MAS 整体安全机制研究

冯乃勤,王 伟,南书坡
FENG Nai-qin,WANG Wei,NAN Shu-po

河南师范大学 计算机与信息技术学院,河南 新乡 453007
Faculty of Computer & Information Technology,Henan Normal University,Xinxiang,Henan 453007,China
E-mail:pwwei6@126.com

FENG Nai-qin,WANG Wei,NAN Shu-po.Research of MAS overall security mechanism.Computer Engineering and Applications,2009,45(22):73-76.

Abstract: In the open network environment,the security problem has already been an important factor that restricts the applicative problem in mobile agent system.After analyzing the security problems and current status of research work,the paper proposes a security design scheme based on the trusted third party to construct an overall security frame of mobile agent in the Internet.It provides an available method to solve the secure problem in the mobile agent field.

Key words: mobile agent;authentication;security domain

摘 要:在开放网络环境中,安全性问题已经成为移动 Agent 应用的重要因素。通过对 Agent 的安全问题及其研究现状的分析,提出了一种基于可信任第三方的移动 Agent 的整体安全设计方案,为解决移动 Agent 问题提供了一个可行的方法。

关键词:移动 Agent;身份认证;安全域
DOI:10.3778/j.issn.1002-8331.2009.22.025 **文章编号**:1002-8331(2009)22-0073-04 **文献标识码**:A **中图分类号**:TP393

1 引言

安全问题是移动 Agent 在 Internet 上广泛应用的前提,移动 Agent 是一个具有自治性和智能性的软件,它能够在较少或完全没有人为干预的情况下自主地从一台主机迁移到另一台主机,并可以与其他 Agent 或资源进行交互。随着移动 Agent 向电子商务、分布式计算、信息搜索等领域的深入,安全性问题显得日益重要。

现有的比较有代表性的移动 Agent 安全性解决方案有 Genera Magic 公司开发的 TeleScript 系统;Dartmouth 大学开发的 D'agent 系统;Tacoma 大学和 Cornell 大学合作开发的 Tacoma 系统;IBM 公司基于 JAVA 开发的 Agelet;Minnesota 大学开发的 Ajanta;Ara 移动 Agent 平台,ObjectSpace 公司开发的 Voyager;日本三菱公开发的 Conoordia 系统;Tilab 开发的 JADE 平台等[1]。大部分 Agent 安全技术是沿用传统技术发展的,采用的服务器保护方案主要有沙盒模型、签名认证授权和资源分配、Proof-Carrying Code、代码检验等。对执行环境中的移动 Agent 的保护方案有基于检测的安全性措施、主动的保护措施等。对传输中移动 Agent 的保护方案,采用加密技术加以保护,典型的加密算法包括对称加密技术(DES、Triple、IDEA、RC4、RC5 等)和非对称密钥加密技术(RSA、SEEK、PGP 和 EU 等)[2]。

目前大多数 Agent 系统处于教学和研究阶段,它们都强调了功能而忽略了安全,虽然一些系统具有一定的安全技术,但是没有整体规划[3]。实际应用期待能有一个更为全面的机制和更灵活的整体安全框架,应能提供更多可选的机制来满足不断变化的需求。

基于上述因素,从移动 Agent 应用的整体安全机制出发,通过可信第三方认证及可信安全域的方法,提出了一套独立的整体解决方案及安全模型来解决目前移动 Agent 系统中存在的安全问题,基于此整体安全性解决方案和安全模型实现了一个智能 Agent 电子商务仿真系统。

2 移动 Agent 安全性和安全对策分析

在 Internet 开放性网络中的信息传输总是不安全的,当移动 Agent 穿行于网络,它的代码和数据都受到各种安全威胁,类似于传统的分布式系统存在的安全问题。

2.1 移动 Agent 存在的安全问题

移动 Agent 因其程序的自由迁移和应用的灵活性而产生许多安全性问题,主要有以下两方面[1]:

(1)恶意 Agent 对目标主机的威胁;

(2)恶意主机或代理服务器对移动 Agent 的攻击。

2.2 移动 Agent 的安全对策分析

移动 Agent 系统的许多安全问题同时也在传统的客户机/服务器中存在。因此,在分布式应用中所使用的许多传统安全技术,依然可以用于移动 Agent 系统。此外,还有许多对传统安全技术的扩展和专门设计用于移动 Agent 系统安全的技术[4-5]。

解决移动 Agent 的安全性问题主要集中在:移动 Agent 通

基金项目:河南省科技攻关计划(the Key Technologies R&D Program of Henan Province,China under Grant No.0324220161)。

作者简介:冯乃勤(1953-),男,教授,博士,硕士生导师,主要研究方向:神经网络、智能 Web 等;王伟(1975-),男,硕士研究生,主要研究方向:智能 Web、神经网络;南书坡(1980-),男,硕士研究生,主要研究方向:神经网络。

收稿日期:2008-05-05 **修回日期**:2008-07-24

信安全对策、保护 Agent 平台的安全对策、保护 Agent 本身的安全对策[6]。

3 基于可信任第三方身份认证的整体移动 Agent 模型

为全面保障 Agent 系统的安全,设计了如下基于可信任第三方身份认证的整体移动 Agent 模型(Overall Mobile Agent security Model based on the Trusted third party,OMAMT)以全面加强 Agent 系统的安全。

3.1 OMAMT 模型设计

在移动 Agent 系统中采用可信任第三方的认证方案[7-9]已得到广泛认同,但如何在移动 Agent 环境中更加有效地从整体上实施可信任第三方的认证方案,从整体上保证移动 Agent 系统的安全性,至今并没有很好解决。从移动 Agent 系统的全局出发,提出一个系统整体安全性模型,如图 1 所示。

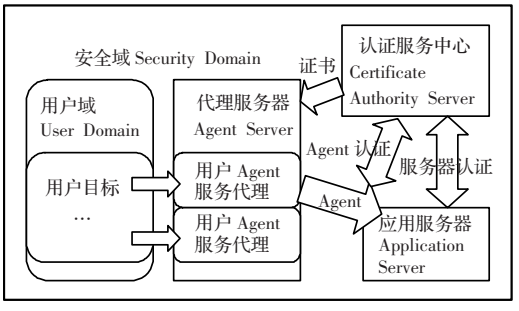

图 1 OMAMT 方案结构示意图

OMAMT 系统中模块的定义及功能如下:

(1)用户域(User Domain):广泛的 Agent 用户向 User Domain 发出服务请求,用户域面对网络用户,提供网络请求服务,根据不同用户的需求,提供全面的信息服务,智能化理解用户意图,具有知识、信念、能力、选择和承诺等人类具有的特性,因此用户域服务器必须具备代理性、主动性、社会性及智能性的属性。

定义 1 信息生成框架 User_Domain 定义为 $Agent\_Massage=(A\_M1,A\_M2,\cdots,A\_Mn)$,$A\_Mn=(Userid,Objectives,Conduct,Content)$,$Userid$ 为用户序号,$Objectives$ 为用户目标,$Conduct$ 用户行为,$Content$ 行为内容。

(2)Agent 服务器(Agent Server):作为移动 Agent 在网络中的载体,为用户的移动 Agent 提供路由策略、加密、接收、跟踪、存储、恢复及向认证机构服务器(Certificate Authority Server)申请证书等。

Agent 服务器接收来自第三方可信认证服务器发送的移动 Agent 身份证书。并将证书加载至移动 Agent 中,为移动 Agent 提供身份证明;同时为移动 Agent 的网络活动提供服务,成为移动 Agent 在网络中的驿站,使其具有自治性、移动性、诚实性的属性。

定义 2 Agent 网络服务器(Agent Server,承载 Agent 的平台容器):$Agent\_Server=(Key\_Management,Agent\_Initialization,Agent\_Receiving)$,密钥管理,Agent 初始化,Agent 接收。初始化 Agent 定义为 $Agent=(Agentid,Agent\_Message,Agent\_Router,Agent\_Key)$,$Agentid$ 为 Agent 网络序号,$Agent\_Message$ 为用户需求,$Agent\_Router$ 为路由策略,$Agent\_Key$ 为检验合法性付予的密钥。

(3)认证机构服务器(Certificate Authority Server):为用户服务器及应用服务提供管理 Agent 身份认证的功能,包括密钥证书的生成、向 Agent 服务器颁发证书、证书的验证等工作。其处于网络的核心地位,为域内网络的安全运行,提供保证,并且通过审计安全域内服务器的安全性能,为 Agent 服务实体生成详细的审计报务,动态评估 Agent 的运行环境,同时建立信用档案。

定义 3 第三方可信服务器(Certificate Authority Server,CAS),$CAS=(Key\_Publishs,Enterprises\_Key,Consumers\_Key,Key\_Checking,Credit\_Record)$,$Key\_Publishs$ 为密钥发布系统,$Enterprises\_Key$ 企业密钥生成系统,$Consumers\_Key$ 消费者密钥生成系统,$Key\_Checking$ 密钥核对系统,$Credit\_Record$ 用户信用记录系统。

(4)应用服务器(Application Server):为用户提供网络的应用服务,典型的如电子商务、电子银行等。接收 Agent 的应用服务器对派遣的移动 Agent 进行身份认证,并且移动 Agent 也需要对服务平台进行身份识别,也就是指双向身份识别,双方共同向 CAS 服务器发送身份证书,由 CAS 服务器来做出双方的身份识别。为保护证书的安全性,移动 Agent 发送需要具有发送携带认证证书的加密子 Agent 的能力,来防止证书的丢失及被破坏。

定义 4 Agent 应用平台(Application Server):$APP\_S=(DataBase,User\_Management,Key\_Management)$,$DataBase$ 为网络信息数据库管理,$User\_Management$ 为对访问用户管理,$Key\_Management$ 为自身密钥管理。

(5)身份认证机制的流程分析:整体的 Agent 系统构成了完整的基于可信任第三方机构为核心的安全体系,其网络信息的传递形式分析如下:

①用户提出需求,生成移动 Agent:

$$User \xrightarrow{Objectives,Conduct,Content} A\_M1$$

②Agent Server 生成 Agent 服务代理:

$$User\_Domain \xrightarrow{Agent\_Router,Agent\_Key} Agent\_1$$

③Application Server 接收到 Agent_1 后,双方将身份信息传递至 CAS 进行身份核对,CAS 并将结果返回:

$$Agent\_1 \xrightarrow{Agent\_Key} CAS.key\_checking$$

$$APP\_S \xrightarrow{APP\_Key} CAS.key\_checking$$

$$CAS.key\_checking \xrightarrow{Checked\_Result} APP\_S \ \&\ Agent\_1$$

④当 Agent 与应用服务器双方身份合法后,可以通讯:

$$Agent\_1 \xleftrightarrow{Message} APP\_S$$

$$Agent\_1 \xleftrightarrow{Message} Other\_Agent$$

⑤当 Agent1 完成当前 APP_S 的任务后,可以继续访问其它的 APP_S,并且 CAS 保存访问记录,建立双方安全性评价的 Credit_Record。

⑥CAS 为保证整个安全域的安全性,一方面定期对发送给双方的密钥进行更新,另一方面对 APP_S 及 Agent_Server 进行信用评价,对安全信用值较低的一方,实施相应措施。

$$CAS.key\_Publish \xrightarrow{User\_key} Agent\_Server$$

$$CAS.key\_Publish \xrightarrow{Enterprise\_key} APP\_S$$

对上述身份认证机制的流程分析如图 2 所示。

3.2 移动 Agent 安全域

在移动 Agent 环境中,由于网络规模的庞大及复杂,需要

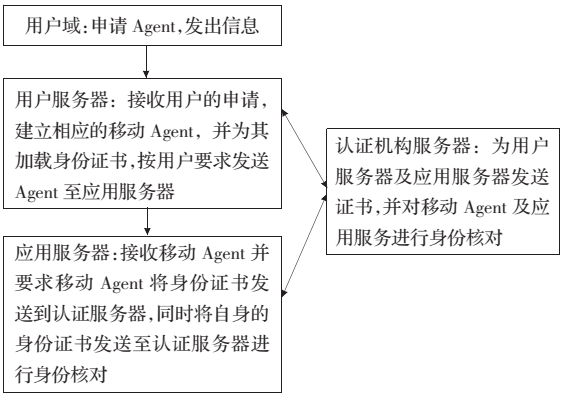

图 2　OMAMT 模型的功能流程图

采用相对独立的信任域的网络结构，各信任域分别信任不同的第三方认证机构，信任域内拥有相对独立的移动 Agent 的生成、认证及服务设施,组成了完整的安全区域(简称安全域 security domain)。

安全域是由第三方服务器划定的需要保护的最小安全单位,整个移动 Agent 系统被定义为一系列安全域的组合,各个域之间具有边界。在安全域中,要求域内具有实时监控能力,由分布在各个域中的监控器来完成,以了解域中移动 Agent 的运行情况[10]。

定义 5 安全域(Security Domain):*Sec_D*=(*User_Domain*, *Agent_Server*,*CAS*,*APP_S*)，整个网络由若干个小的安全域组成,每个域包括有 *User_Domain* 用户域,*Agent_Server* 为对网络中 *Agent* 的管理服务器,*CAS* 为提供密钥管理的应用服务器,*APP_S* 为提供信息服务的应用服务器。

根据移动 Agent 在不同用户域的申请,将移动 Agent 划分到相应的安全域中。通过安全域的建立,采用高强度的公钥机制来保证服务的可信,在两个层面上实现了系统的容侵性。第一是域级的,主要由安全域结合具体的故障模型和故障恢复模型来实现。第二是域间级的,主要由认证机构通过身份认证,通信数据加密，数据一致性检查等方案来保证域间通信的安全性,并且通过域的交互,随时可将异常域屏蔽,保证整体的健壮性。

移动 Agent 的资源访问请求会被资源所在的本地域认证服务设备审核,若该移动 Agent 是本地域用户,则对其认证后,授权该 Agent 访问该资源;若该 Agent 是外地域用户,则需联合外地域的认证服务设备对该 Agent 进行认证。另外,在资源访问过程中,Agent 可以访问不同信任域的资源,为了防止非法窃听者跟踪该 Agent 的资源访问记录,需要在认证过程中隐藏 Agent 的真实身份，使得外地域和非法用户都不能获得 Agent 的真实身份,提供匿名性服务,保护 Agent 用户的隐私。多安全域网络环境中共享资源的分散性以及信任域认证的特点,决定了跨信任域认证应该满足以下安全需求:

(1)访问域认证:Agent 在跨域认证过程中,可认证外地域认证服务设备身份。

(2)Agent 从属域认证:在跨域认证过程中外地域认证服务设备可验证 Agent 是否是一个有效信任域的合法 Agent。

(3)安全密钥协商:Agent 和外地域认证服务设备可在跨域认证过程中协商安全的会话密钥,为资源访问提供数据保密。

(4)Agent 的匿名性和不可跟踪性:它用于跨域认证过程中隐藏 Agent 的真实身份信息,保护主体的资源访问记录不被外地域认证服务设备或者非法攻击跟踪,保护用户隐私。

域的定义可伸缩,如一台认证机构服务器、一台用户服务器、一台应用服务器主机可以是一个安全域,域间级之间加入防火墙的设置,使各个域之间具有边界。安全域可以视作有限的私人域,不同权限具有不同的操作级别。在安全域的层面上解决域间的安全性问题,同时也保证了每个安全域中的认证机构的相对独立性,降低认证机构服务器的负荷。

域结构如图 3 所示。

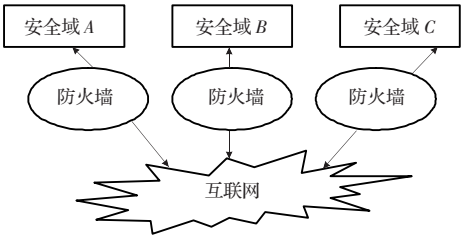

图 3　OMAMT 模型安全域的网络结构

4　OMAMT 模型的安全性能分析及其应用

该认证模型的安全性的前提是需要每个域所信任的 CAS 系统是安全可靠的，而 CAS 系统的安全性取决于身份认证算法的安全性以及 CAS 运营的安全性。

4.1　安全性能分析

移动 Agent 采用可信任第三方认证来解决安全问题,并根据移动 Agent 在网络中的不同阶段解决存在的安全隐患。

(1)针对恶意 Agent 对服务器平台的攻击,模型基于可信任第三方认证机构及 Agent 发布者的信任。当 Agent 执行非法操作时,根据其身份进行追踪、记录,以减少恶意 Agent 非法使用或独占系统网络资源。

(2)恶意的目标主机或代理服务器对移动 Agent 的攻击,主要分为两种攻击。

首先拦截移动 Agent 进行攻击。采用身份认证机制后,在移动 Agent 未得到可信任第三方的服务器认证之前,并不会将自身的信息处于解密状态。安全域体系也可以阻止非法服务器在域内的拦截行为,因此可以解决拦截问题。

其次是在合法的服务器上,被非法 Agent 的攻击。通过证书管理,通过验证其身份减少非法 Agent;采用安全审计,对域内服务器建立信用档案;通过安全域管理,实时监视和评估域内 Agent 运行安全状态,为域内的 Agent 提供安全报警、逻辑隔离及安全恢复等服务。

4.2　方案应用

在模型基础上开发了基于智能 Agent 电子商务仿真系统,开发平台采用 Java 语言和 JSP 技术,数据库采用 MYSQL;在设计中采用用户登录安全策略,在建立 Agent 时,一方面完全采用服务器系统给客户提供的需求方案供用户选择,买方的购买需求通过买方服务器代理发布,卖方产品则通过卖方代理服务器进行发布(如图 4 所示),保证了整个电子商务系统的安全性。另一方面根据用户提供的产品信息,在网络数据库中搜索满足客户需求的产品,并且应用了价格自动协商机制,对产品的价格进行自动协商,在双方认同的价格上进行交易,完全由服务器完成整个交易工作,用户确认即可完成整个商品的交易过程。

通过实际验证，为今后移动 Agent 在 Internet 电子商务中的应用做出了有益的探索。

图4 智能 Agent 电子商务仿真系统

5 结束语

在前人工作的基础上提出了基于可信任第三方的 MAS 整体安全模型。与已有的模型相比其优势有以下几点:

(1)采用用户域服务器方法建立移动 Agent,提高了移动 Agent 的可靠性、高效性及鲁棒性。

(2)使用可信任第三方的认证机制,赋予移动 Agent 合法身份,通过双向认证提高了移动 Agent 及服务器在网络中的可信性,解决了移动 Agent 与 Agent 平台相互信任问题。

(3)采用安全域的网络体系结构,在多信任域的网络环境下,各机构形成了相对独立的信任域,通过有限度的故障排查和恢复,使安全域具有一定的安全免疫性。

综上所述,与以往的 Agent 安全模型相比,综合运用了多种安全技术,使得系统的安全性有了较大提高,突出特点在于其从整体性角度分析解决移动 Agent 面临的安全问题,仿真实验验证了 OMAMT 模型和整体性安全方案的有效性。

参考文献:

[1] 谭湘,顾毓清,包崇明.移动 Agent 系统安全性研究综述[J].计算机研究与发展,2003,40(7):984-993.

[2] 王汝传,徐小龙,郑晓燕,等.移动代理安全机制模型的研究[J].计算机学报,2002,25(12):1294-1301.

[3] Roth V,Jalali M.Concepts and architecture of a security-centric mobile agent server[C]//The 5th Int'l Symposium on Autonomous and Decentralized System.Dallas:IEEE Computer Society Press,2001:435-442.

[4] 李梅,马颖,张劳模.基于内容保护的安全机制在移动应用中的设计[J].河南师范大学学报:自然科学版,2008,36(4):37-39.

[5] 辛向军,潘瑾,李永强.一个新的基于身份的盲签名方案[J].河南师范大学学报:自然科学版,2008,36(3):23-25.

[6] Jansen W.Countermeasures for the mobile agent security[J].Computer Communications,2000,23(10):1667-1676.

[7] Lin Min-hui,Chang C C,Chen Yan-ren.A fair and secure mobile agent environment based on blind signature and proxy host[J].Computers & Security,2004,23(1):199-212.

[8] 马国瀚,李炎.网络安全、可信系统技术分析[J].河南师范大学学报,2008,36(6):144-145.

[9] 杨立身, 郭政慧.COM 技术应用-在 ASP 程序中应用目录服务做身份验证.[J].河南师范大学学报,2007,35(3):39-41.

[10] 鼓华熹.一种基于身份的多信任域认证模型[J].计算机学报,2006,29(8):1271-1280.

(上接 40 页)

基于传统的 Kruppa 方程的摄像机自标定(图中为:traditional Kruppa method)和该文提出的基于 Kruppa 方程摄像机自标定方法(图中为:improved method)进行求精后求出的 5 个内参数值的实验结果与理论值的绝对误差(单位为 mm)随噪声水平的变化曲线。

从图中可以看出, 提出的方法比传统的基于 Kruppa 方程的标定方法标定结果误差更小,提出的方法提高了标定方法的鲁棒性。

2.2 真实图像实验

在真实图像实验中,先将摄像机做三次线性无关的平移运动,摄取了如图 2 的三幅图像。

图2 摄像机做三次线性无关的平移运动摄取的三幅图像

这三次平移运动设置为(单位:mm):((80,100,50),(-50,-70,60),(90,-70,80)),分别选取运动前后像平面间的匹配点对, 运用提出的标定算法得到摄像机内参数 a_x=988.157,a_y=990.659,r=-0.012 3,u_0=2.154,v_0=3.111。此结果是符合实际情况的。

3 结束语

回顾了 Kruppa 方程的基本形式, 研究探讨出了进行摄像机自标定的非线性优化的目标函数,并在此基础上提出了通过摄像机平移运动得来的内参数来确定目标函数中 $\boldsymbol{C}$ 的初值,而后由 Kruppa 方程得来的目标函数来进一步精化内参数矩阵的二步式方法。实验证明这种二步式标定方法是可行的,并且能很好的提高标定结果的鲁棒性。

参考文献:

[1] Maybank S J,Faugeras O D.A theory of self-calibration of a moving camera[J].International Journal of Computer Vision,1992,8(2):123-151.

[2] 孟晓校,胡占义.摄像机自标定方法的研究与进展[J].自动化学报,2003,29(1):110-124.

[3] Luong Q T,Faugeras O D.The fundamental matrix:Theory,algorithms,and stability analysis [J].Int Journal of Computer,1996,17(2):43-75.

[4] 李华,吴福朝,胡占义.一种新的线性摄像机自标定方法[J].计算机学报,2000,23(11):1121-1129.

[5] 雷成,吴福朝,胡占义.Kruppa 方程与摄像机自标定[J].自动化学报,2001,27(5):621-630.

[6] Hartley R I.Kruppa's equations derived from the fundamental matrix[J].IEEE Transactions on Pattern Analysis and Machine Intelligence,1997,19(2):133-135.

[7] Ma Y.Kruppa equation revisited:Its renormailization and degeneracy[C]//Proceedings of ECCV'2000,Dublin,2000.

[8] Lourakis M I,Deriche R.Camera self-calibration using the singular value decomposition of the fundamental matrix:From point correspondences to 3D measurements,Research Report 3748[R].INRIA,Sophia-Antipolis,1999.

[9] 雷成,胡占义,吴福朝,等.一种新的基于 Kruppa 方程的摄像机自标定方法[J].计算机学报,2003,26(5):76-86.

[10] 于洪川,吴福朝.基于主动视觉的摄像机自标定方法[J].机器人,1999,21(1):1-7.