第 39 卷 第 5 期
Vol.39 No.5

计 算 机 工 程
Computer Engineering

2013 年 5 月
May 2013

• 安全技术 •

文章编号：1000—3428(2013)05—0148—04 文献标识码：A 中图分类号：TP393

基于优先权的 P2P 网络信任模型

黎梨苗，陈志刚，桂劲松，邓晓衡

(中南大学信息科学与工程学院，长沙 410083)

摘 要：为解决不同节点信任推荐优先权分配不合理的问题，提出一种基于优先权的对等网络信任模型。对信任度量方法与优先权算法进行设计，采用随时间衰减的优先权算法计算节点信任值，以反映节点的实际情况。实验结果表明，该模型能监测出异常节点的行为，从而有效避免异常节点的破坏活动，随着简单恶意节点、串谋诋毁节点及自私节点的增加，其请求成功率高于 PeerTrust 模型和 EigenTrust 模型。

关键词：对等网络；优先权；信任；信任模型；推荐信任

P2P Network Trust Model Based on Priority

LI Li-miao, CHEN Zhi-gang, GUI Jin-song, DENG Xiao-heng

(School of Information Science and Engineering, Central South University, Changsha 410083, China)

【Abstract】 To solve the problem of different node trust recommendation priority allocated unreasonably, this paper proposes the Peer-to-Peer(P2P) network trust model based on priority. It designs the method of computing trust value and priority algorithm. The priority algorithm of attenuation with time adopts to compute the node's trust value which reflects the actual situation of the node. Experimental results show that this model can detect abnormal behavior of nodes, thus effectively avoides abnormal nodes destruction activity. With the increasing of the proportion of simple malicious nodes, conspiracy to discredit nodes and selfish nodes in the network, the request success rate of this model is higher than PeerTrust model and EigenTrust model.

【Key words】 Peer-to-Peer(P2P) network; priority; trust; trust model; recommendation trust

DOI: 10.3969/j.issn.1000-3428.2013.05.032

1 概述

近年来，随着互联网及电子信息技术的大力发展，以及移动互联网的普及，对等(Peer-to-Peer, P2P)网络技术发展非常迅速，并且成为了目前计算机网络技术领域研究的一个热点[1]。

目前，P2P 网络得到了蓬勃的发展，在许多方面得到了广泛的应用，如协同工作、大规模并行计算、即时通信、分布式信任共享等[2]。P2P 网络不同于传统 C/S 模式，没有中心服务器进行管理，各用户终端能够随意地加入与退出网络，使得网络具有匿名性、自组织性、分布性等特性，这些特性使得 P2P 技术的应用非常便捷。然而，这些特性也给 P2P 网络带来了人们最为担心的安全问题[3]。针对 P2P 网络的安全问题，有不少研究者基于节点信任的动态性与节点信任信息聚合的问题提出了信任模型，以此来抑制 P2P 系统中恶意节点的不良行为[3-4]。比较经典的信任模型有 EigenTrust[5]模型与 PeerTrust[6]模型。EigenTrust 采用信任具有传递特性这一特点，由直接信任值来计算节点的全局信任值，其思想是直接信任值越高，节点推荐的信任值就越可信。因此，在计算全局信任值时赋予了较大的权重。此模型虽然考虑了恶意节点对系统的影响，但在计算信任值时，应当考虑到节点的信任会随时间而衰减，从而使得节点在进行信任推荐时没有将推荐等级区别开来[7]。PeerTrust 在计算直接信任时考虑了 5 个因素：(1)反馈评价。(2)交易的大小。(3)提供反馈评价节点的可信程度。(4)与交易关联的因素，如时间、额度等。(5)与交易环境有关的因素，如为提供反馈的节点进行奖励等[8]。PeerTrust 模型很好地体现了对节点恶意行为的抑制能力，并且，还通过节点反馈评价来激励节点提供信息。但是，此模型也存在不足之处：(1)对节点的恶意行为没有给出惩罚。(2)没有考虑大规模 P2P 系统下计算收敛速度的问题。(3)节点的评价信息在大规模环境下可能显得较稀疏，采用相似性计算节点的信任度时会引起误差。

针对上述网络与模型存在的问题，本文提出一种基于

基金项目：国家自然科学基金资助项目(60873082, 61272494, 60903058)

作者简介：黎梨苗(1979－)，女，博士研究生、CCF 学生会员，主研方向：可信计算，网络安全；陈志刚，教授、博士生导师；桂劲松，副教授、博士；邓晓衡，教授、博士

收稿日期：2012-08-20 **修回日期**：2012-11-02 **E-mail**：305209431@qq.com

优先权的 P2P 网络信任模型。在计算节点的信任值时，考虑了不同节点之间的信任评价因受到一些因素的影响，而给出不同的信任评价值，考虑了信任值随时间而衰减的问题，并且对于直接信任与推荐信任，依据实际情况赋予了节点不同的信任评价优先权值，从而使得对节点信任值的度量更接近实际情况。

2　优先权信任模型

2.1　模型设计思想

基于优先权的 P2P 网络信任模型设计思想是以现实生活中的情况为基础而进行设计的，具体设计思想主要包括：(1)节点掌握的信息资源越多，那么优先权就越高。(2)近期参与过评价的节点优先权高于过去参与的节点。(3)直接信任评价的节点优先权高于间接信任评价的节点。(4)推荐信任评价的节点的优先权由其相应直接信任评价决定。

2.2　信任的度量

定义 1 主体节点 N：指请求要对某个节点的信任进行评价的发起节点，它是想获悉最后评价结果的一个对像，通常进行一次信任评价只有一个这样的节点。

定义 2 目标节点 M：指被其他节点指定要进行信任评价的对象，或指其他节点想要进行交易的对像，但在交易前需对其信任进行评价。

定义 3 推荐节点 I:指对目标节点进行信任评价的除主体节点之外的所有节点。

定义 4 信任度 T：指节点之间的相互信任程度。在本文模型中，信任度采用离散取值法，采用[0,1]之间范围内的数，如完全信任用 1 表示，信任用 0.5 表示，完全不信任用 0 表示。

节点之间的信任度 T 分为直接信任度 Td 与推荐信任度 Tr。

直接信任度 Td 表示为：

$$Td_{NM}=\begin{cases}\dfrac{1}{t}\sum\limits_{i=1}^{t}\lambda T_{NM}(i) & t>0\\ 0 & t=0\end{cases} \tag{1}$$

$$T_{NM}=\alpha\sum\nolimits_{i}^{I(M)}\left(P(M,i)\cdot Tg\left(M(i)\right)\cdot TF(M,i)\right)+\beta\cdot JF(M) \tag{2}$$

$$\lambda=\frac{i}{\sqrt{t^2+1}} \tag{3}$$

其中，$T_{NM}(i)$ 表示在 i 次交易后，节点 N 给予节点 M 的信任评价；$I(M)$是 2 节点进行交易过的总次数；$P(M,i)$表示节点 N 与节点 M 进行第 i 次交易后，节点 N 给予节点 M 的信任评价，且 $0\leqslant P(M,i)\leqslant 1$；$Tg(e)$表示节点本身的可信任程度；$TF(M,i)$是指与节点 M 进行第 i 次交易时，相对应影响信任程度因素所产生的信任因子；$JF(M)$表示与节点 M 相关的，当时交易时影响信任度的各种情况所产生的信任因子；α 和 β 指对信任值进行标准化时的权重参数，且 $\alpha+\beta=1$。如果 $t=0$，则表明 2 个节点一直没有交易历史，则 $Td_{NM}=0$。$i\in\{1,2,\cdots,t\}$ 为时间序列，当 i 值越大，表明节点 N 给予节点 M 信任评价越接近最当前的评价。每增加一个信任评价之后，时间序列相对应会增加一项。λ 为直接信任度随时间衰减的因子。

推荐信任度 Tr 表示为：

$$Tr_{MN}=\frac{1}{t}\sum_{i=1}^{t}\lambda_t R_{iN}\times Td_{Mi} \tag{4}$$

$$\lambda_t\infty\frac{1}{t}\sum_{i=1}^{t}\frac{i}{\sqrt{t^2+1}} \tag{5}$$

其中，$i\in\{1,2,\cdots,t\}$ 表示为时间序列；λ_t 表示推荐信任度随时间衰减的因子，且有 $\sum\limits_{i=1}^{t}\lambda_t=1$；$R_{iN}$ 为节点 i 对节点 N 的推荐信任值；Td_{Mi} 表示本体节点 M 对推荐节点 i 的直接信任值。

随时间衰减的因子双向同步算法表示为：

$$\begin{cases}\lambda=\dfrac{a_t\lambda_t\times a_{t-1}\lambda_{t-1}\times\cdots\times a_1\lambda_1}{\left|\sum\limits_{i=1}^{t}\lambda^2{}_i\times\sqrt{\lambda^2+1}\right|}\\ \lambda_t=\dfrac{b_t\lambda\times b_{t-1}\lambda_{t-1}\times\cdots\times b_1\lambda_1}{\left|\sum\limits_{i=1}^{t-1}\sqrt{\lambda_i^2+1}\right|}\end{cases} \tag{6}$$

其中，$\{a_1,a_2,\cdots,a_4\}$ 为节点的直接信任优先权因子集合；$\{b_1,b_2,\cdots,b_4\}$ 为节点的推荐信任优先权因子集合，优先权因子根据节点之间交易的历史记录而确定。

节点的总信任度表示为：

$$T_{NM}=\begin{cases}Tr_{MN}\\ \dfrac{\delta Td_{NM}+\varepsilon Tr_{MN}}{\sqrt{Td_{NM}^2+Tr_{MN}^2}}\end{cases} \tag{7}$$

$$\delta=(\sum_{i=0}^{n}Sat_{NM}-\sum_{i=0}^{n}UnSat_{NM})/n$$

其中，$\delta+\varepsilon=1$，式(7)分别对应 2 种情况：(1)2 个节点之间没有直接进行过交易，因此，不存在直接信任，只存在推荐信任度。(2)2 个节点之间有过直接交易，因此，既存在直接信任也存在推荐信任。

2.3　优先权算法

在 P2P 网络中，节点之间的信任评价依据包括 2 个部分，即节点提供的资源、节点提供其他服务得到的评价。各个节点建有一个信任值记录表和一个声誉记录表。信任值记录表用来记录其他节点与之交易过后，对其他节点提供服务进行的信任评价。主体节点与目标节点之间在以前有过交易，主体节点后来又得到了目标节点的帮助，从而主体节点对目标节点的信任评价就用信誉表来记录。节点依据这 2 个表的记录得到其他节点的总信任度，从而选择总信任度最高的节点来进行交易。

节点总信任度的更新依据当次交易后给予节点信任评价进行。交易失败指节点之间由于一些因素如提供的服务

没满足需求节点的要求、数据传输速度过慢等而没有达成交易；交易成功是指节点之相的交易双方都满意。从而，节点依据交易成功与否、交易时间及交易的其他情况来给节点重新分配优先权重，得出节点的最新总信任度。

若交易成功，则说明节点的总信任度 T_{NM} 有效地反映了节点的真实情况。然而，在所有给予主体节点帮助的目标节点中，如果 T_{iM} 与 T_{NM} 值相差不大，则表示 i 节点提供了有益的帮助，或者 i 节点和本节点具有一些相似的特性，此时，应该给 i 节点分配比以前高的权重；反之，则应降低 i 节点的权重[9]。

优先权算法描述如下：

输入 本体节点 N 和目标节点 M

输出 本体节点 N 对目标节点 M 的总信任值，以及相应推荐节点的优先权限

```
a[]←0.1
Tr←0.7
T_NM=(a×Td_NM+b×Tr_MN)/(Td_NM^2+Tr_MN^2)^0.5
If(T_NM<Tr_MN)
  a[t+1]←a[t]/2;
  for i=1 to t
a[i]←a[i]/2+a[i−1]
  a[t+1]←−a[t+1]/2+a[t]
  output trusted
  output a[];
else
 a[t+1]←T_NM/2+a[t]
  output not trusted;
output a[];
```

依据优先权算法，能够实时更新与之交易过节点的各权重值。当某一节点的权重值小于给定阈值时，下次将不会选择与其进行交易，这样，使得节点之间的成功交易率高，从而有利于降低网络负载。

2.4 模型性能分析

优先权网络信任模型基于已有信任模型的优点，从而使得其对网络系统中节点的各种异常情况更敏感，同时，通过优先权算法，能够很好地降低网络负载。该模型考虑了网络中不同节点对于交易结果的不同来更新权重分配标准，使得节点在下次参与交易后给出的评价更能反映实际情况。其次，本文模型在计算节点推荐信任度时，采取对整个网络中与目标节点有过交易的或给予过目标节点帮助的所有节点进行统计，对这些节点给出的评价信息进行处理来获得推荐信任值，因此，这样能抑制一些恶意节点来参与活动，从而影响节点的信任值，影响到节点之间的相互信任，保证了系统的安全[10]。本文模型还考虑了网络评价受时间影响的特点，从而引入了随时间衰减的因子，包括直接信任时间衰减因子 λ 和推荐信任时间衰减序列 λ_i，$i\in\{1,2,\cdots,t\}$，并通过双向同步算法，使评价结果更能反映节点的实际情况。

3 实验结果与分析

3.1 实验环境介绍

本文使用了由斯坦福大学开发的查询周期仿真器(QueryCycleSimulator)作为仿真实验工具，采用文件共享模型，在 Windows XP 和 Java 语言 P2P 网络环境下建立了仿真实验[11]。对比模型选用了经典信任模型 EigenTrust(ETrust)、PeerTrust(PTrust)以及本文模型。

在每一个仿真周期里，系统中节点可能处于活跃状态或者处于离线状态。处于活跃状态的每个节点都可以进行一次交易活动。当节点发出请求文件服务信号后，等待愿意提供服务节点的响应，并从中选择节点进行文件服务。直到完成了有效的文件服务或者接受了所有的响应后，一个查询周期才结束，并开始收集数据，这样才算一个完整的仿真周期。设网络中所有节点个数为 1 000，其中，恶意节点占 0~50%，相邻节点个数为 0~20，参与服务的文件总数为 10 000 个，包括 50 种不同类型的文件。

3.2 结果分析

本文通过对网络中正常节点与异常节点文件成功率的下载进行实验，验证模型对异常点活动的敏感程度。对 4 种恶意节点在网络中的攻击情况进行了比较实验，对其网络负载情况进行了测试。

在实验环境中，假设简单恶意提供真实文件的比例为 30%，串谋诋毁节点以 80%的比例向外提供真实文件，而以 80%的比例向内提供真实文件。自私节点在一定时期内提供 80%真实文件，之后不提供文件。

3.2.1 敏感度测试

图 1 为本文模型对异常活动节点的敏感度，即文件服务成功率比较。

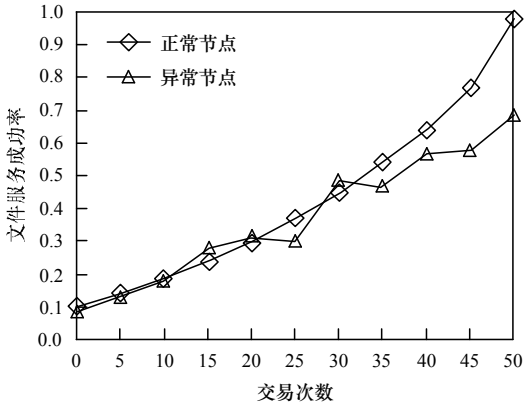

图 1 本文模型的文件服务成功率比较

该实验设置了 2 类节点：(1)正常节点，参与文件服务，这类节点总是追求较好的服务质量，使文件服务成功率不断提高。(2)异常节点，参与文件服务，这类节点为了达到自己的利益而不断改变策略，从而没有保证服务质量，使文件服务成功率出现时高时低的变化。共进行 50 次模拟。

从图 1 可以看出，正常节点在本文模型中，通过不断提高自己的服务质量，文件下载功率随之提高。而异常节点由于带有目的性地在改变自己的服务质量，因此文件下载成功率出现了波动，即时而高、时而低。可见本文模型能够灵敏地监测出异常节点的行为，从而能够有效避免异常节点的破坏活动。

3.2.2　简单恶意节点攻击

当恶意节点比例为 0~50%时，简单恶意节点攻击请求成功率比较如图 2 所示。由于优先权模型能够根据简单恶意节点的行为实时动态更新其信任值，降低提供虚假信息节点的权重，迫使其提供更多真实的信息，从而使得请求成功率优于其他 2 种模型。

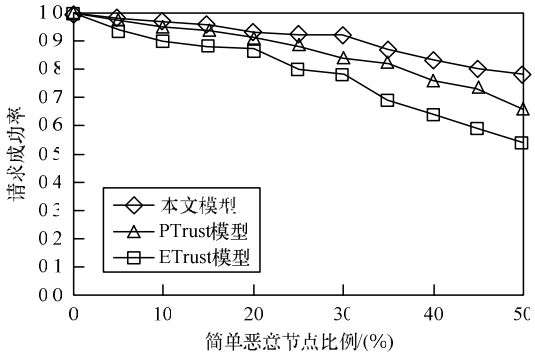

图 2　简单恶意节点请求成功率比较

PeerTrust 模型的成功请求率伴随着恶意节点比例增大而减小，这是因为在 PeerTrust 模型中，没能很好地对恶意节点的行为进行惩罚，从而使得恶意节点有机可乘进行破坏活动。EigenTrust 模型在计算信任值时，应当考虑到节点的信任会随时间而递减，从而使得节点在进行信任推荐时没有将推荐等级区别开来，使得信任值与实际不符，从而导致成功率下降。

3.2.3　串谋诋毁节点攻击

图 3 为串谋诋毁节点请求成功率比较，串谋诋毁攻击性大，对网络影响严重，所以，其请求成功率的影响比简单恶意节点大。网络由于采取的措施不当，会导致许多节点进行串谋，形成具有一定规模恶意集团。在优先权模型中，由于系统对恶意节点行为敏感，能较好地抑制这类节点规模的形成，从而使请求成功率高于其他 2 类。

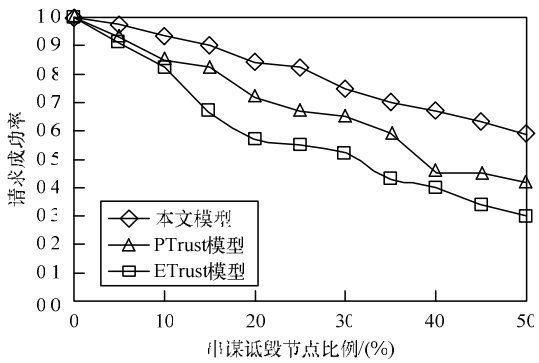

图 3　串谋诋毁节点请求成功率比较

3.2.4　自私节点攻击

图 4 为自私节点攻击请求成功率比较，自私节点在刚开始提供正常信息，一段时间后不提供正常信息，由于优先权模型中的时间衰减因子可以将其最新的表现加大权重，因此其信任值会在不提供正常信息后快速下降，从而迫使其提供更多真实的信息来提供信任度，本文模型具有一定优势。

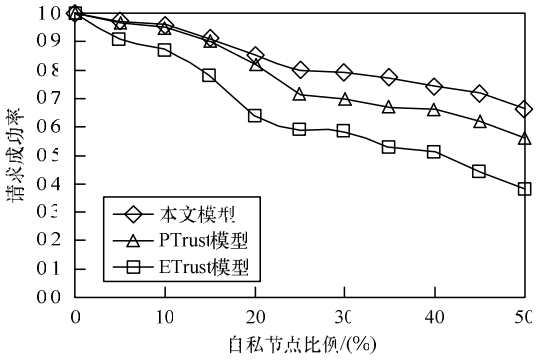

图 4　自私节点请求成功率比较

4　结束语

近年来，P2P 网络技术已经得到了迅猛的发展，但由于其本身的特点，使得系统中的节点相互存在信任问题。为此，本文提出一种基于优先权的 P2P 网络信任模型。采用优先权算法，使计算得到的节点值更能反映节点的真实情况，这样参与交易的节点能很好地利用信任值做参考来选择交易的对像，从而为避开恶意节点攻击提供保证。实验结果表明，该模型能够有效抵抗简单恶意节点攻击、串谋诋毁节点攻击、自私节点欺骗等多种攻击方式。在未来的工作中，将研究恶意节点的惩罚策略与激励机制，使网络系统更加安全，使节点能积极地提供可靠信息与服务。

参考文献

[1] Wang Xuan, Wang Lei. P2P Recommendation Trust Model[C]//Proc. of the 8th International Conference on Intelligent Systems Design and Applications. [S. l.]: IEEE Press, 2008.

[2] Moalla S, Hamdi S. A New Trust Management Model in P2P Systems[C]//Proc. of the 6th International Conference on Signal-image Technology and Internet Based Systems. [S. l.]: IEEE Press, 2010.

[3] 马　礼, 郑纬民. 网格环境下的信任机制研究综述[J]. 小型微型计算机系统, 2008, 29(8): 236-241.

[4] 田春岐, 江建慧, 胡治国, 等. 一种基于聚集超级节点的 P2P 网络信任模型[J]. 计算机学报, 2010, 33(2): 345-354.

[5] Epandar D, Mario T S, Hector G M. The EigenTrust Algorithm for Reputation Management in P2P Networks[C]//Proc. of the 12th International Conference on World Wide Web. Budapest, Hungary: ACM Press, 2003.

(下转第 155 页)