

基于云模型的信任评估方法研究

张仕斌^{1),2)} 许春香¹⁾

¹⁾(电子科技大学计算机科学与工程学院 成都 611731)

²⁾(成都信息工程学院网络工程学院 成都 610225)

摘 要 复杂的网络环境下存在的随机性、模糊性和不可预测性等不确定性因素给网络交易带来了诸多安全问题,而在网络交易中,信任是交易能够顺利进行的前提和关键.文中以复杂的网络环境为研究背景,通过对复杂的网络环境中信任、信任影响因素及信任机制等问题的研究,引入云模型理论,研究并提出了基于云模型的信任评估方法,实现了信任的定性与定量的转换,客观地反映了信任的随机性、模糊性和不可预测性;为了有效地防止不法分子的信用炒作和欺骗行为,文中提出了特殊属性评价方法和信任惩罚方法.通过仿真实验,验证了文中研究的信任评估方法能够对复杂的网络环境中实体的信任做出合理的评价;通过防信用炒作实验和防周期行骗实验,进一步验证了基于云模型的信任评估方法的可行性和合理性,为复杂的网络环境中信任评估的研究提供了有价值的新思路.

关键词 云模型;信任评估;信任云;综合评判;信任等级

中图法分类号 TP393 DOI号 10.3724/SP.J.1016.2013.00422

Study on the Trust Evaluation Approach Based on Cloud Model

ZHANG Shi-Bin^{1),2)} XU Chun-Xiang¹⁾

¹⁾(School of Computer Science & Engineering, University of Electronic Science and Technology of China, Chengdu 611731)

²⁾(College of Network Engineering, Chengdu University of Information Technology, Chengdu 610225)

Abstract In the complex network environment, there is randomness, fuzziness, and unpredictability and so on, which bring a lot of secure issues to network transactions. The premise and foundation of network transactions is trust. In this paper, taking the complex network environment as the research background, by use of cloud model theory, and through researching trust, the impact factors of trust, trust mechanism and etc., we propose the trust evaluation approach based on cloud model. This trust evaluation approach can implement the conversion between qualitative and quantitative of trusts, which objectively reflect the randomness, fuzziness and unpredictability of the trusts. In order to effectively prevent the credit speculation and fraud behaviors of criminals, the evaluation method of special properties and the method of trust punishment are proposed in this paper. The simulation results confirm that this trust evaluation approach can make a reasonable evaluation of the entities' trust in the complex network environment. The simulating experiment of anti-credit speculation and anti-cycle deception further confirms the feasibility, rationality of the trust evaluation approach. The trust evaluation approach proposed in this paper may provide a new promising method for research of trust evaluation in complex networks environment.

Keywords cloud model; trust evaluation; trust cloud; comprehensive evaluation; trust level

收稿日期:2012-06-30;最终修改稿收到日期:2012-08-13. 本课题得到四川省科技支撑计划项目(13ZC2138)、成都信息工程学院中青年学术带头人科研基金(J201107)和电子科技大学博士后基金(73984)资助. 张仕斌,男,1971年生,博士,教授,主要研究领域为计算机应用技术、信息安全和密码学. E-mail: cuitzsb@cuit.edu.cn. 许春香,女,1965年生,博士,教授,博士生导师,主要研究领域为密码学、信息安全、电子商务安全.

1 引言

当前,复杂开放的互联网存在随机性、模糊性和不可预测性等不确定性因素^[1],而电子商务等应用领域的交易过程就是在这样复杂、开放的网络环境下进行的,它利用了网络平台来完成传统交易的各个环节和过程。同时,由于复杂开放的网络交易环境存在虚拟性、交易非面对面、网上支付等特点,也给网络交易带来了诸多安全隐患问题^[2],这些问题也统称为网络交易风险^[3]。事实上,只有在网络交易双方相互信任的情况下,交易才有可能顺利地进行,所以信任是进行网络交易活动的前提和关键。当前,要做到安全的网络交易,我们面临的是信任、风险等一系列安全问题。但是目前信任与风险评估的研究仍存在许多问题需要解决^[4]。例如,如何合理地信任关系进行形式化描述,如何制定信任评估机制,如何评判可信与否,信任评估系统的设计,使用什么样的信任策略,信任与风险之间的关系,新一代网络的可信融合问题等^[5]。

近些年来,关于信任及评估问题的研究,吸引了国内外众多学者。早在1996年,Blaze等人^[6]首次提出了“信任管理”的思想,开发了第一代信任管理系统PolicyMaker^[7];Khambatti等人^[8]提出了基于角色的信任模型;Winsborough等人^[9]提出了自动信任协商模型;Nejdl等人^[10]提出通过协商来建立信任的PeerTrust模型;唐文等人^[11]提出了一种主观信任管理模型;陈贞翔等人^[12]提出了基于信任的服务评价和选择模型;张兴兰等人^[13]提出了一种自治信任管理模型;田立勤等人^[14]提出了一种用户行为信任评估机制;王良民等人^[15]提出了一种基于信任-信心值的二元组模糊信任评估模型;刘亮等人^[16]提出了基于云计算的服务信任评估模型;樊丽杰等人^[17]提出了基于人类信任机制的移动电子商务信任评估方法。虽然这些模型都部分地解决了在不同背景下信任的建模及评估等问题,提出了相应的信任评估模型、评估方法或评估机制,但这些模型^[6-17]仍存在诸多不足之处,比如:由于复杂的网络环境下的信任具有随机性、模糊性和不可预测性等^[18]不确定性特征,很难精确地加以描述,而以上这些模型大多都使用经典的数学理论(比如概率理论)来表述和度量实体间的信任关系,因此这些模型在对信任的(合理)表述、信任的度量(理论)等方面都还不够完善;而且这些模型也没有解决恶意推荐

对信任评估造成的影响;同时,这些模型还缺少灵活的信任评价机制,无法反映不同实体进行信任评估时所具有的个性特点。

实际上,复杂的网络环境中信任问题需要通过建立可行和合理的信任评估模型来解决,因此信任评估模型在信任研究领域发挥着基础性作用,它需使用一种信任评估方法对复杂的网络环境中的用户信息进行信任评估,以期能够较好地反映复杂的网络环境中的随机性、模糊性和不可预测性^[18]。

基于以上原因,本文借鉴已有的研究工作,并结合作者在文献^[18-21]中的研究成果,以复杂的网络环境为研究背景,通过对复杂的网络环境中信任、信任影响因素及信任机制等问题进行研究,引入云模型理论,研究并提出了一个针对复杂的网络环境的基于云模型的信任评估方法。

2 相关问题的研究

2.1 信任

在网络交易(比如电子商务交易)中,信任是一方认为另一方是可靠的并且能够履行自己的承诺^[22]。只有在交易双方相互信任的情况下,交易才可能顺利地进行下去,所以信任是进行交易活动的前提和关键^[23]。在复杂的网络环境中,实体间的信任可以分为直接信任和推荐信任^[20]。直接信任是两个实体根据以往的经验建立起来的直接信任关系;间接信任是指借助于其它实体的推荐建立起来的间接信任关系。因此,信任具有这样一些特征^[24]:非对称性(如果实体A信任实体B,但并不能得出B也信任A)、主观性(信任是评价者对评价对象的主观上判断)、动态性(信任可能会随着时间、环境或者其它因素的变化而变化)、多维性(实体间的信任与多种属性有联系,比如历史信任值、社会地位、收入水平等)、模糊性和不完全可传递性(实体A信任实体B,并且实体B又信任实体C,但是并不一定可以得出A信任C)。

2.2 影响信任的因素

在复杂的网络环境中有许多不确定因素都会对信任产生一定影响^[25],对用户信任产生影响的主要因素有:

(1) 用户反馈评价

在复杂的网络环境中,实体之间交互后对对方信用的反馈评价(如电子商务交易后对物品的质量、服务等的评价)属于主观评价,如果将此评价作为计

算实体的信任值,也具有主观性.为此,本文在计算实体的信任值时将实体的反馈评价作为参考指标之一.

(2) 历史信任值

在淘宝、拍拍、eBay 等交易网站中,会出现这样的现象:用户积累了一定的信用后,可能开始实施欺骗行为.为了抵制这种欺骗行为,在计算用户信任值时,应该考虑用户历史信任值,这样可以激励用户保持一定的信誉.因此,本文计算实体的信任值时将实体的历史信任值也作为参考指标之一.

(3) 评价人信任值

一般来说,信誉越高的人的评价越有价值,越值得信任.而目前的交易网站都没有考虑评价人的信任值,而是采用简单的加减或求均值的方法来计算用户信任值,这为不法用户采取信用炒作、周期行骗等行为提供了机会.为有效地防范这种欺骗行为,本文将评价人信任值作为计算实体信任值的参考指标之一.

(4) 交易物品的价值

一般来说,商品价值与风险是成正比的,风险是随交易商品价值的增大而增大.但目前交易网站只是简单地采取只要成功交易就增加一定的信任值的方式,信任值的增加只与成功交易次数有关,而与交易商品价值没有关系.这就使得行骗者有机可乘,他们利用成功的小额交易来不断累积信任度;当信任值达到一定程度时,就可以进行行骗.为了有效地防范信用炒作,本文在信任评估中考虑了商品价值对信任增长的影响,将交易物品的价值作为计算实体信任值的参考指标之一.

(5) 评价时间权重

一般来说,信任是随着时间的变化而不断积累的过程,近期的评价要比早期的评价更具有说服力和参考价值.所以本文在评价用户信任值时,考虑了评价时间权重,将评价时间的权重作为计算实体信任值的参考指标之一.

3 基于云模型的信任评估方法

3.1 基于云模型的信任评估的思路

定义 1. 设 $U = \{ (x_1, x_2, \dots, x_m) \}$ 是所研究的论域, T 是与 U 相关联的信任描述值,其中 x_1, x_2, \dots, x_m 为论域中各对象的信任评价属性,对于 T 所描述信任隶属度 $C_T(x_1, x_2, \dots, x_m)$ 是一个具有稳定倾向的随机数,该信任隶属度在论域上的分布称为信任隶属云(简称信任云);每一个元素与其隶

属度的序对 $(x_i, C_T(x_i)) (i = 1, \dots, m)$ 称为信任云滴.

针对目前复杂的网络环境中(如电子商务系统)各信任域中的实际情况,本节借助于云模型理论^[26],通过对各实体的属性或特征等来评价各实体的信任值(信任度),客观地反映了复杂的网络环境中信任的随机性、模糊性和不可预测性等.具体过程(如图 1)如下:

(1) 对信任等级进行划分,利用标准信任云生成器生成信任云.

(2) 根据信任评估的需求,采集实体的有关信息(如实体获得的信任评价、评价者的信任值、实体交互信息等),然后对采集到的数据进行预处理(对各属性的评价数据进行格式化等).

(3) 将描述各属性的信息通过信任属性云逆向生成器生成信任属性云.

(4) 对属性云进行合并得到综合信任云.

(5) 根据相似度计算与评价得到实体的信任等级.

(6) 根据历史信任值与当前信任等级综合评价出最终信任值.

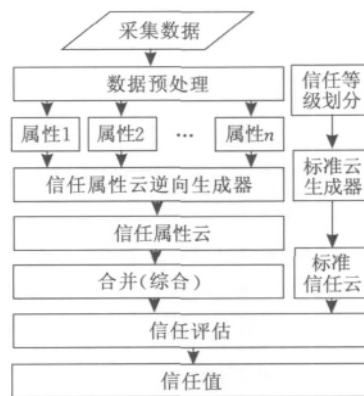


图 1 基于云模型的信任评估的评估过程

3.2 标准信任云生成算法的设计

由于信任等级是建立实体间信任的依据,按照 3.1 节信任评估思想,接下来的工作就是要确定各实体的信任等级,这也是基于云模型的信任评估的关键.

定义 2. 假设系统已预先设定好一系列信任云(供各实体做参考),则每一个信任云称为一个标准信任子云,每一个标准信任子云都有确定的概念,表示相应的信任等级.

假设信任值的取值范围为 $[0, 10]$, 将该区间分为 n 个子区间,其中第 i 个子区间为 $[R_i^{\min}, R_i^{\max}]$, 其

中 R_i^{\min} 和 R_i^{\max} 分别为区间的上限和下限.

算法 1. 标准信任云生成器.

输入: n 个子区间

输出: 标准信任云 $STC_i(Ex_i, En_i, He_i)$, 其中 $i = 1, 2, \dots, n$, Ex_i, En_i, He_i 是标准信任云 STC_i 的期望、熵、超熵^[14]

算法的具体步骤如下:

1. 根据各区间的上下限值, 计算

$$Ex_i = \begin{cases} R_i^{\min}, & i=1 \\ \frac{R_i^{\min} + R_i^{\max}}{2}, & 1 < i < n \\ R_i^{\max}, & i=n \end{cases} \quad (1)$$

2. 根据上一步的计算结果, 计算

$$En_i = \frac{R_i^{\min} + R_i^{\max}}{3} \quad (2)$$

3. 计算 $He_i = \eta$.

η 反映了实体信任值的随机性, 取值不宜过大, 因为 He 越大则 Ex 的误差越大, 信任度的随机性增大, 信任结果难以确定.

建立标准信任云的作用是为了划分信任等级. 在实际应用中, 我们可以根据具体的实际应用情况将信任划分成有限个信任等级; 再根据具体信任等级生成各信任等级对应的信任云.

3.3 信任属性云逆向生成器的设计

定义 3. 设被评价实体共获得 n 个评价, 对应 m 个属性; 若将每个评价作为一个云滴, 根据逆向云生成算法生成 m 个属性的信任云, 则将其称为信任属性云逆向生成器.

由于实体的可信性需重点考查被评价实体的可信性, 而评价的可信程度与评价者的信任等级也有关系. 因此, 为了更合理地处理实体的评价信息, 本节引入加权百分比概念来反应评价的重要性.

定义 4. 某种评价的加权百分比等于每个评价的系数之和除以总评价数, 称之为加权百分比 θ , 即

$$\theta = \frac{\sum_{i=1}^M \lambda_i}{N} \quad (3)$$

其中, N 为总评价数, λ_i 为每个评价的权重 (根据评价方的信任值来确定, 将信任值区间标准格式化到 $[0, 1]$ 上, 以此作为评价的权重). 因为对各个属性的评价是定性分等级, 而每个等级对应的是一个区间, 而非具体的数值. 为了解决这个问题, 我们需要确定某个属性的评价等级, 这个评价等级在特定情况下对应相应的具体数据. 下面引入评价得分值的概念.

定义 5. 设某个属性共有 W 个评价等级, 其

中第 i 等级的评价得分区间为 $[R_i^{\min}, R_i^{\max}]$, R_i^{\min} , R_i^{\max} 分别是该区间的下限和上限, 则该区间的评价得分值记为 α , 计算公式如下:

$$\alpha = R_i^{\min} + \theta \times (R_i^{\max} - R_i^{\min}) \quad (4)$$

在式 (4) 中, 当 $i \geq \frac{W}{2}$ 时, θ 为实体获得的高于或等于 i 级的评价数占总评价数的加权百分比; 当 $i < \frac{W}{2}$ 时, θ 为实体获得的小于 i 级的评价数占总评价数的加权百分比.

比如, 某个属性分为差、中、好 3 个等级, 分别对应 $[0, 4]$ 、 $[4, 6]$ 和 $[6, 10]$ 区间. 若某用户当前共获得 100 个评价 (“差” 30 个、“中” 40 个、“好” 30 个), 假设所有评价的权重均为 1, 则根据式 (4) 计算得到评 “差” 的得分值为 2.8、评 “中” 的得分值为 5.4、评 “好” 的得分值为 7.2, 这就把评价等级做了量化, 从而实现从定性到定量的转换.

根据此方法, 每个实体的评价等级的得分并非固定的, 这也是非常合理的. 但在相同信任等级内的不同实体, 计算出来的信任值也可能是不一样的, 这与他们获得较好的评价有关, 获得的 “好” 评价所占的比例越高, 其得分值就越高.

算法 2. 信任云逆向生成器.

输入: 输入样本点 $X_i(x_{i1}, x_{i2}, \dots, x_{im})$, $i = 1, 2, \dots, n$

(样本点是有序的, 按照评价时间倒序排列)

输出: m 个信任云 ($TPC_1, TPC_2, \dots, TPC_m$) 的数字特征 ($Ex_1, \dots, Ex_m, En_1, \dots, En_m, He_1, \dots, He_m$)

算法具体步骤如下:

1. 计算信任隶属度 $\mu_i = e^{-\frac{2 \ln \frac{1}{2} \times i}{n}}$.
2. 根据 $X_i(x_{i1}, x_{i2}, \dots, x_{im})$ 计算加权样本均值:

$$\bar{x}_1 = \frac{1}{n} \sum_{i=1}^n \left(x_{1i} \times \left(\frac{1}{2} + \mu_i \right) \right),$$

$$\bar{x}_2 = \frac{1}{n} \sum_{i=1}^n \left(x_{2i} \times \left(\frac{1}{2} + \mu_i \right) \right),$$

\vdots

$$\bar{x}_m = \frac{1}{n} \sum_{i=1}^n \left(x_{mi} \times \left(\frac{1}{2} + \mu_i \right) \right).$$

3. $(Ex_1, \dots, Ex_m) = (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_m)$.
4. 计算熵:

$$En_1 = \sqrt{\frac{1}{n-1} \sum_{i=1}^n (x_{1i} - Ex_1)^2},$$

$$En_2 = \sqrt{\frac{1}{n-1} \sum_{i=1}^n (x_{2i} - Ex_2)^2},$$

\vdots

$$En_m = \sqrt{\frac{1}{n-1} \sum_{i=1}^n (x_{mi} - Ex_m)^2}.$$

5. 对于每一个云滴 (X_i, μ_i) , 计算:

$$\begin{aligned} En'_{i1} &= \sqrt{\frac{-(x_{i1} - Ex)^2}{2 \ln \mu_i}}, \\ En'_{i2} &= \sqrt{\frac{-(x_{i2} - Ex)^2}{2 \ln \mu_i}}, \\ &\vdots \\ En'_{im} &= \sqrt{\frac{-(x_{im} - Ex)^2}{2 \ln \mu_i}}. \end{aligned}$$

6. 计算各 En'_i 的标准差, 得到

$$\begin{aligned} He_1 &= \sqrt{\frac{1}{n-1} \sum_{i=1}^n (En'_{i1} - \overline{En'_1})^2}, \\ He_2 &= \sqrt{\frac{1}{n-1} \sum_{i=1}^n (En'_{i2} - \overline{En'_2})^2}, \\ &\vdots \\ He_m &= \sqrt{\frac{1}{n-1} \sum_{i=1}^n (En'_{mi} - \overline{En'_m})^2}. \end{aligned}$$

算法 2 中, 第 1 步中信任隶属度的计算考虑了时间权重, 第 2 步中加权样本均值的计算也考虑了时间权重, 越是近期的评价权重越大, 在信任云逆向生成中起的作用就越大, 这是符合实际情况的。

这样, 利用上述算法 2 可以求出各信任属性云的数字特征 $TPC(Ex, En, He)$ 。

3.4 信任的综合评判

为了更好地评价各实体间的信任, 可以先对各属性进行评价。但由于对各属性的侧重点不同, 所以在对各实体进行评价时, 可以根据具体情况预先指定各属性的权重, 最后再进行综合评判。

根据各信任属性云的数字特征值以及对应的权重计算出新的综合信任云, 计算公式如下:

$$\begin{cases} Ex = \sum_{i=1}^m (Ex_i \times \lambda_i) \\ En = \sqrt{\sum_{i=1}^m (En_i^2 \times \lambda_i)} \\ He = \sum_{i=1}^m (He_i \times \lambda_i) \end{cases} \quad (5)$$

其中, m 为属性的个数; $\lambda_i (\sum_{i=1}^m \lambda_i = 1)$ 为各属性对应的权重。

由式 (5) 得到实体综合信任云的数字特征 (Ex, En, He) 是实体信任的反映, 然后将综合信任云与各信任子云进行比较, 计算出相似度, 找出与该实体综合信任云最接近的标准信任子云, 该标准信任子云对应的信任等级则为实体的信任等级。

定义 6. 设 $TC_1(Ex, En, He), TC_2(Ex, En, He)$ 为两个信任云, 将信任云 TC_1 经过正向云发生

器生成云滴 (x_i, μ_i) , 若 x_i 在云 TC_2 中的隶属度为 μ'_i , 称 $\frac{1}{n} \sum_{i=1}^n \mu'_i$ 为信任云 TC_1 与 TC_2 的相似度, 记为 δ 。

由于 μ'_i 是信任云 TC_1 中的云滴 (x_i, μ_i) 在信任云 TC_2 中的隶属度, 所以 μ'_i 越大, 该云滴对于信任云 TC_2 的隶属度越大, 则这两个云重复的云滴越多, 两个云越相似。

算法 3. 信任云相似度计算。

输入: $TC_1(Ex_1, En_1, He_1), TC_2(Ex_2, En_2, He_2)$

输出: 输出 δ (两个信任云之间的相似度)

算法具体步骤如下:

1. 在信任云 TC_1 中生成以 En_1 为期望和 He_1^2 为方差的一个正态随机数 $En'_i = NORM(En, He^2)$ 。

2. 在信任云 TC_1 中生成以 Ex_1 为期望和 $En_i'^2$ 为方差的一个正态随机数 $x_i = NORM(Ex, En_i'^2)$ 。

3. 将 x_i 代入信任云 TC_2 的期望方程中, 计算

$$\mu'_i = e^{-\frac{(x_i - Ex_2)^2}{2(En_2)^2}}.$$

4. 重复步 2 和 3, 直到生成 n 个 μ'_i 。

5. 计算 $\delta = \frac{1}{n} \sum_{i=1}^n \mu'_i$ 。

反复执行“算法 3”可以分别计算出综合信任云与各标准信任子云间的相似度值, 其中与实体综合信任云相似度最高的那个标准信任子云所对应的信任等级就是该实体的信任等级。

综上所述, 最终评定的信任值包含两部分内容: 一是历史信任值 (前一次评价的信任值); 另一个是评估得到的信任等级, 利用式 (4) 计算得到一个信任值, 两部分综合到一起得出最终的信任值。

3.5 特殊属性评价

对某些特殊属性的评价, 如果利用普通的评价方法很难做到有效和合理。比如电子商务交易中, 若交易商品的价格越高, 在成功交易后获得信任得分越高, 实际上这并不合理。针对这种情况, 本文提出一种新的评价方法 (特殊属性评价方法), 下面以商品价格属性为例进行研究与说明。

设某商家在历史交易中, V_{\min} 为最低商品价格, V_{\max} 为最高商品价格, V_{mean} 为商品平均价格, Len 为最低商品价格和最高商品价格中与平均价格之差最大者, 即

$$Len = \begin{cases} V_{\text{mean}} - V_{\min}, & (V_{\min} + V_{\max})/2 \leq V_{\text{mean}} \\ V_{\max} - V_{\text{mean}}, & (V_{\min} + V_{\max})/2 > V_{\text{mean}} \end{cases} \quad (6)$$

则历史交易中的商品价格区间为 $[V_{\text{mean}} - Len, V_{\text{mean}} + Len]$, 将该价格区间分为 $2k$ 个对称区间, 第 i 个区

间为 $[V_{\text{mean}} - L_i, V_{\text{mean}} - L_{i-1}]$ 和 $[V_{\text{mean}} + L_{i-1}, V_{\text{mean}} + L_i]$, 其中 L_i 为第 i 个区间的下限或上限到商品价格平均值的距离. 此方法划分的等级区间(如图 2 所示), 离平均价格越接近的区间等级越高.

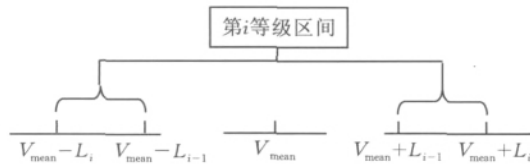


图 2 等级区间划分示意图

在实际应用中, 如果在计算信任值时不考虑商品价格, 那么不法分子可以利用低价商品进行信用炒作; 如果在计算信任值时按照商品价格给予不同的信任得分(高价得高分), 那么不法分子可以通过高价商品进行信用炒作. 因此, 利用本节提出的特殊属性评价方法(如式(6)), 可以有效地防止不法分子利用低价或者高价商品进行信用炒作.

3.6 信任惩罚方法

若某实体最近一次交易失败, 应该对其进行惩罚以防止行骗的发生. 惩罚一般根据交易金额判定惩罚力度, 金额与历史平均值相差越大, 则行骗可能性越大, 那么惩罚力度应该越大. 本节研究的惩罚方法是在现有信任值的基础之上减去一个惩罚分, 计算公式如下:

$$T = T_0 - (R_i^{\max} - R_i^{\min}) \times \left(1 - \frac{\alpha}{10}\right) \quad (7)$$

其中, T 是惩罚后的信任值, T_0 是惩罚前的信任值; R_i^{\min} 、 R_i^{\max} 分别是惩罚前所在信任等级区间的下限和上限; α 为交易金额的等级得分, 可以根据式(4)计算得到, 除以 10 是为了将数据格式化到 $[0, 1]$ 区间上.

4 仿真实验与分析

本节的仿真实验使用的 PC 机的基本配置: Intel® Core™ i3 CPU, 3GB 内存, 操作系统为 Microsoft Windows XP, 在 Matlab 环境下进行仿真实验.

4.1 基于云模型的信任评估方法的仿真实验与分析

本节模拟实际场景进行仿真实验, 以验证本文研究的基于云模型的信任评估方法的可行性.

本仿真实验数据都是来自淘宝网上某商家的交易记录(共 400 条), 每条交易记录包括: 交易的时间、商品名称、商品成交价格、买家对卖家的评价(包

括商品描述的相符度、卖家服务态度和卖家发货速度).

(1) 数据预处理

① 确定信任评价属性(因为淘宝网交易评价有商品描述的相符度、卖家服务态度、卖家发货速度等 3 项, 本仿真实验增加商品价格作为对信任评价属性).

② 将淘宝网上买家对商品描述的相符度、卖家服务态度、卖家发货速度的评价分为 5 个等级, 分别对应 $[0, 2]$ 、 $[2, 4]$ 、 $[4, 6]$ 、 $[6, 8]$ 、 $[8, 10]$ 区间, 由式(4)分别计算得到其得分值, 如表 1 所示.

表 1 评价属性区间的分值

评价属性	等级区间得分值				
	非常差	差	一般	好	非常好
	$[0, 2]$	$[2, 4]$	$[4, 6]$	$[6, 8]$	$[8, 10]$
商品与所描述相符程度	1.9	3.6	5.6	6.6	8.2
服务态度	1.8	3.5	5.5	6.6	8.2
发货速度	1.9	3.8	5.8	6.8	8.3

③ 将商品价格分成 5 个区间, 由式(4)计算出的得分值, 如表 2 所示.

表 2 商品价格属性区间的分值

商品价格区间	等级区间	商品价格区间得分值
$[10, 150]$ $[4930, 5070]$	$[0, 2]$	1.9
$[150, 350]$ $[4730, 4930]$	$[2, 4]$	3.6
$[350, 800]$ $[4280, 4730]$	$[4, 6]$	5.6
$[800, 1500]$ $[3580, 4280]$	$[6, 8]$	6.4
$[1500, 2540]$ $[2540, 3580]$	$[8, 10]$	8.1

④ 信任区间定义.

设信任取值在 $[0, 10]$ 区间内, 根据经验将 $[0, 10]$ 区间划分为 5 个子区间: $[0, 1.5]$ (极不可信), $[1.5, 3.5]$ (不可信), $[3.5, 6.5]$ (低可信), $[6.5, 8.5]$ (一般可信), $[8.5, 10]$ (高可信).

(2) 仿真实验步骤

① 根据算法 1(标准信任云生成算法)将标准信任子云分为极不可信云 $STC_1(0, 0.5, 0.2)$, 不可信云 $STC_2(2.5, 0.67, 0.2)$, 低可信云 $STC_3(5, 1.33, 0.2)$, 一般可信云 $STC_4(7.5, 0.67, 0.2)$, 高可信云 $STC_5(10, 0.5, 0.2)$, 利用正向信任云生成器可生成信任云, 如图 3 所示.

② 将预处理后的数据利用算法 2(信任属性云逆向生成算法)生成属性云.

③ 根据 3.4 节所述的方法将属性云进行合并得到综合评价云 $TC(5.5, 1, 0.4)$, 综合评价云与标准信任云对比如图 4 所示。

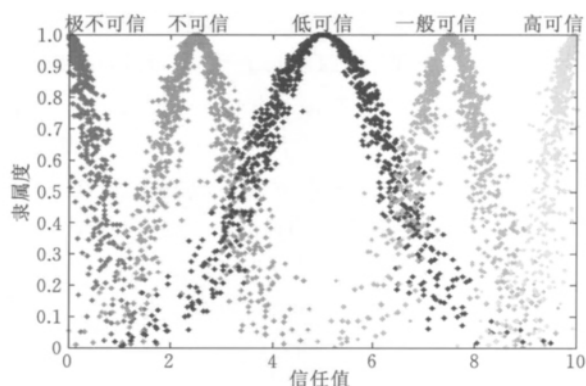


图 3 标准信任云生成图

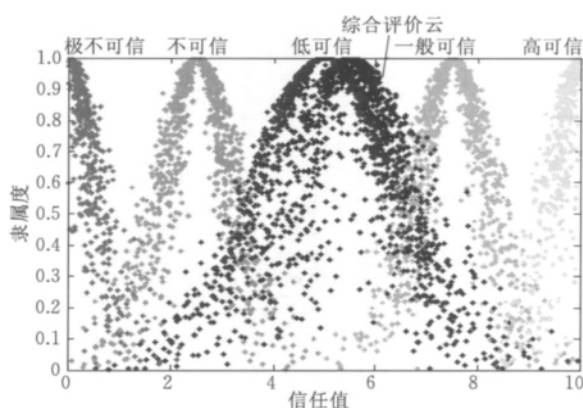


图 4 综合后的综合云与标准云对比图

④ 根据算法 3 (信任云相似度计算算法) 计算出综合评价云与各标准信任子云的相似度 (如表 3 所示), 从表 3 中可知综合评价云与低可信云相似度最高, 所以判定该商家的信任等级为低可信。

表 3 综合评价云与标准信任子云的相似度

标准信任子云	相似度
极不可信云	0.0001
不可信云	0.0403
低可信云	0.7582
一般可信云	0.1434
高可信云	0.0014

⑤ 低可信等级的信任值区间为 $[3.5, 6.5]$, 根据信任云滴的分布, 在低可信及其以上等级中的云滴占总云滴的比例为 90%, 由式 (4) 可以计算出信任值为 6.2。本实验采取历史信任值与当前信任值 (本文的评估方法) 各占 50% 的权重, 前一次评定的信任值为 6, 所以本次最终信任值为 $6 \times 50\% + 6.2 \times 50\% = 6.1$ 。

本节的仿真实验结果与预期结果相同, 证明了

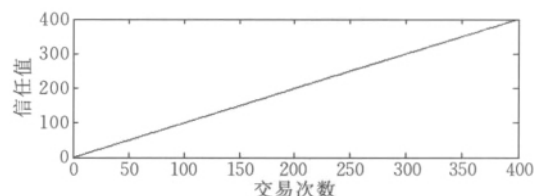
本文研究的信任评估方法是可行的。

4.2 防信用炒作实验

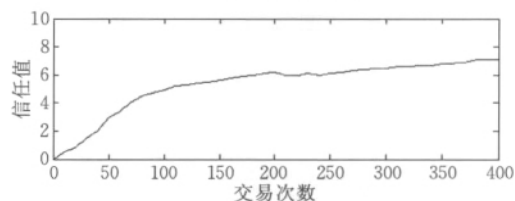
目前, 淘宝网的信用计算方法只是简单地加 1 或减 1, 评价“好”的加 1 分, 评价“中”的不加分, 评价“差”的减 1 分, 没有考虑商品价格因素, 不法商家可以通过大量出售低价的商品迅速地赚取信用分, 即所谓的信用炒作。此外, 淘宝网的信用计算方法所得到的分值是可以无限增大的, 没有上线, 缺少参考标准, 而本文研究的信任评估方法所得到的信任值是在区间 $[0, 10]$ 内。

本节模拟实际场景进行防信用炒作实验, 以验证基于云模型的信任评估方法的合理性。仿真实验数据来自使用了信用炒作的交易数据, 该数据与 3.1 节实验中使用的格式相同。

仿真实验结果如图 5 所示, 图 5(a) 中信用变化曲线是按照淘宝网信用计分法计算的, 从图 5(a) 中可以看出简单的信用值累加方法无法对信用炒作进行有效的防范。图 5(b) 是本文研究的信任评估方法计算的信任值变化曲线, 从曲线的变化趋势可以看出随着交易次数的增多信任值的增长并非像淘宝网的方法那样线性增长, 而是越来越缓慢, 对信用炒作有很好的防范作用。



(a) 采用淘宝网信用计分方法的信任值变化曲线图



(b) 采用本模型的信任值变化曲线图

图 5 防信用炒作实验对比图

本节的仿真实验结果证明了基于云模型的信任评估方法可以防止信用炒作, 也进一步说明该模型的可行性和合理性。

4.3 防周期行骗实验

本节模拟实际场景进行防周期性的行骗实验, 以进一步验证基于云模型的信任评估方法对周期行骗进行控制的可行性和合理性。仿真实验的数据是构造的 (具有欺骗性), 用来模拟不法商家使用周期行骗手段进行交易的数据。

仿真实验结果如图 6 所示,图 6(a)和图 6(b)分别是采用淘宝网信用计分方法和本文研究信任评估计分法的信任值变化曲线图。

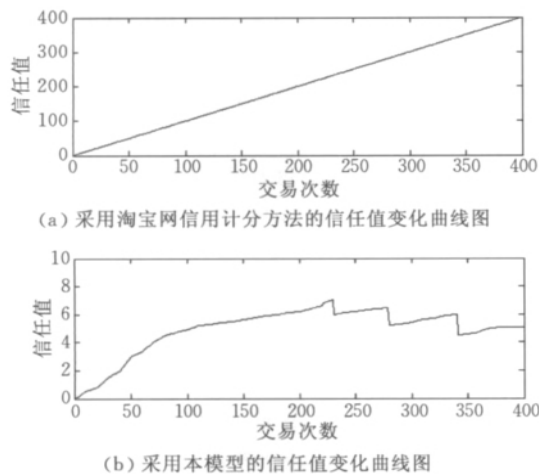


图 6 防周期行骗实验对比图

从图 6(a)中可以看出,简单的信用值累加方法无法对周期行骗有很好的防范,因为卖家的信任值达到一定值的时候,一次或少数次的欺骗交易对信任值几乎没有影响。从图 6(b)中可以看出,在第 230 次、第 280 次、第 340 次附近有交易失败记录,有欺骗行为,信任值陡降,这样可以对欺骗行为进行惩罚,很好地防范周期行骗,也给买方提供了风险参考。

由此可知,使用本文所研究的基于云模型的信任评估方法,可以使具有欺骗行为的卖家的信任值陡降,这也证明了基于云模型的信任评估方法能有效地防止具有欺骗行为的买家,同时也进一步说明本文研究的基于云模型的信任评估方法的可行性和合理性。

5 结 语

在复杂的网络环境中有许多不确定因素(随机性、模糊性和不可预测性等)都会对用户的信任产生一定影响,而在网络交易(例如电子商务交易)中,只有在交易双方相互信任的情况下,交易才有可能顺利地进行下去,所以信任是进行交易活动的前提和关键。本文以复杂的网络环境为研究背景,引入云模型理论和借鉴已有工作,研究并提出了针对复杂的网络环境下的基于云模型的信任评估方法;通过模拟实际场景进行仿真实验,进一步验证了基于云模型的信任评估方法的可行性和合理性。目前,尽管我

们在信任评估方面进行了一些研究,取得了一些阶段性的成果,但是有很多技术还停留在实验室中,距离推广还有很多实际问题需要进一步研究解决;除此之外,研究如何防范具有信任诋毁的信任评估模型也是下一步主要研究的工作。

参 考 文 献

- [1] Zhang Shi-Bin, He Da-Ke, Endo Homare. Research of fuzzy autonomous trust establishment strategy. *Journal of Electronics & Information Technology*, 2006, 28(8): 1492-1496 (in Chinese)
(张仕斌, 何大可, 远藤誉. 模糊自主信任建立策略的研究. *电子与信息学报*, 2006, 28(8): 1492-1496)
- [2] Xi Rong-Rong, Yun Xiao-Chun, Jin Shu-Yuan, Zhang Yong-Zheng. Research survey of network security situation awareness. *Journal of Computer Applications*, 2012, 32(1): 1-4, 59(in Chinese)
(席荣荣, 云晓春, 金舒原, 张永铮. 网络安全态势感知研究综述. *计算机应用*, 2012, 32(1): 1-4, 59)
- [3] Wang Shou-Xin, Zhang Li, Li He-Song. Evaluation approach of subjective trust based on cloud model. *Journal of Software*, 2010, 21(6): 1341-1352(in Chinese)
(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)
- [4] Yang Liu, Lu Ying-Hua. An evaluation model for network risk based on cloud theory. *Computer Simulation*, 2010, 27(10): 95-98(in Chinese)
(杨柳, 吕英华. 基于云模型的网络风险评估技术研究. *计算机仿真*, 2010, 27(10): 95-98)
- [5] Zhang Huan-Guo, Chen Lu, Zhang Li-Qiang. Research on trusted network connection. *Chinese Journal of Computers*, 2010, 33(4): 706-717(in Chinese)
(张焕国, 陈璐, 张立强. 可信网络连接研究. *计算机学报*, 2010, 33(4): 706-717)
- [6] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management//*Proceedings of the Symposium on Security and Privacy*. Oakland, 1996: 164-173
- [7] Blaze M, Feigenbaum J, Keromytis A D. Keynote: Trust management for public-key infrastructures//*Proceedings of the 1998 Security Protocols International Workshop*, Cambridge, England, 1998: 59-63
- [8] Khambatti M, Dasgupta P, Ryu K D. A role-based trust model for Peer-to-Peer communities and dynamic coalitions//*Proceedings of the 2nd IEEE International Information Assurance Workshop*. New York, 2004: 141-154
- [9] Winsborough William H, Seamons Kent E, Jones Vicki E. Automated trust negotiation//*Proceedings of the DARPA Information Survivability Conference & Exposition*. Piscataway, 2000, 1: 88-102
- [10] Nejdil W, Olmedilla D, Winslett M. PeerTrust: Automated trust negotiation for peers on the semantic Web//*Proceedings of the Workshop on Secure Data Management in a Connected World*. Toronto, 2004

- [11] Tang Wen, Hu Jian-Bin, Chen Zhong. Research on a fuzzy logic-based subjective trust management. *Journal of Computer Research and Development*, 2005, 42(10): 1654-1659 (in Chinese)
(唐文, 胡建斌, 陈钟. 基于模糊逻辑的主观信任管理模型的研究. *计算机研究与发展*, 2005, 42(10): 1654-1659)
- [12] Chen Zhen-Xiang, Ge Lian-Sheng, Wang Hai-Yang, Huang Xian-Zhi, Lin Jin-Jiao. A Trust-based service evaluation and selection model in pervasive computing environment. *Journal of Software*, 2006, 17(S): 200-210 (in Chinese)
(陈贞翔, 葛连升, 王海洋, 黄先芝, 林金娇. 普适环境中基于信任的服务评价和选择模型. *软件学报*, 2006, 17(S): 200-210)
- [13] Zhang Xing-Lan, Nie Rong. A self-government model peer-to-peer trust management. *Journal of Beijing University Technology*, 2008, 34(2): 211-215 (in Chinese)
(张兴兰, 聂荣. P2P 系统的一种自治信任管理模型. *北京工业大学学报*, 2008, 34(2): 211-215)
- [14] Tian Li-Qin, Lin Chuang. Evaluation mechanism for user behavior trust based on DSW. *Journal Tsinghua University (Science & Technology)*, 2010, 50(5): 763-767 (in Chinese)
(田立勤, 林闯. 基于双滑动窗口的用户行为信任评估机制. *清华大学学报(自然科学版)*, 2010, 50(5): 763-767)
- [15] Wang Liang-Min, Guo Yuan-Bo, Zhan Yong-Zhao. Fuzzy trust model for wireless sensor networks with intrusion tolerance. *Journal on Communications*, 2010, 31(12): 37-44, 54 (in Chinese)
(王良民, 郭渊博, 詹永照. 容忍入侵的无线传感器网络模糊信任评估模型. *通信学报*, 2010, 31(12): 37-44, 54)
- [16] Liu Liang, Zhou De-Jian, Xie Xiao-Lan, Li Jing. Services trust evaluation model based on cloud computing. *Software Guide*, 2011, 10(5): 75-77 (in Chinese)
(刘亮, 周德俭, 谢晓兰, 李静. 基于云计算的服务信任评估模型. *软件导刊*, 2011, 10(5): 75-77)
- [17] Fan Li-Jie, Wang Su-Zhen, Liu Wei. Evaluation method based on human trust mechanism for mobile e-commerce trust. *Computer Science*, 2012, 39(1): 190-193 (in Chinese)
(樊丽杰, 王素贞, 刘卫. 基于人类信任机制的移动电子商务信任评估方法. *计算机科学*, 2012, 39(1): 190-193)
- [18] Zhang Shi-Bin, Chen Lin, Wang Yi-Chuan. A subjective trust valuation model based on fuzzy reasoning. *Chinese Journal of Scientific Instrument*, 2009, 30(S1): 658-660 (in Chinese)
(张仕斌, 陈麟, 王一川. 一种基于模糊推理的主观信任评价模型. *仪器与仪表学报*, 2009, 30(S1): 658-660)
- [19] Zhang Shi-Bin, He Da-Ke. Fuzzy model for trust evaluation. *Journal of Southwest Jiaotong University (English Edition)*, 2006, 14(1): 23-28
- [20] Zhang Shi-Bin, He Da-Ke, Endo Homare. Research on dynamic definition of trust class based on the fuzzy clustering. *Computer Engineering*, 2006, 32(9): 19-21 (in Chinese)
(张仕斌, 何大可, 远藤誉. 基于模糊聚类的信任类型动态定义机制的研究与分析. *计算机工程*, 2006, 32(9): 19-21)
- [21] Li Fei, Zhang Shi-Bin. Study on the network system status's assessment and forecast model based on cloud model. *Journal of Sichuan University (Engineering Science Edition)*, 2010, 42(6): 99-104 (in Chinese)
(李飞, 张仕斌. 基于云模型的网络系统状态评估与预测模型研究. *四川大学学报(工程科学版)*, 2010, 42(6): 99-104)
- [22] Li Rui-Xuan, Gao Chang, Gu Xi-Wu, Lu Zheng-Ding. Research on credit counting and risk evaluation for C2C e-commerce. *Journal on Communications*, 2009, 30(7): 78-85 (in Chinese)
(李瑞轩, 高昶, 辜希武, 卢正鼎. C2C 电子商务交易的信用及风险评估方法研究. *通信学报*, 2009, 30(7): 78-85)
- [23] Sun Xiao-Yin, Wu Guo-Xin, Dong Yong-Qiang, Ye Ping. New initialization strategy of reputation system based on recommendation. *Journal of Southeast University (Natural Science Edition)*, 2010, 40(1): 41-46 (in Chinese)
(孙啸寅, 吴国新, 董永强, 叶枰. 一种基于推荐的信誉系统初始化定值策略. *东南大学学报(自然科学版)*, 2010, 40(1): 41-46)
- [24] Wei Da, Jia Xiang-Peng, Wang Jian, Liu Yan-Heng. New access model and implementation of trusted network based on trusted certificate. *Journal of Jilin University (Engineering and Technology Edition)*, 2010, 40(2): 496-500 (in Chinese)
(魏达, 贾翔鹏, 王健, 刘衍珩. 基于可信证书的可信网络接入模型及实现. *吉林大学学报(工学版)*, 2010, 40(2): 496-500)
- [25] Tang Zhi-Wei, Gao Tian-Peng. OCTAVE-based risk evaluation for e-government information systems. *Journal of University of Electronic Science and Technology of China*, 2009, 38(1): 130-133 (in Chinese)
(汤志伟, 高天鹏. 采用 OCTAVE 模型的电子政务信息系统风险评估. *电子科技大学学报*, 2009, 38(1): 130-133)
- [26] Li De-Yi, Du Yi. *Artificial Intelligent with Uncertainty*. Beijing: National Defence Industry Press, 2005 (in Chinese)
(李德毅, 杜鹞. 不确定性人工智能. 北京: 国防工业出版社, 2005)



ZHANG Shi-Bin, born in 1971, Ph.D., professor. His research interests include applied computer technology, information security and cryptography.

XU Chun-Xiang, born in 1965, Ph.D., professor, Ph.D. supervisor. Her research interests include cryptography, information security, and secure e-commerce.

Background

Trust evaluation approach is one of the important problems in the network transactions, and the premise and foundation of network transactions is trust in the complex network environment. In recent years, although the trust evaluations of network transactions have been carried out fruitful research by some scholars, there are still many problems need to be solved in the complex network environment. For example, how to reasonably carry out formal description of trust relationship, how to develop trust evaluation mechanism, how to judge the credibility or not, how to design the trust evaluation system, how to use trust policy, how to determine the relationship between trust and risk, and how to achieve the trust integration of the next generation network and so on. The research of trust evaluation approach belongs to the filed of information security. However, the researchers paid more attention to the research of trust management at present. In fact, in complex network environments, the solution of trust issues need be a feasible and reasonable trust evaluation model. This is because the trust evaluation model plays an essential role in the field of trust research. In order to better reflect the randomness, fuzziness, and unpredictability in the complex network environment, the trust evaluation model needs to use a trust evaluation approach to evaluate the information of network users.

By the aid of cloud model theory and the existing research results of the authors, this paper proposed the trust evaluation approach based on cloud model. The main contribution of this paper is in two aspects. Firstly, by defining the trust cloud of all entities, this trust evaluation approach can implement the conversion between qualitative and quantitative of trusts, which objectively reflect the randomness, fuzziness and unpredictability of the trusts in complex network

environment. Secondly, based on the trust evaluation approach based on cloud model, in order to further resolve the validity and rationality of trust evaluation and effectively prevent the users with the credit speculations and fraud behaviors, the evaluation method of special properties and the method of trust punishment were proposed in this paper.

This research is supported by the Sichuan Science and Technology Support Project (No 13ZC2138), Research Fund of Middle-Aged Academic Leaders of CUIT (Chengdu University of Information Technology) (No J201107) and Postdoctoral Fund of UESTC (University of Electronic Science and Technology of China) (No 73984). These projects aim to provide better trust evaluation model and risk assessment model. Our group has working on the researches of trust evaluation model, trust evaluation approach, risk assessment model and risk assessment approach based on cloud model theory and fuzzy theory. Many good papers have been published in respectable international conferences and some academic journals, such as Journal of Electronics & Information Technology, Chinese Journal of Scientific Instrument, Journal of Sichuan University and Journal of Southwest Jiaotong University.

The trust evaluation approach in this paper has implemented the conversion between qualitative and quantitative of trusts, and the evaluation method of special properties and the method of trust punishment proposed in this paper can effectively prevent the users with the credit speculations and fraud behaviors. The trust evaluation approach proposed in this paper may provide a new promising method for research of trust evaluation in complex networks environment. In the future work, we will focus on trust evaluation approach which can prevent trust slander.