一种基于信誉和风险评价的分布式 P2P 信任模型

田春岐　邹仕洪　田慧蓉　王文东　程时端
(北京邮电大学网络与交换技术国家重点实验室　北京　100876)

摘　要：针对目前大规模 P2P 系统不能有效处理恶意节点攻击的问题，该文提出一种新的基于信誉与风险评价的 P2P 系统信任模型，该模型考虑到节点的动态行为影响信任度计算的不确定性，引入风险因素，并提出采用信息熵理论来量化风险，将实体之间的信任程度和信任的不确定性统一起来。仿真试验及分析表明，该信任模型能够有效识别恶意节点，相比已有的一些信任模型较大程度地提高了系统成功交易率，可以使节点之间更有效地建立信任关系。

关键词：Peer to Peer 网络；信任；信誉；局部信任度
中图分类号：TP393.07　　**文献标识码**：A　　**文章编号**：1009-5896(2007)07-1628-05

A New Trust Model Based on Reputation and Risk Evaluation for P2P Networks

Tian Chun-qi　Zou Shi-hong　Tian Hui-rong　Wang Wen-dong　Cheng Shi-duan
(*State Key Lab. of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract: In large scale P2P networks, it is difficult to deal with different type of attacks issued by malicious peers. A novel trust model based on reputation and risk evaluation is proposed in this paper to solve this problem, in which the uncertainty between trust relationships is considered. The risk is quantified using information entropy and further trust degree and uncertainty degree are presented in a uniform form. The simulation results show that the proposed trust model can evidently enhance successful transaction ratio of system and efficiently help peers establish trust relationships in open P2P networks.

Key words: Peer to Peer networks; Trust; Reputation; Local trust value

1　引言

P2P(Peer-to-Peer)网络中节点之间信任问题是现在研究的热点。信任反映的是一个节点对另一个节点行为以及能力的综合评价。目前对 P2P 网络中信任问题的研究主要是在系统中建立可靠的信任管理模型来解决。现存的大多数信任模型都着力于为资源提供者计算信任度，其中全局信任模型[1,2]通过邻居间相互满意度的迭代为网络中的每个节点计算一个唯一的信任度；在基于PKI[3]的信任模型中存在少数领袖节点，领袖节点负责整个网络的监督，定期通告违规的节点，这些领袖节点的合法性通过CA 颁发的证书加以保证；基于推荐信息的信任模型[4–7]与人际社会网络有很大的相似性，是一种在节点对资源提供者了解不充分情况下通过询问朋友节点，依靠这些节点的推荐来确定资源提供者可信度的机制。但是，现存的P2P信任管理机制在设计时没有考虑从节点信任度计算上反映节点以前的不良交易对以后交易产生的不确定性，信任机制要能够监测出恶意节点可能的攻击或者潜在的威胁。

基于此，本文提出一种基于信誉和风险估价的P2P信任模型R^{2}BTM(Reputation and Risk evaluation Based Trust Model)，考虑到不同类型恶意节点可能的攻击，本文在计算节点信任度时，除了计算基于推荐的信誉度外，还通过分析它的历史行为引入隐含不确定性的风险值作为对信誉度的追加。由节点动态行为引起的不确定性为信任度的计算带来了难度，本文借鉴信息熵理论在处理不确定问题上独有的优势并结合P2P网络的特性，利用定义的置信度，较准确地量化了节点的风险值，而且可通过适当调节信誉值和风险值的权重大小，使得节点的信任度受恶意行为的影响更灵敏，在一定程度上达到检测恶意行为的目的。

2　信任管理模型

为使R^{2}BTM更可靠，应使其具有两个特点：一是节点建立信誉比较慢，但是毁坏信誉却相对快，这样可以防止恶意节点伪装成好节点轻松骗取较高的信誉度后开始其恶意行为，但是信誉度却维持在一个可信的范围之内；另一个特点是模型中每个节点都有信任信息存储单元，而不是一个系统级的中央信息库。这样做的好处是节点可以基于推荐节点的可信度有选择地获取信任信息，同时可以避免中央数据库单点失效的危险。

2006-02-08 收到，2006-09-13 改回
国家 973 项目(2003CB314806，2006CB701306)和国家自然科学基金(90604019，60472067，60502037)资助课题

2.1 信任度概述

在R^{2}BTM中,节点信任度是由信誉值和风险值两部分组成。用 T_{ij} 表示节点i对节点j 的信任度，R_e 和 R_i 分别表示节点j 的信誉值和风险值，α,γ 分别是两者的权重，则节点j的信任度为

$$T_{ij}=\alpha R_e-\gamma R_i,\quad 0\le\alpha,\gamma\le 1 \tag{1}$$

α,γ 的取值依据请求节点 i对被评价节点 j交互的乐观程度，对 j 的行为及交互结果越乐观，则选择合适的 α,γ 值使得 α/γ 越大，使信任度受风险的影响小些；相反，对 j的行为越悲观，则选择 α,γ 的值使得 α/γ 越小，以致信任度对风险值越敏感。

本文以 P2P 文件共享系统为例，节点在文件下载完成之后，按照其对服务质量的满意程度可以分为表 1 所示的几类：

表 1 下载文件种类与服务质量描述

种类	文件种类与下载服务质量描述
G(Good)	文件为所请求的且质量好，下载速度高
C(Common)	文件为所请求的但质量一般(保证对)或下载速度慢、有延迟
I(Inauthentic)	文件为不真实文件
N(Noresponse)	无响应或请求被拒绝
M(Malicious)	文件为恶意文件(木马、病毒等)

针对上面 5 种情况，本文定义了一个 Map 函数 f，如式(2)所示。

$$f(x)=\begin{cases}v_1,x=G,0<v_1<1\\ v_2,x=C,0<v_2<v_1\\ v_3,x=N,v_3<0,|v_3|>v_1\\ v_4,x=I,\ v_4<0,|v_4|>|v_3|\\ v_5,x=M,-1\le v_5<0,|v_5|>|v_4|\end{cases} \tag{2}$$

2.2 信誉计算

令 P_i 表示节点 i。

定义 1 $R_{ij}^t=R(P_i,P_j,t)$ 表示节点 i对节点 j在时间区间 t 内直接交互后给出的评价。R_{ij}^t 的值即节点 i 对 j 的局部信任度。时间段 t 的引入，更能反映节点行为随时间变化的状况。

2.2.1 局部评价(Local rating)计算 在R^{2}BTM中，两个节点每交互一次(为方便起见，本文称发起请求并对响应者进行评价的节点为rater，响应的节点为ratee)，rater就对ratee进行评价打分，评价完后本地保留评价结果。

如果 P_i,P_j 之间在时间 t 内交互了 n 次，则评价值为

$$R_{ij}^t=R^t(P_i,P_j)=\begin{cases}\dfrac{\sum_{k=1}^{n}f(x)}{n},n\ne 0\\ 0,\qquad n=0\end{cases} \tag{3}$$

为了准确地计算节点信任度，信任模型必须区分不同时期交易对计算信任度的影响。目前比较一致的做法是为不同时期的交易按当前距离的远近程度分配不同的权重，距离目前越近，赋予的权重越高；距离目前越远，给予的权重越小。本文提出一种衰减函数，利用此衰减函数的约束作用，达到比权重的分配更稳健更合理的效果，因为权重的分配完全是一种主观的、凭经验式的决断，而衰减函数由于受内部参数取值的约束，函数值易于控制，衰减幅度在理论上可操作的灵活性也更强。

定义 2 衰减函数 f：第 k 个时间区间内发生的交易在计算信任度时相比当前时间区间内(第 n 区间)的交易折扣幅度函数称为衰减函数，表示为 $f(k)=f_k=\rho^{n-k},0<\rho<1,1\le k\le n$。

利用定义好的衰减函数 f，对应于每个时间区间都有一个相应的衰减因子(函数值)。如果节点 i 和 j 发生交易的时间段为 $[t_{\text{start}},t_{\text{end}}]=[t_1,t_2,\cdots,t_n]$，$1\le k\le n$，利用衰减函数 f，则 i 对 j 的局部评价为

$$R_{ij}=\sum_{k=1}^{n}f_kR_{ij}^{t_k}\Big/\sum_{k=1}^{n}f_k \tag{4}$$

其中 $f_k=\rho^{n-k}$ 是时间区间 t_k 内交易的衰减因子，且 $0<f_k<f_{k+1}\le 1$，$1\le k<n$。

2.2.2 汇聚Ratings计算 基于推荐的P2P信任系统在处理推荐信息时，有一个实际的问题是推荐节点信誉度有高有低，信誉度高的节点的推荐比信誉度低的推荐更应该值得信赖，所以必须对节点的推荐区别对待，给予不同的权重。R^{2}BTM认为首先加入系统的节点是值得信赖的，因为作为网络的构建者和P2P网络最初的使用者，它们没有动机破坏自己构造的网络，本文把这些节点构成的集合称为亚可信节点集。如果它们是推荐节点，则给予它们很高的推荐权重，譬如为 w_k，其它非亚可信节点的推荐权重设为 w_i ($w_i<\ w_k$)，信誉度越低推荐权重越小。在R^{2}BTM中，rater对非亚可信节点的推荐信息的判决依据一个四元组 $s=<$ Rpt, Di,Ta,Td $>$，式中 Rpt 是推荐者信誉值，Di 是rater对推荐者直接交互经验值，Ta 是推荐者与ratee的交易次数，Td 为交易日期。R^{2}BTM采用的这 4 个指标已完全覆盖与交易有关的所有特征，区别于FuzzyTrust[7]所使用的 3 个指标，FuzzyTrust方案在决定推荐权重的时候没有考虑与推荐者直接交互的经验，是不完备的，而且直接交互的经验有时候起着至关重要的作用，不应该被忽视。

在 rater 对推荐者的推荐信息给出权重后，为了避免汇聚数量大而消耗带宽，rater 可以设定一个权重门限值，只考虑权重在门限以上的推荐。基于以上的分析，可这样定义汇聚后的评价。

定义 3 设 $G=\{G_1,G_2,\cdots,G_n\}$ 是推荐者集合，$G_r\in G$ $(1\le r\le n)$ 表示推荐者 r，则 rater 汇聚评价 AR_j 为

$$\text{AR}_j=\frac{\sum_{\substack{r=1\\G_r\in G}}^{n}W_{G_r}R(G_r,P_j)}{\sum_{\substack{r=1\\G_r\in G}}^{n}W_{G_r}} \tag{5}$$

式中 G_r 的推荐权重为 W_{G_r}， $R(G_r,P_j)$ 为推荐者 r 对节点 j 的局部信任度， W_{G_r} 为 r 的推荐权重。

2.2.3 信誉值计算 信誉是对ratee的过去交互事实累积的主观评价，反映了ratee的长期历史行为的品质状况。在R^{2}BTM中，节点i计算的节点j的信誉值如下：

定义 4 信誉值:节点 j 的信誉值 RE_j 就是 rater 直接交互评价 R_{ij}^t 和 AR_j 加权求和，即

$$\mathrm{RE}_j=\begin{cases}\beta R_{ij}+(1-\beta)\mathrm{AR}_j, G\neq\Phi, 0\le\beta\le 1\\ 0.5, \qquad R_{ij}=0\text{且}G=\Phi\end{cases} \tag{6}$$

式中 $(1-\beta)$ 是推荐的权重，β 是 R_{ij} 的权重。在R^{2}BTM中，规定新加入系统的节点的信誉度为 0.5，文献[8]中指出P2P系统中恶意节点毕竟还是少数，因此对新加入节点的猜疑是导致系统整体性能不高的缘由，由于节点动态地加入或者离开，在证实新节点不可信之前部分相信它将会使系统更有效。本文后续的仿真也证实此观点是正确的。

2.3 风险计算

在已有的基于推荐的信任模型中，只是单纯考虑了信誉值。这种模型普遍存在的问题是在感知节点失常行为时缺乏灵敏性，因为它需要时间来对节点的评价逐渐降低，可以预见，这种信任模型在那些恶意节点尤其是策略恶意节点较多的网络中性能是比较低的，因为它无法识别恶意节点，而风险的引入有助于解决这种问题。

风险是经济学上的概念，在经济学上，风险是指损失发生的不确定性；是由于不确定性造成的后果与预期目标的负偏离。下面先介绍置信度的概念。

假设 $p_i^{t_k}$ ($i=G,C,I,N,M$)表示在 t_k 时间区间内 i 发生的次数在交易总次数中所占的比例。使用衰减函数合成整个交易时间区间内的交易的结果则为

$$\left\{\left(\sum_{k=1}^{n}f_k p_i^{t_k}\right)(G),\left(\sum_{k=1}^{n}f_k p_i^{t_k}\right)(C),\left(\sum_{k=1}^{n}1/f_k\, p_i^{t_k}\right)(I),\left(\sum_{k=1}^{n}1/f_k\, p_i^{t_k}\right)(N),\left(\sum_{k=1}^{n}1/f_k\, p_i^{t_k}\right)(M)\right\}$$

。值得注意的是，我们使用衰减因子的另一方面就是对节点不诚实行为的惩罚作用，体现在对 I，N 和 M 这 3 种不良交易结果的叠加上使用衰减因子的倒数 $1/f_k\,(>1)$。

定义 5 置信度：整个交易时间段内不同质量状况的文件比例在总文件比例中所占的百分比，称为对此类文件的置信度，用 ρ 表示。如上例，节点 i 与 j 交易的结果对 G,C,I,N,M 的置信度分别为

$$\left(\sum_{k=1}^{n}f_k p_i^{t_k}\right)(G)\Big/S_{\mathrm{GCIM}},\left(\sum_{k=1}^{n}f_k p_i^{t_k}\right)(C)\Big/S_{\mathrm{GCIM}},\quad\left(\sum_{k=1}^{n}1/f_k\, p_i^{t_k}\right)(I)/S_{\mathrm{GCIM}},\quad\left(\sum_{k=1}^{n}1/f_k\, p_i^{t_k}\right)(N)\Big/S_{\mathrm{GCIM}}\quad\text{和}\quad\left(\sum_{k=1}^{n}1/f_k\, p_i^{t_k}\right)(M)/S_{\mathrm{GCIM}},$$

其中 $S_{\mathrm{GCIM}}=\left(\sum_{\substack{k=1\\T=G,C}}^{n}f_k p_i^{t_k}\right)(T)+\left(\sum_{\substack{k=1\\T=I,N,M}}^{n}1/f_k\, p_i^{t_k}\right)\cdot(T)$。

我们知道，风险总是由危险、损失等不利后果所造成的，结合P2P文件共享网络实际情况，风险是由发生I，N和M这3 种情形带来的。在R^{2}BTM中，我们引入信息论中信息熵的理论来描述风险。本文只考虑直接交互所带来的风险因素，结合上文提到的文件下载描述和信任模型，风险可量化为

$$R_{isk}=\frac{\sum_{i=I,N,M}f(i)H(\rho_i)}{f(M)} \tag{7}$$

其中 $H(\rho_i)=-\rho_i\log\rho_i$ 为 i ($i=I,N,M$)的熵， ρ_i 为 i 情况的置信度，满足条件 $0\le\rho_i\le 1$， $\sum_{i=I,N,M}\rho_i=1$。

风险的引入有两方面的作用，一方面可以与信誉结合起来更准确地反映节点的信任度。当交互记录中良好的交易多时，则利用式(7)计算出的风险值小，反映在信任度上受风险值的影响小，相反，反映在节点信任度上要对节点信誉值追加一个较大的风险值，从而比单纯依赖信誉计算出的信任度低，因此风险的考虑可看作是对节点不良交易行为的一种惩罚作用；另一方面，因为风险来自于以前交互过程中有失败、损失发生的历史，风险值决定于产生这些失败、损失的频度及恶劣程度，与恶意节点交互自然发生失败和损失的频度和恶劣程度大，也就是风险大，风险值能够被用作预测其未来行为的有力参考，因此可以作为识别恶意节点的有效手段。

2.4 诋毁及合谋欺诈的抑制

诋毁是当节点被询问到对其他节点的信任评价时，为与之有过交易的节点提供不真实的负面评价的行为。合谋欺诈，即恶意节点互相勾结，诋毁好节点并夸大同类节点的行为。

区别于已有的信任模型，在R^{2}BTM中，节点信任度不是由节点信誉度唯一决定，而是基于直接交互记录对异常行为发生的不确定性追加了风险部分，使得节点的信任度受恶意行为的影响更敏感，在一定程度上达到识别恶意节点和潜在恶意行为的目的。本文采取以下几点措施来抑制诋毁和合谋作弊的攻击：

首先，对推荐节点的评价进行 $\dfrac{\left|\mathrm{AR}_j-R_{pj}\right|}{s_j}>1$ 检验，式中 AR_j 为节点rater汇聚后评价， R_{pj} 为某推荐节点p对被评价节点j 的局部信任度， s_j 为所有推荐节点对节点j 的评价的标准偏差。这个公式的目的是检验某个推荐节点对被评价节点j单独给出的局部评价与推荐节点整体给出的评价之间的偏离程度，如果偏离程度超过所有推荐节点对节点j 的评价的标准偏差，则认为该评价失效。所以，恶意节点对攻击目标过分的诋毁或夸大行为很难发生作用。

其次，汇聚推荐信息时对信誉不同的节点的推荐区别对待，如果节点本身为不可信节点，则其推荐信息被打“折扣”，即推荐强度减弱，且信誉度越低减弱幅度越大，所以它对被攻击节点的诋毁或夸大评价很难发生作用。

最后，在R^{2}BTM中，如果目前交易时间区间内I，N和

M的比例高于一定门限，rater要求服务方提交与这些推荐者发生交易的确认，rater通过检查交易记录，如发现有频繁对ratee评价为I，N和M的推荐者，则拒绝接受它的评价；另外，在rater与ratee已有较高的交易量情况下，如果推荐信息与直接交易记录有明显出入，则以直接交互记录为准，忽略推荐信息。

通过以上几点措施，可以较为有效地抑制诋毁或合谋欺诈行为，这点在后续仿真试验中得到了验证。

3　仿真及结果分析

本文仿真基于文件共享P2P网络的查询周期模型[9,10]，同时，我们实现了PET[5]和EigenRep方案，并在简单恶意节点攻击、合谋欺诈和具有复杂策略攻击 3 种不同的攻击模式下，分别对这 3 种机制的成功交易率进行对比分析。

仿真的网络环境为：节点总数为 1000 个，其中恶意节点比例为[0.1–0.5]，好节点度数为 3，恶意节点度数为 6。请求消息 TTL 为 4。好节点和恶意节点均 100%处于积极状态，并在积极状态100%发送文件请求。假设简单恶意节点以40%比例提供可信文件，合谋节点对内 100%提供可信文件，对外 100%为不可信文件。文件个数为 5000 个，文件种类为 100 个，文件在各节点均匀随机分布。仿真中，假设能对系统中的所有文件成功定位，并且系统中每一个文件都至少被一个好节点拥有，同时，假设对于新节点有 10%的被选择概率。

网络中的节点依据行为表现分为以下几种：

好节点：这类节点无论在提供服务上还是在对其他节点的评价上都是真实的，或者称为合作节点。

恶意节点：按攻击方式可进一步分为：

(1)简单恶意节点：这类节点在被选作为下载源时，为请求节点提供不真实的文件，记这类节点为 SM 类。

(2)合谋恶意节点：此类恶意节点互相勾结，为内部成员提供真实文件，但是对外部节点提供不可信文件及虚假的评价。有一种特殊的合谋欺诈即合谋伪装，即合谋节点为了不被识破身份，而是以一定的概率对好节点提供可信文件，企图隐藏其恶意目的。记合谋节点为 Collusive 类，合谋伪装为 CC 类。

(3)策略恶意节点：此类节点可能会视情况以不同的概率提供真实文件，信誉度高时以较低概率提供可信文件，等信誉度低时又以较高比例提供可信文件，从而使自己信誉度始终维持在系统规定的可信门限之内，试图不被系统觉察。记此类节点为 Strategy。

本文仿真了 100 个查询周期，每个节点在整个仿真过程中可完成 100 次交易。试验评估标准是成功交易率(Successful Transaction Rate, STR)，即整个系统成功交易次数在所有交易次数中所占的比例。

3.1 简单恶意节点

图 1 和图 2 分别给出了在简单恶意节点模型下，3 种机制的成功交易率随恶意节点比例(Fraction of Malicious Peers, FMP)变化的情形。在仿真中，假设好节点以 0.96 的概率提供真实文件。在节点选择下载源时，no-reputation system随机选择进行下载，EigenRep、PET和R^{2}BTM对信任度高的以 80%概率选择(以防止高信任度节点过载)。图中括弧内数值分别对应于参数α,β。

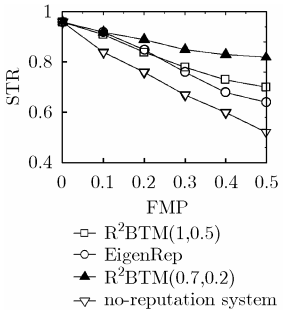

图 1 与 EigenRep 在 SM 下比较

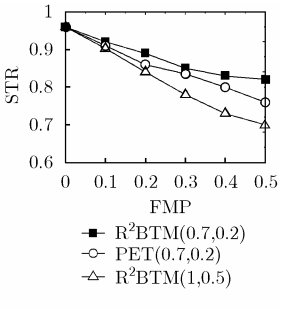

图 2 与 PET 在 SM 下比较

从图 1 可以看出，系统中没有恶意节点时，成功交易率都为 96%。随着恶意节点数的增多，no-reputation system 曲线下降得最快，当系统中恶意节点增至 50%时，成功交易率只有 50%左右；EigenRep 模型因为对这种以一定比例随机提供真实服务的恶意节点欠缺惩罚机制，所以成功交易率也有较大的下降。由于R^{2}BTM($\alpha=0.7,\beta=0.2$)能够有效识别恶意节点，所以它的系统成功交易率随恶意节点比例的增加减小缓慢，即使系统中恶意节点达到 50%时，也保持在 85%左右。

图 2 给出了R^{2}BTM与PET的对比结果，可以看出，随着恶意节点比例的增大，R^{2}BTM显现出较强的优势。这是因为：一方面PET在汇聚推荐信息时不考虑推荐者的可信程度平均对待推荐，这样就使系统不能有效识别恶意节点，造成一些下载为无效下载；另一方面，两者风险值的计算方法不同，本文利用对不确定性描述精确的信息熵来量化风险，使得对节点行为的把握更加准确，从而增加了交易的成功率。

3.2 合谋恶意节点

图 3 对比了 3 种机制在节点合谋欺诈下系统成功交易率情况。由于 EigenRep 模型对合谋作弊这类攻击未作任何处理，因此,恶意节点之间通过相互夸大可信度，从而吸引大量的下载交易，同时由于 EigenRep 无法有效识别恶意节点，造成系统的有效交易明显下降。由于 PET 在计算信誉值时平均对待推荐，当系统中合谋节点比例增大时，成功交易率有很大幅度下降。与之相反，R^{2}BTM对此作了处理，能有

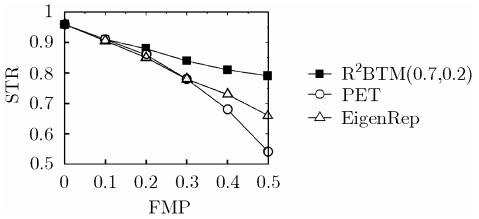

图 3 与 EigenRep，PET 比较

效识别恶意节点，合谋作弊被明显抑制，显示出抵抗合谋作弊的健壮性。图4比较了R^{2}BTM在不同权重下随合谋节点比例变化的各种情况，图中结果说明了风险考虑在合谋欺诈下的必要性和有效性。

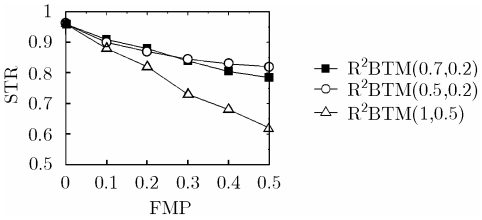

图4 不同权重下本方案比较

图 5 是 3 种机制在合谋恶意节点比例固定为 25%时，节点恶意率(MR，Malicious Rate)从 0 到 1 变化的情况。可以看出，当恶意率小于 0.5 时，系统基本不能辨别是好节点还是恶意节点，所以 3 种机制的成功交易率都有所下降。但随着恶意率的增加R^{2}BTM成功交易率上升速度快于PET，成功交易率也高于EigenRep和 PET，说明R^{2}BTM对此类攻击更灵敏。

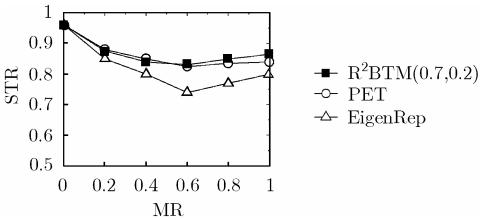

图 5 3 种机制在 CC 下比较

3.3 具有策略的恶意节点

图 6 对比了R^{2}BTM与PET在策略恶意节点攻击下成功交易率情况，仿真中假设信任度低于 0.5 则为不可信节点，同时假设策略恶意节点在其信任度高于 0.6 时以 20%提供可信文件在信任度低于0.6 时以60%提供可信文件。由图可知，在恶意节点比例小于 0.4 时，考虑了风险因素的R^{2}BTM和PET性能相近，但当恶意节点比例增大到 0.5 时，PET成功交易率急剧下降。没有考虑风险的R^{2}BTM成功交易率一直比前两者低，这是由于此方案对这类狡猾的恶意节点不能有效识别，致使成功交易率下降较快。

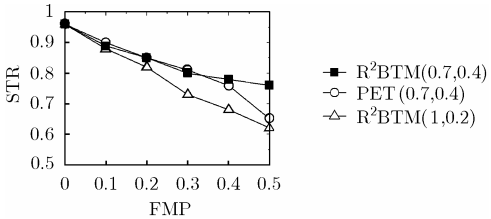

图 6 3 种机制在 Strategy 下比较

4 结束语

由于信任具有不确定性的一面，所以会存在交互的风险。本文通过引入信息熵理论刻画风险，为信任不确定性进行了建模，使节点之间信任关系更加合理。仿真结果表明，R^{2}BT M 较已有的一些方案在某些指标上有明显的改善，在大规模的开放网络环境中具有很好的效果。

参 考 文 献

[1] Kamvar S and Schlosser M. The EigenTrust algorithm for reputation management in P2P networks. Proceedings of the 12th International Conference of WWW, Budapest, Hungary, 2003: 640–651.

[2] Yamamoto A, Asahara D, and Itao T, *et al*.. Distributed pagerank: A distributed reputation model for open P2P networks. Proceedings of the 2004 International Symposium on Applications and the Internet workshops(SAINTW'04), Tokyo, Japan，2004: 389–396.

[3] Altman J. PKI Security for JXTA overlay networks. Technical Report, TR-I2–03–06, Palo Alto: Sun Microsystem, 2003.

[4] Cornelli F, Damiani E, and Vimercati D C, *et al*.. Choosing reputable servents in a P2P network. Proceedings of the 11th International Conference of WWW, Hawaii, ACM Press, 2002: 441–449.

[5] Liang Z Q and Shi W S. PET: A personalized trust model with reputation and risk evaluation for p2p resource sharing. The 38th International Conference on System Science, Hawaii, 2005: 256–264.

[6] Yu B and Singh M P. An evidential model of distributed reputation management. Proceedings of the First Int. Joint Conference on Autonomous Agents & Multiagent Systems (AAMAS), Bologna, Italy, 2002: 254–301.

[7] Song S S, Hwang K, and Zhou R F. Trusted P2P transactions with fuzzy reputation aggregation. *IEEE Internet Computing Magazine*, 2005, 9(6): 24–34.

[8] Friedman E and Resnick P. The social cost of cheap pseudonyms. *Journal of Economics and Management Strategy*, 2001, 10(2): 173–199.

[9] The Stanford P2P Sociology Project http://p2p.stanford.edu /www/demos.htm

[10] Schlosser M, Condie T, and Kamvar S. Simulating a file-sharing P2P network. In First Workshop on Semantics in P2P and Grid Computing, Budapest, Hungary， 2003: 126–137.

田春岐： 男，1975年生，博士生，研究领域为P2P网络、信任管理.

邹仕洪： 男，1978年生，博士，讲师，主要研究领域为IP网服务质量、服务管理、移动自组网、无线传感器网络.

田慧蓉： 女，1980年生，博士生，研究领域为服务管理、P2P网络.

王文东： 男，1963年生，教授，主要研究领域为网络服务质量、服务管理、下一代网络NGN.

程时端： 女，1940年生，教授，博士生导师，主要研究领域为IP 网的服务质量控制、管理、测量理论及技术、下一代互联网的体系结构、协议与应用、宽带网的业务流量工程理论与技术.