

# 对基于可信计算的网格行为信任模型的量化评估方法研究

刘利钊<sup>1</sup> 魏鹏<sup>2</sup> 王颖<sup>1</sup> 李茂青<sup>1</sup>

(1 厦门大学自动化系,厦门市思明区,361005)

(2 莫斯科国立大学计算机系,莫斯科,107076)

**摘要:**针对基于可信计算的网格行为信任模型,运用波动信息能量变换给出了根据实体的交互经验和交互时间计算历史信任值和直接信任值的方法;用 Hausdorff 距离构造了函数相关程度的算法,进而给出了自我信任值的计算方法。通过采用门限值作为平均值、自我信任值为偏差量的正态分布函数构造了推荐信任值的更新函数,给出了域间评估流程图,并用一个有 2 000 个实体的区域网格进行域内数据更新实验。分析结果说明了各评估算法的合理性和有效性。

**关键词:**网格;行为信任;可信计算;量化评估;直接信任值;更新函数

**中图分类号:** TP393

网格技术是以互联网为根基和生存环境的新兴技术,网格信任模型中的行为信任问题已经成为了网格技术的重点问题<sup>[1-6]</sup>。目前,有多种方案针对网格实体间的行为信任问题进行了研究,但是大多数方案都是建立在普通不确定是否可信的网络硬件和计算机硬件平台上,试图以软件为手段屏蔽硬件的不可信,从而建立一个安全可靠的运行和通信环境<sup>[7-20]</sup>。文献[12]以网格为环境构造了一个基于可信计算平台的行为信任模型,如何合理地利用经验来计算信任值、代理推荐信任值的函数设置、自我信任值如何计算等问题是该模型研究中的核心问题,同时也是网格研究的重要问题。本文针对这些问题,从目前建模控制中的能量控制角度进行了研究<sup>[21,22]</sup>。

## 1 基本概念介绍

根据网格实体所属的组织以及地理位置的不同,可将网格划分为多个网格区域,每个域包含多个网格实体和一个信任代理。信任值可以根据交互经验和最后一次交互距评估时的间隔由函数  $f(x, t)$  得出,其中,  $x$  代表经验,  $t$  代表时间值。文献[22]在对实体模型进行分析时,给出了一种

在选定区域内计算某实体所具有的影响力总和的函数,定义为波动信息能量函数,同时给出了在该区域中计算某些局部区域所具有的影响力与总影响力的比例计算方法,定义为波动信息能量比;函数间的相互关联程度可用函数信息相关度表示。

## 2 域内信任量化与评估方法设计

根据波动信息能量理论提出以下推理:

推理 1 假设  $A$  域内实体  $a$  与实体  $b$  在历次直接交互过程中获得经验  $\{x_1, x_2, \dots, x_n\}$ , 每次交互距当前的计算时间为  $\{t_1, t_2, \dots, t_n\}$ , 则实体  $a$  对实体  $b$  的历史信任值为  $\text{history} = \sum_{i=1}^n |f(t_i)(x_i - x_{i-1})|^2 / 2$ 。

区域  $A$  内实体  $b$  对实体  $a$  的历史交互经验在  $a$  对  $b$  进行评价时,相当于  $b$  对  $a$  在本区域内所施加过的影响的总和。而每一次交互的影响都与距离当前时间的间隔相关,随着进一步的经验交互的进行,历史经验的影响将衰减,所以  $f$  在这里代表衰减函数,可以根据不同网络而设定。

推理 2 若区域  $A$  内信任代理对实体  $b$  的第  $i$  次推荐信任误差为  $\text{Sub}_i$ , 可接受的误差门限值

为, 自我信任值为, 则推荐信任值的更新算法为:

$$r_i = \begin{cases} \frac{1}{\sqrt{2}} \exp\left\{-\frac{(Sub_i - )^2}{2^2}\right\} r_i, Sub_i < \\ \frac{1}{\sqrt{2}} \exp\left\{-\frac{(Sub_i - )^2}{2^2}\right\} r_i, Sub_i > \end{cases}$$

当  $Sub_i <$  或  $Sub_i >$  时, 都说明信任代理获得的域内实体对  $b$  的整体评价高于代理的最优期望值, 可能是由代理的直接信任值过低而导致的, 更有可能其他实体在与  $b$  进行交互时判断失误或更新不及时所致, 后者将间接影响到  $a$  对  $b$  的间接信任评估。对于门限值来说, 两种情况所反映出的代理和其余实体对实体  $b$  的最终评价都偏离于最优评估。偏离程度相同时, 评估值对更新推荐信任值  $r_i$  的影响相同, 对于影响大小的误差判断来源于实体  $a$  的自我信任值, 所以 可以表示正态分布函数更新过程中的偏差。

当没有门限值约束时, 在实验中发现, 基于  $t$  分布的更新算法在推荐信任误差值较大时有更好的收敛效果, 可以更大程度地反映出实体自我信任值和信任代理的信任推荐作用, 构造如下:

$$r_i = \frac{\left(\frac{+1}{2}\right)}{\sqrt{\left(\frac{-}{2}\right)}} (1 + \frac{Sub_i}{2})^{-1} r_i$$

同时发现, 基于  $^2$  分布的更新函数可以在误差比较小时快速反映信任推荐误差和自我信任值的影响, 构造如下:

$$r_i = \frac{1}{2^2} \left(\frac{-}{2}\right) Sub_i^{-1} e^{\frac{Sub_i}{2}} r_i$$

推理3 若  $A$  和  $B$  分别代表两个空间离散点集, 则其相关度  $[A, B]$  可用  $hausdorff(A, B)$  表示。

若函数  $I(S)$  和  $M(S)$  分别代表两个空间离散点集的值域,  $S$  为定义域, 其相关度用  $hausdorff$  距离计算时, 距离越大, 相关度越小, 点集与自身的距离为零时, 相关度最大; 条件相关度可以用两个点集的差异与其中一个点集的  $hausdorff$  距离比上两个点集之间的  $hausdorff$  距离来计算, 而此时的被减函数点集到原点的  $hausdorff$  距离与上述点集距离之和等于  $I(S)$  和  $M(S)$  之间的  $hausdorff$  距离:

$$[I(S), M(S)] = hausdorff[I(S), M(S)]$$

$$[I(S) / \prod_{i=1}^n M_i(S)] =$$

$$\frac{hausdorff\left\{ [I(S) - \prod_{i=1}^n M_i(S)], \prod_{i=1}^n M_i(s) \right\}}{hausdorff[I(S), \prod_{i=1}^n M_i(S)]}$$

$$1 - [I(S) / \prod_{i=1}^n M_i(S)] =$$

$$\frac{hausdorff\left\{ O, \prod_{i=1}^n M_i(S) \right\}}{hausdorff[I(S), \prod_{i=1}^n M_i(S)]}$$

推理4 若域  $A$  内实体  $a$  对域内其他实体的直接信任值为  $t_{ai}$ , 其他实体对实体  $a$  的直接信任值为  $t_{ia}$ , 代理对其他实体的直接信任值为  $t_{mi}$ , 则  $a$  的自我信任值为  $[|t_{ai}| |t_{mi}|]$ 。

经过仿真实验发现,  $[|t_{ai}| |t_{mi}|]$  和  $[|t_{ai}| |t_{ia}|]$  均可作为 的初始计算方法和实时更新算法。以  $[|t_{ai}| |t_{mi}|]$  为例, 根据推理3 可得:

$$= [ |t_{ai}| |t_{mi}| ] = \frac{hausdorff\left[ \prod_{i=1}^n |t_{ai}| - \prod_{i=1}^n |t_{mi}|, \prod_{i=1}^n |t_{mi}| \right]}{hausdorff\left( \prod_{i=1}^n |t_{ai}|, \prod_{i=1}^n |t_{mi}| \right)}$$

### 3 域间信任量化评估方法

根据域内信任量化过程, 给出域间量化流程图如图1所示。

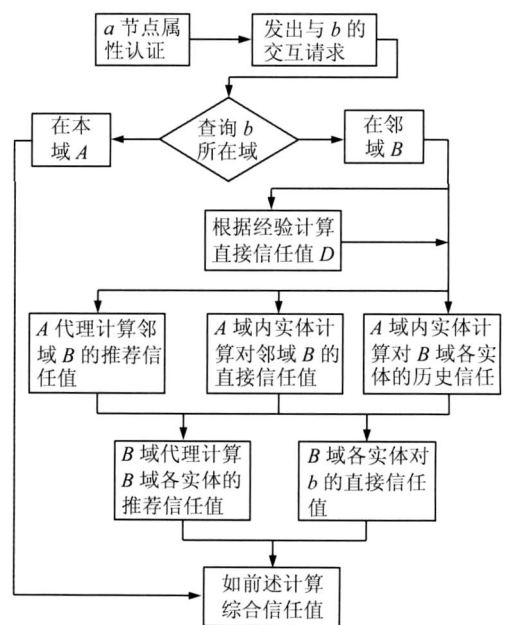


图1 域间量化流程图

Fig. 1 Flowing Chart of Inter-domain Quantization

## 4 应用举例

设置仿真程序: A 域内实体个数为 2 000, 数据误差门限值初始化  $\epsilon = 0.550 0$ , 信任推荐更新函数采用基于正态分布的构造函数  $f(t) = 1/\sqrt{2\pi} \cdot e^{-0.5(t)^2}$ , 时间单位分三次分别设为  $t = 1 s, 1 m, 1 h$ 。计算实体 6 与实体 1 993 的历史信任值, 根据推理 1, 不同时间单位设置下历史信任值的结果相同, 此时为 0.783 3, 直接信任值为 0.989 6 (限于篇幅, 经验数据暂略), 将这两个值作为第一轮更新的初始信任值。

如表 1  $t_1$  所示, 根据推理 4 得自我信任值为 0.695 0。为了加快更新速度, 设置初始值为 0.7, 实时更新信任值, 同时更新代理对所有实体的第

一轮推荐信任值  $r_i$  和各实体对 1 993 的直接信任值  $t_i$ , 进入第二轮计算。具体更新过程和数据如表 1 所示, 此时时间单位为 s, 当前更新至 341 轮。可见, 当  $Sub_i$  逐渐减小时, 代理对实体 1 993 的推荐信任值逐渐增大, 推荐信任值在更新过程中又再次影响到实体 6 和其他实体对 1 993 的评估值, 结合各实体的直接经验值对 1 993 实体在多轮更新中给予了更大的信任值; 同时可以看到, 实体 6 对 1 993 的评估和其他实体对 1 993 的评估同步增减, 所以此时根据推理 4 得实体 6 的自我信任值在更新过程中基本保持不变, 在该网格中可以粗略设置为定值。实验中发现, 在大幅调整代理对 1 993 的推荐信任值时, 实体 6 的自我信任值也大幅波动, 所以严格来讲, 应保持自我信任值的实时更新。

表 1 网格状态仿真表

Tab. 1 Simulation Table of Grid Status

数据误差门 限值初始化	历史更新数据时间间隔设置为 0.5 个时间单位						$t = 1 s$		$= 0.7$		$0.3$	
	第一轮更新	第二轮更新		第三轮更新		...	第 $i = 340$ 轮	第 $i = 341$ 轮				
轮实体标号	$R_1$	$t_1$	$R_2$	$t_2$	$R_3$	$t_3$	...	$R_{340}$	$t_{340}$	$R_{341}$	$t_{341}$	
1	0.500 0	0.504 0	0.508 0	0.512 0	0.516 0	0.519 9	...	0.523 9	0.527 9	0.531 9	0.535 9	
	0.655 4	0.659 1	0.662 8	0.666 4	0.670 0	0.673 6	...	0.677 2	0.680 8	0.684 4	0.687 9	
6	0.691 5	0.695 0	0.698 5	0.701 9	0.705 4	0.708 8	...	0.712 3	0.715 7	0.719 0	0.722 4	
...							...					
1 993	0.989 3	0.989 6	0.989 8	0.990	0.990	0.990 6	...	0.990 9	0.991 1	0.991 3	0.991 6	
	0.997 4	0.997 5	0.997 6	10.997 7	0.997 7	0.997 8	...	0.997 9	0.997 9	0.998 0	0.998 1	
2 000	0.998 1	0.998 2	0.998 2	0.998 3	0.998 4	0.998 4	...	0.998 5	0.998 5	0.998 6	0.998 6	
$Sub_i$	0.695 0	0.059 5	0.055 5	0.051 8	0.048 4	0.045 2	...	0.042 2	0.021 0	0.008 5	0.000 3	
$R_i$	2.878 4	2.860 9	2.845 3	2.831 3	2.818 7	2.807 3	...	2.796 9	2.787 4	3.290 5	3.373 4	

## 5 结 语

通过实验可以看出, 根据波动信息能量理论所建立的信任值计算方法得出的结果满足对目前网格环境实时更新的需要, 对于在传统网格计算中视为定值的数据 (如自我信任值), 也可以实现同步更新, 从而使更新过程更加准确完善; 同时可以把经典数学中的成熟算法引入到网格计算当中。但是也看到一些局限性, 如目前无法找到一个有效的变换, 使数据误差门限值同步更新, 而实际上, 门限值应该可以由波动信息能量比来构造, 但在实验中却无法与其他参数匹配, 所以并未论述; 所构造的推荐信任值更新函数是基于对大量仿真和实验结果的概率统计得出的, 对于不同的网格环境选择合适的更新函数时, 需要依赖于专家经验, 将来则需要建立完整的理论框架, 通过推导证明得出。

## 参 考 文 献

- [1] Foster I, Kesselman C. The Grid: Blueprint for a New Computing Infrastructure[M]. San Fransisco, CA: Morgan Kaufmann, 1999
- [2] Azzedin F, Maheswaran M. Evolving and Managing Trust in Grid Computing Systems [C]. IEEE Canadian Conference on Electrical Computer Engineering, Winnipeg, Canada, 2002
- [3] Novotny J, Tuecke S, Welch V. An Online Credential Repository for the Grid: MyProxy[OL]. <http://www.globus.org/alliance/publications/papers/myproxy.pdf>, 2001
- [4] 刘鹏. 我国网格研究现状 [OL]. <http://Chinagrid.net/grid/paperptlourCONUTRY.pdf>, 2006
- [5] 都志辉, 陈渝, 刘鹏, 等. 网格计算[M]. 北京: 清华大学出版社, 2002: 9-12
- [6] 蒋大保. 网格环境下的安全技术研究 [D]. 北京: 中国科学院高能物理所, 2002

- [7] Jianc C, Wang C, Liu X, et al. A Survey of Job Schedu 2 Ling in Grids [C]. The 9th International Asia2 Pacific Web Conference (APWeb2007), Berlin, Germany, 2007
- [8] Abwajjy H. Fault2tolerant Scheduling Policy for Grid Computing Systems [C]. The 18th IEEE International Parallel and Dist ributed Processing Symposium. Los Alamitos ,Cal, USA, 2004
- [9] 刘玉龙,曹元大,李剑. 一种新型推荐信任模型[J]. 计算机工程与应用, 2004, 40(29):47-49
- [10] 王珊,高迎,程涛远,等. 服务网格环境下基于行为的双层信任模型的研究[J]. 计算机应用, 2005, 25(9):974-977
- [11] 王东安,徐浩,南凯,等. 基于推荐的网格计算的信任模型[J]. 计算机应用研究, 2006, 23(2):96-98
- [12] 耿延军,张红旗,周靖. 基于可信计算的网格行为信任模型研究[J]. 计算机研究与发展, 2008, 43(3):476-482
- [13] Abdul-Rahman A, Hailes S. Supporting Trust in Virtual Communities[C]. The Hawaii International Conference on System Sciences, Maui Hawaii, 2000
- [14] 李文娟,王晓东,傅仰耿,等. 几种网格信任模型的研究[J]. 福州大学学报(自然科学版), 2006, 34(2):78-83
- [15] TCG. TCG Main Specification Version 1. 1b [OL]. <http://www.trustedcomputinggroup.org/home>, 2004
- [16] 干志勤,曾国荪. 网格环境下的基于行为的信任评估模型[J]. 计算机应用与软件, 2005(12):12-14
- [17] 王莉苹,杨寿保. 网格环境中的一种信任模型[J]. 计算机工程与应用, 2004(23):36-40
- [18] 王晓峰,张景,王尚平,等. 网格计算系统中的综合信任评估[J]. 计算机工程, 2006(22):53-58
- [19] 李鑫,刘妍,陈克非. 网格计算中的信任模型研究[J]. 计算机工程, 2008, 31(3):22-26
- [20] 汪进,杨新,刘晓松. 一种新型的网格行为信任模型[J]. 计算机工程与应用, 2003(21):41-45
- [21] Liu Lizhao, Liu Yingchao, Huang Zhili, et al. The Chaotic Disturbance of UAV System ' s Communication and Coping Strategy [C]. ICCAS08, Xiamen, China, 2008
- [22] Liu Lizhao. The Chaotic Characters and New Control Strategy of Unmanned Airplane Information System [C]. International Symposium on Computational Intelligence and Design 2008, Wuhan, China, 2008

第一作者简介:刘利钊,博士生,主要研究方向为系统工程。  
E-mail:kollzok@yahoo.com.cn

## Quantitative Assignment of the Grid Behavior Trust Model Based on Trusted Computing

LIU Lizhao<sup>1</sup> WEI Peng<sup>2</sup> WANG Ying<sup>1</sup> LI Maoqing<sup>1</sup>

(1 School of Information Science and Technology, Xiamen University, Siming District, Xiamen 361005, China)

(2 School of Computer and Communication, Moscow University, Moscow 107076, Russia)

**Abstract:** For the quantitative assignment of the grid behaviors trust model based on trusted computing, it gives an algorithm of calculating the direct trust values and the history trust values from interactive experience and interactive time using fluctuation energy conversion, makes a function correlation algorithm using hausdorff function, and in turn gives a method of calculating the self-confidence value, makes an update function using a normal distribution function with the threshold as average value and self-confidence value as deviation, gives the inter-domain evaluation process, finally shows the reasonableness and effectiveness of the assessment method by running the update process and analysing the result of the data of a regional grid with 2 000 entities.

**Key words:** grid; behavior trust; trusted computing; quantitative assessment; direct trust value; update function

**About the first author:** LIU Lizhao, Ph.D candidate, majors in system engineering.

E-mail: kollzok@yahoo.com.cn