

基于上下文因素的 P2P 动态信任模型

刘义春, 梁英宏

(广东财经大学信息学院, 广东 广州 510320)

摘 要: 构建一个基于上下文因素的多维度 P2P 信任模型, 结合考虑时间衰减、交互重要性和交互次数度量实体交互信任, 基于 Dice 相似度给出信任相似度算法, 设计一种多链路反馈可信度融合算法, 聚合直接交互、评价相似度和信任链传递计算实体的推荐信任, 综合直接信任和推荐信任进行实体信任的评估, 并提出一种新的信任更新和奖惩机制。实例分析表明, 模型较好地体现了上下文因素对信任计算的影响, 增强了模型在上下文因素的敏感性。

关键词: P2P 系统; 信任; 上下文因素; 直接信任; 推荐信任

中图分类号: TP393

文献标识码: A

Dynamic P2P trust model based on context factors

LIU Yi-chun, LIANG Ying-hong

(Information School, Guangdong University of Finance and Economic, Guangzhou 510320, China)

Abstract: A multi-dimensional trust model was constructed based on the context factors. The direct trust of the interactive entities was estimated by integrating the time-decay factor, the transaction impact factor and the participation frequency. The trust similarity algorithm was designed based on the Dice similarity and the feedback credibility was aggregated from multiple trust chains. The direct interaction, the evaluation similarity and the trust chain was integrated for calculating the recommendation trust. The peer's trust was evaluated by combing the direct trust and the recommendation trust. A new mechanism was proposed for the trust's update, incentive or punishment according to the peer's behavior on the interaction. The practical example analysis shows that the proposed model can effectively explain the effect of the transaction contextual factors on the entity trust, and can improve the trust sensitivity to the context transaction factors.

Key words: P2P system, trust, context factor, direct trust, recommendation trust

1 引言

随着分布式技术的发展和互联网的普及, P2P 技术已广泛应用于协同系统、资源共享、网络计算、及时通信等环境, 成为当前重要的网络应用技术。

在传统的 C/S 模式中, 服务器是网络的核心, 所有事务都离不开服务器提供的服务, 因而可以通过使用安全认证、访问控制、日志审计等技术确保系统的安全。P2P 系统具有匿名性、随机性和动态性的特点。P2P 交互双方往往互不相识, 在缺乏可

信第三方的情况下通过网络直接交换信息, 失去了传统网络环境下信任所依赖的基础, 服务欺诈、版权侵害、病毒传播、文件污染、FreeRiding 等安全隐患屡见不鲜, P2P 系统的信任机制日益成为业内人士关注的焦点。

信任可分为基于身份的和基于行为的信任。基于身份的信任用于确认交互实体身份的真实性, 通常采用静态验证机制来判定交互实体身份的可信性, 常用技术包括加密技术、签名技术、认证授权技术、数据隐藏技术及访问控制策略。基于行为的信任用于评估实体行为的可信任程度, 常常通

收稿日期: 2016-02-02; 修回日期: 2016-05-24

基金项目: 教育部研究规划基金资助项目 (No.12YJAZH079); 广东省工业高新技术领域科技计划基金资助项目 (No.2013B01040103)

Foundation Items: The Project of Humanities and Social Sciences (No.12YJAZH079), The Guangdong Provincial Science and Technology Planning Project of China (No.2013B01040103)

过考察受评实体的历史行为记录、当前行为特征来判别其可信度。

P2P 系统中，交互实体不仅希望认证其他实体的身份真实性，更关心其他实体在交互中的可信任程度。P2P 系统中的信任指实体在参与交互、提供信息或服务过程中所表现的可靠性、诚信度、满意度。标识符、数字证书可标识实体的身份，而实体的信任值则标识实体在交互中的可信任程度。实体的用户标识符、数字证书一般相对静态不变，但是实体的信任是动态变化的。在 P2P 等协同系统中，真实性不是衡量实体可信与否的唯一指标，身份的真实性并不能蕴含实体行为的可信性。一个交互参与者身份可能被证实是真实的，但这并不意味着他会诚实地进行交互。要保障 P2P 系统的安全，就必须研究 P2P 系统的信任评价机制，建立有效的 P2P 系统信任模型。

本文通过考虑时间衰减、交互重要性、交互次数等上下文因素对信任评价的影响，利用一个单调递减的时间衰减函数反映时间因素对信任的影响，使用一个单调递增的交互次数影响函数将实体交互活跃度融入直接信任评价模型；对常见的推荐情形进行分析，抽象出基于直接交互经验的信任、基于共同评价相似度的信任和基于推荐信任链的信任这 3 类推荐信任形成机制，基于 Dice 相似度给出一种新的信任相似度算法，设计一种新的多链路反馈可信度融合算法，并实现 3 类推荐信任的聚合；结合直接信任和推荐信任，构建一个用于 P2P 系统的动态信任评价模型；研究实体信任的激励和更新机制，分别提出一类信任激励与惩罚算法、实体信任更新算法、信任推荐实体的反馈可信度更新算法，根据当前交互中实体表现出的交互满意度进行奖励、惩罚和信任的更新。

2 相关工作

Marsh 等^[1]在 1994 年首次系统地论述了信任的形式化问题，并从信任的主观性着手提出了信任评价的数学模型。1996 年，Blaze 等^[2]首次引入了“信任管理”的概念，并提出一个著名的信任管理系统 Policy Maker。Beth 等^[3]将经验分为肯定经验和否定经验，基于 agent 完成一次任务的可能性在 $[0,1]$ 服从均匀分布这一假设提出了一种信任模型。但是该模型在信任关系度量时只利用肯定经验，其信任度计算时对一些节点的恶意行为如恶意推荐无法很

好的识别。Jøsang 等^[4,5]引入观念空间与证据空间等概念，使用主观逻辑来描述和度量信任关系，提出一个由信念建模和信念逻辑算子组成的信任度推导和计算模型，并提供了一套主观逻辑（subjective logic）运算用于信任度的推理和综合计算。Jøsang 的模型没有对直接信任和推荐信任进行明确区分，也无法有效地规避恶意推荐带来的影响。Kamvar 等^[6]提出了一种全局信任模型 EigenTrust，通过对网络中邻居节点之间相互评价进行迭代，计算各个节点的全局可信度。但该模型存在着收敛性问题，且由于采用迭代计算，通信代价太高，不能很好地识别节点的恶意行为。PowerTrust^[7]是在 EigenTrust 基础上提出的一种新的信任模型，该模型采用了动态选举超级可信节点的算法，并使用一种名为“look-ahead”的随机行走策略，以改善全局声誉计算的迭代过程。ServiceTrust^[8]是一种基于节点评价行为相似度的信任模型，模型中全局信誉值的传播基于多跳的朋友圈机制来进行计算，使用了相似度作为信任传播过程的权重。Xiong 等^[9]提出了一种 PeerTrust 信任机制，该模型考虑了影响可信度量的多种因素，提供了一种纯分布式的可信度计算方法，但该模型没有给出信任因素及置信因子的度量方法。Huynh 等^[10]的 FIRE 模型融合了直接信任、基于角色规则的信任、证人信誉和第三方参考，最后用加权平均的方法来计算最终的信任评价。作为一个静态参量模型，FIRE 针对不同的服务需要设置不同的参数，此外模型中实体间的通信量也过大。Fan 等^[11]从云服务的操作性能、QoS、安全隐私等方面考虑，将云服务的适用性、可扩展性、可持续性、可用性、可靠性、一致性、可控性、可审计性等属性作为信任维度建立属性选择空间，提出一种用于各信念度属性的证据推理算法，使用证据推理融合多维信任评价，结合多评价等级效用进行评价融合，提出一个多维度信任感知的云服务选择方案，最后根据活动用户反馈的信任表现对信任证据进行更新。Ashtiani 等^[12]基于量子决策理论(QDT, quantum decision theory)提出一种新的信任评价方法，建立 QDT 和信任构建之间的映射关系，使用量子“干扰”在不同上下文环境、各种不确定性和风险情景下量化信任评价者的情感和主观偏好，根据量子的干扰交叉理论、干扰 $\frac{1}{4}$ 定理给干扰项赋予量值，基于 QDT 在 Hilbert 内积向量空间定义信任

模型,使用归一化的旋转操作改变上下文属性、测度上下文环境的信任值。田春岐等^[13]考虑推荐者的信誉值、信任评价者对推荐者直接交互经验、推荐者与被评为方的交易次数以及交易日期 4 个方面的因素,提出一种基于信誉和风险评价的 P2P 信任模型 R²BTM,将实体之间的信任程度和信任的不确定性统一起来,可以有效识别不同类型恶意节点。李小勇等^[14]提出了一个基于多维决策属性的信任评价模型,综合考虑信任的多种上下文因素,融合多个决策属性进行信任关系的推理和评估,有效解决了传统量化模型对环境的复杂性和不确定性适应能力不足的问题。甘早斌等^[15]提出了一种基于声誉的多维度信任算法,运用自信因子综合直接信任和推荐信任来对网络内的节点进行信任评估,定义时间敏感函数反映信任的动态衰减;选用幂函数构造一个递减的效用函数,描述各维度的递减风险厌恶、比例风险厌恶和递减比例风险厌恶,以增强信任算法在交易单个属性上的敏感性。李峰等^[16]引入历史交互窗口和可信推荐数等证据因素,综合考察实体信任的时间衰减、路径衰减、稳定度等因素,提出了一种基于交互感知的动态自适应信任评估模型,并分析了信任数据的分布存储机制。汪京培等^[17]通过提取主观性、模糊性、时间衰减性、传递性、奖惩等功能参数,分析了时间衰减、差别信任度、评价相似度、活跃度、欢迎度等上下文属性,研究实体的信任奖惩和信任更新机制,在对功能参数建模的基础上提出了一种分布式信任模型。李乔等^[18]使用网络交互拓扑信息建立网络节点间的信任矩阵,结合直接信任度和向量相关度计算网络节点间的相似度,并通过松弛谱聚类算法中的约束条件,增强类数目的自动识别能力,提高节点聚类准确性,提出一种基于信任的网络群体异常行为发现模型。

相关研究存在的问题如下。

1) 时间因素、空间因素会引起已有信任评价有效性的衰减,不同交互业务对实体的信任具有不同影响力,交互次数等因素也影响实体信任评价的可信度,信任评价需要对多种上下文因素的影响同时进行考虑。已有信任模型采用的评估策略评价维度不足,大多只针对单一的影响因素进行研究,没有考虑相关的上下文诸因素的协同影响。

2) P2P 业务大多运行于互联网络,容易同时遭

受多种形式的攻击。已有模型大多只对单一的欺诈进行识别和规避,而不能同时有效识别并抵抗源自多种形式的欺诈和攻击行为。

3) 实际场景中信任推荐的渠道多种,来自不同渠道的信任推荐具有不同的置信度,需要分别进行分析并综合考虑。但相关模型大多只对某类单一的推荐类型进行研究和建模,没有融合几种主要类型的信任推荐,不能有效解决信任推荐的多样性问题。

3 信任评价模型

3.1 总体框架

在 P2P 系统中,所有参与者(包括服务请求者、服务提供者 and 评价者)的集合称为实体集,记为 E 。

定义 1 (信任)。信任是某实体根据已有知识对另一实体特定行为或提供服务的满意程度的主观判断或预期。本文的模型中,将信任评价价值规范化到区间 $[0,1]$ 。信任可定义为论域 E 上二元影射

$$E \times E \rightarrow [0,1]$$

P2P 系统的信任按其来源分为直接信任和推荐信任。

实体 $i \in E$ 根据与实体 $j \in E$ 直接进行交互所得出的直接信任,以及从其他推荐实体处获得的关于实体 j 的推荐信任,进行加权平均即可得出实体 j 的综合信任评价价值。

定义 2 (总体信任度)。实体 $i \in E$ 根据与实体 $j \in E$ 直接交互和其他实体的推荐得出的实体 $j \in E$ 的总体信任度为

$$T(i, j) = \begin{cases} \alpha DT(i, j) + \beta RT(i, j), & DT(i, j) \text{ 和 } RT(i, j) \text{ 都存在} \\ DT(i, j), & RT(i, j) \text{ 不存在} \\ RT(i, j), & DT(i, j) \text{ 不存在} \\ DT_0, & DT(i, j) \text{ 和 } RT(i, j) \text{ 都不存在} \end{cases} \quad (1)$$

其中, $DT(i, j)$ 为实体 i 对实体 j 的直接信任, $RT(i, j)$ 为实体 i 获得的关于实体 j 的推荐信任; α, β 分别为直接信任和推荐信任的权重, $\alpha, \beta \in [0,1]$ 且 $\alpha + \beta = 1$ 。如果实体 i, j 间既无直接交互历史,又无法获得其他实体对实体 j 的推荐信任,则选择缺省信任值 DT_0 作为实体 j 的信任。

直接信任权重 α 、 β 值计算如下

$$\alpha = \frac{n_1^{\frac{3}{2}}}{n_1^{\frac{3}{2}} + n_2}, \beta = \frac{n_2}{n_1^{\frac{3}{2}} + n_2} \quad (2)$$

其中，实体 i 与实体 j 直接交互的次数为 n_1 ，来自其他实体对实体 j 的推荐次数为 n_2 。 n_1 的指数高于 n_2 ，说明直接交互对总体信任度影响大于第三方推荐。

3.2 直接信任

信任随着时间及其他环境因素的变化而变化。评价者的心理、性格、知识、能力、意愿等随时间变化，受评实体提供商品和服务的能力、参与事务的诚信状况、心理个性等因素也可能随时间变化。随着时间的流逝，信任信息对当前信任评价的参考价值愈来愈弱，呈单调递减趋势。越久远的信任评价，其说服力越差。

为了反映信任评价的时效性和动态性，引入动态时间窗口刻画实体在一段时间区间内的行为特征，信任评价时只考虑窗口内的信任记录。

定义 3 (时间窗口)。时间窗口集 $wins$ 是 m 个时间窗口的集合 $wins = \{win^{(1)}, win^{(2)}, \dots, win^{(m)}\}$ 。 $\forall l \in \{1, 2, 3, \dots, m\}$ ，第 l 个时间窗口定义为 $win^{(l)} = ([t_{begin}^{(l)}, t_{end}^{(l)}], s_l)$ ，其中， $t_{begin}^{(l)} \leq t_{begin}^{(l+1)}$ ， $t_{end}^{(l)} \leq t_{end}^{(l+1)}$ ， s_l 为区间 $[t_{begin}^{(l)}, t_{end}^{(l)}]$ 上时间片的数量 (即区间长度)。

如图 1 所示，时间窗口根据交互密集度确定窗口大小，每次向前移动一个时间片。

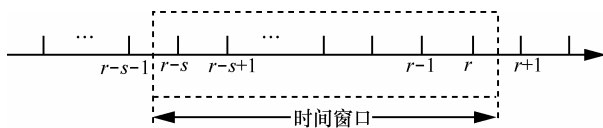


图 1 时间窗口

如果实体间交互变得非常频繁，时间窗口的区间可适当缩小；如果实体间交互变得较为稀疏，时间窗口的区间可适当延伸。如果窗口尺寸 (区间时间片数) 为 s_l 时交互次数为 N ，向前滑动后窗口内交互次数为 \tilde{N} ，则窗口大小调整如下

$$s_{l+1} = s_l - \text{Int} \left[\frac{(\tilde{N} - N)s_l}{N} \right] \quad (3)$$

定义 4 (时间衰减度)。时间衰减度是指随时间的推移，历史交互所表现的实体信任信息对当前实体信任评价影响衰减的程度。

时间衰减度可用一类单调减函数表示。距离当前时间越久远，交互结果对当前影响越小。

时间衰减度用衰减函数表示，衰减函数 $\phi(x)$ 应具有如下性质。

- 1) $\forall x \in (0, \infty)$, $\phi(x) \in (0, 1]$ 。
- 2) $\phi(x)$ 单调减，即当 $x_1 < x_2$ 时， $\phi(x_1) > \phi(x_2)$ 。
- 3) $\phi(0) = 1$ 。

从当前时间 t_r 向前至某个历史交互时刻 t 的时间间隔记为 $\Delta t = t_r - t$ ，时间衰减度用衰减函数表示如下

$$\phi(\Delta t) = e^{-\frac{\Delta t}{\lambda}} \quad (4)$$

其中，参数 λ 调整历史信任随时间的衰减速度，应根据具体的应用设定，一般设定 $\lambda = \frac{T_0}{\ln 2}$ ，使半衰期时信任影响衰减一半， T_0 为信任半衰期。假如 60 个时间片为信任随时间衰减的半衰期，则选择

$$\lambda = \frac{60}{\ln 2}$$

选择 $\lambda = \frac{60}{\ln 2}$ 时，信任随时间衰减的趋势如图 2 所示。

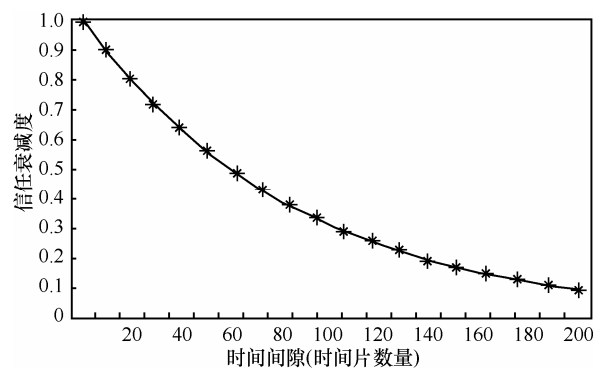


图 2 信任衰减示意

恶意的实体可能在若干普通事务中表现良好以抬高其信任度，而在一次重要事务中表现不诚实。因此分析实体以前参与事务所表现的信任状况以确定实体信任值时，需要考虑所参与事务的重要程度，而不能简单地进行平均计算。为了标识某事务对实体信任的影响程度，引入影响因子 (impact factor) 的概念。事务影响因子越大，表明该事务对实体信任值的影响越大；反之，该事务对实体信任值的影响越小。如大额交易的影响因子大于小额交易，重要文件服务的影响因子大于普通文件服务。

在本文的信任评价模型中，将事务影响因子归

一化到区间[0,1]。一个典型的例子是 P2P 交易情境中，如果交易标的额为 x ，事务影响因子可如式(5)计算。

$$f(x) = \begin{cases} \left(\frac{x}{M_0}\right)^{\frac{1}{2}}, & x < M_0 \\ 1, & x \geq M_0 \end{cases} \quad (5)$$

其中， M_0 为交易标的金额的阈值，交易额大于 M_0 时交易影响因子为 1。

下面给出直接信任的定义。

定义 5 (直接信任)。直接信任 DT_{ij} 是评价实体 $i \in E$ 根据与受评实体 $j \in E$ 的直接交互经验而得出的对受评实体 j 的信任评价。

如果评价实体和受评实体间曾存在一次或多次交互，则可通过历史交互的满意情况评价受评实体的直接信任值。假设实体 i 与实体 j 在时间窗口内共进行了 n 次交互，第 l 次交互时间距今 Δt_l 个时间片，第 l 次交互的事务影响因子为 IF_l ，第 l 次交互后实体 i 对实体 j 进行评价得到评价价值 $S_l \in [0,1]$ ，则直接信任计算如下

$$DT_{ij} = \frac{\sum_{l=1}^n S_l \varphi(\Delta t_l) IF_l}{\sum_{l=1}^n \varphi(\Delta t_l) IF_l} \quad (6)$$

其中， $\varphi(\Delta t_l)$ 为第 l 次交互相对于当前时刻的信任衰减度， IF_l 为第 l 次交互的事务影响因子。

通过一次或几次交互不一定能获得实体的真实信任，恶意的实体可能进行若干次信任积累。计算直接信任时需要考虑当前时间窗口内交互次数的多少。一般来说，2 个实体间交互次数越多，所测信任值越接近客观的信任度。

定义 6 (交互活跃度)。交互活跃度指受评实体在观察时间内参与交互的频度。

实体活跃度反映了实体在网络中的活跃程度与稳定程度。实体活跃度对实体信任的影响用交互次数影响函数 $\rho(x)$ 表示，交互次数影响函数 $\rho(x)$ 应具有如下性质。

- 1) $\forall x \in Z, \rho(x) \in (0,1]$ 。
 - 2) $\rho(x)$ 单调增，即当 $x_1 < x_2$ 时， $\rho(x_1) \leq \rho(x_2)$ 。
 - 3) 当 $x \rightarrow \infty$ 时，有 $\rho(x) \rightarrow 1$ 。
- $\rho(x)$ 可采用如下表达式计算

$$\rho(x) = \frac{\arctan(x - a)}{\pi} + 0.5 \quad (7)$$

其中， x 为实体间交互次数，参数 $a \geq 1$ 为次数调节因子， $\rho(a) = 0.5$ 。本文所述应用中建议参数 a 取值于区间[2,5]的正整数。

取值 $a=3$ 时交互次数影响函数 $\rho(x)$ 变化趋势下图 3 所示。

考虑交互次数后的直接信任计算如下

$$DT_{ij} = \rho(n) \frac{\sum_{l=1}^n S_l \varphi(\Delta t_l) IF_l}{\sum_{l=1}^n \varphi(\Delta t_l) IF_l} + (1 - \rho(n)) DT_0 \quad (8)$$

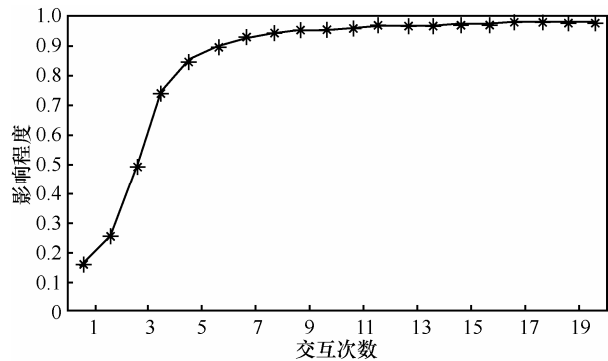


图 3 交互次数影响函数变化

其中， n 为目前所在时间窗口内评价实体 i 与受评实体 j 之间的交互次数。 DT_0 为实体的缺省信任值，标识给予无历史交互记录的实体所赋的信任初值。

在欺诈可能不太高的应用中，建议设 $DT_0 = \frac{\sqrt{5}-1}{2} \approx 0.618$ ；

当容易产生欺诈的应用场景，建议设 $DT_0 = 1 - \frac{\sqrt{5}-1}{2} \approx 0.382$ ；

如果对欺诈可能性无先验知识，则建议设 $DT_0 = 0.5$ 。

当各次直接交互信任评分平均值高于缺省信任值 DT_0 时，式(8)计算所得的直接信任较式(6)计算所得值有所下调；当各次直接交互信任评分平均值低于缺省信任值 DT_0 时，式(8)计算所得的直接信任较式(6)计算所得值有所上调。当交互次数大于 a 值后，式(8)计算所得的直接信任迅速趋近于式(6)计算所得信任值。

3.3 推荐信任

直接信任仅存在于已经有过交互经验的实体之间。直接交互经验固然重要，然而评价实体时常需要面对并不熟悉的陌生实体，往往没有以往的直接交互经验可以借鉴，这时只能依靠来自其他实体的推荐。

实体 i 对实体 j 进行评价时，仅靠自己与实体 j 的交互历史可能还不够客观，尚需其他实体推荐受评实体的信任信息，特别是在实体 i 从未与实体 j 交互过的情况下更是如此。

定义 7 (推荐信任)。推荐信任 RT_{ij} 是评价实体 $i \in E$ 根据第三方实体 $k \in E$ 提供的对实体 $j \in E$ 的信任评价而形成的对实体的信任判断。推荐信任也称间接信任。

定义 8 (反馈可信度)。反馈可信度是实体 $i \in E$ 认为实体 $k \in E$ 作为推荐方所反馈推荐信息的可信程度，用 Cr_{ik} 表示。

实体 i 对推荐实体 k 的了解源于几种情形：1) 实体 i, k 之间曾有过直接交互，由直接交互的满意度可推测实体 k 的反馈可信度；2) 实体 i, k 皆曾对若干共同对象进行信任评价，实体 i 根据评价的相似度可估算实体 k 的反馈可信度；3) 评价实体 i 与推荐实体 k 之间存在一条或多条由若干中介节点组成的推荐链路，利用信任的弱传递性可计算实体 k 信任推荐的反馈可信度。

下面分别就这几种推荐情形进行分析。

3.3.1 基于直接交互的推荐信任

在第 1 种情形下，评价实体 i 与推荐实体之间曾有过直接交互，这类推荐实体集合记为 $RS_1 \subseteq E$ 。任一推荐实体 $k \in RS_1$ 将其对于实体 j 的信任 T_{kj} 反馈给实体 i 。实体 i 以其对推荐实体 k 的直接信任 DT_{ik} 作为实体 k 的反馈可信度，即

$$Cr_{ik}^{(1)} = DT_{ik}$$

由此类推荐产生的推荐信任如下

$$RT_{ij}^{(1)} = \frac{\sum_{k \in RS_1} Cr_{ik}^{(1)} T_{kj} \varphi(\Delta t_k) IF_k}{\sum_{k \in RS_1} Cr_{ik}^{(1)} \varphi(\Delta t_k) IF_k}$$

或

$$RT_{ij}^{(1)} = \frac{\sum_{k \in RS_1} DT_{ik} T_{kj} \varphi(\Delta t_k) IF_k}{\sum_{k \in RS_1} DT_{ik} \varphi(\Delta t_k) IF_k} \quad (9)$$

其中， DT_{ik} 标识实体 i 对于推荐实体 k 的直接信任， T_{kj} 标识推荐实体 k 对于受评实体 j 的信任； $\varphi(\Delta t_k)$ 为实体 i 与实体 k 之历史交互对于当前时刻的信任衰减度， IF_k 为实体 i 与推荐实体 k 交互事务的影响因子。

3.3.2 基于评价相似度的推荐信任

在第 2 种情形下，评价实体 i 与推荐实体之间没有过直接交互，但皆曾对多个相同对象进行信任评价，

这类推荐实体集合记为 $RS_2 \subseteq E$ 。实体 i 根据评价的向量相似度可估算推荐实体反馈信任的反馈可信度。

2 个实体分别对同一组实体进行信任评价，其评价结果为 2 组向量，这 2 组向量的匹配测度反映了 2 组信任评价的相似程度。

定义 9 (向量相似度)。向量相似度表示两组向量的匹配程度。向量相似度可用于衡量 2 个实体的行为相似程度。

向量相似度一般使用向量距离或相关系数来测度，常用的方法有内积法、简单匹配系数法、相关系数法、夹角余弦法、Dice 系数法、Jaccard 系数法(也称 Tanimoto 系数)等。

第 2 类情形下的反馈可信度采用 Dice 相似度进行计算。 $IS \subseteq E$ 表示与 i 交互过的实体集合， $KS \subseteq E$ 表示与 $k \in RS_2$ 交互过的实体集合， $CS = IS \cap KS$ 为既与 i 也与 k 有过交互的实体集合。通过将实体 i 对集合 CS 中各个实体信任评分值、实体 k 对集合 CS 中各个实体的信任评分值进行比较，把计算所得的 Dice 相似度作为实体 k 的反馈可信度。

实体 i 和实体 k 对集合 CS 中实体的信任评分向量分别记为 $(T_{i1}, T_{i2}, \dots, T_{in})$ 和 $(T_{k1}, T_{k2}, \dots, T_{kn})$ ，推荐节点的反馈可信度 $Cr_{ik}^{(2)}$ 可用如下向量相似度衡量。

$$Cr_{ik}^{(2)} = \eta \frac{2 \sum_{l \in CS} T_{il} T_{kl}}{\sum_{l \in CS} T_{il}^2 + \sum_{l \in CS} T_{kl}^2} + (1 - \eta) \frac{2|IS \cap KS|}{|IS| + |KS|} \quad (10)$$

其中， $\eta \in (0.5, 1]$ 控制通过向量相似度计算获得的对一组实体的评分相似度； $1 - \eta$ 控制 i 和 k 共同信任的实体比重，该比重计算采用广义 Dice 系数对应的二值权重方案。

由第 2 种推荐产生的推荐信任如下

$$RT_{ij}^{(2)} = \frac{\sum_{k \in RS_2} Cr_{ik}^{(2)} T_{kj}}{\sum_{k \in RS_2} Cr_{ik}^{(2)}} \quad (11)$$

3.3.3 基于信任链的推荐信任

在第 3 种情形下，评价实体 i 与推荐实体 k 之间没有过直接交互，但存在一条或多条推荐链路，由多个中间节点进行信任的传递，这类推荐实体集合记为 $RS_3 \subseteq E$ 。

定义 10 (信任链)。从评价实体 i 到推荐实体 $k \in RS_3$ 的信任链集合 $CT_{ik} = \{CT_{ij}^{(l)} \mid l=1, 2, \dots, NC\}$ ，

其中 NC 为链路条数, 第 l 条信任链 $CT_{ik}^{(l)} = \{(i, c_1^{(l)}, c_2^{(l)}, \dots, c_{p(l)-1}^{(l)}, k), (T(i, c_1^{(l)}), T(c_1^{(l)}, c_2^{(l)}), \dots, T(c_{p(l)-2}^{(l)}, c_{p(l)-1}^{(l)}), T(c_{p(l)-1}^{(l)}, k))\}$ 。对于整数 $q \in [1, p(l)]$, $T(c_{q-1}^{(l)}, c_q^{(l)})$ 是节点 $c_{q-1}^{(l)}$ 、 $c_q^{(l)}$ 之间的信任度, $p(l) \in \{x | x \geq 2, x \in \mathbb{Z}\}$ 为第 l 条信任链的跳数。为了表示方便, 不妨记实体 i 为 $c_0^{(l)}$, 记实体 k 为 $c_{p(l)}^{(l)}$ 。

从第 l 条信任链获得的关于推荐实体 k 的反馈可信度为

$$\left(\prod_{q=0}^{p(l)-1} T(c_q^{(l)}, c_{q+1}^{(l)}) \right)^{\frac{1}{p(l)}}$$

容易看出, $p(l)=1$ 时就是 i, k 之间存在直接交互的情形, 即 3.3.1 节中论述的第 1 种推荐情形, 即反馈可信度为 i, k 之间的直接信任。

综合考虑 NC 条链路信任传递状况, 可得到基于推荐链路的反馈可信度如下

$$Cr_{ik}^{(3)} = \sum_{l=1}^{NC} \frac{\left(\prod_{q=0}^{p(l)-1} T(c_q^{(l)}, c_{q+1}^{(l)}) \right)^{\frac{1}{p(l)}}}{\sum_{l=1}^{NC} \frac{1}{lb(p(l))}} \quad (12)$$

经由多条不同的链路进行信任传输时, 由于每一节点传递的信任值皆可能具有误差或恶意风险, 链路跳数越多, 误差或恶意风险积累越大。为了应对此问题, 式(12)对多个链路的信任没有采取简单平均, 而是考虑链路长度 $p(l)$, 以 $\frac{1}{lb(p(l))}$ 为权重, 使得较短的信任链路具有较高的权重。

例如, 在图 4 所示的信任传递图中, 从节点 B 到节点 A 有 4 条信任传递链路, 每条边上数值代表边首尾节点之间信任值。链路 $B \rightarrow E_1 \rightarrow C_1 \rightarrow A$ 反馈可信度为 $(0.8 \times 0.75 \times 0.8)^{\frac{1}{3}} = 0.783$, 权重为

$$\frac{\frac{1}{lb3}}{\frac{1}{lb3} + \frac{1}{lb3} + \frac{1}{lb2} + \frac{1}{lb3}} = 0.218; \text{ 链路 } B \rightarrow E_2 \rightarrow C_1 \rightarrow A \text{ 反}$$

馈可信度为 $(0.75 \times 0.8 \times 0.8)^{\frac{1}{3}} = 0.783$, 权重为

$$\frac{\frac{1}{lb3}}{\frac{1}{lb3} + \frac{1}{lb3} + \frac{1}{lb2} + \frac{1}{lb3}} = 0.218; \text{ 链路 } B \rightarrow C_2 \rightarrow A \text{ 的反}$$

馈可信度为 $(0.65 \times 0.75)^{\frac{1}{2}} = 0.698$, 权重为

$$\frac{\frac{1}{lb2}}{\frac{1}{lb3} + \frac{1}{lb3} + \frac{1}{lb2} + \frac{1}{lb3}} = 0.346; \text{ 链路 } B \rightarrow E_3 \rightarrow C_2 \rightarrow A \text{ 反}$$

馈可信度为 $(0.8 \times 0.75 \times 0.75)^{\frac{1}{3}} = 0.766$, 权重为

$$\frac{\frac{1}{lb3}}{\frac{1}{lb3} + \frac{1}{lb3} + \frac{1}{lb2} + \frac{1}{lb3}} = 0.218。 \text{ 综合 4 条推荐链路的反}$$

馈可信度为 $0.783 \times 0.218 + 0.783 \times 0.218 + 0.698 \times 0.346 + 0.766 \times 0.218 = 0.750$ 。

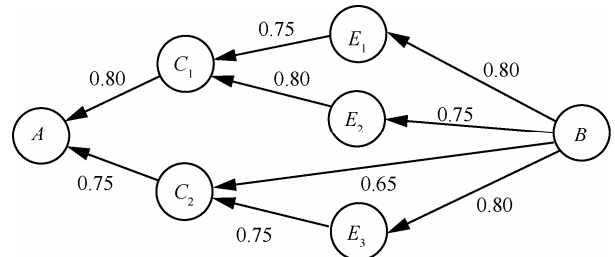


图 4 信任传递示意

由第 3 种推荐产生的推荐信任如下

$$RT_{ij}^{(3)} = \frac{\sum_{k \in RS_3} Cr_{ik}^{(3)} DT_{kj}}{\sum_{k \in RS_3} Cr_{ik}^{(3)}} \quad (13)$$

3.3.4 推荐信任的融合

综合式(9)、式(11)和式(13) 3 种推荐情形的信任, 得到实体 i 获得推荐实体集的对实体 j 的推荐信任如下

$$RT_{ij} = w_1 RT_{ij}^{(1)} + w_2 RT_{ij}^{(2)} + w_3 RT_{ij}^{(3)} \quad (14)$$

3 种推荐情形的信任 $RT_{ij}^{(1)}$ 、 $RT_{ij}^{(2)}$ 、 $RT_{ij}^{(3)}$ 的权重 w_1 、 w_2 、 w_3 计算如下

$$\begin{cases} w_1 = \frac{|RS_1|^{1.5}}{|RS_1|^{1.5} + |RS_2|^{1.5} + |RS_3|} \\ w_2 = \frac{|RS_2|^{1.5}}{|RS_1|^{1.5} + |RS_2|^{1.5} + |RS_3|} \\ w_3 = \frac{|RS_3|}{|RS_1|^{1.5} + |RS_2|^{1.5} + |RS_3|} \end{cases} \quad (15)$$

其中, $|RS_1|$ 、 $|RS_2|$ 、 $|RS_3|$ 分别为 3 类推荐实体集合 RS_1 、 RS_2 、 RS_3 之阶。

通过进行加权而非简单平均, 既综合考虑 3 种不同情形的信任推荐, 又使有直接接触的邻居节点

的推荐信任较其他推荐节点的推荐值有更大的权重。经过的中间环节越多，信任推荐参考价值越小，这也符合已有的经验和常识。

3.4 信任的更新与奖惩

3.4.1 信任更新

在 P2P 服务、电子商务交易等分布式系统中，每次交互之后，有必要对交互实体的信任进行更新，以更客观地体现交互实体的信任变化。如果此次交互中目标实体表现的信任度高于预估的信任度，适当调高实体的信任度，反之则调低受评实体的信任度。

如果交互前评估的实体信任度为 T_{ij} ，本次交互中实体表现的信任值为 S_{ij} ，交互结束后实体信任更新如下。

$$T_{ij} \leftarrow \theta S_{ij} + (1 - \theta) T_{ij} + \delta \quad (16)$$

其中， θ 为信任更新调节因子， δ 为信任奖惩分量。

信任更新调节因子 θ 计算如下

$$\theta = \begin{cases} 1 - \sqrt{\frac{S_{ij} - 0.5}{T_{ij}}}, & \frac{S_{ij}}{T_{ij}} \geq 0.5 \\ 1, & \frac{S_{ij}}{T_{ij}} < 0.5 \end{cases} \quad (17)$$

如果此次交互中受评实体所表现的信任度高于原有直接信任度，即 $S_{ij} \geq T_{ij}$ ，信任更新更多考虑历史评价构成的直接信任度；如果此次交互中受评实体所表现的信任度低于原有直接信任度，即 $S_{ij} < T_{ij}$ ，信任更新更多地综合本次交互的信任度；如果此次交互中受评实体所表现的信任度与原有直接信任度相等，即 $S_{ij} = T_{ij}$ ，实体信任度维持不变；如果此次交互中受评实体所表现的信任度不高于原有直接信任度之半，即 $S_{ij} \leq 0.5 T_{ij}$ ，信任的更新仅考虑本次交互的信任，而忽略既有历史信任因素。

表 1 列出部分 $\frac{S_{ij}}{T_{ij}}$ 比值以及对应的 θ 值，反映 $\frac{S_{ij}}{T_{ij}}$

值与信任更新调节因子之关系。

由表 1 可以看出，当平时信任评价不高的恶意实体为骗取信任而欲通过一次交互表现高信任度时， S_{ij} 值远大于 T_{ij} ，根据式(17)计算出的信任更新调节因子 θ 远小于 0.5，本次交互所表现信任值在信任评价中权重较小，恶意实体的图谋不能得逞。

对于信任表现时高时低的实体，通过信任更新使对“摇摆”实体的信任评价更倾向于其表现较劣时的信任度。

表 1 $\frac{S_{ij}}{T_{ij}}$ 值与信任更新调节因子之关系

$\frac{S_{ij}}{T_{ij}}$	θ 取值
≤ 0.5	1
0.75	0.622
1	0.5
1.5	0.368
2	0.293
2.5	0.244
3	0.209
3.5	0.184
4	0.163
4.5	0.147
5	0.134
5.5	0.123

3.4.2 信任的奖惩

每次信任更新时，应根据本次交互中实体表现的满意度对实体进行信任奖惩，表现好的实体交互后应得到适当奖励，表现不好的实体交互后应得到一定惩罚。实体参与交互越积极，交互次数越多，越利于信任评价。因此，信任评估模型中的奖惩机制应考虑实体参加交互的积极性。

每次交互之后，有必要根据本次交互中实体的表现进行奖励或惩罚。信任奖惩分量 δ 如下

$$\delta = \begin{cases} \left(1 - e^{-\frac{n}{2a}}\right) T_{ij} (1 - S_{ij}) (S_{ij} - T_{ij}), & S_{ij} \geq T_{ij} \\ \left(1 - e^{-\frac{n}{a}}\right) S_{ij} (1 - T_{ij}) (S_{ij} - T_{ij}), & S_{ij} < T_{ij} \end{cases} \quad (18)$$

在式(18)中， n 为目前所在时间窗口内评价实体 i 与受评实体 j 之间的交互次数；参数 $a \geq 1$ 依然采用式(7)中的次数调节因子。

式(18)所述奖惩机制具有下述性质。

性质 1 当 $S_{ij} > T_{ij}$ 时， $\delta < 1 - S_{ij}$ ；当 $S_{ij} < T_{ij}$ 时， $\delta > -T_{ij}$ 。

证明 当 $S_{ij} > T_{ij}$ 时，由于 $S_{ij} \in [0, 1]$ ， $T_{ij} \in [0, 1]$ ，

$$\begin{aligned} \delta &= (1 - e^{-\frac{n}{2a}})T_{ij}(1 - S_{ij})(S_{ij} - T_{ij}) \\ &< T_{ij}(1 - S_{ij})(S_{ij} - T_{ij}) \\ &\leq T_{ij}(1 - S_{ij})(1 - T_{ij}) \\ &< 1 - S_{ij} \end{aligned}$$

当 $S_{ij} < T_{ij}$ 时, 由于 $S_{ij} \in [0, 1]$, $T_{ij} \in [0, 1]$, 有

$$\begin{aligned} \delta &= (1 - e^{-\frac{n}{a}})S_{ij}(1 - T_{ij})(S_{ij} - T_{ij}) \\ &> -S_{ij}(1 - T_{ij})(T_{ij} - S_{ij}) \\ &> -S_{ij} \\ &> -T_{ij} \end{aligned}$$

性质 1 保证经过式 (17) 的信任更新和奖惩实施, 实体信任度虽有所上升或下降, 但调整后的信任度之值维持在区间 $[0, 1]$ 之内。

性质 2 本次交互满意度 S_{ij} 较 T_{ij} 上升时, 升幅越大, 奖励比率反而越小。

证明 发生本次交互前, 式 (18) 中 T_{ij} 项已经获得。 $S_{ij} > T_{ij}$ 时, S_{ij} 越大, $1 - S_{ij}$ 反而越小, 亦即 S_{ij} 升幅越大奖励比率反而越小。

性质 2 能够防止出现摇摆攻击时因实体满意度遽升而给予过高奖励, 从而减免摇摆攻击的影响。

性质 3 时间窗口内交互次数越大, 信任的奖励 (或惩罚) 值也越大。

证明 设 $f(x) = 1 - e^{-\frac{x}{2a}}$ ($a > 1$), 则 $f'(x) = \frac{1}{2a}e^{-\frac{x}{2a}} > 0$, $f(x)$ 为单调增函数, n 越大则 $f(n) = 1 - e^{-\frac{n}{2a}}$ 越大, 信任的奖励值越大。

同理可证, $1 - e^{-\frac{x}{a}}$ 亦为单调增函数, n 越大则 $1 - e^{-\frac{n}{a}}$ 亦越大, 信任的惩罚值越大。

3.4.3 反馈可信度更新

每次交互之后, 除了对交互实体的信任进行更新外, 也有必要利用本次交互的结果对推荐实体的反馈可信度进行更新。如果此次交互中目标实体表现的信任度高于原来估算出的推荐信任度, 适当调高各推荐实体的反馈可信度, 否则将调低推荐实体的反馈可信度。

如果第 l 类推荐情形下推荐实体 k 反馈可信度评估为 $RC_{ik}^{(l)}$, 推荐实体推荐的实体 k, j 间的信任为 T_{kj} , 本次交互中实体表现的信任值为 S_{ij} , 本次反

馈信任偏离度计算如下

$$Diff_{ik} = \frac{|S_{ij} - T_{kj}|}{\min(S_{ij}, T_{kj})} \quad (19)$$

根据反馈信任偏离度计算出的推荐实体本次反馈可信度如下

$$Cr' = e^{-\sigma Diff_{ik} Diff_{ik}} \quad (20)$$

其中, 参数 σ 建议取值于区间 $[5, 8]$ 。 $Diff_{ik} \rightarrow 0$ 时, $Cr' \rightarrow 1$; 随着 $Diff_{ik}$ 逐渐增大, Cr' 值急剧下降并向 0 趋近。

交互结束后推荐实体反馈可信度更新如下

$$Cr_{ik}^{(l)} \leftarrow \mu^{(l)} Cr_{ik}^{(l)} + (1 - \mu^{(l)}) Cr', \quad l = 1, 2, 3 \quad (21)$$

其中, $\mu^{(l)}$ 为第 l 种推荐情形下反馈可信度更新调节因子。第 l 种推荐情形下反馈可信度更新调节因子 $\mu^{(l)}$ 计算如下

$$\mu^{(l)} = \frac{n^{(l)} - 0.5}{n^{(l)} + N^{(l)} - 1} \quad (22)$$

其中, $n^{(l)}$ 为第 l 种推荐情形下实体 k 的推荐次数, 参数 $N^{(l)} \in Z$ (Z 代表正整数集) 为均衡次数。 $n^{(l)} = N^{(l)}$ 时反馈可信度更新中, 基于反馈信任偏离度的反馈可信度与 3.3 节中计算的反馈信任度各占一半; 当推荐次数少于 $N^{(l)}$ 时, 权重 $\mu^{(l)}$ 值小于 0.5, 更新后的反馈可信度更侧重于本次交互的影响; 当推荐次数大于参数 $N^{(l)}$ 时, 权重 $\mu^{(l)}$ 值大于 0.5, 更新后的反馈可信度更侧重于历史反馈信任度的影响。

由于直接接触的邻居节点的推荐较经过多个中间节点的信任链路推荐具有更高的反馈可信度, 第 1 种推荐情形被认为比较可靠, 而第 3 种推荐情形相对来说被认为可信度较低。因此, 参数 $N^{(l)}$ 的选择应遵循 $N^{(1)} < N^{(2)} < N^{(3)}$ 的原则。

4 仿真及结果分析

通过 NetLogo 平台模拟一个多主体交互环境, 对文章提出的模型及已有的相关模型进行比较、分析。 NetLogo 系统是美国西北大学提出的多主体建模环境, 采用 Java 语言编写, 能够跨异构平台运行。

4.1 直接信任计算的有效性

一个恶意的实体为了骗取信任, 可能先在一系列交互活动中伪装成可信实体, 当其信任积累

到一定程度后进行恶意攻击。为了考察本文所提出模型对此类攻击的反应敏感程度，将本模型与 R^2BTM 模型以及简单信任模型进行比较。简单信任模型指直接将各次直接交互的信任评分作为直接信任值，不考虑信任随时间的衰减和事务影响因子等上下文因素的影响； R^2BTM 模型考虑了信任随时间的衰减影响，但未考虑事务影响因子等其他因素的影响；本文提出的模型既考虑了信任随时间的衰减影响，也考虑了事务影响因子等其他上下文属性的影响。

实验模拟了恶意实体的 2 类攻击行为：1) 恶意实体首先在多次交互中表现可信，积累一定信任后进行恶意攻击；2) 恶意实体在诚信交互和恶意攻击之间振荡，即著名的摇摆攻击。

针对前者的实验场景为：恶意实体与评价实体进行了 20 次交互，前 10 次交互均为高可信度，后 10 次交互可信度较低。实验演示恶意实体通过多次较低影响因子的可信交互并积累一定的信任评价后，进行不合作交互行为时信任值的变化情况。参数取值 $\lambda=28.85$ 。模型对滥用信任的敏感程度如图 5 所示。

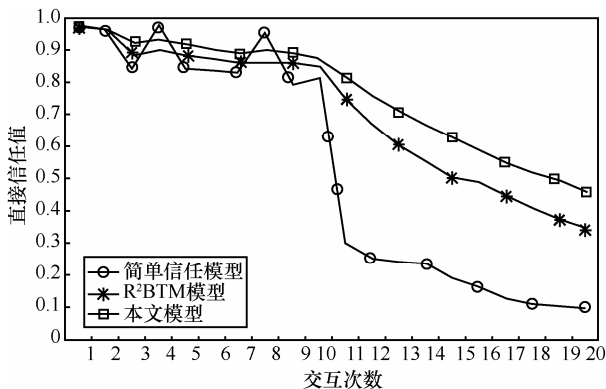


图 5 第 1 种攻击下直接信任的变化情况

图 5 中的本文模型和 R^2BTM 模型曲线均较简单模型更为平滑，因为每一交互时间节点实体的信任值均为前面历次交互信任值的加权平均，所以信任值变化幅度较小。本文模型较 R^2BTM 模型增加了事务影响因子的考虑，所仿真得出的信任值小于 R^2BTM 模型，但变化趋势大体一致。虽然恶意实体蓄意在较低事务影响因子的交互中表现较高信任度以骗取信任积累，本文模型考虑了事务影响因子的影响，适当降低了实体的信任评价以减轻实体欺骗的影响，从而更客观反映实

体的信任程度。

针对摇摆攻击的实验场景为：恶意实体与用户进行了 20 次交互，高可信度和低可信度的交互交替出现。参数仍取值 $\lambda=28.85$ 。模型对滥用信任的敏感程度如图 6 所示。

图 6 中的本文模型的变化曲线较简单模型信任值振幅小得多，这是因为每一交互时间节点的信任值均为前面历次信任值的加权平均，所以信任值相对稳定一些。本文模型所仿真得出的信任值明显小于 R^2BTM 模型。虽然恶意实体蓄意在较低影响因子的交互中表现较高信任度以骗取信任积累，本文模型通过考虑事务影响因子对信任的影响，降低了摇摆攻击实体的信任评价，从而更有效地消除了恶意实体欺诈的影响。

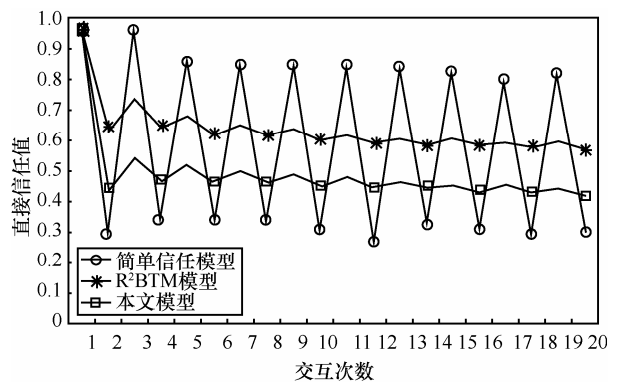


图 6 第 2 种攻击下直接信任的变化情况

4.2 推荐信任计算的有效性

为了考察推荐信任值、时间衰减因素以及推荐信任的事务影响因子等因素对间接信任的影响，将本模型与 R^2BTM 模型以及简单信任模型进行比较。简单信任模型指直接将各推荐者的信任评价平均值作为间接信任值，不考虑信任随时间的衰减和事务影响因子等上下文因素的影响；在决定推荐信任权重时， R^2BTM 模型考虑了推荐信任随时间的衰减影响，但未考虑事务影响因子等其他因素的影响；本文提出的模型既考虑推荐信任随时间衰减的影响，也考虑事务影响因子等其他因素的影响。

实验模拟了 2 类不同的推荐情景：1) 在正常情形下，事务影响因子高低与信任推荐值没有明显的关联；2) 低影响因子事务的信任推荐值较高，高影响因子事务的信任推荐值较低，这一般意味可能存在恶意的信任积累。

针对第 1 种情景的实验场景为：评价者先后获

得 20 次来自不同推荐实体的信任推荐。实验演示正常情形下的间接信任计算值的变化。参数取值 $\lambda=28.85$ 。模型对信任推荐的敏感程度如图 7 所示。

由图 7 可看出，本文的模型和 R^2BTM 模型曲线均较简单信任模型更为平滑，因为每一事件节点的信任值均为前面历次信任值的加权平均，所以信任值相对稳定。本文模型虽然较 R^2BTM 模型增加了事务影响因子的考虑，但如果事务影响因子高低与信任推荐值没有明显的关联，仿真得出的信任值与 R^2BTM 模型信任值变化基本一致。

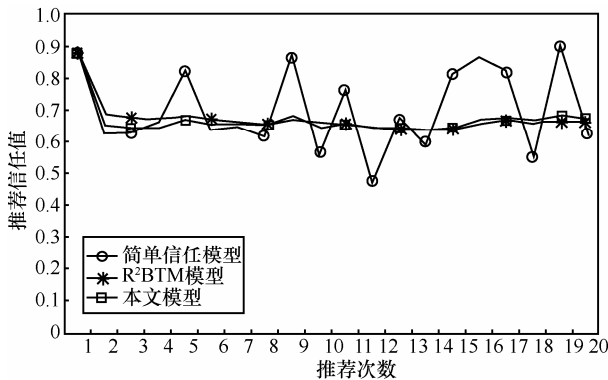


图 7 第 1 种情景下推荐信任的变化情况

针对第 2 种情景的实验场景为：评价者也先后获得 20 次来自不同推荐实体的信任推荐，低影响因子的事务信任推荐值较高，高影响因子的事务信任推荐值较低。实验演示可能存在恶意的信任积累情形下的间接信任计算值的变化。参数仍取值 $\lambda=28.85$ 。模型对信任推荐的敏感程度如图 8 所示。

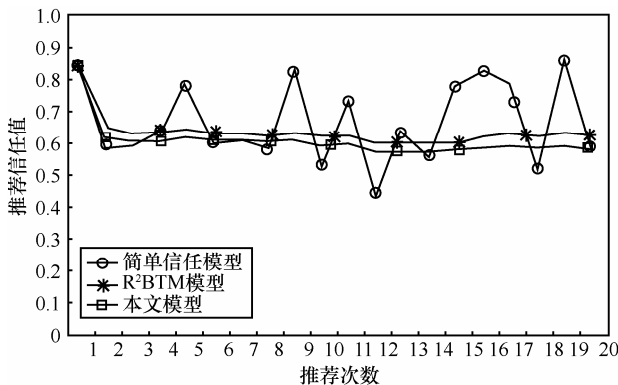


图 8 第 2 种情景下推荐信任的变化情况

由图 8 可看出，如果受评实体在低影响因子的事务信任推荐值较高，高影响因子的事务信任推荐值较低，本文模型通过增加事务影响因子等

因素的考虑，仿真得出的信任值比 R^2BTM 模型信任值有所降低。如果受评实体蓄意在较低影响因子的事务交互中表现较高信誉以进行信任积累，本文模型通过考虑事务影响因子对信誉的影响降低实体的信誉，从而更加客观反映实体的可信任程度。

5 结束语

本文考虑 P2P 系统中上下文因素对实体信任度的影响，对相似度计算、时间衰减函数、交互次数函数等不确定性因素进行了定量描述，基于直接交互经验、共同评价相似度和推荐信任链这 3 类推荐信任形成机制分别探析推荐信任的评价算法及信任融合，提出一种结合直接信任和推荐信任的动态信任评价模型，研究实体信任的奖惩算法和更新机制，并使用一种模拟的多主体环境来对文中所提出的模型及其相关算法的性能进行仿真分析。分析和仿真结果表明所提信任模型是合理和有效的，相对于相关对照模型表现较为优越。下一步的研究包括进一步增加系统的上下文属性，提高信任模型的评价维度，改进信任模型的风险调节机制等。

参考文献:

- [1] MARSH S P. Formalising trust as a computational concept [D]. University of Stirling, Stirling, 1994.
- [2] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management[C]//17th Symposium on Security and Privacy. IEEE Computer Society Press. c1996: 164-173.
- [3] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open network[C]//European Symposium on Research in Security (ESORICS). Springer-Verlag, c1994: 3-18.
- [4] JØSANG A, ISMAIL R, BOYD C. A survey of trust and reputation systems for online service provision[J]. Decision Support Systems, 2007, 43(2): 618-644.
- [5] JØSANG A, KNAPSKOG S J. A metric for trusted systems[C]//Austrian Computer Society. c1998: 541-549 .
- [6] KAMVAR S. The EigenTrust algorithm for reputation management in P2P networks[C]//12th International World Wide Web Conference. c2003: 640-651.
- [7] ZHOU R F, KAI H W. PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing[J]. IEEE Transaction on Parallel and Distributed Systems, 2007, 18(4): 460-473.
- [8] SU Z, LIU L, LI M, et al. ServiceTrust : trust management in service provision networks[C]//10th International Conference on Services Computing. c2013: 272-279.

- [9] XIONG L, LIU L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities [J]. IEEE Transactions on Knowledge Data Engineering, 2004, 16(7): 843-857.
- [10] HUYNH T D, JENNINGS N R, SHADBOLT N R. An integrated trust and reputation model for open multi-agent systems[J]. Autonomous Agents and Multi-Agent Systems, 2006, 13 (2): 119-154.
- [11] FAN W, YANG S, PERROS H, et al. A multi-dimensional trust-aware cloud service selection mechanism based on evidential reasoning approach[J]. International Journal of Automation and Computing, 2015, 12(2): 208-219.
- [12] ASHTIANI M, AZGOMI M A. A formulation of computational trust based on quantum decision theory[C]//Information System Frontiers. Springer US, c2015: 1-30.
- [13] 田春岐, 邹仕洪, 田慧蓉, 等. 一种基于信誉和风险评价的分布式 P2P 信任模型[J]. 电子与信息学报, 2007, 29(7): 1628-1632.
TIAN C Q, ZOU S H, Tian H R, et al. A new trust model based on reputation and risk evaluation for P2P networks[J]. Journal of Electronics & Information Technology, 2007, 29(7): 1628-1632.
- [14] 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): 405-415.
LI X Y, GUI X L. Trust quantitative model with multiple decision factors in trusted network[J]. Chinese Journal of Computers, 2009, 32(3): 405-415.
- [15] 甘早斌, 丁倩, 李开, 等. 基于声誉的多维度信任计算算法. 软件学报, 2011, 22(10): 2401-2411.
GAN Z B, DING Q, LI K, et al. Reputation-based multi-dimensional trust algorithm[J]. Journal of Software, 2011, 22(10): 2401-2411.
- [16] 李峰, 申利民, 司亚利, 等. 基于交互感知的动态自适应的信任评估模型[J]. 通信学报, 2012, 33(10): 60-70.
LI F, SHEN L M, SI Y L, et al. Dynamic adaptive trust evaluation model based on interaction-aware[J]. Journal on Communications, 2012, 33(10): 60-70.
- [17] 汪京培, 孙斌, 钮心忻, 等. 基于参数建模的分布式信任模型. 通信学报, 2013, 34(4): 47-59.
WANG J P, SUN B, NIU X X, et al. Distributed trust model based on parameter modeling[J]. Journal on Communications, 2013, 34(4): 47-59.
- [18] 李乔, 何慧, 方滨兴, 等. 基于信任的网络群体异常行为发现[J]. 计算机学报, 2014, 37(1): 1-14.
LI Q, HE H, FANG B X, et al. Awareness of the network group anomalous behaviors based on network trust [J]. Chinese Journal of Computers, 2014, 37(1): 1-14.

作者简介:



刘义春 (1965-), 男, 湖南华容人, 博士, 广东财经大学副研究员, 主要研究方向为信息安全与信任计算。

梁英宏 (1978-), 男, 安徽蚌埠人, 博士, 广东财经大学副研究员, 主要研究方向为智能计算与电子商务。