P2P 网络环境下的基于 Vague 集的抗攻击信任模型*)

陈旭日　徐炜民　沈文枫　袁世忠
(上海大学计算机工程与科学学院　上海 200072)

摘　要　由于P2P网络的信任机制经常受到恶意节点的欺骗和攻击，提出一种基于Vague集的抗攻击信任模型，用隶属度度量具有不确定信息的信任度，引入时间敏感系数和惩罚系数，处理资源提供者的直接反馈信息，用Vague集相似度量评价推荐节点的回馈信息，并给出该信任模型的实现方案和仿真实验。实验结果表明该信任模型能够抵御各类欺骗和攻击行为。

关键词　信任模型，Vague集，不确定性，相似度

Attack-resisted Trust Model Based on Vague Set in P2P Networks Environments

CHEN Xu-ri　XU Wei-min　SHEN Wen-feng　YUAN Shi-zhong
(School of Computer Engineering and Science, Shanghai University, Shanghai 20072, China)

Abstract　Since trust protocols in P2P networks are subject to spite node cheats and attacks, a vague set-based attack-resisted trust model is proposed, which uses degree of membership to measure trust degree of uncertainty information, employs time sensitivity coefficient and punish coefficient to deal with direct feedback information of resource provider, introducs similarity of vague set to evaluate return-information in recommended nodes and present practice schemes and emulational experiments of trust model. And the results of experiments show that the trust model can resist various of cheat and attack action.

Keywords　Trust model, Vague set, Uncertainty, Similarity measure

1　引言

P2P系统已经成为互联网上最重要的应用之一。然而，P2P网络的匿名性和动态性等特点使其成为各种欺诈行为的温床，同时，由于P2P系统中的节点更多地表现出理性(只想索取资源而不愿贡献资源的行为)，最大化自身的网络效用，这些现象严重影响了系统整体的可用性[1]。信任机制通过对系统中的用户或资源进行评价来预测该用户或资源的未来行为，从而起到鼓励用户良性行为、打击用户恶意行为、辅助用户决策的作用。信任机制已经成为当前的研究热点之一，并出现了多种实用系统和理论模型。随着用户对信任机制的了解，出现了各种针对信任机制的攻击。主要存在以下几类攻击方法[2]：(1)背叛。在正常使用系统一段时间并积累一定信任值后，突然出现恶意行为；(2)策略摇摆。在积累信任和滥用信任之间摇摆，以使其利益最大化，如使用 m 次交易进行信任积累，然后使用 n 次交易进行攻击，以此反复，或者利用小金额交易积累信任，大金额交易进行攻击；(3)诋毁攻击。通过伪造交易数据，降低或者提升某些内容的信任值；(4)串谋。多个用户结成私党，对圈内的用户互相吹捧，对圈外的用户一起诋毁。

本文提出基于Vague集的信任模型，从肯定、否定和不确定三元组角度来表示和处理信任信息，精确量化节点提供资源行为的有效性，阻止节点的背叛和策略摇摆行为。利用成熟的Vague集相似度量理论分析节点推荐行为，识别节点反馈信息是否真实，有效防范诋毁和串谋攻击行为。

2　相关工作

目前存在若干基于P2P环境的信任模型[3]，可以归为以下几类：

① 基于PKI的信任模型。在这类系统中，中心节点的合法性通过CA颁发的证书加以保证。但系统是中心依赖的，具有可扩展性差、单点失效等问题，如eBay，eDonkey等系统。

② 基于局部推荐。在这类系统中，节点通过询问有限的其它节点以获取某个节点的信誉度，一般采取简单的局部广播的手段，其获取的节点信誉度往往是局部的和片面的。PeerTrust[4]是基于信誉的局部信任模型，该模型通过节点的交易回馈信息来量化、比较节点的可信度，并针对结构化P2P提出了分布式的回馈信息保存方案和信誉值计算方案。但是基于分布式Hash表的回馈信息的管理开销不容忽视。

③ 全局可信度模型。为获取全局的节点可信度，该类模型通过相邻节点间相互满意的迭代，从而获取节点全局的信誉度。EigenRep[5]等全局信任模型中，信任度通过邻居参与者间相互满意度的迭代计算得到。这类全局信任模型存在以下几个问题：模型没有考虑到信誉度本身所具有的不确定性，一个节点对另一个节点只有信任与不信任之分，而没有考虑到信任的不确定性；模型的实现没有考虑网络的性能开销，每次交易都会导致在全网络范围内的迭代，这在大规模网络环境中缺乏工程上的可行性。

④ 基于模糊的信任模型[6]。它们认为信任具有模糊性，不能用精确的数学模型来描述，引入模糊集合论中隶属度的

*)基金项目：湖南省自然科学基金资助项目(05JJ40101)；湖南省教育厅项目(05C740)。陈旭日　博士生，副教授，研究方向为网格计算、网络安全。

概念来描述信任的模糊性，用信任向量度量信任值，并且利用模糊综合评判和模糊推理进行信任运算和推导。该信任模型仅使用隶属度描述信任，还不能完全体现信任的不确定性；信任类型的划分主观性较重，没有统一的标准，难于推广。

3 Vague 集理论

Vague 集是 Gau 和 Bueher 于 1993 年提出的一种新的处理模糊信息的理论[7]。在 Vague 集中，隶属程度采用区间的表示形式，这个区间既给出了支持证据的程度，同时也给出了反对证据的程度，从而能够表示、处理模糊集无法表示和处理的模糊信息[8]。

3.1 Vague 集的定义

定义 1 令 U 是一个点(对象)的空间，其中的任意一个元素用 x 表示，U 中的一个 Vague 集用一个真隶属函数 t_v 和一个假隶属函数 f_v 表示，$t_v(x)$ 是从支持 x 的证据所导出的 x 的隶属度下界，$f_v(x)$ 则是从反对 x 的证据所导出的 x 的否定隶属度下界，$t_v(x)$ 和 $f_v(x)$ 将区间 $[0,1]$ 中的一个实数与 U 中的每一个点联系起来，即

$t_v: U \to [0,1]$

$f_v: U \to [0,1]$

其中 $t_v(x)+f_v(x) \leqslant 1$。

设 V 为一个 Vague 集，当 U 是连续的时候，有

$$V=\int_U [t_v(x),1-f_v(x)]/x, \quad x \in U$$

当 U 是离散的时候，有

$$V=\sum_{i=1}^{n}[t_v(x_i),1-f_v(x_i)]/x, \quad x_i \in U$$

3.2 Vague 集的相似度量

定义 2 假定 $X=[t_x,1-f_x]$ 是论域 U 上的一个 Vague 值，其中 $t_x \in [0,1]$，$f_x \in [0,1]$ 且 $t_x+f_x \leqslant 1$，那么 X 的核可由如下的函数 S 进行计算：

$$S(X)=t_x-f_x \tag{1}$$

显然，$S(X) \in [-1,1]$。

定义 3 假定 $X=[t_x,1-f_x]$，$Y=[t_y,1-f_y]$ 是论域 U 上的两个 Vague 值，则 X 和 Y 之间的相似程度可由如下的函数 M 计算：

$$M(X,Y)=1-\frac{|S(X)-S(Y)|}{4}-\frac{|t_X-t_Y|+|f_X-f_Y|}{4} \tag{2}$$

定理 1 $M(X,Y) \in [0,1]$

证明：

$$M(X,Y)=1-\frac{|S(X)-S(Y)|}{4}-\frac{|t_X-t_Y|+|f_X-f_Y|}{4}$$

$$\leqslant 1-\frac{0}{4}-\frac{0}{4}=1$$

由于 $|S(X)-S(Y)| \leqslant 2$，$|t_X-t_Y| \leqslant 1$，$|f_X-f_Y| \leqslant 1$，故有

$$M(X,Y)=1-\frac{|S(X)-S(Y)|}{4}-\frac{|t_X-t_Y|+|f_X-f_Y|}{4}$$

$$\geqslant 1-\frac{2}{4}-\frac{2}{4}=0。$$

定义 4 假定 A 和 B 是论域 $U=\{u_1,u_2,\cdots,u_n\}$ 上的两个 Vague 集，其中

$$A=[t_A(u_1),1-f_A(u_1)]/u_1+[t_A(u_2),1-f_A(u_2)]/u_2+\cdots+[t_A(u_n),1-f_A(u_n)]/u_n=\sum_{i=1}^{n}[t_A(u_i),1-f_A(u_i)]/u_i$$

$$B=[t_B(u_1),1-f_B(u_1)]/u_1+[t_B(u_2),1-f_B(u_2)]/u_2+\cdots+[t_B(u_n),1-f_B(u_n)]/u_n=\sum_{i=1}^{n}[t_B(u_i),1-f_B(u_i)]/u_i$$

假定 $V_A(u_i)=[t_A(u_i),1-f_A(u_i)]$ 表示 Vague 集 A 中 u_i 的隶属值，$V_B(u_i)=[t_B(u_i),1-f_B(u_i)]$ 表示 Vague 集 B 中 u_i 的隶属值，则 A 和 B 的核分别为 $S(V_A(u_i))=t_A(u_i)-f_A(u_i)$ 和 $S(V_B(u_i))=t_B(u_i)-f_B(u_i)$，其中 $i=1,2,\cdots,n$。Vague 集 A 和 B 的相似程度可由如下的函数 T 进行计算：

$$T(A,B)=\frac{1}{n}\sum_{i=1}^{n}M(V_A(u_i),V_B(u_i))$$

$$=\frac{1}{n}\sum_{i=1}^{n}\left(1-\frac{|S(V_A(u_i))-S(V_B(u_i))|}{2}-\frac{|t_A(u_i)-t_B(u_i)|+|f_A(u_i)-f_B(u_i)|}{4}\right) \tag{3}$$

定理 2 $T(X,A) \in [0,1]$

证明：由定理 1 即可证明。

4 基于 Vague 集的信任模型

4.1 信任评估算法

本文的信任度评估模型借鉴 Jϕsang 模型[9]的思想，采用概率论的二项事件后验概率理论。根据社会学个人信任行为，实体的行为近似于概率 P 的二项事件，因此可利用二项事件后验概率分布服从 Beta 分布的特性推导信任关系。设概率变量为 θ，r 和 s 分别表示观测到的实体所产生的肯定事件数和否定事件数，则实体的概率确定性密度函数为：

$$\varphi(\theta|r,s)=\frac{\Gamma(r+s+2)}{\Gamma(r+1)\Gamma(s+1)}\theta^r(1-\theta)^s,$$

$$0 \leqslant \theta \leqslant 1, r \geqslant 0, s \geqslant 0 \tag{4}$$

根据 Jϕsang 模型，观念空间(Opinion Space)的信任度等价于证据空间(Evidence Space)的概率确定性密度函数，本文用 Vague 集替代 Jϕsang 模型的观念空间的三元组。即实体的信任度由 Vague 集 $[t_x,1-f_x]$ 描述，其中 $t_x=\frac{r}{r+s+2}$，$f_x=\frac{s}{r+s+2}$，t_x 和 f_x 分别描述对实体的信任程度和不信任程度。

为了方便信任值的计算，引入“否定性标记 i”和“不确定性标记 j”，一个实体信任度可描述成如下表达式：

$$T=t_x+f_x i+(1-t_x-f_x)j \tag{5}$$

设 U 为 P2P 网络中的资源请求者，P 为资源提供者，设 $D_{U \to P}$ 为 U 对 P 的直接信任度，表示 U 根据与 P 的直接交易回馈信息得到的信任关系。$R_{U \to P}$ 为 U 对 P 的推荐信任度，表示 U 根据其它节点的推荐而得到的对 P 的信任关系。

则 U 对 P 的信任度为

$$T_{U \to P}=\lambda \times D_{U \to P}+(1-\lambda) \times R_{U \to P} \tag{6}$$

4.1.1 直接信任度的计算

定义 5 设 r_0 为 U 与 P 在单位交易额下成功的次数，s_0 为在单位交易额下交易失败的次数。r 为 U 与 P 在某个固定时间段内交易成功的次数，s 为交易失败的次数，则 $r=f(r_0)$，$s=f(s_0)$。

直接信任经常遭遇背叛攻击。背叛是指某节点在一段时间内提供良好的服务，积累一定的信任值，突然出现恶意行为，而其它用户在其信任值降低到一定程度前，还认为它是一个值得信任的节点，并与其进行交易，从而使自己的利益受到

伤害。针对这种情况，本文的方法是增加信任机制的灵敏性，引入信任时间敏感因子和惩罚系数，使信任值能够立刻反映节点的恶意行为。

把一段时间分为若干时间帧，时间帧的长度根据具体的应用场景来确定。设节点在第 n 帧时的直接信任值为 $D_{U\to P}^{n}$，可以根据节点在第 n 帧内交易的情况计算得出。节点在第 n 帧之前的历史直接信任值为 $D_{U\to P}^{n}$，$D_{U\to P}^{n-1}$ 由用户在第 $n-1$ 帧时计算出来，存储在用户机器内。因此节点在整个时间段内的直接信任值为

$$D_{U\to P}=\rho D_{U\to P}^{n}+(1-\rho)D_{U\to P}^{n-1}$$

$\rho(0\leqslant\rho\leqslant1)$称为信任时间敏感系数，$\rho$ 越大，历史信任值作用越小，若 ρ 等于 1，以前的历史就完全不起作用。

直接信任也易遭遇到策略摇摆方式的攻击。在基本背叛的基础上，某些恶意节点在积累信任和滥用信任之间摇摆，以使其利益最大化。策略摇摆主要有以下 2 种表现形式：一种是使用 m 次交易进行信任积累，然后使用 n 次交易进行攻击，以此反复。针对这样的行为，我们设定 $s=f(s_0)=\sigma s,\sigma\geqslant 1$，称为惩罚系数，节点摇摆行为越多，其信任值将会降低得越快，或者上升得越慢。另一种表现形式是利用小金额交易积累信任，大金额交易进行攻击。为了克服这种攻击行为，r 与 s 必须与交易额相关，设基本交易额为 v_0，实际交易额为 v，则

$$r=f(r_0)=\frac{v_0}{v}r_0,s=f(s_0)=\frac{v_0}{v}\sigma s$$

节点在第 n 帧时间内的直接信任值：

$$\begin{aligned}D_{U\to P}^{n}&=\frac{r}{r+s+2}+\frac{s}{r=s+2}i+\frac{2}{r+s+2}j\\&=\frac{v_0}{v}\left(\frac{r_0}{r_0+\sigma s_0+2\frac{v}{v_0}}+\frac{\sigma s_0}{r_0+\sigma s_0+2\frac{v}{v_0}}i+\right.\\&\left.\frac{2\frac{v}{v_0}}{r_0+\sigma s_0+2\frac{v}{v_0}}j\right)\end{aligned}\tag{7}$$

4.1.2 推荐信任度的计算

设 RSet 为推荐节点集，即除 U 外与 P 有过交易的节点集合，$\forall R\in RSet$ 为推荐节点，$C_{u\to R}$ 为 U 对 R 推荐节点的推荐可信度，则 U 与 P 的推荐信任度可以表示为：

$$R_{U\to P}=\sum_{R\in RSet}\frac{C_{U\to R}\times D_{R\to P}}{\sum_{R\in RSet}C_{U\to R}}\tag{8}$$

其中 $D_{R\to P}$ 为节点 R 与 P 的直接信任度。

一组节点向用户推荐某资源的过程中，这组节点可能存在诋毁攻击和串谋攻击。诋毁攻击为节点向网络中的其它节点提供不真实的较低的回馈信息，降低资源的可信度，或者提升同伙资源的可信度。串谋是一种较难防范的攻击行为，一组攻击节点协同合作，对圈内的节点互相吹捧，对圈外的节点一起诋毁，影响用户对资源的正确判断和选择。为了消除这两类攻击，必须对推荐节点的历史行为进行深入分析。根据社会行为学原理，不诚实节点经常对外表现不诚实的行为，因此我们借用与推荐节点有过交易的节点的回馈信息，判断推荐节点是否存在诋毁攻击和串谋攻击的趋势。

设 $C_{up}=\{c_1,c_2,\cdots,c_n\}$ 为与用户 U 和推荐节点 R 均有过交易的节点集合，A 是 U 对集合 C_{up} 中每个节点的交易回馈评分的一个 Vague 集。B 是 R 对集合 C_{up} 中每个节点的交易回馈评分的一个 Vague 集。Vague 集 A 和 B 有相同的论域 C_{up}，A 和 B 中的元素是论域 C_{up} 元素 c_i 的隶属值。推荐节点的推荐可信度 $C_{U\to R}$ 可以由两个 Vague 集 A 和 B 的相似度来衡量，计算公式定义 4 给出：

$$\begin{aligned}C_{U\to R}=T(A,B)&=\frac{1}{n}\sum_{i=1}^{n}M(V_A(c_i),V_B(c_i))\\&=\frac{1}{n}\sum_{i=1}^{n}\left(1-\frac{|S(V_A(c_i))-S(V_B(c_i))|}{2}-\right.\\&\left.\frac{|t_A(c_i)-t_B(c_i)|+|f_A(c_i)-f_B(c_i)|}{4}\right)\end{aligned}\tag{9}$$

假设用户 U 对集合 C_{up} 中每个节点的交易回馈评分较为准确，如果推荐节点 R 对集合 C_{up} 中每个节点的交易回馈评分也较为客观，U 和 R 对集合 C_{up} 应具有相似的评分，则 R 的推荐可信度 $C_{U\to R}$ 较大，趋向于 1，若 R 提供不诚实的推荐信息，则 U 和 R 对集合 C_{up} 交易评分相差较大，R 的推荐可信度 $C_{U\to R}$ 较低，趋向于 0。

4.2 信任模型的实现方案

本文信任模型中的每个节点存储两类信息。一类是节点与资源提供者交易后，资源提供者的可信程度信息。另一类是资源推荐者向节点推荐某资源后，资源推荐者的可信程度信息。

节点用一个五元组集 Φ 来存储资源提供者的历史信息，其中每个元素 $\Phi=(Servernt\_id,SFTrust,SFTime,Snum\_add,Snum\_min\ us)$，Servent_id 是资源提供者在网络中的唯一标识符，SFTrust 表示前一时间段资源的历史可信度，SFTime 前段历史可信度的计算时间，Snum_add 表示近段时间内交易成功的次数，Snum_minus 表示近段时间内交易失败的次数。

推荐者的推荐能力与提供资源能力相关，但不能把两者等同起来，本系统另设立数据结构存储推荐者的推荐能力。由于推荐者的推荐可信度与时间关系不大，为了便于计算和存储，我们忽略时间对推荐可信度的影响。节点用一个三元组集 Γ 来存储推荐者的历史推荐信息。其中每个元素 $\Gamma=(Recommend\_id,Rnum\_agree,Rnum\_disagree)$。Recomment_id 为推荐者在网络中的唯一标识符，Rnum_agree 是以往推荐的意见与最终交易的结果相匹配的次数，Rnum_disagree 是不匹配的次数。

5 模拟实验及分析

本仿真实验以 P2P 文件共享应用为基础，对信任模型抵御各类欺骗和攻击进行模拟分析。仿真是基于斯坦福大学开放的查询周期访真器。仿真网络环境为：P2P 网络包含 1000 个节点，每个节点都可以向其它节点提供文件下载服务。文件个数为 10000 个，均匀随机分布在各节点上。进行 100 轮模拟，各节点每一轮都发出一次服务请求，从随机产生的 5 个响应节点中选择信任度最高的节点请求服务，并对服务结果做出评价。对信任模型的评价标准是整个网络中服务的成功率，即成功下载的次数与理想情况下（所有的节点都是善意节点）的成功下载次数之比，其中理想情况下的成功下载次数为 10^5。服务成功率越高，信任模型越能够抑制恶意行为。

仿真中的服务节点分为善意节点和恶意节点。善意节点既提供真实的服务又客观地评价其它节点。为了仿真实验的方便，把恶意节点分为 3 类：① 单纯恶意节点，它只提供不真实的文件下载服务；② 诋毁节点，它诋毁所有与之交易过的善意节点；③ 合谋节点，它们串通在一起，相互之间给予正反馈。

模拟实验 1：普通恶意行为模拟

本实验模拟在有无信任机制下，不同恶意节点比例与服

（下转第 87 页）

floods // Proceedings of 2000 USENIX Security Symposium. Denver, Colorado, USA, 2000: 199-212
[2] Burch H, Cheswick B. Tracing anonymous packets to their approximatesource // Proceedings of 2000 USENIX LISA Conference. Seattle. Washington, USA, 2000: 319-327
[3] Jing Y N, Li J T, Wang X P, et al. Distributed-log-based IP traceback scheme to defeat DDoS attacks // Proceedings of 20th International Conference on Advanced Information Networking and Applications (AINA 2006). Vienna, Austria. April 2006, 2: 25-32
[4] Thing V L L, Lee H C J, et al. Enhanced ICMP traceback with cumulative path. IEEE VTC2005 'Spring. Stockholm, Sweden, June, 2005, 4: 2415-2419
[5] Dean D, Franklin M, Stubblefield A. An algebraic approach to IP traceback // Proceedings of 2001 Network and Distributed System Security Symposium. Sand Diego, California, USA, 2001: 3-12
[6] Savage S, Wetherall D. Network support for IP traceback. IEEE/ ACM Transactions on Networking, 2001, 9(3): 226-237
[7] Song D, Perrig A. Advanced and authenticated marking schemes for IP traceback // Proceedings of the IEEE INFOCOM. Anchorage, Alaska USA, 2001, 2: 878-886
[8] Li Dequan, Su Purui, Feng Dengguo. Notes on packet marking for IP traceback[J]. Journal of Software, 2004, 15(2): 250-258
[9] Internet Mapping Project. http://cm. bell-labs. com/who/ches/ map/ dbs/index. html, 2006

(上接第 83 页)

务成功率的关系，以此分析该信任模型的有效性，实验结果如图 1 所示，在有信任机制和无信任机制下，随着网络中恶意节点比例的增加，服务成功率都相应地减小，但是有信任机制情况下服务成功率下降得慢，甚至当网络中存在 90% 的恶意节点时，服务成功率还为 47%。

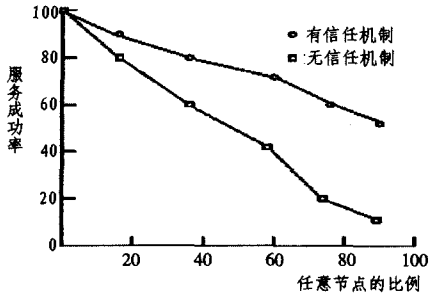

图 1 普通恶意行为模拟图

模拟实验 2：诋毁行为模拟

本实验模拟在有诋毁攻击时善意节点和恶意节点的服务成功率，以检验信任模型对诋毁攻击的抵御能力。假设网络中存在 20% 的恶意节点，实验结果如图 2 所示，随模拟周期的增加，善意节点的服务成功率的有所下降，但恶意节点的服务成功率远低于善意节点，这些现象表明诋毁攻击对善意节点的影响并不大，系统有良好的抵御诋毁攻击的能力。

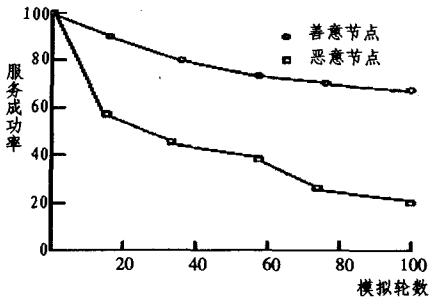

图 2 诋毁行为模拟图

模拟实验 3：串谋行为模拟

本实验模拟在有串谋攻击时善意节点和恶意节点的服务成功率，以检验信任模型对串谋攻击的抵御能力。假设网络中存在 20% 的恶意节点，实验结果如图 3 所示，实验结果与诋毁行为结果相似，只不过结果变化平稳些，一般来说，这两类攻击联系在一起，形成串谋诋毁攻击。

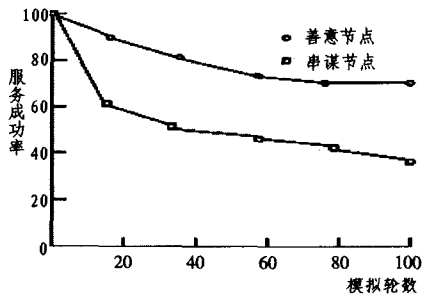

图 3 串谋行为模拟图

结束语 本文提出基于 Vague 集的信任模型，Vague 集的隶属度能够很好地表示和处理不确定信息，信任度具有主观性，包含不确定信息，用隶属度度量信任度是一种理想的度量方法。信任机制常受到 4 类行为的攻击，本文深入分析这些攻击行为的本质，引入信任时间敏感系数和惩罚系数，对资源提供者的反馈信息做出了合理的处理，使信任值正确反映资源的价值，有效地克服了背叛和策略摇摆攻击。Vague 集的相似度量理论较为成熟，本文采用 Vague 集相似度量理论评价推荐节点的回馈信息，判断推荐节点是否存在诋毁攻击和串谋攻击的趋势。本文给出该信任模型的实现方案，并进行了仿真实验，实验表明该信任模型是科学、合理和可行的。

参 考 文 献

[1] Shneidman J, Parkes D. Rationality and self-interest in peer to peer networks [C] // the 2nd Int'l Workshop on Peer-to-Peer Systems(IPTPS2003). Berkeley, CA, USA, 2003
[2] Duma C, Shahmehri N. Dynamic trust metrics for peer-to-peer systems// Proc. of 2nd IEEE workshop on P2P Data Management. security and trust, 2005
[3] 窦文，王怀民，贾焰，等. 构建基于推荐的 peer-to-peer 环境下的 Trust 模型[J]. 软件学报，2004, 15(4): 571-583
[4] Xiong L, Lin L. A reputation-based trust model for peer-to-peer E-commerce communities [C] // IEEE Conf. on E-commerce. Newport Beach, California, USA, 2003
[5] Kamvar S. EigenRep: Reputation management in P2P networks [R]. Tech Rep: SCCM-02-16. Stanford University, 2002
[6] Song S, Hwang K, Zhou R, et al. Trusted P2P transactions with fuzzy reputation aggregation, Internet Computing, IEEE, 2005 (9): 24-34
[7] Gau, Wenlung, Buehrer D J. Vague sets IEEE Transactions on systems. Man and Cybernetics, 1993, 23(2): 610-614
[8] 李凡，徐章艳. Vague 集之间的相似度量[J]. 软件学报，2001, 12 (06): 922-926
[9] Jϕsang A, Knapskog S J. A metric for trusted systems. Global IT Security. Wien: Austrian Computer Society, 1998: 541-549