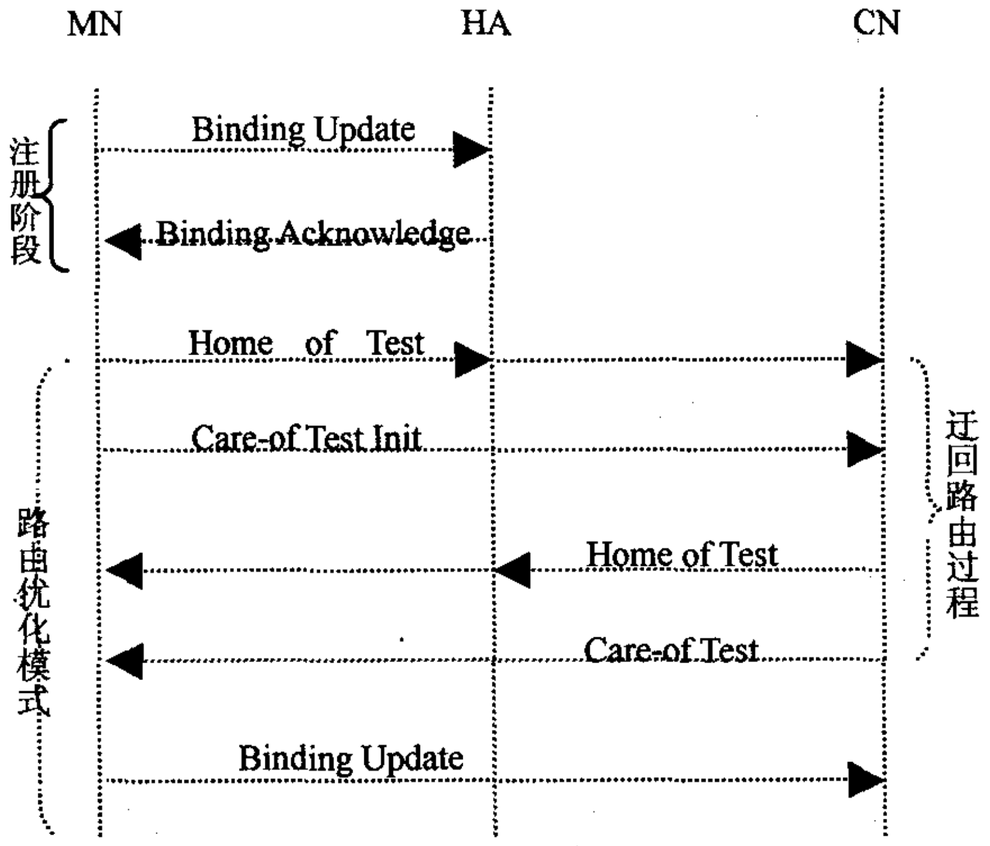

图 1　MIPv6 路由优化模式

迂回路由过程有四个信令:Home of Test Init (HoTI); Home of Test (HoT); Care - of Test Init (CoTI)和 Care - of Test (CoT)。通信双方通过这四个信令生成 Kbm(公共密钥),如图 1 所示,HoTI 报文通过 HA 发送给 CN,CoTI 直接发送给 CN。其中 HoTI 用于把 MN 的家乡地址和 Cookie 通知 CN,请求 CN 生成家乡密钥生成令牌,CoTI 用于把 MN 的转交地址和 Cookie 通知 CN,请求生成转交密钥生成令牌。CN 收到后分别处理这两个报文,并将处理的结果分别以 HoT、CoT 报文返回给 MN,当 MN 收到时从报文中提取出密钥生成令牌,计算出 Kbm。MN 利用 RRP 生成的密钥向 CN 注册当前的转交地址。这样一个路由优化模式就完成了,MN 和 CN 就可以直接进行通信了。

2　引入 AAA 后的移动 IPv6

当 MIPv6 部署在商业化的网络中,MN 需要 AAA 允许访问家乡域以外的管理域提供的资源。也就是 AAA 需要确定 MN 的身份、确定 MN 使用资源的权限、收集 MN 使用资源的计费信息。AAA 是一个分布式安全模型,由中心服务器和分布式客户机组成,实体间的链接通过 IPsec 和 TLS 安全协议进行安全保证。具有 AAA 功能的 MIPv6 的体系结构如图 2 所示。

在图 2 中,AAAH 是 MN 的家乡网络的 AAA 服务器,AAAL 是本地网络的 AAA 服务器,AAA Attendant 是本地 AAA 系统的入口点并提供和注册本地地址。AAAL 和 AAAH、AAAH 和 HA、AAAL 和 AAA Attendant 之间的安全关联通过 IPsec 和 TLS 来保证。AAA Attendant 可以在访问路由器(AR)来实现。

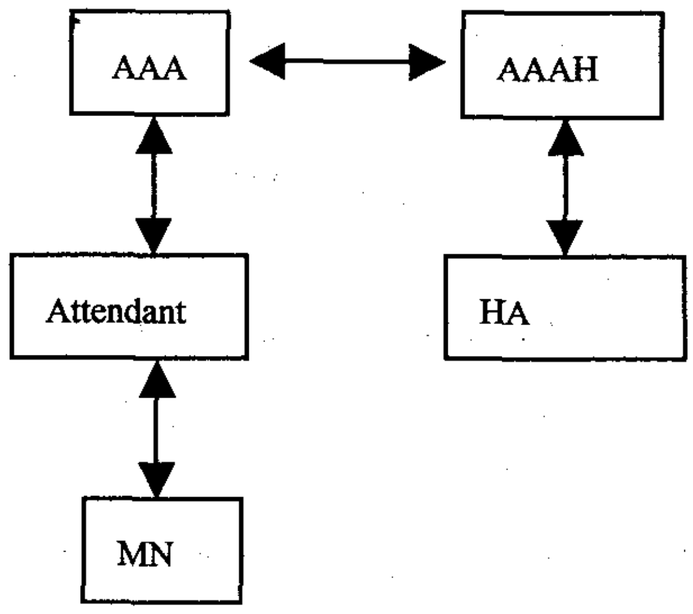

图 2　MIPv6 的 AAA 模型

当 MN 移动到外地域时,通过 AAA 获得授权,得到访问链接的外地域的权限,然后 MIPv6 支持它的移动性。但是怎样使这两种相互独立的协议高效地结合起来,使得融合后的切换满足人们的需求成为人们研究的难题。

3　现有结合方案分析

文献[3~5]给出了这两种协议的结合方案,笔者选取了两种具有代表性的方案进行分析,从协议报文的交互过程入手,重点分析了 MN 的注册过程。

3.1　MIPv6 与 AAA 注册相分离的结合方案

文献[3]提出了一种结合方案。在这种方案中,AAA 体系向 MN 提供认证、授权并创建安全证书以保证以后的 AAA 和 MIPv6 注册的安全。MIPv6 负责 MN 的移动性支持,这两种协议的注册过程依次进行。详细的注册过程如图 3 所示。

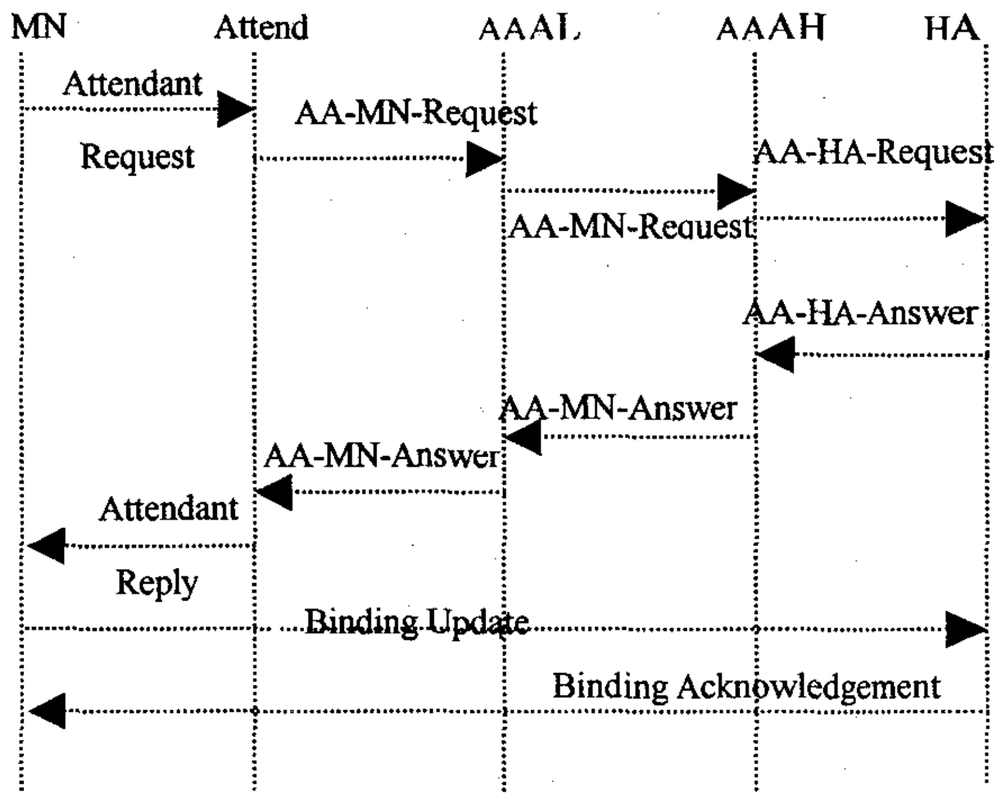

图 3　文献[3]的信令交换过程

在图 3 中,当 MN 到达一个新的管理域,提出访问请求,接着 Attendant 发出 AMR 报文,这是第一个 AAA 报文,通过 AAAL 转发给 AAAH,然后 AAAH 发送第二个 AAA 报文 AHR 到 HA,HA 收到后对请求进

行处理,然后将处理的结果以 AHA 报文、AAAH、AAAL、Attendant 依次进行处理并进行答复。MN 得到认证、授权后将执行 MIPv6 的注册过程来支持其通信的连续性,注册结束后 MN 执行路由优化模式来直接和 CN 通信。

这个方案的 AAA 过程和 MIPv6 的注册过程是依次进行的。虽然满足了 MN 的 AAA 需求和移动性支持,但是没有有效地将这两种独立的方案融合为一体,这样信令开销和切换时延比较大,难以满足实时通信的要求。

3.2 MIPv6 和 AAA 融合一体的结合方案

文献[4]将 MIPv6 注册和 AAA 认证、授权融合在一次注册过程中。在图 4 中,MIP Reg. Req. 报文是 MIPv6 注册请求报文,它同时请求 AAA 认证和 MIPv6 注册。与之对应 MIP Reg. Reply 是 MIPv6 注册应答报文,将返回注册请求的结果。详细的报文交换过程如图 4 所示。

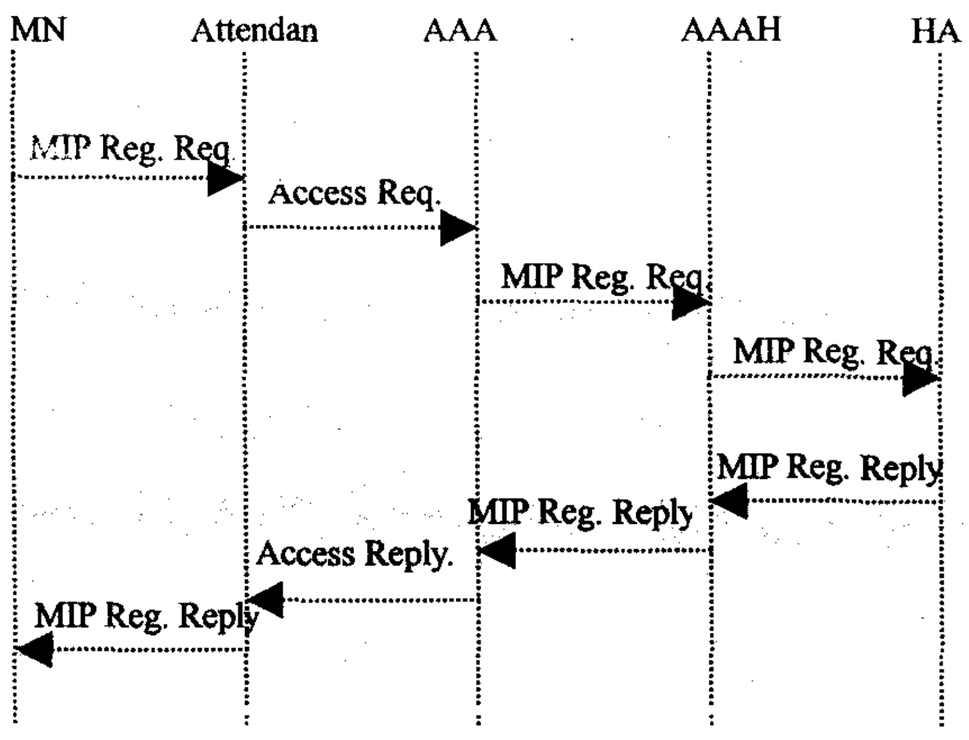

图 4 文献[4]的信令交换过程

如图 4 所示,当 MN 移动到一个新的管理域的时候,收到路由公告,然后向 Attendant 发出注册请求。Attendant 将转发请求给 AAAL,通过 AAAL 请求报文转发到 AAAH,对 MN 的身份进行核查。当 AAAH 核查成功后,将 MIP 注册报文发给 HA。HA 对收到的报文进行处理,更新地址项,然后将处理的结果通过 MIP Reg. Reply 报文告知 AAAH。AAAL、Attendant 依次做出反应,最后将注册请求的结果发送给 MN。注册成功后,MN 使用路由优化模式就可以和 CN 直接通信了。

与文献[3]中的方案相比,这种方案将移动 IPv6 和 AAA 的注册信令整合成一个信令,大大减少了信令开销,同时将 MIPv6 和 AAA 两个分离的、依次执行的注册过程整合成一次同时注册,大大减少了切换时延。因此这种方案比文献[3]中的方案的切换性能有了较大的提高。

4 一种新的针对路由优化模式的优化方案

4.1 现有的结合方案中存在的问题

在现有的结合方案中,文献[4]更好地对 AAA 和 MIPv6 的融合过程进行了优化,即满足了 MN 的移动性要求又对认证、授权、注册过程进行了优化。但是在这种方案中执行路由优化模式时仍然采用了迂回路由过程算法(RRP),由于这种算法使用了较多的信令报文,必然会导致过多的信令开销和较长的切换时延。这对一些应用特别是多媒体实时应用产生了严重的影响。

4.2 对路由优化模式的优化方案

为了解决路由优化模式采用 RRP 带来的上述问题,IETF 建议使用 HA 和 CN 之间的 AAA 基础设施来代替 RRP 执行路由优化[6]。当 MN 请求 AAA 认证的时候,在报文中嵌入家乡绑定更新和 CN 的信息(CN 的地址、NAI)。当 HA 通过 AAA 的体系机制收到家乡绑定更新报文和 CN 的信息的时候,执行家乡绑定更新并利用收到的关于 CN 的信息创建一个绑定更新报文(BU)发送给 CN。CN 收到后做出处理,对 MN 的转交地址进行更新,就可以直接和 MN 进行通信了。由于在传送报文的过程中在通信双方之间建立了安全关联,利用 AAA 的安全机制,使用 IPsec 和 TLS 协议使得通信时的安全得到保证。注册过程如图 5 所示。

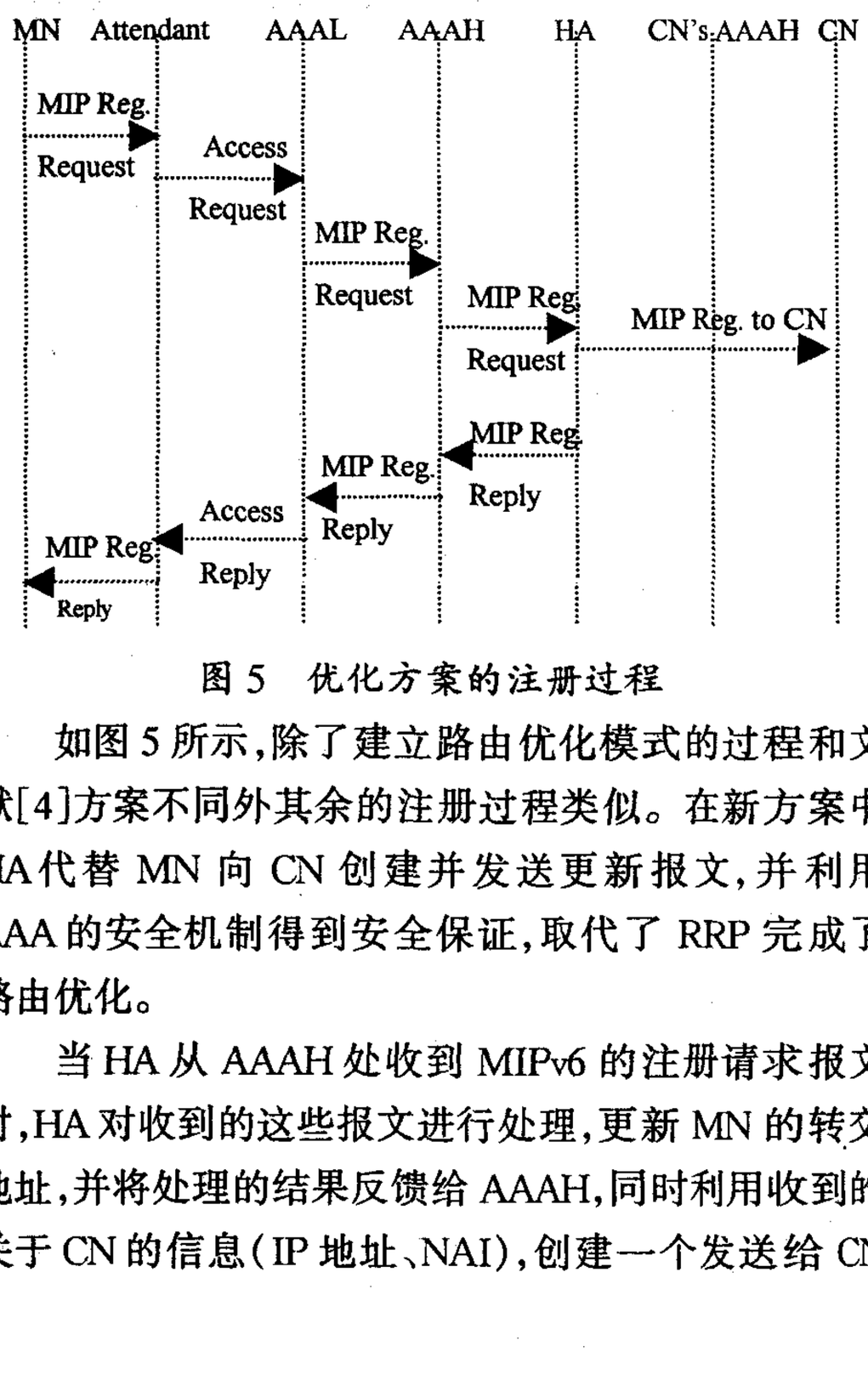

图 5 优化方案的注册过程

如图 5 所示,除了建立路由优化模式的过程和文献[4]方案不同外其余的注册过程类似。在新方案中 HA 代替 MN 向 CN 创建并发送更新报文,并利用 AAA 的安全机制得到安全保证,取代了 RRP 完成了路由优化。

当 HA 从 AAAH 处收到 MIPv6 的注册请求报文时,HA 对收到的这些报文进行处理,更新 MN 的转交地址,并将处理的结果反馈给 AAAH,同时利用收到的关于 CN 的信息(IP 地址、NAI),创建一个发送给 CN

的更新报文(BU)。在更新报文中,将 MN 的转交地址作为源 IP 地址,将 CN 的地址作为目的 IP 地址,MN 的家乡地址填写在家乡地址选项中,发送给 CN,使之更新 MN 的位置为直接和 MN 通信做好准备。这样一个路由优化模式完成了,MN 和 CN 可以进行直接通信了。

4.3 优化方案的信令和时延分析

在文献[4]的方案中,MN 发送绑定更新(BU)来更新 CN 的绑定缓存表项(Binding Cache Entry)执行路由优化模式,总共需要 6 条信令。MN 与 CN 直接进行交换的信令 CoTI&CoT,通过 MN 的 HA 与 CN 交换的信令 HoTI&HoT。如果这 4 条信令成功交换后,MN 再发送绑定更新 BU 至 CN 更新绑定缓存表项,成功后 CN 发送绑定确认(BA)给 MN 对 BU 进行确认。其中 HoTI 和 CoTI 信令同时发送,响应信令 HoT 和 CoT 也几乎同时返回。这 4 条信令就是迂回路由过程(RRP),交换信令的通信过程需要 1 个往返时延。CN 的绑定更新过程交换的信令 BU 和 BA 需要 1 个往返时延。这样在路由优化模式中就需要 2 个 MN 到 CN 的往返时延,这对于一些对时延敏感的多媒体实时应用有着严重的影响。

另一方面,路由优化模式要求 MN 和 CN 计算一个共享的密钥(Kbm),而每计算一次需要交换 4 个信令信息(*CoTI*、*CoT*、*HoTI*、*HoT*)。如果在信令交换的通信过程中 4 个信令信息丢失任意一个,MN 则需要和 CN 交换 2 个以上的信令信息,进一步增加了信令开销和通信时延。

由以上分析可以看出迂回路由过程使用了过多的信令,这些信令的交互带来至少 2 个 MN 到 CN 的往返时延,而在实际的应用中,MN 和 CN 之间的距离一般都比较远,所以信令交互带来的通信时延难以满足实际的应用,特别是对一些多媒体实时业务(VoIP,视频等)。由于文献[4]在路由优化模式中采用了迂回路由过程,切换性能难有突破性的进展,整体效果仍然不是很理想。

优化方案利用 AAA 机制取代了迂回路由过程,降低了信令开销和交互这些信令的通信时延,切换性能有了显著提高。

5 总　结

在下一代以移动为特征的互联网环境中,AAA 如何与移动 IPv6 合理部署以及 AAA 协议和移动 IPv6 协议的融合是解决移动节点跨域移动问题的关键,也是研究的难点。文中讨论了三种融合的方案,并在信令开销和切换时延方面进行了分析比较,并详细描述了 AAA 认证和 MIPv6 注册融合时信令交互的过程。

从信令开销和切换时延上看,新的优化融合方案更符合要求。下一步的研究工作将集中在完善优化方案中的报文的格式,并将该方案应用到 FMIPv6 或者 HMIPv6 中,进一步加强移动 IPv6 的性能。

参考文献:

[1] Johnson D, Perkins C, Arkko J. Mobility Support in IPv6. RFC 3775[S]. IETF, 2004.

[2] Guy C. 移动 IPv6 介绍[EB/OL]. 2004 - 09 - 01. http://www. microsoft. com/china/technet/community/ columns/cableguy/cg0904. mspx.

[3] DuPont F, Laurent - Maknavicius M, Bournelle J. AAA for Mobile IPv6. Draft draft - dupont - mipv6 - aaa - 01. txt [S]. IETF,2002.

[4] Wang R C, Chen R Y, Chao Han - Chieh. AAA architecture For Mobile IPv6 based on WLAN[J]. Int. J. Network Mgmt, 2004,14(5):305 - 313.

[5] Le F, Patil B, Perkins C, et al. Diameter Mobile IPv6 Application. Draft draft - le - AAA - diameter - mobileipv6 - 04. txt[S]. IETF,2005.

[6] Ryn S, Mun Y. An Enhanced Mobile IPv6 Handover for Roaming between Administrative Domains Based on AAA. Draft - mun - mipshop - emipv6 - aaa - 00. txt[S]. IETF, 2006.

(上接第 21 页)

ence on Web Intelligence (WI'03). Washington D. C.: IEEE Computer Society, 2003:68 - 74.

[3] Deshpande M, Karypis G. Item - Based Top - N Recommendation Algorithms[J]. ACM Transactions on Information Systems, 2004,22(1):143 - 177.

[4] 熊　馨,王卫平,叶跃祥. 基于概念分层的个性化推荐算法[J]. 计算机应用,2005,25(5):1006 - 1008.

[5] Kim Dong - Ho, Im I, Atluri V. A Clickstream - based Collaborative Filtering Recommendation Model for E - Commerce [C]//Proceedings of the Seventh IEEE International Conference on E - Commerce Technology (CEC'05). Washington D. C.: IEEE Computer Society, 2005:84 - 91.

[6] Sarwar B, Karypis G, Konstan J, et al. Item - based collaborative filtering recommendation algorithms[C]//Proceedings of the 10th International Conference on World Wide Web. New York: ACM Press, 2001:285 - 295.

[7] Shardanand U, Maes P. Social information filtering: algorithms for automating "word of mouth"[C]//Proceedings of the SIGCHI conference on Human factors in computing systems. New York: ACM Press/Addison - Wesley Publishing Co., 1995:210 - 217.