

P2P 系统中基于声誉的信任评估机制

王 亮, 郭亚军

WANG Liang, GUO Ya-jun

华中师范大学 计算机科学系, 武汉 430079

Department of Computer Science, Huazhong Normal University, Wuhan 430079, China

E-mail: wangliang@mails.ccnu.edu.cn

WANG Liang, GUO Ya-jun. Reputation-based on trust evaluation mechanism for P2P system. Computer Engineering and Applications, 2009, 45(15): 136-138.

Abstract: P2P system can enable the nodes that are strangers to one another to make online transactions with each other, but the problem of security is attracting more and more people's attention. Hence, how to construct an effective trust mechanism to help build trust among the nodes is an important issue for the research of P2P technology nowadays. This paper proposes a novel reputation-based trust evaluation mechanism for P2P system. This mechanism takes into account the comprehensive factors affecting the trust level, improves the calculation methods of the local reputation and global reputation, reduces the computing load of the trust level, and introduces the blacklist mechanism into P2P system. The experiment result shows that this proposed mechanism can effectively evaluate the trust level of node and detect and separate the malicious nodes from P2P system to improve the rate of successful transaction, and can be effectively applied to P2P system.

Key words: P2P (Peer to Peer) system; reputation; trust mechanism

摘 要: P2P 系统能够使陌生节点之间进行在线交易, 但安全问题越来越受到人们的关注。因此, 如何在 P2P 系统中构建一个有效的信任机制来帮助在节点之间建立信任是目前 P2P 技术研究的一个热点。提出了一种新的 P2P 系统中基于声誉的信任评估机制, 该机制较全面地考虑了影响信任度的因素, 改进了局部声誉与全局声誉的计算方法, 降低了信任度的计算负载, 并且引入了黑名单机制。实验结果表明, 该机制能有效地评估节点的信任度, 识别和隔离恶意节点, 提高系统交易成功率, 并能有效地应用于 P2P 系统中。

关键词: P2P 系统; 声誉; 信任机制

DOI: 10.3778/j.issn.1002-8331.2009.15.039 **文章编号:** 1002-8331(2009)15-0136-03 **文献标识码:** A **中图分类号:** TP393

1 引言

P2P 系统的不断普及促进了电子商务、文件共享、即时通信等新技术的发展。在 P2P 系统中, 节点既是消费者也是服务者, 它们能随意地加入和离开系统, 并能匿名地进行交易。然而, 由于在 P2P 系统中没有一个中心权威来监督和管理节点的行为, 这就为在节点之间建立信任提出了挑战。服务请求方需要服务提供方能够提供诚信服务以及不泄露有关服务请求方的私人或敏感的信息; 服务提供方需要信任服务请求方能够回报服务(例如, 购买某种商品、文件共享等等)。虽然 P2P 系统具有动态性和开放性, 方便了实体之间的交易, 但即使在线交易能够提供一个几乎匿名的中介, 与现实的交易相比, 人们更加容易被欺骗, 这是因为恶意节点能够进行欺诈等破坏系统安全的恶意行为, 从而使用户蒙受损害。因此, 如何在 P2P 系统中的节点之间建立起信任关系, 让双方互相知晓, 并评估它们交易的风险是目前 P2P 技术研究的一个热点。

最近的研究表明^[1-3], 基于声誉的信任机制可以有效地识别恶意节点并避免恶意行为。目前, 基于声誉的信任机制提出了很多, 下面我们分析一些现有比较典型的基于声誉的信任机制: Kamvar 等人^[4]提出了 P2P 环境下基于全局声誉的信任模型 EigenRep。EigenRep 通过邻居节点间的满意度的迭代来获取节点的可信度。在无恶意节点的网络中, 该模型可以较好地反映出节点的真实行为, 但该模型存在着收敛性问题, 且具有较高的计算和通信代价。窦文等人^[5]在迭代收敛性和模型安全性方面对 EigenRep 进行了改进, 但改进后的模型不易实现, 具有较高的计算和通信代价。Song 等人^[6]提出了基于模糊逻辑推理规则来计算节点的全局声誉的 FuzzyTrust 信任模型。该模型具有较高的恶意节点检测率, 但计算代价和通信代价比较高, 而且该模型没有考虑影响信任评价的各种信任因素, 也没有对模型的收敛性进行论证。袁巍等人^[7]提出了一个基于局部声誉的信任模型 HBDTM, 但该模型没有给出交易时间影响因子的确定

基金项目: 中国博士后基金(China Postdoctoral Science Foundation No.20070410953); 湖北省教育厅科技基金(Educational Committee of Hubei Province Foundation No.B20084002); 武汉市教育局科研基金(Wuhan Education Bureau Foundation No.200765)。

作者简介: 王亮(1982-), 男, 硕士生, 研究领域为信息安全、可信网络等; 郭亚军(1965-), 男, 博士后, 副教授, 研究领域为信息安全、可信网络等。

收稿日期: 2008-03-31 **修回日期:** 2008-06-17

方法且模型本身抗攻击能力较差。在分析了上述现有的基于声誉的信任机制所存在的一些问题的基础上,提出了一种新的P2P系统中基于声誉的信任评估机制。

2 信任评估机制

在人类社会中,人们常常基于信任进行交互,人们是通过自身的直接交互历史或者其他人的推荐来建立起彼此之间的信任,人们之间的信任是通过长期积累而形成的,即信任是动态的,累积的。因此,根据人类交互行为,一个节点的信任度取决于两个方面:节点自身的直接交易历史和其他节点的推荐,即节点的局部声誉和全局声誉。综合这两个方面,定义节点信任度的计算公式为:

$$T(i,j,t)=\alpha D(i,j,t)+\beta R(j,t), \quad \alpha+\beta=1 \text{ 且 } \alpha,\beta \geq 0$$

其中, $T(i,j,t)$ 表示在当前时刻 t 时节点 i 对节点 j 的信任度, $D(i,j,t)$ 和 $R(j,t)$ 分别表示在当前时刻 t 时节点 i 对节点 j 的直接信任度(节点 j 的局部声誉)和节点 i 从其他推荐节点获得的对节点 j 的推荐信任度(节点 j 的全局声誉), α 和 β 分别表示局部声誉权重系数和全局声誉权重系数,其值可根据用户所需的具体策略来制定。在计算出节点 j 的信任度后,节点 i 需要设置一个信任阈值 δ ,当 $T(i,j,t) \geq \delta$ 时,则在最近的时间段 t 内节点 i 信任节点 j ;反之,当 $T(i,j,t) < \delta$ 时,则在最近的时间段 t 内节点 i 不信任节点 j ,用户可根据自己的信任策略来制定信任阈值。

2.1 局部声誉

局部声誉(直接信任度)是节点 i 对节点 j 历史行为的观察或评价信息而得出的对节点 j 未来行为的期望。节点之间的信任度会随着交易的好坏、时间、环境的变化而变化。好的交易能够提高节点的信任度;相反,坏的交易则会降低节点的信任度。此外,在不同的时间和环境下的信任度是不同的。因此,在局部声誉计算中,引入了以下四个重要参数:

(1)交易次数:双方交易的次数越多,那么双方越对对方熟悉,就越容易在双方之间建立起信任。

(2)交易满意度:在每次交易完成之后,双方各自给出对此次交易的满意度。

(3)交易环境满意度:双方对此次交易所处的环境(例如:网络的稳定性、防火墙安全强度、加密技术等)的满意度。

(4)交易时间:距离当前时刻越近的交易行为越能比较真实地反映出节点的近期行为,从而对声誉影响就越大;反之,交易的时间距离当前时刻越远,对声誉的影响就越小^[9]。

在当前时刻 t 时,节点 i 对节点 j 的直接信任度的计算公式定义如下:

$$D(i,j,t)=\frac{\sum_{k=1}^{I(k)} S(i,j,t_k)E(i,j,t_k)\varphi(t_k)}{I(k)} + \sum_{k=1}^{I(k)} f(k)e^{-\frac{1}{n}}$$

这个公式由两部分构成:第一部分是在时间段 t 内,节点 i 对节点 j 的总评价的平均值与矫正系数的乘积,其中 $\sum_{k=1}^{I(k)} S(i,j,t_k)E(i,j,t_k)\varphi(t_k)$ 是利用时间衰减因子对历次节点 i 对节点 j 的交易评价进行衰减后得到的交易评价期望,即交易评价总和;第二部分是在时间段 t 内,节点 j 每次交易失败后的惩罚值的总和。该公式各项具体的定义如下所示。

$I(k)$:节点 i 与节点 j 在时间段 t 内的交易总次数。

r :矫正系数, $r=\sqrt{I(k)/(I(k)+1)}$ 。在历史交易次数很少或等于零时,节点的局部声誉可能很快就达到较高的值。这样,恶意节点就可以在一开始伪装成诚实的节点,等积累到一定声誉后就开始进行欺骗。因此,为了防止一些恶意节点通过少量的成功交易来抬升声誉,引入了矫正系数 r 。通过矫正,节点只有通过多次获得好的评价才能得到较高的声誉。

$S(i,j,t_k)$:在时刻 t_k 时,节点 i 对节点 j 此次交易的交易满意度,取值区间为 $[0,1]$,其交易满意度评价等级如表1所示。

表1 交易满意度评价等级表

$S(i,j,t_k)=0$	完全不信任(交易失败)
$0 < S(i,j,t_k) < 0.5$	不太信任
$S(i,j,t_k)=0.5$	不确定
$0.5 < S(i,j,t_k) < 1$	一般信任
$S(i,j,t_k)=1$	完全信任

$E(i,j,t_k)$:在时刻 t_k 时,节点 i 对节点 j 此次交易所处的环境的交易环境满意度,其取值与交易满意度相同。

$\varphi(t_k)$:时间衰减函数, $\varphi(t_k)=e^{-\lambda(t-t_k)}$,其中 $\lambda > 0$ 且 $\lambda \in R$, λ 为时间衰减系数,其值可根据用户所需的具体策略来制定。

$f(k)e^{-\frac{1}{n}}$:交易失败后的惩罚项,其中

$$f(k)=\begin{cases} -1 & \text{第 } k \text{ 次交易失败} \\ 0 & \text{第 } k \text{ 次交易成功} \end{cases}, e^{-\frac{1}{n}} \text{ 为惩罚因子, } n \text{ 是失败的次数}$$

当出现交易失败时,惩罚因子会使节点的信任值迅速下降,这使得节点在获得较好的声誉后不会轻易做不诚实的交易,并使恶意节点为积累声誉付出更大的代价;同时由于惩罚值随着 n 的增大而增大,是一条单调递增的向上凸的曲线(如图1所示),从而可以防止因一两两无意的交易失败而导致惩罚过重的现象出现。

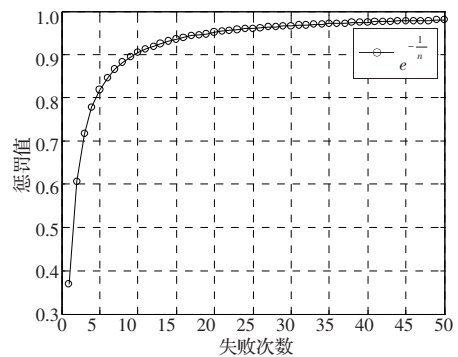


图1 惩罚因子函数曲线图

2.2 全局声誉

节点 j 的全局声誉(推荐信任度)是根据节点 j 的推荐节点对 j 的评价而得出的对 j 的推荐信任度。

节点 j 的全局声誉与下列因素有关:

(1)节点 j 的推荐节点数目:推荐节点的数目越多,则 j 的全局声誉越准确,但如果推荐节点与全局声誉的计算无关,则不能准确地反映 j 的全局声誉,并很有可能有一些恶意节点会通过共谋来抬升彼此的声誉,从而欺骗用户,使用户遭受损失^[9]。

(2)节点 j 的推荐节点对 j 的直接信任度:节点 j 的推荐节点对 j 的直接信任度越大,则对 j 的全局声誉影响就越大。

(3)节点 j 的推荐节点对 j 的信任评价权重:节点 j 的推荐节点对 j 的信任评价权重越高,则节点 j 越可信;反之,则节点 j

越不可信。

在当前时刻 t 时, 节点 j 的全局声誉计算公式定义如下:

$$R(j, t) = \frac{\sum_{i=1}^{|C(j)|} Wv_i \times D(v_i, j, t)}{|C(j)|}, v_i \in C(j)$$

这个公式计算是节点 j 的所有推荐节点对 j 的总评价的平均值, 即节点 j 的全局声誉, 其各项具体的定义如下: $C(j)$ 是节点 j 的推荐节点的集合, $|C(j)|$ 是推荐节点的总个数, v_i 是 j 的一个推荐节点。

Wv_i : v_i 对 j 的信任评价权重, 影响 Wv_i 的因素: 推荐节点 v_i 对 j 的交易满意度和交易时间, 其变化规则如下: (1) 如果交易满意度越高且交易时间很新, 那么权值就很大; (2) 如果交易满意度越低且交易时间很旧, 那么权值就很小。 Wv_i 计算公式定义如下:

$$Wv_i = e^{-1/\sum_{k=1}^{I(k)} S(v_i, j, t_k) \varphi(t_k)}$$

其中 $\sum_{k=1}^{I(k)} S(v_i, j, t_k) \varphi(t_k)$ 是通过时间衰减因子对历次推荐节点 v_i 对节点 j 的交易满意度进行衰减后得到的交易满意度期望。

需要指出的是, 节点 j 的推荐节点只选取与 j 有直接交易历史的邻居节点。之所以只选取与 j 有直接交易历史的邻居节点来计算节点 j 的全局声誉是基于以下两个原因: (1) 降低全局声誉的计算负载。因为, 在一些模型中, 节点的全局声誉是通过多个中间节点传递推荐来得到的, 这就势必会增加计算负载, 但本计算方法不考虑中间节点的传递推荐, 从而使计算的负载要小得多; (2) 为了防止与节点 j 无关的推荐节点进入到节点 j 的全局声誉的计算中, 从而避免一些恶意节点对节点 j 进行诋毁、夸大或共谋行为。

2.3 黑名单机制

在 P2P 系统中, 引入了黑名单机制。一旦发现恶意节点, 恶意节点就会被记录在黑名单内, 在以后的交易中节点就不会与恶意节点进行任何交易, 这样就可以有效地过滤和隔离恶意节点, 从而营造一个良好的交易环境。

设 B_i 为节点 i 的黑名单, 用于记录在节点 i 看来的恶意节点。例如在节点 i 和节点 j 的交易中, 如果节点 i 认为节点 j 对自己造成了损害, 那么节点 i 就将 j 的 ID 和 IP 地址加入 B_i 相应的数据结构中, 在以后的交易中, 节点 i 将不再与节点 j 进行任何交易, 如图 2 所示。

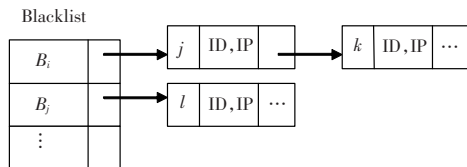


图 2 黑名单

3 仿真实验

对提出的信任评估机制进行了模拟仿真实验。节点的交易方式为文件下载, 仿真实验的硬件环境为 CPU: Intel Pentium 820D, 内存 2 GB, 仿真软件为 Matlab 7.1。仿真系统中参数的默认值如表 2 所示。

在模拟仿真的 P2P 系统中有两种类型的节点: 一类是诚信节点, 诚信节点能提供诚信交易, 在系统中具有良好的行为, 因此, 诚信节点的信任度和交易成功率都比较高; 另一类是恶意节点, 在 P2P 系统中进行一些破坏系统安全性的恶意行为, 例

表 2 系统参数默认值表

参数	参数说明	默认值
α	局部声誉权重系数	0.6
β	全局声誉权重系数	0.4
λ	时间衰减系数	1.0
δ	信任阈值	0.5

如提供带有病毒的文件、恶意广告、虚假文件等等, 从而严重地影响了系统的性能, 因此, 恶意节点的信任度和交易成功率都很低, 并且最有可能进入黑名单, 也最容易从系统中隔离出去。

实验考察了无信任机制的 P2P 系统和带有本文的信任评估机制的 P2P 系统在随着恶意节点比例增多时, 各自交易成功率变化的对比情况, 如图 3 所示。在实验中, 没有考虑因网络故障造成不能提供下载的文件。设定所有加入系统的节点的初始信任度为 0.5, 观察的节点总个数为 100, 其中诚信节点比例为 50%~100%, 恶意节点比例为 0%~50%, 每个节点的共享文件种类 50 个, 每个节点有选择地从其他节点下载文件 30 次, 仿真系统中所有参数值按表 2 中参数默认值设定。

由图 3 可以看出, 当系统存在恶意节点时, 带有黑名单机制的信任评估机制的 P2P 系统具有较高的交易成功率, 即使当恶意节点的比例达到 50% 时, 仍然具有较高的交易成功率。这是因为当系统引入黑名单机制后, 节点不会与列入黑名单的节点进行交易, 随着越来越多的节点将恶意节点列入黑名单, 恶意节点就很难通过与其他节点进行交易来提高自己的信任度, 从而恶意节点就会很快地被隔离掉。

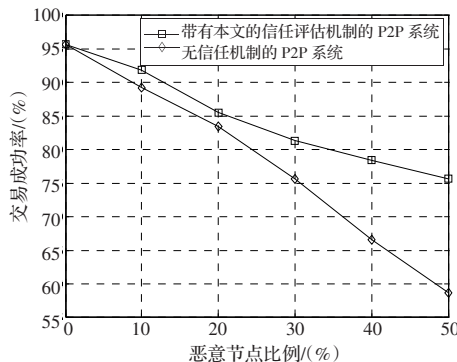


图 3 两种系统的交易成功率对比图

4 结论

针对 P2P 系统提出了一种新的基于声誉的信任评估机制, 该机制根据节点的直接交易历史和其他节点的推荐来计算节点的信任度, 较全面地考虑了影响信任度的因素, 改进了局部声誉与全局声誉的计算方法, 降低了信任度的计算负载, 并引入了黑名单机制。实验结果表明, 提出的信任评估机制能有效地评估节点的信任度, 隔离恶意节点, 提高系统交易成功率。由于 P2P 系统的复杂性和信任问题的难解性, 本文的信任机制仍需要不断的改进。在未来的工作中, 将会引入风险机制和激励机制, 使该信任机制具有更强的抗击恶意节点的能力。

参考文献:

[1] Kamvar S D, Schollosser M T, Molina H G. The EigenTrust algorithm for reputation management in P2P networks[C]// Proceedings of the 12th Int'l World Wide Web Conference. Budapest: ACM Press, 2003: 640-651.