基于 Agent 的网格安全跨域扩展研究

张 琳,王汝传,王海艳
(南京邮电大学 计算机学院,江苏 南京 210003)

摘 要:网格安全已成为网格计算的核心问题。大多数的网格体系都只是提供了安全基础设施,而没有规定具体的安全措施实施框架和安全交互过程。结合移动代理技术提出了一个网格安全跨域扩展模型(MA-GSME),介绍了工作流程及主要实现技术。借助一种数据结构,使移动代理的智能性得以充分发挥,进而在一定程度上解决了网格跨域访问的难题。分析结果表明,新模型在一定程度上增强了网格单点登录的功能,并提高了系统实施跨域访问的透明性及有效性。

关键词:移动代理;网格安全;跨域访问
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2010)10-0198-05

Research of Grid Security Multi-Domain Extensible Model Based on Mobile Agents

ZHANG Lin, WANG Ru-chuan, WANG Hai-yan
(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Security has become a key problem in grid environment. For most grid systems, there only is a security infrastructure without a detailed implementation framework or secure cooperation process. Provide a grid security multi-domain extensible model called MA-GSME by using mobile agents, introduce its work mechanism and main implementing technology. By virtue of a kind of data structure, make mobile agents deploy their intelligence adequately and solve the difficult problem of multi-domain access in grid to a certain extent. Analysis results show that the new model enhances the function of single sign-on in grid to a certain extent and heightens the transparence and validity of multi-domain access in grid system.

Key words: mobile agents; grid security; multi-domain access

0 引 言

网格计算作为下一代网络技术有着广阔的发展前景,它通过高速网络把分散在各处的硬件、软件、信息资源连接成一个巨大的整体,从而使得人们能够利用地理上分散于各处的资源,完成各种大规模的、复杂的计算和数据处理的任务。与以前的协同工作(Cooperative Work)、分布式计算(Distributed Computing)等概念相比较,网格计算的集成程度更高、使用更加方便、资源的利用更加充分和有效。目前,各国政府和大公司近年来纷纷投入巨资开展网格相关的研究开发工作,其中有代表性的成果有 Globus、Legion、欧洲数据网格和织女星网格[1]等。

网格计算的安全问题[2~6]是网格计算技术的关键问题之一,特别随着网格计算技术从传统的科学计算进入商业应用领域,安全问题的解决更是迫在眉睫。以 Globus 为例,它通过提出网格安全基础设施 GSI,来提供在网格计算环境中的安全认证和安全通信等能力。其目标有:支持在网格计算环境中主体之间的安全通信,防止主体假冒和数据泄密;支持跨虚拟组织的安全;支持网格计算环境中用户的单点登录,包括跨多个资源和地点的信任委托和信任转移等。不难发现 GSI 所提供的安全机制较单一,有些跨域访问方面的安全问题还没有得到彻底解决,无法切实地满足网格用户实施共享资源与协同工作的需要,有待进一步地发展与完善。

文中首先介绍了移动代理技术,给出了它的特点及优势;将其引入网格安全的研究领域,以扬长避短为原则,借助移动代理的移动性、自主性和智能性等特点,提出了一个网格安全跨越扩展模型,并详细介绍了

收稿日期:2010-02-26;**修回日期**:2010-05-21
基金项目:国家自然科学基金(60773041);国家高科技 863 项目(2007AA701301,2007AA701302,2007AA01Z404,2007AA01Z478);江苏省自然科学基金(BK2008451);南京邮电大学科研基金项目(NY209015)

作者简介:张 琳(1980-),女,江苏丰县人,讲师,博士,研究方向为计算机网络和网格计算、信息安全和移动代理技术等;王汝传,教授,博士生导师,研究方向是计算机软件、计算机网络和网格、信息安全、无线传感器网络、移动代理和虚拟现实技术等。

工作流程;对其中的关键技术进行了解析,给出了具体的实施方案及性能分析,初步解决了移动代理自身的弱智能性及网格环境中的跨域安全访问等问题。

1　移动 Agent 技术

移动代理是一段独立于操作平台和操作系统的程序代码,称为移动码,移动代理能自主地在网络中从一个节点迁移至另一个节点,利用合适的计算资源,代表用户完成特定的任务。移动代理具有以下特征:能够转移到不同的地址空间中执行,并且转移后其执行是持续的,即从转移时的下一条指令开始继续执行,转移过程中保持自身的状态。移动的目的是使程序的执行尽可能靠近数据源,降低网络通信开销,节省带宽,平衡负载,加快任务的执行,从而提高分布式系统的处理效率。

基于移动代理的系统具有生存、计算、安全、通信、迁移机制。生存机制指的是移动代理的产生、销毁、启动、挂起、停止等服务;计算机制指的是移动代理及其运行环境所具备的计算推理能力,包括数据操作和线程控制原语;安全机制描述移动代理访问其它移动代理和网络资源的方式;通信机制定义移动代理之间及其和其它实体之间的通讯方式;而迁移机制负责组织移动代理代码及其执行时的中间状态,使得它在不同位置间移动。

对移动代理来说每个网络设备上均存在一个移动代理执行环境,也可以称之为移动代理服务设施或移动代理服务器。不同的移动代理系统的体系结构各不相同,但几乎所有的移动代理系统都包括如下两部分:移动代理执行环境和移动代理。其系统模型见图 1。

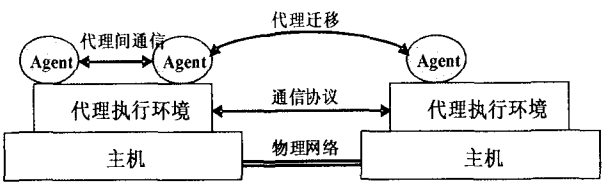

图 1　一个典型的移动 Agent 系统模型

移动代理技术是分布式技术与代理技术相结合的产物,它除了具有智能代理的基本特性——自主性、反应性、能动性、通信性等以外,还具有移动性,其主要特性包括:

1. 自主性:自主性是代理最基本的特性,指行动上的独立性。代理一旦被初始化以后便独立执行,无需后来的直接干预,它控制着自身的内部状态和外部行为,也可被授权去做某种决定,完成一些重要事情。

2. 反应性:是指代理能感知和作用于其所处的环境,从而对环境的变化做出及时的响应。这些环境可以是物理的世界、使用图形接口的用户、其它代理集合或者所有这些的组合。

3. 能动性:为了达到目标,代理不是等着接收指令,而是事先有计划,并做一些初始化。代理能探测到适合用户目标的有利场景,通知用户这个场景出现的时机。也就是说,代理不仅能对所处的环境作出响应,还能主动地展现面向目标的行为。

4. 通信性:通信性是指代理之间的交互。代理之间的接口和联系不是固定不变的,而是随着任务驱动者的改变而改变。为了协作完成一件复杂的任务,一些代理可以形成代理群,代理之间的接口可以在运行中协商,这样就减少了代理之间的耦合性,意味着代理可以以最小的代价和较小的冲突加入系统或从系统中删除。

5. 移动性:移动性是移动代理最重要的特性之一,它是指代理可以在一个网络上随时、随地、自主地从一台主机迁移到另一台主机上。正在运行中的代理状态可以被存储且传送到新主机上,在新主机的代理执行环境中被恢复并且从暂停处继续执行。代理将代码和数据封装在执行的一个线程中,每个代理独立于其它代理之外。

谈到移动代理,不可逃避其安全问题,它是制约该技术得以迅速普及的一个主要因素。概括来说,移动代理系统存在三个安全问题:服务器资源所面临的攻击、移动 Agent 面临的攻击、数据传输中的安全问题。

针对这三方面的问题,目前已经有了较成熟的解决方案。对于服务器资源的保护主要有:沙盒模型,签名、认证、授权和资源分配,Proof - carrying code,代码检验,限制技术,核查记录;对于执行环境中移动 Agent 的保护方案,可分为基于被动检测的安全措施和基于主动的保护措施,后者主要有加密函数、有限黑匣子法、共享秘密与互锁、可抵御攻击的硬件等安全方法;而对于传输中移动 Agent 的保护方案,则主要是用加密技术来实现。

强调一点,在网格安全领域中引入移动代理并不是过多地考虑其安全问题,而是借鉴了它在移动性和智能性等方面的优势,使之辅助网格自身的安全机制来完成各种安全检验。

2　应用移动代理的网格安全跨域扩展模型(MA - GSME)

2.1　模型的组成结构

移动代理是一段独立于操作平台和操作系统的程序代码,能自主地在网络中从一个节点迁移至另一个节点,代表用户完成特定的任务。几乎所有的移动代

理系统都包括如下两部分:移动代理执行环境和移动代理。移动代理的主要特性包括:自主性、反应性、能动性、通信性和移动性。其中,安全问题是制约该技术得以迅速普及的一个主要因素,目前已有了较成熟的解决方案,不再详述。但需强调一点,引入移动代理并不是过多地考虑其安全问题,而是借鉴了它在移动性和智能性等方面的优势,使之辅助网格自身的安全机制来完成各种安全检验工作。图 2 给出了一个网格安全的跨域扩展模型(Grid Security Multi - domain Extensible Model Using Mobile Agents, MA - GSME)。

2.2 模型的运行机理

为了更好地描述网格安全架构中的跨域问题,本模型以三个虚拟组织(VO1、VO2、VO3)为例进行了跨域的描述。为了提供移动代理的执行环境,在每个处理节点上分别安装了 grasshopper。以下是网格跨域安全实施的整个过程。

第一步 网格用户如果是新用户,则需通过该步骤向 VO1 的认证中心 CA 提交用户身份、公钥等信息以备验证和签发用户证书;如果是合法用户则直接转向步骤三。

第二步 验证通过后向用户返回签发的证书。

第三步 用户向 VOS 提交作业请求信息和用户信息(包括自己的证书)。每个 VO 中都有一个 VOS,掌握着该虚拟组织上层的管理信息,作为 VO 面向用户的窗口,用来接收用户作业请求并返回作业处理结果。

第四步 VOS 每接收一个用户请求就会自动生成一个对应的用户信息 agent,用以代替用户完成各种作业请求。VOS 以最小化原则将所有用户需要用到的信息赋予该 agent,便于它在移动过程中面对不断变化的上下文信息能够自主地作出智能的决策(具体实现技术见下节)。Agent 生成后,它将按照计划移动到第一个安全检验部门 AES 处进行用户身份的认证。

第五步 每个安全构件内部都有一个 agent 守护进程实时启动,便于对到达的各个 agent 即时地实施安全验证。用户信息 agent 和 agent 守护进程进行交互后,如果通过认证,该 agent 将移动到下一个安全检验部门 TUS 处进行信任等级的评估,同时,守护进程会将此次认证的结果送入用户信息 agent 的数据区,为其将来作出智能决策提供依据;如果认证失败,该 agent 将携带失败信息返回 VOS 处,由 VOS 通知用户交易失败。

第六步 同步骤五,用户信息 agent 和 agent 守护进程进行交互,如果信任的综合计算值大于信任模块的最低门限级别,表明该 agent 通过了信任的验证,可以接着移动到 GIS 处,同时守护进程会将最终的信任等级送入 agent 的数据区;否则返回失败信息。具体的信任模块部署方案可参考已有的研究成果[7~11]。

第七步 RIS 声称资源信息服务器,它相当于整个

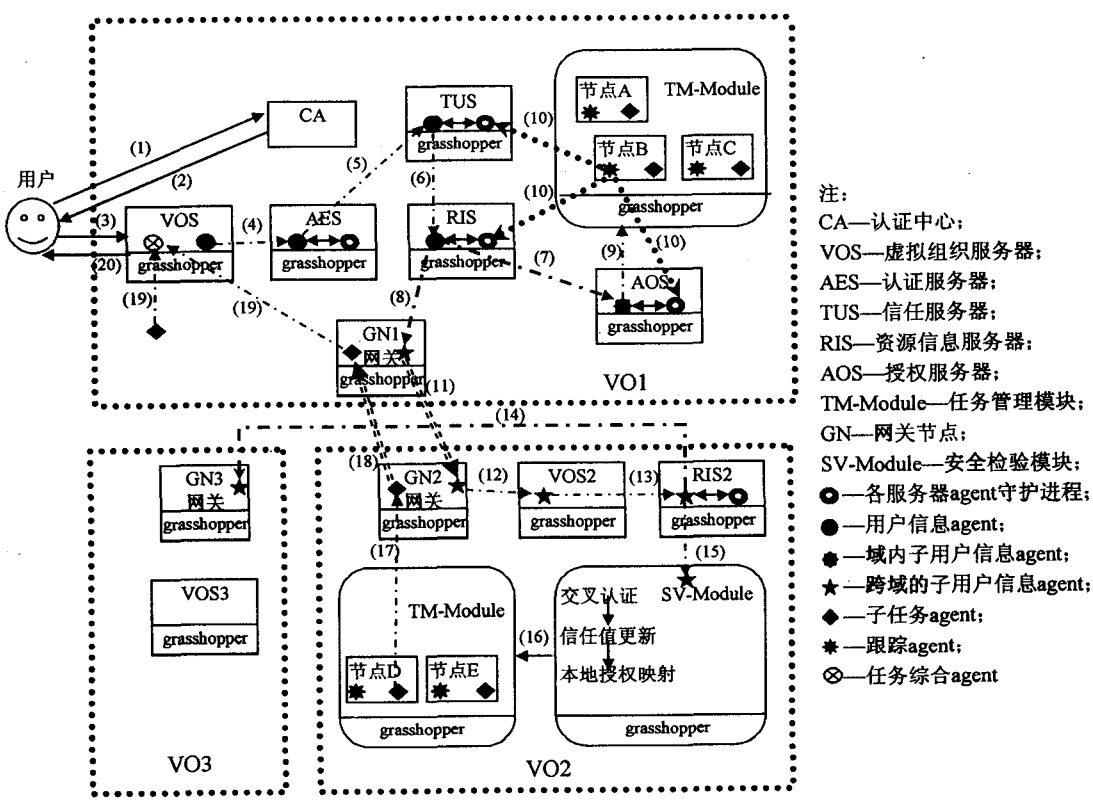

图 2 应用移动代理的网格安全跨域扩展模型

VO 的资源注册中心,掌控着本域所有的资源信息,随着资源动态地加入或撤离 VO 而动态的更新变化。用户作业在被授权之前需要先访问该服务器,了解本 VO 的现有活动资源是否可以完全满足用户作业的需求。如果只能满足部分需求,那么用户信息 agent 就会自主地生成两个子 agent 继续移动,它们分别继承了父 agent 的相关信息,又各自携带有新的子作业请求信息,其中一个在本域内继续移动(域内子用户信息 agent),另一个负责跨域移动(跨域的子用户信息 agent)。在域内移动的 agent 将进入 AOS 等待被授权。

第八步 相对而言,跨域的子用户信息 agent 要携带更多的信息才能实现跨域的安全访问,比如交叉证书等。它直接移动至网关节点处做好进行跨域的准备。

第九步 域内子用户信息 agent 的作业请求策略与守护进程提供的作业策略相匹配,如果成功,则对其进行授权并将权限结果送入该 agent 的数据区,然后它将移动到任务管理模块等待任务的控制与分配等。

第十步 根据用户子作业的请求信息,任务管理模块会进行任务的分解、分配、调度、监视等操作[12]。此过程中,各任务节点上均将产生子任务 agent 和跟踪 agent。跟踪 agent 将实时监视任务的执行情况、资源的可用情况以及用户代理有没有破坏本地资源等,然后分别反馈给 TUS、RIS 和 AOS 的 agent 守护进程以便执行安全信息的实时更新操作。如果用户代理没有按照双方协商的计划执行任务或者有意破坏了本地资源,那么在收到跟踪 agent 的反馈信息后,TUS 会降低该用户的全局信任度,AOS 则适当地降低其访问权限或设置其为拒绝访问。

第十一步 跨域的子用户信息 agent(以下记为 MS-agent:Multi-domain Sub-agent)在域内网关节点处自主搜集路由信息,试探向邻近的 VO 寻求能够完成跨域子作业的网格资源。带着用户的证书链等安全验证信息及跨域子作业的请求策略,该 agent 根据得到的路由信息自动迁移到 VO2 的网关节点 GN2 上。

第十二步 MS-agent 从 GN2 处获得 VOS2 的 IP 地址直接迁移到这个节点上,并将已经访问过的 GN2 的 IP 地址添加到自己的数据区,以备将来按照原路径返回至 VO1。

第十三步 MS-agent 从 VOS2 上获得相关信息并迁移到 RIS2 处。

第十四步 MS-agent 与 RIS2 的 agent 守护进程进行信息交互,以粗略的形式了解 VO2 是否可以独立完成跨域子作业的任务请求。如果不能完成,MS-agent 会根据自己携带的路由信息自主地迁移到下一个虚拟组织 VO3 的网关 GN3 处进行同样的工作,以后的步骤依次类推。

第十五步 如果 VO2 现有的活动资源能够胜任 MS-agent 携带的跨域子作业请求,那么接下来就要进行安全验证,MS-agent 将迁移至安全检验模块接受相应的操作。由于是跨域的安全检验,则可能涉及到交叉认证、信任值的重新计算以及跨域访问控制的映射等问题,较域内的安全验证要复杂些。

第十六步 同步骤九,验证通过后 MS-agent 迁移至任务管理模块。

第十七步 跨域子任务 agent 在完成其分配的任务后根据其携带的路由信息直接迁移至网关节点 GN2 处,做好返回 VO1 的准备。

第十八步 同步骤十,主要进行信息的反馈以增强安全模块的健壮性。

第十九步 跨域子任务 agent 携带着作业处理结果返回 VO1 的 GN1 处。

第二十步 域内的以及跨域的子任务 agent 将各自的处理结果返回给 VOS,此时 VOS 需要重新生成一个任务综合 agent 用以整合各子任务 agent 的处理结果。

第二十一步 将最终计算结果以可视化界面的形式返回给网格用户。

3 MA-GSME 相关技术及性能分析

3.1 Agent 的智能性

在模型的步骤四中提到,VOS 要为每个用户信息 agent 以最小化原则赋予足够的信息,二者并不矛盾。最小化原则体现在 agent 在移动的过程中较轻便、灵活并能减少网络流量的负载;足够则体现在 agent 可以根据这些信息能够自主地在各节点间移动,而无需用户进行干预,即对用户透明。兼顾这两个方面,为 agent 提供的信息有:用户基本信息、证书信息、作业的请求信息、创建该 agent 的 VOS 的 IP 地址、创建时间等。为了体现 agent 智能移动的特性,采用了一种数据结构加以实现,如表 1 所示。

表 1　Agent 在域内移动的 path 表

域内 path	地址	访问时间	验证结果	备注
认证服务器	10.10.138.2	2006/4/17 8:00	T	
信任服务器	10.10.138.8	206/4/17 8:20	T	信任等级 T4
资源信息服务器	10.10.138.4	2006/4/17 9:12	T	
授权服务器	10.10.138.7	2006/4/17 1:05	F	权限级别 P2
作业服务器				
……	……	……	……	……

其中,"域内 path 途径"这个字段记录了 agent 移动的先后顺序,"验证结果"记录 agent 是否通过了该

服务器的安全验证,T 表示通过,F 表示验证失败。Agent 每到一个节点,都会将节点对它的验证结果记录下来,另外附带添加"访问时间"和"备注"(可选),表现在数据表中就是为某一条记录添加字段值。

对于资源信息服务器这条记录,当 VO1 域内的现有活动资源不能为用户作业提供任何一种服务时,其"验证结果"字段才记为:F。另外,一旦某个字段值首次被标为 F,系统则立即中断服务,并将访问失败的信息反馈给用户。

将此数据结构放入 agent 的数据区内,能让 agent 表现出更好的自主性、灵活性和智能性,这也是在网格安全体系架构下引入移动代理的初衷。

3.2 安全的透明性

在模型的步骤七和八中提到,如果用户信息 agent 检测到 VO1 的活动资源不能完全满足其作业请求时,它将根据目前的资源信息自动产生两个子 agent 而无需禀报网格用户,同时为它们分别签署临时证书。对于在域内移动的子 agent 它将继承父 agent 的相关信息,然后再添加创建时间、新的子作业请求信息、证书链和新的域内 path 表等信息;而对于跨域的子 agent,它要充分发挥自身的智能性,自主地去寻找进行跨域安全认证的信息,除了需要携带上述这些信息之外,它还要到 CA 处获得有关交叉认证证书的信息并创建域间移动的 path 表。在 VO1 的网关处,它需自动搜索路由信息并加入到自己的数据区为跨域路由做准备。这些操作均由 agent 自己完成,从而表现出了用户跨域访问网格的透明性。

3.3 模型的有效性

在进行跨域访问时,代表用户的子 agent 首先被 VOS2 派遣到 RIS2 处,询问该虚拟组织是否可提供执行跨域子作业所需的全部资源,而不是先对 agent 进行安全检验,这比较符合人类社会中的交往规则,也是本模型设计的又一特色,充分体现了安全实施的有效性。如果你能满足我的请求,我再进一步接受你对我的安全验证;否则,我就没必要接受你的安全检验,按照自己携带的路由信息立即转身到下一个 VO 处请求服务。

4 结束语

Globus 在安全机制方面尚存众多不完善之处,文中基于移动代理给出了一个网格安全架构的跨域扩展模型(MA-GSME),在一定程度上增强了网格单点登录的功能,并提高了系统实施跨域访问的透明性及有效性。其优点主要有:借助 MA 的智能性和灵活性,使网格用户在提交完作业请求后不需要再次进行干预,MA 会根据文中提供的域内 path 表以及周围环境的变化自主地做出处理决策,包括进行跨域的资源访问,所有这些操作都对用户透明,基本上可以完成 Globus 单点登录的功能;MA 的移动性可以减少网络负载,它直接移动到目标节点处与之进行本地通信,而只是携带运算结果返回;在进行跨域访问时,agent 先向 GIS 咨询现有的活动资源能否满足其子作业的请求,若可以满足,才进行跨域的安全检验,否则 agent 立即离开该虚拟组织而转向其他地方寻求服务,这种方式较符合人际交往规则,将其引入网格中可提高系统的健壮性。

另外,信任已成为国内外学者目前研究的热点,作为网格安全针对用户和资源在主观因素方面做出的评判,结合 Globus 传统的在客观方面的安全机制,如认证、访问控制、授权等,在本模型中体现出了一种主客观结合的网格安全跨域访问的机制,为网格安全的实施提供了新的思路。

参考文献:

[1] 徐志伟,李 伟.织女星网格的体系结构研究[J].计算机研究与发展,2002,39(8):923-929.

[2] Chen J G,Wang R C,Wang H Y. The extended RBAC model based on grid computing[J]. The Journal of China Universities of Posts and Telecommunications,2006,13(3):93-97.

[3] 姚红岩,李明楚,崔永瑞.网格中一种改进的代理证书链验证方案[J].小型微型计算机系统,2009,30(8):1611-1615.

[4] 于代荣,杨 扬,李盛阳,等.基于身份的网格安全体系结构研究[J].四川大学学报,2009,41(2):200-205.

[5] 王胜川,刘方爱,石晓晶.基于网格环境的动态自适应信任机制研究[J].计算机技术与发展,2008,18(9):151-154.

[6] 李 钦,余 谅.基于免疫遗传算法的网格入侵检测模型[J].计算机技术与发展,2009,19(5):162-169.

[7] 陈建刚,王汝传,王海艳.网格资源访问的一种主观信任机制[J].电子学报,2006,34(5):817-821.

[8] 陈建刚,王汝传,张 琳,等.基于模糊集合的网格资源访问的信任机制[J].计算机学报,2009,32(8):1676-1682.

[9] 张 琳,王汝传,张永平.一种基于模糊集合的可用于网格环境的信任评估模型[J].电子学报,2008,36(5):862-868.

[10] Zhang Lin,Wang Ru chuan, Wang Hai yan. Trusted decision mechanism based on fuzzy logic for open network[J]. Journal of Computers, 2008,3(12):76-83.

[11] Zhang Lin, Wang Ru chuan, Wang Hai yan. Grid trust based on pre-measure and two-level reputation[J]. The Journal of China University of Posts and Telecommunications,2007,14(4):70-76.

[12] 王汝传,徐小龙,黄海平.智能 Agent 及其在信息网络中的应用[M].北京:北京邮电大学出版社,2006:181-183.