第32卷 第22期 计 算 机 工 程 2006年11月
Vol.32 No.22 Computer Engineering November 2006
·博士论文· 文章编号：1000—3428(2006)22—0040—03 文献标识码：A 中图分类号：TP393.08

网格计算系统中的综合信任评估

王晓峰，张 璟，王尚平，张亚玲
(西安理工大学密码理论与网络安全研究室，西安 710054)

摘 要：网格是个动态变化的环境，网格站点间的信任关系受到一些因素的制约，该文提出了一个网格安全信任模型，把信任的概念建立在网格站点的身份信任和行为信任、计算能力、单元服务开销、先前的工作成功率、入侵检测和入侵抵抗能力的基础上，构造了一个评估网格站点行为信任度的算法。基于模糊数学中的模糊综合评估算法理论，该文构造了一个网格站点信任度的综合评估算法，利用该算法可以比较全面地评估网格站点的信任度，最大程度地保证网格行为的安全可靠。

关键词：网格计算；信任度；行为信任；信任评估；模糊综合评估

Integration Trust Evaluation in Grid Computation System

WANG Xiaofeng, ZHANG Jing, WANG Shangping, ZHANG Yaling
(Research Center of Password Theory and Network Security, Xi'an University of Technology, Xi'an 710054)

【Abstract】 Grid computation system is a dynamically changed environment, the trust relationship among sites is restricted by some factors. This paper proposes a new grid security trust model, and establishes the concept of trust on the foundation of grid site's identity trustworthiness and behavior trustworthiness, computing power, unit server cost, previous success rate of job, intrusion detection capability and intrusion resistance capability. A new algorithm to evaluate grid site's behavior trustworthiness is constructed. An algorithm to evaluate grid site's integrated trustworthiness is proposed based on fuzzy integration evaluation theory of fuzzy mathematics. By means of the algorithm, trustworthiness among sites can be evaluated comprehensively and completely. Security and reliability of grid behavior can be guaranteed greatly.

【Key words】 Grid computation; Trustworthiness; Behavior trustworthiness; Trustworthiness evaluation; Fuzzy integration evaluation

网格技术[1]是近年来发展起来的新技术，是由地理上分布的异构计算机和资源组成的分布式高性能计算机环境。这样的环境具有极强的数据处理能力，同时也存在巨大的安全隐患。网格计算不仅会遇到如认证、访问控制、完整性、机密性、不可否认性等安全问题，同时因其自身特点，要面对前所未有的安全挑战。例如网格系统具有异构性、动态性、分布式系统和并行计算系统的特征。并行计算涉及数以百计不同安全域的计算机，大量计算资源的介入导致无法像通常的基于C/S模式建立直接的安全关系。由于网格的动态和异构特征，要求同时使用多个管理域的资源、动态资源请求、复杂的通信结构及严格的性能等，因此很难在各站点间事先建立信任关系。

网格站点间的信任问题格外重要，它不同于一般分布网络中的信任[2]。一般分布网络只涉及身份信任、网格站点间信任的概念，除身份信任外，还应建立在站点完成指定工作任务的安全可靠性基础上。前者以站点的身份可靠性和行为可靠性保证，后者以站点的性能可靠性保证。对站点的信任应包括身份信任、行为信任、计算能力、单元服务开销、以往的工作成功率、入侵检测和入侵抵抗[3]能力。身份信任主要负责用户身份验证和权限等问题，可通过加密、数字签名、认证协议等方法实现。其他一切都应建立在身份可信的基础上，行为信任是更广义的可信赖性问题，站点间可监视和管理站点行为并基于这些行为建立信任等级，据此及时地、动态地调整信任关系，最大程度地保证网格行为安全可靠。

1 网格安全信任模型的定义

在现实生活中，对一个人的信任一般取决于直接接触的经验、可靠朋友的介绍、声誉(由先前行为决定)。在网格环境中，信任不是“黑或白”的，而是表示站点完成指定工作任务的可信度的灰色区域。把现实生活中的信任模型映射到网格环境中，就得到直接信任、推荐信任和声誉[4,5]等概念。

所谓信任度是指对某个实体的行为和性能能否达到所期望值的可靠性。这个值是由很多因素决定的动态值，范围可从“完全不可信”到“完全可信”。直接信任是指2个实体间根据以往的直接交往行为得出的信任等级关系。实体的声誉是指其他实体通过观察其过去行为并根据其表现而得出的综合期望值。在进行信任决策时，当2个实体间没有直接交往接触时，可借助对方的声誉(间接信任)抉择。当实体间长期没有直接或间接信任接触时，其信任关系会随时间而衰减。

在网格环境下，站点R_j向站点R_i提出服务请求，R_i计算评估R_j的信任度，如果其值大于一个预先规定值，R_i就为R_j提供服务(否则拒绝提供服务)。假设站点身份完全可信，定义站点的综合信任度如下：

定义1 考虑m个站点，第i个站点被描述为

基金项目：国家自然科学基金资助项目(60273089)；陕西省自然科学研究计划基金资助项目(2005F02)；西安理工大学科技创新基金资助项目(108210402)；西安市集成电路与软件专项基金资助项目(ZX04011)

作者简介：王晓峰(1966－)，女，博士生、副教授，主研方向：密码理论与网络安全，网格安全；张 璟，教授、博导；王尚平，教授；张亚玲，副教授

收稿日期：2006-01-29 **E-mail：**xfwang66@sina.com.cn

$R_i=\{B_i,P_i,C_i,JSR_i,IDC_i\}=\{u_1,...,u_5\}$

其中，$B_i(=u_1)$为行为信任度；$P_i(=u_2)$为计算能力；$C_i(=u_3)$表示单元服务开销；$JSR_i=(u_4)$表示先前的工作成功率；$IDC_i(=u_5)$为入侵检测和抵抗能力。

第 i 个站点的综合信任度为 $H=\Lambda(R_i)$，H 的确定与用户对站点的行为信任、计算能力、单元服务开销、以前的工作成功率、入侵检测和抵抗能力的不同要求相关。如机密性高的任务，用户可偏重对站点信任度的要求；要求效率高的任务，用户可偏重对单元服务开销的要求。当 H 超过某个值(如0.6)时，站点是可信的，即信任它有能力完成指定的任务。

2 网格站点行为信任度评估算法

关于行为信任度评估方法，文献[4,5]中提出了基于网格信任管理和把信任并入网格资源管理的方法；文献[6]提出了利用模糊逻辑理论评估行为信任度的方法。本文通过引进直接推荐信任因子、信任因子、信任程度阈值以及惩罚因子等参数，从数学的角度构造一个评估网格站点的行为信任度的新算法。

考虑 m 个资源站点，定义站点R_j的行为信任向量为

$B_j=(T_{1j},T_{2j},...,T_{mj})^T$

其中，T_{ij} $(1\le i,j\le m)$ 代表站点 R_i 对 R_j 的行为信任度，范围为[0,1]，0 代表完全不信任，1 代表完全信任。组合所有站点的行为信任向量，得到具有 m 个站点的网格环境的行为信任矩阵(trust matrix)为

$M=(B_1,B_2,...,B_m)=(T_{ij})_{m\times m}$

计算行为信任度 T_{ij}，站点R_j为了得到站点 R_i 提供的服务，首先从一个(或多个)可信站点 N_0 处提出申请，N_0 可作为 R_j 的直接推荐者。由于存在从 R_j 到 N_0 的路径和从 N_0 到 R_i 的路径，通过路径搜索服务可从目标站点 R_j 到源站点 R_i 定义路径为

$R_j\to N_0\to...\to N_k\to R_i$

其中，$N_1,...,N_k$ 为 N_0 的中介直接推荐者。

2.1 符号定义

(1) $dtv_{R_j}^{N_0}$:表示 N_0 对R_j的直接信任值，$dtv_{R_j}^{N_0}\in[0,1]$。

(2) $rtv_{R_j}^{N_0}$:表示 N_0 对 R_j 的推荐信任值，$rtv_{R_j}^{N_0}\in[0,1]$。

(3) $Cert_X$:站点 X 的证书。

(4) $History_{R_j}^{N_0}$: N_0 是 R_j 的直接推荐者的历史记录。

其中，N_0 为最近一次推荐 R_j 的直接信任值，记为 $Ndtv_{R_j}^{N_0}$；N_0 推荐R_j的总次数为成功次数 p 与失败次数 q 的和；每次推荐中含R_j到 N_0 的路径。

若 N_0 没推荐过R_j，则 $History_{R_j}^{N_0}\leftarrow NULL$。

(5) $History_{N_0}^{R_i}$: R_i 信任 N_0 的历史记录，记录了最近一次的 $rtv_{N_0}^{R_i}$，记为 $Nrtv_{N_0}^{R_i}$。

2.2 直接信任值的计算

输入 $(Cert_{N_0},Cert_{R_j},History_{R_j}^{N_0})$

计算 检查证书 $Cert_{N_0}$ 和 $Cert_{R_j}$ 的有效性。其中至少有一个无效时，则 $dtv_{R_j}^{N_0}\leftarrow 0$，否则

$$dtv_{R_j}^{N_0}\leftarrow\begin{cases}dt\times Ndtv_{R_j}^{N_0}+(1-dt)\times(1-\sigma^{p-\lambda q}), & p>\lambda q\\ 0, & p<\lambda q\end{cases}$$

其中，$dt\in[0,1]$是直接推荐信任因子，由 N_0 根据被推荐者的声誉来决定，如果 $Ndtv_{R_j}^{N_0}$ 不在历史记录中，即 N_0 第 1 次推荐 R_j，则 $dt=0$。$\sigma\in(0,1)$ 是 N_0 对 R_j 的信任程度的阈值，由系统初始化时决定，σ 越大，表示需要经过多次成功推荐后，才能达到较高的信任程度。λ 是惩罚因子，由系统初始化决定，N_0 推荐R_j的成功率越低，λ 越大。

输出 $dtv_{R_j}^{N_0}$，并且 $Ndtv_{R_j}^{N_0}\leftarrow dtv_{R_j}^{N_0}$。

2.3 推荐信任值的计算

源站点 R_i 核对路径搜索服务提供的路径，并计算路径上的推荐信任值。

假设 $P_1,...,P_k$ 是提供给 R_i 的 k 条路径，是授权路径。设 $N(P_i)$ 表示第 i 条路径上的推荐者集合$\{N_{i_1},N_{i_2},...,N_{i_{h_i}}\}$，$h_i$ 表示第 i 条路径上的推荐者个数。

若 $\forall P_s,P_t,N(P_s)\cap N(P_t)=\phi$，$(1\le s,t\le k)$，则称 $P_1,...,P_k$ 是相互独立的，记为 $DP(P_1,...,P_k)$。

若存在 s、t，满足 $N(P_s)\cap N(P_t)\ne\phi$，$(1\le s,t\le k)$，则称 $P_1,...,P_k$ 是相关的，记为 $RP(P_1,...,P_k)$。

推荐信任值 $rtv_{N_0}^{R_i}$ 的计算如下：

输入 $(History_{N_0}^{R_i},rtv_{P_1},rtv_{P_2},...,rtv_{P_k})$，$rtv_{P_l}=\min(dtv_{N_0}^{N_{j_1}},dtv_{N_{j_1}}^{N_{j_2}},...,dtv_{N_{j_k}}^{R_i}),(1\le l\le k)$

(1)当 $(P_1,...,P_k)$ 为独立路径时，推荐信任值为

$rtv_{N_0}^{R_i}=rt\times Nrtv_{N_0}^{R_i}+(1-rt)\times rtv_{comb}$

其中，$rtv_{comb}=\frac{1}{k}\sum_{l=1}^{k}rtv_{P_l}$，$rt$ 为信任因子，由 R_i 根据被推荐者的声誉决定，若 $Nrtv_{N_0}^{R_i}$ 不在历史记录中，$rt=0$。

(2) $(P_1,...,P_k)$ 是 k 个相关的路径时，把它们分成 w 个集合，记为 $SP_1,...,SP_w$，使每个集合中的路径独立，推荐信任值为

$rtv_{N_0}^{R_i}=rt\times Nrtv_{N_0}^{R_i}+(1-rt)\times rtv_{comb}$

其中，$rtv_{comb}=\frac{1}{w}\sum_{l=1}^{w}rtv_{P_{l_j}}$，$P_{l_j}$ 是从集合 SP_l 中随机选择的路径。rt 是信任因子，由 R_i 根据被推荐者的声誉决定，若 $rtv_{N_0}^{R_i}$ 不在历史记录中，$rt=0$。(在每个集合 SP_l 中随机选择一条路径作为计算推荐信任值的输入，是为了减少 R_i 的计算复杂度。)

2.4 行为信任度的计算

站点 R_i 计算对R_j的行为信任度 T_{ij}。

输入 $(History_{R_j}^{N_0},History_{N_0}^{R_i},dtv_{R_j}^{N_0},rtv_{N_0}^{R_i})$

计算 $T_{ij}=\mu\ dtv_{R_j}^{N_0}+\delta\ rtv_{N_0}^{R_i}$，$\mu,\delta\in[0,1]$为权重，由 R_i 根据 $History_{R_j}^{N_0}$ 和 $History_{N_0}^{R_i}$ 决定。

输出 T_{ij}。

3 网格站点信任度模糊综合评估算法

综合评估是对受到多个因素制约的对象作出总评价。由于从多个方面评价，难免带有模糊性和主观性，因此采用模糊数学方法综合评估将使结果尽量客观、真实。

(1)建立评估对象因素集：设第 i 个站点被描述为

$R_i=\{B_i,P_i,C_i,JSR_i,IDC_i\}=\{u_1,...,u_5\}$

其中，符号意义同第 1 节定义 1。假设身份完全可信，定义 R_i 为评估站点信任度的因素集。

(2)建立评估集为

$V=\{v_1,v_2,...,v_n\}$

其中，n 为评估等级数(正整数)，$v_t\in[0,1]$ $(1\le t\le n)$ 为第 t 级

评估标准。它们的值由具体应用决定。

(3)建立单因素评估：即建立从 R_i 到 $F(V)$的模糊映射

$f: R_i \to F(V), \forall u_s \in R_i$

$$u_s \mapsto f(u_s) = \frac{r_{s1}}{v_1} + \frac{r_{s2}}{v_2} + ... + \frac{r_{sn}}{v_n},\ 0 \le r_{st} \le 1,\ 1 \le s \le 5,\ 1 \le t \le n$$

其中，$\frac{r_{st}}{v_t}$ 表示 r_{st} 与 v_t 之间的对应关系，r_{st} 表示第 s 个因素 u_s 对于第 t 个等级 v_t 的隶属度。

由 f 可以诱导出模糊关系，得模糊评价矩阵为

$$\Delta = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ r_{51} & r_{52} & \cdots & r_{5n} \end{bmatrix}$$

其中，Δ 为单因素评估矩阵，于是(R_i, V, Δ)构成了对第 i 个网格站点的综合评估模型。

(4)综合评估：由于对 R_i 中各因素有不同侧重，需要对每个因素赋予不同权重(据具体应用确定)，它可表示为 R_i 上的一个模糊子集 $A = (a_1, a_2, ..., a_5)$，且规定 $\sum_{l=1}^{5} a_l = 1$。

综合评估模型为 $H = A \circ \Delta$。V 上的模糊子集为 $H=(h_1, h_2, ..., h_n)$

其中，$h_t = \sum_{l=1}^{5} (a_l \cdot r_{lt})$，($t$=1,2,...,$n$)。

如果 $\sum_{t=1}^{n} h_t \neq 1$，就对其结果进行归一化处理。

(5)用等级量化值$Y=(Y_1, Y_2, \ldots, Y_n)$对第 i 个站点的评估结果量化处理得出最终结果的量化值为

$$w_i = \sum_{l=1}^{n} (Y_l \cdot h_l)$$

如果该值大于某个预定的值(例如0.6)就认为站点是可信的，否则认为是不可信的。

在本方案中，确定权重分配 A 是项关键工作，可以根据不同类型的应用确定。

4 应用举例

评估集$V=\{v_1, v_2, ..., v_6\}=\{I,II,III,IV,V,VI\}$，如表 1 所示。

表 1 评估集

信任等级	量化值	具体描述
I	1.0	信任等级极高，没有任何潜在危害性
II	0.8	信任等级非常高，潜在危害性很小
III	0.6	信任等级高，潜在危害性比较小
IV	0.4	信任等级一般，潜在危害性一般
V	0.2	信任等级较低，潜在危害性比较大
VI	0.0	信任等级非常低，潜在危害性很大

假设某个站点被描述为

$R_i = \{B_i, P_i, C_i, JSR_i, IDC_i\} = \{u_1, ..., u_5\}$

权重分配为 A=(0.4, 0.2, 0.1, 0.2, 0.1)

假设对第 i 个网格站点进行的 100 次评估中，各因素在各个等级的分布如表 2 所示。

表 2 等级分布

信任等级 因素\评语	I	II	III	IV	V	VI
行为信任度	60	10	20	10	0	0
计算能力	50	30	10	5	5	0
单元服务开销	40	20	10	10	10	10
以前的工作成功率	50	20	10	10	5	5
入侵抵抗能力	40	40	5	10	5	0

评价矩阵为

$$\Delta = \begin{bmatrix} 0.60 & 0.10 & 0.20 & 0.10 & 0.00 & 0.00 \\ 0.50 & 0.30 & 0.10 & 0.05 & 0.05 & 0.00 \\ 0.40 & 0.20 & 0.10 & 0.10 & 0.10 & 0.10 \\ 0.50 & 0.20 & 0.10 & 0.10 & 0.05 & 0.05 \\ 0.40 & 0.40 & 0.05 & 0.10 & 0.05 & 0.00 \end{bmatrix}$$

评估结果为

$H = A \circ \Delta = (h_1, h_2, \ldots, h_6) = (0.52, 0.2, 0.135, 0.09, 0.035, 0.02)$

由输入等级量化值

$Y=(Y_1, Y_2, \ldots, Y_6)=(1.0, 0.8, 0.6, 0.4, 0.2, 0.0)$可知，第 i 个网格站点的最终评估结果为

$w_i = \sum_{l=1}^{6} (Y_l \cdot h_l) = 0.804$

即认为该结果是可信的。

5 结束语

网格计算被视为 21 世纪的新型网络基础架构以及未来 10 年中 IT 商业应用的主流。网格安全是影响网格技术应用的主要问题，网格站点间信任模型和信任关系的建立是网格安全关键技术之一，这些问题的研究对网格技术应用以及信息产业发展具有重要意义。

参考文献

1 Foster I, Kesselman C, Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations[J]. International Journal on Supercomputer Applications, 2001, 15(3).

2 Grandison T, Sloman M. A Survey of Trust in Internet Applications[J]. IEEE Communications Surveys & Tutorials, 2000, 3(4).

3 Ryutov T, Neuman C, Zhou L. Integrated Access Control and Intrusion Detection Framework for Secure Grid Computing[EB/OL]. http://gridsec.usc.edu/files/TR/TR9_IACIDRyutov.pdf, 2004.

4 Azzedin F, Maheswaran M. Evolving and Managing Trust in Grid Computing Systems[C]. Proc. of IEEE Canadian Conference on Electrical and Computer Engineering, Winnipeg, Manitoba, Canada, 2002-05: 1424-1429.

5 Azzedin F, Maheswaran M. Integrating Trust into Grid Resource Management Systems[C]. Proc. of International Conference on Paralle Processing, 2002-08: 47-54.

6 Song S, Hwang K, Macwin M. Fuzzy Trust Integration for Security Enforcement in Grid Computing[R]. USC Internet and GridComputing Lab, TR2004-2, 2004.