基于层次化管理的移动IPv6网络接入认证研究

马同杰[1],陈蜀宇[2],陈孝文[1]
(1.重庆大学 计算机学院,重庆 400030;2.重庆大学 软件工程学院,重庆 400030)

摘 要:移动IPv6网络为用户随时随地接入网络提供了可能性,也给用户的接入控制和管理提出新的挑战。为改善此情况,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,利用层次化思想对接入认证和移动注册进行层次化管理,减少了切换认证处理流程;基于矢量的双向认证机制实现了用户和移动网络的双向认证;当移动节点远离家乡域及在一定范围内频繁移动时,将层次化移动切换过程和认证过程进行了有机整合,减少了延迟和开销,提高了认证切换性能。

关键词:移动IPv6网络;接入认证;层次化管理;AAA认证;快速切换
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2009)10-0022-04

Study on Mobile IPv6 Network Access Authentication Strategy Based on Hierarchical Management

MA Tong-jie[1],CHEN Shu-yu[2],CHEN Xiao-wen[1]
(1.Department of Computer,Chongqing University,Chongqing 400030,China;
2.Department of Software,Chongqing University,Chongqing 400030,China)

Abstract:The IPv6 mobile network provides the possibility for users to access network anytime, and also puts forward a new challenge on accessing control and management. In order to improve this situation,proposes a mobile network environment in the hierarchical IPv6 access authentication methods, using hierarchical thought to access authentication and mobile registered for hierarchical management, reduce the switching certification process. Based on vector two-way authentication mechanism achieved users and mobile network two-way certification. When moving away from your hometown node in a certain range domain and frequent mobile, mobile switching and hierarchical authentication process integration, reduce the cost, improve the delay and authentication switching performance.

Key words:IPv6 mobile network;access authentication;hierarchical management;AAA certificate;fast switching

0 引 言

移动IPv6(Mobile IPv6,MIPv6)网络为用户随时随地接入网络提供了可能性,也给用户的接入控制和管理提出了新的挑战。在开放的移动IPv6网络中,用户的位置不确定,用户的行为难以预测,各管理域往往隶属于不同的管理机构,从保障网络安全可靠运营的角度看,各个域之间必须协作实现对移动节点的接入控制。

互联网是一个开放的网络环境,允许各种类型的用户和设备接入网络,如果不对其进行有效的控制和管理,将使得的互联网暴露于各种安全风险中[1],而接入控制可以很好地解决这一问题。网络接入控制能够对接入网络的用户的身份进行验证,能够对用户的行为进行限制,能够对产生不良后果的行为进行追踪审计。网络接入控制[2]是指基于网络策略对用户接入网络进行控制的能力。用户身份识别和验证是一种重要的判断是否允许接入的网络策略。在移动IPv6网络中,用户需要在任意位置接入网络,这些网络可能属于不同的运营商,每一个运营商必须对通过自己的管理域接入网络的移动节点实施接入认证。在移动IPv6网络中用户可以从非家乡域接入网络,需要在各个管理域之间建立信任关系,通过域之间的协作实现对用户的跨域信任控制。从用户的角度看,用户希望看到的是一个普遍存在的网络服务,只需要通过一个统一的接口获取网络服务。

基于现行技术在移动IPv6网络中实现接入认证存在问题:首先,实现移动切换和接入认证分别有各自的基础设施,增加了硬件成本和管理成本;其次,移动IP信令和接入认证信令并存,增加了网络复杂度和网

收稿日期:2009-02-28;**修回日期**:2009-05-21
基金项目:科技部科技型中小企业技术创新基金(05C26215111378)
作者简介:马同杰(1983-),男,山东潍坊人,硕士研究生,研究方向为网络与移动计算机及嵌入式系统;陈蜀宇,教授,博士生导师,研究方向为网络与移动计算机及嵌入式系统。

络管理的难度;另外,移动 IP 技术要求较低的切换延迟,但是认证过程推迟了切换过程,增加了移动过程中通信中断的时间。

文中提出了一种适用于移动 IPv6 环境的层次化接入认证策略,将层次化切换[3]过程和认证过程进行了有机整合,这种基于层次化移动管理协议的接入认证策略,称为层次化接入认证机制(HAMIPv6)。该策略将分层移动 IPv6(HMIPv6[4])中引入的移动锚点(MAP)同时作为认证锚点,标记为 MAP－AAAc,通过移动节点(MN)在 MAP－AAAc 域内移动时认证和注册的本地化,避免了移动节点域其家乡域的不必要交互,提高了认证切换性能,减少了延时和开销[5]。

1　移动 IP 中实施接入认证

移动 IP 技术是移动互联网的基础,接入控制是大规模部署移动互联网的前提,而集成接入控制后的切换性能提升是实施实时应用的关键。AAA 技术能够解决这个问题,解决用户在同一管理域和不同的管理域之间的认证和授权,对保障网络安全和可靠运营起着重要作用,在移动 IP 中引入 AAA 技术有助于解决网络部署中的问题。

AAA 技术是为解决网络部署时的认证、授权等问题而提出的,是网络部署和运营的保障和前提。最初,它应用于拨号服务,以防止网络服务被盗用,提供用户级的接入授权和计费等功能。

认证是指对实体身份或者消息来源的验证,是各种安全服务所依托的最基本的安全服务。网络上的认证行为可以分为身份认证和消息认证。消息认证是对接收到的消息来源和真实性进行认证,主要采用数字签名、消息摘要等密码学方法。身份认证用于网络接入和使用服务等场合,主要采用口令、密码算法、证书等认证协议。移动 IPv6 网络的认证主要关注网络接入时对实体身份的认证,从实质上讲,身份认证是用户利用一个只有自己知道、别人可以验证的秘密来证实自己的身份。要实现一套完整的网络接入认证流程,现有的接入认证体系主要包括认证实现层、认证控制层、接入控制层。

移动 IPv6 技术很好地解决了无缝移动漫游问题,但随之带来的漫游管理以及如何保证用户和网络资源提供商的合法权益等诸多问题,需要 AAA(认证、授权和计费)技术来保证。因此,AAA 技术和 M IPv6 技术的结合势在必行。

基于 AAA 的移动 IP(MIP－AAA)解决了移动 IP 的认证、授权、注册及密钥分发等问题,为移动 IP 的大规模实施提供了安全保障。但当 MIP－AAA 中的节点发生切换时,不仅要执行移动 IP 的注册过程,还要完成 AAA 对用户的认证和授权。因此相对于单纯的移动 IP 协议,MIP－AAA 在切换中存在更大的时延。

目前有的 MIP－AAA 方案将移动 IP 注册消息嵌入在 AAA 消息中,合并认证与注册过程,这在一定程度上减少了切换时延。但是,方案仍然存在很大的弱点,即每次切换都要经过家乡域对用户进行认证和授权,这必然不能很好地解决切换时延问题。因为:

(1) 外地域与家乡域可能距离很远,单边的消息传输就会消耗较长时间。认证过程的时延主要来自于外地域与家乡域间的信息交换。

(2) 当节点切换频繁时,将不断发送认证及注册消息,特别是在移动节点数目较多的情况下,中间网络将因此而承载非常大的负荷。因此,在改进方案中着重解决了这一问题,特别是当移动节点在同一管理域内的不同子网间切换时,认证过程不再经过家乡域,从而缩短了切换时延。

目前,讨论如何将 AAA 与移动 IP 结合的方案比较多,但是,现有方案多为讨论 AAA 与移动 IP 结合的条件和应用模型,涉及具体认证方案的还很少,并且均未解决移动 IP 的快速切换问题。当移动节点发生越区切换时,认证注册过程仍然存在较大的时延,容易丢失数据包。MIP－AAA 提供了一种切换快速、安全级别高、适宜无线移动环境实施的认证注册方案。MIP－AAA 将移动 IP 的认证和注册过程分开,由 AAA 服务器(AAAl 和 AAA H) 完成对用户身份的认证,家乡代理和外地代理不再参与认证过程,只负责注册和更新移动节点的绑定列表,并为 MN 转发移动 IP 消息。若移动节点被成功认证,外地域将根据用户的使用权限为其提供网络服务。若移动节点向家乡域注册成功,它可以收到家乡域为其转发来的数据包。通过减少认证过程中外地域与家乡域交换的消息数量来缩短切换时间,特别是在域内切换情况下,外地域可以直接认证用户身份,不再需要家乡域参与认证过程,极大地提高了切换效率。

2　层次化认证框架

分层移动 IPv6(HMIPv6)网络是对原有移动 IPv6 网络的改进。它与底层的接入技术无关,是一种网络层移动性管理技术。通过将网络划分为不同的区域,使主机的移动分为域间(宏) 移动和域内(微) 移动。移动 IP 协议因用于处理域间(宏) 移动而被称为宏移动协议,其分级扩展协议则用于处理域内(微) 移动,因而称为微移动协议。当移动主机进行微移动时,微

移动协议要求移动主机只需要向域内移动锚点(Mobility Anchor Point,MAP)发送绑定更新消息,不必再向其归属代理发送绑定更新消息,从而缩短了绑定更新时延,改善了网络性能。

层次化接入认证机制[6]系统框架[7]基于 HMIPv6 设计,该系统每个区域中存在一个 AAA 服务器,MAP 即区域移动代理,AR 为接入路由器,AAAs 为 AAA 服务器,AAAl 代表本地 AAA 服务器,AAAh 代表家乡域 AAA 服务器,将 HMIPv6 中的 MAP 扩展为 MAP--AAAc,同时作为移动锚点和认证锚点。一个管理域中至少有一个认证服务器,一个或多个 MAP-AAAc 域,系统框架如图 1 所示。

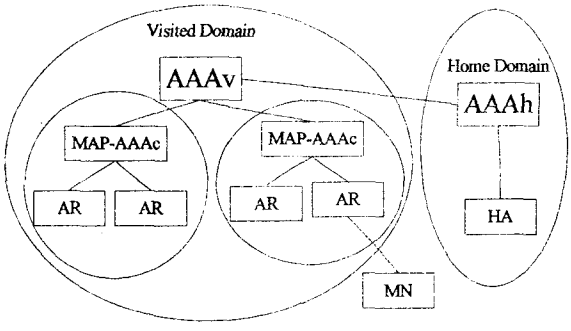


图 1 层次化接入认证机制的系统框架

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 域内不同的 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与会员密钥发放,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移动时,这样的层次化管理策略明显减少认证切换延时及信令开销,提高移动性能[8]。

3 基于认证矢量的双向认证方法

HAMIPv6[9]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。HAMIPv6 实现用户与网络间的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 是用于一次认证的五元组,包括随机数(RAND)、预期应答(XRES)、加密密钥(CK)、完整性密钥(IK)和认证令牌(AUTH)。利用 AV 实现认证和密钥发放的流程如图 2 所示。

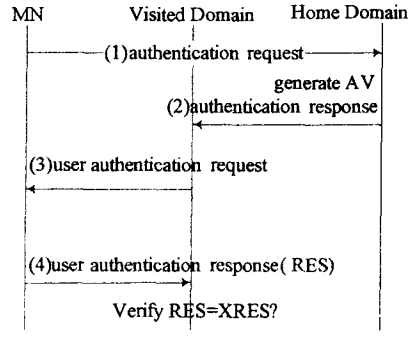
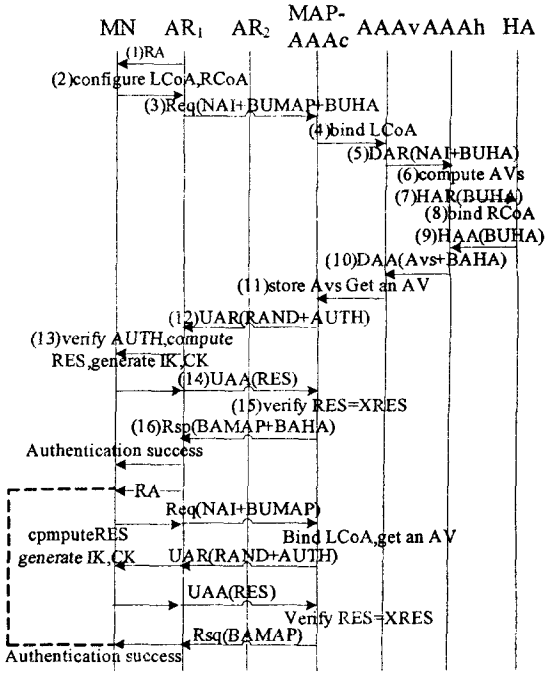


图 2 利用 AV 实现双向认证和密钥发放

HAMIPv6 结合 AAA 认证机制和图 1 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 AAAc 利用其保存的 AVs 中的一个 AV 完成认证及密钥发放。

4 融合认证的切换流程

在移动 IP 网络中,移动切换和接入认证往往同时进行,图 3 简单说明了移动 IPv6 层次化接入认证机制的具体处理流程。



Req: registration-Request Rsp:registration-Response
DAR:diameter-AVs-Request DAA:diameter-Avs-answer
HAR:home-Agent-Request HAA:home-Agent-answer
UAR:User-AuthenticationRequest UAA:User-Authentication-Answer

图 3 HAMIPv6 认证机制处理流程

(1) 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:根据路由器宣告消息,配置新 LCoA 和 RCoA。

(2) AAAh 利用根据网络地址标识符(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,代替 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性保障的会话密钥)。

(6) MAP - AAAc 比较 AV 中的 XRES 和从 MN 收到的 RES。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;不同,则 MN 认证失败,向其应答认证失败消息。

这样就完成了一次认证和移动注册,同时实现了 CK 和 HK 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 发送注册请求信息。

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。

5　结束语

通过分析现有 MIP - AAA 方案在切换时延方面存在的不足,提出一种快速认证注册方案。新方案通过减少认证过程中外地域与家乡域交换的消息数量来缩短切换时间,特别是在域内切换情况下,外地域可以直接认证用户身份,不再需要家乡域参与认证过程,极大地提高了切换效率。新方案为实现 AAA 环境下移动 IP 的快速、安全、扩展性好且低成本的认证注册提供了一种思路。随着社会的不断发展,信息化程度的不断提高,互联网和移动网络的迅猛发展,基于移动 IPv6 的实时应用的不断引入,节点的移动速度不断变快,而如何提高节点切换和接入认证的效率问题是非常有意义的。

文中利用层次化基于身份签名方案的特性,将层次化移动切换过程和认证过程进行了有机整合,减少了访问网络和家乡网络之间的消息交互,减少了延迟和开销,提高了认证切换性能。

参考文献:

[1] 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.

[2] 王　政,陈　萍. 宽带用户接入认证方式浅析[J]. 山东通信技术,2002,22(3):31 - 33.

[3] 林嘉燕,俞鹤伟. 移动 IPv6 切换技术[J]. 计算机技术与发展,2008,18(10):158 - 161.

[4] 陈　蕾,杨　鹏,何剑锋. 基于 HMIPv6 的域间无缝切换方案[J]. 计算机工程与设计,2008,29(15):3885 - 3888.

[5] Gergiades M, Akhtar N. AAA context transfer for seamless and secure multimedia services over All - IP infrastructures [C]//international Conference on Telecommunications(ICT). Polynesia, France: [s. n.], 2003:597 - 603.

[6] 田　野,张玉军,张瀚文,等. 移动 IPv6 基于身份的层次化接入认证机制[J]. 计算机学报,2007,30(6):905 - 915.

[7] Eronen P, Hiller T, Zorn G. Diameter extensible authentication protocol(EAP) application[S]. IETF RFC 4072, 2005.

[8] 田　野,张玉军,刘　莹,移动 IPv6 网络基于身份的快速认证方法[J]. 软件学报,2006,17(9):1980 - 1988.

[9] Soliman H, Castelluccia C , Malki K E, et al. Hierarchical Mobile IPv6 mobility management (HMIPv6)[S]. IETF RFC 4140, 2005.

(上接第 21 页)

[J]. 计算机技术与发展,2008,18(9):177 - 179.

[3] 曹逸峰,陈一民,顾文望. 虚拟机床可视化设计相关技术的研究与应用[J]. 计算机技术与应用进展,2004,16(8):520 - 523.

[4] 张小超,王精业. 虚拟场景漫游系统的体系结构分析[J]. 系统仿真学报,2005,17(4):917 - 919.

[5] Elsadek H, Eleeeb H, Horikoshi J. New technique for investigating three dimensional 3D Mouse[J]. Systems, Man, and Cybernetics, 1998, 5(5):4344 - 4347.

[6] 张向波,邢朝伟. 人机交互中的场景开发[J]. 微机发展(现更名:计算机技术与发展),2003,13(12):98 - 101.

[7] 刘　良,黄路炜. 基于 Open GL Performer 的视景优化研究[J]. 计算机技术与发展,2007,17(8):77 - 80.

[8] 3DxWare SDK 1.0 for Windows 98/ME and Windows NT (4.0/2000/XP32)[M]. [s. l.]: [s. n.], 2000.

[9] Ishii Y, Osaki K, Watanabe T. Evaluation of Embodied Avatar Manipulation Based on Talker's Hand Motion by Using 3D Trackball[C]// The 17th IEEE International Symposium on Robot and Human Interactive Communication. Technische Universität München, Munich, Germany: [s. n.], 2008:653 - 658.