计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
44(1):51~57, 2007

移动 IPv6 网络层次化接入认证方法

张瀚文[1,2] 张玉军[1] 田 野[1,2] 肖文曙[1,2] 李忠诚[1]
[1](中国科学院计算技术研究所 北京 100080)
[2](中国科学院研究生院 北京 100049)
(hwzhang@ict.ac.cn)

Hierarchical Access Authentication Method in Mobile IPv6 Networks

Zhang Hanwen[1,2], Zhang Yujun[1], Tian Ye[1,2], Xiao Wenshu[1,2], and Li Zhongcheng[1]
[1](*Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100080)
[2](*Graduate University of Chinese Academy of Sciences, Beijing* 100049)

Abstract Access authentication is very important for mobile IPv6 networks. In this paper, hierarchical access authentication method in mobile IPv6 (HAMIPv6) is proposed. The method can accomplish access authentication and mobile registration while reducing exchanges between mobile node and home domain by utilizing authentication vector and message piggyback. The method simplifies handoff authentication process by reducing handoff delay and cost. Also the method supports mutual authentication between terminal and network. Performance evaluation shows that the proposed method is better than the others, especially in the conditions that MN is far from home domain and move frequently within a domain.

Key words MIPv6; access authentication; hierarchical MIPv6; AAA

摘 要 对接入用户实施认证是移动 IPv6 实用化的前提.提出一种适用于移动 IPv6 网络环境的层次化接入认证方法 HAMIPv6,对接入认证和移动注册进行层次化管理,利用认证矢量和消息捎带,减少切换认证过程中移动节点与家乡域的交互. HAMIPv6 简化了切换认证处理流程,减小了切换延时和信令开销,实现了用户与网络相互认证及会话密钥发放.通过分析比较证明,HAMIPv6 比传统方法处理效率更高,尤其是在 MN 远离家乡域及在一定范围内频繁微移动的情况下.

关键词 移动 IPv6;接入认证;层次化移动 IPv6;AAA

中图法分类号 TP393.08

基于移动 IP 技术的移动互联网是未来网络的发展方向,其开放特性增大了潜在的安全威胁,必须对接入用户进行认证.移动 IPv6 协议作为一个网络层的路由协议[1],只解决了节点在移动过程中如何保持连接的问题,并不提供对网络的接入控制及数据传输的安全性保障,这限制了其大规模的商业部署. AAA(authentication, authorization and accounting)技术(如 Diameter 协议[2])正是为了解决接入控制等问题而提出的,IETF 的 MIP4,MIP6,AAA 等工作组正致力制定移动 IP 协议和 AAA 协议的有效结合方案[3-4],但安全性和实时性的矛盾难以解决.

本文提出了一种适用于移动 IPv6 网络环境的层次化接入认证方法,在保证切换效率和接入安全的基础上,实现用户与网络间的双向认证及会话密钥发放.

1 现有方案分析

针对移动环境下的接入认证,国内外已有的方案主要包括以下几类:①基于消息捎带的策略[4-5],在认证消息中捎带移动注册消息以减小处理延时,但这些策略只是将移动处理简单挪动到认证过程

收稿日期:2005-08-19;修回日期:2006-10-08
基金项目:国家自然科学基金项目(90604014)

中,实际的移动注册仍是在认证成功后进行;②基于二层(数据链路层)"暗示"的策略[6-7],利用二层触发信号,在 MN 移动到新子网前就开始认证和预切换处理,将认证与快速切换进行结合,但由于没有考虑到移动注册过程,对移动认证切换整个过程的优化效果并不明显;③基于移动 IP 增强协议的策略[6-8],将接入认证与移动 IP 的增强方案结合以提高认证切换性能,但没有明确具体的认证方法;④基于特定认证方法的策略[9],结合 AAA 和更适合无线环境的认证方法(如 USIM 认证机制[10]). 上述策略都是从某一个角度去研究快速的接入认证,并未有效地将接入认证和移动切换过程进行有效融合,最大程度地提升整体切换性能. 同时,对用户与网络的相互认证及会话密钥的发放等问题也缺少考虑.

IETF 提出的基于移动 IPv6 的 AAA 接入认证机制 DAMIPv6[4]通过将切换处理过程中的绑定更新/确认消息携带在 AAA 认证消息中,减小 MN 与家乡域的交互次数,以提高移动性能(见图 1). 该机制考虑了认证和切换的融合,但只是将切换处理简单挪动到认证处理过程中,实际的绑定更新仍是在认证成功后进行. 考虑到具体认证方法时,即使采用最简单的 EAP-MD5 单向认证方法,完成整个认证过程也至少还需要在图 1 所示的流程中增加一轮 MN 与 AAAh 间的交互,若需要实现双向认证,则需要增加更多轮的交互次数,极大降低 MN 的移动切换效率.

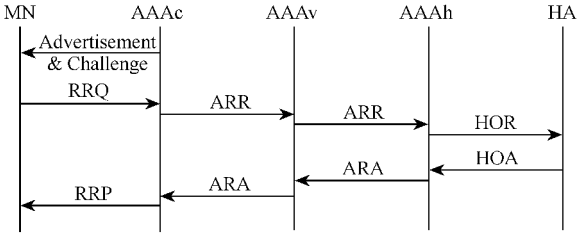

Fig. 1 DAMIPv6 protocol.

图 1 DAMIPv6 认证流程

2 移动 IPv6 网络层次化接入认证方法

层次化管理思想已被引入到移动管理的位置登记中[11],以减小用户微移动时频繁注册带来的延时和开销. 本文将层次化管理思想用于认证,基于层次化移动 IPv6(HMIPv6)[11]实现移动和认证的层次化管理. 将 HMIPv6 中引入的实体移动锚点(mobility anchor point, MAP)也作为认证锚点,即 MAP-AAAc,通过 MN 在 MAP-AAAc 域内移动时认证和注册的本地化,避免 MN 与其家乡域不必要的交互,减小延时和开销,提高认证切换性能.

2.1 层次化认证框架

移动 IPv6 层次化接入认证机制(HAMIPv6)系统框架基于 HMIPv6 设计,将 HMIPv6 中的 MAP 扩展为 MAP-AAAc,同时作为移动锚点和认证锚点(见图 2). 一个管理域中至少有一个认证服务器、一个或多个 MAP-AAAc 域. 当 MN 漫游到一个新的 MAP-AAAc 域时,通过路由器宣告配置新的链路转交地址(LCoA)和区域转交地址(RCoA),分别向 MAP-AAAc 和 HA 进行转交地址注册,同时进行用户和网络间的相互认证及会话密钥的发放;当 MN 在 MAP-AAAc 域内不同 AR 间移动时,作为移动锚点,MAP-AAAc 使得 MN 只需向其注册新的 LCoA,无需与 HA 进行交互;作为认证锚点,MAP-AAAc 代替家乡域认证服务器实现 MN 与网络间的相互认证及会话密钥发放,避免 MN 与其家乡域的交互. MAP-AAAc 实现了认证和移动注册的本地化,当 MN 在远离家乡域或在一定范围内频繁微移动时,这样的层次化管理策略能明显减少认证切换延时及信令开销,提高移动性能.

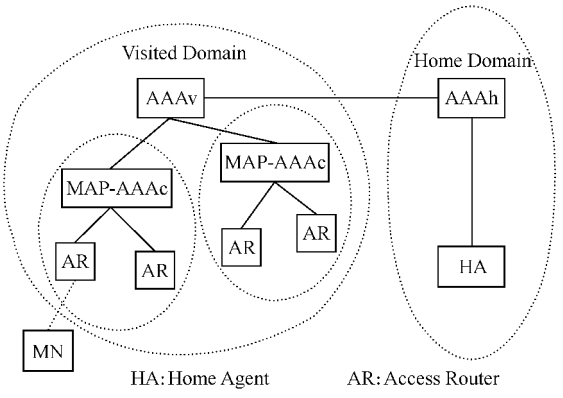

Fig. 2 Framework of HAMIPv6.

图 2 HAMIPv6 系统框架

2.2 基于认证矢量的双向认证方法

HAMIPv6 机制利用认证矢量 AV 实现认证的层次化管理、实现用户和网络的双向认证及会话密钥的发放. 不同于 DAMIPv6,HAMIPv6 实现用户与网络间双向认证所需的认证方法,无需依赖于全局的 PKI 构架及证书管理,更适合于无线移动网络.

认证矢量 AV[10]是用于一次认证的五元组，包括随机数（random number，RAND）、预期应答（expected response，XRES）、加密密钥（cipher key，CK）、完整性密钥（integrity key，IK）和认证令牌（authentication token，AUTH）. 图 3 简要说明如何利用 AV 实现认证和密钥发放：

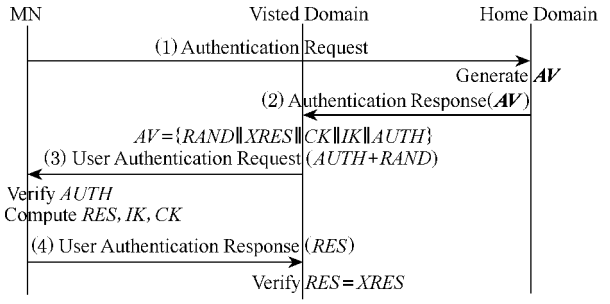

Fig. 3 Authentication mechanism using AV.

图 3 利用 AV 实现双向认证和密钥发放

本文结合 AAA 认证机制和图 3 所示的具体认证方法实现认证的层次化管理. MN 要求接入网络时，由 AAAh 根据用户相关信息生成一组认证矢量 AVs 发送给当前访问域的 MAP-AAAc，由 MAP-AAAc 代替 AAAh 实现对 MN 的认证；MN 在该 MAP-AAAc 域内的不同 AR 间移动时，直接由 MAP-AAAc 利用其保存的 AVs 中的一个 AV 完成认证及密钥发放.

2.3 融合认证的切换流程

图 4 为移动 IPv6 层次化接入认证机制的具体处理流程：

当 MN 进入一个新的 MAP-AAAc 域时，认证切换处理包括以下几个步骤：

1）根据路由器宣告，配置新 LCoA 和 RCoA；

2）AAAh 利用根据 NAI 查找到的用户信息生成一组认证矢量 AVs，同时将 BU_{HA} 消息转发给 HA. HA 对新 RCoA 进行绑定更新；

3）AAAh 将 AVs 和 BA_{HA} 应答给 MAP-AAAc；MAP-AAAc 存储这组 AVs；

4）MAP-AAAc 取出一个 AV，将其 RAND 和 AUTH 发送给 MN，替代 AAAh 进行认证；

5）MN 利用 AUTH 对网络认证成功后，根据 RAND 和它与 AAAh 共享的 SA 计算出 RES 发送给 MAP-AAAc，同时计算出 CK 和 IK（实现后续通信数据传输安全保障的会话密钥）；

6）MAP-AAAc 比较 AV 中的 XRES 和从 MN 收到的 RES. 如相同则 MN 通过认证，向其应答认证成功消息，并捎带 LCoA 和 RCoA 的绑定确认消息 如不同，则 MN 认证失败，向其应答认证失败消息.

这样完成了一次认证和移动注册，同时实现了 CK 和 IK 在 MAP-AAAc 和 MN 的发放.

当 MN 在 MAP-AAAc 域内的不同 AR 间移动时，MAP-AAAc 实现认证和注册本地化，无需与家乡域进行交互，具体步骤如下：

1）MN 首先获得一新的 LCoA；

2）MN 向 MAP-AAAc 发送注册请求消息；

3）MAP-AAAc 执行移动锚点功能，对 MN 的新 LCoA 进行绑定更新；

4）MAP-AAAc 执行认证锚点功能，取出保存的 AVs 中的一个，完成认证及会话密钥发放.

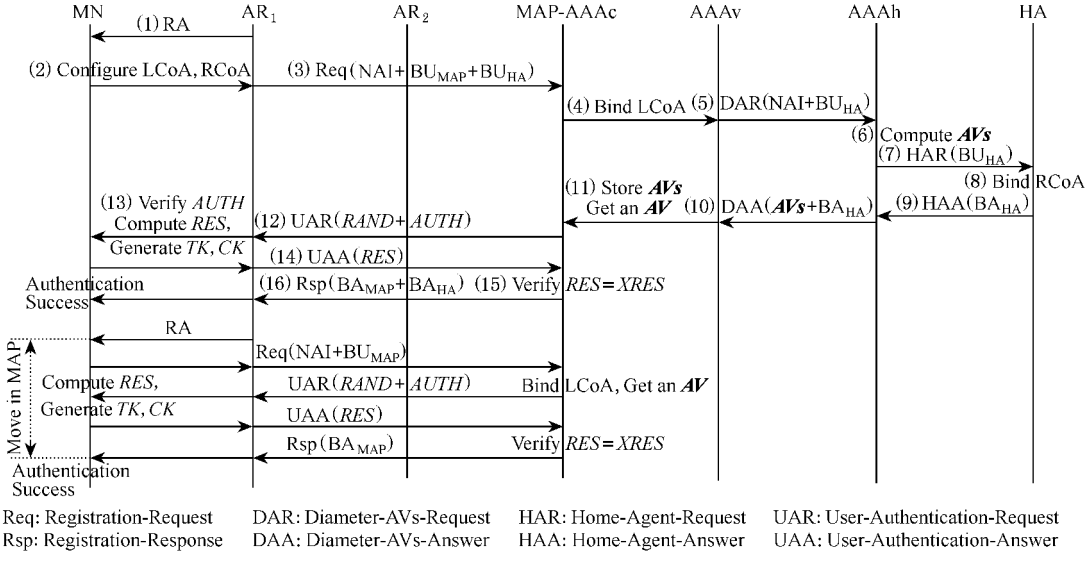

Fig. 4 HAMIPv6 mechanism.

图 4 HAMIPv6 认证机制

3 性能分析

处理延时和信令开销是评价认证和切换融合机制效率的两个重要指标,本节从这两个方面对HAMIPv6机制的性能进行评价,并与DAMIPv6进行分析比较. 表1为性能指标分析中所用到的各参数说明:

Table 1 Parameters

表1 参数说明

Parameter	Explanation
T_{HAMIPv6}	authentication & handoff delay
T_{DAMIPv6}	
P_{total}	handoff processing time
W_{total}	message transfer delay in wireless/wired link
L_{total}	
AU_{total}	authentication processing time
M^w/M^L	message transfer delay in wireless/ wired link of one message
C_h	hops between AAAv and AAAh
$E[N]$	MN average movement times within a MAP-AAAc domain
λ	MN authentication request arrival rate
MC_{HAMIPv6}	signaling overhead
MC_{DAMIPv6}	

3.1 认证切换延时分析

认证切换延时的定义是从MN移动到一个新子网开始到认证、移动注册处理完成的时间间隔,即 $T = P_{\text{total}} + W_{\text{total}} + L_{\text{total}} + AU_{\text{total}}$.

一条消息的发送时间包括发出时间、传输时间和处理时间,即 $M = \alpha + \beta + \gamma$. 其中 $\alpha = b/B$,b 为控制信令的长度,B 为链路带宽(B^L,B^W 分别针对有线、无线链路).

考虑无线链路的失效重传,令 t_w 为检测分组丢失的检测时间,消息发出 t_w 后未收到ACK重传. 令 $Prob(N_f)$为经过 N_f 次失败后发送成功的概率,则在无线链路的发送时间为 $W_i = M^w + (t_w + M^w)\sum_{N_f=0}^{\infty}(N_f \times Prob(N_f))$. $q \in (0,1)$为无线链路失败率,则 $\sum_{N_f=0}^{\infty}(N_f \times Prob(N_f)) = \sum_{N_f=0}^{\infty}(N_f \times q^{N_f}(1-q)) = \frac{q}{1-q}$. 通常 q 取值为0.5[12],因此 $w_i = 2M^w + t_w$. 有线链路不需考虑重传,则有发送时间为 $L_i = M^L$.

由图4计算认证切换延时,设各节点的移动处理及消息生成时间为 P,RES和XRES计算时间都为 AU,则MN进入一个新的MAP-AAAc域后其切换延时为

$$T_{\text{HAMIPv6-inter}} = 12P + 5(2M^w + t_w) + (8M^L + 2M^L \times C_h) + 2AU. \quad (1)$$

MN在MAP-AAAc域内移动的认证切换延时为

$$T_{\text{HAMIPv6-intra}} = 7P + 5(2M^w + t_w) + 4M^L + AU. \quad (2)$$

HAMIPv6中MN的平均认证切换延时为

$$T_{\text{HAMIPv6}} = \frac{1}{1+E[N]}T_{\text{HAMIPv6-inter}} + \frac{E[N]}{1+E[N]}T_{\text{HAMIPv6-intra}}. \quad (3)$$

基于图1,考虑最简单的EAP-MD5认证方法,需添加MN到AAAh间的一轮交互,可得DAMIPv6机制的认证切换延时为

$$T_{\text{DAMIPv6}} = 8P + 5(2M^w + t_w) + 6M^L + 4M^L \times C_h + 2AU. \quad (4)$$

图5、图6分别给出了随着AAAv和AAAh间跳数 C_h 变化及随着MN在一MAP-AAAc域内平均移动次数 $E[N]$变化时,HAMIPv6和DAMIPv6认证切换延时的变化情况. 各性能参数取值见表2[12-15]所示:

Table 2 Performance Parameters

表2 性能参数

Parameter	Value
b(B)	50
B^L(Mbps)	155
B^w(Mbps)	144
β^L(ms)	0.5
β^w(ms)	2
γ(ms)	0.5
t_w(ms)	2
P(ms)	0.5
AU(ms)	6

在图5中,只考虑MN在外地网络的情况(C_h从1开始取值). HAMIPv6比DAMIPv6具有更高切换性能,且随 C_h 的增大,DAMIPv6认证延时的增幅明显大于HAMIPv6. 因此,当MN所处的访问域离家乡域越远,HAMIPv6更能显著地降低移动IPv6网络的认证切换延时.

图6在 C_h 为1的情况下,$E[N]$对切换延时的影响. DAMIPv6每次移动后,都由家乡域的AAAh实现对MN的认证,切换延时均值为定值. HAMIPv6中,随着 $E[N]$增大,切换延时递减,即MN在一定范围内微移动越频繁(这符合大多数移动用户的运动模式——教授运动模式),HAMIPv6的认证切换性能越高.

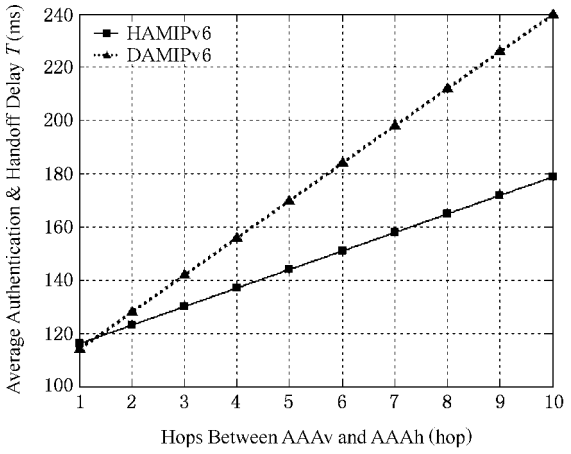

Fig. 5 Average authentication & handoff delay.

图 5 MN 的平均认证切换延时($E[N]=0$)

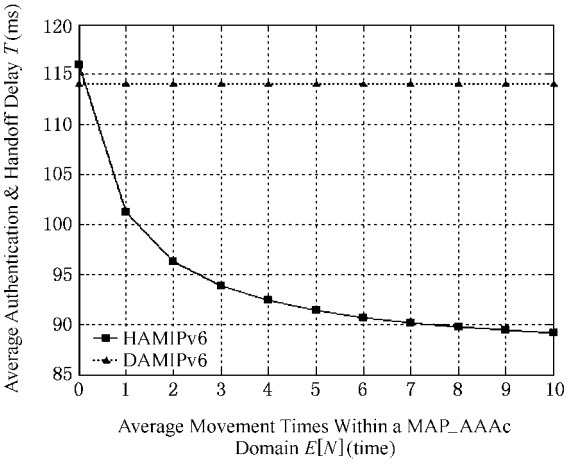

Fig. 6 Average authentication & handoff delay.

图 6 MN 的平均认证切换延时($C_h=1$)

3.2 单位时间系统信令总开销分析

对于信令开销的分析,本文假设单位时间内请求接入网络的 MN(包括初始接入网络引起的请求和移动切换引起的请求)的到达率为 λ. MN 初始接入网络/MAP-AAAc 域间移动和 MAP-AAAc 域内移动引起的接入请求到达率分别为 $\lambda\times\frac{1}{E[N]+1}$, $\lambda\times\frac{E[N]}{E[N]+1}$. 根据图 4 可得单位时间内系统信令总开销为

$$MC_{\text{HAMIPv6}}=\lambda\times\frac{1}{E[N]+1}\times(12+2C_h)+\lambda\times\frac{E[N]}{E[N]+1}\times 8=\frac{2\lambda}{E[N]+1}\times(6+C_h+4E[N]). \tag{5}$$

DAMIPv6 单位时间内系统信令总开销为

$$MC_{\text{DAMIPv6}}=\lambda\times(10+4C_h). \tag{6}$$

DAMIPv6 与 HAMIPv6 单位时间内系统信令总开销差值为

$$\Delta MC=MC_{\text{DAMIPv6}}-MC_{\text{HAMIPv6}}. \tag{7}$$

图 7 给出了随着变化,DAMIPv6 与 HAMIPv6 单位时间内系统信令总开销差值的变化情况. 当 $C_h>1$,DAMIPv6 的系统信令开销总大于 HAMIPv6,且随 C_h 增长 DAMIPv6 信令开销的增幅比 HAMIPv6 更大. 随着 λ 取值的增大,ΔMC 的斜率更大,即 DAMIPv6 信令总开销的增幅比 HAMIPv6 更大. 因此,当 MN 所处的访问域距家乡域越远,或单位时间内请求接入的 MN 数量越多,HAMIPv6 机制的系统信令总开销更为明显地低于 DAMIPv6.

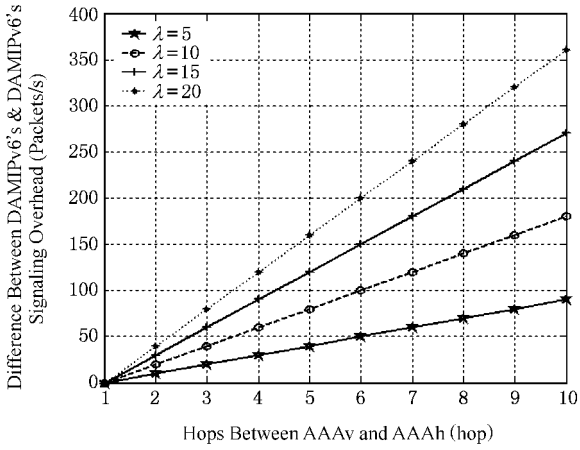

Fig. 7 Difference between DAMIPv6 's and DAMIPv6 's signaling overhead.

图 7 DAMIPv6 与 HAMIPv6 单位时间系统信令总开销之差($E[N]=0$)

图 8 在 $C_h=1$ 的情况下,$E[N]$ 对 ΔMC 的影响. 由图 7 可知,当在一定范围内微移动越频繁,或

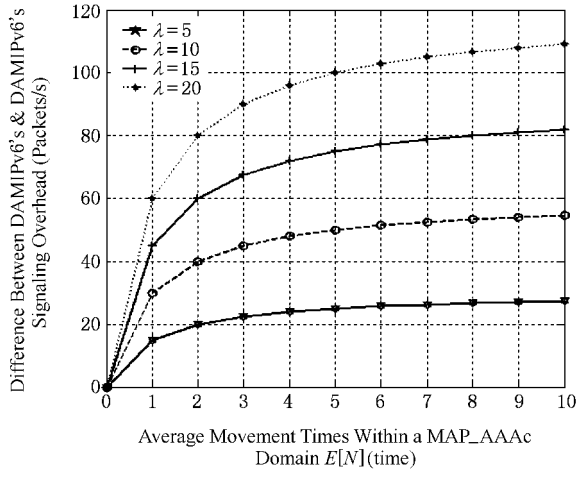

Fig. 8 Difference between DAMIPv6 's and DAMIPv6 's signaling overhead.

图 8 DAMIPv6 与 HAMIPv6 单位时间系统信令总开销之差($C_h=1$)

单位时间内请求接入的 MN 数量越多,HAMIPv6 机制的系统信令总开销更为明显地低于 DAMIPv6. 在大多数移动用户所遵循的教授运动模式下,从系统信令总开销看来,HAMIPv6 机制比 DAMIPv6 更优.

4 结束语

本文提出了一种高效的移动 IPv6 层次化接入认证方法 HAMIPv6,降低了认证切换延时和带宽开销. HAMIPv6 可在没有 PKI 支持的前提下实现用户和网络的双向认证及会话密钥的发放. 通过性能分析证明本方法在认证切换延时及系统信令开销方面都表现出比传统方法更高的性能. 目前,HAMIPv6 机制还未对 MN 在 MAP-AAAc 域间及管理域间移动时的情况进行优化. 可以考虑采用二层触发预测切换,通过预切换和认证减少延时及丢包率;同时,采用上下文转移机制,在不同域的 MAP-AAAc 间传递认证状态信息,减少域间移动情况下 MN 与 AAAh 的交互次数以提高认证移动性能,这些将是我们下一步工作中的研究重点.

参 考 文 献

[1] C E Perkins, D B Johnson. Mobility support in IPv6 [S]. IETF RFC 3775, 2004

[2] P Calhoun, J Loughney, *et al*. Diameter base protocol [S]. IETF RFC 3588, 2003

[3] P Calhoun, T Johansson, *et al*. Diameter mobile IPv4 application [S]. IETF RFC 4004, 2005

[4] F Le, S Faccin. Diameter mobile IPv6 application [OL]. http://www.tools.ietf.org/htul/dreft-le-aaa-diameter_mobileipv6-04

[5] S Yoo, D Choi, *et al*. Seungwon Son. Authentication mechanism of mobile IPv6 over wireless LAN in diameter [C]. The 8th Int'l Conf on Cellular and Intelligent Communications-Formerly CDMA (CIC 2003), Seoul, 2003

[6] C Kim, Y S Kim, *et al*. Performance improvement in mobile IPv6 using AAA and fast handoff [C]. Int'l Conf on Computational Science and It's Applications (ICCSA '04), Assisi, Italy, 2004

[7] Y Choi, H Choo, B L Lee. Secure handoff based on dual session keys in mobile IP with AAA [C]. Int'l Conf on Computational Science and It's Applications(ICCSA '04), Assisi, Italy, 2004

[8] P Engelstad, T Haslestad, F Paint. Authenticated access for IPv6 supported mobility [C]. The 8th IEEE Int'l Symp on Computers and Communication(ISCC '03), Antalya, Turkey, 2003

[9] H Kim, H Afifi. Improving mobile authentication with new AAA protocols [C]. IEEE Int'l Conf on Communications (ICC '03), Anchorage Alaska, USA, 2003

[10] 3GPP. 3GPP ts 33.102 3g security; security architecture. 3rd Generation Partnership Project [R]. Tech Rep: v3.11.0, 2002

[11] H Soliman, C Castelluccia, *et al*. Hierarchical mobile IPv6 mobility management (HMIPv6) [S]. IETF RFC 4140, 2005

[12] J McNair, I F Akyildiz. An inter-system handoff technique for the IMT-2000 system [C]. IEEE INFOCOM 2000, Tel Aviv, Israel, 2000

[13] A Hess, G Schafer. Performance evaluation of AAA/mobile IP authentication [C]. 2nd Polish-German Teletraffic, Gdansk, Poland, 2002

[14] J McNair, I F Akylidiz. Handoff for real-time traffic in mobile IP version 6 networks [C]. IEEE GLOBECOM '01, San Antonio, Texas, USA, 2001

[15] J Xie, I Akylidiz. An optima location management scheme for minimizing signaling cost in mobile IP [C]. IEEE Int'l Conf on Communications(ICC '02), New York, USA, 2002

Zhang Hanwen, born in 1981. Received her B. S. degree in the University of Electronic Science and Technology of China, Sichuan, China. Now she is a Ph. D. candidate in the Institute of Computing Technology, the Chinese Academy of Sciences, Beijing, China. Her main research interests include wireless and mobile networks, dependable and secure computing.

张瀚文,1981 年生,博士研究生,主要研究方向为无线移动网络、可信计算.

Zhang Yujun, born in 1976. Associate professor of the Institute of Institute of Computing Technology, the Chinese Academy of Sciences. Serior member of China Computer Federation. His main research interests include next generation network and mobile computing.

张玉军,1976 年生,副研究员,中国计算机学会高级会员,主要研究方向为下一代网络、移动计算.

Tian Ye, born in 1979. Received his Ph. D. degree in the Institute of Computing Technology, the Chinese Academy of Sciences, Beijing, China. His main research interests include security in next generation network.

田 野,1979 年生,博士,主要研究方向为下一代网络安全.

Xiao Wenshu, born in 1980. Ph. D. candidate in the Institute of Computing Technology, the Chinese Academy of Sciences, Beijing, China. Her main research interests include next generation network and security in wireless network.

肖文曙,1980 年生,博士研究生,主要研究方向为下一代互联网、无线移动网络安全.

Li Zhongcheng, born in 1962. Professor and Ph. D. supervisor of the Institute of Computing Technology, the Chinese Academy of Sciences. Serior member of China Computer Federation. His main research interests include computer network and fault-tolerant computing.

李忠诚,1962 年生,研究员,博士生导师,中国计算机学会高级会员,主要研究方向为计算机网络、容错计算.

Research Background

Access control is essential for mobile IPv6 networks. However, deploying access control mechanism in mobile IPv6 will absolutely degrade the handoff performance. It is necessary to study an effective authentication method for wireless mobile IPv6 network. HAMIPv6 (hierarchical access authentication in MIPv6) is such a method. It simplifies handoff authentication process by reducing handoff delay and cost. Also the method supports mutual authentication between terminal and network. Our work is supported by the National Natural Science Foundation of China (90604014) which is focus on the study of access control mechanism for mobile network.