一种网格节点信誉评价算法及其在服务网格虚拟组织构建中的应用

崔永瑞[1],李明楚[1],江 贺[1]
(1.大连理工大学软件学院,辽宁大连 116621)

摘 要: 本文提出了一种新的服务网格节点信誉评价算法.通过构建由实体间的直接信任构成的有向加权图,并通过修改经典的Dijkstra算法来计算实体间的推荐信任,结合直接信任刻画实体间的信誉评价,同时,该算法参考虚拟组织发起者对虚拟组织愿景特征的理解,将组织间信任关系以及虚拟组织所需服务或资源的种类作为信誉评价的重要依据,细粒度刻画候选者实体的信誉,从而适合具有自治域的服务网格环境中虚拟组织的构建.仿真实验表明,该算法能够较为真实地反映网格实体间的信任关系,有效遏制不良节点对服务网格系统的危害,对虚假交易攻击以及诽谤攻击均具有较强的抵御能力.

关键词: 信誉;虚拟组织构建;网格;协同攻击
中图分类号: TP393.08 **文献标识码:** A **文章编号:** 0372-2112 (2010) 07-1557-06

A New Reputation Evaluation Algorithm for Grid Nodes and Its Applications in Service Grid Virtual Organization Formation

CUI Yong-rui[1], LI Ming-chu[1], JIANG He[1]
(1. *Software School, Dalian University of Technology, Dalian, Liaoning* 116621, *China*)

Abstract: A novel reputation evaluation algorithm for service grid nodes is proposed, which computes the transitive trust between entities by performing a modified Dijkstra algorithm on a directional weighted overlay graph consists of grid entities and their direct trust values, and predicts the evaluation of reputation between entities by taking account of the inter-organization trust relationship, direct and transitive trust together. Besides, the proposed algorithm considers the VO (virtual organization) perspective idea of VO initiator and takes services or resources the target VO required as one of the most important fine-granularity evaluation criterion, which makes the algorithm more suitable for constructing VO in a category of service grid environment which includes autonomic organizations. Simulation experiment results show that our algorithm restrains the bad performers and resists against fake transaction attack and slander attack efficiently. It provides a clear advantage in the design of a VO infrastructure.

Key words: reputation; virtual organization formation; service grid; coordinated attacks

1 引言

网格技术将地理上广泛分布的计算资源、存储资源、网络资源、软件资源、信息资源等通过计算机网络连成一个逻辑整体,像一台超级计算机一样为用户提供一体化的应用服务,并且为大规模的可信计算以及跨组织的资源共享与协作等科研与应用领域提供基础设施,成为科学界乃至工业界共同关注的热点[1].OGSI(Open Grid Service Infrastructure)及WSRF(Web Service Resource Framework)等标准的制定以及服务网格的提出标志着网格的商业化已经进入起步阶段.在服务网格中,服务需求者可以通过建立虚拟组织(VO)[2]来获取服务,完成合作或交易.若将一个VO的生命期看成一个状态模型[3,4],则大体将包括如下四种状态:识别[5];构建;运行;解体.安全合理的VO构建算法成为一个VO能够高效运行的前提,是网格系统最为关注的问题之一,也是本文关注的焦点.现有的VO构建算法大都通过客观因素的评价来选择最佳VO成员.然而,网格VO的发起者经常会面对没有过交互经验的陌生组织和实体,很难全面地得到候选者的信息,从而无法对候选者的能力进行

收稿日期:2008-05-07;修回日期:2010-01-30
基金项目:国家自然科学基金(No.60903153);国家973重点基础研究发展规划(No.2007CB714205);国家自然科学基金重点项目(No.90715037);高等学校博士学科点基金(No.20080141028);重庆自然科学基金(No.2007BA2024)

评估.信任是一个实体根据直接或间接的经验对另一实体未来行为的期望.VO的发起者在无法根据经验以及其它客观因素对候选者进行评价时,候选者的信誉便成为不可或缺的主观评价因素.此时,信誉系统可以帮助VO发起者评价陌生候选成员的信誉,完成VO的构建.本文提出了一种基于信誉系统的VO构建算法,该算法充分考虑网格特点,在准确反映网格节点间的信任关系的同时,能够有效抵御各种针对信誉系统的攻击,从而更好地帮助VO发起者选择最佳合作伙伴,构建VO.

2 相关工作

如何构建信誉系统是基于信誉系统的VO构建算法的核心问题.信誉系统在在线商务系统及P2P系统中已经得到了广泛的应用[9].而信誉系统在P2P网络环境中的应用,对网格信誉系统的研究具有重要的借鉴价值.Eigentrust算法[6]是一个经典的全局信誉算法,该算法根据节点的交易历史,形成直接信任邻接矩阵,并通过迭代求得节点的全局信誉值.该算法有效遏制了非法资源在P2P系统中的流通.文献[10]也提出了一种全局信誉算法,但该算法并未选择节点间的信任网络作为信誉值的参考.文献[11]提出了一种P2P层次化信任模型,利用本地信任信息或所属群组的推荐信任确定给定节点的信任值,能有效识别同谋攻击的恶意节点.Whitby等人[12]提出了一种在Bayesian信誉系统中过滤不公平信任评价的方法,可有效抵抗不公平信任评价攻击.然而,上述信誉系统的共同弱点是对虚假交易攻击及诽谤攻击的抵御效果不佳.

信誉系统在VO构建上的应用仍处于起步阶段[13,16].Voss[14]首次提出将信誉系统引入到VO的构建中,但并未给出具体方法.Von Laszewski等人将Eigentrust[6]的思想引入到网格环境中,提出了GridEigentrust[7],针对网格系统的异构特性,将信任划分为组织内部与组织间两层,利用Eigentrust算法计算组织间信誉,并将其作为参数构建组织内部节点的全局信誉,从而对VO发起者选取合作伙伴提供有效帮助.但该算法未克服Eigentrust算法的缺点,也未对算法健壮性进行评估.文献[15]借鉴人类社会建立推荐信任模型的方法,引入基于服务质量的偏序关系建立可信度函数,网格实体可依据可信度函数评价候选服务提供节点,从而选取可靠服务.但其假设节点间交互的历史记录权值相等,与现实情况不符,且未对算法健壮性做出评测.Kerschbaum等人[8]提出了Pathtrust模型来构建VO,该算法建立用户信任关系图,并选取参与者之间的最重加权路经的权重刻画二者的信任关系,该模型采用个人化信誉机制,使得VO发起者能更加准确地选择候选参与者,同时,该模型可以有效抵抗虚假交易攻击,但其缺乏对不良节点信誉的真实刻画,导致无法有效遏制不良节点获取利益.

综上所述,现有的信誉系统在网格VO的构建上的应用还存在不足,主要体现在:①多数由P2P系统演化而来,在信誉初始值设定及域间信任关系评价方面,无法真实反映带有自治域结构特点的网格实体间的信任关系,使得VO发起者无法依据信誉系统选择最佳合作伙伴;②系统的健壮性还有待于进一步加强,尤其对虚假交易,诽谤等攻击的抵御能力并不理想.针对上述的缺陷与不足,本文提出了一种新的基于信誉的VO构建算法.

3 基于信誉的VO构建算法

本节提出的基于信誉的VO构建算法,能够准确反映网格实体间的真实信任关系,有效遏制不良节点的不良行为,并且能够有效抵抗虚假交易与诽谤等攻击.

3.1 个人化信誉值的计算

在网格环境下,评价另一个实体的信誉时,需要注意以下四个主要影响因素:①直接信任,是实体间通过直接交互而累积的经验.②推荐信任.网格环境下常常需要依靠实体间的推荐来建立信任关系.③域间信任.网格实体所在的各自管理域间的信任关系.④发起者对VO的愿景.发起者对候选实体的信任程度和他对VO的远景特征的理解有密切关系.以服务网格为例,发起者在构建VO时,根据其所需服务的不同,对提供不同服务的候选实体的信任度要求也有所不同.

设S_set表示VO发起者构建VO所需服务(或其他资源)的集合,且sn表示S_set中的一种服务,即$sn \in S_set$.而$s(i,j,sn)$代表实体i在使用j提供的sn服务后,对j的积极反馈次数;$uns(i,j,sn)$代表实体i在使用j提供的sn服务后,对j的消极反馈次数.

3.1.1 实体间的直接信任

设$S_s(i,sn)$与$S_uns(i,sn)$分别表示实体i对与之交互的拥有服务sn的所有实体的积极反馈总和与消极反馈总和;$DT(i,j,sn)$表示实体i使用j提供的sn服务时,对实体j的直接信任;n_i为与实体i交互的节点总数.则

$$S\_s(i,sn)=\sum_{k=1}^{i-1}s(i,k,sn)+\sum_{k=i+1}^{n_i}s(i,k,sn) \tag{1}$$

$$S\_uns(i,sn)=\sum_{k=1}^{i-1}uns(i,k,sn)+\sum_{k=i+1}^{n_i}uns(i,k,sn) \tag{2}$$

而

$DT(i,j,sn)=$

$$\begin{cases} init, & 当\ s(i,j,sn)=uns(i,j,sn)=0 \\ \max(init, m(i,j,sn)), & 当\ r(i,j,sn)\geqslant 0 \\ \max(\frac{init}{100}, init\cdot(1-|m(i,j,sn)|)), & 当 r(i,j,sn)<0\ \&\ |m(i,j,sn)|\leqslant 1 \\ \frac{init}{100}, & 当 r(i,j,sn)<0\ \&\ |m(i,j,sn)|>1 \end{cases} \tag{3}$$

其中 $$m(i,j,sn)=\frac{r(i,j,sn)}{S\_s(i,sn)+S\_uns(i,sn)} \tag{4}$$

而 $r(i,j,sn)$代表 i 以自身的交互经验为基础结合与 j 的交互历史对 j 的信誉评价,即

$$r(i,j,sn)=s(i,j,sn)-\max(1,\frac{s\_s(i,sn)}{s\_uns(i,sn)})\cdot uns(i,j,sn) \tag{5}$$

本算法在计算 $r(i,j,sn)$时,加重 j 的不良表现所带来的影响.而 $init$ 表示当 i 与 j 以往并无交互时,i 为 j 设置的信誉初始值.该值应较发起者评价认可实体所得到的信誉值低几个数量级.另一方面,为了保证网格系统的开放性,使得 VO 发起者有机会与陌生实体进行交互,$init$ 的值应大于 0.在式(3)中,我们将 $DT(i,j,sn)$规范化到区间(0,1].当 i 与 j 为陌生实体时,将 $DT(i,j,sn)$赋值为 $init$;当 $r(i,j,sn)\geqslant 0$ 时,表明 i 以自身经验判断 j 为表现较好的认可实体;反之,$r(i,j,sn)<0$ 则表明 i 以自身经验判断 j 为表现较差的实体,若 $|r(i,j,sn)|/(S\_s(i,sn)+S\_uns(i,sn))\leqslant 1$,$i$ 将在区间[$init/100, init$]上对 j 进行评价,若 $|r(i,j,sn)|/(S\_s(i,sn)+S\_uns(i,sn))>1$,表示 i 对 j 已经失去信心,将 $DT(i,j,sn)$设置为 $init/100$.为了避免出现异常,本算法规定当 $S\_uns(i,sn)=0$ 时,$r(i,j,sn)=s(i,j,sn)-uns(i,j,sn)$.

3.1.2 实体间的推荐信任

如果将各实体看作顶点,将实体间的 DT 值看作顶点之间的有向边上的权,则可以构成一个包含各实体及其直接信任关系的加权有向图,记作 G_{DT},如图 1.定义从顶点 i 经过 k 到达顶点 j 的路径 $<i,k,j>$ 的权值为

$$W(i,k,j,sn)=DT(i,k,sn)\cdot DT(k,j,sn) \tag{6}$$

将 $W(i,k,j,sn)$看作实体 k 向实体 i 推荐的实体 j 关于服务 sn 的信任值.由公式(3)和(6)可知,$W(i,k,j,sn)\in(0,1]$,且每一条路径的权值都是随长度递减的.因此,将传统的 Dijkstra 算法中路径权重的计算规则由路径上所有边的和修改为路径上所有边的乘积,便可法求出两实体间的最重的路径权值.为了得到实体 i 与实体 j 之间的最佳推荐信任值 $RT(i,j,sn)$,首先,提取 G_{DT}的子图 G_{RT},$G_{RT}=G_{DT}-\vec{ij}$($\vec{ij}$为 G_{DT}中的顶点 i 与 j 之间的有向边).再利用 Dijkstra 算法思想求出 i 与 j 间最重的路径权值,记为 $w_{max}(i,j,sn)$.则有

$$RT(i,j,sn)=w_{max}(i,j,sn) \tag{7}$$

例如,图 1 中,根据公式修改的 Dijkstra 算法可以计算出由 A 到 E 的最重路径 <A,D,E>,即图中实心箭头标识的路径.路径上的边值的乘积即为 A 对 E 的推荐信任值.

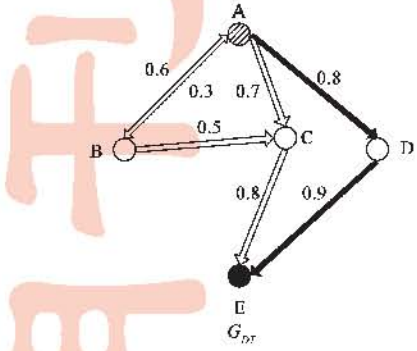

图1 实体间推荐信任模型

3.1.3 域间信任关系计算

如果组织 O_i 关于服务 sn 对组织 O_j 有过初始的认知信息,可以将其作为信任评价的初始值,记作 $IT(O_i,O_j,sn)$.当前信任评价记为 $LT(O_i,O_j,sn)$,则 O_i 与 O_j 的信任关系可表示为 $IT(O_i,O_j,sn)$与 $LT(O_i,O_j,sn)$的规范化加权和.本文通过计算 O_i 中与 O_j 交互的实体对 O_j 的信任反馈的平均值来获取 $LT(O_i,O_j,sn)$的值.假设 $E_T(O_i,O_j,sn)$表示 O_i 中与 O_j 中拥有服务 sn 的实体交互过的实体的集合,而 $E_R(O_i,O_j,m,sn)$表示 O_j 中与集合 E_T 中的实体 m 交互的实体的集合,实体间的信任反馈规则如式(3),则有

$$LT(O_i,O_j,sn)=\frac{\sum_{et\in E_T}DT(et,E_R(O_i,O_j,et,sn),sn)}{|E_T|\cdot|E_R|} \tag{8}$$

继而,推算出 O_i 对 O_j 的信任评价

$$ODT(O_i,O_j,sn)=\frac{(\alpha_o\cdot IT(O_i,O_j,sn)+\beta_o\cdot LT(O_i,O_j,sn))}{\alpha_o+\beta_o} \tag{9}$$

其中,α_o,β_o 分别为 $IT(O_i,O_j,sn)$与 $LT(O_i,O_j,sn)$在评价组织间信任时所占的权重,且 $0\leqslant\alpha_o,\beta_o<1$.

3.1.4 实体间的信誉评价

定义实体 i 对实体 j 的信誉评价如式(10):

$$R(i,j,sn)=ODT(O_i,O_j,sn)\cdot(\alpha\cdot DT(i,j,sn)+\beta\cdot RT(i,j,sn)) \tag{10}$$

其中,$\alpha\geqslant 0,\beta\geqslant 0$,且 $\alpha+\beta=1$.α 与 β 的取值取决于信誉系统的具体应用环境,但通常情况下应满足 $\alpha>\beta$.

3.2 选取 VO 成员

VO 发起者可以在网格注册机构上寻找满足条件

的候选成员，继而向信誉系统查询其对这些候选成员的信誉评价.本文采用概率模型指导 VO 发起者选取 VO 成员.假设 M 为候选成员集合，则发起者 I 选择候选成员 $C\in M$ 的概率为

$$P(C)=\frac{R(I,C,sn)}{\sum_{m\in M}R(I,m,sn)} \tag{11}$$

3.3 VO 构建新算法描述

综上所述，本小节将给出本算法的简单描述.设网格节点所能提供的全部 n 种服务的集合为 SE，VO 的发起者 *Inti* 需要使用服务子集合 SR 来构建 VO，其中 $SR=\{sr_i\mid sr_i\in SE,0\leqslant i\leqslant |SR|\}$.则在构建 VO 时，将经历如下几个步骤：

Inti sends service or resource request SR to *grid registration institute*;
Grid registration institute returns candidate service provider set CSP after verified the identity of *Inti*, where $CSP=\{csp_j(S)\mid 0\leqslant j\leqslant |CSP|, S\subset SR\}$;
For each $sr_i\in SR$ do
For each $csp_j(sr_i)$ do
Calculate *Direct trust value* between *Inti* and $csp_j(sr_i)$ according to section 3.1.1;
Calculate *Recommand trust value* between *Inti* and $csp_j(sr_i)$ according to section 3.1.2;
Calculate *Inter-organization trust value* between O_{Inti} and $O_{csp_j(sr_i)}$ according to section 3.1.3, where O_{Inti} and $O_{csp_j(sr_i)}$ are organizations *Inti* and $csp_j(sr_i)$ belongs to respectively;
Calculate reputation value of $csp_j(sr_i)$ *in Inti*'s views according to section 3.1.4;
Calculate $csp_j(sr_i)$'s probability being selected according to section 3.2;
End
Select $csp_j(sr_i)$ which has the max probability as the *decided provider*;
End
Negotiate with the *decided providers* and construct VO.

3.4 新算法的复杂性及优势分析

从 3.1 节的算法描述不难看出，VO 发起者应用本算法构建一个 VO 的运算量主要与候选成员的数量以及一次对候选成员信誉评价的计算量相关.而网格实体间，一次信誉评价的主要运算量主要集中在使用修改的 Dijkstra 算法计算推荐信任值.本算法只对路径权重的计算规则稍作修改，运行一次 Dijkstra 算法即可求得从 VO 发起者到所有其他实体(当然，其中包括所有候选成员)的最重路径，继而计算出 VO 发起者与候选成员的推荐信任值.因此，可以忽略候选成员数量对算法复杂性的影响，又由于本算法并未改变 Dijkstra 算法的复杂性，因此，假设参与信誉评价的网格实体总数为 n，则本算法的时间复杂度为 $O(n^2)$.

与现有的网格信任评价算法相比较，本算法在信任表达与算法健壮性方面作出如下创新：

①本算法针对服务网格环境特点，采用分段函数细粒度刻画服务网格节点的行为，并将 VO 发起者对未来 VO 的愿景作为参考因素，更加准确的反映 VO 发起者进行信任评价时的主观性，使得信任表达更加贴近服务网格环境.

②本算法充分利用了图的全局特性计算实体间推荐信任，这使得本算法刻画的实体间的信任关系理论上是网格中全部与两实体相关联的实体共同作用的结果.一个攻击者通过虚假交易(其同谋伙伴在未进行实际交互的情况下给出虚假的积极反馈)只能增加其与同谋伙伴之间的直接信任边的权重，而与其它诚实节点之间并未建立直接信任关系.只有当该攻击者与其他诚实节点发生了实际交互的情况下，他们之间的直接信任关系才会发生改变.因此，本算法可有效抵御虚假交易攻击.

③如果某攻击者对提供同种服务的竞争对手进行诽谤(不切实际的给出消极反馈)，则他们之间的直接信任关系受到损害，但由于本算法采用直接信任与推荐信任相结合的信誉评价方法，并且选取最重的路径权值作为推荐信任值，因此，保证了对诽谤攻击的抵御能力.在保证针对上述攻击的健壮性的同时，本算法对不良实体也进行了有效地遏制.

4 仿真实验与安全性分析

由于网格环境庞大繁杂，这使得构建一个具体的网格环境并获得实际的用户反馈信息变得异常困难，因此，现有的关于网格信任模型的研究文献大部分以仿真实验的形式模拟真实的网格环境，进而通过实验证明模型的合理性与安全性.本文着重进行网格信任模型的理论研究，在假设参与实验的节点能够按策略进行交互，并忽略节点间通讯滞时的前提下，将通过模拟 VO 的构建过程为例，在评价实体间信任关系时，与 Eigentrust 和 Pathtrust 算法进行对比，检验本系统的性能以及对各种攻击的抵御能力.仿真实验模拟 VO 的构建过程，并在同等条件下与 Eigentrust 和 Pathtrust 算法进行比对.

本文采用 800 个参与者模拟服务网格环境，参与者被平均分配成 10 个小组模拟参与者所在的自治域，共有 30 种服务平均分布在参与者之中，每一个参与者提供三种服务.这样，在模拟网格环境中，每一种服务拥有 80 个提供者.为方便讨论，本文在计算实体间各种信任时，只讨论发起者构建 VO 时只需要一种服务的情况.VO 发起者总是任意选取一种服务作为需求服务，当选取需求服务以后，该发起者便向网格注册机构查询能够提供此服务的参与者，并向信誉系统查询对这些候选参与者的信誉评价，根据前面概率模型选取最佳合作伙伴构建 VO.为使得模拟环境趋于真实，每一次 VO 的组建，都随机选取发起者与所需服务.在合作结束时，发起者将对其合作伙伴进行随机反馈.而服务提供者将得到一定的利

益,这里统一假设为数值 100.另外,为防止恶意节点通过重新申请账号来获得利益,将新节点的初始信任值设置为较低的数值,即 $init = 0.001$;正在运行中的网格系统更加关注组织间当前的信任评价,因此,为模拟正常运行的网格环境,设置公式(9)中的 $\alpha_0 = 0.4$, $\beta_0 = 0.6$;显然,信誉系统应该更加关注直接信任关系对信任评价的影响,因此,设置公式(10)中的 $\alpha = 0.7$, $\beta = 0.3$.在测试之前,系统首先随机产生一些参与者的反馈信息,模拟一个运行良好的网格环境.

以下对于每一种攻击模型的抵抗能力测试均在上述基本模拟环境下实施.仿真实验分为 20 回合,每回合模拟 10000 次 VO 的组建,将 20 回合的平均值作为最终实验结果.

4.1　虚假交易攻击模型

虚假交易攻击是指攻击者未进行真实交易而通过与恶意同伙合谋给出积极反馈来企图提高自身的信誉,从而获得更多的交易机会.信誉系统对虚假交易攻击的抵御能力主要体现在能否使得攻击者在付出很大代价的同时得到较少的利益,迫使攻击者停止作弊行为.在本次仿真实验中,依次选择占总数 1% ~ 10% 的实体作为攻击者,每一个攻击者在进行一次真实交易以后便在恶意实体集合中挑选一个实体进行 10 次虚假交易.图 2 对本文给出的算法与 Eigentrust 算法以及 Pathtrust 算法进行了比对.图中横坐标表示攻击者所占总实体数的比例,而纵坐标表示攻击者平均所得利益与诚实实体平均所得利益的比率.

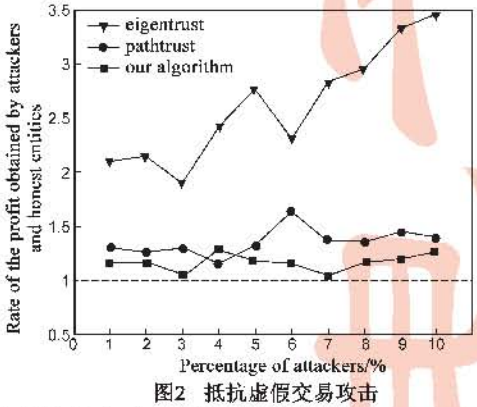

图2　抵抗虚假交易攻击

实验结果表明,随着攻击者比率的升高,攻击者获得的利益并未比诚实节点明显增多,其抵御效果稍优于 Pathtrust 算法,较 Eigentrust 算法有很大提高.

4.2　诽谤攻击模型

本次仿真实验同样依次选取占总数 1% ~ 10% 的实体作为攻击者,每一个攻击者在进行一次真实交易以后便在受害者集合中选取一个实体给出 10 次消极反馈.即受害者集合中的实体互相诽谤企图降低对方的信誉值.图 3 给出了分别应用三种算法时,受害者集合与诚实实体所获得的平均利益的对比.不难看出,在应用本算法组建 VO 时,受害者集合并未因为互相遭受诽谤而使得所得利益发生明显下降.

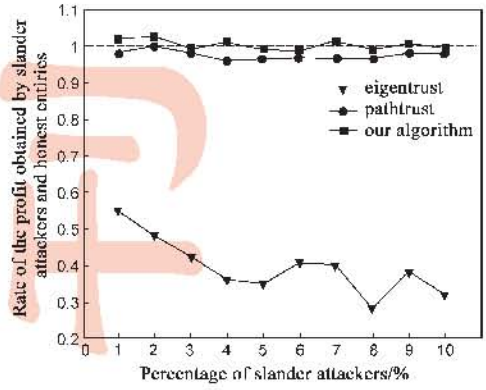

图3　抵抗诽谤攻击

4.3　对不良实体的遏制

在本次仿真实验中,选择 10% 的实体作为不良实体,使其提供良好服务的概率低于其他正常实体 40%.分别使用三种算法指导 VO 发起者组建 VO,考察其对不良实体的遏制能力,图 4 给出了实验选取的 10% 的不良实体在 100 次交互行为中发生的性能变化及其相应的信誉值变化情况,显然,在发生明显变化的三个阶段中,本算法都较为准确地给出了相应的信誉评价.图 5 则给出了不良实体所获得的利益与其他正常实体所获得利益的对比.从图 5 中我们可以看出,本文较 Pathtrust 算法更好地遏制了不良实体的不良行为.

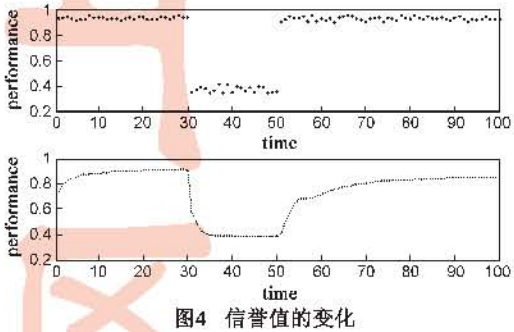

图4　信誉值的变化

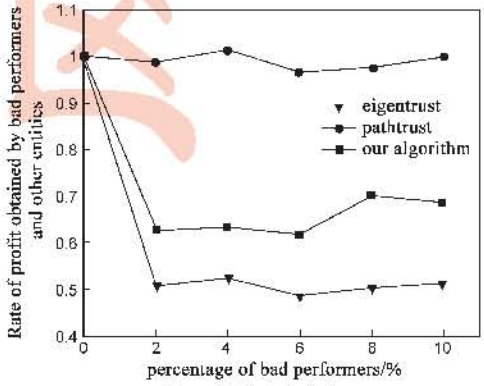

图5　遏制不良实体

5 结语

本文提出了一种新颖的网格节点信誉评价算法并将其应用在服务网格 VO 的构建中,该算法针对不同实体计算个人化信誉,利用图的全局特性,同时参考直接信任、推荐信任以及域间信任,较为真实地描述网格实体间的信任关系;能够有效抵御虚假交易攻击与诽谤攻击;对不良实体具有较强的遏制能力;另外,在拥有性能表现相近的实体的环境中,该算法仍能有效抵御较差实体的恶意攻击.

参考文献:

[1] Humphrey M, Thompson M R, Jackson K R. Security for grids [J]. Proceedings of IEEE, 2005, 93(3): 644 – 652.

[2] Foster I, Kesselman C, Tuecke S. The anatomy of the grid: enabling scalable virtual organizations[J]. International Journal of High Performance Computing Applications, 2001, 15(3): 200 – 222.

[3] Robinson P, Karabulut Y, Haller J. Dynamic virtual organization management for service oriented enterprise applications [A]. Proceedings of the 1st International Conference on Collaborative Computing[C]. San Jose, CA, USA: IEEE Computer Society, 2005. 1 – 10.

[4] Strader T, Lin F, Shaw M. Information infrastructure for electronic virtual organization management[J]. Decision Support Systems, 1998, 23(1): 75 – 94.

[5] Haller J, Karabulut Y, Robinson P. Security controls in collaborative business processes [A]. Proceedings of the 6th IFIP Working Conference on Virtual Enterprise [C]. Valencia, Spain, 2005, 186(9): 247 – 254.

[6] Kamvar S D, Schlosser M t, Garcia-Molina H. The eigentrust algorithm for reputation management in p2p networks[A]. Proceedings of the 12th international conference on world wide web[C]. Budapest, HUNGARY, 2003. 640 – 651.

[7] Laszewski G V, Alunkal B E, Veljkovic I. Towards reputable grids[J]. Scalable computing: Practice and Experience, 2005, 6(3): 95 – 106.

[8] Kerschbaum F, Haller J, Karabulut Y, et al. Pathtrust: A trust-based reputation service for virtual organization formation[A]. Proceedings of 4th International Conference on Trust Management[C]. Pisa, Tuscany, Italy, 2006. 193 – 205.

[9] 张宇,陈华钧,姜晓红,等.电子商务系统信任管理研究综述[J].电子学报,2008,36(10):2011 – 2020.
Zhang yu, Chen Hua-jun, Jiang Xiao-hong, et al. A survey of trust management for e-commerce systems[J]. Acta Electronica Sinica, 2008, 36(10): 2011 – 2020. (in Chinese)

[10] L Xiong, L Liu. A reputation-based trust model for peer-to-peer ecommerce communities[A]. Proceedings of the IEEE Conference on E-Commerce[C]. Newport Beach, California, USA: IEEE Computer Society, 2003. 275 – 284.

[11] 田慧蓉,邹仕洪,王文东,等.P2P 网络层次化信任模型[J].电子与信息学报,2007,29(11):2560 – 2563.
Tian Hui-Rong, Zou Shi-Hong, Wang Wen-Dong, et al. A hierarchical reputation model for P2P networks[J]. Journal of Electronics & Information Technology, 2007, 29(11): 2560 – 2563. (in Chinese)

[12] A Whitby, A Josang, J Indulska. Filtering out unfair ratings in bayesian reputation systems[J]. The Icfain Journal of Management Research, 2005, 4(2): 48 – 64.

[13] Silaghi G C, Arenas A E, Silva L. Reputation-based trust management systems and their applicability to grids[R]. Technical report, TR-0064, Institutes on Knowledge and Data Management & System Architecture, CoreGRID-Network of Excellence, 2007.

[14] M Voss, W Wiesemann. Using reputation systems to cope with trust problems in virtual organizations[A]. Proceedings of the 3rd International Workshop on Security in Information Systems [C]. Miami, USA, 2005. 186 – 195.

[15] 林剑柠,吴惠中.基于主观逻辑理论的网格信任模型分析[J].计算机研究与发展,2007,44(8):1365 – 1370.
Lin Jianning, Wu Huizhong. Research on a trust model based on the subjective logic theory[J]. Journal of Computer Research and Development, 2007, 44(8): 1365 – 1370. (in Chinese)

[16] 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.
Chen Jian-gang, Wang Ru-chuan, Wang Hai-yan. A subjective trust mechanism of resource access in grid[J]. Acta Electronica Sinica, 2006, 34(5): 817 – 821. (in Chinese)

作者简介:

崔永瑞 男,1981 年 11 月生于辽宁营口.先后于 2002 年及 2005 年在辽宁师范大学计算机与信息技术学院获得学士和硕士学位,并于 2009 年在大连理工大学软件学院获得博士学位.现为大连理工大学信息与通信工程博士后流动站博士后.主要研究方向为网络安全、信任模型与信誉系统.

E-mail: cyr811127@yahoo.com.cn

李明楚 男,1963 年出生于江西省.1997 年在加拿大多伦多大学获得博士学位.现为大连理工大学软件学院副院长,教授,博士生导师.在国内外顶级刊物上发表论文 100 余篇,已主持多项 863,973 及国家自然科学基金重大项目.研究方向为图论、信息安全与网络安全、应用密码学、信任模型与信誉系统等.

江 贺 男,1980 年出生于江西.博士,大连理工大学软件学院副教授,博士生导师.主要研究方向为:组合优化与智能计算.