文章编号:1674-7070(2010)04-0328-04

P2P 信任管理模型的公平性研究

陈祥云[1]　陈珊珊[1]

摘要

在众多相关文献中,P2P 信任管理模型设计更多考虑效率,抵抗恶意攻击性等方面,而"公平性"作为影响网络整体性能提高的重要因素却没有得到重视. 将影响公平性的行为分类,着重考虑"非恶意行为"所造成的"隐性不公平",最后通过仿真验证了信任管理模型可以在实现负载均衡的同时达到降低无效下载次数的目的.

关键词

P2P;信任管理;公平性

中图分类号 TP39

文献标志码 A

0　引言

Introduction

目前 P2P(Peer-to-Peer)网络得到迅速发展,不同于 C/S(客户端/服务器)结构,网络中所有节点地位平等,参与节点既可以是服务的提供者也可以是消费者,但由于资源可以轻易地发布和得到,给那些恶意代码的传播提供了机会,因此 P2P 网络在给用户带来便利的同时,也存在着严重的安全隐患. P2P 信任管理技术的思想是模仿现实社会中的信任建立过程,根据用户之间过去发生的交易行为及其参与节点的反馈信息,对网络中的每个节点给出一个"可信程度"的评价,节点在请求服务时可以根据此评价值来选择"可信"的服务提供者. 目前评价信任管理系统的标准主要集中在通信量代价、可扩展性、高可信性、激励性和惩罚性等方面. 本文认为建立信誉机制的最终目的是通过增加网络整体吞吐量和提供服务的多样性来提高用户的满意度,而公平性对网络整体性能的提高及未来可持续发展都具有重要意义,因此有必要将公平性作为衡量信誉机制优劣的重要指标. 本文将影响公平性的行为分类,着重考虑"非恶意行为"所造成的隐性不公平现象,最终提出了一种公平的信任管理模型.

1　影响信任管理公平性的行为

The behaviors affecting fairness in trust management

公平理论又称社会比较理论,它是美国行为科学家斯塔西亚当斯在《工资不公平对工作质量的影响》、《社会交换中的不公平》等著作中最先提出的. 该理论的基本要点是:人们总会自觉或不自觉地将自己付出的劳动代价及其所得到的报酬与他人进行比较,并对公平与否做出判断,由此产生的公平感将直接影响职工的工作动机和行为.

公平并非一般意义上的平等,公平性追求的目标是让整个组织达到一种和谐,每个成员都愿意为集体贡献自己的资源潜力,这与 P2P 网络的初衷是完全一致的. 在网络中,不同努力程度的节点应该有不同的信誉值,这是公平性的内在要求,但是如果同一网络环境中,两个节点拥有相似的服务和主观诚信度,却在长时间具有不同的交易量和信誉评估值,这就成为信誉机制中的"不公平"现象. 显而易见的是恶意行为必然造成信誉管理的不公平性,通过对网络中的节点行为分析发现,有些"非恶意行为"也会对网络的公平性产生影响.

收稿日期 2010-03-11

资助项目 江苏省研究生创新工程项目(CX07B_109z);国家自然科学基金(60873231);江苏省自然科学基金(BK2009426)

作者简介

陈祥云,男,硕士生,研究方向为计算机通信与网间互联. nopains@126.com

1　南京邮电大学　计算机学院,南京,210003

1.1 非恶意行为对网络公平性的影响

1)节点选择不对所接受的服务做出评价.如某个节点的信誉值很高,其他节点与其交易时将考虑到此节点的"报复性评价"将对自己造成的影响,故选择对其恶意行为不评价,长此以往,该节点的负面评价信息将会缺失.

2)"小社区"内部长期合作节点互相给出高评.一些节点之间具有长期交易行为,节点之间会由于这种长期合作而给对方大量"好评",这种基于"面子"的评价信息不利于对节点的进一步的激励.

3)主观性评价倾向造成反馈信息的不公平.由于评价的主观性,某些节点的所给评价始终高于其他节点的评价,这些节点的交易伙伴比网络中的其他节点信誉值提高更快.

4)长尾现象[1].拥有冷门稀有资源的节点因为提供服务的机会较少,跟拥有热门资源的节点相比缺少激励措施,而稀缺资源本身对于提高整个网络服务的多样性非常重要.

5)超级节点的存在(将在下文做详细分析).

1.2 超级节点存在对网络公平性的影响

公平理论将基于公平的比较分为水平比较和纵向比较,水平比较指当事人与其他人进行比较,纵向比较指当事人将自己目前的状况与过去的状况比较,本文将利用比较理论对超级节点存在的情况进行分析.

网络中的信誉机制的发展跟社会网络非常相似.在网络初期,节点之间进行自由竞争,经过一段时间的发展,超级节点(信誉大量集中在少数这些节点身上)开始出现,这种"垄断"对整个网络的发展不利.这里所说的超级节点不同于混合式 P2P 网络结构中的具有性能上优势的节点,本文中所考虑的 P2P 网络环境中每个节点的地位是均等的,超级节点的出现指的是信誉资源过分集中在少数节点身上的现象.

1)由于超级节点的绝对"发展优先权"将会影响新节点的加入和当前网络中普通节点的参与积极性.信誉这种资源大量集中在某些节点身上将会出现"富者逾富,信誉高者更高"现象,普通节点因为自身的信誉值比较低,因此在大多情况下即使响应服务请求也不会得到提供服务的机会,如果这种"不公平性"超过了节点的忍受程度,网络中的普通节点会因为发展的困难导致心理上的"不公平",而停止上传资源或者选择对超级节点实施"坏嘴攻击"(多个恶意节点同时对一个节点给出不公正的评价);新节点的加入也会出现缺乏机会而面临更为严峻的"冷启动"问题.

2)"超级节点"将失去进一步提高服务质量的激励.因为信誉的增加是一个过程,同时信誉的削减也需要一定时间,所以节点即使无法(或不再愿意)提供与其信誉相称的服务时,由于大量节点总是选择高信誉节点交互,其信誉却可以在一定时间内维持原来相近的水平.

3)超级节点成为网络瓶颈,不利于网络的整体性能提高.这些超级节点将成为网络交互最为频繁的地方,这不符合网络的负载均衡要求;由于"超级节点"的地位在网络中的地位提高,其服务质量却没有提高,这必然引起网络整体性能下降;超级节点具有最高的"攻击性价比",这将使得它们将成为网络主要的安全隐患.

2 公平的信任模型设计

The design of fair trust model

对恶意行为的防范在诸多文献[2]中已经有所涉及,本文所做的工作在于消除非恶意行为导致的不公平性.i 对 j 的最终信任值计算为

$$T_{ij} = \alpha \times T_{ij}^{\mathrm{dir}} + (1-\alpha) RT_j.$$

下面将对公平信任模型的直接信任和推荐信任的计算分别进行阐述.

2.1 直接信任值计算

1)节点之间没有先前交互行为

简单地将没有发生过交易的节点直接信任初始值设置为 0 将会导致"冷启动"的问题,而设置为 0.5 则可能导致"女巫攻击",且这两种设置都缺乏动态性[3].本文认为初始值的设定与网络的应用环境,节点本身的要求以及目前网络中的普遍信誉值有关.设 SP 表示服务提供者,SR 表示服务请求者,φ 指用户自身要求的安全系数,由用户自己设定的 SL_i 表示网络安全要求,$SL_{\max}$ 表示 SL_i 的最大值.ψ 表示安全因素:$\psi = 1 - \dfrac{(SL_i - 1) \times \varphi}{SL_{\max}}$.$t$ 是 SR 在网络中随机选择的 n 个节点的信誉平均值,默认的 SP 信誉值计算 $T_{\mathrm{default}}^{\mathrm{dir}} = t \times \psi$.

2)节点间有历史交互行为

将没有反馈评价信息的行为定义为"隐式差评"[4].设节点 j 接到 i 的好评次数为 m^+,差评次数为 m^-,没有评价信息的次数为 m^*,i 对 j 的直接信誉值

$T_{ij}^{\mathrm{dir}} = \dfrac{m^+}{m^+ + \alpha m^* + (1+\beta)m^-}$,其中 $0 \leqslant \alpha, \beta \leqslant 1$.

2.2 推荐信任值计算

为了消除信誉评价的主观性所引起的偏颇,本文引入了“主观评价倾向”[4]概念: $E_k = \overline{R_k} - \overline{R_{\mathrm{a}}(k)}$. 其中 $\overline{R_k}$ 是从 k 给出的所有评价的平均值, $\overline{R_{\mathrm{a}}(k)}$ 是所有其他节点对那些与 k 交易过的节点的评价的平均值. 由于 k 节点在评价中倾向于给出偏高(或偏低)评价,因此在执行推荐信誉计算时应该消除这种“主观偏颇”,其中 w_k 是节点 k 的推荐权值 $RT_j = \sum_{k \in Q} w_k \times (T_{kj}^{\mathrm{dir}} - E_k)$.

假设与节点 i 和节点 k 都有过交易的节点组成一个有 n 个节点的集合 P,可将节点 i、k 对这 n 个节点的直接信任值节点 i 的 n 维向量 $(T_{i1}^{IJ}, T_{i2}^{IJ}, \cdots, T_{in}^{IJ})$ 和节点 j 的 n 维向量 $(T_{k1}^{IJ}, T_{k2}^{IJ}, \cdots, T_{kn}^{IJ})$ 分别看作是这个 n 维空间的一个向量,这样两个节点之间的相似程度可以用向量的夹角余弦值来度量,值越大相似程度越高,说明 k 作为推荐者的可靠性越高[6]:

$$C_{ik} = \cos\theta_{ik} = \frac{\sum_{t=1}^{n} T_{it}^{\mathrm{dir}} \times T_{kt}^{\mathrm{dir}}}{\sqrt{\sum_{t=1}^{n} T_{it}^{\mathrm{dir}} \times \sum_{t=1}^{n} T_{kt}^{\mathrm{dir}}}}.$$

其中 w_k 计算公式如下:

$$w_k = \frac{C_{ik}}{\sum_{t \in P} C_{it}}.$$

2.3 信任值更新阶段

在信任值的更新阶段本文主要考虑如何消除小社区,低信誉节点缺乏服务机会和长尾现象等 3 方面的不公平因素:

1) 对交易的评价分为深度和广度,降低超级节点信誉的过快增长速度和“小社区”的影响. 对节点信誉增长进行简单的限制将会使受限制节点产生不公平感,本文采取将信誉“二维化”的方法来减缓超级节点信誉的过快增长速度. 深度(TD)体现了某个节点 i 与其他节点之间重复交易次数的最大值,而广度(TB)表示该节点与多少个不同节点有过交易. TD 体现了该节点被其他节点的认为的可靠程度,TB 则体现了在整个网络中该节点被接受的广泛程度. 当节点 i 与新节点发生成功交易后 TD 增加,则 $m_{\mathrm{new}}^+ = m^+ + \varepsilon$;如果 TB 增加,则 $m_{\mathrm{new}}^+ = m^+ + \lambda$,其中 $\lambda + \varepsilon = 1$;其余情况下,$m_{\mathrm{new}}^+ = m^+ + 1$.

2) 增加对资源请求发出响应的节点信誉值. “响应”也是节点对网络贡献的一种表现,响应节点的多少决定了网络的吞吐量,同时也给请求者提供了更多的选择余地,还可以降低“低信誉者”的饥渴状态,提高节点延长在线提供服务的时间的积极性. 每次 SR 发起请求时,记录那些响应节点,即使没有被选择为服务节点,仍然对其好评进行较小的增加, $m_{\mathrm{new}}^+ = m^+ + 0.1$. 由于增加量很小,该节点有任何恶意行为都将会抵消这种信誉的增加,因此不用担心节点里可能会利用机会来骗取信誉值.

3) 降低稀缺资源成功下载次数的评价权重,增加在线提供服务时间的权重达到消除“长尾现象”的目的. 设 p 是该资源在线时间与一般受欢迎程度资源的下载间隔时间的比值, σ 表示在线时长的评价权重, δ 表示成功提供一次服务的权重,则 $m_{\mathrm{new}}^+ = m^+ + \sigma p + \delta$.

3 仿真分析
Simulation and analysis

本文设计了一个虚拟的网络平台来模拟 P2P 文件共享,系统共生成 8 个节点,每个节点拥有 3 个邻居节点,每个节点被随机分配 10 个资源,其中被设置为恶意的成员总是不提供正常的服务,参数 TTL 为 6. 每次实验中随机选择 1 个节点发出 50 次服务请求,服务成功次数 m_{s},实验的恶意下载率为 $1 - m_{\mathrm{s}}/50$,每个节点所提供服务的次数与整个网络所提供的服务的比值定义为该节点的负载率. 使用同样的场景设置,本文还模拟了 EigenTrust 信任模型[6],并对它们进行了比较分析. 仿真结果表明,公平性因素的加入在实现负载均衡(图 1)的同时降低了恶意下载率(图 2),从而表明新模型对节点行为的评价更为公正准确.

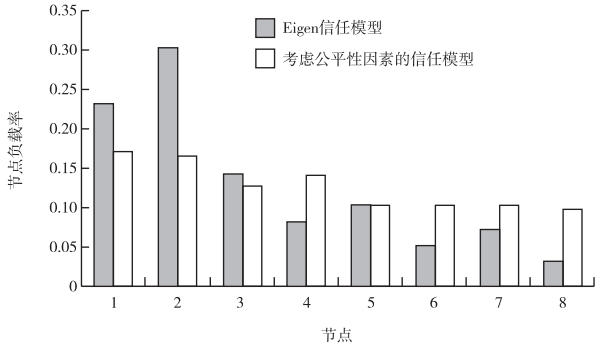


图 1 节点负载率

Fig. 1 Node load factor

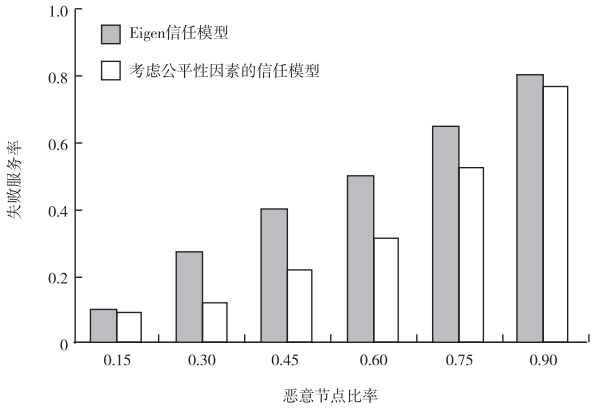


图2 失败下载率

Fig. 2 Rate of download failure

4 结束语

Conclusions

信誉管理网络中的情形与社会网络非常相似,网络的健康可持续发展与公平性有重要关系. 结合P2P网络应用环境的特点,并借鉴社会学和心理学的相关理论构建一个公平的信任管理模型将是下一步的工作.

参考文献

References

[1] Dellarocas C. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior[C]//Proceedings of the 2nd ACM Conference on Electronic Commerce. Minneapolis,USA,2000:150-157

[2] Xiong L, Liu L. PeerTrust: Supporting reputation-based trust in peer-to-peer communities[J]. IEEE Transactions on Data and Knowledge Engineering(Special Issue on Peer-to-Peer Based Data Management),2004,16(7):843-857

[3] Quercia D, Hailes S, Capra L. TRULLO-local trust bootstrapping for ubiquitous devices[C]//In Proceedings of the 4th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Philadelphia, Pennsylvania, USA, 2007:1-9

[4] Wierzbicki A. The case for fairness of trust management[J]. Electronic Notes in Theoretical Computer Science, 2008, 197(2): 73-89

[5] Cho J, Kwon K, Park Y. Q-rater: A collaborative reputation system based on source credibility theory[J]. Expert Systems with Applications, 2009, 36(2): 3751-3760

[6] Kamvar S, Schlosser M, Garcia-Molina H. The eigen trust algorithm for reputation management in P2P networks[C]//Proceedings of the 12th WWW Conference. Budapest: ACM Press, 2003: 640-651

Study of the fairness on P2P trust management model

CHEN Xiangyun[1] CHEN Shanshan[1]

1 School of Computer, Nanjing University of Posts & Telecommunications, Nanjing 210003

Abstract Among the relevant literatures, efficient and effective block to malicious attacks is considered more by P2P trust model designers than "fairness", which is an important factor in improvement of the overall web performance. This paper classifies the behaviors affecting fariness in trust management, and focuses on hiden unfairness caused by unmalicious acts, then proposed a trust model. The simulation results show that this model can achieve load balancing while reducing the rate of malicious download.

Key words P2P; trust management; fairness