一种基于模糊集合的可用于网格环境的信任评估模型

张 琳[1], 王汝传[1,2], 张永平[3]
(1. 南京邮电大学计算机学院, 江苏南京 210003; 2. 南京大学计算机软件新技术国家重点实验室, 江苏南京 210093; 3. 中国矿业大学计算机学院, 江苏徐州 221008)

摘 要: 信任模型已成为网络安全研究的热点. 结合模糊集合理论在网格环境下重新给出了信任的描述机制. 在信任的综合评判中, 融入中间推荐节点的直接交互经验, 充分体现了主观因素的重要性. 鉴于信任的动态性, 结合时间衰减和路径衰减两因素给出了新的信任更新模型. 实验结果显示了模型的准确性和健壮性. 相信该模型的提出能为信任模型的进一步研究起推动作用.

关键词: 网格安全; 模糊集合; 信任评估; 信任更新
中图分类号: TP393 文献标识码: A 文章编号: 0372-2112 (2008) 05-0862-07

A Trust Evaluation Model Based on Fuzzy Set for Grid Environment

ZHANG Lin[1], WANG Ru-chuan[1,2], ZHANG Yong-ping[3]
(1. *College of Computer, Nanjing University of Post and Telecommunications, Nanjing, Jiangsu 210003, China;*
2. *State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu 210093, China;*
3. *College of Computer, China University of Mining and Technology, Xuzhou, Jiangsu 221008, China*)

Abstract: Trust model has become the focus of network security. The description of trust is given newly with fuzzy set theory for grid environment. In course of trust synthesis evaluation, direct interaction information of the middle recommendation node is presented, which expresses the importance of subjective factor. According to the dynamic character of trust, a new model of trust renewal is provided, which is based on the two factors of time attenuation and path attenuation. Experimental results show that the model is exact and robust. It can impel the further research of trust model.

Key words: grid security; fuzzy set; trust evaluation; trust renewal

1 引言

网格环境的异构性和动态性等特点对安全问题提出了新的要求, 传统的基于静态的认证和访问控制等机制已不能满足用户的需求. 以网格安全基础设施 GSI (Grid Security Infrastructure) 为例, 针对外部的威胁, 它可以提供身份认证、通信加密等安全措施, 但是, 并不能保证加入网格的实体都是善意的实体, 即不能对实体在网格中的行为进行评判. 因此, 对信任模型的研究逐渐被提到日程上来, 现已成为各应用领域(网格、P2P 和网构软件等) 中对安全机制研究的热点.

信任是一个对象从自身角度出发对另一对象行为的合作程度(提供高质量服务、无恶意性等) 的主观度量, 它独立于对合作过程的监控, 评判结果除了满意和不满意之外, 还包括一种不确定性的因素. 现有典型的信任模型有 Beth 模型[1]、Jøsang 模型[2,3] 和 Abdul-Rahman 模型[4] 等, 他们都试图用概率论作为数学工具来解决信任模型中遇到的各种问题, 无法确切地描述信任模型中的不确定性因素. 人们需要寻求新的方法来解决这个问题, 文献[5] 首次将 D-S (Dempster-Shafer) 证据理论引入进来试图解决不确定性问题, 其在对独立证据的信息合并方面表现出一定的优势, 但在信任值的获取方面仍存在不足; 文献[6] 结合模糊集合理论给信任模型的研究提供了一个新的思路, 但概念比较抽象, 缺少具体化的深入描述. 除这些研究成果外, 结合网格环境, 文献[7] 还给出了基于行为的信任模型.

因此, 我们讲信任作为一种信念的体现, 具有不确定性, 不能简单地使用概率论等精确的数学模型加以描

收稿日期: 2006-12-14; 修回日期: 2007-05-20
基金项目: 国家自然科学基金(No. 60573141, No. 70271050); 江苏省自然科学基金(No. BK2005146); 江苏省高技术研究计划(No. BG2004004, No. BG2005037, No. BG2005038, No. BG2006001); 国家高科技 863 项目(No. 2006AA01Z201, No. 2006AA01Z219, No. 2006AA01Z439); 南京市高科技项目(2006 软资 105); 现代通信国家重点实验室基金(No. 9140C1101010603); 江苏省计算机信息处理技术重点实验室基金(No. kjs050001, No. kjs06006)

述, 有必要结合模糊集合对其加以扩充, 本文对现有模型做了进一步探讨, 分别从信任的描述机制、信任的综合评判和信任更新三个方面展开了论述, 并给出了具体的定义与推导模型.

2　网格环境中的信任描述机制

回顾信任模型的发展历程, 早在 1994 提出的 Beth 模型[1] 中, 为了表达和度量信任关系, 它赋予信任一个实数值 $v(v\in[0,1])$. 该值描述了实体能够成功完成任务的概率, 由交互过程中累积的肯定经验与否定经验的统计数据根据精确的概率模型得出. 这种描述方法忽略了信任的模糊性和不确定性. Jøsang 模型[2,3] 作为另一经典的信任模型, 引入了事实空间和观念空间的概念, 使用三元组(b, d, u)来定义信任度. 其中 b, d, u 分别表示对陈述的信任程度、不信任程度和不确定程度. 模型虽考虑了不确定性的因素, 较 Beth 模型有所进步, 但归根到底还是依据精确模型加以解决, 换言之, 就是把信任的主观性等同于随机性.

文献[6] 将模糊集合理论成功地引入至信任模型中来, 较好地解决了信任的模糊性问题. 为了便于表达, 我们首先引入隶属函数的定义.

定义 **1**　设 U 是论域, 称映射 $\mu_A: U\to[0,1]$, $x\mapsto\mu_A(x)\in[0,1]$ 确定了一个 U 上的模糊子集 A, 映射 μ_A 称为 A 的隶属函数, $\mu_A(x)$ 称为 x 对 A 的隶属度.

以网格为研究背景, 将论域 U 定为实体集, 实体间的信任等级表述为 U 上的多个模糊子集, 例如分别用 T_1, T_2, T_3, T_4 表示"不信任"子集、"一般信任"子集、"非常信任"子集和"完全信任"子集. 则, 网格实体的信任度可用实体对各模糊子集的隶属度所组成的向量来表示, 即 $\boldsymbol{T}=(t_1, t_2, t_3, t_4)$.

这种描述方法能够解决非此即彼的排他关系, 已成为概率论的有力补充. 通常情况下, 人们会根据极大隶属度原则得出评判结果, 即取 $T'=\max\{t_1, t_2, t_3, t_4\}$. 由于评价集本身具有模糊性, 因此, 采用这种原则得出的结果较为粗糙. 另外, 这种向量的表示方法虽包含有模糊的信息, 但不具有直观性.

人们还是习惯于用一个数来进行评判, 因此, 我们将定量化处理[8] 引入进来, 具体可采用对各个信任等级实行百分制记分的办法. 比如记 $50\leqslant c_1<60$(不信任)、$60\leqslant c_2<70$(一般信任)、$70\leqslant c_3<80$(非常信任)、$80\leqslant c_4<90$(完全信任). 这样就得到关于信任等级的分数向量 $\boldsymbol{C}=(c_1, c_2, \cdots, c_n)$, 然后计算得分 S,

$$S=\frac{\boldsymbol{T}\boldsymbol{C}^{\mathrm{T}}}{\sum_{i=1}^{n}t_i}=\frac{\sum_{i=1}^{n}t_ic_i}{\sum_{i=1}^{n}t_i}$$

由于各信任等级的得分是一个区间, 所以我们选择一个具有代表性的得分 $S_{中}$, $S_{中}=\dfrac{\sum_{i=1}^{n}t_i\boldsymbol{c}_{中i}}{\sum_{i=1}^{n}t_i}$.

其中, $\boldsymbol{c}_{中i}$ 为各元素取区间的中间值组成的信任等级分数向量, 具体为$(c_{中1}, c_{中2}, c_{中3}, c_{中4})=(55, 65, 75, 85)$. 举例来说, 当网格资源节点的信任向量 $\boldsymbol{T}=(0.20, 0.28, 0.28, 0.32)$, 则有

$$S_{中}=\frac{(0.20\ 0.28\ 0.28\ 0.32)\cdot(55\ 65\ 75\ 85)^{\mathrm{T}}}{0.20+0.28+0.28+0.32}=71.67$$

由于 $70\leqslant71.67<80$, 因此该资源节点被评为"非常信任".

这种定量描述方法由于建立在模糊集合的基础之上, 因此, 评价结果中并没有丢失信任的模糊信息, 相反, 它综合了各信任等级的评价因素, 加之定量化处理, 使得结果更加直观. 当然, 这种方法同 Beth 模型提供的单一数值的描述方法存在有质的差别.

另外, 结合网格特色, 文献[9] 提出了分层的信任模型, 大致概括为域内直接信任, 域间直接信任, 域内推荐信任和域间推荐信任. 不管是哪一种信任, 都要首先解决信任类型的定义问题. 借鉴文献[10] 提到的信任粒度细化的思想, 我们给出了网格环境下作为评估对象的网格节点的信任树, 如图 1 所示.

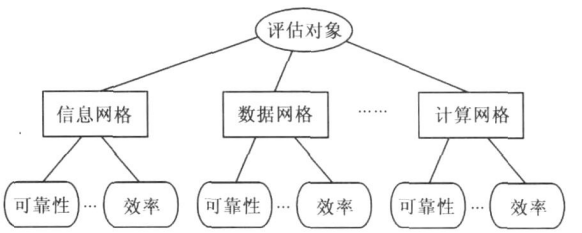

图 1　针对网格节点的信任树

考虑到网格实体均有所擅长, 比如说, 有的实体偏重于处理信息, 而不善于提供高性能计算, 我们称这样的实体集为信息网格. 同理, 还有数据网格, 计算网格和知识网格等. 在进行信任评估时, 为了不抹煞网格实体的个性, 我们将信任实体的粒度进行细化, 即, 按照实体的兴趣分为信息网格、数据网格等, 这也是信任本身的需求, 以免将评估结果一概而论. 比如, 网格用户关于资源处理计算的能力与数据网格中的实体 A 进行交互, 由于 A 擅长处理数据而不是计算, 因此, 网格用户对它的满意程度会很低. 在没有进行粒度细化之前, 网格用户会把这次交互结果作为对实体 A 的评价而保存下来, 很明显, 这样会以偏概全; 粒度细化后, 我们会把这次交互结果作为实体 A 在计算能力方面的评价记录下来, 而非对 A 的整体评价.

在实际工作中, 对一个事物的评价往往涉及多个因素或指标, 这时就需要根据这些因素对事物做出综

合评价, 而不是只从某一因素的情况去评价事物, 这就是综合评判. 比如, 有些网格用户对实体完成作业的可靠性比较关心, 而其他用户可能更关心效率, 将这些因素分别作为实体的属性加以考虑, 便得到了图 1 所示的二级信任树. 鉴于以上描述, 我们给出评估对象的信任类型定义.

定义 **2** 网格评估对象定义为一个五元组 O, $O=(\boldsymbol{IV}, \boldsymbol{AV}, \boldsymbol{TLV}, \boldsymbol{IM}, \boldsymbol{AM})$. 其中: $\boldsymbol{IV}$ 为网格节点的兴趣向量, $\boldsymbol{AV}$ 为节点属性向量, $\boldsymbol{TLV}$ 为信任等级向量, $\boldsymbol{IM}$ 为兴趣评判矩阵, $\boldsymbol{AM}$ 为属性评判矩阵.

下面以网格实体的兴趣为例, 给出模糊综合评判的数学模型的描述.

设 $\boldsymbol{IV}=(i_1, i_2, \cdots, i_m)$ 为 m 个兴趣分量, $\boldsymbol{TLV}=(v_1, v_2, \cdots, v_n)$ 为 n 个评判等级, 对每个兴趣针对评判等级作模糊映射, 便得到兴趣的隶属向量 $(r_{i1}, r_{i2}, \cdots, r_{in})$, 将这些隶属向量作为行构成的矩阵 $\boldsymbol{IM}=\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{m1} & \cdots & r_{mn} \end{pmatrix}$ 称为兴趣评判矩阵. 由于每个网格资源节点的特长不同, 因此, 需要为各特长赋予不同的权重向量 $\boldsymbol{W}=(w_1, w_2, \cdots, w_m)$, 以便能得到关于该节点的较客观的评价. 最后, 将权重向量与兴趣评判矩阵进行一次模糊变换便得到了各兴趣的综合评判向量. 以模型 $M(\wedge, \vee)$ 为例, 综合评判向量 $\boldsymbol{B}=(b_1, b_2, \cdots, b_n)$ 表示为:

$$(w_1, w_2, \cdots, w_m) \circ \begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{m1} & \cdots & r_{mn} \end{pmatrix} = (b_1, b_2, \cdots, b_n)$$

其中, "$\circ$" 为模糊运算符, $b_j=\bigvee_{i=1}^{m}(w_i \wedge r_{ij})$ $(j=1, 2, \cdots, n)$, $\vee$ 和 $\wedge$ 为扎德 max 和 min 算子.

依据本文提到的信任值的新描述方法, 最后需对评判向量进行定量化处理, 以使结果更加简洁明了.

3 信任评估模型

有了信任的定义, 接下来主要讨论信任评估模型, 分别对信任的传递、合并与更新三个方面作了阐述.

在信任网络中, 存在有三个实体: 评估者、推荐者和评估对象. 当评估者与评估对象之间存在有历史交互经验时, 我们说, 二者有直接信任关系; 否则, 评估者需要从熟人集合(推荐者集合)中选择自己认为信任度比较高的实体作为推荐者(其对评估对象有直接信任关系或推荐信任关系), 从而间接得到对评估对象的信任值, 我们称其为推荐信任关系.

考虑一下这两种信任关系. 在直接信任关系中, 评估者充当了交互的参与方, 由自己的经验得出直接信任值, 因此, 可信度较大. 但是, 不能完全相信直接信任关系. 为了抬高自己的信任度, 在交互初期, 评估对象可能故意表现地很优秀, 让评估者得到满意的交互结果, 所以, 评估者即便直接参与了交互, 其得到的直接信任值也未必是完全可信的.

对于推荐信任关系, 虽然评估者缺少直接经验, 但并不能忽略它. 我们说某个评估对象具有欺骗行为, 并不表示它对网格中的所有实体都有欺骗行为, 它只对某些网格实体具有针对性, 否则, 对其展开研究就失去了实际意义. 换言之, 评估对象可能在和评估者的直接交互中表现出欺骗性而不被觉察, 但对其他网格实体而言没必要实施欺骗, 即便存在这种行为, 真正具体到与每个网格实体进行交互时, 欺骗也已经被分担了. 因此, 由多个推荐者提供的有关评估对象的信任值对评估者有一定的参考价值.

简言之, 任何一个网格实体(包括评估者和推荐者)在评判评估对象的信任值时, 不仅要依据直接信任值, 还要考虑推荐信任值, 将二者以某种计算方法综合起来便得到了实体对评估对象的最终信任值.

通常情况下, 评估者和评估对象之间存在有一条推荐路径, 以网格域内推荐为例有 $A \Leftarrow B \Leftarrow C \leftarrow O$, 即, C 对 O 有直接信任关系, B 对 C 关于 O 有推荐信任关系, A 对 B 关于 O 也有推荐信任关系, 则 A 对 O 有推荐信任关系. 在对这种传递信任进行综合时, 不仅要考虑每个推荐者的推荐能力, 还要考虑各推荐者对评估对象的直接信任值. 另外, 还要关心路径的长度, 当长度大于某一指定阈值时, 将放弃这条推荐路径.

文献[11]在信任的传递过程中, 以路径 $A \Leftarrow B \Leftarrow C \leftarrow O$ 为例, 有, B 向 A 提供的有关 O 的推荐信任信息 = A 对 B 的推荐信任 $\otimes$ C 向 B 提供的有关 O 的推荐信息. 其中考虑了 B 的推荐因子这个因素, 但没有考虑 B 对 O 的直接信任值, 它在信任模型中是个比较重要的因素, 反映了 B 对 O 进行评判的个人意见, 即 B 的主观性的实施.

另外, 文献[11]所给模型使用二元组 $R=\langle t, d\rangle$ (其中, t 表示信任, d 表示不信任, 且 $t+d=1$)来量化实体间的信任关系, 这种精确的模型不能很好地描述信任的固有属性 ——不确定性.

为此, 我们借助模糊集合理论, 对信任信息的传递与合并机制展开了进一步的研究. 为便于描述, 我们首先给出算子 $\dot{+}$ 的定义, 其用意是将多个具有相同维数的向量矩阵化, 具体描述如下:

定义 **3**(算子 $\dot{+}$) 假设 P, Q 和 R 均是 n 维行向量, 即: $\boldsymbol{P}=(p_1, p_2, \cdots, p_n)$, $\boldsymbol{Q}=(q_1, q_2, \cdots, q_n)$, $\boldsymbol{R}=(r_1, r_2, \cdots, r_n)$, 则,

$$\boldsymbol{P}\dot{+}\boldsymbol{Q}\dot{+}\boldsymbol{R}=(p_1,p_2,\cdots,p_n)\dot{+}(q_1,q_2,\cdots,q_n)\dot{+}(r_1,r_2,\cdots,r_n)=\begin{bmatrix}p_1 & p_2 & \cdots & p_n\\ q_1 & q_2 & \cdots & q_n\\ r_1 & r_2 & \cdots & r_n\end{bmatrix}_{3\times n}$$

3.1　信任信息的传递

网格环境的动态性使得在不同的上下文环境中对同一网格实体的信任程度可能不同, 因此, 为了方便下文描述, 均默认: 所有公式的推演过程均是在同一上下文环境中进行.

为了将各章节连贯起来系统化, 我们依然把评判等级分为 n 级, 即有 n 个模糊评判子集. 我们把实体间的直接信任关系对各模糊子集的隶属度所组成的向量称为直接信任向量; 网格推荐者提供的经自己处理过的有关评估对象的信任评价结果对各模糊子集的隶属度所组成的向量称为推荐信息向量; 另外, 为了描述信任的传递机制, 我们还要用到两个变量: 推荐者的推荐因子和权重向量(各实体针对个人情况对直接信任和推荐信任赋予的不同权重所组成的二元向量). 这 4 个元素的符号描述如下:

(1) 直接信任向量: $\boldsymbol{DT}_O^A=(v_O^A(1),v_O^A(2),\cdots,v_O^A(n))$;

(2) 推荐信息向量: $\boldsymbol{RT}_{O(h)}^{A\leftarrow R_h}=(v_{O(h)}^{A\leftarrow R_h}(1),v_{O(h)}^{A\leftarrow R_h}(2),\cdots,v_{O(h)}^{A\leftarrow R_h}(n))$;

(3) 推荐因子: $\boldsymbol{RW}_O^{R_{i+1}\leftarrow R_i}$;

(4) 权重向量: $\boldsymbol{W}_{dr}=(w_d,w_r)$.

其中, $\boldsymbol{DT}_O^A$ 表示 A 对 O 的直接信任; $\boldsymbol{RT}_{O(h)}^{A\leftarrow R_h}$ 表示 R_h 提供给 A 的有关评估对象 O 的推荐信息, h 表示 R_h 是推荐路径中的第 h 个推荐者(离评估对象最近的那个推荐者称为第 1 个推荐者), 其在一定程度上反映了推荐路径的长度, 对推荐路径的取舍起到重要作用; $\boldsymbol{RW}_O^{R_{i+1}\leftarrow R_i}$ 表示 R_i 在向 R_{i+1} 提供有关 O 的信任评价的过程中 R_i 的推荐因子, 其反映了 R_i 作为推荐者提供有关 O 的推荐信息的准确性; 在权重向量 $\boldsymbol{W}_{dr}=(w_d,w_r)$ 中, w_d 表示网格实体对直接信任赋予的权值, w_r 则表示对推荐信任赋予的权值, 且有 $w_d+w_r=1$.

结合图 2, 我们给出信任传递的模型. 其中, A 为评估者; O 为评估对象; $R_i(i=1,2,\cdots,h)$ 为推荐路径上的各个中间推荐者.

图 2　信任传递

定义 **4**(推荐信息)　信任信息在推荐路径上进行传递的过程中, 每个中间推荐者都会对从其前一个推荐者处传过来的关于评估对象信任值的推荐信息进行再加工, 即, 融入自己对评估对象的直接信任的评价, 将二者按照权重综合后, 再得到关于评估对象的信任信息(推荐信息). 以由 R_h 向 A 提供的关于 O 的推荐信息 $\boldsymbol{RT}_{O(h)}^{A\leftarrow R_h}$ 为例, 采用递归的定义方法, 有:

$$\boldsymbol{RT}_{O(h)}^{A\leftarrow R_h}=\boldsymbol{W}_{dr(h)}\bullet\left(\boldsymbol{DT}_O^{R_h}\dot{+}(\boldsymbol{RW}_O^{R_h\leftarrow R_{h-1}}*\boldsymbol{RT}_{O(h-1)}^{A_h\leftarrow R_{h-1}})\right)=(v_{O(h)}^{A\leftarrow R_h}(1),v_{O(h)}^{A\leftarrow R_h}(2),\cdots,v_{O(h)}^{A\leftarrow R_h}(n))$$

或

$$(v_{O(h)}^{A\leftarrow R_h}(1),v_{O(h)}^{A\leftarrow R_h}(2),\cdots,v_{O(h)}^{A\leftarrow R_h}(n))=(w_{d(h)},w_{r(h)})\bullet\begin{bmatrix}v_O^{R_h}(1) & v_O^{R_h}(2) & \cdots & v_O^{R_h}(n)\\ \boldsymbol{RW}_O^{R_h\leftarrow R_{h-1}}*v_{O(h-1)}^{A\leftarrow R_{h-1}}(1) & \boldsymbol{RW}_O^{R_h\leftarrow R_{h-1}}*v_{O(h-1)}^{A\leftarrow R_{h-1}}(2) & \cdots & \boldsymbol{RW}_O^{R_h\leftarrow R_{h-1}}*v_{O(h-1)}^{A\leftarrow R_{h-1}}(n)\end{bmatrix}_{2\times n}$$

其中, "•" 为普通矩阵乘法算子; $w_{d(h)}$ 为第 h 个推荐者对直接信任赋予的权值, $w_{r(h)}$ 则为对推荐信任赋予的权值. 显而易见, 各个推荐者根据个人信念情况可以给出不同的权重向量值, 即任何一个网格推荐实体的主观意志都可以对最终推荐结果做出贡献, 从而形象地刻画了网格环境中自治域内的信任模型.

说明: (1) $\boldsymbol{RT}_{O(1)}^{A\leftarrow R_1}=\boldsymbol{DT}_O^{R_1}$

(2) $\boldsymbol{TT}_O^A=(w_{d(A)},w_{r(A)})\bullet\left(\boldsymbol{DT}_O^A\dot{+}(\boldsymbol{RW}_O^{A\leftarrow R_h}*\boldsymbol{RT}_{O(h)}^{A\leftarrow R_h})\right)$

其中, $\boldsymbol{TT}_O^A$ 为该传递路径提拱的关于 O 的信任信息向量. 该模型隐藏了推荐路径的拓扑信息, 仅蕴含有路径长度 h 的信息, 因此, 具有一定的安全性.

3.2　信任信息的合并

当存在多条推荐路径时, 我们需要提供适当的策略对它们进行合并, 以便得出评估者对评估对象的最终信任评估值. 在各传递路径中存在两种普遍现象: 传递路径间相对独立与传递路径间存在有中间推荐节点的交叉现象. 针对第二种现象, 我们采取的合并策略是: 在这些交叉路径中, 随机选出一条路径作为这组交叉路径的代表, 然后与第一种现象中的各相对独立的路径按照下文提供的具体方案进行信任信息的合并.

在这种理论背景下, 结合图 3, 我们给出信任合并的模型. 其中, A 为评估者; O 为评估对象; 由于评估者只关心离其最近的推荐者所提供的信任信息, 则用 $R_i(i=1,2,\cdots,m)$ 分别表示各推荐路径的最后一个推荐者. 这样, A 就需要将多条推荐信息以某种策略加以合并, 从而得到

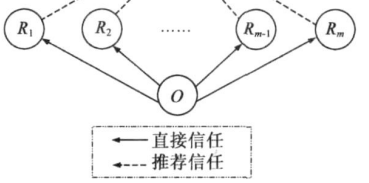

图 3　信任合并

关于 O 的最终推荐信息.

定义 5(合并信息) 我们用 $\boldsymbol{CT}_O^A$ 表示 A 通过合并处理后得到的关于 O 的推荐信息; $\boldsymbol{W}_{CT}$ 表示 A 对推荐信息进行合并时所赋予的各条推荐路径的权重向量, 有:

$$\boldsymbol{CT}_O^A = \boldsymbol{W}_{CT} \cdot \left(\boldsymbol{RT}_{O(h_1)}^{A\leftarrow R_1} \dot{+} \boldsymbol{RT}_{O(h_2)}^{A\leftarrow R_2} \dot{+} \cdots \dot{+} \boldsymbol{RT}_{O(h_m)}^{A\leftarrow R_m} \right)$$
$$= (\boldsymbol{CT}_O^A(1), \boldsymbol{CT}_O^A(2), \cdots, \boldsymbol{CT}_O^A(n))$$

其中,

$$\boldsymbol{W}_{CT} = \left(\boldsymbol{RW}_O^{A\leftarrow R_1} \Big\backslash \sum_{j=1}^{m} \boldsymbol{RW}_O^{A\leftarrow R_j}, \boldsymbol{RW}_O^{A\leftarrow R_2} \Big\backslash \sum_{j=1}^{m} \boldsymbol{RW}_O^{A\leftarrow R_j}, \cdots, \boldsymbol{RW}_O^{A\leftarrow R_m} \Big\backslash \sum_{j=1}^{m} \boldsymbol{RW}_O^{A\leftarrow R_j} \right)$$
$$\left(\boldsymbol{RT}_{O(h_1)}^{A\leftarrow R_1} \dot{+} \boldsymbol{RT}_{O(h_2)}^{A\leftarrow R_2} \dot{+} \cdots \dot{+} \boldsymbol{RT}_{O(h_m)}^{A\leftarrow R_m} \right)$$
$$= \begin{bmatrix} v_{O(h_1)}^{A\leftarrow R_1}(1) & v_{O(h_1)}^{A\leftarrow R_1}(2) & \cdots & v_{O(h_1)}^{A\leftarrow R_1}(n) \\ v_{O(h_2)}^{A\leftarrow R_2}(1) & v_{O(h_2)}^{A\leftarrow R_2}(2) & \cdots & v_{O(h_2)}^{A\leftarrow R_2}(n) \\ & \cdots & & \\ v_{O(h_m)}^{A\leftarrow R_m}(1) & v_{O(h_m)}^{A\leftarrow R_m}(2) & \cdots & v_{O(h_m)}^{A\leftarrow R_m}(n) \end{bmatrix}_{m\times n}$$

$h_i (i = 1, 2, \cdots, m)$ 表示第 i 条推荐路径所蕴含的路径长度. 随着 h_i 的增大, 该路径所提供的推荐信息的可信度将降低, 而当 h_i 大于某一指定阈值时, 将不再合并该推荐路径.

在信任信息的传递与合并过程中都提到了推荐因子, 许多文献也只是引用了其含义, 很少有对其展开具体描述的. 在此, 我们给出了一种具体表达方式, 以供参考. 以 $\boldsymbol{RW}_O^{A\leftarrow R_i}$ 为例, 有:

$$\boldsymbol{RW}_O^{A\leftarrow R_i} = \frac{S_{AR_i}}{F_{AR_i} + S_{AR_i}} * \beta^{\frac{1}{F_{AR_i}+S_{AR_i}}} * e^{-\left(\frac{\Delta\tau_i}{\alpha_\tau} + \frac{h_i}{\alpha_h}\right)}, \quad 0 < \beta < 1$$

其中, S_{AR_i} 表示 A 与 R_i 交互成功的次数, F_{AR_i} 表示交互失败的次数. 则, $\frac{S_{AR_i}}{F_{AR_i}+S_{AR_i}}$ 为 A 与 R_i 交互成功的频率, 当交互次数很多时, 可看成交互成功的概率; $\beta^{\frac{1}{F_{AR_i}+S_{AR_i}}}$ 则反映了交互的次数对推荐因子的影响, 即, 交互次数越多, 所提供的推荐信息的可信度越高, 相应地, 推荐因子也就越大. 这两项均由交互的历史记录数据计算而来, 因此可作为推荐因子的初始值, 并随着交互的动态进行而实时更新.

另外, 在指定的网格上下文环境中(R_i 作为 A 对 O 传递信任路径中的一个中间推荐者), $\Delta\tau_i$ 表示 R_i 参与的本次交互与最近的上一次交互之间的时间间隔; h_i 表示 R_i 在推荐路径中的位置. $e^{-\left(\frac{\Delta\tau_i}{\alpha_\tau} + \frac{h_i}{\alpha_h}\right)}$ 作为动态性的一面, 反映了推荐因子随时间间隔和路径长度的变化而波动的趋势, 即, 随着时间间隔和推荐路径的增加, 推荐因子将会降低, 其中, α_τ 和 α_h 分别为常量, 称为时间衰减因子和路径衰减因子. 概括而言, 该表达式能从一个侧面客观地反映各因素对推荐因子的影响.

到目前为止, 我们经过了信任的传递与合并, 得到的依然是对评估对象 O 的推荐信任信息. 如果想得到 A 对 O 的最终信任信息还需要将 A 对 O 的直接信任信息综合进来. 若我们用 $\boldsymbol{T}_O^A$ 表示 A 对 O 的最终信任向量, 则有:

$$\boldsymbol{T}_O^A = (w_{d(A)}, W_{r(A)}) \cdot \left(\boldsymbol{DT}_O^A \dot{+} \boldsymbol{CT}_O^A \right)$$

依据本文思想, 最后需要将向量 $\boldsymbol{T}_O^A$ 进行定量化处理成一个数值(信任值). 若该值能够满足 A 的需求(大于等于 A 事先规定的一个信任阈值), 则, A 相信 O 能提供相关服务, 可以和它进行作业交互; 否则, A 不信任 O, 拒绝与之进行作业交互.

3.3 信任信息的更新

任何一个实体的信任信息都不是一成不变的, 因此, 在综合评判之后, 我们需要对其进行实时更新, 为了降低系统实施维护的成本, 可采用定期更新的思想, 这在现实中也是可行的.

为便于表达更新模型, 需借鉴模糊集合中有关贴近度的概念. 它是对两个模糊集接近程度的一种度量, 在此, 我们对其加以修改, 用来表示两个信任向量接近程度的一种度量.

定义 6(贴近度函数) 假设有两个信任向量 $\boldsymbol{A} = (a_1, a_2, \cdots, a_n)$ 和 $\boldsymbol{B} = (b_1, b_2, \cdots, b_n)$, 分别进行归一化运算, 即

$$\boldsymbol{A}' = (a_1', a_2', \cdots, a_n') = \left(a_1 \Big\backslash \sum_{i=1}^{n} a_i, a_2 \Big\backslash \sum_{i=1}^{n} a_i, \cdots, a_n \Big\backslash \sum_{i=1}^{n} a_i \right),$$
$$\boldsymbol{B}' = (b_1', b_2', \cdots, b_n') = \left(b_1 \Big\backslash \sum_{i=1}^{n} b_i, b_2 \Big\backslash \sum_{i=1}^{n} b_i, \cdots, b_n \Big\backslash \sum_{i=1}^{n} b_i \right),$$

则 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 的最大最小贴近度函数 $N_M(\boldsymbol{A}, \boldsymbol{B})$ 为:

$$N_M(\boldsymbol{A}, \boldsymbol{B}) = \frac{\sum_{i=1}^{n} (a_i' \wedge b_i')}{\sum_{i=1}^{n} (a_i' \vee b_i')}$$

由定义知, $0 < N_M(\boldsymbol{A}, \boldsymbol{B}) \leqslant 1$, 且当它越趋近于 1 时, 说明 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 两向量越接近.

我们分别将其用于信任向量的更新和各实体推荐因子的更新, 如果令 $N_M = N_M(\boldsymbol{T}_O^A, \boldsymbol{Old\_T}_O^A)$(其中, $\boldsymbol{Old\_T}_O^A$ 为本次交互之前的信任向量值)和 $N_M' = N_M(\boldsymbol{T}_O^A, \boldsymbol{RT}_{O(h_i)}^{A\leftarrow R})$, 则有下面两个更新公式:

(1)信任的更新:

$$\boldsymbol{New\_T}_O^A = \begin{cases} N_M * \boldsymbol{Old\_T}_O^A + (1 - N_M) * \boldsymbol{T}_O^A, & 0 \leqslant N_M \leqslant 0.5 \\ (1-\delta) * \boldsymbol{Old\_T}_O^A + \delta * \boldsymbol{T}_O^A, & 0.5 < N_M \leqslant 1 \end{cases} \quad (0 < \delta < 1)$$

(2) 推荐因子的更新:

$$New\_\ \boldsymbol{RW}_O^{A\leftarrow R_i}=\begin{cases}\varepsilon, & N'_M \leqslant \omega\\ \varepsilon+\dfrac{N'_M-\omega}{\Omega-\omega}*(1-2\varepsilon), & \omega\leqslant N'_M<\Omega\\ 1-\varepsilon, & N'_M\geqslant\Omega\end{cases}$$

在信任的更新过程中, 当 $N_M \leqslant 0.5$ 时, 说明前后两次得到的信任值差别较大, 因此, 更新时权值偏重于 $\boldsymbol{T}_O^A$; 当 $N_M > 0.5$ 时, 说明二值比较接近, 谈不上孰重孰轻, 所以可按照习惯给定一个权重参数 δ 来实施更新操作.

在对各实体的推荐因子进行更新时, 需要设定两个门限 ω 和 Ω, 其中 $0<\omega<\Omega<1$. 当 $N'_M \leqslant \omega$ 时, 我们认为该推荐者提供的推荐信息不真实, 或者说是"恶意"的推荐者, 那么就将其推荐因子降为最低值 ε 以示惩罚; 而当 $N'_M \geqslant \Omega$ 时, 虽然其推荐的信息很真实, 为了防止欺骗行为我们不可以将推荐因子升为最高值 1, 而是以某个上限值 $1-\varepsilon$ 来代替; 其他情况下, 我们就依据 N'_M 的大小来更新推荐因子, 当 N'_M 的值增加时, 我们便抬高其推荐因子; 否则, 降低其推荐因子.

4　仿真分析

实验一　信任传递仿真.

该实验主要是证明, 在信任的传递路径中, 各中间推荐者与评估对象的直接交互经验对最终推荐信息的影响. 结合文献[11]提到的信任传递的思想, 给出了两种模型的对比测试方案. 以图 2 的拓扑结构作为本实验的背景, 令 $h=5$, 即存在 5 个中间推荐者, 分别为 R_1~R_5, 评估者 A 通过 R_1~R_5 的推荐得到关于评估对象 O 的推荐信任信息. 实验结果如图 4 所示.

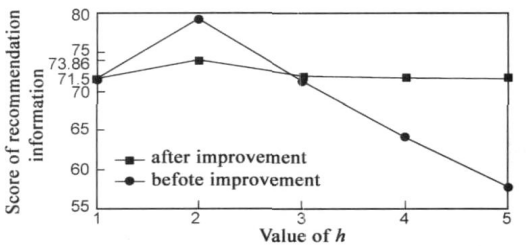

图 4　信任传递仿真

其中, 横坐标表示信任的传递过程, 即从 R_1 传到 R_5, 最后提交给 A; 纵坐标表示推荐信息的分数值. 我们将信任等级分为 3 级, 分别为"不信任"、"一般信任"和"完全信任". 并对这三个等级以百分制记分的方法加以定量化处理, 取 $40\leqslant c_1<60$(不信任)、$60\leqslant c_2<80$(一般信任)、$80\leqslant c_3<100$(完全信任), 则, $(c_{中1}, c_{中2}, c_{中3})=(50, 70, 90)$. 为突出本实验的仿真重点, 我们将影响推荐信息的其他因素作了简化, 令 $\alpha_h=20$; 各中间推荐者关于直接信任和推荐信任所给的权重向量值相等, 均为 $(w_{d(h)}, w_{r(h)})=(0.8, 0.2)$; R_1~R_5 的推荐因子均取 $\boldsymbol{RW}_O^{R_{i+1}\leftarrow R_i}=0.9$; O 的真实评估向量值通过交互的统计数据得(0.4, 0.4, 0.5), 即评分为 71.539 分.

假设推荐节点 R_1 是"恶意"的, 其他节点均为"善意"的, 则各节点得到的关于 O 的直接交互信息都是准确的, 均为 71.539 分. 至于得到的各推荐信息, 两模型表现出了明显的不同. R_1 为了有意提高 O 的交互能力, 将得到的直接信任向量(0.4, 0.4, 0.5)篡改为(0, 0.1, 0.9)之后再传递给 R_2, 即把评分由 71.539 分改为 88 分. 文献[11]在信任的传递过程中由于未考虑推荐者的直接交互经验, 因此, R_2 得到的关于 O 的推荐信息分值降为 79.2 分; 改进之后, R_2 在收到 R_1 提供的恶意推荐信息后, 将自己对 O 的直接交互信任值融入进来, 得到自己关于 O 的推荐信息 $\boldsymbol{RT}_{O(2)}^{A\leftarrow R_2}=(0.8\ \ 0.2)\cdot\begin{bmatrix}0.4 & 0.4 & 0.5\\ e^{-1/20}*0.9*0 & e^{-1/20}*0.9*0.1 & e^{-1/20}*0.9*0.9\end{bmatrix}=(0.32\ \ 0.3371\ \ 0.5541)$, 即 73.866 分. 与 O 的真实得分 71.539 分相比, 改进后的模型对"恶意"推荐有较强的抵御能力.

另外, 改进后的模型由于考虑的因素较为全面, 推荐信息的分值随着推荐路径的推移呈现平稳变化的趋势, 而且最终推荐信息的分值 71.547 分比较靠近真实得分 71.539 分; 而改进前的模型, 曲线变化波动较大, 最终推荐信息的分值 57.737 分与真实得分偏差较大. 因此, 改进后的模型具备了准确性和健壮性的优点.

实验二　信任更新仿真.

该实验主要展示, 各推荐者的推荐因子随更新次数不断增加的变化趋势. 实验结果如图 5 所示. 我们设定每 10 次交互更新一次推荐因子, 则横坐标表示更新的次数; 纵坐标代表了推荐因子这个分量.

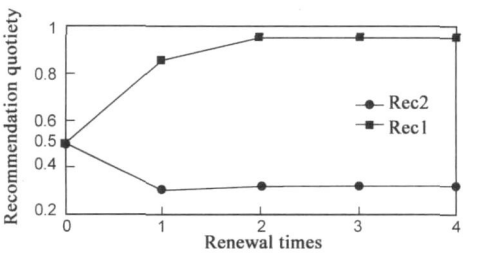

图 5　信任更新仿真

实验背景仍以图 2 的传递拓扑结构为例, 令 $h=2$, 即存在两个推荐者 R_1 和 R_2, 同样, 设 R_1 为"恶意"的, 其他均为"善意"节点. 为了强调推荐因子对评估结果的影响, 令权重向量 $(w_{d(h)}, w_{r(h)})=(0.6, 0.4)$; 由于背景是信任传递, 因此, 计算推荐因子时忽略时间衰减因素, 突出路径衰减因素, 取 $\alpha_h=20$; 假定通过交互的历史数据得 R_1 和 R_2 的推荐因子的初始值均为 0.5, O 的真实信任值和 R_1 的恶意程度同实验一; 另外, 对于推荐

因子的更新模型取 ε= 0.05, ω= 0.1, Ω= 0.9.

结果显示, 当第 2 次更新时, R_2 的推荐因子就已从初始值 0.5 升至最高值 1- ε= 0.95(R_2 是善意的, 推荐的信息具有高可信性); 相反, 由于 R_1 是恶意的, 其推荐因子也由 0.5 相应地降到 0.3, 说明模型具有高可分辨性. 另外, 经过数次交互, 各推荐因子在短期时间内都应该逐渐趋于平稳, 由实验曲线的变化趋势知, 本模型从一个侧面也能反映这一特征.

5 结束语

信任具有的主观性与不确定性的固有属性, 使得精确的数学模型难以进行描述, 结合模糊集合论的优势, 本文对信任过程的关键环节重新加以定义及具体化, 提高了模型的可用性. 首先, 利用计分的定量化处理方法, 在信任值隶属向量表示法的基础之上, 将各模糊信息再进行综合, 改为人们早已习惯的数值表示法; 结合网格特点, 对信任类型的定义加以细化, 使其能客观地反映网格节点的个人兴趣; 在信任的综合评判中, 我们强调各节点的主观意念, 将各自得到的直接交互经验融入其中, 给出了新的评估模型; 为了系统化地描述信任模型, 最后, 我们结合贴近度给出了信任的更新模型. 仿真结果表明了模型的精确性及健壮性.

参考文献:

[1] Beth T, Borcherding M, Klein B. Valuation of trust in open networks[A]. Gollmann D, ed. Proceedings of the European Symposium on Research in Security (ESORICS) [C]. Brighton: Springer-Verlag, 1994. 3- 18.

[2] Jøsang A, Knapskog SJ. A metric for trust systems[A]. Global IT Security[C]. Wien: Austrian Computer Society, 1998. 541- 549.

[3] Jøsang A. A logic for uncertain probabilities[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001, 9(3): 279- 311.

[4] Abdul-Rahman A, Hailes S. A distributed trust model[A]. Proc of the' 97 New Security Paradigms Workshop[C]. Cumbria: ACM, 1997. 48- 60.

[5] Yu B, Singh M P. An evidential model of distributed reputation management[A]. Proceedings of First International Joint Conference on Autonomous Agents and Multi-Agent Systems[C]. Bologna: ACM, 2002. 294- 301.

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

[7] Azzedin F, Maheswaran M. Evolving and managing trust in grid computing systems[A]. Electrical and Computer Engineering, IEEE CCECE 2002[C]. Canadian, 2002. 1424- 1429.

[8] 王新洲, 史文中, 王树良. 模糊空间信息处理[M]. 武汉: 武汉大学出版社, 2003. 124- 132.

[9] Azzedin F, Maheswaran M. A trust brokering system and its application to resource management in public-resource grids[A]. 18th International Parallel and Distributed Processing Symposium (IPDPS' 04) [C]. Santa Fe: IEEE Computer Society, 2004. 22- 32.

[10] 张骞, 张霞, 文学志, 刘积仁, Ting Shan. Peer-to-Peer 环境下多粒度 Trust 模型构造[J]. 软件学报, 2006, 17(1): 96- 107.
Zhang Q, Zhang X, Wen XZ, Liu JR, Ting Shan. Construction of peer-to-peer multiple-grain trust model[J]. Journal of Software, 2006, 17(1): 96- 107. (in Chinese)

[11] 王远, 吕建, 徐锋, 张林. 一个适用于网构软件的信任度量及演化模型[J]. 软件学报, 2006, 17(4): 682- 690.
Wang Y, Lü J, Xu F, Zhang L. A trust measurement and evolution model for internetware[J]. Journal of Software, 2006, 17(4): 682- 690. (in Chinese)

作者简介:

张 琳 女, 1980 年出生于江苏丰县, 南京邮电大学计算机学院 2005 级博士研究生. 主要研究领域为网格计算、网络安全、可信计算.
E-mail: wangrc@njupt.edu.cn

王汝传 男, 1943 年出生于安徽合肥, 教授、博士生导师. 主要研究方向是计算机软件、计算机网络和网格、信息安全、无线传感器网络、移动代理和虚拟现实技术等.

张永平 男, 1958 年出生于辽宁丹东, 副教授. 主要研究领域为信息安全、密码学.