



增强交易因素影响的 P2P 网络信任评估模型研究 *

张祖昶, 王 诚

(南京邮电大学通信与信息工程学院 南京 210003)

摘 要: 在交易评估机制中, 信任度由多种因素构成, 但由于各个因素自身的特点, 其影响和作用大小不一。通过采用适当的关联关系, 增强某些重要交易因素的影响和作用, 可以有效地提高评估模型的准确率和有效性。由此提出一种增强交易因素影响的 P2P 网络信任评估模型, 给出了新的信任评估计算方法和仿真实验。实验结果表明, 该评估模型效果显著。

关键词: 对等网络; 信任度; 增强; 交易因素

doi: 10.3969/j.issn.1000-0801.2013.10.015

Research on a Model of Enhancing Factors' Effects Based on Trust Evaluation for P2P Network

Zhang Zuchang, Wang Cheng

(College of Telecommunications & Information Engineering, Nanjing University of
Posts and Telecommunications, Nanjing 210003, China)

Abstract: In the transaction evaluation mechanism, trust is formed by many kinds of factors, but due to the characteristics of its own, its effects and influences are different. By using the relationship between appropriate, it enhances the effects of some important factors and the role of trade. That can effectively improve the accuracy and validity of the evaluation model. A model of enhancing the factors' effects based on the trust evaluation for P2P network was proposed, a new calculation method of the trust evaluation, and the model's simulation results were given. The experimental results show that the evaluation model has significant effect.

Key words: peer-to-peer network, trust, enhancing, trading factor

1 引言

P2P (peer-to-peer) 网络是一种开放、自由、分布式的网络, 这相对于传统网络而言有很多优点。目前, P2P 技术广泛应用于文件共享、分布式计算、协同工作、即时通信、电子商务等领域^[1], 特别是电子商务领域。由于 P2P 电子商务的快速发展, P2P 技术在商业经济中发挥着越来越重要的作用。在 P2P 网络中, 网络节点之间是相互平等

的, 具有开放、动态、匿名和无中心等特点^[1], 这使得网络节点在交易过程中, 容易出现大量的安全问题, 这些安全问题直接制约了 P2P 技术的进一步发展。根据以往的研究结论和经验^[1-15], 解决这一问题的有效办法是在 P2P 网络节点之间建立信任评价模型, 这是降低交易风险和提高 P2P 系统整体可用性的有效解决方案。因此, 如何在 P2P 网络节点间建立有效的信任评价模型, 已经成为当前研究的重点。

* 江苏省基础 Research 计划 (自然科学基金) 基金资助项目 (No.BK2012434)

2 相关工作

在 P2P 网络中,存在很多不确定因素和巨大的安全风险。为了解决这些问题,有很多学者和机构正进行相关的研究^[1-15],如贝叶斯信任模型^[8]、基于时间帧的动态信任模型^[9]以及基于相似度加权推荐的信任模型^[14]等。在这些模型中,大部分思想都源自于人类社会的交易模式。

目前,P2P 网络的信任模型主要分为集中式管理模型和对等信任模型两大类^[7,9,10]。集中式管理模型主要是将传统网络有效的管理方法应用到 P2P 网络中,此类模型有一定的效应,但由于管理办法出自于传统网络,必然会失掉一些 P2P 网络的优点,因此不具备一般性;对等信任模型主要是依靠 P2P 网络节点自身进行信任评估,具有一般性,但由于网络节点之间彼此独立、自由,因此难于建立网络节点之间的信任评估模型,这一直是 P2P 网络安全研究的方向,也是研究的重点和难点。

就 P2P 网络的网络特性而言,P2P 网络与人类社会很相似,因此 P2P 网络的信任评估模型也与人类社会的交易信任评估模型相似。在人类社会中,对个体的信任一般由直接信任和间接(或推荐)信任组成,简称信任度。这些信任的形成来自于个体交易的历史信息,这些历史信息包括交易成本、交易次数、交易频率、交易风险、欺诈历史和持续时间等因素。人类社会的交易历史经验证明,这些因素在交易信任评估机制中确实起到了很重要的借鉴作用和影响,是构成信任评估结论的事实依据。但由于这些因素各具自身的特点,且对交易的情况和条件的要求也有所不同。因此,在分析这些因素产生的具体作用和影响时,要根据交易当时的情况和条件进行评估,这样才能建立起正确、有效的信任评估模型。

依据上述思想,在建立网络节点之间的信任评估模型时,充分考虑网络节点之间交易时的情况和条件,并在构建评估模型的关联公式时,对影响效果较大的交易因素进行适度的效能放大。希望通过此思路建立起一种有效的 P2P 网络信任评估模型,使其有助于 P2P 网络更进一步地完善和发展。

3 信任评估模型

对于 P2P 网络而言,P2P 网络节点之间的交易行为与人类社会个体之间的交易行为很相似。因此,P2P 网络节点之间的信任评估模型可以借鉴人类社会的交易信任评

估模型构建。

3.1 模型相关定义

定义 1 令 $\Omega=\{r_1, r_2, \dots, r_p\}$ 是含节点数为 p 的 P2P 网络节点的集合, $N(r_i, r_j)$ 为集合 Ω 中任意两个不同节点 r_i 和 r_j 之间交易的次数, $n \in [0, N(r_i, r_j)]$ 。

定义 2 在集合 Ω 中,对于 $\forall r_i \in \Omega, \forall r_j \in \Omega$, 且 $r_i \neq r_j$, 令 $F(r_i, r_j)$ 是节点 r_i 对 r_j 的恶意访问次数, $D(r_i, r_j)$ 是节点 r_i 对 r_j 的恶意访问造成的损失。

定义 3 对于 $\forall r_i \in \Omega, \forall r_j \in \Omega$, 且 $r_i \neq r_j$, 令 $T(r_i, r_j)_D$ 为节点 r_i 对节点 r_j 的第 $N(r_i, r_j)+1$ 次直接信任估值, 则有:

$$T(r_i, r_j)_D = \frac{\sum_{0 \leq n \leq N(r_i, r_j)} \left(\frac{T(r_i, r_j)_{D_n} - D(r_i, r_j)_n}{F(r_i, r_j)_n} \right)}{N(r_i, r_j)} \quad (1)$$

定义 4 对于 $\forall r_i \in \Omega, \forall r_j \in \Omega$, 且 $r_i \neq r_j$, 令 $T(r_i, r_j)_R$ 为节点 r_i 对节点 r_j 的第 $N(r_i, r_j)+1$ 次推荐信任估值, 则有:

$$T(r_i, r_j)_R = \frac{\sum_{0 \leq n \leq N(r_i, r_j)} T(r_i, r_j)_{R_n}}{N(r_i, r_j)} = \frac{\sum_{0 \leq m \leq N(r_i, r_j)_n} \left(\frac{T(r_i, r_j)_{D_m} - D(r_i, r_j)_m}{F(r_i, r_j)_m} \right)}{\sum_{0 \leq n \leq N(r_i, r_j)} \frac{N(r_i, r_j)_n}{N(r_i, r_j)}} \quad (2)$$

定义 5 对于 $\forall r_i \in \Omega, \forall r_j \in \Omega$, 且 $r_i \neq r_j$, 令 $T(r_i, r_j)$ 为节点 r_i 对节点 r_j 的第 $N(r_i, r_j)+1$ 次信任估值, 则有:

$$T(r_i, r_j) = \lambda \cdot T(r_i, r_j)_D + \mu \cdot \sum_{\substack{\forall i, j, k \in (0, p) \\ i \neq j, i \neq k, j \neq k}} T(r_i, r_k)_D \cdot T(r_k, r_j)_R \quad (3)$$

其中, $\lambda + \mu = 1$, 且 $\lambda > 0, \mu > 0$ 。

由式(3)可知,网络节点之间的信任值 $T(r_i, r_j)$ 主要由 r_i 和 r_j 之间的直接信任值 $T(r_i, r_j)_D$ 和间接信任值 $T(r_i, r_j)_R$ 加权组成,而且在间接信任值 $T(r_i, r_j)_R$ 中,还加入了节点 r_i 对推荐节点 r_k 的直接信任值 $T(r_i, r_k)_D$,在一定程度上增强了节点 r_i 在评估模型中的影响和作用,提高了模型的主动性和灵活性,避免了盲目听从推荐节点的情况发生。从逻辑推理上来说,这可以有效地提高评估模型的正确性和有效性,跟人类社会的交易信任评估判断方法的原理是相符的。在现实生活中,人类社会的个体在交易的过程中,大部分情况下会选择倾听他人的意见,再结合自身对交易对方的信任程度做出最后的判断。特别是在交易双方彼此陌生的情况下,希望借助第三方意见的意图更加明显。但从现实的经验和例子可知,不是任何第三方的意见都能信。人类社会对交易行为总结出一个结论:越值得信赖的人或机



构,其给出的意见越权威或值得信赖。因此,在式(3)中,节点 r_i 对推荐节点 r_k 的直接信任值 $T(r_i, r_k)_D$ 的加入,符合上述交易评估思想,使得交易节点 r_i 在整个交易评估过程中的影响放大,有利于模型做出正确的决断。

这种增强交易因素影响的思想在式(1)中也有体现。在式(1)中,突出了恶意访问次数 $F(r_i, r_j)$ 和恶意损失 $D(r_i, r_j)$ 这两个对信任评估产生重大影响的因素。对于恶意访问次数 $F(r_i, r_j)$,模型的思路是不管是否造成交易方节点 r_i 的损失,只要节点 r_j 存在过恶意访问,对于节点 r_j 的信任值将迅速大幅度下降。因此,在式(1)中对恶意访问次数 $F(r_i, r_j)$ 采用反比例的关联形式。对于恶意损失 $D(r_i, r_j)$ 因素,在网络节点之间的交易行为中一般比较容易进行评估,而且数值一般比较大,因此直接在式(1)中作为负面评价因子出现,可以直接体现其影响和作用。

本文模型主要依据人类社会交易评判思想和方法,对交易过程中一些重要因素的影响和作用加以放大,以构建出一个增强某些重要交易因素的信任评估模型,从而使得整个网络形成一套良好的交易机制。

3.2 滤除伪节点

P2P 网络为人类社会所创造,因此包含很多人类的元素,会出现许多类似于人类社会的现象和事件。P2P 网络存在大量恶意的伪节点就是其中一种普遍的情况。这种情况严重地危及了 P2P 网络的安全,因此必须采取措施进行处理。对于此类情况,一般都采用相关相似性原理计算节点之间的相关程度^[14],以此滤除 P2P 网络中的伪节点。本文将节点交易评估过程和评估值保存下来,采用 PCC (pearson correlation coefficient) 计算方法计算节点之间的相关程度,以此滤除 P2P 网络中的伪节点。

定义 6 令矩阵 E 为 P2P 网络节点间历史推荐评估转换而来的 $p \times p$ 信任矩阵, p 是节点总数, E_{ij} 为信任矩阵 E 中的任意一个元素,若满足 $e_{ij} = \begin{cases} T(r_i, r_j)_k, & i \neq j \\ 1, & i = j \end{cases}$, 则

$$E = \begin{pmatrix} e_{11} & \cdots & e_{1p} \\ \vdots & \ddots & \vdots \\ e_{p1} & \cdots & e_{pp} \end{pmatrix}^0$$

定义 7 对于 $\forall r_i \in \Omega, \forall r_j \in \Omega$, 设 $M = \{r_1, r_2, \dots, r_s\}$ 为节点 r_i 与节点 r_j 共同访问过的节点集合,且对于节点集合 M 有 $s < p, M \subseteq \Omega$ 约束条件, E 和 Q 分别表示节点 r_i 与节点 r_j 对节点集合 M 的信任矩阵, $\bar{e}_i$ 和 $\bar{q}_j$ 分别表示节点 r_i 与节点 r_j 对节点集合 M 的所有节点评价的平均值,则节点集合 Ω 的节点间相关性计算式为:

$$\text{sim}(i, j) = \frac{\sum_{\substack{r_i \in \Omega, r_j \in \Omega, r_k \in M, \\ r_i \notin M, r_j \notin M, r_i \neq r_j}} (e_{iw} - \bar{e}_i) \cdot (q_{jw} - \bar{q}_j)}{\sqrt{\sum_{\substack{r_i \in \Omega, r_j \in \Omega, r_k \in M, \\ r_i \notin M, r_j \notin M, r_i \neq r_j}} (e_{iw} - \bar{e}_i)^2} \cdot \sqrt{\sum_{\substack{r_i \in \Omega, r_j \in \Omega, r_k \in M, \\ r_i \notin M, r_j \notin M, r_i \neq r_j}} (q_{jw} - \bar{q}_j)^2}} \quad (5)$$

在式(5)中, $\text{sim}(i, j) \in [0, 1]$, $\text{sim}(i, j)$ 的取值越大,表示节点 r_i 与节点 r_j 之间的相关性越大,反之亦然。根据这一特性,通过对 P2P 网络节点的历史交易行为按式(5)进行相关性计算,将 $\text{sim}(i, j)$ 取较大值的节点滤除,就可以将大部分 P2P 网络伪节点滤除。

4 实验数据及分析

定义 8 对于 $\forall r_i \in \Omega, \forall r_j \in \Omega$, 且 $r_i \neq r_j$, 令 $G(r_i, r_j)$ 为节点 r_i 遭到节点 r_j 恶意访问的总次数, $V(r_i, r_j)$ 为节点 r_i 对节点 r_j 的恶意访问做出正确判断的总次数, $\rho(r_i, r_j)$ 为节点 r_i 对节点 r_j 的恶意访问做出正确判断的成功率,则 $\rho(r_i, r_j) = V(r_i, r_j) / G(r_i, r_j)$ 。

为验证本文模型的正确性和有效性,采用 C 语言编写仿真程序,通过网络访问模拟节点访问过程进行实验仿真。仿真环境采用 20 台 PC 机互联组成 P2P 网络,每台 PC 机随机安装不同的操作系统模拟网络节点。为了便于实验,在这 20 台 PC 机中指定其中的 10 台 PC 机作为恶意节点或伪节点,令其随意地攻击或欺骗其他节点。在实验中,节点之间的信任评估值 $T(r_i, r_j)$ 的取值范围为 $[0, 1]$,按照式(3)计算,通过对式(3)中的权值 λ 和 μ 取不同值进行多次仿真实验。在实验初始化时,每个节点的信任评估值 $T(r_i, r_j)$ 均为 0.5。在实验过程中,节点间访问的次数、性质、结果及直接评估和推荐评估都将被记录,当节点的信任评估值 $T(r_i, r_j) < 0.2$ 时将被禁止访问。

通过进行多次实验,以不同的网络访问次数 G 为条件时,对比网络对恶意访问行为做出正确判断的成功率 ρ ,从而验证模型是否有效。实验仿真的具体结果见表 1。

从表 1 可以得出如下结论:从整体上看,网络访问次数 G 取不同值时,网络对于恶意访问行为的成功识别率 ρ 的取值是比较相近的,且随着网络访问次数 G 的增大,网络成功识别率 ρ 的取值总体趋势是缓慢增大的;在权值 λ 和 μ 的比值相近时,网络成功识别率 ρ 的取值处于低谷状态,其取值相对高于权值 λ 和 μ 的其他取值情况。

图 1 是实验仿真结果曲线,通过图 1 可以更加直观地发现上述规律。权值 λ 和 μ 的不同取值,直接影响式(3)中

表 1 实验仿真结果

权值	次数					
	$G=300$	$G=600$	$G=900$	$G=1\ 200$	$G=1\ 500$	$G=1\ 800$
$\lambda=0.1, \mu=0.9$	77.73%	78.33%	78.23%	78.03%	78.13%	78.33%
$\lambda=0.3, \mu=0.7$	79.33%	80.13%	80.63%	81.13%	81.53%	81.43%
$\lambda=0.5, \mu=0.5$	79.63%	80.53%	80.73%	81.23%	81.83%	81.93%
$\lambda=0.7, \mu=0.3$	78.43%	79.73%	79.47%	79.93%	80.33%	80.43%
$\lambda=0.9, \mu=0.1$	77.23%	78.43%	78.53%	78.33%	78.73%	78.93%

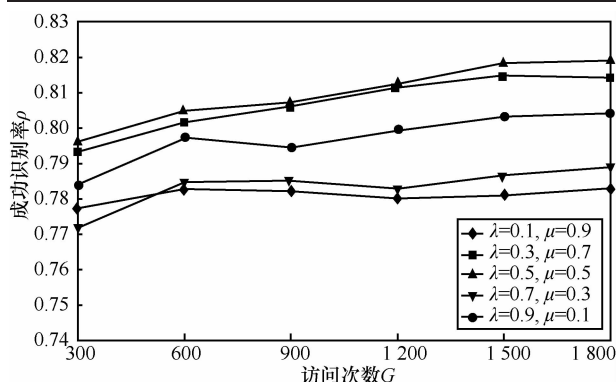


图 1 实验仿真结果

的直接信任值 $T(r_i, r_j)_D$ 和间接信任值 $T(r_i, r_j)_R$ 的影响力。从实验结果的数据中可以看出,在信任评估中,需要结合直接信任和间接信任两个因子,两者互为补充,缺一不可。

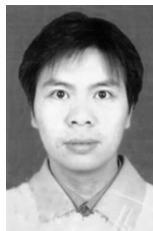
5 结束语

仿真实验结果表明,在本文的信任评估模型中,所考虑的交易因素关联关系是正确的,能起到正向的作用;对于整个模型来说,这些措施有助于提高整体网络的防御能力,提升网络的安全度;对于网络节点而言,通过本文的模型可以建立一个有效、判断正确的信任评估机制,而且本文的模型实现也不是很困难。综上所述,在 P2P 网络中,通过一定的算法可以判断来访节点的真实意图,能有效地拒绝恶意节点的入侵,保证 P2P 网络中正常信息交互的进行。

参考文献

- Lua E K, Crowcroft J. A survey and comparison of peer-to-peer overlay network schemes. IEEE Communications Survey and Tutorial, 2004(3):1~22
- Asnar Y, Zannone N. Perceived risk assessment. Proceedings of the 4th ACM Workshop on Quality of Protection (QoP'08), New York, USA, 2008: 59~63
- Singh A, Lilja D. Improving risk assessment methodology: a statistical design of experiments approach. Proceedings of the 2nd International Conference on Security of Information and Networks (SIN'09), New York, USA, 2009: 21~29
- Costa C, Soares V, Almeida J, et al. Fighting pollution dissemination in peer-to-peer networks. Proceedings of ACM Symposium on Applied Computing, Seoul, ACM Press, 2007:1586~1590
- Wang X F. On the policy description and quantification model for trust management. National University of Defense Technology, 2009
- Xiong L, Liu L. Peer trust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7):843~857
- Beth T, Borcharding M, Klein B. Valuation of trust in open network. Proceedings of European Symposium on Research in Security, Springer-Verlag, Brighton, 1994
- Wang Y, Vassileva J. Bayesian network trust model in peer-to-peer networks. Proceedings of the 2nd Int'l Workshop on Agents and Peer-to-Peer Computing, Springer-Verlag, Berlin, 2004: 23~34
- 常俊胜,王怀民,尹刚. 一种 P2P 系统中基于时间帧的动态信任模型. 计算机学报, 2006, 8(29): 1301~1307
- Huang C L, Hu H P, Wang Z Y. Modeling time-related trust. Proceedings of the 3rd International Conference on Grid and Cooperative Computing, Wuhan, China, 2004: 382~389
- Wang Y, Lin F. Trust and risk evaluation of transactions with different amounts in peer-to-peer e-commerce environments. Proceedings of IEEE International Conference on eBusiness Engineering(ICEBE'06), Shanghai, China, 2006: 102~109
- 王勇,云晓春,李奕飞. 对等网络拓扑测量与特征分析实例. 软件学报, 2008,19(4):981~992
- 韩正平,蔡凤娟. 网络安全信息关联分析技术与应用. 计算机应用研究, 2006, 23(10): 93~100
- 李景涛,荆一楠. 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
- 孟宪福,张磊,王旭. P2P 电子商务信任模型研究. 计算机应用研究, 2009, 26(8): 3067~3069

[作者简介]



张祖昶,男,南京邮电大学通信与信息工程学院工程师,主要研究方向为信息技术与决策支持系统。

王诚,男,南京邮电大学通信与信息工程学院副教授,主要研究方向为信息技术与决策支持。

(收稿日期:2013-06-01)