软件学报 ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*,2012,23(12):3187−3197 [doi: 10.3724/SP.J.1001.2012.04180]

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

# 一种角色分离的信任评估模型*

周国强[1,2,3], 曾庆凯[1,2+]

[1](计算机软件新技术国家重点实验室(南京大学),江苏 南京 210093)

[2](南京大学 计算机科学与技术系,江苏 南京 210093)

[3](南京邮电大学 计算机学院,江苏 南京 210003)

## Trust Evaluation Model Based on Role Separation

ZHOU Guo-Qiang[1,2,3], ZENG Qing-Kai[1,2+]

[1](State Key Laboratory for Novel Software Technology (Nanjing University), Nanjing 210093, China)

[2](Department of Computer Science and Technology, Nanjing University, Nanjing 210093, China)

[3](College of Computer Science, Nanjing University of Posts and Telecommunication, Nanjing 210003, China)

+ Corresponding author: E-mail: zqk@nju.edu.cn

**Zhou GQ, Zeng QK. Trust evaluation model based on role separation. *Journal of Software*, 2012,23(12): 3187−3197 (in Chinese).** http://www.jos.org.cn/1000-9825/4180.htm

**Abstract**: To address the recommendation problems from malicious entities, a role separation based trust evaluation model (RSTrust) is proposed in this paper. In RSTrust, roles which entities act during trust evaluation are classified into transaction roles and recommendation roles. Trust on entity is therefore described as transaction trust and recommendation trust according to their associated roles, which leads to the separation of interference between different roles on different trusts. During the calculation of the global trust for an entity, the global recommendation trust of a recommender is used as a trust weight in RSTrust, and the disturbance of recommendation from malicious entities on global trust can be eliminated effectively. Analysis and simulation results demonstrate that RSTrust model has the fine feature of anti-malicious recommendation and good astringency.

**Key words**: peer-to-peer; trust model; recommendation trust; role separation

**摘 要**: 针对实体恶意推荐问题,提出了一种角色分离的信任评估模型(RSTrust).模型将实体在信任评估中承担的角色分为交易角色和推荐角色两类,分别用交易信任度和推荐信任度来描述其可信性,区分不同角色对实体不同信任度的影响;在计算实体全局信任度时,RSTrust 将推荐者的全局推荐信任度作为其推荐证据的可信权重,消除恶意推荐对全局信任度计算的干扰.分析和仿真结果表明,模型具有良好的抗恶意推荐能力和收敛性.

**关键词**: 对等网络;信任模型;推荐信任;角色分离

**中图法分类号**: TP393 **文献标识码**: A

由于 P2P 系统具有开放性和匿名性的特点,恶意实体和服务可以随意进入系统,从而导致大量的安全问题.

* 基金项目: 国家自然科学基金(61170070, 90818022, 61021062); 国家科技支撑计划(2012BAK26B01); 高等学校博士学科点专项科研基金(200802840002); 江苏省科技支撑计划(BE2010032)

收稿时间: 2011-04-11; 修改时间: 2011-10-08; 定稿时间: 2011-12-31

信任模型可为 P2P 网络环境下实体服务的正常运行提供可信支持.

现有的信任模型通过实体间的交易历史来预测实体的未来行为[1−10],根据交易历史给出信任度,评估与其交易的风险性,因此对恶意实体有一定的抑制作用.然而,这些模型中实体的信任度通常不反映其推荐历史,实体在信任反馈时存在散布虚假、伪劣的信息,甚至恶意推荐[11]的可能.因此,现有的信任模型通过信任度无法有效隔离恶意推荐实体,使得推荐信任关系难以保证.

为消除恶意推荐给 P2P 系统带来的安全隐患,本文提出了一种角色分离的信任评估模型(a trust evaluation model based on role separation,简称 RSTrust).针对系统可能存在的灰色实体(即交易行为和推荐行为不一致的实体),用交易角色和推荐角色对实体进行刻画,实体扮演的角色构成评估粒度,系统可以根据角色对实体进行评估、选择和隔离;模型认为互相有直接交易历史的实体才可生成原始推荐证据;推荐者的全局推荐信任度决定其推荐证据的可信程度,不同推荐者的推荐证据共同确定被推荐实体的全局信任度;实体全局推荐信任度由实体的推荐行为决定且不受交易行为的影响,避免实体交易行为和推荐行为互相干扰.通过与典型的信任模型对比分析表明,RSTrust 比其他模型有更强的抗恶意推荐能力.

## 1 相关研究

在线交易平台 eBay 的信誉管理系统使用交易完成后买家和卖家互相评分界定双方信誉,参与者的全局信任度为其他用户对其最近 6 个月的评分之和,淘宝网也采用类似的交易评价系统.此类信誉管理系统以实体的评价信息构成推荐证据,比如在 P2P 文件共享系统中,实体 $i$ 从实体 $j$ 中下载文件后,它可以给出对这次交易的评价:正面评价、负面评价或介于正面和负面之间的其他评价.

现有的信任评估模型对于恶意推荐实体的处理方式大致分为无防范、推荐证据过滤和推荐反馈等 3 类.

(1) 无防范型模型.交易信任度高的实体其推荐行为信任度也高,且用单值信任度表示实体的安全属性.如:eBay,Amazon 计算所有评价(包含正面和负面)的平均值作为实体的信誉值[11];文献[12]根据评价交易行为的多维历史向量的融合作为实体的信任值;文献[13−15]根据实体间的交易结果建立概率模型来估测实体的可信度,认为发布评价意见的实体其推荐默认可信.EigenTrust[16],PowerTrust[17]模型将实体的推荐行为作为一个重要因素纳入到实体信任值的计算中,利用信任的传递特性,由实体的本地信任值计算全局信任值.然而,实体信任度均由实体间直接交易历史确定而不是推荐历史.都认为信任度越高的实体其推荐行为的信任度也高,因此在计算实体全局信任度时赋予较大权重,没有考虑到恶意推荐对信任度的影响;另外,对实体间的交易频度没有关注,导致恶意实体可以用少量的交易次数获得较高的信任度.

(2) 证据过滤型模型通过实体间协作对推荐证据进行分析,从而过滤掉恶意推荐.Douwen 模型[11]将不同时间段内过于夸张或者诋毁的推荐证据视为恶意推荐证据而不予采纳.文献[18]通过分析某证据与其他证据间一致性程度确定噪音信息.文献[19]用行程编码压缩被推荐实体的行为轨迹作为推荐证据进行排序,将推荐力度最强和最弱的和一个时间周期内推荐频度过高的推荐视为恶意推荐.以上模型均通过事先局部单纯对推荐证据进行分析从而判定恶意推荐证据,对抑制离谱的恶意推荐具有一定的效果,但对恶意推荐实体没有惩罚机制而让其留在网络中继续发挥作用;同时,对实体恶意推荐行为信息不提供网络共享机制,不认为恶意推荐是实体的一个恶劣品质;另外,在分布环境中,各个档案实体的局部评价标准难以统一.

(3) 推荐惩罚型模型将推荐行为反馈作为惩罚因素修正实体的信任度,多次恶意推荐积累的惩罚可以导致实体信任度降低,从而被系统视为恶意实体进行隔离.文献[3,20,21]通过反馈来计算推荐实体的直接交易信任度,利用两实体对相同交易实体的评价的相似性计算实体评价的可信度,两个节点评价越相似、交易量越频繁,则对方的评价信息越可信.文献[22,23]也提出了相似度的观点,但不是为了度量实体推荐可信度,而是识别恶意服务实体(团队).尽管反馈惩罚型信任模型可以在一定程度上防范恶意推荐行为,但通过推荐反馈来修正实体的服务信任度,对于那些灰色实体(如善意服务、恶意推荐)有误伤的可能,其实质还是将交易信任度看成推荐信任度,混淆了实体的交易角色和推荐角色.

本文认为,现有评估模型的问题主要源于忽略了交易和推荐的区别,计算实体信任度时采用的方法过于简

单.虽然在非黑即白实体占据多数的网络环境中此类评估模型可发挥一定作用,但在灰色实体(即服务和推荐不一致的实体)具有一定数目的环境中,现有评估模型显现出两个缺陷:一是未将实体推荐行为作为独立的安全属性进行评估.由于交易和推荐性质完全不同,交易可信度只取决于实体自身的表现,而推荐可信度同时还取决于被推荐实体的表现,决定评价指标的主体不完全一样;另一个是推荐信息融合的方法不准确.在实体全局信任度的迭代计算中,灰色实体的交易可信度可能对推荐可信度造成计算上的干扰,实体的交易和推荐不一定存在必然的联系,实体的恶意推荐可以通过大量直接交易积累较高的信任度而被其他实体采信.因此,将实体的"推荐"与"交易"属性分离,对实体的推荐行为进行独立评估,从而确定恶意推荐实体并拒绝其推荐.在此基础上构建的基于推荐的信任模型,将具有较强的抗恶意推荐能力.

因此,RSTrust 模型在计算一个实体全局信任度时,考虑了以下 3 个方面:

(1) 只有与实体有直接交易历史的实体才能生成本地推荐证据,对多个推荐证据进行融合才能形成实体的全局信任度,而推荐证据的可信程度取决于推荐者的全局推荐信任度;

(2) 在计算实体全局信任度时,对推荐路径中的实体,根据它们扮演的角色而相应地采信它们本地交易信任度或本地推荐信任度;

(3) 实体的全局推荐可信度由推荐者的本地推荐信任度和全局推荐信任度决定.

本文提出的角色分离的信任评估方法不但可操作性强,还具有高效的遏制各种类型恶意实体的能力.

## 2 角色分离的信任评估模型(RSTrust)

P2P 网络是一组互相协作、共享资源的实体构成的集合[24],其中,实体扮演交易和推荐两种角色.在 RSTrust 模型中,当一个实体请求交易时,在响应实体中选择一个全局交易信任度最高的实体进行交易,交易完成之后,请求者将评价信息保存在响应者的档案实体中,计算响应者的本地交易信任度;同时,由于请求者进行评价之后,作为推荐者,其推荐证据已经更新,因此所有接受过其推荐的实体需要重新计算推荐者的本地推荐信任度,计算结果保存在推荐者的档案实体中.实体的本地信任度和全局信任度由其档案实体计算和存储,在计算过程中隔离信任度低于阈值的实体活动.这就是 RSTrust 模型的基本思想.

在 RSTrust 中,实体均持有一个与它有交易历史的实体的本地交易信任度,这些实体是其交易实体的潜在推荐者;一个实体作为推荐者,将其对另一实体的本地交易信任度作为推荐证据向网络推荐,而推荐证据的权值由推荐者的全局推荐信任度确定.

### 2.1 相关概念

**定义 1(本地交易、推荐信任度)**. 描述实体对目标实体能够正确执行交易、推荐角色行为的认可程度,是历史经验的总结,具有本地特征,包括本地交易信任度和本地推荐信任度.

实体 $i$ 对 $j$ 的本地交易信任度(local transaction trust degree,简称 LTD)和本地推荐信任度(local recommendation trust degree,简称 LRD)可分别记为 $LTD_{ij}$ 和 $LRD_{ij}$,反映他们之间的协作历史[9−11]和推荐历史,与交易成功率和交易频度有关,交易频度决定了实体之间的熟悉程度.

**定义 2(全局交易、推荐信任度)**. 在全网的角度对实体交易行为或推荐行为的评价,反映了实体被一个实体群所广泛认同的交易、推荐行为的可信程度,具有全局特征,包括全局交易信任度或全局推荐信任度.

实体 $i$ 的全局交易信任度(gloab transaction trust degree,简称 GTD)和全局推荐信任度(gloab recommendation trust degree,简称 GRD)可分别记为 $GTD_i$,$GRD_i$,反映全网实体对 $i$ 的交易行为和推荐行为的评价.

### 2.2 本地交易信任度

#### 2.2.1 交易满意度(TSD)

**定义 3(交易满意度)**. 分布网络中两实体发生一次交易活动后,申请者对服务提供者进行评价的结果为交易满意度.

实体 $i$ 对 $j$ 的交易满意度(transaction satisfied degree)可记为 $TSD_{ij}$, 一种简单有效且被大家认可的方式是 $i$

根据交易情况进行打分.因此,$TSD_{ij}$ 的计算模型为

$$TSD_{ij}=\begin{cases}1, & \text{totally satisfactory}\\ -1, & \text{totally unsatisfactory}\\ \alpha(\in(-1,1)), & \text{else}\end{cases} \tag{1}$$

实体 $i$ 根据 $j$ 的服务质量对其进行评价,1 表示完全满意,0 表示完全不满意,$\alpha$介于满意与不满意之间.值越大,表示满意度越高,从而区分 $j$ 提供的不同服务质量.

2.2.2 本地交易信任度(LTD)

本文采用的方式是将实体 $i$ 对 $j$ 的每次交易满意度进行融合,从而得到 $j$ 的本地交易信任度 $LTD_{ij}$;但在对交易满意度进行融合时进行平均化处理,否则,恶意实体可以通过积累大量不太成功的交易而获得较高本地交易信任度,从而引发安全问题.因此,本地交易信任度 $LTD_{ij}$ 计算模型为

$$LTD_{ij}=\begin{cases}\dfrac{\sum_{k=1}^{m}TSD_{ij}}{m}\times\beta^{\frac{1}{m}}, & m\neq 0\cap\sum_{k=1}^{m}TSD_{ij}>0\\ 0, & \text{else}\end{cases} \tag{2}$$

其中,$m$ 表示 $i$ 与 $j$ 交易的总次数,$\beta\in[0,1]$为熟悉因子.

当 $m$=0 时,实体 $j$,$i$ 之间没有交易历史,互相不熟悉,故将 $LTD_{ij}$ 记为 0;另外,当 $\sum_{k=1}^{m}TSD_{ij}$ <0,说明 $j$,$i$ 之间交易满意度非常低,这种情况下,$LTD_{ij}$ 可记为 0.

尽管 $\dfrac{\sum_{k=1}^{m}TSD_{ij}}{m}$ 避免了累积较低交易满意度引发的安全问题,但实体间熟悉程度受他们之间交易次数的影响,次数越多说明他们之间越熟悉,给出的本地信任度值就越可信,因此,熟悉因子$\beta$根据 $i$,$j$ 之间的交易次数修正本地交易信任度.

实体 $i$ 对 $j$ 的本地交易信任度 $LTD_{ij}$ 一方面反映 $i$ 对与 $j$ 交易历史的评价,另一方面以此为据向其他网络实体推荐 $j$.因此,$LTD_{ij}$ 可作为评价 $j$ 的交易行为和 $i$ 的推荐行为的依据.

### 2.3 推荐信任度

2.3.1 本地推荐信任度(LRD)

本文认为,可用实体的推荐历史来预测未来推荐的可信程度.本地交易信任度 $LTD_{ij}$ 反映实体 $i$ 对与 $j$ 历史交易行为的评价,因此可将 $LTD_{ij}$ 看成实体 $i$ 推荐 $j$ 的证据;$LTD_{kj}$ 为 $k$ 对实体 $j$ 的本地交易信任度,实体 $k$ 可以通过与 $j$ 的交易情况来评估 $i$ 推荐 $j$ 的可信性.可将两实体对共同发生过交易活动实体的评价吻合程度来描述推荐满意度.

**定义 4(推荐满意度)**. 实体 $k$ 关于 $j$ 的本地交易信任度 $LTD_{kj}$ 与实体 $i$ 关于 $j$ 的推荐证据 $LTD_{ij}$ 的吻合程度,为 $k$ 对 $i$ 推荐 $j$ 的满意度(recommendation satisfied degree),记为 $RSD_k^{i\to j}$,其计算模型为

$$RSD_k^{i\to j}=\begin{cases}\dfrac{LTD_{ij}}{LTD_{kj}}, & LTD_{kj}\geqslant LTD_{ij}\\ \dfrac{LTD_{kj}}{LTD_{ij}}, & \text{else}\end{cases} \tag{3}$$

实体 $i$ 向 $k$ 夸大推荐($LTD_{ij}\geqslant LTD_{kj}$)和诋毁推荐($LTD_{kj}\geqslant LTD_{ij}$)实体 $j$ 均影响吻合度,式(3)的 $RSD_k^{i\to j}$ 值介于 0 与 1 之间,保证了 $i$ 的夸张和诋毁推荐导致吻合度同向减小.吻合度高,说明实体 $k$ 对 $i$ 推荐 $j$ 满意,反之不满意.

由于实体 $i$ 存在向 $k$ 推荐多个实体的可能,因此可将 $i$ 向 $k$ 多次推荐的推荐满意度进行融合,从而得到 $k$ 关于 $i$ 的推荐信任度 $LRD_{ki}$.另外,会存在恶意推荐实体通过大量质量不高的推荐反而可获取较高的推荐信任度的现象,从而引发安全问题.因此,结合这两方面问题的考虑,本地推荐信任度 $LRD_{ki}$ 计算模型为

$$LRD_{ki}=\begin{cases}\dfrac{\sum\limits_{j\in JSet(i,k)}RSD_k^{i\to j}}{|JSet(i,k)|}, & JSet(i,k)\neq\varnothing\\ 0, & \text{else}\end{cases} \tag{4}$$

实体 $i$ 向 $k$ 推荐其他实体个数的集合为 $JSet(i,k)$,$|JSet(i,k)|$为集合的势,当 $JSet(i,k)$为∅时,说明 $i$ 没有向 $k$ 推荐的历史,所以将 $LRD_{ki}$ 定义为 0.

2.3.2 全局推荐信任度(GRD)

全局推荐信任度 $GRD_i$ 指网络实体 $i$ 被一个实体群所广泛认同的推荐能力.因此,网络 $N$ 中任意实体 $i$ 的 $GRD_i$ 由每个接受过 $i$ 推荐的实体 $p$ 决定,实体 $p$ 发表对 $i$ 推荐行为的评价 $LRD_{pi}$,实体 $p$ 评价的可信程度由其全局推荐信任度决定,因此 $LRD_{pi}$ 的权值为 $GRD_p$.实体 $i$ 的全局推荐信任度计算模型为

$$GRD_i=\frac{\sum\limits_{p\in P\wedge GRD_p\geqslant\alpha}(GRD_p\times LRD_{pi})}{|P|} \tag{5}$$

其中,$P$ 为接受过 $i$ 推荐的实体集合,集合中实体个数记为$|P|$;$\alpha$为阈值,当某一实体 $p$ 的 $GRD_p$ 小于它时,那么 $p$ 的推荐为恶意推荐,拒绝其推荐从而消除恶意推荐的影响;当 $p\in p\wedge GRD_p\geqslant\alpha$,实体 $p$ 对 $i$ 的推荐被系统认可,其推荐的可信权值为 $GRD_p$.

设全局推荐信任度向量 $\boldsymbol{GRD}=[GRD_1,GRD_2,\ldots,GRD_n]^T$,则称公式(5)的矩阵形式:

$$\boldsymbol{GRD}=\boldsymbol{R}\times\boldsymbol{GRD} \tag{6}$$

为网络 $N$ 关于推荐信任关系矩阵 $\boldsymbol{R}$ 的信任方程.由公式(6)和推荐信任度定义以及迭代收敛性,可以保证 $0\leqslant GRD_i\leqslant 1$.其中,$\boldsymbol{R}$ 定义为本地推荐信任度矩阵,矩阵元素为 $R_{ij}=LRD_{ij}\big/|P|$.

### 2.4 全局交易信任度(GTD)

全局交易信任度描述网络对候选实体能够正确执行角色行为的判断,基于历史协作经验给出的评价为全局属性.只有与候选实体交易过的实体才可以发表评价形成推荐证据,全局推荐信任度为其推荐证据权重.另外,为了避免累积现象,将平均化推荐者的推荐证据.

因此,候选实体 $i$ 的全局交易信任度 $GTD_i$ 的计算模型为

$$GTD_i=\frac{\sum\limits_{m\in P\vee m\neq i\wedge GRD_m\geqslant\alpha}(LTD_{mi}\times GRD_m)}{|P|} \tag{7}$$

其中,$\boldsymbol{P}$ 为与实体 $i$ 有直接交易历史的实体集合;$LTD_{mi}$ 为 $m$ 关于 $i$ 的本地交易信任度,形成 $m$ 推荐 $i$ 的证据;$GRD_m$ 为 $m$ 的全局推荐信任度,作为推荐权重.全局推荐信任度低于$\alpha$的实体的推荐行为为恶意,所以当 $GRD_m<\alpha$时,拒绝其推荐,计算 $GTD_i$ 过程中进行了剥离.

### 2.5 算法性质

**定理 1(收敛性)**. 对于 $N$ 个实体的全局推荐信任度构成的向量 $\boldsymbol{GRD}$,初始 $\boldsymbol{GRD}^{(0)}$为任意值,基于公式(6)的 $\boldsymbol{GRD}^{(k+1)}=\boldsymbol{R}^T\times\boldsymbol{GRD}^{(k)}$简单迭代方法收敛.

证明:定理 1 迭代收敛的充分条件是矩阵 $\boldsymbol{R}^T$ 的范数$\|\boldsymbol{R}^T\|<1$.因为范数

$$\|\boldsymbol{R}^T\|=\max_i\sum_{p\in P}\left|\frac{LRD_{pi}}{|P|}\right|<\frac{\sum\limits_{p\in P}\max\limits_i|LRD_{pi}|}{|p|} \tag{8}$$

由公式(4)和 $RSD_p^{i\to j}<1$可知,

$$\max_{p,i}|LRD_{pi}|=\max_{p,i}\left|\frac{\sum\limits_{j\in JSet(i,p)}RSD_p^{i\to j}}{|JSet(i,p)|}\right|<\max_{p,i}\left|\frac{|JSet(i,p)|}{|JSet(i,p)|}\right|<1 \tag{9}$$

因为|p|值为集合 P 节的元素个数,因此由公式(9)可得

$$\sum_{p\in P}\max_{i}|LRD_{pi}|<|p| \tag{10}$$

由公式(8)、公式(10)可得$\|\boldsymbol{R}^T\|<1$. □

## 3 仿真和分析

仿真主要考察 RSTrust 抵御恶意推荐实体的能力.仿真实验的背景为 P2P 网络的文件下载服务,当实体发起请求后,从响应实体中选择一个进行文件下载,直到下载了有效文件或者失败,一个查询周期结束,并进行数据收集.根据场景我们设计了以下几类实体,即:

(1) 善意实体(G).这类实体服务和推荐都是真实的,称为 GoodNode,记为 G 类;
(2) 恶意实体(M).这类实体服务和推荐都是不真实的,称为 MaliciousNode,记为 M 类;
(3) 恶意服务实体(MS).这类实体只提供不真实的下载服务,但推荐都是真实的,称为 Malicious Service Node,记为 MS 类;
(4) 恶意推荐实体(MR).这类实体提供真实的下载服务,但推荐存在欺诈行为,分为诋毁推荐(DMR)和夸大推荐(MMR),诋毁所有与之交易的善意实体,夸大所有与之交易的恶意实体,称为 Malicious Recommence Node,记为 MR 类;
(5) 协同恶意实体(CM).这类实体形成协同作弊的小团伙,对内提供真实服务,对外提供不真实服务;且夸大推荐同伙,诋毁非团伙实体,称为 Collusive Malicious,记为 CM 类.

在仿真过程中,实体交易目标是选择一个自己不持有的文件进行下载,交易成功使得该用户拥有该文件,失败的交易不会增加该用户拥有的文件.最终的评估标准用整个网络成功交易的次数占整个交易次数的比例(successful service percentage,简称 SSP)表示.

我们选择典型的 EigenTrust 和 FCTrust 信任评估模型作为参照,与本文提出的 RSTrust 模型进行比较,评价他们在抗恶意推荐行为方面的性能差异.其中:EigenTrust 模型中的信任度不反映其推荐行为善恶性;FCTrust 模型中通过反馈因子修正信任度,从而反映其推荐行为善恶性.

### 3.1 实验设置

仿真网络环境为:实体既是文件持有者能贡献自身存储的文件资源供其他实体下载,又是文件的申请者.申请者从其他实体下载完成后发表对这次交易的评价.实体总数为 $n$ 个,文件被切割成 $m$ 个子块存放在 $n$ 个实体中.其中,恶意实体的比例为 $r_m$,实体互相熟悉的实体不超过 $r_a$,每个实体持有子块的数目随机,但每个实体至少有一个文件子块,至少每个文件子块有一个拷贝在善意实体中.新加入实体被选中的概率为 $p$,每个用户在整个仿真过程中必须完成 $k$ 次交易(下载 $k$ 次),每次交易用户申请其没有的文件子块.

在基本实验参数设置为 $n$=1000,$m$=10000,$k$=100,$r_m\in$[0,0.5],$r_a$=0.05,$p$=0.1 的情况下,我们对比了在 M 类、MS 类、CM 类和混合模式这 4 种场景下,RSTrust,EigenTrust 和 FCTrust 这 3 种信任模型成功交易率 SSP 情况.

### 3.2 抗恶意推荐测试

#### 3.2.1 M 类仿真

M 类仿真是指网络中恶意实体均是 M 类.

由图 1 可见:与 EigenTrust 和 FCTrust 模型相比,在系统没有恶意实体的时候($r_m$=0),SSP 都可以达到接近 100%;当恶意实体规模不大的时候($r_m$<10%),我们的模型与 EigenTrust 和 FCTrust 效果相当;但随着 $r_m$ 增大,EigenTrust 和 FCTrust 曲线下降得比 RSTrust 模型要快.由于 EigenTrust 模型假设了一个亚可信实体集合,当恶意实体规模不大时,可以稀释恶意推荐的影响,从而减少选择的盲目性;FCTrust 考虑了推荐反馈意见对信任度的影响,所以随着 $r_m$ 变大,交易成功率下降得比 EigenTrust 慢.然而,FCTrust 用反馈因子用乘关系修正实体信任度,因此交易或推荐行为都对实体信任度产生影响,这两方面影响了交易成功率.

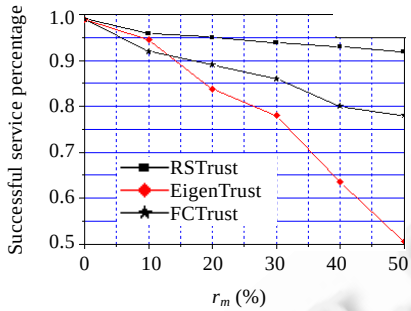



Fig.1 At different scale of M entities, the ratio to ideal case on successful service

图 1 不同规模 M 类恶意实体下,与理想情况的成功交易比

3.2.2 MS 类仿真

MS 类仿真是指网络中实体均是 MS 类.

在网络中只存在 MS 实体的情况下,由于不存在恶意推荐,所以从理论上来说,RSTrust 模型交易成功率应该为 100%;但是由于某些持有子文件的实体可能为新实体,只能被系统随机选中,因此从图 2 中可以看出,随着 $r_m$ 的增大,本模型的 SSP 略有下降.

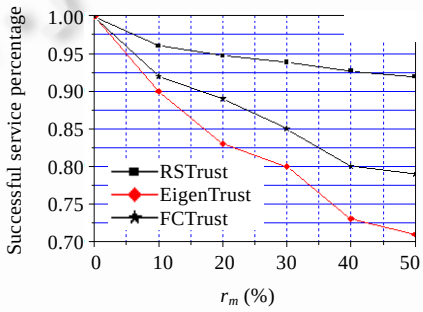



Fig.2 At different scale of MS entities, the ratio to ideal case on successful service

图 2 不同规模 MS 类恶意实体下,与理想情况的成功交易比

对于 FCTrust 模型来说,它的反馈因子等于 1,近似等同于 EigenTrust 模型.从图 2 可以看出,当 $r_m$=0 时,交易成功率接近 100%.随着 MS 类实体的增多,EigenTrust 和 FCTrust 几乎以近似斜率下降.由于 EigenTrust 和 FCTrust 模型将实体交易信任度看成推荐信任度,在一个不存在恶意推荐行为的网络环境中,强行制造出一个存在恶意推荐的氛围.

3.2.3 CM 类仿真

CM 类仿真是指网络中实体均为 CM 类.

随着 $r_m$ 的增大,互相吹捧的实体增多,恶意实体可以容易获取较高的信任度,所以 RSTrust 模型刚开始的时候交易成功率有点波动.随着交易的次数增多,恶意推荐实体的恶意推荐行为逐步曝光,进而给予惩罚,所以当恶意团体数目到达 50%时,SSP 仍能达到 91%;由于 EigenTrust 一方面将实体的推荐和交易行为不加区分,另外还缺乏惩罚机制,从而造成系统交易成功率下降;而 FCTrust 尽管有推荐反馈因子修正实体信任度,但由于将信任度等同于推荐信任度,导致恶意推荐实体的推荐行为最终影响交易信任度,SSP 随着团队规模的扩大而下降(如图 3 所示).

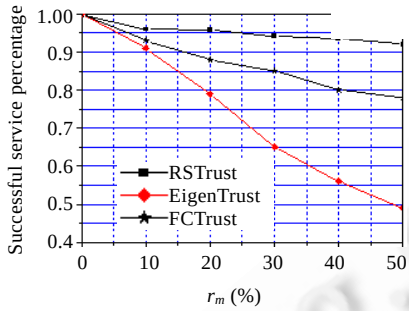
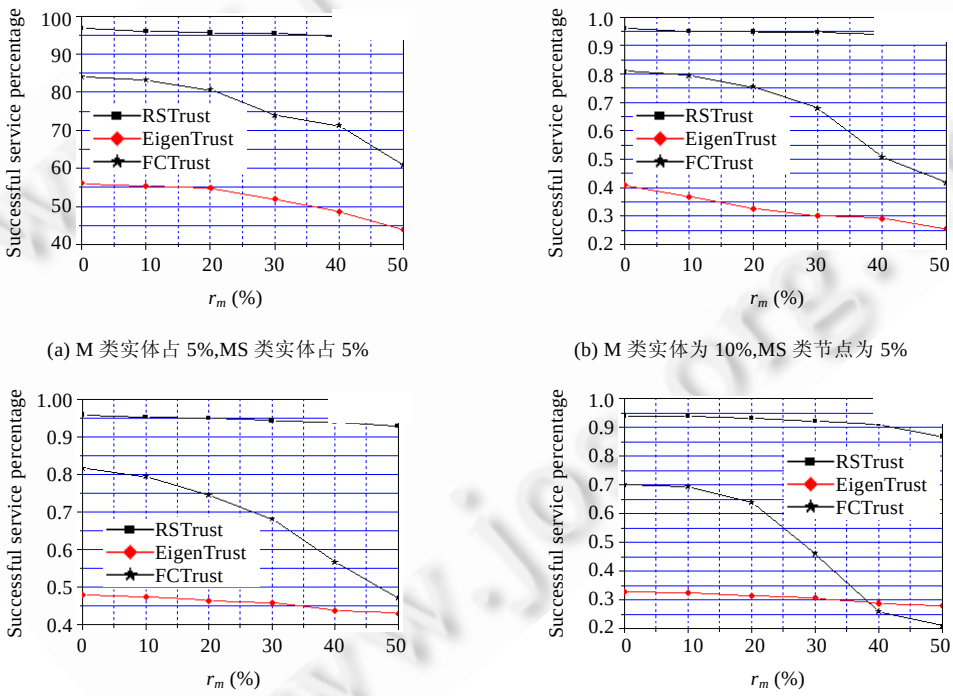



Fig.3 At different scale of CM entitiesthe ratio to ideal case on successful service

图 3 不同规模 CM 类恶意实体下,与理想情况的成功交易比

3.2.4 混杂模式

混合模式仿真是指网络中均存在 M 类、MS 类、MR 类实体.该类实验主要是检验各种恶意实体按照一定比例以混杂的方式存在于网络中时对 RSTrust 的影响.首先,分别按图 4(a)~图 4(d)所示用标注的 M 类与 MS 类实体比例初始化网络,再观察 SSP 随 MR 类实体规模变化的规律.




(a) M 类实体占 5%,MS 类实体占 5%

(b) M 类实体为 10%,MS 类节点为 5%

(c) M 类实体为 5%,MS 类节点为 10%

(d) M 类实体为 15%,MS 类节点为 10%

Fig.4 At different scale of MR, MS, M entities, the ratio to ideal case on successful service

图 4 不同规模 M 类、MS 类、MR 类恶意实体下,与理想情况的成功交易比

从图 4 可以看出,由于 M 类实体的存在,当 $r_m$=0 时,RSTrust 在图 4(a)和图 4(c)中的 SSP 基本相同接近 96%,图 4(b)中的 95.3%和图 4(d)中的 94%;随着 $r_m$ 的增大,SSP 略有下降,在图 4(d)中下降最厉害的 SSP 也达到 86%.EigenTrust 由于对恶意推荐毫无防范性,当 $r_m$=0 时,由于网络中存在 M 类实体,导致 SSP 不高.由于 FCTrust 用推荐反馈因子修正实体信任度,所以当 $r_m$ 不大时,对恶意推荐有一定的抑制作用.在图 4(a)和图 4(c)中,$r_m$=0 时,SSP

都在 80%左右;在图 4(b)和图 4(d)中,由于 M 类实体较多,SSP 跌到 70%左右;随着 $r_m$ 的增大,下降程度较大.

上述实验在多个场景中验证了 RSTrust 抗实体恶意推荐行为的有效性.

RSTrust 的有效性源于以下两个原因:

(1) 信任数据表征的合理性.推荐和交易是实体的两种不同行为,体现实体不同的安全品质.RSTrust 对实体的交易活动和推荐活动分开进行评估,分别用推荐信任度和交易信任度表征实体推荐行为和交易行为的可信程度,因此,评估数据更能准确地反映实体行为的安全性;

(2) 方法的合理性.体现在两个方面:首先,如果实体的全局推荐信任度低于阈值时,就可以拒绝其推荐;其次,当一个实体多次进行恶意推荐,这样会快速导致其他实体对其本地推荐信任度降低,从而全局推荐信任度也会同时降低,低于阈值时,它的推荐行为就随之被隔离.因此,RSTrust 具有较强的抗恶意推荐特点.

### 3.3 RSTrust的优点

在 P2P 系统中,使用 RSTrust 模型有两个方面的优点:

(1) 隔离恶意推荐实体.实体的全局交易信任度融合了多个推荐实体的推荐证据,这些推荐证据中可能存在恶意推荐者的推荐.当一个实体发布请求后,系统可能有多个实体响应,那么它可选择全局交易信任度最大的实体进行交易;交易完成后请求实体对本次交易进行评估,如果评估结果与推荐者的推荐证据不吻合,则会影响推荐者的推荐信任度.如果实体多次进行恶意推荐,那么它的推荐信任度就会降低到阈值以下,从而被系统隔离,从此拒绝它的推荐;

(2) 刺激实体积极推荐.目前,P2P 系统中,许多实体在交易完成后对交易评价不重视,有的随意给个评价,有的在商家的一再请求或者骚扰甚至威胁下给个好评.因此,可以采取一定的激励措施鼓励交易方进行推荐评价.比如,可以用推荐信任度对实体进行排名从而提高被关注度,或者用带宽奖励诚实推荐者等手段刺激用户积极推荐.并且明确告诉系统实体,它的推荐信任度由其推荐行为决定,交易行为对推荐可信度没有直接影响.以前的信任模型没有反映实体推荐行为的数据,所以基于推荐的奖励无法实施,奖励措施有两大好处:一方面鼓励实体积极诚实推荐,可以与其他实体分享它的使用经验,提高整个系统的安全水平;另一方面,刺激那些随意实体改变习惯,交易完成后进行认真推荐.这样,可以让恶意实体曝光的几率增加,有助于净化电子商务环境.

## 4 结 论

本文将实体的交易行为和推荐行为分开进行考虑,提出了一种对角色分别进行评价的抗恶意推荐的信任评估模型 RSTrust.消除了实体的交易行为和推荐行为对不同信任数据的干扰,有助于更准确地界定实体推荐行为的可信性.仿真实验结果表明,模型在遏制广泛类型的恶意推荐以及恶意服务方面有较大的提高.进一步的工作是改进基于角色推荐信任模型的效率,包括研究推荐者个性对推荐证据的影响以及推荐证据的收集方式,同时,开展根据推荐者信息如何选择交易者方法的研究.

**致谢** 在此,我们向本文的审稿人表示感谢,感谢他们对本文提出的深入而有建设性的修改意见.

**References**:

[1] Li YJ, Dai YF. Research on trust mechanism for peer-to-peer network. Chinese Journal of Computers, 2010,33(3):1−18 (in Chinese with English abstract).

[2] Wang Y, Vassileva J. Bayesian network trust model in peer-to-peer networks. In: Moro G, ed. Proc. of the 2nd Int'l Workshop on Agents and Peer-to-Peer Computing. Berlin: Springer-Verlag, 2004. 23−34. [doi: 10.1007/978-3-540-25840-7_3]

[3] Xiong L, Liu L. PeerTrust: Supporting reputation-based trust in peer-to-peer communities. IEEE Trans. on Data and Knowledge Engineering (Special Issue on Peer-to-Peer Based Data Management), 2004,16(7):843−857. [doi: 10.1109/TKDE.2004.1318566]

[4] Jiang SX, Li JZ. A reputation-based trust mechanism for P2P e-commerce systems. Journal of Software, 2007,18(10):2551−2563 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/2551.htm [doi: 10.1360/jos182551]

[5] Zhang Q, Zhang X, Wen XZ, Liu JR, Ting S. Construction of peer-to-peer multiple-grain trust model. Journal of Software, 2006,17(1):96−107 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/96.htm [doi: 10.1360/jos170096]

[6] Tang W, Chen Z. Research of subjective trust management model based on the fuzzy set theory. Journal of Software, 2003,14(8): 1401−1408 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1401.htm

[7] Wang SX, Zhang L, Li HS. Evaluation approach of subjective trust based on cloud model. Journal of Software, 2010,21(6): 1341−1352 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3501.htm [doi: 10.3724/SP.J.1001.2010.03501]

[8] Tian CQ, Jiang JH, Hu ZG, Li F. A novel super-peer based trust model for peer-to-peer networks. Chinese Journal of Computers, 2010,33(2):345−354 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016..2010.00345]

[9] Liu W, Cai JY, He YP. A trustworthiness based ad-hoc secure interoperation method. Journal of Software, 2007,18(8):1958−1967 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/1958.htm [doi: 10.1360/jos181958]

[10] Jin Y, Gu ZM, Gu JG, Zhao HW. Two-Level trust model based on mutual trust in peer-to-peer networks. Journal of Software, 2009,20(7):1909−1920 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3284.htm

[11] Dou W, Wang HM, Jia Y, Zou P. A recommendation-based peer-to-peer trust model. Journal of Software, 2004,15(4):571−583 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/571.htm

[12] Tan ZH, Wang XW, Cheng W, Chang GR, Zhu ZL. A distributed trust model for peer-to-peer networks based on multi-dimension-history vector. Chinese Journal of Computers, 2010,33(9):1725−1735 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2010.01725]

[13] Despotovic Z, Aberer K. Probabilistic prediction of peers' performance in P2P networks. Engineering Applications of Artificial Intelligence, 2005,18(7):771−780. [doi: 10.1016/j.engappai.2005.06.001]

[14] Josang A, Haller J. Dirichlet reputation systems. In: Werner B, ed. Proc. of the 2nd Int'l Conf. on Availability, Reliability and Security Vienna. Los Vaqueros: IEEE Computer Society, 2007. 112−119. [doi: 10.1109/ARES.2007.71]

[15] Xu LF, Hu HF, Sang ZX, Xu FM, Zou DQ. A prestige reporting mechanism based on gray system theory. Journal of Software, 2007,18(7):1730−1737 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/1730.htm [doi: 10.1360/jos181730]

[16] Sepandar DK, Mario TS, Hector GM. The EigenTrust algorithm for reputation management in P2P networks. In: Proc. of the 12th Int'l Conf. on World Wide Web. Budapest: ACM Press, 2003. 640−651. [doi: 10.1145/775152.775242]

[17] Zhou RF, Hwang K. PowerTrust: A robust and scalable reputation system for trusted peer-to-peer computing. IEEE Trans. on Parallel and Distributed Systems, 2007,18(4):460−473. [doi: 10.1109/TPDS.2007.1021]

[18] Tian CQ, Zou SH, Wang WD, Cheng SD. A new trust model based on recommendation evidence for P2P networks. Chinese Journal of Computers, 2008,31(2):270−281 (in Chinese with English abstract).

[19] Fang Q, Ji Y, Wu GX, Zhao SH, Wu P. Run length coding-based dynamic trust model for P2P network. Journal of Software, 2009,20(6):1602−1616 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3408.htm [doi: 10.3724/SP.J.1001. 2009.03408]

[20] Hu JL, Wu QY, Zhou B, Liu JH. Robust feedback credibility-based distributed P2P Trust model. Journal of Software, 2009,20(10):2885−2898 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3554.htm [doi: 10.3724/SP.J.1001. 2009.03554]

[21] Chang JS, Wang HM, Yin G. DyTrust: A time-frame based dynamic trust model for P2P systems. Chinese Journal of Computers, 2006,29(8):1301−1307 (in Chinese with English abstract).

[22] Li JT, Jing YN, Wang XP, Zhang GD. A trust model based on similarity-weighted recommendation for P2P environments. Journal of Software, 2007, 18(1):157−167 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/157.htm [doi: 10.1360/jos180157]

[23] Miao GS, Feng DG, Su PR. Colluding clique detector based on activity similarity in P2P trust model. Journal on Communications, 2009,30(8):9−20 (in Chinese with English abstract).

[24] Peng DS, Lin C, Liu WD. A distributed trust mechanism directly evaluating reputation of nodes. Journal of Softwars, 2008,19(4): 946−955 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/19/946.htm [doi: 10.3724/SP.J.1001.2008.00946]

**附中文参考文献:**

[1] 李勇军,代亚非.对等网络信任机制研究.计算机学报,2010,33(3):1−18.

[4] 姜守旭,李建中.一种 P2P 电子商务系统中基于声誉的信任机制.软件学报,2007,18(10):2551−2563. http://www.jos.org.cn/1000-9825/18/2551.htm [doi: 10.1360/jos182551]

[5] 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.软件学报,2006,17(1):96−107. http://www.jos.org.cn/1000-9825/17/96.htm [doi: 10.1360/jos170096]

[6] 唐文,陈钟.基于模糊集合理论的主观信任管理模型研究.软件学报,2003,14(8):1401−1408. http://www.jos.org.cn/1000-9825/14/1401.htm

[7] 王守信,张莉,李鹤松.一种基于云模型的主观信任评价方法.软件学报,2010,21(6):1341−1352. http://www.jos.org.cn/1000-9825/3501.htm [doi: 10.3724/SP.J.1001.2010.03501]

[8] 田春岐,江建慧,胡志国,李峰.一种基于聚集超级节点的 P2P 网络信任模型.计算机学报,2010,33(2):345−354. [doi: 10.3724/SP.J.1016.2010.00345]

[9] 刘伟,蔡嘉勇,贺也平.一种基于信任度的自组安全互操作方法.软件学报,2007,18(8):1958−1967. http://www.jos.org.cn/1000-9825/18/1958.htm [doi: 10.1360/jos181958]

[10] 金瑜,古志民,顾进广,赵红武.一种对等网中基于相互信任的两层信任模型.软件学报,2009,20(7):1909−1920. http://www.jos.org.cn/1000-9825/3284.htm

[11] 窦文,王怀民,贾焰,邹鹏.构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型.软件学报,2004,15(4):571−583. http://www.jos.org.cn/1000-9825/15/571.htm

[12] 谭振华,王兴伟,程维,常桂然,朱志良.基于多维历史向量的 P2P 分布式信任评价模型.计算机学报,2010,33(9):1725−1735. [doi: 10.3724/SP.J.1016.2010.01725]

[15] 徐兰芳,胡怀飞,桑子夏,徐凤鸣,邹德清.基于灰色系统理论的信誉报告机制.软件学报,2007,18(7):1730−1737. http://www.jos.org.cn/1000-9825/18/1730.htm [doi: 10.1360/jos181730]

[18] 田春岐,邹仕洪,王文东,程时端.一种基于推荐证据的有效抗攻击 P2P 网络信任模型.计算机学报,2008,31(2):270−281.

[19] 方群,吉逸,吴国新,赵生慧,吴鹏.一种基于行程编码的 P2P 网络动态信任模型.软件学报,2009,20(6):1602−1616. http://www.jos.org.cn/1000-9825/3408.htm [doi: 10.3724/SP.J.1001.2009.03408]

[20] 胡建理,吴泉源,周斌,刘家红.一种基于反馈可信度的分布式 P2P 信任模型.软件学报,2009,20(10):2885−2898. http://www.jos.org.cn/1000-9825/3554.htm [doi: 10.3724/SP.J.1001.2009.03554]

[21] 常俊胜,王怀民,尹刚.DyTrust:一种 P2P 系统中基于时间帧的动态信任模型.计算机学报,2006,29(8):1301−1306.

[22] 李景涛,荆一楠,肖晓春,王雪平,张根度.基于相似度加权推荐的 P2P 环境下的信任模型.软件学报,2007,18(1):157−167. http://www.jos.org.cn/1000-9825/18/157.htm [doi: 10.1360/jos180157]

[23] 苗光胜,冯登国,苏璞睿.P2P 信任模型中基于行为相似度的共谋团体识别模型.通信学报,2009,30(8):9−20.

[24] 彭冬生,林闯,刘卫东.一种直接评价节点诚信度的分布式信任机制.软件学报,2008,19(4):946−955. http://www.jos.org.cn/1000-9825/19/946.htm [doi: 10.3724/SP.J.1001.2008.00946]

**周国强**(1968－),男,湖北大冶人,博士生,副教授,CCF 会员,主要研究领域为信息安全,分布计算.

**曾庆凯**(1963－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为信息安全,分布计算.