软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(12):3130−3148 [doi: 10.3724/SP.J.1001.2012.04204]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种正态分布下的动态推荐信任模型*

邵 堃[1+], 罗 飞[1,3], 梅晓雄[1], 刘宗田[2]

[1](合肥工业大学 计算机与信息学院,安徽 合肥 230009)

[2](上海大学 计算机工程与科学学院,上海 200072)

[3](中国邮政储蓄银行 安徽省分行 科技发展部,安徽 合肥 230031)

Normal Distribution Based Dynamical Recommendation Trust Model

SHAO Kun[1+], LUO Fei[1,3], MEI Niao-Xiong[1], LIU Zong-Tian[2]

[1](School of Computer & Information, Hefei University of Technology, Hefei 230009, China)

[2](School of Computer Engineering and Science, Shanghai University, Shanghai 200072, China)

[3](Postal Savings Bank of China Anhui Branch, Department of Science and Technology, Hefei 230031, China)

+ Corresponding author: E-mail: shaokun@hfut.edu.cn

Shao K, Luo F, Mei NX, Liu ZT. Normal distribution based dynamical recommendation trust model. *Journal of Software*, 2012,23(12):3130−3148 (in Chinese). http://www.jos.org.cn/1000-9825/4204.htm

Abstract: On the basis of a continuous process, the recommendation trust model is built for depicting indirect trust, the most complicated trust relationship. The model is also significant for the security and reliability of an open environment and open systems. After the factors influencing indirect trust are quantified, the filtrated recommendations are regarded as samples from the normal process, and the Bayesian estimation value of posteriori distribution expectation is obtained from calculation. Next, after an elaborate discussion of the trust evolution and the relationship between trust value and trustworthiness along with some propositions and proofs are proposed. Experimental data show that with the capacity of resisting malicious attacks improved, the model gives a more effective and precise result, which is also consistent with mathematical deduction.

Key words: recommendation trust model; Bayesian estimation; normal distribution; trustworthiness; convergence

摘 要: 建立基于连续过程的推荐信任模型,描述间接信任这种最复杂的信任关系,在保障开放环境的安全和开放系统的可靠运行方面有着重要意义.通过量化间接信任影响因素,运用分级剪枝方法过滤推荐信息,将结果作为正态过程的采样样本,计算获取后验分布期望的 Bayesian 估计值.在此基础上,详细阐述信任动态演化的过程,深入探讨信任度和可信度之间的关系,给出了命题及其数学证明.实验数据表明,模型提高了抵御恶意攻击的能力,得出了更加有效和精确的结果,与相关命题的数学推导相一致.

关键词: 推荐信任模型;Bayesian 估计;正态分布;可信度;收敛性

中图法分类号: TP311 **文献标识码**: A

* 基金项目: 国家自然科学基金(60975033, 60575035, 60275022, 69985004); 安徽高校省级自然科学研究重点项目(KJ2010A272)

收稿时间: 2010-12-13; 修改时间: 2011-11-03; 定稿时间: 2012-02-22

1 引 言

1.1 背 景

信任管理[1,2]理论中的重要基础工作是建立动态信任模型[3−25].目前,研究的重点是对参与交互的对象之间的信任度进行实时计算,获得交互行为应该有的可能信任度,并提供决策帮助.针对开放环境,许多学者使用数学方法和工具建立了不同的模型,有效地推动了相关理论研究的发展.影响动态推荐信任模型的因素有很多,现有模型都认可直接信任的重要性,其次才是间接信任的影响.所谓直接和间接信任的建立主要是依赖信息收集,并通过相关计算得到.信任关系是一个逐步建立的过程,直接和间接信任在不同的时期起着不同的作用.

对间接信任建模是信任关系中最复杂和最困难的工作.现有模型希望通过量化信任关系中的各种要素,并在此基础上建立适当的信任描述.Beta 分布由于其本身的特性——变量取值范围在(0,1)区间,十分符合信任的特点,因此,许多模型用 Beta 分布来描述信任关系,但一些问题没有引起足够的重视:

1) 孤立地看待推荐信任度.计算过程中,仅仅使用推荐信任度的数值而没有考虑到数值之间存在的关联关系,比如偏差、数量、冲突等等;不能排除恶意和错误的推荐,推荐信息并不是精确的;割裂了直接信任与间接信任,从而忽视了两者之间的关系;
2) Bernoulli 过程的局限.Beta 分布是基于 Bernoulli 过程的,Bernoulli 实验只有两种结果.在 Beta 分布中,同一类型结果的信任度之间是无差别的,仅仅是数量的累积,并不能真正反映推荐的结果.文献[3]认为,“信任度失去容易得到困难”,因此无法排除 Bernoulli 过程中采样结果顺序的影响;
3) 信任动态性的认知问题.研究认为,开放环境下,信任具有动态性,但是现有文献对动态的刻画并不充分.信任的动态性并不等同于随机性,其变化过程有特定的原因,并遵循一定的规律.现有文献和模型对动态性的认知显然不足,仅仅强调信任是动态变化的,而没有提出是如何变化的.

信任本质上是一个社会心理关系,间接信任的形成,是人们通过直接经验或者心理预期并参考第三方的推荐形成的.这个过程中,存在着直接信息与间接信息的比较,以及对推荐信息的分析、辨别和过滤等行为.本文借鉴这一心理过程,使用 Bayesian 估计,建立了一种新的基于正态分布的推荐信任模型.针对直接信任和间接信任的关系,提出偏差、了解度、冲突及推荐数量等概念并将其量化,以此为基础,给出一种剪枝过滤机制.一个实体的可信度应该由其固有属性决定,外部实体对其充分的统一认知就是该实体的信誉,信任主体和其他实体对该实体的认知不足,是信任动态演化的一个原因,信任值的演化方向是该实体的信誉(可信度).针对这个观点,提出一些结论并予以证明.

本文第 1 节介绍一些背景和相关工作的研究进展.第 2 节详细讨论基于正态分布使用 Bayesian 估计的推荐信任模型.第 3 节给出动态性分析的一些结论及其证明.第 4 节通过模拟实验对本文的模型和观点进行论证和分析.第 5 节进行总结,并提出下一步的研究方向.

1.2 相关工作分析

1996 年,Blaze 等人[1,2]首次提出信任管理的概念,信任管理系统[2]也相应地在此基础上发展起来.近些年,随着开放、动态和难控网络环境[28]的发展,有关的安全问题得到了空前的重视.针对不同的环境,许多不同的信任关系模型被提了出来.如:Almenárez 等人[3−5]基于证据理论提出的 PTM 模型;Hassan 等人[7]提出了一种基于向量机制的信任模型;Jøsang[8]提出了一种使用 Beta 声誉的基于贝叶斯网络的信任模型;Dimitri[9]提出一种基于 Bayesian 网络模型、使用 Kalman 信息过滤机制的模型;George 等人[10,11]提出的基于半环的信任模型;Sun 等人[12,13]提出的基于熵理论的信任模型;He 等人[14]提出的基于云模型[15]的信任模型;以及 Song 等人[16]提出的基于模糊逻辑的信任模型等;Li 等人[17]结合人类社会的认知行为,提出了一种符合人类心理认知习惯的动态信任预测模型;Sun 等人[18]提出了一种使用 Beta 分布的基于贝叶斯决策的推荐信任度修正模型.

网构软件[28−32]是为了应对 Internet 环境对软件技术的挑战而提出的新概念,系统安全保障可信化[29]是重要的研究方向之一.信任管理和信任评估在网构软件的设计中非常重要,是系统安全保障可信化的基础.信任模型 TEM 和 DTME[26,27]分别就网构软件中推荐信任的收集与合并以及软件实体联盟的形成进行了深入研究.本文

的工作主要针对网构软件可信化保障问题展开,同时,这一研究工作也适用于其他开放的、动态的和难控的网络环境.

2 间接信任模型

信任的主体对客体完全不了解或者不够了解的时候,需要通过第三方建立信任关系,这种通过非直接交互行为得到的信任关系称为间接信任.许多文献认为,信任有弱单向传递性[4−8,25,26].即在一定约束条件下,主体可以通过第三方实体建立对客体的信任关系.推荐就是一种比较典型的信任传播方式.

间接信任是信任关系中最困难和最复杂的,因为它是涉及多方实体的关系.推荐信任关系中,并不能保证所有的推荐者都是诚实的,也不能确定所有诚实推荐者的推荐都是准确或者比较准确的.不仅如此,诚实推荐者之间的推荐同样存在差异.针对间接信任的特点,借鉴人类接受推荐的心理过程,建立了一种抵御恶意和错误推荐的机制,利用 Bayesian 估计模拟人类综合多种推荐信息做出判断的认知行为,使用连续过程的抽样,能够反映不同推荐度之间的差异,较现有模型更加合理.

2.1 分级剪枝过滤

推荐信任度和直接信任度的不一致,导致人们需要去考虑推荐信息.即主体的直接认识或者心理预期与第三方的推荐存在差异,是迫使人们考虑推荐信任度的直接原因.两者存在差异,表示不能确定直接信任是正确的,因此需要考虑推荐信息的价值.两者差异很小,说明外界对客体的认识基本趋于统一,此时,直接信任基本可信赖.

主体和第三方对客体认知不够完全和统一导致差异的产生,这就需要对不同推荐者的推荐进行区分和综合,得到间接信任度.推荐信息是推荐者对客体的直接认知(不考虑多级推荐),推荐关系是主体通过推荐信息对客体的间接认知.间接信任是通过对推荐信息分析、判断和处理形成的.推荐信任度和推荐者被主体信任的程度(主体对推荐者的信任度),是影响间接信任的最主要的因素.此外,其他一些因素也会影响到间接信任.

定义 1(偏差). 记 $t_{A,C}$ 为主体 A 对客体 C 的直接信任度,$r_{A,C}^{B_i}$ 为推荐者 B_i 的推荐信任度,偏差为

$$d_i = | r_{A,C}^{B_i} - t_{A,C} | \tag{1}$$

显然,推荐的偏差越大,可接受的程度越小.当还未直接交互时,$t_{A,C}$ 可用 0.5 或 A 的预期值代替.

定义 2(了解度). 推荐实体 B_i 对被推荐者 C(客体)的了解度为

$$u_i = \frac{n}{N} \mathrm{e}^{-\lambda(t-t_0)} \tag{2}$$

其中,N 表示一段时间内对客体完全了解所需的交互次数,n 表示实际成功交互次数,λ是系数,t_0 表示时间起点.了解度随交互成功次数递增,随时间递减,并且 $u_i \in [0,1]$.

定义 3(推荐冲突). 推荐实体 B_i 和其他推荐者之间的差异为

$$c_i = \sum_{j \neq i} | r_{A,C}^{B_j} - r_{A,C}^{B_i} | \tag{3}$$

c_i 越大,表示 B_i 的推荐越偏离大多数的推荐者,可接受的程度越小.

除了上述因素之外,推荐数量也是一个影响因素.

推荐信任中,并不能完全保证推荐者都是非恶意的.从推荐信任值来看,包括恶意高推荐和恶意低推荐;从推荐者来看,有高信任度者的恶意推荐和低信任度者的恶意推荐.恶意的高推荐和低推荐表现为推荐信任度的偏差过大.相比较来说,高信任度者的恶意推荐,比低信任度者的恶意推荐更隐蔽,更具有破坏性.

因此,在计算间接信任度之前,首先要过滤掉恶意和无用的推荐.可信度较低的推荐者推荐的参考价值是很低的;对于偏离直接经验或心理预期过大的推荐,也是难以接受的;对客体了解较多的推荐者的推荐值得参考,而了解较少的推荐者的推荐参考较少;多数者的意见比少数者的意见更值得信赖,所以推荐冲突较大的推荐也是不被接受的.根据这一认知过程,建立一种剪枝过滤机制,体现了在接受推荐信任中筛选有用信息的过程.

该机制是一种分层的结构,首先,根据信任主体对推荐者的信任度的等级对其进行划分;然后,考虑不同信

任等级的推荐者的推荐信任度所处的等级;综合考虑各种因素选择推荐信息.对信任度较高的推荐者,如果其推荐偏离直接信任度,在一定的偏差范围内认为该推荐也是可以接受的;而对信任度较低的推荐者,相应的,可接受的偏差范围会较小.

文献[7]给出了 *trust mapping* 的定义,根据不同的信任度划分不同的等级,给予不同的权限.

$$m(x)=\begin{cases}k, & r_k \leqslant x \leqslant 1\\ k-1, & r_{k-1} \leqslant x < r_k\\ \vdots & \vdots\\ 1, & r_1 \leqslant x < r_2\\ 0, & 0 \leqslant x < r_1\end{cases} \tag{4}$$

其中,x 表示信任度,k 表示等级.

图 1 表示分级过滤的示意图.$\{B_1,B_2,\ldots,B_n\}$表示某段时间内推荐者集合,首先,根据信任主体(A)对它们的信任度 (t_{A,B_i}) 将其划分为 k+1 级,不同的等级包含不同的推荐者集合$\{B_i\}_j$,不同等级的推荐者有不同的接受范围.

$$r_{A,C}^{B_{ij}} \in [t_{A,C}-\varepsilon_1^j, t_{A,C}+\varepsilon_2^j].$$

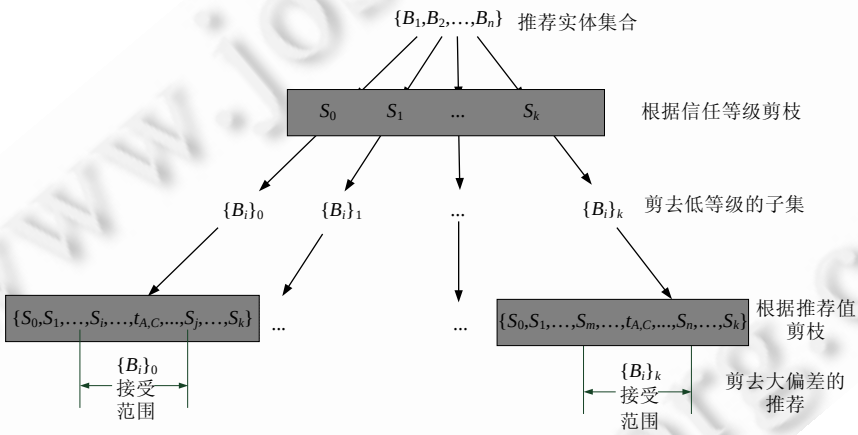


Fig.1 Filtrated by classification and pruning

图 1 分级剪枝过滤

分级剪枝过滤的过程如下:

1) 根据主体对推荐者的信任等级剪枝.在对$\{B_1,B_2,\ldots,B_n\}$划分级别的过程中,首先对左边信任度较低的集合进行剪枝,直接排除低信任度者的推荐;
2) 根据推荐的推荐信任度的等级剪枝.每个推荐者 B_{ij} 对客体(C)有不同的推荐度 $r_{A,C}^{B_{ij}}$,
   - 若 $r_{A,C}^{B_{ij}} \in [t_{A,C}-\varepsilon_1^j, t_{A,C}+\varepsilon_2^j]$,接受该推荐信任度;
   - 否则不接受,对步骤 1)中每个集合内部再次进行剪枝;
3) 根据单个推荐者进行剪枝.经过步骤 2)得到的集合中,综合考虑主体对推荐者的了解程度、推荐冲突及推荐数量,对每个推荐做进一步的评估.

分级剪枝过滤机制是一个由粗略到精确的剪枝过程.首先,直接剪去信任度较低的推荐者,减少了恶意推荐的可能;其次,在保留的集合内部再次剪去偏差较大的推荐,减少了不准确推荐的可能;最后,通过对单个推荐的综合分析,对不同的推荐做出具体的判断.该机制在最大程度上排除了恶意的和非正确的推荐结果,保证了信息的有效性和可用性.

2.2 基于正态分布的推荐信任模型

基于 Bernoulli 过程的 Beta 分布在 Bayesian 推断中很有用,但它局限于 Bernoulli 过程的假设,每次试验只能有两个可能的结果.事实上,信任度可以是[0,1]内的任何实数.用 Bernoulli 过程来描述推荐信任,只能简单地把结果分成两类,没有区分同类结果中不同推荐信任值的差别.在使用该过程的模型中,假如 0.8 和 0.85 两种推荐信任度在 Bernoulli 过程中属于同一类结果,则无法区分两者的不同.即在 Bernoulli 过程中,两者仅仅是数量上无差别的累积.在第 2.1 节的相关描述中,本文已经针对不同推荐信任值可能存在很大差别这一现象进行了深入的分析.

信任是一个动态过程,在直接交互和间接推荐的过程中不断演化.人类在处理推荐信息时,总是以直接经验为基础,参考推荐信息,然后做出判断.借鉴这一过程,首先把已知的间接信任作为先验分布;推荐信息作为抽样样本分布,得到样本边际密度函数;根据 Bayesian 公式就可以得出间接信任的后验分布;使用 Bayesian 估计得到的期望估计值即为参考推荐样本信息后间接信任的演化结果.

设间接信任度为μ,它是推荐者提供的对客体的认知结果,那么在非恶意和相对正确的推荐中,推荐信任值应当分布在μ附近.因此,把每一个推荐都看作是来自一个平稳的正态过程的采样,并且不同推荐者的推荐是独立的,相互之间没有影响,即可认为推荐信任度 $r_1,r_2,\ldots,r_n$ 是正态分布(μ,σ^2)的一个样本,其中,μ和σ都是未知的.

在接受第三方推荐的时候,对推荐者的信任度会在很大程度上影响对推荐信息的接受程度.对客体完全认知之前,主体和推荐者对客体的认知没有达到统一,推荐信任度和直接信任度之间存在偏差.显然,主体对其信赖的推荐者的推荐偏差容忍程度较大,而对信任度低的推荐者的推荐偏差容忍程度就较小.因此,对推荐信任度作如下修正:

$$\hat{r}_i = \hat{t}_i + t_i \times d_i \tag{5}$$

其中,d_i 是偏差,$\hat{t}_i$ 表示的是修正后的直接信任度.记推荐信息的样本向量为 $\vec{X} = (x_1, x_2, ..., x_n)$,其中,$x_i = \hat{r}_i$,因此,推荐信息样本联合条件概率函数为

$$p_{\vec{X}|\mu}(\vec{X} \mid \mu) = (2\pi\sigma^2)^{-\frac{n}{2}} \exp\left\{-\frac{1}{2\sigma^2}\sum_{i=1}^{n}(x_i-\mu)^2\right\} \tag{6}$$

均值μ是未知的,设μ是来自先验分布随机变量,那么它将分布在真实的间接信任度附近,认为μ服从以期望为θ,标准差为τ的正态分布,即

$$\mu \sim N(\theta, \tau^2),$$

μ是推荐信任度,$\mu\in[0,1]$.但正态分布均值和方差都可以为任意值,应该设定一个以θ为中心、概率为 0.95 的置信区间,即控制$\mu\in[\theta-a,\theta+a]\subseteq[0,1]$,以保证信任值分布在区间[0,1].

把θ假设为真实的间接信任度是合理的,但它是无法获取的.现有文献和人类的经验都强调直接经验的重要性,推荐信任度偏离直接信任度过大,则认为其参考价值也是很小,因此,一种合理的方式是使用直接信任代替θ,随着交互次数的增加,θ值越来越精确.考虑到时间因素的影响,对直接信任度作如下修正:

$$\hat{t}_i = 0.5 + (t_i - 0.5)\mathrm{e}^{-\lambda(t-t_0)} \tag{7}$$

表示直接信任是随时间而不断衰减的.若两个实体从未发生过交互,则令 $\hat{t}_i = 0.5$.

间接信任μ的先验分布为

$$p_\mu(\mu) = (2\pi\tau^2)^{-1/2} \exp\left\{-\frac{1}{2\tau^2}(\mu-\theta)^2\right\} \tag{8}$$

根据公式(6)和公式(8),得到 $\vec{X}$ 和μ的联合分为

$$F(\vec{X},\mu) = \frac{(2\pi)^{-(n-1)/2}}{\tau\sigma^n} \exp\left\{-\frac{1}{2}\left[\frac{n\mu^2 - 2n\mu\bar{x} + \sum_{i=1}^{n}x_i^2}{\sigma^2} + \frac{(\mu-\theta)^2}{\tau^2}\right]\right\} \tag{9}$$

进而得到样本边际密度函数 $p_{\vec{X}}(\vec{X})$ 为

$$p_{\vec{X}}(\vec{X})=\frac{(2\pi)^{-(n-1)/2}}{\tau\sigma^{n}}\exp\left\{-\frac{1}{2}\left(\frac{\sum_{i=1}^{n}x_i^2}{\sigma^2}+\frac{\theta^2}{\tau^2}-\left(\frac{n\bar{x}}{\sigma^2}+\frac{\theta}{\tau^2}\right)^2\Big/\left(\frac{n}{\sigma^2}+\frac{1}{\tau^2}\right)\right)\right\}\left(2\pi\Big/\left(\frac{n}{\sigma^2}+\frac{1}{\tau^2}\right)\right)^{1/2} \tag{10}$$

根据 Bayesian 公式,可得到间接信任的后验分布:

$$p_{\mu|\vec{X}}(\mu\mid\vec{X})=\frac{F(\vec{X},\mu)}{p_{\vec{X}}(\vec{X})}=\left\{2\pi\Big/\left(\frac{n}{\sigma^2}+\frac{1}{\tau^2}\right)\right\}^{1/2}\exp\left\{-\frac{1}{2\Big/\left(\frac{n}{\sigma^2}+\frac{1}{\tau^2}\right)}\left(\mu-\left(\frac{n\bar{x}}{\sigma^2}+\frac{\theta}{\tau^2}\right)\Big/\left(\frac{n}{\sigma^2}+\frac{1}{\tau^2}\right)\right)^2\right\} \tag{11}$$

这说明在参考样本信息 $\vec{X}$ 以后,μ的后验分布变为

$$\mu\mid\vec{X}\sim N\left(\frac{n\bar{x}/\sigma^2+\theta/\tau^2}{n/\sigma^2+1/\tau^2},\frac{1}{n/\sigma^2+1/\tau^2}\right)$$

使用 Bayesian 估计,得到μ的后验均值的估计值为

$$\hat{\mu}=\frac{n/\sigma^2}{n/\sigma^2+1/\tau^2}\bar{x}+\frac{1/\tau^2}{n/\sigma^2+1/\tau^2}\theta \tag{12}$$

式(12)表明,当总体方差σ^2较小(即样本精度较大)或者样本量 n 较大时,样本所占的权重较大;当先验方差τ^2较小(即先验精度较大)时,先验均值的权重就比较大.这显然符合实际经验.推荐信任度估计的过程如图 2 所示.

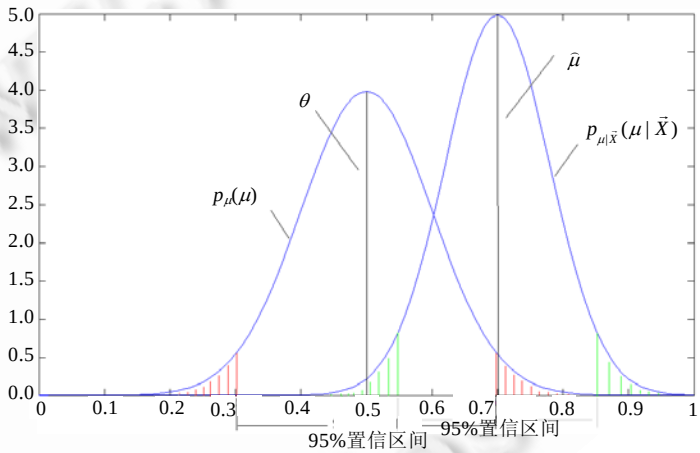


Fig.2 Recommendation trust model

图 2 推荐信任模型

在 Bayesian 估计中,本文假设采样过程的方差σ^2和μ的方差τ^2是已知的,这是一个主观的假设.实际中,过程的方差可能是未知的,那么必须评定一个有关均值和方差的联合先验分布,并且基于样本信息去修改它,这是一个复杂的工作.因为σ^2仅仅与样本信息相关而与先验信息无关,用样本方差作为σ^2的一个近似估计,在某些情况下,这个近似可以提供足够精确的解.

3 动态信任模型的稳定性分析

3.1 动态信任的稳定性

对信任关系动态性的研究,现有工作并不充分.实体之间的信任关系是动态的、变化的过程,但这并不代表动态性等同于随机性.两个实体之间信任度的演化,是认知不完全造成的.一个实体对另一个实体有足够的交互和充分的认知,那么前者会得到一个关于后者相对稳定的信任度.另一方面,实体之间的认知不同,也是导致信

任度演化的原因,此时,信任主体之间需要相互参考,得到一个比较统一的认识.根据上述分析,对一个实体来说,影响信任度的因素是交互次数和与之交互的实体的个数.随着两者数量的增加,信任度都将趋于一个稳定值.

如图 3 所示,只考虑实体 A 和 C 建立信任关系的过程.从客体 C 的角度来看,主体 A 和推荐者集合$\{B_i\}$是无差别的,它们都属于对 C 认知的实体集合.集合$\{A\}\cup\{B_i\}$中的实体通过与客体直接交互和相互之间的推荐与 C 建立信任关系,A 和 C 的关系只不过是我们所关注的和感兴趣的而已.图中的 A,B_i 和 C 都有直接交互的经验(实线),A 还通过 B_i 获得对的间接信任(虚线);同样,B_i 也会从 A 和$\{B_i\}-B_i$等实体中获得间接经验.因此,在对 C 的认知过程中,A 和$\{B_i\}$中的实体元素之间是完全平等的关系.

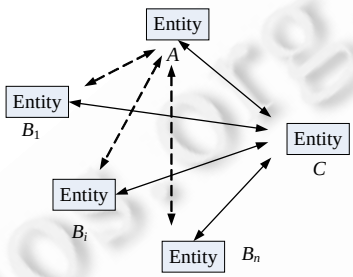


Fig.3 Interaction between entities

图 3 实体交互示意图

在$\{A\}\cup\{B_i\}\cup\{C\}$中,假设环境基本维持在相同的条件,实体 C 本身没有发生剧烈的改变.那么,任意两个实体之间都发生足够多的交互以后,应该认为 A 和每一个 B_i 对 C 的认知都是充分的,$\{A\}\cup\{B_i\}$中的实体对 C 的认知结果应该是基本相同的.另一方面,$\{A\}\cup\{B_i\}$中的一个实体与 C 发生足够的多交互以后,它对 C 的信任度也将会稳定,这个稳定值是由 C 的本身属性决定的,此时,其他实体与 C 交互的结果对该认知不再产生影响.事实上,C 的本质属性决定其在交互过程中的行为,其他实体通过对这些行为的捕捉逐步对其产生认识,随着交互次数的增加,认识是不断深入的.不失一般性,以 A 和 C 之间的关系为例,A 作为信任主体,C 作为信任客体,$\{B_i\}$作为推荐者,因此,如果用信任度来表示,则有

$$\lim_{k\to\infty} t_{A,C} = \lim_{\substack{k\to\infty \\ i=1,\ldots,n}} t_{B_i,C} = re\ .$$

上式表示在足够多的交互次数下,即认知是充分和统一的情况下,$\{A\}\cup\{B_i\}$对 C 的认知将趋于一致.那么,此时所有推荐信任度应该是相同的.

$$\lim_{\substack{k\to\infty \\ i=1,\ldots,n}} t_{A,C}^{B_i} = \lim_{\substack{k\to\infty \\ i=1,\ldots,n}} t_{B_i,C} = re\ .$$

因此,A 获得的的关于 C 的间接信任也应该与之相同.其中,k 表示交互次数,re 表示一个固定的值.

实际中,这种被外界充分和统一的认知,称为 C 的信誉;而 re 表示其大小,称为信誉值.

另一方面,当对 C 的认知并没有达到充分和统一的时候,不同的认知主体之间会存在相对的偏差.显然,在起始阶段,是混乱性和随机性最大的时候.此时,单个信任主体对信任客体的认知具有很大的随机性,但是大量信任主体的认知会表现出一定的规律性,而且在实体个数不断增多的情况下,这种规律会越来越明显,即实体间的认知会趋向稳定.

初始阶段,A 对 C 的认知不一定是正确的,需要参考其他实体的推荐信息.一方面,参考多个实体的交互结果可以有效减少随机性的影响;另一方面,直接交互较少的情况下,使用大量实体一次交互结果代替单个实体多次交互结果显然是一种合理的方式,也符合人类实际的行为活动.直观上,$\{A\}\cup\{B_i\}$中的实体与 C 交互的结果总会分布在正确的结果附近,偏离越大则可能性越小.单个实体的交互结果具有一定的随机性,但是大量实体的交互结果具有稳定性.因此,随着交互次数和交互实体个数的增加,单个实体的认知偏差会逐渐缩小.

对比人类社会,从长期来看,社会实体之间的信任关系会进入一个相对稳定的状态.也就是通过多次的交互行为和结合别人推荐结果,两个实体之间能够建立一个相对稳定的信任关系,这种信任关系达到稳定值,也就形成了信誉.

3.2 命题及其证明

开放环境下,动态性是信任的一个属性.通过对实体行为的判断和量化可以认为,在某一时刻或者某段时间内,信任关系的值是一个相对静态和稳定的量.

定义 4(可信度). 可信度(trustworthiness)表示一个实体值得信任的程度.

一个实体的可信度是由其本质属性或者内因决定的,在环境和实体都未发生重大变动的情况下,可信度应该是相对稳定的.在推荐信任中,如果没有或者剔除了恶意推荐,那么推荐信任值应该集中在可信度的附近.显然,推荐者对实体的了解程度越高,其推荐信任度就越接近可信度.因此,随着信任主体对客体的认知不断加深,信任度是收敛的,并且其收敛结果是信任客体的可信度.

可信度是对信任客体内在的一个度量,而信任客体本质属性是无法检验和量化的,只能通过其外在表现间接地获得,而这种外在表现的度量,就是信誉值.本文认为,在极限的条件下,可信度和信誉值是相等的.

信任关系中,可信度是一个未知的值.信任模型的任务之一就是确定这个未知的量,从而可以进行预测和决策.从上述分析中可以发现,在多次交互以后,间接信任度和直接信任度会趋于一致.本文模型中,使用每次交互产生的直接信任代替间接信任的期望值来简化问题,随着交互次数的增加,这个近似代替将越来越精确,因此对结论不会产生影响.

不失一般性,假设初始的信任度是低于可信度(re)的.如图 4 所示,虚线表示交互结果分布在 re 的附近,但这是一个实际存在却无法知道的假想分布.同理,推荐信任也应该分布在 re 附近.θ表示信任度的期望,由于使用直接信任度进行近似代替,模型认为,分布在θ附近的推荐信息才是可以接受的,从而推荐样本是从两者的 95%置信区间的交集中取得的,如图中阴影部分所示.

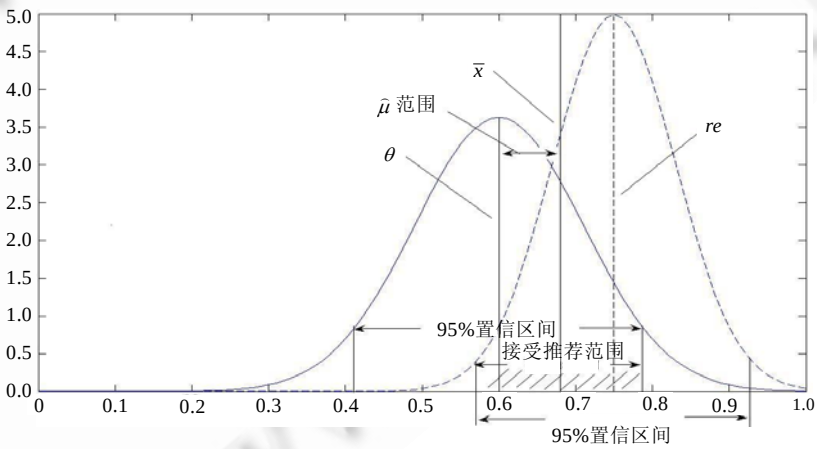


Fig.4 Change of trust degree

图 4 信任度的演化过程

通过 Bayesian 估计得到间接信任度的估计值 $\hat{\mu}$,应该介于θ和样本均值 $\bar{x}$ 之间,即 $\hat{\mu}$ 是不断趋向于 re 的.随着交互次数的增加,直接和间接信任度都是无限趋近于可信度的.采用文献[17]中的权重取值方法,严格的数学证明如下所述.

命题 1(收敛性). 信任度是收敛的.

证明:设第 k 次交互预测的结果为

$$T^{(k)}=\frac{1}{1+\beta(m)^{(k)}}T_D^{(k)}+\frac{\beta(m)^{(k)}}{1+\beta(m)^{(k)}}T_I^{(k)},$$

其中,T_D 是直接信任,T_I 为间接信任,$\beta(m)$[17]为权重计算公式.由前文分析,令

$$T_D^{(k)}=T^{(k-1)}.$$

在排除恶意和错误推荐的情况下,这是可以接受的.显然,

$$T_I^{(k)}=\hat{\mu}^{(k)}.$$

因此,

$$T^{(k)}=\frac{1}{1+\beta(m)^{(k)}}T^{(k-1)}+\frac{\beta(m)^{(k)}}{1+\beta(m)^{(k)}}\hat{\mu}^{(k)}.$$

经过 Bayesian 估计,精度会产生相应的变化,因此,

$$\hat{\mu}^{(k)}=\frac{n/\sigma^2}{n/\sigma^2+1/\tau_{(k-1)}^2}\bar{x}^{(k)}+\frac{1/\tau_{(k-1)}^2}{n/\sigma^2+1/\tau_{(k-1)}^2}T^{(k-1)}.$$

代入上式得

$$T^{(k)}=\frac{1}{1+\beta(m)^{(k)}}T^{(k-1)}+\frac{\beta(m)^{(k)}}{1+\beta(m)^{(k)}}\left(\frac{n/\sigma^2}{n/\sigma^2+1/\tau_{(k-1)}^2}\bar{x}^{(k)}+\frac{1/\tau_{(k-1)}^2}{n/\sigma^2+1/\tau_{(k-1)}^2}T^{(k-1)}\right),$$

其中,

$$\frac{1}{\tau_{(k)}^2}=\frac{n}{\sigma^2}+\frac{1}{\tau_{(k-1)}^2}.$$

$T^{(k)}$在[0,1]内可以任意取值,显然是有界的.因此,

$$T^{(k)}-T^{(k-1)}=\frac{\beta(m)^{(k)}}{1+\beta(m)^{(k)}}\frac{n/\sigma^2}{n/\sigma^2+1/\tau_{(k-1)}^2}(\bar{x}^{(k)}-T^{(k-1)}).$$

$\bar{x}^{(k)}$ 是样本分布均值的无偏估计,在大样本条件下,有

$$\lim_{n\to\infty}P\{|\bar{x}^{(k)}-\mu|<\varepsilon\}=1.$$

即 $\bar{x}^{(k)}$ 是依概率收敛于μ的,$\bar{x}^{(k)}\xrightarrow{P}\mu$.其中,$n$ 表示样本容量,n 较大的情况下,$\bar{x}^{(k)}$ 是基本稳定的.

当初始条件 $T^{(0)}>\bar{x}^{(1)}$,先验信息的信任度高于样本均值时,由 $T^{(k)}$的表达式易知 $\bar{x}^{(k)}<T^{(k)}<T^{(k-1)}$,即

$$T^{(k)}-T^{(k-1)}<0.$$

同理,当 $T^{(0)}<\bar{x}^{(1)}$ 时,

$$T^{(k)}-T^{(k-1)}>0,$$

并且,由于 $\frac{\beta(m)^{(k)}}{1+\beta(m)^{(k)}}\frac{n/\sigma^2}{n/\sigma^2+1/\tau_{(k-1)}^2}$,$\bar{x}^{(k)}$ 和 $T^{(k-1)}$都在[0,1]范围内,从而有

$$0<T^{(k)}-T^{(k-1)}<1.$$

在两种情况下,迭代序列$\{T^{(k)}\}$都是单调有界的,因而是收敛的. □

命题 2. $\{T^{(k)}\}$收敛于可信度.

证明:由命题 1 的证明可知$\{T^{(k)}\}$是收敛的,因此极限必然存在.

记

$$\lim_{k\to\infty}T^{(k)}=L.$$

因为

$$T^{(k)}=\frac{1}{1+\beta(m)^{(k)}}T^{(k-1)}+\frac{\beta(m)^{(k)}}{1+\beta(m)^{(k)}}\left(\frac{n/\sigma^2}{n/\sigma^2+1/\tau_{(k-1)}^2}\bar{x}^{(k)}+\frac{1/\tau_{(k-1)}^2}{n/\sigma^2+1/\tau_{(k-1)}^2}T^{(k-1)}\right).$$

对上式两端取极限,得

$$L\lim_{k\to\infty}\frac{1}{1+\beta(m)^{(k)}}\frac{n/\sigma^2}{n/\sigma^2+1/\tau_{(k-1)}^2}=\lim_{k\to\infty}\frac{1}{1+\beta(m)^{(k)}}\frac{n/\sigma^2}{n/\sigma^2+1/\tau_{(k-1)}^2}\bar{x}^{(k)}.$$

由$\beta(m)^{(k)}$的定义可知, $\lim_{k\to\infty}\frac{1}{1+\beta(m)^{(k)}}=1$.随着样本的不断增加,样本精度逐渐增大, $\lim_{k\to\infty}\frac{n/\sigma^2}{n/\sigma^2+1/\tau_{(k-1)}^2}=1$.

因此,

$$L=\lim_{\substack{k\to\infty\\ n\to\infty}}\bar{x}^{(k)}.$$

由于 $\bar{x}^{(k)}$ 是依概率收敛于μ的, $\bar{x}^{(k)}\xrightarrow{P}\mu$,因此 $L=\lim_{k\to\infty}T^{(k)}=\mu$,即收敛于可信度. □

命题 3. $\{T^{(k)}\}$是线性收敛的.

证明:记 $e^{(k)}=T^{(k)}-\mu$,

$$\lim_{k\to\infty}\frac{|e^{(k)}|}{|e^{(k-1)}|^p}=\lim_{k\to\infty}\frac{|T^{(k)}-\mu|}{|T^{(k-1)}-\mu|^p}=q.$$

令 p=1,则有

$$\lim_{k\to\infty}\frac{|e^{(k)}|}{|e^{(k-1)}|^p}=\frac{\left|\frac{1}{1+\beta(m)^{(k)}}(T^{(k)}-\mu)+\frac{\beta(m)^{(k)}}{1+\beta(m)^{(k)}}\frac{1/\tau_{(k-1)}^2}{n/\sigma^2+1/\tau_{(k-1)}^2}(T^{(k-1)}-2\mu+\bar{x}^{(k)})\right|}{|T^{(k-1)}-\mu|}.$$

考虑分子中的高阶无穷小

$$\lim_{k\to\infty}\frac{\beta(m)^{(k)}}{1+\beta(m)^{(k)}}\frac{1/\tau_{(k-1)}^2}{n/\sigma^2+1/\tau_{(k-1)}^2}\left|\frac{T^{(k-1)}-2\mu+\bar{x}^{(k)}}{T^{(k-1)}-\mu}\right|.$$

显然有,

$$\lim_{k\to\infty}\frac{\beta(m)^{(k)}}{1+\beta(m)^{(k)}}=\lim_{k\to\infty}\frac{1/\tau_{(k-1)}^2}{n/\sigma^2+1/\tau_{(k-1)}^2}=0,$$

$$\lim_{k\to\infty}\left|\frac{T^{(k-1)}-2\mu+\bar{x}^{(k)}}{T^{(k-1)}-\mu}\right|=\lim_{k\to\infty}\left|2-\frac{T^{(k-1)}-\bar{x}^{(k)}}{T^{(k-1)}-\mu}\right|=1.$$

因此,高阶无穷小的极限为 0,从而得到

$$q=\lim_{k\to\infty}\frac{|e^{(k)}|}{|e^{(k-1)}|^p}=1.$$

即$\{T^{(k)}\}$是线性收敛的. □

对本文提出的收敛性,可以给出一个直观的说明.不失一般性,假设可信度大于初始直接信任,$\mu>t_0$.那么,非恶意的推荐总是分布在μ附近,因此,这些推荐度也应该大于初始信任度.所以,经过一次 Bayesian 估计,得到的间接信任度 $\hat{\mu}^{(1)}$ 应该是介于 t_0 和样本均值 $\bar{x}^{(1)}$ 之间,所以,融合直接信任度后的信任值 $t_{A,C}^{(1)}$ 是必然大于 t_0.即,一次估计以后信任值朝着可信度方向变化.同理, $\hat{\mu}^{(2)}$ 必然介于 $t_{A,C}^{(1)}$ 与 $\bar{x}^{(2)}$ 之间,因此在多次交互过程中,信任度是不断接近于可信度的.

4 模拟实验和结果分析

NetLogo 是美国西北大学 Center for Connected Learning(CCL)开发的一款可编程建模环境,它提供一个开放的模型平台,自身带有模型库,可以根据多种条件进行设置.在 NetLogo 平台上实现了本文提出的推荐信任模型,并对一个小规模环境中的信任关系进行模拟实验.

为了对模型的有效性进行衡量和评估,对于模拟实验,给出如下基本预期目标:

1) 模型应该能够给出相对正确的结果,计算出一个实体准确或者相对准确的信誉值.即能够给出可以帮助信任实体做出决策的有效间接信任度;

2) 模型应该能够处理恶意节点的恶意推荐和非恶意节点的非正确的推荐,减少这些推荐对推荐结果的影响.

4.1 实验设置

NetLogo 是一个开放的模拟平台,使用基于 Multi-Agent 复杂开放系统仿真建模的思想进行研究,平台中可以设置多个“独立”的 Agent,并可以分别对其下达指令.根据模型的计算方法,利用系统中 Agent 之间随时间不断的演化,从而获取模拟数据.

文献[19]提供了一种实验环境、参数设置的方法.该环境中的每个 Agent 实体既可以作为服务提供者(service provider,简称 SP),也可以作为服务接收者(service receiver,简称 SR),而相关联的 Agent 实体之间都是邻居(neighbors)关系.在间接信任关系的研究中,可以认为系统中只存在一个 SP,它为所有的 SR 提供服务,即 SP 作为信任客体;而其他 Agent 实体全部作为 SR,它们从 SP 接收服务.从特定时间点开始,存在一个特殊的 SR,记作 sr,它与 SP 之间不再存在直接的交互关系,而是通过其他的 SR 为其提供的推荐信息对 SP 的服务做出判断,此时,sr 作为 SP 的信任主体;则其余的 SR 实体作为 sr 的推荐者实体并提供推荐信任度.本文主要研究从 0 时刻开始 sr 与 SP 之间的间接信任关系.

系统中每一个 Agent 实体都是相互独立的,一段时间内,每一个 SR 都与 SP 进行直接交互,根据交互结果和其自身的判断,SR 能够得到对 SP 的认知,即 SR 对 SP 的信任度,SP 把这个信任值提供给 sr 作为推荐信任值.随着时间的增加,大量的推荐信任值就组成了间接信任演化的样本数据.在实际环境中,不能保证每一个 SR 提供的数据都是诚实的和正确的,这与每一个 SR 本身的属性有关.SR 实体是否为恶意实体、是否已经对 SP 做出正确的判断、sr 是否信任 SR、sr 是否接受 SP 的推荐等因素,都会对该实体的推荐结果造成影响.表 1 给出了系统中部分参数和符号及其说明.

Table 1 Simulation experimental parameters and notations

表 1 模拟实验参数及符号说明

Parameters and notations	Possible values	Description
SP	1	Service provider[19]; trustee entity
sr	1	Special service receiver; trust entity
SR	1~50	Service receiver[19]; recommend entities
ε	0~1	Precision of the direct trust
n	1~+∞	Times of interaction between SP and sr corresponds to ε
Steps	1~+∞	Times of recommendation iteration

4.2 模型的有效性

为了研究推荐信任度,从特定时间开始,SP 和 sr 之间不再存在直接交互,令在此之前两者直接交互形成的直接信任度作为第一次 Bayesian 估计先验信息.直接交互显然是一个 Bernoulli 过程,设前 n 次交互中成功的次数为 m,那么如果要求第 n+1 次的交互结果使直接信任度产生的变化不超过ε,那么交互次数 n 必须满足:

$$\left|\frac{m}{n}-\frac{m+1}{n+1}\right|<\varepsilon 或 \left|\frac{m}{n}-\frac{m}{n+1}\right|<\varepsilon.$$

n 表示总的交互次数,m 表示成功的次数,显然有 $0\leqslant m\leqslant n$.

当 $\frac{n-m}{n(n+1)}<\varepsilon$ 或 $\frac{m}{n(n+1)}<\varepsilon$,并且由 $\frac{n-m}{n},\frac{m}{n}\in[0,1]$,则有

$$n>\frac{k}{\varepsilon}-1 \tag{13}$$

其中,$k=\frac{n-m}{n}$ 或 $k=\frac{m}{n}$.不失一般性,假设 SP 和 sr 在 0 时刻之前存在 50,100,200 和 500 次直接交互,令 k=1,相应的ε为 0.02,0.01,0.005 和 0.002.以此作为先验信息,验证模型的有效性.

设置 SP 的可信度(信誉)为 0.8,从 0 时刻开始,sr 和 SP 之间不存在直接交互,图 5(a)~图 5(d)表示在 0 时刻之

前,sr 和 SP 分别交互了 50,100,200 和 500 次,得到的直接信任度都是 0.5.系统有 50 个推荐实体 SR,分别做出独立的推荐.推荐实体是否能够给出正确和诚实的推荐度是未知的,所有的推荐值都经过了剪枝和过滤.在 SP 和系统环境不会发生突变的情况下,对上述 4 种情形分别作 1 000 次 Bayesian 估计,结果如图 5 所示.

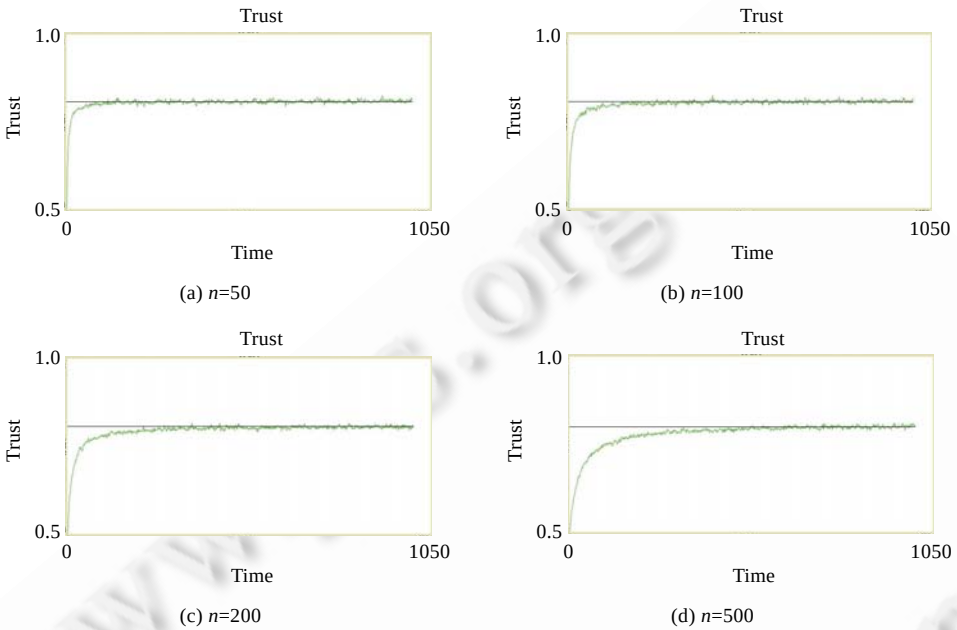


Fig.5 Experiment results of recommendation model

图 5 推荐信任模型的结果

从图 5 中可以看出,初始条件下,信任主体对信任客体的认知是通过以往直接交互获得的;在 0 时刻后,实体 sr 和 SP 之间不存在直接交互,sr 对 SP 认知的演化只能通过间接信任获得.经过推荐者的推荐,信任主体参考推荐样本信息,对间接信任做出新的评估,得到间接信任的后验分布均值的估计.由于推荐样本是分布在信任客体的可信度附近的,第 1 次估计以后,推荐信任度偏离初始值,趋向于可信度.在相对稳定的环境下,重复上述过程,多次参考推荐样本信息,间接信任度的变化趋势是基本固定的,即趋向于可信度(信誉),并最终稳定在一个固定值附近.从结果来看,这个固定值就是信任客体的可信度(信誉).因此,实验结果表明,本文所提出的推荐信任模型是能够给出足够正确的间接信任结果的.

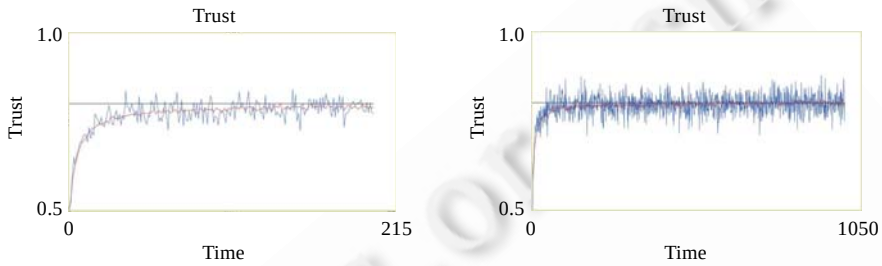
另一方面,由实验容易看出,在 0 时刻之前,sr 与 SP 交互的次数越多,间接信任收敛的越慢.由公式(13)可以知道,直接交互的次数 n 越大,先验信息的精度越高,则推荐信任度在公式(12)中所占的权重越小,因此间接信任度收敛的速度较慢.实际上,人们在直接信息充分并且对其有足够信心的时候,直接信任在信任中占据相当的比重;当直接交互很少甚至不存在直接交互的时候,间接经验则起到很重要的作用.上述实验结果显然与人类正常思维方式相符合的.

4.3 模型抵御恶意推荐的能力

推荐信任是信任关系中最复杂的一环,这是因为推荐信任关系涉及到三方(信任主体、信任客体、推荐者)和大量的节点(直接信任只有两个节点).一方面,推荐信任不是能够直接获得的;另一方面,大量的推荐者之中必然存在恶意和非正确的推荐.显然,处理恶意和非正确推荐的能力是一个模型能否给出正确结果的重要因素.图 6 给出过滤恶意推荐和没有过滤恶意推荐的实验结果:图 6(a)给出一个清晰的结果,表示经过 200 次推荐迭代后的结果;而图 6(b)表示经过 1 000 次推荐后的结果.

从实验结果可以看出,在没有过滤恶意推荐的情况下,虽然推荐信任度最终也会稳定在可信度附近,

即有 $t_{A,C}^{B_i} \in [re-\varepsilon_1, re+\varepsilon_2]$,但是波动比较大;尤其在恶意推荐与实际可信度偏差比较大的情况下,推荐结果会出现突变.由图 6 还可以看出,恶意推荐不仅仅导致一次判断失误,而且还会影响到其后的间接信任值的判断.当恶意推荐出现以后,需要多次推荐才能重新得到正确的推荐.相比较来说,经过过滤恶意推荐的结果,在达到稳定值以后基本不会出现很大的波动,距离可信度的偏差程度显然远远小于没有过滤的情况.因此,本文所提出的分级剪枝过滤机制是有效的,并且从实验结果来看,本文模型对于感知恶意推荐也是相当灵敏的.



(a) Step=200 (b) Step=1000

Fig.6 Experiment results of filtrating malicious recommendations or not

图 6 过滤与未过滤恶意推荐的对比

模拟实验对过滤和未过滤两种情况分别进行 50,100,200,500,1 000,2 000 和 5 000 次推荐迭代作比较,见表 2,可以看出,经过分级剪枝过滤后得到的推荐信任值与可信度(信誉)的偏差远远小于未经过过滤的结果,后者的平均波动幅度是前者的 2~5 倍.此外,随着推荐次数的不断增加,间接信任值与可信度(信誉)之间的偏差是逐渐减少的,这与模型结论是完全一致的.

Table1 2 Effects on indirect trust of using filtration or not

表 2 过滤机制对推荐信任的影响对比

Steps	过滤		未过滤	
	平均偏差	偏差百分比(%)	平均偏差	偏差百分比(%)
50	0.014 017	1.752 10	0.027 683	3.460 39
100	0.008 891	1.111 39	0.028 400	3.549 94
200	0.006 503	0.812 834	0.023 202	2.900 27
500	0.004 959	0.619 824	0.024 001	3.000 15
1 000	0.004 434	0.554 311	0.023 165	2.895 58
2 000	0.004 139	0.517 411	0.022 955	2.869 34
5 000	0.003 983	0.497 918	0.022 438	2.804 75

4.4 与基于Beta分布的模型比较

使用概率统计方法研究信任模型中,文献[4]根据 Bayesian 理论推导了基于行为结果的信任度是服从 Beta 分布的;文献[8]使用统计学方法建立了一个基于 Beta 分布的声誉系统;文献[18]提出一种基于 Beta 分布的决策模型.在已有文献理论成果的基础之上,本文在 NetLogo 平台上实现了一种基于 Bate 分布推荐信任模型,并且在不同的环境下,分别与本文模型进行比较.模拟实验结果表明,本文模型克服了 Beta 分布模型的一些不足之处.

与本文模型不同,Beta 分布模型中,推荐信息不是信任值,而是系统环境中每一个 SR 和 SP 之间的交互结果.从 0 时刻开始,每一个 SR 分别与 SP 交互,在同一时刻,每个 SR 都会提供一次交互结果;而从一段时间来看,每个 SR 提供了一个交互结果序列.SP 通过向 sr 提供已有的交互结果信息,使其能够判断整个系统中总的成功次数,这显然是服从共轭 Beta 分布的.因此,Beta 分布模型是通过已获得的交互结果为先验信息,以当前时刻获得的推荐为样本信息,根据共轭分布得到后验 Beta 分布,获得间接信任值.

4.4.1 安全环境

系统处于安全环境,是指 SP 在一定的时间内不会发生突变,根据本身属性(可信度/信誉)提供相应的服务;

环境中不存在恶意的 SR 实体;每一个 SR 尽最大努力为 sr 提供诚实的推荐信息.

在安全环境下,系统中有 50 个 SR 实体.不失一般性,初始时刻设置 n=200,推荐迭代次数为 1 000.在上述系统中,分别使用 Beta 分布模型和本文模型对推荐信任度的演化过程进行模拟.几种典型的实验结果如图 7 所示.

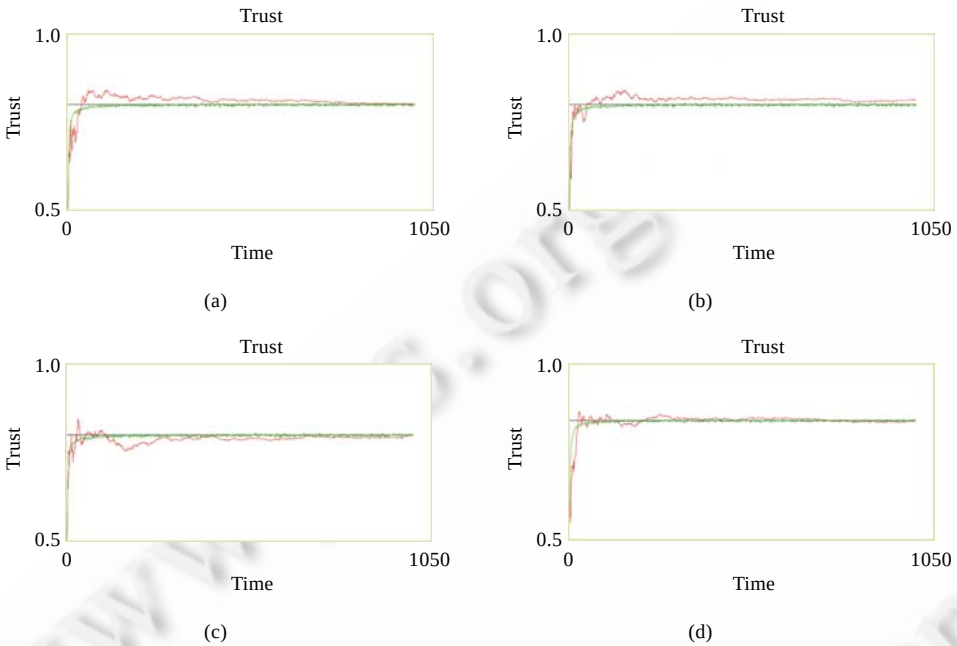


Fig.7 Compare with Beta distribution model (n=200)

图 7 与 Beta 模型的比较结果(n=200)

从图中可以看出:

1) Beta 分布模型最终也是收敛的,并且收敛到信誉值.但是其收敛速度较慢,并且在有些情况下甚至不能在较短时间内达到收敛,如图 7(b)所示.但是本文模型能够在有限时间内迅速收敛至正确的信任值,并且一旦达到收敛值之后不会发生重大的突变,而是以可信度为中心上下小范围内波动.造成 Beta 模型收敛较慢原因是,基于 Bernoulli 过程,Beta 模型每次接受的推荐信息是交互结果,这样导致不同的 SR 的推荐信息是毫无差别的,无法进行区分;另一方面,它无法消除系统推荐中随机性的高推荐或低推荐对间接信任的影响,因此只有足够数量的信息才能够使其逼近正确的结果.

2) 由实验结果可以看出,在 Beta 分布模型达到收敛之前,其稳定性很差,尤其是在推荐迭代开始阶段,如图 7(c)、图 7(d)所示.而本文模型的间接信任在初始阶段受到直接信任的影响较大,而推荐信任只能起到逐渐修正的作用,因此得到的结果是近似平滑稳定的.由共轭 Beta 分布容易知道,造成 Beta 模型不稳定的原因是初始阶段先验信息数量较少,因此,新的样本很容易对先验信息造成剧烈的影响.直到推荐累积到一定的数量,才会大致形成相对正确的认知并占据主导地位,此时受到样本信息的影响较小,即如图 7 中模拟实验结果所示.

3) Beta 模型无法排除初始阶段样本顺序的影响.即使系统中不存在恶意节点,但是并不能保证每个 SR 的推荐值都是正确的,这种随机性的存在也对 Beta 模型造成了影响.如果在初始阶段存在较多的偏高推荐,则 Beta 模型的间接信任值会在很长的时间内高于信誉值,即间接信任是递减收敛至信誉值,如图 7(a)、图 7(b);反之若存在偏低推荐,则存在相反的情况,如图 7(c)所示.而在本文模型中则不存在这些情况.造成上述结果的原因是,在初始条件下,少量的样本就决定了间接信任的起始值;而随着演化的进行,样本数量越大,间接信任越难被改变.也就是相同的样本在推荐迭代初期与后期起到的作

用相差很大,因此,Beta 模型由于其本身的原因无法克服这个问题.

为了进一步对比两种模型,将模拟实验重复多次,选取 Beta 模型迅速并且稳定收敛的 10 次实验,并对数据进行分析.由此可以得到两种演化模型的间接信任平均偏差值和平均偏差百分比,模拟实验比较结果如图 8 所示.显然,本文模型比 Beta 模型更加精确,平均偏差较低;并且在稳定的环境中,多次实验结果也基本不变.

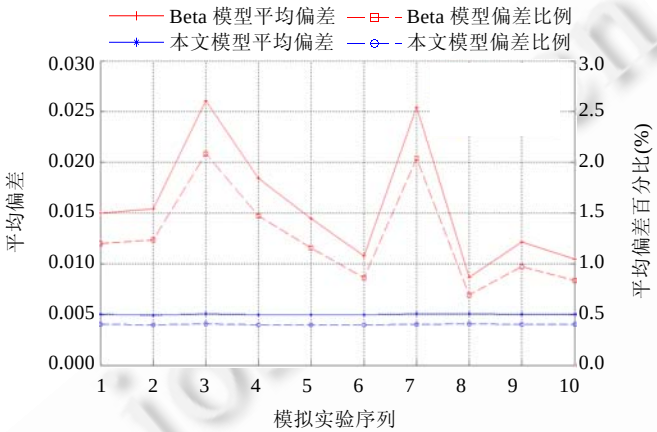


Fig.8 Experimental results of models' accuracy

图 8 模型准确性比较

4.4.2 非安全环境

非安全的环境,指 SP 自身保持不变.系统中会存在一定数量的恶意节点,它们通过提供与 SP 不相符的推荐达到攻击的目的.不失一般性,设定 SP 的可信度为 0.8,即认为 SP 在大多数情况下是提供可信的服务的,而恶意节点会提供相反的信息.系统环境保持稳定,设置环境中存在 20%的恶意节点,这些节点可以随意地加入和脱离系统环境,并且通过向 sr 推荐错误的信息进行攻击,这是符合开放环境的实际情况的.在开始的条件下,系统环境是安全的,从不同的时刻起,恶意节点开始攻击,实验结果如图 9 所示.在这种情况下,由于 Beta 分布模型只根据交互结果判断,而不能像本文模型对推荐信息进行比对、分析和过滤,所以基本不可能得到正确的结论,即 Beta 模型的间接信任度无法收敛至 SP 真实的可信度.

图 9(a)~图 9(d)分别表示在非安全的环境中,恶意实体在推荐迭代已经进行 400,500,600 和 700 次的时候进行攻击.事实上,SP 本身提供可信服务的能力没有改变,即信誉值不变;但是由于恶意节点的存在,使得系统中每一个与恶意节点相关联的实体对 SP 的认知产生混乱.Beta 分布模型只根据交互结果获取信任度,恶意的推荐也被采用,从受到攻击开始,间接信任的演化就逐渐偏离了 SP 真实的信誉值(SP 初始信誉值设置为 0.8,因此,一般认为 SP 多数情况下都能够提供可信的服务的,那么恶意节点的攻击应该提供“SP 是不可信的”信息,从而受到攻击后间接信任值是递减的).而本文的模型通过对比分析不同节点提供的推荐信息,对恶意节点有着较强的抵御能力,因此在受到攻击的情况下,依然能够得到正确的结果.但是从实验结果能够明显看出,间接信任值的波动幅度增加了,即在恶意节点的攻击下,精确度有所下降.以上对比实验表明,本文模型较之已有的基于 Beta 分布理论的模型有了较大的改进.在模型准确性、间接信任演化速度以及抵御恶意攻击的能力上都有了改善.

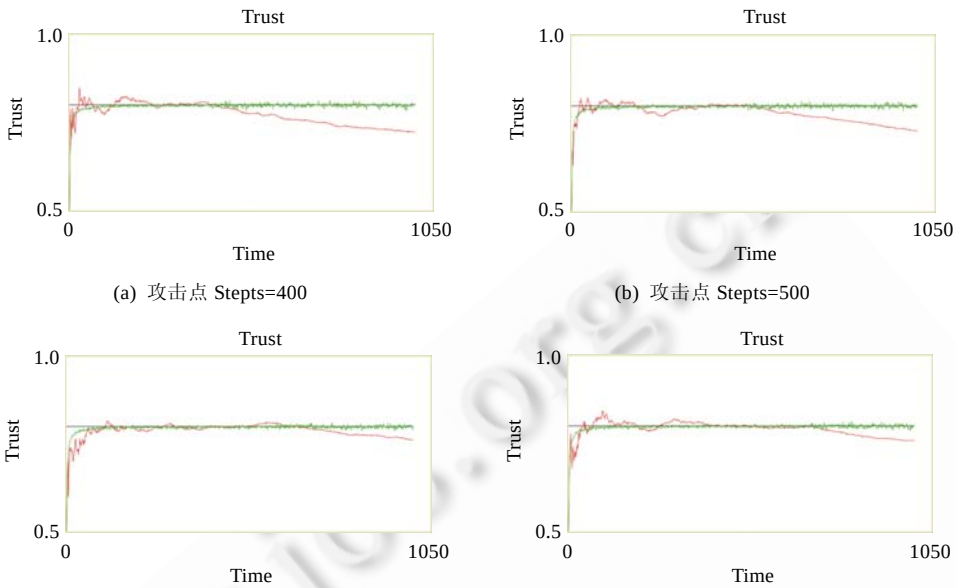


Fig.9 Evolution of indirect trust in the unsafe environment

图 9 间接信任在非安全环境中的演化

4.5 影响模型结果的因素

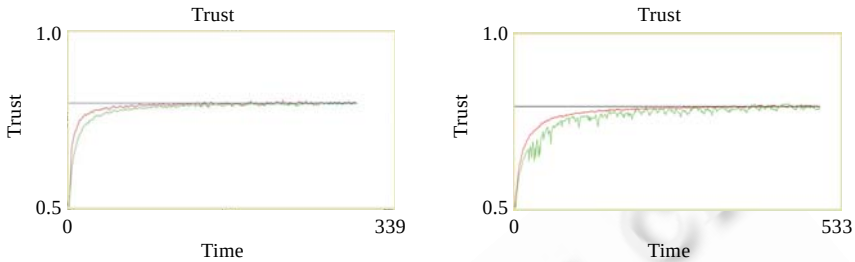
本文的工作主要针对网构软件安全性问题,即在开放、动态和难控的环境下,对自主的智能软件实体之间的信任度演化进行描述,模型也是适用于开放的普适环境.因此,外部条件的开放性是影响模型结果的因素之一.模型是以已知间接信任度为先验分布,参考推荐信息样本,得到间接信任度的后验均值的估计值.这个过程中,推荐信息样本是主要的变化因素.从统计学的角度来看,样本的数量是一个重要的因素;由于经过剪枝过滤,样本均值是大致确定的,因此,样本的精度是另一个重要的因素.如下实验给出了两个因素对推荐信任度的影响结果.

由公式(12)可以看出,后验均值是样本信息与先验均值的加权平均,两者的权重是由样本数量和精度决定的.在先验精度和样本精度固定的条件下,样本信息的权重是随着样本规模增加而增大的.在推荐信任模型中,信任主体和客体之间没有交互,推荐起着主要的作用,因此,样本量增大,间接信任度的收敛速度是应该加快的.同样,样本精度的增大,间接信任度的收敛速度也是增加的.

图 10(a)是不同规模的推荐节点的模拟实验结果.推荐者数量(样本规模)分别为 50 和 30,推荐次数为 300 次,计算中过滤了恶意和非正确推荐.模拟实验表明,50 个推荐节点的间接信任度的收敛速度是大于 30 个推荐节点的.图 10(b)是两种不同精度的推荐信息样本.分别设置样本精度为 10 和 2,推荐次数为 500 次,计算中过滤恶意和非正确推荐.模拟实验结果表明,样本精度较大的时候,间接信任度收敛速度比较快,并且稳定性比较好.

上述实验表明,在先验信息不足的条件下,通过增加样本数量和样本精度,可以在 Bayesian 估计中提高样本所占的权重,增加模型结果的准确性.在计算过程中,先验信息是不断完善并且接近可信度的,因此,后验均值最终会稳定在一个固定值附近.该结果与第 3.1 节中的分析一致.

通过模拟实验,首先证明了本文模型是有效的;接着比较了分级过滤机制的作用,实验数据表明,本文模型在抵御恶意推荐上的效果是显著的;通过已有的理论基础,实现了一个 Beta 分布模型,比较实验说明,本文模型在一些方面有了改善;最后,通过实验分析了影响模型结果的因素.



(a) 样本数量 (b) 样本精度

Fig.10 Factors that have effects upon the speed of convergence

图 10 影响收敛速度的因素

5 结论和进一步的工作

建立动态信任模型是用数学的方法对信任关系进行量化描述,Bayesian 估计是一个接近人类思维方式的过程.针对 Beta 分布的不足,本文在 Bayesian 估计中使用连续的正态过程,给出了一种新的间接信任模型.推荐是信任传递的一种方式,间接信任是推荐行为的结果,而推荐信任并不能完全脱离直接信任.以直接信任为基础,获得间接信任的先验分布,以分级剪枝过滤推荐信息作为样本,根据 Bayesian 估计得到间接信任的后验分布期望,从而得到间接信任的估计值.实验结果表明,模型能够获得更好的结果,并对恶意推荐有较强的抵御能力.

开放环境下,获取节点的精确的信任值是几乎不可能做到的,判断一个模型的正确性和有效性也是一个很困难的事情.但是,在外部条件不发生重大变化的情况下,可以认为信任值是相对稳定的,即信誉度.那么,在足够次数的交互以后,信任度应该与信誉值相同.本文给出了信任收敛性的证明,明确了信任动态性和可信度(信誉)之间的关系.

获取随机变量的分布是一项漫长而艰苦的工作,通过实际数据判断间接信任的精确分布是一件困难的事情.因此,模型采用了数学性质良好的正态分布,并且假设其精度(方差)是已知的.在今后的工作中,对未知精度分布的研究、使用统计学的方法获得精确的分布以及建立更加快速收敛的模型,都是完善工作的方向.另外,本文模型只考虑直接推荐,而在庞大的开放环境中,多级推荐将更加普遍,因此,如何使得正确的推荐传播得更快,而错误的推荐传播得更慢,是信任模型研究中很有意义的问题.

References:

[1] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management. In: Dale J, Dinolt G, eds. Proc. of the 17th Symp. on Security and Privacy. Oakland: IEEE Computer Society Press, 1996. 164−173. [doi: 10.1109/SECPRI.1996.502679]

[2] Blaze M, Feigenbaum J, Keromytis AD. Keynote: Trust management for public-key infrastructures. In: Christianson B, Crispo B, William S, *et al*., eds. Proc. of the Cambridge 1998 Security Protocols Int'l Workshop. Berlin: Springer-Verglag, 1999. 59−63. [doi: 10.1007/3-540-49135-X_9]

[3] Almenárez F, Andrés A, Campo C, García RC. PTM: A pervasive trust management model for dynamic open environments. In: Proc. of the 1st Workshop on Pervasive Security, Privacy and Trust. 2004. [doi: 10.1.1.99.7607]

[4] Almenárez F, Marín A, Díaz D, Sanchéz J. Developing a model for trust management in pervasive devices. In: Werner B, ed. Proc. of the 3rd IEEE Int'l Workshop on Pervasive Computing and Communication Security (PerSec 2006). Washington: IEEE Computer Society Press, 2006. 267−272. [doi: 10.1109/PERCOMW.2006.41]

[5] Almenárez F, Marín A, Campo C, García RC. TrustAC: Trust-Based access control for pervasive devices. LNCS 450, Berlin: Springer-Verlag, 2005. 225−238. [doi: 10.1007/11414360_22]

[6] Beth T, Borcherding M, Klein B. Valuation of trust in open networks. In: Gollmann D, ed. Proc. of the European Symp. on Research in Security (ESORICS). Brighton: Springer-Verlag, 1994. 3−18. [doi: 10.1007/3-540-58618-0_53]

[7] Jameel H, Hung LX, Kalim U, Sjjad A, Lee SY, Lee YK. A trust model for ubiquitous systems based on vectors of trust values. In: Proc. of the 7th IEEE Int'l Symp. on Multimedia. Washington: IEEE Computer Society Press, 2005. 674−679. [doi: 10.1109/ISM.2005.22]

[8] Jøsang A, Ismail R. The beta reputation system. In: Proc. of the 15th Bled Electronic Commerce Conf. 2002. [doi: 10.1.1.60. 5461]

[9] Melaye D, Demazeau Y. Bayesian dynamic trust model. LNCS 3690, Berlin: Springer-Verlag, 2005. 480−489. [doi: 10.1007/11559221_48]

[10] Theodorakopoulos G, Baras JS. On trust models and trust evaluation metrics for ad-hoc networks. IEEE Journal on Selected Areas in Communications, 2006,24(2):318−328. [doi: 10.1109/JSAC.2005.861390]

[11] Theodorakopoulos G. Distributed trust evaluation in ad-hoc networks [MS. Thesis]. Maryland: University of Maryland, 2004.

[12] Sun Y, Yu W, Han Z, Liu KJR. Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE Journal on Selected Areas in Communications, 2006,249(2):305−319. [doi: 10.1109/JSAC.2005.861389]

[13] Sun Y, Yu W, Han Z, Liu KJR. Trust modeling and evaluation in ad hoc networks. In: Proc. of the Global Telecommunications Conf. (Globecom 2005). Washington: IEEE Computer Society Press, 2005. 1−10. [doi: 10.1109/GLOCOM.2005.1577971]

[14] He R, Niu JW, Zhang GW. CBTM: A trust model with uncertainty quantification and reasoning for pervasive computing. LNCS 3758. Berlin: Springer-Verlag, 2005. 541−552. [doi: 10.1007/11576235_56]

[15] Li DY, Meng HJ, Shi XM. Membership clouds and membership clouds generator. Journal of Computer Research and Development, 1995,32(6):15−20 (in Chinese with English abstract). [doi: CNKI:SUN:JFYZ.0.1995-06-002]

[16] Song SS, Hwang K, Macwan M. Fuzzy trust integration for security enforcement in grid computing. In: Proc. of the Int'l Symp. on Network and Parallel Computing (NPC 2004). LNCS 3222, Berlin: Springer-Verlag, 2005. 9−21. [doi: 10.1007/978-3-540-30141-7_6]

[17] Li XY, Gui XL. Cognitive model of dynamic trust forecasting. Journal of Software, 2010,21(1):163−176 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3558.htm [doi: 10.3724/SP.J.1001.2010.03558]

[18] Sun YX, Huang SH, Chen LJ, Xie L. Bayesian decision-making based recommendation trust revision model in ad hoc networks. Journal of Software, 2009,20(9):2574−2586. http://www.jos.org.cn/1000-9825/579.htm [doi: 10.3724/SP.J.1001.2009.00579]

[19] Liang ZQ, Shi WS. Analysis of ratings on trust inference in open environment. Journal of Performance Evaluation, 2008,65(2):99−128. [doi: 10.1016/j.peva.2007.04.001]

[20] Carbone M, Nielsen M, Sassone V. A formal model for trust in dynamic networks. In: Proc. of the Int'l Conf. on Software Engineering and Formal Methods (SEFM 2003). IEEE, 2003. [doi: 10.1109/SEFM.2003.1236207]

[21] Hung NQ, Shehzad A, Liaquat S, Riaz M, Lee SY. Developing context-aware ubiquitous computing systems with a unified middleware framework. In: Proc. of the 2004 Int'l Conf. on Embedded and Ubiquitous Computing. Springer-Verlag, 2004. 672−681. [doi: 10.1007/978-3-540-30121-9_64]

[22] Ashri R, Ramchurn SD, Sabater J, Luck M, Jennings NR. Trust evaluation through relationship analysis. In: Proc. of the 4th Int'l Joint Conf. on Autonomous Agents and Multi-Agent Systems. 2005. 1005−1011. [doi: 10.1145/1082473.1082625]

[23] Ren K, Li T, Wan Z, Bao F, Deng R, Kim K. Highly reliable trust establishment scheme in ad hoc networks. Computer Networks, 2004,45:687−699. [doi: 10.1016/j.comnet.2004.01.008]

[24] Li XY, Gui XL. Research on dynamic trust model for large scale distributed environment. Journal of Software, 2007,18(6):1510−1521 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/1510.htm [doi: 10.1360/jos181510]

[25] Xu F, Lü J. Research and development of trust management in Web security. Journal of Software, 2002,13(11):2057−2064 (in Chinese with English abstract). http://www.jos.org.cn/ch/reader/view_abstract.aspx?flag=1&file_no=20021101&journal_id=jos

[26] Wang Y, Lü J, Xu F, Zhang L. A trust measurement and evolution model for internetware. Journal of Software, 2006,17(4):628−690 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/682.htm [doi: 10.1360/jos170682]

[27] Xu F, Lü J, Zheng W, Cao C. Design of a trust valuation model in software service coordination. Journal of Software, 2003,14(6):1043−1051 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1043.htm

[28] Yang FQ, Mei H, Lü J, Jin Z. Some discussion on the development of software technology. ACTA ELECTRONICA SINICA, 2003,26(9):1104−1115 (in Chinese with English abstract). [doi: CNKI:ISSN:0372-2112.0.2002-S1-000]

[29] 吕建,马晓星,陶先平,徐锋,胡昊.网构软件的研究与进展.中国科学(E 辑:信息科学),2006,36(10):1037−1080.

[30] 吕建,马晓星,陶先平,曹春,黄宇,余萍.面向网构软件环境驱动模型与支撑技术研究.中国科学(E 辑:信息科学),2008,38(6):864−900.

[31] 杨芙清,吕建,梅宏.网构软件技术体系:一种以体系结构为中心的途径.中国科学(E 辑:信息科学),2008,38(6):818−828.

[32] 吕建,陶先平,马晓星,胡昊,徐锋,曹春.基于 Agent 的网构软件模型研究.中国科学(E 辑:信息科学),2005,35(12):1233−1253.

附中文参考文献:

[15] 李德毅,孟海军,史雪梅.隶属云和隶属云发生器.计算机研究与发展,1995,32(6):15−20. [doi: CNKI:SUN:JFYZ.0.1995-06-002]

[17] 李小勇,桂小林.动态信任预测的认知模型.软件学报,2010,21(1):163−176. http://www.jos.org.cn/1000-9825/3558.htm [doi: 10.3724/SP.J.1001.2010.03558]

[24] 李小勇,桂小林.大规模分布式环境下动态信任模型研究.软件学报,2007,18(6):1510−1521. http://www.jos.org.cn/1000-9825/18/1510.htm [doi: 10.1360/jos181510]

[25] 徐锋,吕建.Web 安全中的信任管理研究与进展.软件学报,2002,13(11):2057−2064. http://www.jos.org.cn/ch/reader/view_abstract.aspx?flag=1&file_no=20021101&journal_id=jos

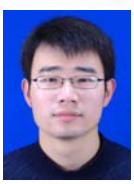
[26] 王远,吕建,徐锋,张林.一个适用于网构软件的信任度量及演化模型.软件学报,2006,17(4):628−690. http://www.jos.org.cn/1000-9825/20060404.htm [doi: 10.1360/jos170682]

[27] 徐锋,吕建,郑玮,曹春.一个软件服务协同中信任评估模型的设计.软件学报,2003,14(6):1043−1051. http://www.jos.org.cn/1000-9825/20030603.htm

[28] 杨芙清,梅宏,吕建,金芝.浅论软件技术发展.电子学报,2003,26(9):1104−1115. [doi: CNKI:ISSN:0372-2112.0.2002-S1-000]

邵堃(1967－),男,安徽寿县人,博士,副教授,主要研究领域为软件理论,需求工程.

梅袁雄(1986－),男,硕士生,主要研究领域为软件理论,软件架构.



罗飞(1986－),男,硕士,主要研究领域为软件理论,软件架构.

刘宗田(1946－),男,教授,博士生导师,主要研究领域为智能信息处理.