基于反馈机制的网格动态授权新模型

李明楚[1)] 杨 彬[1)] 钟 炜[1)] 田琳琳[1)] 江 贺[1)] 胡红钢[2)]

[1)](大连理工大学软件学院 辽宁 大连 116621)

[2)](中国科学院软件研究所信息安全国家重点实验室 北京 100049)

摘 要 网格现有的授权系统存在静态性问题,表现为没有提供机制来反馈用户对授予的权限的使用情况.当一个本来可信的用户或服务变成不可信时,授权系统不能及时发现,对其权限进行调整可能导致恶意用户对网格系统的破坏.因此,在授权系统中建立反馈机制,根据用户的行为动态地调整用户角色,对于网格系统的安全具有重大意义.文中分析了网格中现有的授权系统及信任模型的特点,指出它们存在的不足.在此基础上提出一种基于反馈机制的动态授权新模型,很好地解决了现有授权系统的静态性的缺点.该模型是对 CAS 授权系统的改进,增加了反馈机制和信任度计算机制.其中,信任度计算机制中提出的基于行为的分层信任新模型较以往的信任模型相比,使用服务权值来区分重要服务和普通服务,从而保护了网格中的重要服务并且能有效地抑制恶意节点的行为;文中提出了一种新的更加精确地计算域间推荐信任度的方法,从而解决了不诚实反馈的问题.反馈机制则利用基于行为分层信任模型给出的用户信任度的变化,实现了根据用户的行为动态调整他的角色.文中还设计了三组模型实验,分别验证新模型的特点、对网格中恶意实体行为的抑制情况,从不同的角度对模型进行了实验,对基于行为的分层信任模型对行为的敏感性、收敛性、有效性及合理性加以了证明.

关键词 反馈机制;群组授权服务;信任模型;动态授权;网格计算

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2009.02187

Grid Dynamic Authorization Model Based on Feedback Mechanism

LI Ming-Chu[1)] YANG Bin[1)] ZHONG Wei[1)] TIAN Lin-Lin[1)] JIANG He[1)] HU Hong-Gang[2)]

[1)](*School of Software, Dalian University of Technology, Dalian, Liaoning* 116621)

[2)](*Laboratory of National Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100049)

Abstract There is a problem of static status in the existing authorization systems of grids that don't provide feedback mechanism to feedback the use of permission by users. When a user or a service with creditability at the past would become unlikelihood, the authorization systems could not find this status in time to adjust the user's permission, so that it is possible for malicious users to destroy the grid systems. Thus, building feedback mechanism in authorization to adjust users' roles by their behavior dynamically is necessary to the security of grid systems. In this paper, we analyze the characteristics of the existing authorization systems and trust models in grid, and point out their shortcomings. This paper proposes a new dynamic authorization model based on feedback mechanism to solve static state of mechanisms. This model improves the authorization system for CAS, and adds trust degree computing mechanism and feedback mechanism to CAS. This paper proposes a new trust model with two layers based on behavior in the trust de-

收稿日期:2007-12-20;最终修改稿收到日期:2009-01-03.本课题得到国家自然科学基金(90715037, 60673046,60805024)、辽宁省自然科学基金(20051082)、高等学校博士学科点基金(200801410028)、重庆科技局自然科学计划项目(2007BA2024)、国家"九七三"重点基础研究发展规划项目基金(2007CB714205)资助.**李明楚**,男,1963 年生,教授,博士生导师,主要研究领域为信息安全、网格计算、图论. E-mail: mingchul@dlut.edu.cn; li_mingchu@yahoo.com. **杨 彬**,女,1978 年生,硕士研究生,研究方向为信息安全. **钟 炜**,男,1978 年生,硕士研究生,研究方向为信息安全. **田琳琳**,女,1979 年生,讲师,研究方向为信息安全与密码学. **江 贺**,男,1980 年生,博士,副教授,研究方向为算法与复杂性、智能计算. **胡红钢**,男,博士,研究方向为信息安全与密码学.

gree computing mechanism to distinguish important services and common services by using service weight, so it effectively protects important services in grid from the attack of malicious nodes; This paper also use a new method to account trust degrees between domains to solve the problem of dishonesty feedback. By using two-layer trust model based on behavior to get the changes of trust degrees, the feedback mechanism can adjust users' roles by users' behavior. In this paper, a series of simulation experiments are designed such as validating the characteristic of new model, controlling to malicious nodes. These experiments validate the sensitivity, astringency, validity and rationality with behavior in the two-layer trust model based on these behaviors.

Keywords feedback mechanism; CAS; trust model; dynamic authorization; grid computing

1 引 言

网格是一种信息社会的网络基础设施[1],它是构筑在 Internet 上的一组新兴技术.可实现互联网上所有资源(包括计算资源、存储资源、通信资源、软件资源、信息资源、知识资源等)的互联互通,消除信息孤岛和资源孤岛,实现网络虚拟环境上的资源共享和协同工作.网格环境是一个开放、动态的环境,其中实体具有自主性,实体之间的协作具有动态性,仅用证书来约束它们之间的访问控制是不够的.在这样的环境下,实体间的访问控制关系会受到对方的行为表现所影响呈动态性,且各个实体有自身的主观倾向,无法使用静态的策略进行表达.因此,在网格安全基础设施(GSI)中需要提供:实体间可根据过去相互间直接的或间接的行为接触经验而及时动态地调整更新彼此间的信任关系,从而最大限度地保证网格行为的安全可靠.

人们在 GSI 研究的基础上提出了许多基于策略的授权系统,例如:CAS[2],VOMS[3],Permis[4],Akenti[5]等.这些系统是针对不同的网格应用环境而提供不同的解决方案.但是由于它们都是基于数字证书体系建立起来的,所以它们在授权上都缺少动态性.

另一方面,人们希望所建立的信任模型能更贴切地模拟了人类社会中的信任机制,实体可以搜集、处理、扩散其他实体在该系统中的多方面信息,并建立与其的信任关系,相应地也可以评估其所提供资源或服务的信任,建立起动态的、主观的信任关系.因此,如果将信任度的评估引入到现有的授权机制中,将会有效地增强现有的授权机制的动态性,最大限度地保证网格的安全性.而且信任模型和授权机制的研究都是网格安全中的热点.

信任模型的研究主要集中在 4 个方面:基于凭证的信任管理、自动的信任协商、基于信誉的计算模型、信任和信誉计算模型.其中信任度评估是这些研究的核心.在网格环境下的很多信任模型研究仅仅提出了一个粗略的框架,并没有很好地将网格本身的结构特征融合到信任模型中.文献[6]提出的信任模型忽略了管理域内部实体信任值的不同,模型在判断网格中两个实体之间的信任值的时候,仅根据实体所在的管理域之间的直接信任和推荐信任关系来计算.文献[7]将 EigenTrust 模型应用到了网格中,提出了网格环境下的 Grid Eigen Trust 模型,但是并没有解决 EigenTrust 模型本身的缺点,对于恶意节点的恶意评分以及协同欺诈问题没有很好的解决方案.文献[8]通过多个虚拟组织来建立管理域间实体的信任关系,在虚拟组织中实体通过推荐建立信任关系.但是,模型没能很好地处理虚拟组织中推荐信任值的综合和修改.文献[9]中提出的信任模型利用实体之间的直接信任值和全局信任值来确定两个实体的信任关系,但是模型中没有管理域之间信任关系的确定方法.

因此建立一个完善的分层的信任模型具有现实意义,该信任模型应该能够解决以下问题:利用分层的思想,降低网格信任计算的复杂度;分别考虑域内实体的信任关系,域间实体的信任关系;能很好地处理虚拟组织中推荐信任值的综合和修改,能有效地抑制恶意节点的行为;解决不诚实反馈的问题,这也是本文所要研究的内容之一(见第 2 节).

一个完整的授权机制应该包括任务执行前的授权,执行中的授权和执行后的授权.任务执行前的授权主要是在用户加入虚拟组织或一个系统的时候对用户的角色、权限的定制;执行中的授权指用户在请求服务的时候,权威机构为用户颁发属性声明,资源的提供者或权威机构验证用户授权信息;执行后授

权指当用户完成任务后,服务提供者、用户或权威机构根据双方在执行过程中的行为做出评估,对前面的授权进行修正.上面 4 种网格授权机制(CAS[2]、VOMS[3]、Permis[4]、Akenti[5])都很好地完成了执行中的授权,但是对于执行前的授权实现得不够完善,并且对于执行后的授权没有涉及.

(1)执行前授权实现的不完善性

从体系结构来看,现有的授权机制都是基于策略服务中心的,其中中心服务器负责创建、维护和验证身份、组和角色.其优点在于控制高度集中,单点管理,有灵活的策略标记语言.缺点则是这样的中心服务器是由虚拟组织的管理员或资源提供者人工来维护的,而对于一个虚拟组织来说成员可以动态地加入和退出组织,每加入一个成员都要由管理员来配置组等信息,管理员能拿来作为给成员授权的依据很少(比如只有用户的实体证书),这样可能在不能完全掌握成员信息的状况下就对成员授权,这样的授权是不够精确的且是比较主观、绝对化的.如果恶意的用户得到授权,就可以在虚拟组织中攻击资源.因此,在现有的授权机制上迫切需要一种方法来量化用户和服务的行为,并将其作为依据来动态调整管理员做出的授权策略.

(2)执行后授权的必要性

在现有的授权机制中采用了认证和基于身份的授权来保证网格资源不被破坏.但随着时间的推移以及服务交互的次数的增加,用户和服务之间的信任程度都会发生不同程度的变化.当一个本来可信的用户或服务变成不可信时,授权系统的管理员和资源提供者应该及时发现并做出相应措施,否则会对整个网格系统造成极大破坏.因此,在现有的授权机制中,应该添加判断用户、服务的信任程度及其变化趋势的机制.本文将对这个问题进行探究(见第 3 节).

2　基于行为的分层新信任模型

结合服务网格的结构特征和上节对信任模型的分析,本节提出了一种基于行为的分层信任新模型,并且给出了可行的信任计算和更新的方法,以求克服现有模型在以下两个方面中存在的不足:恶意用户通过使用简单服务对重要服务进行攻击;不诚实的反馈.通过比较和分析,我们的模型是合理并且有效的.

2.1　模型的基本思想

本节提出了基于行为的分层信任新模型,见图 1.该模型分为域间和域内上下两层:下层,即域内,采用全局信任模型,包括域管理者对域内实体在相互协作过程中的行为进行监控、评估,从而确定每一个实体在域内的信任值.这个值也是管理域向网格中其它域声明的域中实体的信任值;上层,即域间,采用局部信任模型,指不同管理域之间的信任、推荐信任关系的建立和修改.在该模型的管理下,网格中的提供者可以根据域间信任、推荐关系和域内实体的信任值来确定两个实体之间的信任关系从而接受或拒绝用户的申请.

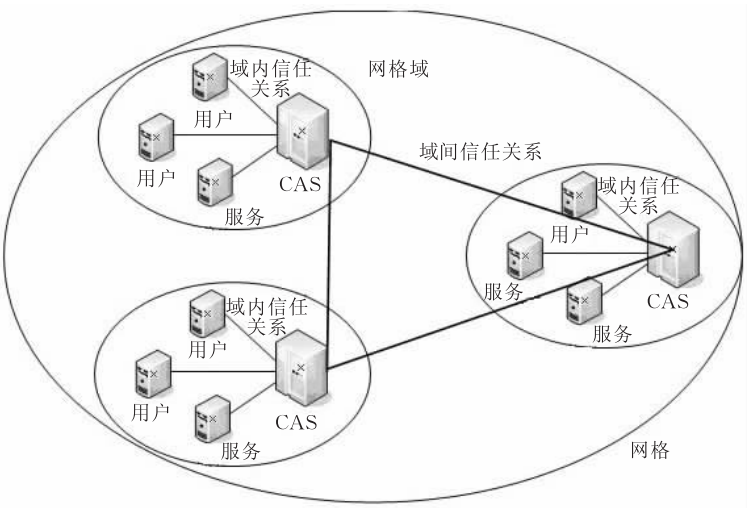

图 1　实体、自治域与网格的关系

2.2　信任度计算

在建立了域内和域间信任关系的管理后,就可以用信任值来具体量化每个域以及域中的用户和服务在网格中的行为,以实现对它们的管理.下面给出我们的新模型所需要的各种信任度的计算方法.

2.2.1 实体域内信任度

定义 1. 实体域内信任度 T_i 表示实体在域内的可信程度.

对于用户可用下面公式来计算和更新 T_i:

$$T_i = \delta \times \frac{\sum_j e_{ji} w_{ij}}{\sum_j w_{ij}} \tag{1}$$

其中,$e_{ji}(0 \leq e_{ji} \leq 1)$为在一段时间 τ(τ 为一时间段,其取值随具体的网络规模而定,可以设为一个月或更长)内用户 i 和服务 j 每次交互之后由服务 j 提供的对用户使用服务后的满意度评价.评价可以根据用户使用服务资源的情况,给出资源的使用的合理性,如:是否消耗了过多的资源,资源的使用的时间长短,使用资源后是否遗留有垃圾数据等.服务 j 可用下面公式来计算满意度 e_{ji}:

$resourceConsumeRate(j,i)$=max{0.01,(服务 j 允许消耗的总资源量−用户 i 实际消耗的资源量)÷服务 j 允许消耗的总资源量};

$garbageRate(j,i)$=max{0.01,(服务 j 允许的垃圾数据−用户 i 实际遗留的垃圾数据)÷服务 j 允许的垃圾数据};

$timeConsumeRate(j,i)$=max{0.01,(服务 j 允许的时间−用户 i 实际消耗的时间)÷服务 j 允许的时间};

$otherConsumeRate(j,i)$=服务 j 给出用户 i 其它使用的合理性;

$$e_{ji} = resourceConsumeRate(j,i) \times garbageRate(j,i) \times timeConsumeRate(j,i) \times otherConsumeRate(j,i). \tag{1.1}$$

该参数为本节各个信任模型所共有的.

参数 w_{ij}、δ、τ 为本模型所特有的参数.w_{ij} 为服务 j 为用户 i 所提供的服务的权值,服务的权值和提供该服务所需要的时间、空间复杂度有关.一般来说,提供服务所需要的时间、空间复杂度越大,相应服务的权值就越高,而且 $w_{MIN} \leq w_{ij} \leq w_{MAX}$,其中 w_{MIN} 和 w_{MAX} 为权值的上、下限,而且当一个域加入网格系统时,它们是从其它已存在域那里继承过来的.而 w_{ij} 的值是在服务加入域的时候,由域的管理员根据服务的描述等信息和根据域本身的策略制定的.该权值的制定主要用来解决问题:在现有的信任模型中,对于恶意用户的攻击考虑不足.

通常恶意用户策略地改变行为方式来对系统中的服务进行攻击,如:恶意用户首先通过良好的交互行为来建立较高的信任值,然后利用建立的信任值突然改变行为进行攻击,并且用户还可以反复地重复上述行为进行恶意攻击.在这种攻击模式下,恶意用户通常选择简单的服务的交互以较小的时间、费用等代价来提高信任值,然后攻击重要服务.现在设置了权值来判断服务的重要程度,可以抑制这样的现象的发生.当恶意用户认为信任度值积累到一定程度时,对重要服务进行攻击,由于重要服务的权值比较高,导致恶意用户的信任度值迅速下降.这样一来,恶意用户再想通过简单服务提高信任度值是非常困难的.这点将在第 5 节实验部分再作说明.

δ 为交互次数影响因子,$0<\delta<1$,并且随着用户使用服务的次数的增加而无限地趋近于 1(如:根据实际情况可以令 $\delta=\frac{m+2}{m+3}$,m 为 τ 内用户使用服务的次数).设置 δ 的意义在于:它是一个和交互次数有关的函数,并随着交互次数的增加而无穷的趋向于 1.这样就能做到让信任度能够更公平表现实体的行为,更符合实际.另一方面,也能鼓励实体多提供服务,因为每多提供一次服务它的信任度就有提升的机会.

对于服务可用下面公式来计算 T_i:

$$T_j = \frac{\delta}{m} \times \sum_i e_{ij} \tag{2}$$

其中,m 为一段时间 τ 内服务 j 提供的服务总次数,e_{ij} 为交互之后由用户 i 对服务 j 提供的服务的满意度评价(见(1.1.1 节)).δ 为交互次数影响因子,且 $0<\delta<1$,并且随着用户使用服务的次数的增加而无限的趋近于 1.

2.2.2 域间直接信任度

域间直接信任度是指两个域中的实体曾经有过直接的交易,从而在两个域之间建立了一种直接信任关系,信任值来源于两个域中的实体的交易情况得出的直接经验.

定义 2. 在服务网格中,设域 i 对域 j 的域间直接信任度为 D_{ij},可由下面公式来计算和更新 D_{ij}:

$$D_{ij} = \delta \times \frac{\sum e_{ij} w_{ij}}{\sum w_{ij}} \tag{3}$$

其中,$e_{ij}(0 \leq e_{ij} \leq 1)$为在一段时间 τ 内(τ 为一时间段,其取值随具体的网络规模而定,可以设为一个月或更长)域 i 内实体和域 j 内实体每次交互之后,域 i 内实体提交的对域 j 内实体的满意度评价(见(1.1.1 节)),1 表示域 i 对域 j 完全满意,0 表示域 i 对域 j 完全不满意,值越大表示满意的程度越高.

w_{ij} 为域 j 为域 i 所提供的服务的权值,服务的权值和提供该服务所需要的时间、空间复杂度有关.一般地,提供服务所需要的时间、空间复杂度越大,相应服务的权值就越高,$w_{MIN}\leq w_{ij}\leq w_{MAX}$,$w_{MIN}$ 和 w_{MAX} 为权值的上、下限.δ 为交互次数影响因子,$0<\delta<1$,并且随着交互次数增加而无限地趋近于 1(如可以令 $\delta=\frac{m+2}{m+3}$,m 为 τ 内 i、j 域的交互次数的).

2.2.3　域间间接信任度

在网格复杂的环境下,当对一个域评估信任的时候,有可能评估者对其一无所知;而且即使是在相对熟悉的情况下,获得的信息越全,越有助于评估.因此,还需要计算由推荐信任形成的域间间接信任度.

定义 3.　当域 i 要得到域 j 域间间接信任度(域间信誉)时,它首先会去寻找在最近的一段时间 τ 内和域 j 进行交互的域集合,并获取他们对域 j 的域间直接信任度,根据域 i 对域集合内的每个域的推荐信任度,综合得出域间间接信任度 RS_{ij},用公式表示如下:

$$RS_{ij}=\sum_{r\in S(j)}\frac{R_{ir}\times D_{rj}}{\sum_{r\in S(j)}R_{ir}} \tag{4}$$

其中,$S(j)$ 为一段时间 τ 内和域 j 进行交互的域集合,但不包括域 i,R_{ir} 为域 i 对域 r 的推荐信任度.

在此我们认为对推荐关系形成推荐信任路径进行过深的研究不仅没有太大的实际意义,反而会降低模型的可操作性.

2.2.4　域间最终信任度

域 i 对域 j 的域间最终信任度 T_{ij} 可用下面公式计算得出:

$$T_{ij}=\lambda\times D_{ij}+(1-\lambda)\times RS_{ij} \tag{5}$$

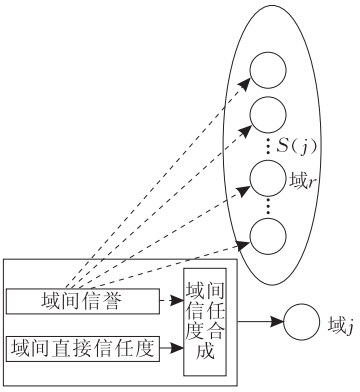

图 2　域间最终信任度的计算

其中,D_{ij} 为域 i 对域 j 的域间直接信任度,RS_{ij} 为域 i 对域 j 的域间间接信任度,λ 为信心因子,λ 的取值和交互的数目有关,交互的数目越多则 λ 取值越大,$0\leq\lambda\leq1$,我们可以取 $\lambda=h/H$,其中 h 为在时间段 τ 内,域 i 和域 j 之间交互的数目,H 为设定的交互数目门槛值.如果出现 $h>H$ 的时候,将 λ 取 1.

2.2.5　推荐信任度

我们认为一个域提供信息的可信程度不能简单地等同于这个域行为(使用或提供服务)的可信程度,于是我们定义了推荐信任度来度量 R_{ir} 来表示域 i 对域 r 提供信息的信任程度,并用它来抑制域之间提供不诚实反馈信息的现象.

设 $DSet(i,r)$ 为在一段时间 τ 内和域 i、域 r 都有过交互的域集合,并且集合中有 n 个元素,则域 i 和域 r 对这 n 个域的域间直接信任度构成了向量:

$$\boldsymbol{V}_i=(D_{i1},D_{i2},\cdots,D_{in})$$

和　$\boldsymbol{V}_r=(D_{r1},D_{r2},\cdots,D_{rn})$(参考图 3).

定义 4.　向量夹角 $\theta=\arccos\frac{\boldsymbol{V}_i\cdot\boldsymbol{V}_r}{\|\boldsymbol{V}_i\|\times\|\boldsymbol{V}_r\|}\frac{1}{2}$

其中,$0^\circ\leq\theta\leq90^\circ$,两向量的内积 $\boldsymbol{V}_i\cdot\boldsymbol{V}_r=\sum_{k=1}^{n}(D_{ik}\times D_{rk})$,向量的长度 $\|\boldsymbol{V}_r\|=\sqrt{\boldsymbol{V}_i\cdot\boldsymbol{V}_r}=\sqrt{\sum_{k=1}^{n}D_{ik}^2}$.

定义 5.

向量长度的相似度

$$\alpha=\begin{cases}\frac{\|\boldsymbol{V}_r\|}{\|\boldsymbol{V}_i\|}, & \|\boldsymbol{V}_r\|\leq\|\boldsymbol{V}_i\|\\ \frac{\|\boldsymbol{V}_i\|}{\|\boldsymbol{V}_r\|}, & \|\boldsymbol{V}_r\|>\|\boldsymbol{V}_i\|\end{cases} \tag{6}$$

方向相似度

$$\beta=1-\frac{\theta}{90^\circ} \tag{7}$$

域间推荐信任度更新计算公式:

$$R_{ir}=\rho\times R_{ir}+(1-\rho)\times\alpha\times\beta \tag{8}$$

其中,$\rho(0\leq\rho\leq1)$ 为信任学习因子,ρ 越小,先前的经验就越容易被遗忘,若 $\rho=0$,那么以前的历史信息就完全被遗忘.

优点:因为域是域内实体综合表现的结果,所以域的行为表现出来的现象就是多变的,即时而表现得诚实,时而不诚实.我们用基于向量夹角的评价方法,能够很好地检测并抑制域在对某些域提供不诚实评价的现象,并且能够避免因为向量夹角相同而长度不同带来的错误判断现象,综合考虑了向量的夹角和长度,这样对域提供信息可信程度的判断将更加准确.

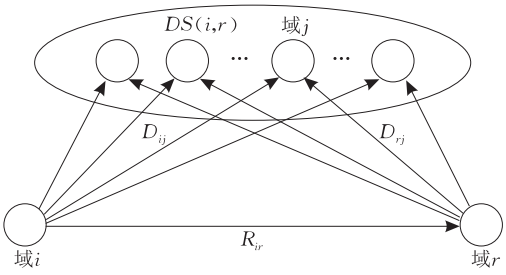

图 3 推荐信任度的评价和更新

3 基于反馈机制的动态授权新模型

3.1 动态授权新模型

基于反馈机制的动态授权新模型是在 CAS 授权框架上进行改进的(如图 4). 可以看出原 CAS 服务器主要实现对于身份授权的管理. 虚拟组织的管理员通过使用命令可以完成虚拟组织的授权策略的初始化,包括了用户的角色、权限等定制. 用户可以通过 CAS 服务器得到授权声明.

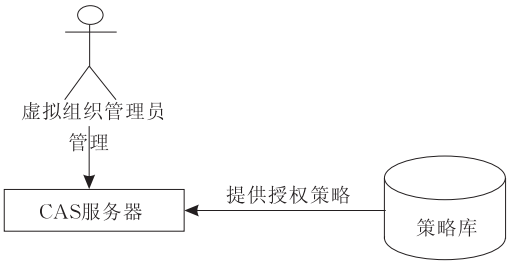

图 4 CAS 授权框架

基于反馈机制的动态授权模型(见图 5)是在 CAS 服务器原有的身份授权管理的基础上,添加了信任度计算机制和反馈机制. 信任度计算机制用来实现第 3 节提出的基于行为的分层信任模型,主要为实现根据行为动态调整角色来提供用户行为的量化值——信任度的计算. 包括查询、更新、转化模块. 查询模块包括对域内用户、服务信任度,域间直接、推荐信任度的查询;更新模块包括对域内用户、服务信任度,域间直接、推荐信任度的更新;转化模块是当出现跨域访问时,用以将外域提供的服务、用户的信任度,综合考虑域间的直接、推荐信任度转化为本域中的信任度值.

反馈机制主要根据信任度计算机制提供的信任度的变化来动态地调整用户的角色. 包括用户角色调整、角色矩阵初始化、角色信任度关系初始化、角色信任度范围检查 4 个模块. 这点将在 3.3 节做详细的介绍.

为了支持新添加的机制,还需要向策略数据库添加了以下几个表:域间直接信任度表(域标识符、信任度、一段时间内权值和等信息),域内服务信任度表(服务 DN、信任度、一段时间内的服务次数等信息),域内用户信任度表(用户 DN、信任度、权值和等信息),域间推荐信任度表(域标识符、推荐信任度等信息),角色-信任度表(角色名称、信任度范围等信息),角色矩阵.

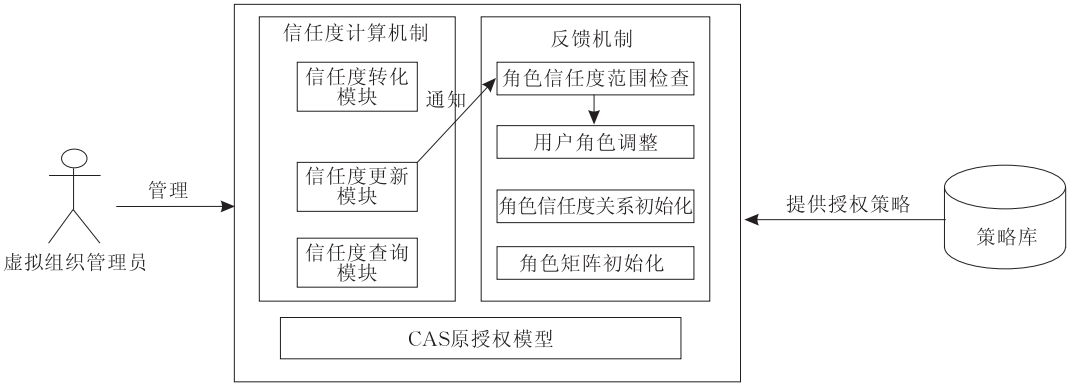

图 5 动态授权新模型的授权框架

3.2 授权流程

3.2.1 域内授权流程

域内授权流程考虑的是用户和服务都在一个虚拟组织中的情况,如图 6 所示.

首先初始化域内用户和服务的信任度值. 在 CAS 服务器初始化时,当管理员添加角色的同时,也为每个角色设定一个信任度变化的区间. 当一个

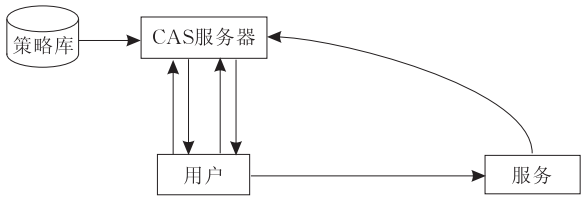

图 6 域内授权流程

用户请求加入虚拟组织时,管理员将用户设置角色,然后用户自动地继承了角色所具有的信任度变化区间的中间值.对于服务的信任度值选取该虚拟组织中服务的信任度值的平均值,因为在服务被使用之前,CAS 服务器没有依据说明虚拟组织对该服务的信任程度,该值设置太高,太低对于服务都是不公平的.下面是授权流程:

(1)用户首先向 CAS 服务器发送查询服务信任度的请求.由于用户通过网格找到能够满足它任务要求的服务不止一个,所以用户提交的查询的服务可能是多个.向 CAS 服务器发送一个签名的 XML 请求,包括 subjectDN、serviceDN、用户持有的代理证书.

(2)CAS 服务器接收到用户的请求后,先检查请求消息的完整性.然后处理用户的查询,返回一个由 CAS 服务器签名的响应消息,包括 subjectDN、serviceDN、trustDegree.

(3)用户接收到消息,选择最合适的服务.

(4)用户发送消息给 CAS 服务器,进行常规的授权(cas-proxy-init 命令).

(5)CAS 服务器端确认用户的身份,将请求中的信息与其策略库比较,综合考虑 VO 和资源所有者的策略控制,然后返回一个签名的 SAML 授权声明,还包括了该用户的信任度.

(6)用户生成一个新的代理证书并将这个声明嵌入到代理证书的扩展项中,然后提交给服务,服务认证后将从 CAS 服务器签发的授权声明中提取用户的信任度,与自己设定的最小值比较.如果大于最小值,则认为用户是可以信任的,则将该声明的其它部分与本地策略及本地委托给 CAS 服务器的策略相比较,响应授权请求.否则,返回失败信息给用户.

(7)当用户使用完该服务的时候,用户和服务都分别对对方使用评估函数进行评价(见式(1)和(2)),服务与用户都必须及时地向 CAS 服务器提交其对与之交互的用户、服务的评价.服务须提供 e_{ji},CAS 通过查找服务信任度表,得到 w_{ij},用户需要提供 e_{ij}.

(8)CAS 服务器根据用户及服务信任度更新的算法对信任度进行更新.

对于用户信任度的更新,步骤如下:

① 根据服务提交的 e_{ji} 及 CAS 查找到的 w_{ij},计算它们的乘积.

② 根据 CAS 数据库中存放的用户信任度表,计算出未更新前的 $\sum_j e_{ji}w_{ij}$,与①的结果相加;将未更新前的 $\sum_j w_{ij}$ 与服务提交的 w_{ij} 相加;将得到的两个值相除,并将结果更新到用户信任度表中.

对于服务信任度的更新,步骤为:CAS 从数据库取出该服务一段时间内的总评价与用户提供的 e_{ij} 相加;将表中存放的次数加 1;将得到的两个值相除,并将结果更新到服务信任度表中.

(9)CAS 服务器根据用户的信任度值的变化,调整用户的角色.这个部分将在反馈机制中给出,此处不详述.

3.2.2　域间授权流程

域间内授权流程考虑的是用户和服务在不同的虚拟组织中的情况,如图 7 所示.

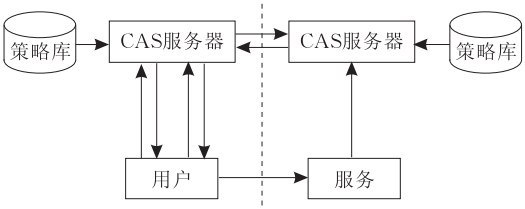

图 7　域间授权流程

(1)用户首先向 CAS1 服务器发送查询服务信任度的请求.由于用户通过网格找到能够满足它任务要求的服务不止一个,所以用户提交的查询的服务可能是多个.向 CAS 服务器发送一个签名的 XML 请求,请求包括 subjectDN、serviceDN、用户持有的代理证书.

(2)本域 CAS1 服务器向用户所请求的服务所在域的 CAS2 服务器发送一个签名的查询服务信任度的请求(由于用户可能提交的是多个相似的服务,而这些服务分布在不同的域),请求包括 subjectDN、serviceDN、本域 CAS1 的 X.509 实体证书.

(3)外域 CAS2 服务器接到请求,确认信任关系,判断消息的完整性后,发送该服务的信任度给本域的 CAS1 服务器.该签名的响应信息包括 subjectDN、serviceDN、trustDegree、外域 CAS2 的 X.509实体证书.

(4)本域的 CAS1 服务器接到消息,确认信任关系,判断消息的完整性后,由公式 $T_{ij}=\lambda\times D_{ij}+(1-\lambda)\times RS_{ij}$ 计算本域对该外域的最终信任度,期间涉及到域间直接信任度、域间间接信任度、推荐信任度的评价的计算.域间的最终信任度与外域提供的服务的信任度综合,得到最终的服务信任度,发送给用户.消息包括 subjectDN、serviceDN、trustDegree、消息由 CAS1 服务器签名.

(5)用户根据本地的策略选择一个最优的服

务,进行常规的授权(cas-proxy-init 命令).

(6)CAS1 服务器端确认用户的身份,将返回一个签名的 SAML 授权声明,包括了该用户的信任度.

(7)用户生成一个新的代理证书并将这个声明嵌入到代理证书的扩展项中;用户使用新的代理证书与外域的 CAS2 服务器交互.外域 CAS2 服务器确认用户的身份,将请求中的信息与其策略库比较,综合考虑 VO 和资源所有者的策略控制,返回一个签名的 SAML 授权声明,包括了该用户的信任度.此信任度的计算方法与步 4 类似.

(8)用户将该授权声明提交给服务,服务认证后将从 CAS2 服务器签发的授权声明中提取用户的信任度,与自己设定的最小值比较.如果大于最小值,则认为用户是可以信任的,则将该声明的其它部分与本地策略及本地委托给 CAS 服务器的策略相比较,响应授权请求.

(9)当用户使用完该服务后,用户和服务对对方使用评估函数进行评价,过程同域内授权流程状况 7.

(10)CAS 服务器根据域间信任度更新的算法对信任度进行更新.

①用户和服务分别将对对方的评价信息发送给其所在域内的 CAS,此处为 CAS1、CAS2.消息包括用户/服务对服务/用户的评价,serviceDN/subjectDN,serviceID/subjectDN,交互完成时间.

②CAS1,CAS2 根据收到的评价信息,使用式(3)更新两交互域之间的直接信任度,其中 w_{ij} 需要交互获得.

③CAS1 和 CAS2 分别给对方发消息,消息包括用户/服务对服务/用户的评价,serviceDN/subjectDN,serviceID/subjectID,交互完成时间.

④CAS1 和 CAS2 接到对方所发的消息后,分别采用式(1)和(2)更新域内用户和服务的信任度,至此信任度更新完毕.

3.3 反馈机制

3.3.1 反馈机制的必要性分析

首先,在 CAS 授权模型中,每加入一个成员都要由管理员来配置组等信息,管理员能拿来作为给成员授权的依据很少,比如只有用户的实体证书,可能在不能完全掌握成员信息的状况下就对成员授权,这样的授权是不够精确的,比较主观和绝对化.其次,随着时间的推移以及服务交互次数的增加,用户和服务之间的信任程度都会发生不同程度的变化.当一个本来可信的用户或服务变成不可信时,授权系统的管理员和资源提供者应该及时发现并做出相应措施,否则会对整个网格系统造成极大破坏.因此,需要反馈机制来实现用户的角色能随着用户的行为自动地变化.当用户的信任度值改变到一定程度时,反馈机制将动态地调节用户的角色,从而达到动态改变用户权限的目的.

3.3.2 反馈机制的设计思想

反馈机制主要是基于以下事实设计的:

(1)从第 2 节的 CAS 的介绍中我们得知,CAS 数据库主要存储有关用户身份、组关系以及权限的相关描述.CAS 将权限授予用户组,也就间接地授权给组中的用户.(用户组相当于角色,只是叫法不同,下文中我们用角色代替用户组)CAS 服务器实现包括了用户、角色、权限、对象等 RBAC 模型的要素.实际上 CAS 的授权机制就是一个复杂的 RBAC 模型.

(2)当一个虚拟组织的 CAS 服务器的管理员为一个用户制定一个角色,也反映了管理员对于用户信任程度的判断.一个用户得到较高的角色,拥有更多的权限,是因为管理员对该用户的信任程度高.

因此,在 CAS 服务器初始化时,当管理员添加角色的同时,也为每个角色设定一个信任度变化的区间.当一个用户请求加入虚拟组织时,管理员将用户添加到角色,用户自动地继承了角色所具有的信任度变化区间的中间值.此后,用户的信任度值会根据一段时间内用户所使用的各个服务对用户的评价发生变化(参考信任度计算部分).当用户的信任度值超出或小于用户角色的信任度区间时,反馈机制会做提升或降低角色的处理.

3.3.3 反馈机制相关算法

在 RBAC 中,角色是核心概念,对角色的基本操作是其角色管理的一个重要方面.当给某个用户授予一定的权限时,需要判断该用户将以什么角色进行访问,该角色处于何种地位,具有什么性质,与其它角色有何关系等,需要进行角色的查找操作.当组织有所变动时,需要对角色集进行角色的添加、删除或修改操作,角色的操作方法直接影响着系统管理的复杂性和工作量.在本文模型的反馈机制部分,实现的是用户的角色能随着用户的行为相应自动地变化,那么首先我们要确定 CAS 数据库中存放的各个角色之间的关系.其次,需要将这些角色之间的关系记录下来,当用户的角色发生变化的时候,能根据角色之间的关系来找到该角色对应的提升和下降的

角色.下面我们将分别完成以上 3 个工作:

(1)角色关系的确定

该部分涉及到反馈机制中角色信任度关系初始化和角色矩阵初始化.当管理员进行虚拟组织初始化配置的同时,需要定义出角色与信任度变化范围之间的对应关系,并添加到策略数据库中,即完成角色信任度关系初始化模块的功能.还需要建立角色之间的层次关系,并添加到策略数据库中,即完成角色矩阵初始化模块的功能.步骤主要为:首先初始化一个空的角色树;其次,在空角色树中添加第一个角色,即根角色,用来表示虚拟组织中最高的权限;再次,根据虚拟组织需要定义其他角色.在角色树的根角色处逐一添加相应的下层各个角色,之后再依次添加其下层角色,直到添加完毕,角色树形成.

因为在 RBAC 中,角色权限之间的关系决定角色之间的关系.角色之间的关系包括:互不相干、包含关系、相交关系和增广关系.

定义 6(互不相干).　对于某角色 r_i,拥有的权限表示为 $r_i \cdot prms$.给定两个角色 r_1 和 r_2,若 $r_1 \cdot prms \cap r_2 \cdot prms = \varnothing$,则称角色 r_1 和 r_2 互不相干.

定义 7(包含关系).　给定两个角色 r_1 和 r_2,若 $r_1 \cdot prms \supseteq r_2 \cdot prms$,则称角色 r_1 包含 r_2,或 r_2 包含于 r_1.

定义 8(相交关系).　给定两个角色 r_1 和 r_2,给定第 3 个角色 r_3,使得 $r_3 \cdot prms = r_1 \cdot prms \cap r_2 \cdot prms$,其中 $r_3 \cdot prms \neq \varnothing$,且 $r_1 \cdot prms$ 和 $r_2 \cdot prms$ 都不是 $r_3 \cdot prms$ 的超集,则称角色 r_1 和 r_2 相交,用 $r_1 \wedge r_2$ 来表示角色间的这种关系.

定义 9(增广关系).　给定 n 个角色 $r_1, r_2, \cdots, r_n$ 和一个角色 r_{n+1},若 $r_{n+1} \cdot prms$ 是 $r_1 \cdot prms$, $r_2 \cdot prms, \cdots, r_n \cdot prms$ 的超集,则称角色 r_{n+1} 和 $r_1, r_2, \cdots, r_n$ 满足增广关系,用 $r_{n+1} = r_1 \oplus r_2 \oplus \cdots \oplus r_n$ 来表示角色间的这种关系.

定义 10(角色关系图).　在以角色为节点的图中,若 r_1 包含 r_2,则存在边 $\langle r_1, r_2 \rangle$,称由此构成的图为角色关系图.图 8 用角色关系图表示了角色间的上述 4 种关系.

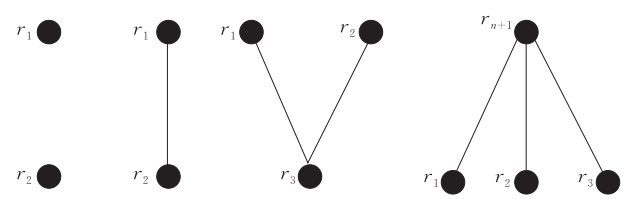

图 8　角色间的 4 种关系

所以建立起来的角色树实际上是一张有向图,如图 9 所示.

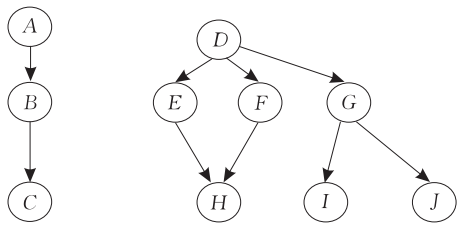

图 9　角色树

本文采用邻接矩阵来存储图的结构.对于图 9 可以制作以下两个邻接矩阵:

$$\begin{array}{c} \\ r_d \\ r_e \\ r_f \\ r_g \\ r_h \\ r_i \\ r_j \end{array} \begin{array}{c} \begin{array}{ccccccc} r_d & r_e & r_f & r_g & r_h & r_i & r_j \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array} \qquad \begin{array}{c} \\ r_a \\ r_b \\ r_c \end{array} \begin{array}{c} \begin{array}{ccc} r_a & r_b & r_c \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \end{array}$$

(2)角色信任度范围检查及用户角色调整

该模型中信任度计算机制将进行信任度的更新.此后,信任度更新模块将向角色信任度范围检查模块发送更新的信息.该模块将对照角色-信任度表、用户信任度表及用户角色表,找出小于或超过定义的信任度范围的用户,并将这些用户的信息(用户标识、角色、角色信任度范围、用户信任度)发送给用户角色调整模块.

用户角色调整模块,依据检查模块发送的消息,参看角色矩阵,对用户的角色进行调整.算法如下.

PROCEDURE newRole adjustRole

(userDN, role, range, trustDegree)

BEGIN

1. //判断用户信任值 *trustDegree* 与角色信任值下限 //*role.range.floor* 之间的关系:

if(用户信任值 *trustDegree*<= 该角色信任值下限 *role.range.floor*)

then 在相应的邻接矩阵中查找角色 role 对应的 n 个行元素,查找其中所有值为 1 的元素所对应的列元素,记录在数组 $r[]$ 中,然后转到步 2;

else if (用户信任值 *trustDegree*> 该角色信任值上限 *range.ceiling*)

then 在相应的邻接矩阵中查找角色 role 对应的 n 个列元素,查找其中所有值为 1 的元素对应的行元素,记录在数组 $r[\ ]$ 中,然后转到(-2);

2. //遍历数组 $r[\ ]$ 中的所有元素 $r[i]$,产生数组 $bag[]$: //在角色-信任度范围表中查找元素 $r[i]$ 对应的

```
        //信任度范围,判断用户信任值是否在该角色所
        //要求的信任值区间内
    if(r[i].range.floor<=trustDegree<=
                        r[i].range.ceiling)
      then 则将 r[i]记录到数组 bag[]中,且继续查找;
           然后转到(3);
3. //判断数组 bag[]:
   if(bag.length==1)   //只找到一个角色
     then 将用户赋予该角色,返回该新角色算法结束;
   if(bag.length>1)//找到多个角色
     then 根据适当规则调整用户为其中一个角色,返
          回该新角色算法结束.规则可以根据实际系
          统情况而灵活定义,比如用户和角色的期望
          信任值的贴近程度等;
   if(bag.length==0 并且数组 r[]为空)
                    //没有找到适合的角色并且已经
                    //到达角色树的顶或底部
     then 发送消息(userDN,null)给管理员,管理员可以
          根据实际情况采取措施(比如创建新角色等);
   else //没有找到适合的角色并且还没到达角色树的
        //顶或底部递归地为数组 r[]中的每个角色元
        //素对象向上或向下寻找上层或下层角色节点;
END
```

其中,对于 $bag.length==0$ 的情况下,需要向上(或向下)查找上或下一层的角色节点,如果没有找到,再查找上或下一层节点,一直下去直到找到 $bag.length$ 不为 0 的节点,或者达到角色树的顶部或底部.这样的话,时间复杂性为 $O(n^2)$.可行性受到影响.但是在我们的模型实际应用中,该模型的基于行为的信任部分的信任度的更新部分是每次服务后就被及时更新的,而且模型中,角色的个数是有限的,角色的信任度值能覆盖[0,1]区间,就是说能够保证每个信任度值都至少对应一个角色,并且随着角色由上到下,其信任度范围是递减的,所以即使在最坏的情况下,也是可以在很短的时间内完成查找.

4 模拟实验

本模拟实验设置了和实际相近的环境,并构造了多个模拟实验来检测我们的模型,验证新信任模型的对行为的敏感性、收敛性、有效性以合理性.在这里我们对用户使用服务的行为和其对服务质量的反馈加以区分.根据用户的行为,我们将其进行了以下分类:

(1)善意行为用户:这类用户在使用服务过程中完全的合作;

(2)静态恶意行为用户:这类用户在使用服务过程中完全的不合作;

(3)动态恶意行为用户:这类用户策略性地改变行为方式来使用服务.

根据用户对服务质量的反馈,我们将其分为以下几类:

(1)诚实反馈用户:这类用户在使用完服务后,能对该服务提供真实可信的评价;

(2)静态不诚实反馈用户:这类用户总是诋毁所使用的服务质量,提供不真实的评价;

(3)动态不诚实反馈用户:这类用户策略性地提供反馈.

实验的模拟环境为 PIV 2.0GHz,512MB.仿真实验代码用 Java 语言编写,IDE 为 eclipse 3.0.1 SDK,对模拟实验中用到的有关参数说明如下:

在实验中模拟一个有 N 个域的网格,在每个域中平均又有 M 个用户和 P 个服务(服务有 Q 种).在每个模拟周期内,每个用户以概率 p 的机会申请某一类服务,其中 $N=200$,$M=3$,$P=2$,$Q=5$,$p=66.7\%$.

本模拟实验主要用于分析新信任模型的有效性和正确性,所以对网格中信息检索功能做了简化处理,使得用户能够方便地找到所有服务和其所在的域信息.

在服务选择策略上采用公平策略,即服务以 $\left(r_i^\alpha/\sum_j r_j^\alpha\right)$ 的概率被用户选上.在这里我们令 $\alpha=1$.

在服务的权值 w_{ij} 的设置上,我们将它简单地分为 3 个等级,分别为非常重要、重要、一般,其权值分别对应为 5、3、1.实体在攻击服务方面他们更倾向于攻击权值较大的服务,并且我们假设他们攻击某服务的概率和该服务的权值成正比.

在信任传递的计算函数上,我们在实验里简单地将其假设为 $f(t_{ij},t_k)=t_{ij}\times t_k/100$.

在模拟实验中,恶意行为用户和不诚实反馈用户分别占用户总数的 30%和 35%.

其它参数,如 τ 取 100 个时间单位,交互次数影响因子 $\delta=\dfrac{m+2}{m+3}$,m 为 τ 时间段内交互的次数.交互数目门槛值 $H=50$,累积信任偏差的阈值 $\theta=3^\circ$.

4.1 交互次数影响因子实验

实验目的:体现交互次数影响因子在用户初始加入网格时对信任值的抑制作用,以防止用户在进行第一次交互后就轻易获得相对于多次交互用户来说较高的信任值.研究用户在加入网格后通过正确地使用服务,并逐渐建立起信任关系的整个过程中,

比较在有无交互次数影响因子的情况下信任度的变化.

图 10 中显示了信任度和交互次数的关系(在不被恶意实体诋毁的情况下),从图中可以看出在实体每次都正确地使用服务的情形下,当在信任度的计算过程中考虑到交互次数影响因子时,信任度随着交互次数的增加,无限地趋向于 1,而在不考虑交互次数影响因子时,信任度的上升是迅速的.前者符合我们的思想:即对于长期提供相同质量服务的实体,它们的信任度因该比短期内提供该质量服务的实体的信任度高,也就是说我们更看中实体长期的表现,并且鼓励实体多提供服务.

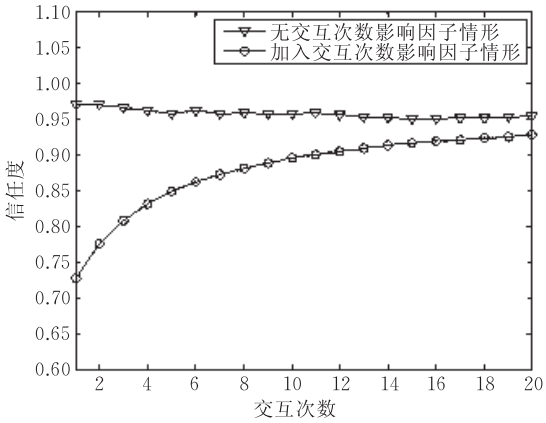

图 10　模拟实验 1 结果

4.2　服务权值实验

本实验考察服务权值对模型的影响,即研究用户在网格中经过一段时间地交互并积累一定的信任关系以后,突然对网格中重要服务进行攻击,并在之后企图通过普通服务迅速提高信任关系的整个过程中,服务权值对信任度变化的影响.

图 11 中显示了如果用户对网格中的重要(权值较高的)服务进行了攻击,他的信任关系将迅速下降,并将很难在短期内通过频繁的提交高质量的普通(权值较低的)服务,来改善他的信任关系,而不是像在没有权值的情况下,信任度能够迅速上升.这样能使用户不攻击重要服务或尽可能少地攻击重要服务,即在某种程度上保护了网格中的重要服务.

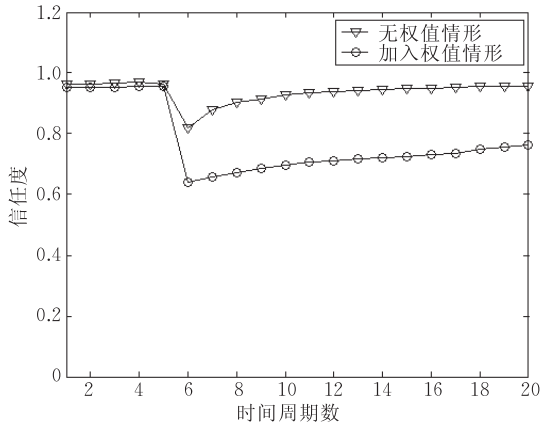

图 11　模拟实验 2 结果

4.3　新模型对网格中恶意实体行为的抑制

本次实验是在网格中存在 30% 恶意行为实体的情况下,观察比较网格中实体在无信任机制情形和新模型存在时网格中服务的失败比率随时间周期的变化情况.并以此为基础分析新模型的有效性.结果如图 12 所示.

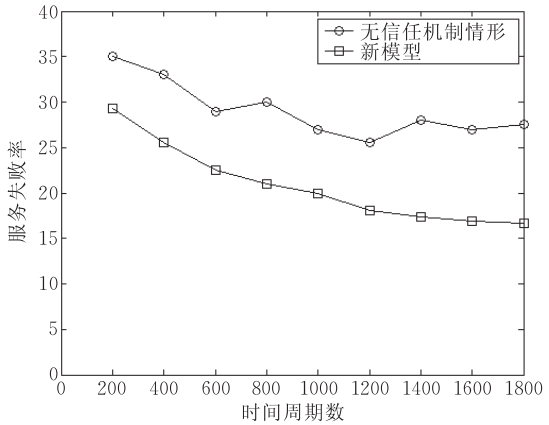

图 12　模拟实验 3 结果

如图 6 所示,在无信任机制的情形下,由于网格中没有一种检测机制对恶意行为实体进行检测和必要的惩罚机制来实现对恶意实体行为的抑制,所以恶意实体继续着他们的行为.从图上可以看出随着模拟周期的增加,网格中服务的失败率和开始时变化不大.然而在新模型中,因为存在信任机制时,可以通过实体之间交互的评价来反映对方的行为,检测出恶意实体并降低了他们的信任度,这使得他们对服务的使用变得困难,从而抑制了有恶意行为实体的对服务的使用,使得网格中服务的失败率有明显的下降,比较上述两种情形可以看出新模型能够有效检测和抑制网格中恶意实体的行为,提高了网格中服务的成功率.

5　结　论

本文首先在研究网格中信任模型的基础上,提出了一种以信任度为决策依据的信任模型.该模型与以前的模型相比,提出使用服务权值区分重要服

务和普通服务,从而保护了网格中的重要服务并且能有效地抑制了恶意节点通过多次交互普通服务提高信任度的意图;采用基于矢量比较的方法计算域间推荐信任度,解决不诚实反馈的问题;最后,结合提出的信任模型,对 CAS 现有的授权机制进行改进,给出了基于反馈机制的动态授权模型.该模型在 CAS 基于身份的授权基础上,增加了基于信任度的授权和反馈机制,很好地解决了现有机制的静态性的缺点,实现根据用户的行为动态调整他的角色.

本文的工作还只是一个起步的工作,网格的复杂性决定了我们还必须不断完善我们的工作:

(1)本文所提出的基于行为的分层信任模型存在着不足:模型对于协同不诚实反馈的现象不够敏感,特别是当这些提供不诚实反馈的实体分布在多个域中时,这一现象就会更为明显.因为域内用户与服务之间的交互会影响域间的信任关系,诚实可靠的交易会.域间的用户和服务之间可能通过协同欺骗故意提高或降低域与域之间的信任值,从而增强或降低其在推荐信任中的影响度,即可能利用较大的推荐值来操纵计算结果,此时模型的性能较差.因此对协同不诚实反馈抑制的研究将是我们下一步研究的工作.

(2)本文所提出的基于反馈机制的动态授权模型是基于分布式信任假设,认为处于不同信任域的授权系统可以在有限时间内通过认证建立信任关系,但是在实际的网格环境下,域间的信任关系很难建立.所以,提供一个更有效的分布式的信任机制将成为我们的下一步研究工作.

参 考 文 献

[1] Dou Zhi-Hei, Chen Yu, Liu Peng et al. Grid Computing. Beijing: Tsinghua University Press, 2002
(都志辉, 陈渝, 刘鹏等. 网格计算. 北京: 清华大学出版社, 2002)

[2] Pearlman L, Welch V, Foster I et al. A community authorization service for group collaboration//Proceeding of the IEEE Workshop on Policies for Distributed Systems and Networks. California, 2002: 50-59

[3] Alfieri R, Cecchini R, Ciaschini V et al. From gridmap-file to VOMS: Authorization in a grid environment. Future Generation Computer Systems, 2005, 21(4): 549-558

[4] Chadwick D W, Otenko A. The PERMIS X.509 role based privilege management infrastructure. Future Generation Computer Systems, 2003, 19(2): 277-289

[5] Thompson M, Johnston W, Mudumbai S et al. Certificate-based access control for widely distributed resources//Proceeding of the 8th USENIX Security Symposium. Washington, 1999: 215-228

[6] Azzdin F, Maheswaran M. Integrating trust into grid resource management systems//Proceeding of the 2002 International Conference on Parallel Processing (ICPP'02). Vancouver, British Columbia, Canada, 2002: 47-54

[7] Alunkal B, Veljkovic I, Laszewski G. Reputation-based grid resource selection//Proceeding of the Workshop on Adaptive Grid Middleware. USA, 2003: 1-10

[8] Li T Y, Zhu H F, Lam K Y. A novel two-level trust model for grid//Proceeding of the ICICS, 2003: 214-225

[9] Gui X I, Xie B, Li Y N et al. Study on the behavior-based trust model in grid security system//Proceedings of the 2004 IEEE International Conference on (SCC'04), 2004: 506-509

[10] Pearlman L, Welch V, Foster I et al. A community authorization service for group collaboration//Proceedings of the IEEE Workshop on Policies for Distributed Systems and Networks. California, 2002: 50-59

[11] Chadwick D W, Otenko A. The PERMIS X.509 role based privilege management infrastructure. Future Generation Computer Systems, 2003, 19(2): 277-289

[12] Thompson M, Johnston W, Mudumbai S et al. Certificate-based access control for widely distributed resources//Proceedings of the 8th USENIX Security Symposium. Washington, 1999: 215-228

[13] Thompson M R, Essiari A, Mudumbai S. Certificate-based authorization policy in a pki environment. ACM Transactions on Information and System Security, 2003, 6(4): 566-588

[14] Pearlman P, Kesselman C, Welch V et al. The community authorization service status and future//Proceedings of the Computing in High Energy and Nuclear Physics. California, 2003: 1-9

[15] Markus Lorch, Bob Cowles, Rich Baker et al. Conceptual grid authorization framework and classification. Global Grid Forum, 2004: 21-22

[16] Cannon S, Chan S, Olson D et al. Using CAS to manage role-based VO sub-groups//Proceedings of the Computing in High Energy Physics. La Jolla, California, 2003

[17] Alfieri R, Cecchini R, Ciaschini V et al. Voms: An authorization system for virtual organizations//Proceedings of the 1st European Access Grids Conference. Santiago de Compostela, 2003: 33-40

LI Ming-Chu, born in 1963, Ph.D., professor, Ph. D. supervisor. His main research area includes information security, graph theory, grid computing, computational Complexity.

YANG Bin, born in 1978, M. S. candidate. Her research interest is in information security.

ZHONG Wei, born in 1978, M. S. candidate. His research interest is in Information Security.

TIAN Lin-Lin, born in 1979, lecturer. Her main research area includes information security and cryptography.

JIANG He, born in 1980, Ph. D. , associate professor. His main research interest includes algorithms and complexity, intelligent computing.

HU Hong-Gang, Ph. D.. His main research area includes information security and cryptography,

Background

The study of authorization model is an important research area in information security, and many authors are interested in the topic, and many results have been obtained. There is a problem of static status in the existing authorization systems of grids that don't provide feedback mechanism to feedback the use of permission by users. When a user or a service with creditability at the past would become unlikelihood, the authorization systems could not find this status in time to adjust the user's permission, so that it is possible for malicious users to destroy the grid systems. Thus, building feedback mechanism in authorization to adjust users' roles by their behavior dynamically is necessary to the security of grid systems.