一种基于近期表现的 P2P 网络信任模型

崔 磊,谢显中
CUI Lei,XIE Xian-zhong

重庆邮电大学 个人通信研究所/计算机网络与通信信息产业部重点实验室,重庆 400065
Department of Computer Science,Institute of Personal Communication/MII Key Lab of Computer Network and Communication,Chongqing University of Posts and Telecommunications,Chongqing 400065,China
E-mail:cuileiwork@126.com

CUI Lei,XIE Xian-zhong.Recent-behavior based on trust model for P2P systems.Computer Engineering and Applications,2009,45(30):107-109.

Abstract: This article proposes a novel trust models based on the recent behavior of peers to solve the problem of the large computation and dynamics in the existing trust model.The recent fail ratio of one peer records its recent state.The reputation of one malicious peer will fall to 0,when the node has vicious behavior,then the course of accumulated the trust will become slow.The response of the system changes fast,because it adopts the posterior method and cuts down the computations before the transaction.Theoretical analysis and simulation show that the models use the trust of dynamic computation,and meet the order of small computation,prevent the mutual behavior efficiently.

Key words: peer-to-peer;trust model;security;recent behavior

摘 要:针对现有动态信任模型计算量大的问题,给出了基于近期表现的 P2P 网络信任模型。利用近期失败率来记录与该节点交易的最近状态,当某节点突然"爆发"恶意本性时,可以很快地将其信任值降到 0,当某节点有过恶意行为后,再去积累信任值,积累过程会变慢。由于采用信任值的后验方式,减少了交易前的计算量,提升了系统的反应速度。仿真实验分析表明,该模型提供了信任值计算的动态性,同时满足了小计算量的要求,而且可以有效防止共谋行为。

关键词:P2P 网络;信任模型;安全;近期表现
DOI:10.3778/j.issn.1002-8331.2009.30.032 **文章编号:**1002-8331(2009)30-0107-03 **文献标识码:**A **中图分类号:**TP393.07

1 引言

随着 P2P 网络应用的深入人心,对等网中的交易安全也越来越引起人们的重视。由于 P2P 网络具有天然的"无政府状态",每个系统中都有可能存在大量的恶意节点,而系统本身又缺少对恶意节点的惩罚,以至很多善意节点遭受到侵害,因此交易安全已经成为众多 P2P 系统不得不解决的问题[1]。

在 P2P 系统中建立有效的信任模型可以较好地解决对等系统中的安全问题[2]。对于 P2P 网络系统,既要考虑信任模型中信任值的参考价值,同时还要考虑信任值的计算量是否影响到了整个系统的反应速度。早期的信任模型大多只考虑直接信任和间接信任,然后进行信任值的累加,这种模型在计算量上是很小的,但是它们没有引入动态的概念,当一个"伪装"的善意节点爆发时,无法很快的制止与该节点的交易。后来人们逐渐把时间因素引入信任值的计算,使得信任模型有了动态性,可以克服上述缺点,比较经典的有:PeerTrust 模型[3]、基于社会机制实现的信誉管理 P2Prep[4]、基于 Bayesian Network 的信任模型[5],以及 DyTrust 信任模型[6]等,但这无疑增加了节点的计算量。这类动态模型由于信任值的计算量相对比较大,所以节点间的反应速度比较慢,影响了整个网络的性能[7-8]。针对上述不足,给出了基于近期表现的 P2P 网络信任模型。模型利用近期失败率来记录与该节点交易的最近状态,当某节点突然"爆发"恶意本性时,可以很快的将其信任值降到 0,当某节点有过恶意行为后,再去积累信任值时,积累过程会变慢。由于采用信任值的后验方式,减少了交易前的计算量,提升了系统的反应速度。在计算信任值时引入时间属性的要求,而且满足了计算量相对较少。仿真实验分析表明,该模型提供了信任值计算的动态性,同时满足小计算量的要求,而且可以有效防止共谋行为。

2 基于近期表现的动态信任模型

2.1 信任评价

在该模型中,假设节点 i 要与节点 j 交易,为了避免风险,

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60572089);重庆市科委自然科学基金;重庆市教委应用基础研究基金项目资助。
作者简介:崔磊(1981-),男,研究生,研究方向:计算机网络与通信;谢显中(1966-),男,教授,博士,研究方向:移动通信、计算机网络。
收稿日期:2008-06-10 **修回日期:**2008-09-04

节点 i 要先获得节点 j 的信任值。信任值的取值范围是[0,1],值越大就越信任该节点。站在节点 i 的角度去思考,如果交易很有信心,就可以完全依靠人们的经验,即在以往交易中对节点 j 积累的信任值,称为直接信任值;如果对交易的信心没有达到最大化,还需要其他节点的推荐,称为推荐信任值。通常情况下,应选择后者。当然,其他节点也不可以完全相信,这里利用节点 i 与其他节点的公共交易节点的信任值来求出评价差异,以此来衡量推荐信任值的可信度。于是就有了计算信任值的总公式:

$$R_{ij}=\lambda R'_{ij}+(1-\lambda)\frac{\sum_{k\in I(i,j)}(1-d_{ik})\times R_{kj}}{|I(i,j)|} \tag{1}$$

其中,R'_{ij} 是根据以往交易经验所得的直接信任,λ 为交易时的信心因子,$I(i,j)$是与 j 节点有过交易,并且与 i 节点有共同交易节点的节点集,R_{kj} 为节点 k 对节点 j 的信任值,用来做节点 j 的推荐信任值,d_{ik} 为 i 节点与 k 节点的评价差异,引入 DyTrust[6] 中信心因子和评价差异的概念。从公式(1)中可以看出交易时对直接信任值的侧重取决于信心因子 λ,λ 越大,直接信任值的可信度越大,间接信任值的可信度就越小。另外,利用两节点间的评价差异来度量推荐信任的可信度。

定义 1 某次交易时,直接信任值所占比重称为信心因子λ,信心因子的计算公式为:

$$\lambda=\frac{h}{H} \tag{2}$$

其中,h 为两节点交易次数的积累,H 为用户自定的交易量阀值,λ 初值为 0。此处的 H 可以由用户根据自己交易的风险要求来设定,H 值越大说明该种交易越依赖其他节点的推荐。

定义 2 如果节点 i 要从节点 k 中获取对节点 j 的推荐,利用节点 i 和节点 k 对公共交易节点的评价差 d_{ik} 异来衡量这个推荐的可信度,d_{ik} 的计算公式为:

$$d_{ik}=\frac{\sum_{j\in I(i,k)}|R_{ij}-R_{kj}|}{|I(i,k)|} \tag{3}$$

其中,$I(i,j)$为与节点 i 和节点 k 都有过交易的节点的集合。R_{ij} 与 R_{kj} 分别为节点 i 和节点 k 对节点 j 的信任值,利用这两个值的差来计算两个节点间的评价差异。

2.2 信任值的更新

当交易完成后,要对该节点的信任值进行更新。以前,大多都是把此次交易时的信任值作为更新值。这里采用根据交易是否成功来重新评价信任值的方法,这样做有两个方面的好处。第一,更能反应模型的动态性,并且此处的计算是在交易后,不会影响系统的性能;第二,由于是根据交易成败来更新信任值,可以有效防止恶意节点间的共谋行为。设置一个整数 F,定义如果与该节点交易连续 F 次失败,该节点信任值降为 0。

定义 3 在近期交易中,失败交易占最近交易总次数的比率称为近期交易失败率,失败率 β 的计算公式为:

$$\beta=\frac{f}{n} \tag{4}$$

其中 f 为近期交易失败次数,这里的"近期"其实是一个可以自动调节大小的滑动窗口,窗口的大小就是 n。当交易失败频繁时,窗口会变小,反之变大。当 n 小于 F 时,n 取值为 F,反之,n 取值为当前窗口中的交易次数。当 f 小于 F 时,f 取值于当前窗口中失败交易的次数,反之,f 取值为 F。

交易序列的滑动窗口方案如图 1 所示。当本次交易成功时,交易序列由图 1 中 a 状态转到 b 状态,即窗口的大小 n 增加 1,但窗口并不向后滑动,由公式(4)知,此时近期交易失败率 β 变小;当本次交易失败时,交易序列从 a 状态转到 c 状态,窗口向后滑动,滑动的位移取决于窗口中第 1 次失败交易和第 2 次失败交易之间成功的次数。此时 n 减小,同时 f 增大,由公式(4)得近期交易失败率 β 增大。

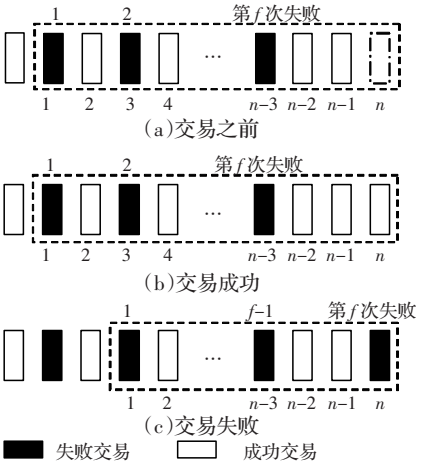

图 1 交易序列中的滑动窗口

定义 4 把成功交易后信任值递增的步长称为信任递增因子 α,α 的计算公式为:

$$\alpha=(1-\frac{\beta}{2})\times\alpha \tag{5}$$

当成功交易后,利用信任递增因子 α 使信任值递增。每发生一次失败交易,α 就会减少一次,用来惩罚该节点,使其积累信任值更加困难,从而达到信任值减少和增加不对称的目的。α 只有在交易失败时才会发生改变,并且应该是在对 β 值修改后进行的。

交易完成后,下一步的工作就是更新信任值了。

更新信任值的主原则:交易成功导致信任值增加,交易失败导致信任值减少,并且信任值的增加过程与下降过程是不对称的。在日常社会生活中,有这样的经验,要考察一个人的信誉时,他做的好事越多信誉也就越好,也许某人做了很多的好事,积累了很高的信誉,但是如果其连续做几件坏事就会使人们开始不相信他,甚至完全对其丧失信心。这就是所谓的信任值的积累与下降不对称的观点。为了使信任模型符合这一规律,采用以下公式来更新交易后的信任值。

$$R_{ij}=\begin{cases}(1-\beta)R_{ij} & \text{交易失败时}\\ (1+\alpha)R_{ij} & \text{交易成功时}\end{cases} \tag{6}$$

其中,右边的 R_{ij} 是交易时所参考的信任值,左边的是交易后要更新的信任值,作为下一次交易的直接信任值。β 为近期交易失败率。当 β 增大到 1 时,即公式(4)中 $n=F$ 时,表示与该节点交易连续失败达到阀值,信任值降为 0。

根据交易的成败来更新信任值的方式,可以减少对推荐信任的依赖,从而降低系统中恶意节点间共谋的风险。当交易失

败时,修改 β 和 α 值,并参考修改后的近期交易失败率来更新直接信任值,可以快速降低恶意节点的信任值;当交易成功时,利用信任递增因子 α 来对直接信任值进行更新。

2.3　算法步骤

当要与某一节点交易时,接下来的处理步骤是什么呢? 首先需要知道每个节点要维护的数据。从上文可知,每个节点要维护的数据有:直接信任值、交易总次数、近期失败交易次数 f(或 F)和倒推 f 次失败交易至今(近期交易序列窗口)的总交易数 n。假设节点 i 要与节点 j 进行交易,用以下算法完成一次交易。

Transaction(i,j):

(1)遍历与节点 j 有过交易的节点得到节点集 $C(j)$;

(2)与节点 i 有过交易的节点,得到节点集 $C(i)$;

(3)逐个遍历 $C(j)$中每个节点 $k_1,k_2,\cdots,k_n$ 的所有交易节点,得到节点集 T;

(4)求得 $C(i)$与 T 的交集利用公式(1)(2)(3)求出当前节点 j 信任值;

(5)交易;

(6)根据公式(4)(5)求出 β 和 α,修改窗口大小并向后滑动;

(7)据公式(5)修改直接信任值,以备下一次交易使用;

(8)完成一次交易。

3　仿真实验及其分析

对该模型进行算法实现,模拟交易。实验参数如表 1 所示。

表 1　实验参数

参数	描述	初始值
N	系统中节点总数	50
R	彼此节点间的信任初始值	0.5
F	连续失败容忍阈值	10
H	信心因子中交易次数的阈值	100
α	信任递增因子初始值	0.001

系统中设定 4 类节点,第 1 类是善意节点(始终提供好的服务),第 2 类是恶意节点(始终提供坏的服务),第 3 类是伪善节点(刚开始是善意节点,但会突然爆发恶意),第 4 类节点是最初提供好的服务,出现失败交易后又继续表示善意。分别对上述 4 类节点进行信任值测试。仿真环境是 Pentium IV 1.8 GM,256 MB,基于 C 语言实现,进行 25 万次虚拟交易得出 4 类节点获得信任值和交易次数。数据分布如图 2 所示,其中横坐标为交易次数,纵坐标为信任值。

根据图 2 的结果,第 1 类节点,始终提供好的服务,由于得到了大量好的推荐,随着成功交易次数的增加其直接信任值也是一路飙升。第 2 类节点,从一开始就提供错误交易,又由于是根据交易成败动态更新信任值,并且引入信心因子的概念,很好地抵制了共谋现象,经过连续交易失败,其信任值迅速降为 0。第 3 类节点,是一种伪善的节点,其先通过大量成功交易获得高的信任值,然后突然爆发恶意行为,对于这类节点,实验结果表明,当其爆发恶意行为时,本模型可以有效地做出反应,使节点的信任值迅速降为 0。第 4 类节点,刚开始节点提供好的服务,当然交易都是成功的。所以信任值像第一类节点那样一路爬升,但是到了中途则出现失败交易,使得信任值迅速减小,当节点重新恢复善意时信任值的积累过程明显变慢。

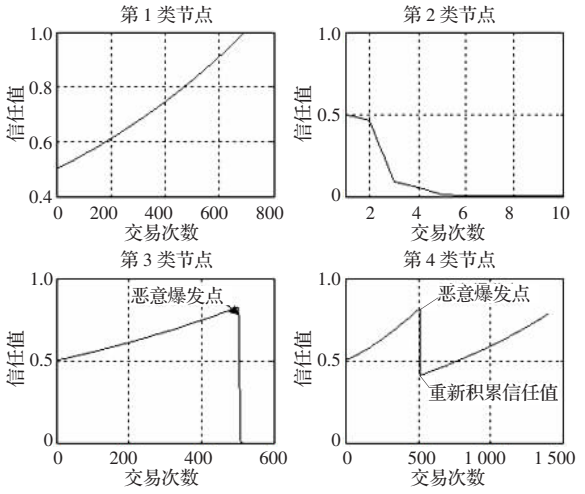

图 2　实验数据分析

与现有的 P2P 系统信任模型相比较,该模型在计算量上有了很大的约减,并且在计算信任值的方法上满足动态性原则,可以有效惩罚系统中的恶意节点,并抵制恶意节点之间的共谋行为。

4　总结

给出了基于近期表现的 P2P 网络信任模型,采用近期失败率、信任递增因子、根据交易成败更新信任值以及计算量后移等方法,改善了现有部分模型的非动态性、大量的计算等缺点。实验结果表明,该模型在保持系统性能的同时,有效提高了模型的动态性和抵御共谋的能力,其具有结构简单、节点计算量小、可操作性强等特点,因而具有较强的工程应用价值。

参考文献:

[1] Dou Wen,Wang Huai-min,Jia Yan,et al.A recommendation-based Peer-to-Peer trust model[J].Journal of Software,2004,15(4):571-583.

[2] 罗杰文.Peer to Peer(P2P)综述[EB/OL].(2005-11-03).http://www.huihoo.com/p2p/1/.

[3] Xiong L,Liu L.PeerTrust:Supporting reputation-based trust for peer-to-peer electronic conmmnities[J].IEEE Transactions on Knowledge and Data Engineering,2004,16(7).

[4] Damiani E,De Capitanidi Vimercati S,Paraboschi S,et al.Managing and sharing servents' reputations in P2P systems[J].IEEE Transactions on Data and Knowledge Engineering,2003,15(4):840-854.

[5] Wang Y,Vassileva J.Bayesian network based trust model[C]//Proceedings of the IEEE/WIC International Conference on Web Intelligence (WI'03),Halifax,Canada,2003:372-378.

[6] 常俊胜.DyTrust:一种 P2P 系统中基于时间帧的动态信任模型[J].计算机科学,2006,29(8).

[7] 张骞,张霞,文学志,等.Peer-to-Peer 环境下多粒度 Trust 模型构造[J].软件学报,2006,17(1):96-107.

[8] 杨德仁,顾君忠.网格与 P2P 的趋同性研究[J].计算机应用与软件,2007,24(1):35-37.