Journal of Computer Applications
计算机应用,2013,33(6):1612 - 1614
ISSN 1001-9081
CODEN JYIIDU
2013-06-01
http://www.joca.cn

文章编号:1001 - 9081(2013)06 - 01612 - 03
doi:10.3724/SP.J.1087.2013.01612

P2P 网络中基于权重因素的信任模型

陈珊珊*
(南京邮电大学 海外教育学院, 南京 210003)
(*通信作者电子邮箱 moist_css@163.com)

摘　要:针对 P2P 网络内部的安全问题,提出了一种 P2P 网络基于直接交易信任和推荐信任的模型,运用了直接交易信息参数、推荐信息的评价可信度和动态平衡权值参数,较简单准确地描述了节点的综合信任值,在进行交易前与目标节点建立信任关系,能有效抑制恶意节点对网络中其他节点的恶意交易行为和评价欺骗,提高网络交易的安全性。

关键词:直接信任;推荐信任;动态平衡权重;恶意
中图分类号:TP309　　**文献标志码**:A

Trust model based on weight factor in P2P network

CHEN Shanshan*
(*College of Oversea Education, Nanjing University of Posts and Telecommunications, Nanjing Jiangsu* 210003, *China*)

Abstract: According to the inner security issue of Peer-to-Peer (P2P) networks, a trust model based on direct transaction and recommendation in P2P network was proposed. Parameters of direct transaction information, rating confidence degree of recommendation information and dynamic balance weight were applied in the model. The model described peer's integration trust simply and accurately, and established trust relationship with target peer before transaction, which can restrain malicious peer to do malice behavior and rating cheat to other peers in the network, and improve the security of network trade.

Key words: direct trust; recommendation trust; dynamic balance weight; malice

0　引言

在 P2P 网络应用系统中,能查找并获得预期的资源是系统中的关键问题。文献[1-2]描述了 P2P 资源搜索的方法。本文研究节点基于信任进行资源选择的问题,用于处理网络中的节点自私行为和恶意行为,提高网络服务质量。根据社会网络[3]的概念和经典信任模型[4-7]的研究基础,本文提出一种新颖的信任系统 WeightTrust,更好地解决了信任模型计算过程中的权重问题。

1　相关研究

文献[8]在对以前研究进行归纳总结的基础上,提出了一种 P2P 文件共享系统的信任关系评估模型——PET,总体信任度(Overall Trust Degree, OTD)采用基于风险的直接信任和基于推荐的反馈信任耦合的方式得到,PET 模型首次将风险作为影响信任关系的要素之一引入可信性评估之中,但模型对信任随时间变化的动态属性也没有进行合理的建模。

针对现有的信任模型对反馈信息的有效聚合能力不足,文献[9]提出一个基于时间帧的动态信任模型 DyTrust,使用时间帧标示出经验和推荐的时间特性,引入近期信任、长期信任、累积滥用信任和反馈可信度 4 个参数来计算节点信任度。

文献[10]讨论了 P2P 信誉机制中反馈行为在信任评估中的作用,文献[11]研究了异构 P2P 网络中基于信誉的信任管理,文献[12]分析了分布式系统中基于信誉的信任威胁模型,文献[13]采用市场化方法管理 P2P 交易中存在的风险,文献[14]提出一种改进的信誉准确排名机制。

2　信任模型 WeightTrust

定义 1　直接信任值。

以节点 i 对目标节点 j 的动态历史交易经验作为影响因素,获得某个时间节点 i 对节点 j 的直接信任值。

定义 2　交易信息参数。

衡量此次交易信息(时间、价值)在双方交易历史上所占的权重以影响直接信任值的计算。

直接信任值的计算方法如式(1)所示:

$$TD_{i\to j}=\frac{1}{n}\sum_{k=1}^{n}\left(e^{-Time\left(t_{i\to j}^{(k)}\right)}\times Val\left(m_{i\to j}^{(k)}\right)\times TD_{i\to j}^{(k)}\right)\quad(1)$$

$TD_{i\to j}^{(k)}$ 是指第 k 次交易时节点 i 对节点 j 的直接信任值,$TD_{i\to j}^{(k)}\in[0,1]$,0 代表不信任,1 代表信任,初始直接信任值 $TD_{i\to j}^{(0)}=0.5$;

$Time\left(t_{i\to j}^{(k)}\right)$ 是指以时间为因素的交易信息参数,在对节点双方历史交易的处理时考虑参考此次交易的时间因素,这里定义为:$Time\left(t_{i\to j}^{(k)}\right)=\frac{t_{i\to j}^{(k)}-t_{i\to j}^{(k-1)}}{t_{i\to j}^{(k)}-t_{i\to j}^{(0)}}$。其中 $t_{i\to j}^{(0)}$ 为初始时间,时间越近的交易,在直接信任值计算过程中所占的权重越大。

$Val\left(m_{i\to j}^{(k)}\right)$ 是指以交易价值为因素的交易信息参数,在对节点双方历史交易的处理时参考此次交易的价值因素(交易数量或交易金额),这里定义 $Val\left(m_{i\to j}^{(k)}\right)=m_{i\to j}^{(k)}/\left(\sum_{k=1}^{n}m_{i\to j}^{(k)}\right)$,此次交易在历史价值因素方面所占的权重越大对直接信任值的影响越大。

收稿日期:2013-01-07;**修回日期**:2013-03-06。
基金项目:国家 973 计划项目(2011CB302903);国家自然科学基金资助项目(61272084)。
作者简介:陈珊珊(1980 -),女,安徽安庆人,副教授,博士,主要研究方向:计算机网络、信息安全。

定义 3　评价可信度。

参考其他节点对目标节点的推荐信任的同时必须参考推荐节点的自身推荐信任,以决定是否相信它的推荐。评价可信度是全局信任值计算的重要组成部分。

节点 i 从节点 p 获得对目标节点 j 的评价,节点 i 会对节点 p 给出的评价进行衡量,计算评价偏离程度以决定对目标节点 j 评价的权重。

设集合 $U_{p,i}$ 中的元素为与节点 i、节点 p 都交易过的节点,$num(U_{p,i})$ 为集合 $U_{p,i}$ 的大小,则评价的可信度 η_p 计算如下:

$$\eta_p = 1 - \frac{1}{num(U_{p,i})}\sum_{x\in U_{p,i}} |TD_{p\to x} - TD_{i\to x}|;\eta_p \in [0,1] \tag{2}$$

当 $num(U_{p,i}) = 0$,即节点 p 与节点 i 没有共同交易过的节点,令 $\eta_p = 0.5$。

考虑到在求评价可信度时,若是在一个小的网络,节点与节点之间的访问(交易)比较多,即集合 $U_{p,i}$ 元素个数不会很少甚至为零,所以上述的模型方法是可行的。但是若是大型的网络,节点与节点之间访问(交易)极少,此时的集合 $U_{p,i}$ 元素个数会经常为零,这对评价的比较造成了障碍。

此时,可以采用从全局角度进行评价可信的比较。例如,对节点 p,求其评价可信度时,把节点 p 评价交易过的节点都考虑进去,取其中一次评价如节点 p 对节点 y 的评价信任值 $TD_{p\to y}$,此时的比较对象不仅仅是 i 对 y 的评价,是全网络节点对 y 的评价,类似于式(2)通过取信任值之差、绝对值、累加并分析可得节点 p 的一次评价的公平度(偏离度),然后以此类推,评价节点 p 的每次评价综合可得节点 p 的评价可信度。

此种方法虽然计算复杂度计较大,但是对于大型网络尤其适用,由于考虑网络中所有的节点评价影响,可以抑制恶意节点的多种恶意行为(如联合诋毁、恶意夸大等)。

定义 4　全局信任值。

参考网络中其他节点对目标节点的推荐信任,通过其他节点评价可信度和推荐信任值综合计算出全局信任值。

设集合 V_j 为与节点 j 交易过的节点,即此集合中的元素评价过节点 j。全局信任值 T_j 计算方法见式(3):

$$T_j = \sum_{p\in V_j}(Val(m_{p\to j}) \times \eta_p \times TD_{p\to j}) \tag{3}$$

其中:$Val(m_{p\to j})$ 指节点 p 与节点 j 的交易中交易价值占与所有与 j 交易节点(V_j 中元素)交易价值总和的比例。

定义 5　综合信任值。

节点 i 对节点 j 的综合信任值根据双方的直接历史交易信息以及其他节点对节点 j 的推荐信任值来决定。

综合信任值 $G_{i\to j}$ 计算方法见式(4):

$$G_{i\to j} = \delta \times TD_{i\to j} + (1-\delta)T_j \tag{4}$$

其中:$TD_{i\to j}$ 为节点 i 通过与节点 j 的直接交易历史而积累的信任经验;T_j 为网络中与节点 j 交易过的节点的推荐综合得到的;δ 为平衡直接信任和推荐信任在综合信任中的权值,称为平衡权值,$\delta \in [0,1]$ 且可动态变化。

3　WeightTrust 模型的主要特点

1)信任值计算过程中参数的考虑较为全面,直接信任过程考虑了交易时间和交易价值参数,推荐信任过程考虑了评价可信度参数,综合信任值设置了直接信任的权重参数,可动态变化。

2)信任值的分布式存储,将直接信任值存储于本节点,只有网络中某个节点准备向目标节点获得服务前,计算目标节点的综合信任时,则需要从其他节点处获得目标节点的推荐信任,能有效解决分布式存储问题。

4　仿真实验

基于 Java 构建了一个适用于 P2P 网络的仿真平台来验证文中所提模型的有效性。其中:网络中有 1 000 个节点,拓扑结构任意生成,拓扑一旦生成在整个实验过程中不再发生变化;恶意节点比例由 10% 到 50% 不等,剩余节点均为善意节点;资源查询过程用泛洪的方式,每个节点有 5 个邻居节点,查询消息通过邻居节点向网络其他节点进行转发,查询消息的跳数为 3。网络中共有 100 种资源,每个节点拥有任意 5 种资源,善意节点收到查询消息后会检查自身拥有的资源,如果和查询资源相匹配,则向查询消息的节点发起响应,恶意节点无论是否有资源总是以虚假资源积极响应查询。平衡权值 δ 的初始值为 0.5,每个实验结果为 5 次实验的平均值。

实验 1　比较系统中随着恶意节点比例的增加,进行多次下载后的成功交易率的情况。

从图 1 可以明显看出,恶意节点的增加会在一定程度上影响系统的成功交易率,经过同样的交易次数后,系统中恶意节点的比例高则成功交易率低。但是由于该模型的使用,即使恶意节点的数量达到总节点数的 50%,系统进行 5 000 次交易后,成功交易率也有明显提升,达到 70% 以上,说明了该模型的有效性。

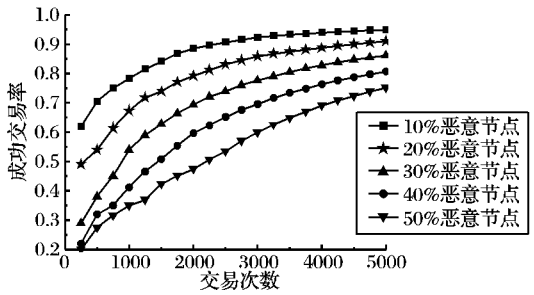

图 1　恶意节点的增加对成功交易率的影响

实验 2　WeightTrust 模型和 EigenTrust 模型[4] 中随着恶意节点数量的增加,网络中进行 100 000 次交易后,恶意交易概率的对比实验结果。

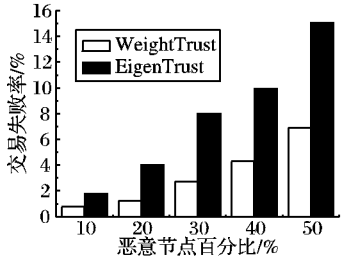

图 2　WeightTrust 和 EigenTrust 模型的恶意交易率比较

两种模型都能较好地抑制恶意交易发生率,恶意交易发生的比例都随着恶意节点的增加而增加,图 2 中显示,本文模型效果较好,即使有 50% 的恶意节点仍能将恶意交易发生率控制在 8% 以内。

实验 3　平衡权值 δ 的选择。

权值 δ 是动态的,这样能适应交易不断变化的规律,通过分析实际中,节点 i 在对节点 j 综合评价时,若节点 i 几乎没有和节点 j 交易过,此时双方直接的历史交易信息在分析综合评价时,已经是微不足道了,此时更倾向于依靠其他节点的反馈推荐;若节点 i 与节点 j 交易过很多次,双方的交互信息已经很丰富了,这个时候节点 i 更愿意相信自己历史中给节点 j 的信任评价,所以平衡权值 δ 受节点 i 与节点 j 交易次数的影响,即 δ 随交易次数的增多而则增大。

定义平衡权值 δ 为：

$$\delta = \frac{1}{1 + e^{-\left(\frac{x}{a}+b\right)}} \tag{5}$$

其中待定系数 a、b 可以根据需求改变，构造的平衡权值 δ 的变化曲线大体形状为 S 型，若设待定系数 $a = 8, b = -2.8$，此时函数曲线如图 3 所示。

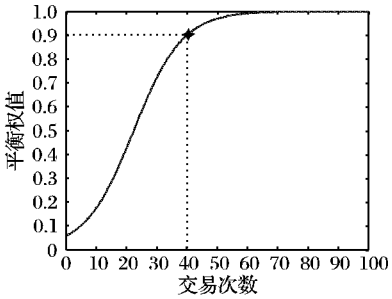

图 3 当 $a = 8, b = -2.8$ 时的平衡权值变化

从图 3 可以看出，当节点 i 和节点 j 的历史交易次数小于 5 次时，$\delta < 0.1$；当节点 i 与节点 j 的直接交易次数达到 40 次以上时，$\delta > 0.9$，此时综合信任值几乎取决于双方直接交互的历史，满足了平衡权值随直接交易次数而动态变化。

5 结语

本文模型提供了较为可靠的直接信任、推荐信任和综合信任服务，能处理节点的恶意行为和恶意推荐，节点还可以通过调整平衡权值来主观地定制个性化的综合信任服务。

参考文献：

[1] GKANTSIDIS C, MIHAIL M, SABERI A. Random walks in peer-to-peer networks: Algorithms and evaluation[J]. Performance Evaluation, 2006, 63(3): 241 - 263.

[2] MASSOULIÉL, le MERRER E, KERMARREC A M, *et al*. Peer counting and sampling in overlay networks: random walk methods [C]// Proceedings of the 25th Annual ACM Symposium on Principles of Distributed Computing. New York: ACM, 2006: 123 - 132.

[3] SABATER J, SIERRA C. Reputation and social network analysis in multi-Agent systems[C]// Proceedings of the 1st International Joint Conference on Autonomous Agents and Multiagent Systems. New York: ACM, 2002: 1 - 8.

[4] KAMVAR S, SCHLOSSER M, GARCIA-MOLINA H. The eigentrust algorithm for reputation management in P2P networks[C]// Proceedings of the 12th International Conference on World Wide Web. New York: ACM, 2003: 640 - 651.

[5] XIONG L, LIU L. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities [J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843 - 857.

[6] ZHOU R, HWANG K. PowerTrust: A robust and scalable reputation system for trusted peer-to-peer computing[J]. IEEE Transactions on Parallel and Distributed Systems, 2007, 18(4): 460 - 473.

[7] ZHOU R, HWANG K, CAI M. GossipTrust for fast reputation aggregation in peer-to-peer networks[J]. IEEE Transactions on Knowledge and Data Engineering, 2008, 20(9): 1282 - 1295.

[8] LIANG Z Q, SHI W S. PET: A personal trust model with reputation and risk evaluation for P2P resource sharing[C]// Proceedings of the 38th Annual Hawaii International Conference on System Sciences. Washington, DC: IEEE Computer Society, 2005: 201.

[9] 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[J]. 计算机学报, 2006, 29(8): 1301 - 1307.

[10] AZZEDIN F, RIDHA A. Feedback behavior and its role in trust assessment for peer-to-peer systems[J]. Telecommunication Systems, 2010(44): 253 - 266.

[11] CHU X, CHEN X, ZHAO K, *et al*. Reputation and trust management in heterogeneous peer-to-peer networks[J]. Telecommunication Systems, 2010, 44(3/4): 191 - 203.

[12] MARMOL F, PEREZ G. Security threats scenarios in trust and reputation models for distributed systems[J]. Computers & Security, 2009, 28(7): 545 - 556.

[13] ANDROUTSELLIS-THEOTOKIS S, SPINELLIS D, LOURIDAS P, *et al*. A market-based approach to managing the risk of peer-to-peer transactions[J]. Computer Networks, 2010, 54(5): 675 - 688.

[14] WANG Y, NAKAO A. Poisonedwater: An improved approach for accurate reputation ranking in P2P networks[J]. Future Generation Computer Systems, 2010, 26(8): 1317 - 1326.

(上接第 1611 页)

进行改进。通过将图分为敏感区和非敏感区对社会网络进行扰动，排除无效扰动提高了网络的隐私保护程度；通过灵活运用谱约束条件调整扰动次序，比较前一次扰动后图与原始图的两个谱的大小选择合适的边进行扰动，而不是机械地轮流同时变大和变小，提高了扰动后社会网络数据的可用性。

参考文献：

[1] YING X W, WU X T. On link privacy in randomizing social networks[C]// Pacific-Asia Conference on Knowledge Discovery and Data Mining. Berlin: Spring-Verlag, 2009: 28 - 39.

[2] LIU K, TERZI E. Towards identity anonymization on graphs[C]// Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data. New York: ACM, 2008: 93 - 106.

[3] YING X W, WU X T. Randomizing social networks: a spectrum preserving approach[C]// Proceedings of the 8th SIAM Conference on Data Mining. Atlanta: SIAM, 2008: 739 - 750.

[4] 强小强，何小卫，韩建民，等. 基于谱约束的随机化社会网络多点扰动方法[J]. 计算机工程, 2011, 37(9): 98 - 103.

[5] 徐黎明，强小强，宋转. 谱半径和特征显著性约束的随机化社会网络方法[J]. 计算机应用, 2012, 32(2): 485 - 488.

[6] ZHOU B, PEI J. Preserving privacy in social network against neighborhood attack [C]// Proceedings of the 24th IEEE International Conference on Data Engineering. Washington, DC: IEEE Computer Society, 2008: 506 - 515.

[7] SWEENEY L. K-anonymity: a model for protecting privacy[J]. International Journal on uncertainty, Fuzziness and Knowledge-based System, 2002, 10(5): 557 - 570.

[8] ZHELEVA E, GETOOR L. Preserving the privacy of sensitive relationships in graph data[C]// Proceedings of the 1st ACM SIGKDD International Conference on Privacy, Security, and Trust. New York: ACM, 2008: 153 - 171.

[9] 兰丽辉，孙英慧，鞠时光. 社会网络发布中敏感边的隐私保护[J]. 吉林大学学报, 2011, 29(4): 323 - 330.

[10] ZOU L, CHEN L, ÖZSU M T. K-Automorphism: General framework for privacy reserving network publication[J]. Proceedings of the VLDB Endowment, 2009, 2(1): 946 - 957.

[11] 王兴科. 某些图的谱半径与代数连通度[D]. 青岛: 中国石油大学, 2009.

[12] CVETKOVIC D, ROWLINSON P, SIMIC S. Eigenspaces of graphs[M]. Cambridge: Cambridge University Press, 1997.

[13] SEARY A J, RICHARDS W D. Spectral methods for analyzing and visualizing networks: an introduction[EB/OL]. [2012-10-20]. http://www.sfu.ca/~richards/Pages/NAS.AJS-WDR.pdf.

[14] NEWMAN M E J, GIRVAN M. Finding and evaluating community structure in networks[J]. Physical Review E, 2004, 69(2): 026113.

[15] COSTA L F, RODRIGUES F A, TRAVIESO G, *et al*. Characterization of complex networks: A survey of measurements[J]. Advances in Physics, 2007, 56(1): 167 - 242.