改进的计算网格域内实体信任模型设计

杨章伟 王立平 赖文萍

(萍乡学院现代教育技术中心 萍乡 337000)

摘 要 传统基于信任域的网格信任模型以自治域内的实体数目作为信任值计算复杂度的唯一参数,安全性较低。在现有计算网格信任模型基础上,提出一种改进的自治域内实体信任模型,将时间衰减和惩罚因子引入到模型中,建立GSP对用户的直接信任度和推荐信任度计算模型,通过仿真实验验证其具有更高的抗Whitewashing攻击能力。

关键词 计算网格,信任模型,UTA,GSP,Whitewashing攻击

中图法分类号 TP393.1 **文献标识码** A

Improved Design for Trust Model on Domain Entity of Computing Grid

YANG Zhang-wei WANG Li-ping LAI Wen-ping

(Department of Modern Education and Technology, Pingxiang University, Pingxiang 337000, China)

Abstract Traditional trust model of computing grid based on trusted domains has less secure, which uses the number of entity as the only parameter of trust value calculation complexity. The paper proposed an improved autonomous entity trust model based on existing model of computing grid, introduced the time decay and penalty factor and established a direct and recommendation trust model of GSP for user. The simulation results show that the proposed model has a higher defense capabiliy to Whitewashing attack.

Keywords Computing grid, Trust model, UTA, GSP, Whitewashing attack

1 引言

网格计算致力于高性能计算能力的共享,与云计算提供商业化的数据处理服务不同,网格计算广泛应用于科学研究等特定领域[1]。为了使网格计算更安全、更具吸引力,使网格实体间交流更加方便,用户实体间的信任问题显得格外重要。

信任是网格安全问题的一个重要方面,是保证网格安全的重要手段。实体间的信任具有较强的自主性,其很大程度上由实体自身的过去行为所决定,并且随实体的行为变化而动态变化[2]。在网格计算环境中,节点之间应该建立良好的信任关系,现有高性能计算系统基本是基于信任机制而开放给用户使用的,网格节点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。因此,如何准确地计算自治域内实体的信任值并建立合理的信任值更新机制,是解决网格安全问题的一个重要部分。

2 几种信任模型分析

基于信任域的信任模型[3]的设计思想是:将网格划分为若干管理域,将节点间信任关系分为域内信任关系和域间信任关系,采用不同的策略来处理它们。其中,域内信任值的计算复杂度仅依赖于域内节点数目,域间计算复杂度仅取决于域的个数。

传统基于信任域的网格信任模型以自治域内的实体数目作为信任值计算复杂度的唯一参数,其优点是算法复杂度小,但也存在一些缺点,如:(1)没有考虑交易上下文,而通常上下文环境是决定信任的一个必要因素;(2)对于信任关系的初始机制和信任值的更新机制没有给出建立办法;(3)没有考虑时间衰减对信任值的影响,降低了信任值的精度;(4)没有考虑对恶意节点的惩罚,降低了信任安全。针对传统计算网格信任模型的缺陷,已出现了几种改进的信任模型。

(1)基于Dempster-Shafer(D-S)证据理论[4]的信任模型:通过制定相应的规则对信任度进行分类评估(分信任、不信任和不确定3类),用于刻画主观信任度;

(2)基于模糊集合的信任关系[5]:对信任关系进行等级划分,建立信任集合的隶属函数;

(3)基于概率统计的信任关系[6]:统计交互成功和交互失败的次数来作为信任等级划分的标准;

(4)基于行为的网格信任模型[7]:最早由F. Azzedin提出,以信任和声望作为度量,并引入信任衰减函数来反映信任随时间而变的特性。

其中,基于D-S证据理论的信任模型用基本可信度函数对信任度进行评估,由于该函数基于古典概率设计,因此忽略了不同信任证据对信任值的不同影响;基于模糊集合和概率

本文受江西省自然科学基金(20144BAB2020010),江西省科技厅软科学计划项目(20122BBA10094),江西省教育厅科学技术项目(GJJ14789),萍乡市科技指导性计划资助。

杨章伟(1982—),硕士,副教授,CCF会员,主要研究方向为分布式计算、云计算、网格安全,E-mail:yang505412@163.com;**王立平**(1979—),男,硕士,副教授,主要研究方向为云计算、虚拟仿真、数据挖掘。

统计的信任模型用概率来表示信任的不确定性，必须基于知识的随机概率分布而建立，不适用于复杂网格环境中的不确定性信息的计算；Azzedin 提出的基于行为的信任模型以直接信任关系表（Direct Trust Table，DTT）和推荐信任关系表（Recommended Trust Table，RTT）为基础引入信任度和声望，加入时间衰减因子，并使用模糊逻辑来判断信任行为，但是该模型维护节点间的信任关系较为繁琐，且难以找到合适的时间衰减函数。

由于计算网格具有开放性、动态性等特点，现有信任模型应用在网格中将面临恶意用户发动的 Whitewashing 攻击，从而危害网格系统安全，因此，对现有信任模型进行改进、保证用户信任度评估的准确性是网格安全的重要保障。

3 改进的信任模型

3.1 分层信任评估框架

由于网格的分布式、异构和动态性强的特点，计算网格无法提供一个统一的信任评估值，而必须采用分布式信任管理方式。然而，网格由众多大小不一的自治域组成，尽管网格用户和资源具有动态性，但它们相对于自治域是较稳定的。因此，应对计算网格的信任管理进行重新设计，增加自治域用户信任代理（User Trust Agent，UTA）层，避免网格服务提供商（Grid Service Proxy，GSP）直接与用户接触。

在评估用户信任度时，自治域 UTA 负责评估和管理本域内用户的直接信任度，GSP 负责处理 UTA 的信任数据，而自治域内的网格用户则通过 UTA 评估 GSP 的信任度。其分层结构如图 1 所示。

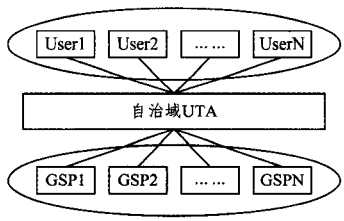

图 1 分层信任模型框架

使用如上信任管理模型后，当用户需要申请计算网格服务时，该模型的执行流程如下：

①用户向自治域 UTA 提出申请，查询满足信任条件的 GSP；

②UTA 根据本域内用户与 GSP 的交易记录，评估各 GSP 的信任度，并将评估结果返回给用户；

③用户选择满足需求的 GSP 后，向自治域 UTA 申请 CA 证书，证书包含了用户在自治域中的信任度，用户向 GSP 申请服务时提交该证书，使 GSP 能够了解用户身份及其信任度；

④GSP 验证用户证书，根据证书中包含的用户信任度和对 UTA 的信任度决定是否提供服务；

⑤如 GSP 拒绝提供服务，则用户申请失败；

⑥如 GSP 提供服务，GSP 将在服务完成后根据服务是否成功更新对该自治域 UTA 的信任度，并由 UTA 更新自治域内该用户的信任度。

使用分层信任评估框架来进行交易，由于 GSP 只需处理 UTA 的信任度，因此能够提高 GSP 的处理效率，同时 UTA 对自治域内用户的信任评估也更为准确。但是，分层信任评估框架模型使信任关系变得更复杂，需要考虑 GSP 对 UTA 信任评估的问题。

3.2 计算直接信任度

3.2.1 直接信任度评估

GSP 对某自治域 UTA 进行信任评估的依据是与该自治域内用户的交易结果，根据其交易的成功和失败次数来进行判定。由于 GSP 每次与网格用户进行交易都必须通过 UTA 来完成，因此 UTA 能够记录每个用户交易成功和失败的次数。用 N_s 和 N_f 分别表示 GSP 与该自治域内用户交易成功和失败的次数，那么利用贝叶斯后概率验证公式得到该用户的直接信任度 T 如下：

$$T=\frac{N_s+1}{N_s+N_f+c} \tag{1}$$

其中，c 为一个常量，用来确保交易次数较少时评估结果的准确性，c 的取值根据交易次数在 2～6 之间变化。

GSP 对 UTA 的信任取决于 UTA 评估该自治域内用户信任度的准确程度，因此 UTA 的信任度可用三元组（T，D，S）来表示。其中，T 表示每个域内用户的直接信任度，由式（1）可取得；D 表示所有交易的信任偏差之和，由式（2）取得；S 表示交易信任偏差度方差，由式（3）取得。

定义 1 交易的信任偏差 D 定义为自治域内的用户信任度与完全信任或完全不信任之间的偏差，可通过式（2）计算。

$$\begin{cases} D_i=1-t_i, & \text{successful} \\ D_i=0-t_i, & \text{fail} \end{cases} \tag{2}$$

其中，D_i 表示第 i 次交易的信任偏差，t_i 表示 GSP 与用户第 i 次交易时该用户的直接信任度。

定义 2 交易信任偏差度方差 S 定义为所有交易偏差度平方的平均值与基准偏差度平方平均值的商，可通过式（3）来计算。

$$S=\frac{1}{n}*\sum_{i=1}^{n}\frac{D_i^2}{D_s^2} \tag{3}$$

其中，n 表示 GSP 与该用户的交易总次数，D_s 表示基准偏差度。

3.2.2 加入惩罚因子

在 GSP 与用户进行交易时，不可避免会出现恶意交易，为遏制恶意交易对网格安全的影响，可以加入惩罚因子。当自治域内用户出现恶意交易后，UTA 将快速降低该用户的信任度，使其下次申请资源时受到一定限制。根据如上分析，对式（1）进行改进，加入惩罚因子 λ，得到如下信任度 T 的计算公式：

$$T=\frac{N_s+1}{\lambda(N_s+N_f)+c} \tag{4}$$

其中，惩罚因子 λ 的取值为 $\lambda\in[1,\infty)$，λ 的取值为 0 时表示不惩罚，当 λ 的取值越大表示该用户的信任度降低速度就越快，对该用户的惩罚就越大。

为了界定在具体交易中惩罚因子 λ 的取值是否能够迅速降低恶意用户的信任度，需定义一个评估基准值作为 λ 的取值参考。

定义 3 评估基准值 $C1-C5$ 的取值分别为 GSP 与用户

正常交易时，恶意交易率分别为 0、10%、20%、50%和 100%等 5 种不同情况下的折算值，C1—C5 的取值见表 1。

表 1　评估基准值取值

评估基准	恶意交易比例	λ取值
C1	0	1
C2	10%	(N_s+N_f)
C3	20%	$(N_s+N_f)^2$
C4	50%	$(N_s+N_f)^5$
C5	100%	$(N_s+N_f)^{10}$

根据评估基准值在不同恶意交易情况下的取值，当用户进行无恶意交易的正常交易时，信任度 T 即为利用贝叶斯后概率验证公式得到的该用户的直接信任度；当恶意交易开始增多后，信任度 T 的取值以指数形式减小；恶意交易达到 100%时，T 的取值接近于 0，使用户无法再进行交易。

3.2.3　引入时间衰减处理机制

当 GSP 与用户的交易次数较多时，相对于老的交易，最新的交易结果更容易反映该用户当前的信任度。因此，在计算用户的直接信任度时，需要考虑时间衰减对于信任值的影响。目前许多信任模型采用加权的方式随着时间衰减而动态更新信任值，为更方便地实现模型，本文中的加权函数以对数来实现。如式(1)和式(3)是以用户所有交易的成功和失败次数为参数进行计算而得到直接信任度，考虑到新的交易更容易反映出用户的信任度，在计算直接信任度时取最新的 M 个交易结果代入到式(1)中。

$$M=\mathrm{Log}_n(N_s+N_f) \tag{5}$$

$$T=\frac{N_s+1}{\lambda M+c} \tag{6}$$

其中，$n\in[1,10]$且其取值随着 GSP 与用户总交易次数的增加而递增。因此，相对于出现时间更早的恶意交易来说，新出现的恶意交易能够更快地降低用户信任度。

3.3　计算推荐信任度

推荐信任是通过与用户本身进行过交易的实体来寻求一条能够抵达目标实体的路径，从该路径中获取目标实体的推荐信任度。当某个 GSP 需要获取目标用户的推荐信任度时，其过程如下：

①该 GSP 向所有 GSP 通过广播发送请求；

②GSP 收到请求后进行转发，并检查自身是否与目标用户发生过交易，如果存在交易，则将其直接信任度 T 发送给请求方；

③通过多个 GSP 的直接信任度 T 的数据，GSP 就可以获得该用户的推荐信任数据。

由于推荐信任涉及多个与目标用户交易过的用户，为保证推荐信任的可靠性，在网格中为每个用户增加一个信任代理。代理的功能是为用户采集 GSP 的信任值，当用户需要目标对象的信任信息时由该对象的信任代理提供。一般来说，推荐信任的计算过程中会有多个代理的信任数据，将这些数据通过式(7)进行计算就可以得到目标用户的推荐信任值。

$$T=\sum\frac{X_i\cdot N_i\cdot R_i\cdot F_i}{\sum X_i\cdot N_i\cdot F_i} \tag{7}$$

其中，X_i、N_i 和 R_i 分别为用户 i 所对应代理的信任值、推荐次数和目标用户推荐信任值；F_i 则是时间参数，随着上次推荐时间的增加而减少。

同时，推荐信任和实体本身的声誉存在一定的模糊性，采用一个精确数值来表述推荐信任度难以体现模糊性。因此，本文设计一个推荐信任基准，将信任度按照值域划分为 5 个等级。将信任值的值域范围定义为[0,1]，则基准集合$RTS=\{RTS_1(0.9,0.05,0.02),RTS_2(0.7,0.05,0.02),RTS_3(0.5,0.05,0.02),RTS_4(0.3,0.05,0.02),RTS_5(0.1,0.05,0.02)\}$，如图 2 所示。

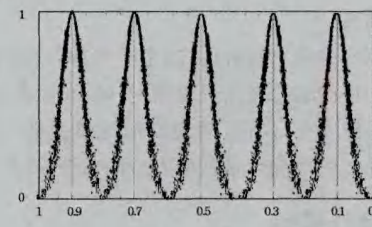

图 2　推荐信任基准集合

在具体的计算网格环境中，推荐信任基准集合是根据信任等级划分的，本文中设定信任等级 RTS_1-RTS_5 为从非常信任到不信任的 5 个等级。

3.4　仿真实验与分析

为验证该计算网格信任模型的有效性，本文设计了一个中等规模的计算网格仿真实验环境。该环境划分了 10 个用户自治域和 GSP，所有的 GSP 提供完全相同的计算服务，每个自治域中包含数百个网格用户，其中含少量恶意用户。实验过程分 3 个场景实现，场景 1 不使用自治域 UTA 管理信任度，由 GSP 直接管理用户信任；场景 2 通过 UTA 管理信任度，场景 3 使用本文信任模型管理信任度。当用户向 GSP 申请计算服务，并伴随恶意用户 Whitewashing 攻击时，3 个场景被攻击成功的次数如图 3 所示。

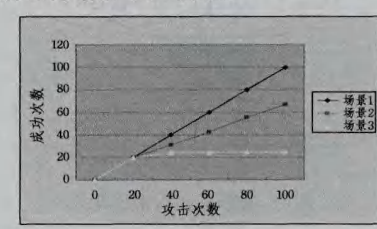

图 3　仿真实验结果

从仿真结果可以看出，上述 3 个场景中，场景 1 中 GSP 允许恶意用户申请服务，无法防范 Whitewashing 攻击；场景 2 和场景 3 都使用了 UTA 信任模型，由于场景 3 加入时间衰减和惩罚因子，在 GSP 受到一次 Whitewashing 攻击后迅速降低该用户的信任度，使其无法再申请该 GSP 提供的服务，故其具有更好的抗攻击性。

结束语　在现有信任模型的基础上，引入 UTA 分层管理机制，并将时间衰减和对恶意推荐的处理引入到模型中，建立直接信任度和推荐信任度的计算模型。通过仿真实验可以看出，该改进的信任模型通过迅速降低恶意用户的信任度，使其无法申请新的服务，从而能够提高计算网格中 GSP 抵抗 Whitewashing 攻击的能力。

参 考 文 献

[1]　Yang Zhang-wei. Research on trust model inautonomous domain of campus grid[C]// Proceedings of 2011 International Confe-

rence on Computer Science and Service System. IEEE Computer Society, 2011

[2] 马礼,郑纬民. 信息网格环境下的综合信任度评价模型[J]. 清华大学学报(自然科学版),2009(4):599-603

[3] Rahman A A, Hailes S. Supporting Trust in Virtual Communities[C]// Proceedings of the 33rd Hawaii International Conference on System Sciences. Washington DC, USA: [s. n.], 2000: 6007-6016

[4] Josang A, Knapskog S J. A metric for trusted systems[C]// Proceedings of the 21st National Security Conference. NSA, 1998

[5] Azzedin F, Maheswaran M. Towards Trust-Aware Resource Management in Grid Computing Systems[C]// Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid. 2002: 1-6

[6] 李小勇,桂小林. 可信网络中基于多维决策属性的信任量化模型[J]. 计算机学报,2009,32(3):405-416

[7] Josang A, Hird S, Faccer E. Simulating the Effect of Reputation Systems on e-Markets[C]// the Proceedings of the First International Conference on Trust Management. Creece, 2003: 179-194

(上接第 380 页)

交叉概率有利于云团性能朝最优状态转移,同时避免陷入局部最优;而在后期随着云团整体性能的提高,云滴之间的性能差异变小,此时小的交叉概率便能优化云滴性能,并且交叉概率越小系统开销越小,对应的误差越小。

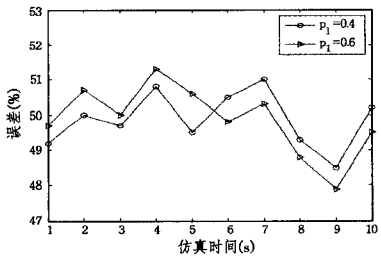

图 4 不同变异概率 p_1 下数据包长度检测结果比较

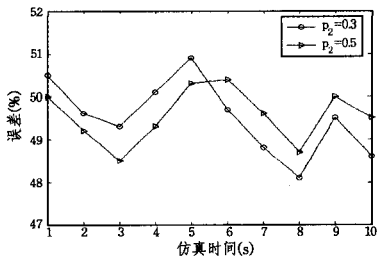

图 5 不同交叉概率 p_2 下数据包长度检测结果比较

结束语 在对已有网络异常检测方法分析的基础上,本研究结合云模型提出了一种新的检测算法 DMCM。该算法首先针对数据包属性的离散度和偏差进行定义,给出了样本判断指标,同时基于云模型定义了数据包的期望 Ex、熵 En 以及超熵 He,并通过计算属性标准差分布来判断数据包是否存在被攻击的可能。最后,以 OPNET 和 MATLAB 进行仿真实验,对比研究了该算法与 RETMMAD 算法以及实际监听的情况,结果发现 DMCM 性能较 RETMMAD 算法有大幅度提高,和实际情况比较吻合。在今后的研究中,可以考虑针对 DoS、Probe、R2L 和 U2R 等各种攻击的具体状况,来建立完善的检测方法。

参 考 文 献

[1] Varadharajan V, Tupakula U. Counteracting security attacks in virtual machines in the cloud using property based attestation [J]. Journal of Network and Computer Applications, 2014, 40(7): 31-45

[2] Younis Y A, Kifayat K, Merabti M. An access control model for cloud computing [J]. Journal of Information Security and Applications, 2014, 19(1): 45-60

[3] 杨宏宇,常媛. 基于 K 均值多重主成分分析的 App-DDoS 检测方法[J]. 通信学报,2014,35(5):16-24

[4] Yu Yong, Niu Lei, Yang Guo-min, et al. On the security of auditing mechanisms for secure cloud storage [J]. Future Generation Computer Systems, 2014, 30(1): 127-132

[5] 王会梅,鲜明,王国玉. 基于扩展网络攻击图的网络攻击策略生成算法[J]. 电子与信息学报,2011,33(12):3015-3021

[6] 谢柏林,余顺争. 基于应用层协议分析的应用层实时主动防御系统[J]. 计算机学报,2011,34(3):452-463

[7] 程宏兵,容淳铭,黄晓,等. 高效的攻击检测与数据融合算法[J]. 通信学报,2012,33(9):85-94

[8] 张玲,白中英,罗守山,等. 基于粗糙集和人工免疫的集成入侵检测模型[J]. 通信学报,2013,34(9):166-175

[9] 席荣荣,云晓春,张永铮,等. 一种改进的网络安全态势量化评估方法 [J]. 计算机学报,2014,31(3):95-101

[10] 储泽楠,李世扬. 基于节点生长马氏距离 K 均值和 HMM 的网络入侵检测方法设计[J]. 计算机测量与控制,2014,37(10):1-12

[11] 张冰涛,王小鹏. 面向 WSN 安全路由协议的自适应威胁模型[J]. 计算机应用研究,2014,31(4):1208-1211

[12] Vissers T, Somasundaram T S, Pieters L, et al. DDoS defense system for Web services in a cloud environment [J]. Future Generation Computer Systems, 2014, 37: 37-45

[13] 朱建明,宋彪,黄启发. 基于系统动力学的网络安全攻防演化博弈模型[J]. 通信学报,2014,35(1):54-61

[14] 刘禹,李德毅,张光卫,等. 云模型雾化特性及在进化算法中的应用[J]. 电子学报,2009,37(8):1651-1658

[15] 张亚玲,韩照国,任娇霞. 基于相对熵理论的多测度网络异常检测方法[J]. 计算机应用,2010,30(7):1771-1774

[16] Worku S G, Xu Chun-xiang, Zhao Ji-ning, et al. Secure and efficient privacy-preserving public auditing scheme for cloud storage [J]. Computers & Electrical Engineering, 2014, 40(5): 1703-1713