基于模糊集合的网格资源访问的信任机制

陈建刚[1)] 王汝传[1),2)] 张 琳[1)] 王海艳[1)]

[1)](南京邮电大学计算机学院 南京 210003)

[2)](南京大学计算机软件新技术国家重点实验室 南京 210093)

摘 要 针对网格环境的特点,分析了资源访问过程中所遇到的信任管理问题,通过引入管理域内和管理域间的实体间的信任关系,结合信任的主观性特点,提出了基于模糊集合的网格资源访问信任机制,即通过建立信任链路和模糊算子的合成规则得到用户对资源访问点的信任关系,并与用户要求的信任策略相比较,从而决定是否访问资源.最后建立了网格的信任体系模型.

关键词 网格计算;模糊集合;信任关系;管理域

中图法分类号 TP393 **DOI 号**: 10.3724/SP.J.1016.2009.01676

The Resource Access Mechanism in Grid Based on Fuzzy-Trust

CHEN Jian-Gang[1)] WANG Ru-Chuan[1),2)] ZHANG Lin[1)] WANG Hai-Yan[1)]

[1)](*Institute of Computer Science, Nanjing University of Post and Telecommunications, Nanjing* 210003)

[2)](*State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing* 210093)

Abstract This paper analyses the question about trust management during the access to grid resources. Through introduction of trust relation among the entities of the intra-domain and inter-domain, the subjective property of trust relation considered, the trust mechanism of resource access in the grid computing based on the fuzzy set is proposed, that is, the user for resource access builds the recommendation trust links and computes the synthetical trust relation based on the synthesis rules of the fuzzy arithmetic operators and through comparing with the trust policy of the user to decide whether to use the resource. At last, the paper gives the grid trust model.

Keywords grid computing; fuzzy set; trust relation; management domain

1 引 言

网格计算技术最早起源于高性能计算,是一种崭新的资源共享和协同应用模式,最近的网格计算逐步向商业计算演化,Web 服务技术成为主流网格计算技术的基础.网格计算的安全主要是作为早期网格计算工具箱的一个功能模块提供的.由于网格环境的大规模性、异构性、分布性、动态性和开放性等特点,随着网格计算技术的逐渐发展,过去的安全技术或者措施已经不能适应网格应用的需要,尤其是安全授权机制,如访问控制列表、一些传统的公钥证书体系等,很难在网格环境中成功实施.人们迫切需要对网格计算的安全策略进行专门的系统研究,

收稿日期:2006-09-18;最终修改稿收到日期:2008-12-25.本课题得到国家自然科学基金(60573141,60773041)、国家"八六三"高技术研究发展计划项目基金(2006AA01Z201,2007AA01Z404,2007AA01Z478)、江苏省自然科学基金(BK2008451)、江苏省高技术研究计划(BG2006001)、现代通信国家重点实验室基金(9140C1105040805)、江苏省高校自然科学研究计划(07KJB520083)、江苏省博士后基金(0801019C)、江苏高校科技创新计划项目(CX08B-085Z,CX08B-086Z)资助.**陈建刚**,男,1978 年生,博士研究生,主要研究方向为网格计算、信息安全等.**王汝传**,男,1943 年生,教授,博士生导师,主要研究领域为计算机软件、计算机网络和网格、信息安全、无线传感器网络、移动代理技术等.E-mail: wangrc@ njupt.edu.cn.**张 琳**,女,1980 年生,博士研究生,主要研究方向为计算机网络和网格技术、信息安全等.**王海艳**,女,1974 年生,博士研究生,主要研究方向为计算机软件、信息安全等.

并针对新的网格计算需要提出新的方法和思路.

近年来,国外很多研究机构针对 P2P、Ad hoc 等开放网络体系展开了信任机制的研究,以克服传统安全机制的缺陷[1-2].信任管理机制也是网格安全的一个重要组成部分,是其它安全设施执行的重要前提.目前基于行为的网格信任模型由 Azzedin 提出[3-4],该基于行为的网格信任模型以信任和声望作为度量,提出了用一个信任中介系统来扩展网格信任的范围.但这种信任机制没有考虑到主观信任的模糊性特点,参照通常社会网络中的信任关系,这种主观性的信念应该是建立在模糊集合的基础上加以描述和验证[5].

网格计算的本质是资源共享和协同服务,网格计算集成了各类资源(如不同部门的高性能计算机、各种专业软件等),这些资源分散在各个不同的管理域中.网格资源访问是指借助于网格计算中所提供的共享资源执行用户所提交的作业任务的过程.在执行这种网格资源访问过程时,首先需要建立用户和资源提供者之间的信任关系.从用户角度考虑,为了保证用户所提交作业不至在恶意的资源节点上运行,用户需要建立对资源节点的信任关系;从资源角度考虑,为了保证资源不被用户所提交的恶意作业所破坏,资源需要建立对用户的信任关系.只有用户和资源所建立的信任关系达到双方的信任期望程度时,才可以产生资源访问过程.本文就针对这种场景,通过引入模糊信任机制来分析两者信任关系的建立.同时这种信任机制也很容易推广到不同实体间的交互协作过程中所遇到的信任问题.

本文第 2 节引入网格计算环境的信任关系;第 3 节讨论基于模糊集合的资源访问信任关系;第 4 节讨论该信任关系的建立过程;第 5 节总结资源访问的信任关系模型;第 6 节对基于模糊集合的信任关系进行模拟实验;第 7 节是本文的总结.

2　网格计算环境的信任关系

定义 $D=\{D_0,D_1,D_2,\cdots,D_n\}$ 为组成网格的不同管理域,$D_i=\{d_i^0,d_i^1,d_i^2,\cdots,d_i^m\}$ 为管理域 D_i 中不同实体.根据网格环境的特点,我们将网格中的信任关系分为直接信任和声望信任两种,直接信任是指两个实体根据过去发生的直接交往行为而得出的信任等级关系[3],这种交互包括实体间协作完成某项任务、用户使用资源提交作业等,也包括电子商务类型的商业服务,而不包括一般的访问浏览服务.由于实体分别属于不同的管理域,因而实体间的信任关系有域内和域间之分,相应地,直接信任也分为域内直接信任(Intra-Domain Direct Trust,IaDDT)和域间直接信任(Inter-Domain Direct Trust,IeDDT).直接信任关系由于只是涉及到和该实体发生交互关系的实体,而当该实体很少与其它实体交互,或者交互的实体怀有恶意,伪装成诚实实体交互,或者这些实体合谋进行欺骗行为时,后面建立的对别的实体的信任关系将完全不可靠,因而直接信任只能作为局部信任关系[6],需要再引入声望信任,用于维护全局信任关系.声望信任是指通过管理域中有声望实体的推荐而得出的信任等级关系.我们在每个管理域中引入一个信任服务提供者(Trust Service Provider,TSP)来表示这种实体.信任服务提供者(TSP)维持着两种信任关系:对本管理域各成员的信任关系和对其它管理域中的 TSP 的信任关系,分别对应于域内声望信任(Intra-Domain Reputation Trust,IaDRT)和域间声望信任(Inter-Domain Reputation Trust,IeDRT).假设管理域内的实体总是完全信任本管理域的 TSP,因而每个实体都只需维护一张直接信任关系表(Direct Trust Table,DTT),用来记录与该实体发生直接交互形成的 IaDDT 和 IeDDT;同时 TSP 也维护着一张声望信任表(Reputation Trust Table,RTT),该表分别记录着 IaDRT 和 IeDRT.

3　基于模糊集合的网格资源访问信任关系

在网格资源访问过程中,用户为了使自己利益不遭受恶意破坏,需要对资源进行多方面的考虑(如该资源是否可靠等),即对资源的各种属性提出要求,建立属性集 $ATTR$:{诚实性($attr_0$),资源运行的可靠性($attr_1$),资源的易用性($attr_2$),容错性($attr_3$),运行效率($attr_4$),成功率($attr_5$)…},用 $ATTR=\{attr_0,attr_1,attr_2,\cdots,attr_n\}$ 表示,其中 $attr_i$ 表示用户对资源提供者进行评判的第 i 种属性.诚实属性($attr_0$)是用户使用该实体作为推荐者建立信任链路的一个重要参数.对于每一种属性,我们都建立相应的信任关系,采用自然语言来刻画信任等级[5],即建立信任域 $U=\{u_0,u_1,\cdots u_4\}$ 如下:

u_0 表示“完全信任”;u_1 表示“非常信任”;

u_2 表示“一般信任”;u_3 表示“有点信任”;

u_4 表示“不信任”.

在此并没有像文献[7]中的主观逻辑那样引入不确定的信任关系,因为用模糊论的观点,这种划分本身就反映了不确定因素.

令$\underset{\sim}{\boldsymbol{A}}(u,attr_i,t,c)=\mu_{\underset{\sim}{\boldsymbol{A}}}(u_0,u_1,\cdots,u_4,d_p^s\rightarrow d_q^t,t,c,attr_i)=\{a_{i0},a_{i1},\cdots,a_{i4}\}$表示实体$d_p^s$对实体$d_q^t$的属性$attr_i$在时间$t$,上下文$c$下评判的信任向量,其中$a_{iw}(w=0,\cdots,4)$表示$u_w(w=0,\cdots,4)$的隶属度.因而不同属性集的信任度评价就构成了模糊关系$\underset{\sim}{\boldsymbol{R}}$,得到模糊矩阵为

$$\underset{\sim}{\boldsymbol{R}}=\begin{bmatrix}a_{00} & a_{01} & \cdots & a_{04}\\ a_{10} & a_{11} & \cdots & a_{14}\\ \cdots & \cdots & \cdots & \cdots\\ a_{n0} & a_{n1} & \cdots & a_{n4}\end{bmatrix},$$

$\underset{\sim}{\boldsymbol{R}}$称为属性评判矩阵,$(ATTR,U,\underset{\sim}{\boldsymbol{R}})$构成一个综合评判模型,称为综合评判空间[8].

在每一次交互结束后,用户根据交互过程中对各个属性的满意程度进行相应评判,给出每个属性信任向量的隶属度.这种评判结果可以根据隶属函数$\underset{\sim}{\boldsymbol{A}}(u,attr_i,t,c)$来确定,隶属函数的确定主要考虑如下参数:交互权限(P)、交互的时间长短(T)和交互次数(N)等,交互权限是指资源提供者允许用户利用资源所从事操作的权限,这些操作包括查看资源、使用资源、更新资源等,定义权限集合$P=\{p_0,p_1,p_2,\cdots,p_n\}$,这些权限的关系为$p_0\subset p_1\subset p_2\subset\cdots\subset p_n$表示后一种操作权限包含前一种操作权限,如获得更新资源的权限同样也拥有查看、使用资源的权限.这些权限反映了使用者对资源提供者的熟悉程度.同样交互时间长短、交互次数多少也反映了用户对资源提供者的熟悉程度,因为按博弈论观点,当交易双方仅发生单次交易时,必然会出现损人利己行为,而随交易次数增加,对长期利益的考虑导致诚信交互的出现,长期信任机制便得以形成.三者对$U=\{u_0,u_1,\cdots,u_4\}$的影响体现在交互时间短而权限低、次数少时,不信任隶属度就应该更大些.交互权限、交互次数等参数用上下文c来表示.另外,不同属性的隶属函数与属性本身的特点也有关.隶属函数的确定有很大的主观性,在建立时需要综合考虑到上面几个因素.设$\underset{\sim}{\boldsymbol{A}}_{\text{act}}(u,attr_i,c,t)$表示本次交互过程所确定的对对方的信任向量隶属度,结合交互前的信任向量隶属度$\underset{\sim}{\boldsymbol{A}}(u,attr_i,t_{\text{past}},c)$,得到交互后的信任向量隶属度$\underset{\sim}{\boldsymbol{A}}(u,attr_i,t,c)$:

$$\underset{\sim}{\boldsymbol{A}}(u,attr_i,t,c)=(1-\delta)\underset{\sim}{\boldsymbol{A}}(u,attr_i,t_{\text{past}},c)\oplus\delta\underset{\sim}{\boldsymbol{A}}_{\text{act}}(u,attr_i,t,c)\quad(1)$$

其中$\delta\in[0,1]$,$\oplus$表示模糊"或"算子,考虑到权重因子δ,$\oplus$可以取普通实数"+"运算.可以理解,当交互的时间t越长,δ越大.最后用$\underset{\sim}{\boldsymbol{A}}(u,attr_i,t,c)$更新直接信任表.

另外,综合信任度也是实体间整体信任度量的一个反映,因而也需要计算,令

$$\underset{\sim}{\boldsymbol{A}}(u,t,c)=\mu_{\underset{\sim}{\boldsymbol{A}}}(u_0,u_1,\cdots,u_4,d_p^s\rightarrow d_q^t,t,c)=\{a_0,a_1,\cdots,a_4\}$$

表示实体d_p^s对实体d_q^t在时间t,上下文c的综合信任向量,其中$a_w(w=0,\cdots,4)$表示实体d_p^s对实体d_q^t的综合隶属度.根据$ATTR$中各属性的不同权重,建立权重因子模糊集$\underset{\sim}{\boldsymbol{Q}}=(q_1,q_2,\cdots,q_n)$,其中$\sum_{i=1}^{n}q_i=1$,模糊集$\underset{\sim}{\boldsymbol{Q}}$可以用判断矩阵分析法[8]来确定.

在$\underset{\sim}{\boldsymbol{R}}$与$\underset{\sim}{\boldsymbol{Q}}$确定后,则综合评判为

$$\underset{\sim}{\boldsymbol{A}}(u,t,c)=\underset{\sim}{\boldsymbol{Q}}\circ\underset{\sim}{\boldsymbol{R}}=\{a_0,a_1,\cdots,a_4\},$$

其中$a_j=\overset{n}{\underset{i=1}{\overset{+}{\overset{\cdot}{*}}}}(q_i\overset{\cdot}{*}a_{ij})$,$(j=0,1,\cdots,4)$,而$(\overset{\cdot}{*},\overset{+}{*})$为广义模糊"与"和"或"算子[8],在对权重因子集$\underset{\sim}{\boldsymbol{Q}}$归一化后,可以取普通实数的$(*,+)$.同样与式(1)相似,可以更新综合信任表项$\{a_0,a_1,\cdots a_4\}$.

根据前面分析,构造的直接信任表如表1所示,表中包含的数据结构为

{{各属性的信任向量隶属度,综合信任向量隶属度},
交互时间(T),交互权限(P),交互次数(N),
身份标识(ID)},

从表1中就能够确定对交互实体的信任关系,因而在进行下次交互时就可以参考这种信任关系来决定是否进行交互.

表1 直接信任表

	信任关系的隶属度								交互时间(T)	交互权限(P)	交互次数(N)	身份标识(ID)
	$attr_0$			…	…	综合信任评价						
	u_0	u_1	u_2	…		u_0	u_1	u_2	…				
IaDDT												
IeDDT												

而TSP的声望信任表(RTT)只是提供一个全局信任作用,给出的是本TSP对对方的诚实属性的评价,这种评价是根据综合各实体的信任关系来确定,其信任表结构如表2所示.

表 2　声望信任表

	信任关系的隶属度					时间 (T)	身份标识 (ID)
	u_0	u_1	u_2	u_3	u_4		
IaDRT							
IeDRT							

信任表中的时间(T)是更新信任值时间,根据人们的经验,信任关系随着时间而衰减[3],我们定义时间衰减函数:

$$\psi(u_i,t-t_f,c)=\mathrm{e}^{\frac{-(t-t_f)}{b_i}},\quad t\geq t_f \tag{2}$$

其中,t_f是上次交互(更新)时间,参数 b_i随 u_i而变,对于 u_0(完全信任),随着时间的推移应该衰减较快,因而 b_0也相应的要小些,而对于 u_4(不信任)则随时间推移反而应该增加,因而 b_4也相应要大. 身份标识(ID)则表明是对哪个实体的信任评价.

4　资源访问的信任关系建立过程

在网格环境中,处于不同管理域的交互双方的信任关系建立过程如图 1 所示,设管理域 D_0的用户 d_1^0需要访问 D_5的资源提供者 d_5^0提供的资源,规定 4 种信任关系表示形式如下:

IaDDT: $d_1^0\rightarrow d_1^1$;

IeDDT: $d_1^0\Rightarrow d_5^0$;

IaDRT: $TSP_1\mapsto d_1^0, d_1^0\mapsto TSP_1$;

IeDRT: $TSP_1\models TSP_2$.

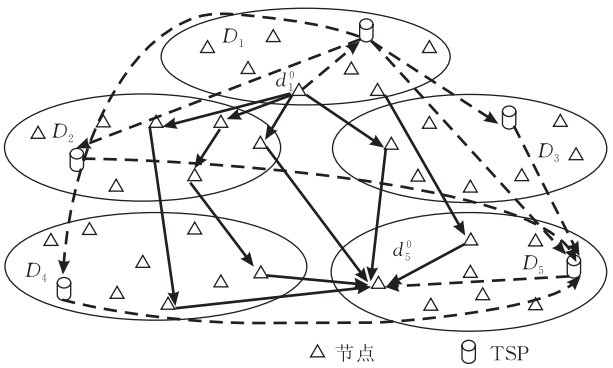


图 1　网格环境下信任链路的建立

根据前面假设,$d_1^0\mapsto TSP_1$总是完全信任的,即 $\underset{\sim}{\boldsymbol{A}}(u)=\mu_{\underset{\sim}{\boldsymbol{A}}}(u_0,u_1,\cdots,u_4,d_i^s\mapsto TSP_i)=\{1,0,0,0,0\}$,规定只有用户可以查询该域的 TSP 来建立信任链路,而在建立信任链路过程中,中间实体则不必再次查询其管理域内的 TSP,这种假设目的是避免中间实体在链路上多次出现,使信任关系链路过于复杂.

从图 1 可看出从用户出发有如下 2 类路径:

声望信任路径:

$d_1^0\mapsto TSP_1\models TSP_2\models\cdots\models TSP_5\mapsto d_5^0$;

直接信任路径:

$d_1^0\rightarrow(\Rightarrow)d_1^1\rightarrow(\Rightarrow)d_2^0\rightarrow(\Rightarrow)\cdots\rightarrow(\Rightarrow)d_5^0$,

因而在计算路径信任度时要对这 3 种信任关系进行带权重合成,并且在建立链路时应该对直接信任、声望信任这两种信任分别进行搜索.

用户根据自己需要交互的情况,对资源实体的不同属性有相应的信任等级需求,在进行信任匹配时,我们将用户所要求的条件以策略的形式来表示,即

$$Policy\{\{\underset{\sim}{\boldsymbol{A}}(u,attr_0),\underset{\sim}{\boldsymbol{A}}(u,attr_1),\cdots,\underset{\sim}{\boldsymbol{A}}(u)\},\bar{p}\},$$

其中$\{\underset{\sim}{\boldsymbol{A}}(u,attr_0),\underset{\sim}{\boldsymbol{A}}(u,attr_1),\cdots,\underset{\sim}{\boldsymbol{A}}(u)\}$表示对不同属性的信任等级需求和综合的信任等级需求,$\bar{p}$表示期望的交互权限.

使用如下搜索步骤建立直接信任链路:

1. 用户 d_1^0查询 DTT 表,找出诚实属性($attr_0$)中信任分量 u_0的隶属度 $a_{00}\geq\lambda$ 的前 m 个最大值的实体$\{d_i^0,d_j^1,d_k^2,\cdots\}$,并对每个实体都发送消息:

$\{\langle d_1^0,d_5^0\rangle,length\leq l_0,t\geq t_0,a_{00}\geq\lambda,\{d_i^0,d_j^1,d_k^2\cdots\}\}$.

//其中 l_0表示搜索路径的最大长度,t_0表示交互的最早时//间,而 λ 表示对 a_{00}取值的阈值.

对于每个实体 d_i^0

2. 先用时间衰减函数 $\psi(u_i,t-t_f,c)$更新 $attr_0$,

3. 查找 DTT 表,是否有目的实体 d_5^0,若有,则返回初始实体 d_1^0消息:

$\{\langle d_1^0,d_i^0\rangle,\langle d_i^0,d_5^0\rangle,\underset{\sim}{\boldsymbol{A}}(u,attr_i,d_i^0\rightarrow d_5^0,t,c),\underset{\sim}{\boldsymbol{A}}(u,d_i^0\rightarrow d_5^0,t,c),p\}$.

//返回信任路径、对目的节点的各种属性的信任值、综合信//任值和交互权限.

存储消息$\{\langle d_1^0,d_5^0\rangle,length\leq l_0,t\geq t_0,a_{00}\geq\lambda\}$.

//若后面还有相似搜索路径经过该实体,则中止该路径搜索.

//该实体完成搜索.

4. 若无,则查找其 DTT 表中交互实体集合去掉$\{d_i^0,d_j^1,d_k^2\cdots\}$集合中的实体,同样找出满足 $t\geq t_0,a_{00}\geq\lambda$ 的诚实属性($attr_0$)中 a_{00}最大值的实体 d_i^1,并对该实体发送消息:

$\{\langle d_1^0,d_i^0\rangle,\langle d_1^0,d_5^0\rangle,\langle l,l_0\rangle,t\geq t_0,a_{00}\geq\lambda,\{d_i^0,d_j^1,d_k^2,\cdots,d_i^1\},a_{00}(d_i^0\rightarrow d_i^1)\}$.

//l 表示当前路径长度,$a_{00}(d_i^0\rightarrow d_i^1)$表示实体 d_i^0对实体 d_i^1//的诚实属性($attr_0$)信任分量 u_0的隶属度

存储消息$\{\langle d_1^0,d_5^0\rangle,length\leq l_0,t\geq t_0,a_{00}\geq\lambda\}$.

对于实体 d_i^1,先检查 $l+1$ 是否大于 l_0,若大于,则停止搜索.

若小于,重复上面步 2～4,只是消息内容要做些改动.

同样类似地可建立声望信任链路,由于 TSP 只保存诚实属性信任向量隶属度,因而这些链路只是

用于检验资源提供者的诚实属性.

链路中最后实体给出了目的实体的诚实属性($attr_0$)的信任度评判,因而首先可以根据这些信任值剔除掉那些带欺骗行为的实体.假设没有大范围的欺骗行为(事实上,搜索路径中的中间实体都只参与其中一条链路,这样就尽量减少了欺骗行为的蔓延),只是单独的欺骗行为,因而带欺骗行为的路径上的最终实体给出的对目的实体诚实属性($attr_0$)信任隶属度,和没有欺骗行为的实体给出的诚实属性($attr_0$)信任隶属度相差很大,可进行如下步骤进行筛选:

1. 若 $p_i \subset \bar{p}$,则去掉该链路,其中 p_i 为返回的各条链路消息中的交互权限;

2. 根据最大隶属度原则,将每条链路消息中的对目的实体的诚实属性信任向量隶属度转化成信任等级,即若 $a_{0w}(d_i^0 \to d_5^0) = \max\{a_{00}, a_{01}, \cdots a_{04}\}(w=0,1,\cdots,4)$,则将 $d_i^0 \to d_5^0$ 的诚实属性归为 u_w,即将该链路归为 u_w 信任等级;

3. 统计出各条链路处于不同信任等级的数目;

4. 去掉那些处于信任等级数目最少的相应链路.

//被认为是带欺骗行为的链路

对于剩下的信任链路,需要进行各种属性的信任向量合成运算,在对信任向量进行运算时,相应模糊算子的选取很重要,因为要能够反映参加运算的各个实体的信任度,所以不能仅仅选择查德算子来运算,采用概率算子来作为模糊算子[8].

定义 1. 称$(\cdot, \hat{+})$为概率算子,对 $\forall \underset{\sim}{A}(u), \underset{\sim}{B}(u) \in [0,1]$,有

连接("与")运算:

$$(\underset{\sim}{A} \cdot \underset{\sim}{B})(u) = \underset{\sim}{A}(u) * \underset{\sim}{B}(u);$$

合成("或")运算:

$$(\underset{\sim}{A} \hat{+} \underset{\sim}{B})(u) = \underset{\sim}{A}(u) + \underset{\sim}{B}(u) - \underset{\sim}{A}(u) * \underset{\sim}{B}(u),$$

其中$\underset{\sim}{A}(u), \underset{\sim}{B}(u)$分别表示 $u \in U$ 对模糊集合 A, B 的隶属度,本文中只需要合成算子.

对于上面得到的不同信任链路中对目的实体的属性 $attr_i$ 的各个信任向量:

$$\boldsymbol{A}_1 = \{a_{i0}^1, a_{i1}^1, \cdots, a_{i4}^1\},\ \boldsymbol{A}_2 = \{a_{i0}^2, a_{i1}^2, \cdots, a_{i4}^2\},$$
$$\boldsymbol{A}_3 = \{a_{i0}^3, a_{i1}^3, \cdots, a_{i4}^3\}, \cdots,$$

合并运算如下:

$$A = \boldsymbol{A}_1 \hat{+} \boldsymbol{A}_2 \hat{+} \boldsymbol{A}_3 \hat{+} \cdots \Leftrightarrow$$
$$A = \{a_{i0}, a_{i1}, \cdots a_{i4}\}$$
$$= \{a_{i0}^1 \hat{+} a_{i0}^2 \hat{+} a_{i0}^3 \hat{+} \cdots, a_{i1}^1 \hat{+} a_{i1}^2 \hat{+} a_{i1}^3 \hat{+}, \cdots,$$
$$a_{i4}^1 \hat{+} a_{i4}^2 \hat{+} a_{i4}^3 \hat{+} \cdots\},$$

链路中间实体的诚实属性 a_{00} 作为系数参加运算,还需要考虑不同类型信任关系的权重.得到各种属性的合成信任向量隶属度后,再和用户要求的策略集合进行匹配,若能够符合就可以对该资源节点进行访问.

5 网格计算的资源访问信任关系模型

综合以上过程,得到网格计算环境下资源访问过程中信任关系模型如图 2 所示.图中所示只是从用户的角度来建立信任关系,而信任评判是交互双方都需要进行的,资源提供者为了保护本地资源不被非法用户使用,同样也需要对用户进行信任分析,与用户对资源提供者建立信任过程相类似,资源提供者也通过相应的中间实体搜索对用户的信任关系,并与资源本地的使用策略相对照,从而决定是否同意该用户使用资源.因而只有交互双方都通过了对对方的信任关系的评价,资源访问过程才能实施.

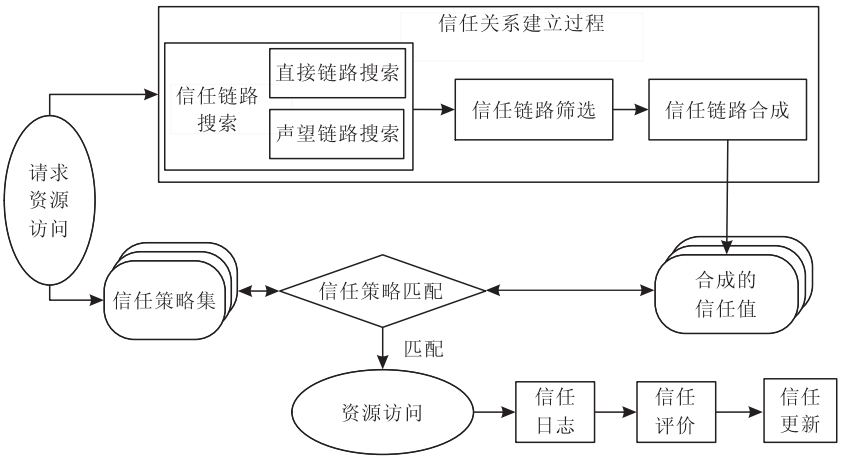


图 2 网格资源访问的信任关系模型

6　模拟实验

我们对上述过程进行了模拟实验,为了简化,只考虑直接信任链路中诚实属性的合成.选取 100 个节点,通过产生[0,1]区间的随机数来表示中间节点间的诚实属性 a_{00} 的取值,使用 MATLAB6.5 模糊系统设计工具来进行实验,根据论域[0,100]确定信任域 $U=\{u_0,u_1,\cdots u_4\}$ 相应的隶属函数模型,经过反复实验比较,我们得到一组较好反映该信任模型的参数,隶属函数的确定如表 3,而推理规则为

$$(A_1\in u_0)\,|\,(A_2\in u_0)\Rightarrow A\in u_0;$$
$$(A_1\in u_1)\,|\,(A_2\in u_1)\Rightarrow A\in u_1;$$
$$(A_1\in u_2)\,|\,(A_2\in u_2)\Rightarrow A\in u_2;$$
$$(A_1\in u_3)\,|\,(A_2\in u_3)\Rightarrow A\in u_3;$$
$$(A_1\in u_4)\,|\,(A_2\in u_4)\Rightarrow A\in u_4,$$

其中"|"取概率算子"$\hat{+}$".

表 3　隶属函数表

u_0	u_1	u_2	u_3	u_4
smf[80 95]	$trimf$[70 85 100]	$trimf$[40 60 80]	$trimf$[20 45 60]	zmf[20 50]

同时参数 $Aggregation$="probor", $Defuzzification$="centroid".由此得到的模糊信任合成视图如图 3 所示.实验结果表明,当搜索出的信任链路存在欺骗行为时,中间合成信任值会产生较大波动,因而最终得到的信任值也不可信.经过筛选,中间结果的波动性较小,因而最终结果也是可信的.

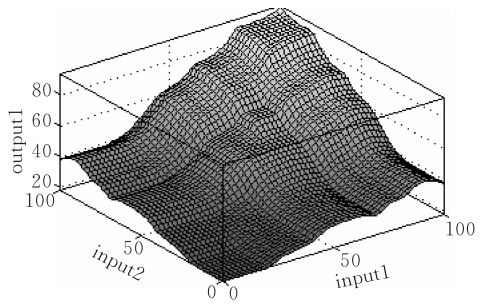


图 3　模糊信任合成视图

7　结　论

安全问题是网格计算的一个核心问题,现有的安全设施在网格环境中较难部署,本文从资源访问过程中交互双方建立的相互信任出发,结合信任关系的主观性模糊性特点,提出了基于模糊集合的网格资源访问信任关系,并讨论了资源访问中信任关系的整个实现过程.针对信任关系建立过程中的扩散性和带有欺骗性特点,通过使用一些限制条件,较好地解决了这些问题.

参　考　文　献

[1] Selcuk A A, Uzun E, Pariente M R. A reputation-based trust management system for P2P networks//Proceedings of the 4th IEEE/ACM International Symposium on Cluster Computing and the Grid. Chicago, Illinois, USA, 2004: 251-258

[2] Li Xiao-Qi, Lyu M R, Liu Jiang-Chuan. A trust model based routing protocol for secure ad hoc networks//Proceedings of the 2004 IEEE Aerospace Conference Proceedings. Big Sky, Montana, USA, 2004, 2: 1286-1295

[3] Azzedin F, Maheswaran M. Evolving and managing trust in grid computing systems//Proceedings of the Canadian Conference on Electrical & Computer Engineering. Winnipeg, Manitoba, Canada, 2002, 3: 1424-1429

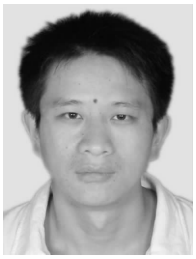
[4] Azzedin F, Maheswaran M. A trust brokering system and its application to resource management in public-resource grids//Proceedings of the 18th International Parallel and Distributed Processing Symposium. Santa Fe, New Mexico, 2004: 22-31

[5] Tang Wen, Chen Zhong. Research of subjective trust management model on the fuzzy set theory. Journal of Software, 2003, 14(8): 1401-1408(in Chinese)
(唐文, 陈钟. 基于模糊集合理论的主观信任管理模型研究. 软件学报, 2003, 14(8): 1401-1408)

[6] Dou Wen, Wang Huai-Min, Jia Yan, Zou Peng. A recommendation-based Peer-to-Peer Trust model. Journal of Software, 2004, 15(4): 571-583(in Chinese)
(窦文, 王怀民, 贾焰, 邹鹏. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型. 软件学报, 2004, 15(4): 571-583)

[7] Jøsang A. A logic for uncertain probabilities//Proceedings of the International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. River Edge, NJ, USA, 2001, 9(3): 279-311

[8] Xiao Wei-Shu. Fuzzy Mathematics Basis and Applications. Beijing: Aviation Industry Press, 1992: 152-190(in Chinese)
(肖位枢. 模糊数学基础及应用. 北京: 航空工业出版社, 1992: 152-190)



CHEN Jian-Gang, born in 1978, Ph. D. candidate. His research interests include grid computing, information security and so on.

WANG Ru-Chuan, born in 1943, professor, Ph. D. supervisor. His research interests include computer software, computer network, grid computing, information security, wireless sensor network, mobile agent and so on.

ZHANG Lin, born in 1980, Ph. D. candidate. Her research interests include computer network, grid computing, information security and so on.

WANG Hai-Yan, born in 1974, Ph. D. candidate. Her research interests include computer software, information security.

Background

This paper is one of the research results of the projects funded by National Natural Science Foundation of China and the National High Technology Research and Development Program (863 Program) and other foundations. These projects are directed towards providing a secure middleware platform based on mobile agent technology in open network environment, e. g. grid computing system and Peer-to-Peer system, in order to avoiding the attack of malicious nodes. Now the research team has realized a prototype system of grid security key technology with java programming language, such as authentication, single sign on, trust, access control, authorization, etc.

Security has been the focus of grid systems recently. As a kind of tool, GSI (Grid Security Infrastructure) provides the authentication and authorization services and so on. These mechanisms mostly belong to the objective factors, which have not met the needs of security. As the subjective factor, trust model plays an important role in security field. This paper mainly talks about how to apply the fuzzy set theory to build the trust mechanism in grid environment for enhancing security ability of system. Now researches usually focus their research on the trust modeling, the quantitative measurement mechanism, type definition, the establishment of initial trust values, trust storage, trust transitivity, trust synthesizing, trust renewal etc. Among these, the studies of trust model are still not enough.

The dynamic and unpredictable grid environment makes it hard for nodes to collaborate in security. To solve this problem, the authors propose a subjective trust model of grid system based on fuzzy set theory. Through introduction of trust relation among the entities of the intra-domain and inter-domain, the subjective property of trust relation considered, the trust mechanism of resource access in the grid computing based the fuzzy set is proposed, that is, the user for resource access builds the recommendation trust links and computes the synthetical trust relation based on the synthesis rules of the fuzzy arithmetic operators and through comparing with the trust policy of the user to decide whether to use the resource. Thus the grid trust model is given.

勘 误

本刊第 7 期金海燕的文章《基于 CP 和多小波 HMT 模型的克隆选择遥感图像融合》的式(21)更改为

$$\bar{g}=\frac{1}{(M-1)(N-1)}\times\sum_{i=1}^{M-1}\sum_{j=1}^{N-1}\sqrt{\left(\left(\frac{\partial f(x_i,y_j)}{\partial x_i}\right)^2+\left(\frac{\partial f(x_i,y_j)}{\partial y_i}\right)^2\right)\Big/2} \tag{21}$$