基于集对分析的 P2P 网络安全中的信誉度改进算法

胡 波[1],王汝传[1,2],王海艳[1]
(1. 南京邮电大学计算机学院,江苏南京 210003;2. 南京大学计算机软件新技术国家重点实验室,江苏南京 210093)

摘 要: P2P 安全是 P2P 技术中的关键问题.传统基于信誉度的投票选举方法能够很好地反映 P2P 网络中未知节点的表现,为该节点的可信度提供可靠依据,但该方法并未将 P2P 网络中的不确定因素考虑进去.集对分析理论是一种研究不确定性问题的数学方法.本文提出了一种基于节点的不确定性的 P2P 网络信誉度安全机制,并采用集对分析方法对信誉度进行了定量分析.最后对两种算法做了对比分析,指出了改进算法的优越性.

关键词: P2P 网络; 安全机制; 信誉度; 集对分析
中图分类号: TP309.2 **文献标识码**: A **文章编号**: 0372-2112 (2007) 02-0244-04

A Modified Security Solution Based on SPA for Servents' Reputations in P2P Systems

HU Bo[1], WANG Ru-chuan[1,2], Wang Hai-yan[1]
(1. *College of Computer, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu 210003, China;*
2. *State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu 210093, China*)

Abstract: The security is a key problem in P2P network. A proposed reputation-polling protocol could resolve it by reflecting the credibility with the former performances of unknown servents. Unfortunately, it didn't take account of the uncertainty in P2P systems. SPA is a new way about dealing with uncertainties problems. We proposed a security solution which was based on servents' uncertainties, and took quantitative analysis with SPA for servents' reputation. In the end, a comparison was made to testify the solution's superiority.

Key words: P2P network; security; reputations; set pair analysis (SPA)

1 引言

P2P(Peer-to-Peer)网络指其中各个节点提供相同服务、从事相同动作的网络.与 C/S 结构不同,P2P 代表了一种新的体系结构,其中的用户克服了传统的网页浏览中的被动角色,获得了一个能够对外提供自己资源的积极角色.P2P 通信软件正在逐渐被广泛使用,它使得个体主机能够通过互联网共享和分配各种类型的信息.然而,由于缺乏集中的安全管理机制和认证机构,P2P 网络中遍布于不同物理地点的各个网络节点很难建立起一种信任关系[1].通常,用户应该只在他们信任的节点上进行共享资料的下载,否则就无法保证资料的安全性,很容易受到各种木马和恶意代码的攻击[2].

为提高未知节点提供的共享资源的可用性,目前已经提出一种"投票选举"的方法,即根据网络中相关节点的意见来建立一个节点的"信誉度".信誉度[3]代表了一个节点在以往的交互活动中给其它相关节点的印象,反映了这个节点的可信任程度.其它节点根据一个节点的信誉度来决定是否下载它所提供的资源,这能够有效避免恶意节点提供虚假信息.

集对分析[4]是近年来才被提出的一种研究不确定性的数学方法,它把对不确定性的辩证认识转换成一个具体的数学工具.

本文提出了一种在 P2P 网络中基于信誉度的改进安全信任机制,来保证网络中各个节点的信任关系,并用集对分析的方法来解决信誉度计算存在的不确定性问题.

2 基于节点信誉度的传统 P2P 网络安全机制

在 P2P 网络中,文件交换要经历两个阶段:搜索和下载.要搜索特定的文件时,节点 p 向网络中其它节点发出查询信息的广播,收到查询信息并且存有相应文件的节点向 p 返回一个应答消息.节点 p 可以从若干个应答的节点中选择一个来下载文件,选择的依据是这些节点能够提供的下载质量,包括了下载的线程数和下载速度等.当然,下载质量是在应答消

收稿日期:2006-02-06;修回日期:2006-06-30
基金项目:国家自然科学基金(No. 60573141, No. 70271050);江苏省自然科学基金(No. BK2005146);江苏省高技术研究计划(BG2004004, No. BG2005037, No. BG2005038, No. BG2006001);国家 863 高科技研究计划(No. 2006AA01z201, No. 200601z219, No. 2006AA01z439);南京市高科技项目(No. 2006 软资 105);江苏省计算机信息处理技术重点实验室基金(No. kjs050001, No. kjs06006);江苏省高校自然科学研究计划(No. 05KJB520092)

息中由提供文件的节点自己申明的,其中可能存在虚假消息.

为了保证应答消息的可靠性,在下载之前,p 需要通过一种"投票选举"的方法来获取文件提供者的信誉度.这个方法有两个阶段:征收选票和选票估算.节点 p 根据应答消息中申明的下载质量从中选择若干个节点 $c_m(m=1,2,\cdots)$,然后向网络中发出广播,要求其它节点对节点 c_m 的信誉度进行投票.在收集到其它相关节点的选票后,p 对选票进行相应的估算并做出下载决定.当然并不是所有的选票都能够真实反映节点 c_m 的信誉度,网络中可能存在恶意节点伪造虚假选票,干扰投票结果.所以每个投票者 $t_n(n=1,2,\cdots)$ 的可信程度是不同的,用可信任度来表示.

在这个安全信任机制中,每个节点都存储有两种信息,一种反映其它节点在以往提供资源时的可信任程度(即其它节点的信誉度),另一种反映其它节点在以往的投票中的表现(即投票时的可信任度).在这两种信息的基础上,通过三个步骤来实现节点之间的投票过程.第一,每个投票者 t_n 把自己存储的节点 c_m 的以往表现聚合为选票,并发送给 p;第二,投票的发起者 p 把每个投票者 t_n 的以往表现聚合为投票者的可信任度;第三,p 根据收到的选票和投票者 t_n 的可信任度聚合出各个节点 c_m 的信誉度,并对其进行排序,从中选择最佳的资源提供者来下载.

2.1　选票的聚合

网络中每个节点 s 用一个三元组集 Ψ 来存储以往文件交互活动所有的历史记录信息,其中每个元素 $\Psi=$(servent_id,num_plus,num_minus).Servent_id 是 s 在交互活动中的对象节点 c_m 在 P2P 网络中的唯一标识,num_plus 和 num_minus 分别是与 c_m 交互活动中下载成功与失败的次数,两者都会随着每次下载的结果不同不断地更新.

节点 s 要根据以上信息聚合出一个二进制数值 0 或 1,来表示对象节点 c_m 信誉度为不可信或可信.这个过程需要一个合适的算法来完成转换 $\phi:\Psi\to\{0,1\}$,而这个算法在不同的方案中可能不同.例如,一个节点可能只为没有不良记录的节点投可信票(在这种情况中,$\phi(\Psi)=1$ 当且仅当 num_minus = 0);也可能它采用一种更加带有补偿性质的算法:$\phi(\Psi)=1$ 如果 num_plus-num_minus ≥ 0,否则 $\phi(\Psi)=0$.

2.2　投票者可信任度的聚合

和选票的聚合方法相似,节点 s 用一个三元组集 Θ 来存储以往投票活动中各个投票者的表现,其中每个元素 $\theta=$(servent_id,num_agree,num_disagree).Servent_id 是每个投票者 t_n 在网络中的唯一标识,num_agree 是在以往发起的投票中 t_n 的意见和最终下载(这意味着 s 确实曾经下载,无论投票者投的是可信还是不可信选票)的结果相匹配的次数,num_disagree 则是不匹配的次数.

仿照选票聚合的方法,节点 s 要根据以上记录映射出一个二进制数值 0 或 1,来代表每个投票者 t_n 是否可信.s 可以构造一个算法实现转换 $\phi:\Theta\to\{0,1\}$.通常采用以下算法:$\phi(\theta)=1$ 如果 $\phi=$ num_agree/(num_agree + num_disagree) $\geq k$,否则 $\phi(\theta)=0$.其中 $k\in(0,1)$,一般取以往网络中可信投票者的 $\phi(\theta)$ 平均值 ϕ,网络可以根据需要动态地调整 k 的取值.

2.3　资源提供者信誉度排名的计算

最终,节点 p 要根据它收到的投票以及投票者 t_n 的可信任程度,对资源提供者 c_m 的信誉度进行聚合和排名,然后选择最佳的若干进行资源的下载.投票和投票者信任度的聚合可以依靠不同的技术来完成,一种简单的方式是将两者相乘,即用投票者的可信任度对投票进行加权.

在现有提出的方法中,将投票和投票者可信任度作为确定的两个因素来简化聚合方案.这样虽然计算简便,但聚合的结果很不准确.而且,在把信誉度简单判定为 0 或 1 的机制中,一个节点只要表现好于临界值,信誉度即为 1.这显然不能准确反应各个节点的不同表现.

3　集对分析理论

3.1　集对分析的定义

定义 1[5]　设有两个非空有限集合 $X=\{x\mid \forall x\in X, X\neq\phi\}$ 和 $Y=\{y\mid \forall y\in Y, Y\neq\phi\}$,其基数(元素个数)分别为 $\overline{\overline{X}}=m$ 和 $\overline{\overline{Y}}=n$,则称 $H(X,Y)=X\times Y=\{(x,y)\mid \forall x\in X \,\&\, y\in Y\}$ 的非空有限序偶集为由 X 与 Y 构成的"集对直集",其基数为 $\overline{\overline{H}}=N=mn$.

定义 2　有问题 W:"X 和 Y 两集合间有无关系 f?"若:

(1)"$x\in X$ 与 $y\in Y$ 有关系 f",记为"xf^+y",称为"x 与 y 在问题 W 下具有同一性",称序偶子集:$H_f^+(X,Y)=\{(x,y)\mid \forall x\in X \,\&\, y\in Y, xf^+y\}$ 为集合 X 与集合 Y 在问题 W 下的同一性序偶集,显然 $H_f^+(X,Y)\subset H(X,Y)$,若 $\overline{\overline{H_f^+}}=S$ 为 $H_f^+(X,Y)$ 的基数,则 $\overline{\overline{H_f^+}}/\overline{\overline{H}}=S/N$ 称为集合 X 与 Y 在问题 W 下的同一度,简记为 a.

(2)"$x\in A$ 与 $y\in Y$ 无关系 f",记为"xf^-y",称为"x 与 y 在问题 W 下具有对立性",与同一性类似,有对立性序偶集 $H_f^-(X,Y)$,其基数 $\overline{\overline{H_f^-}}=P$,对立度 $c=P/N$.

(3)"$x\in X$ 与 $y\in Y$ 不确定有无关系 f",记为"$x\bar{f}y$",称为"x 与 y 在问题 W 下具有不确定性",同理有不确定性序偶集 $H_{\bar{f}}(X,Y)$,其基数 $\overline{\overline{H_{\bar{f}}}}=F$,不确定度 $b=F/N$.

综合上面三种情况,引入"不确定性标记 i"和"对立性标记 j",则表达式:

$$u(X,Y)=S/N+(F/N)i+(P/N)j \tag{1}$$

称为同异反联系度,它反映了集合 X 和 Y 在问题 W 下的联系程度.式(1)可简写成:

$$u(X,Y)=a+bi+cj \tag{2}$$

其中:$a,b,c\in[0,1]$ 为实数,由于 $H(X,Y)=H_f^+(X,Y)+H_f^-(X,Y)+H_{\bar{f}}(X,Y)$,故满足归一化条件:

$$a+b+c=1 \tag{3}$$

从定义可知,集对分析的对象"集对"就是"序偶集",所谓"联系度"就是两个集合在问题 W 下发生联系的程度.

3.2　联系度的优先关系与运算规则

定义 3　设 U 是由全体同异反联系度为元素构成的集合,又设:$u_1=a_1+b_1i+c_1j$,$u_2=a_2+b_2i+c_2j$ 且 $u_1,u_2\in U$,$a_1,a_2,b_1,b_2,c_1,c_2\in[0,1]$,有:

(1) 若 $a_1 = a_2$, $b_1 = b_2$, 则称同异反联系度 u_1 与 u_2 等价或相等, 记为 $u_1 = u_2$.

(2) 若 $a_1 \leq a_2$, $b_1 \geq b_2$, 则称同异反联系度 u_2 比 u_1 优先, 并记为 $u_1 \leq u_2$; 若 $a_1 < a_2$, $b_1 > b_2$, 则称同异反联系度 u_2 比 u_1 严格优先, 并记为 $u_1 < u_2$.

定义 4 设联系数 $u_1 = a_1 + b_1 i + c_1 j$, $u_2 = a_2 + b_2 i + c_2 j$, …, $u_N = a_N + b_N i + c_N j$, 其中: a_n, b_n, $c_n \in [0,1]$, 且 $a_n + b_n + c_n = 1 (n = 1,2,\cdots,N)$, 则有以下运算规则:

(1) 加法规则

$$u_1 + u_2 + \cdots + u_N = \sum_{n=1}^{N} u_n = \left(\sum_{n=1}^{N} a_n\right)/N + \left(\sum_{n=1}^{N} b_n\right) i/N + \left(\sum_{n=1}^{N} c_n\right) j/N \tag{4}$$

(2) 乘法规则

$$\begin{aligned} u_1 \cdot u_2 &= (a_1 + b_1 i + c_1 j) \cdot (a_2 + b_2 i + c_2 j) \\ &= a_1 a_2 + (a_1 b_2 + a_2 b_1) i + b_1 b_2 i \cdot i + (b_1 c_2 + b_2 c_1) i \cdot j + (a_1 c_2 + a_2 c_1) j + c_1 c_2 j \cdot j \\ &= a_1 a_2 + (a_1 b_2 + a_2 b_1 + b_1 b_2 + b_1 c_2 + b_2 c_1) i + (a_1 c_2 + a_2 c_1 + c_1 c_2) j \end{aligned} \tag{5}$$

其中指标运算规则为: $i \cdot i = i^2 = i$, $i \cdot j = j \cdot i = i$, $j \cdot j = j^2 = j$.

另外, 运算满足加法交换律、加法结合律、乘法交换律、乘法结合律和乘法分配律.

4 信誉度的聚合与排序改进算法

改进算法的关键是考虑各个环节存在不确定性因素的前提下, 如何通过合理的聚合机制使得信誉度能够定量比较, 且最终如何进行排序.

4.1 信誉度聚合与排序的基本机制

4.1.1 带有不确定性的信誉度表示

若一个节点 s 可信 (Good) 的概率为 $p(G)$, 不可信 (Bad) 的概率为 $p(B)$, 可信性不确定 (Uncertain) 的概率为 $p(U)$, 其中 $p(G)$, $p(U)$, $p(B) \in [0,1]$ 且满足归一化条件 $p(G) + p(U) + p(B) = 1$, 则节点 s 的信誉度 $p(s)$ 可表示为:

$$p(s) = p(G) + p(U) i + p(B) j \tag{6}$$

于是, 资源提供者 c_m 在以往交互活动中的表现被聚合为选票: $p_t(c_m) = a_1 + b_1 i + c_1 j$, 同时各个投票者 t_n 在以往投票中的表现被聚合为可信任度: $p(t_n) = a_2 + b_2 i + c_2 j$, 选举发起者 p 将选票 $p_t(c_m)$ 和投票者的可信任度 $p(t_n)$ 聚合为该资源提供者的信誉度 $p(c_m)$, 并根据其优先关系来形成信誉度的排名.

4.1.2 信誉度的聚合

选票 $p_t(c_m) = a_1 + b_1 i + c_1 j$ 与投票者可信任度 $p(t_n) = a_2 + b_2 i + c_2 j$ 的聚合算法, 即两个带有不确定性因式的合成算法, 可以按照集对论的乘法运算法则进行.

例如, 若选票 $p_t(c) = 0.8 + 0.1 i + 0.1 j$, 投票节点的可信任度 $p(t) = 0.6 + 0.2 i + 0.2 j$, 则投票发起者 p 聚合信誉度 $p(c)$ 的算法如下:

$$\begin{aligned} p(c) &= p_t(c) \cdot p(t) = (0.8 + 0.1 i + 0.1 j)(0.6 + 0.2 i + 0.2 j) \\ &= 0.48 + 0.28 i + 0.24 j \end{aligned}$$

通常聚合之后节点的可信概率会减小, 而不确定概率和不可信概率会增大. 根据 Dempster-Shafer 原理, 可信概率的减小符合信任传递的衰减原则. 事实上, P2P 网络中节点的增加也会导致不确定性因素的增多, 使不确定概率和不可信概率增大. 节点信誉度中可信概率的减小并不会给其它节点一种不可信任的感觉, 因为节点信誉度的最终排名才是投票发起者关心的问题.

4.1.3 信誉度的排序

假设节点 p 发起一个选举, 对资源提供者 $c_m (m = 1,2,\cdots)$ 的信誉度投票. 对于每一个资源提供者, 网络中如果只有一个投票者为其投票, 那么按照上面的算法, p 很容易聚合出各个资源提供者的信誉度, 并根据优先关系进行排序. 但是事实上, 对于每一个资源提供者, 都会有若干个投票者, 于是 p 需要针对每一个投票者计算出一个信誉度, 并再次将这些信誉度聚合为一个最终的信誉度.

例如: 有 20 个节点: t_{1k}、t_{2k}, $(k = 0,1,\cdots,9)$, 分别对资源提供者 c_1、c_2 进行投票. 投票发起者 p 利用信誉度聚合方法, 已经分别计算出针对各个投票者的信誉度 $p_k(c_1)$、$p_k(c_2)$, $(k = 0,1,\cdots,9)$, 如表 1、表 2 所示:

表 1 c_1 针对投票者 $t_{1k} (k = 0,1,\cdots,9)$ 的信誉度

c_1 信誉度 $p_k(c_1)$	t_{10}	t_{11}	t_{12}	t_{13}	t_{14}	t_{15}	t_{16}	t_{17}	t_{18}	t_{19}
同一度	0.5	0.5	0.4	0.6	0.9	0.3	0.8	0.7	0.6	0.6
不确定度 (i)	0.3	0.2	0.2	0.3	0.1	0.5	0.1	0.2	0.1	0.2
对立度 (j)	0.2	0.3	0.4	0.1	0	0.2	0.1	0.1	0.3	0.2

表 2 c_2 针对投票者 $t_{2k} (k = 0,1,\cdots,9)$ 的信誉度

c_2 信誉度 $p_k(c_2)$	t_{20}	t_{21}	t_{22}	t_{23}	t_{24}	t_{25}	t_{26}	t_{27}	t_{28}	t_{29}
同一度	0.8	0.6	0.5	0.7	0.6	0.9	0.7	0.5	0.6	0.7
不确定度 (i)	0.2	0.3	0.4	0.2	0.2	0.1	0.1	0.2	0.1	0.3
对立度 (j)	0	0.1	0.1	0.1	0.2	0	0.2	0.3	0.3	0

由表中数据聚合出 c_1、c_2 信誉度 $p(c_1)$、$p(c_2)$, 利用集对论的加法运算法则. 即:

$$\begin{aligned} p(c_1) &= \sum_{k=0}^{9} p_k(c_1) \\ &= (0.5 + 0.5 + 0.4 + 0.6 + 0.9 + 0.3 + 0.8 + 0.7 + 0.6 + 0.6)/10 \\ &+ (0.3 + 0.2 + 0.2 + 0.3 + 0.1 + 0.5 + 0.1 + 0.2 + 0.1 + 0.2)\, i/10 \\ &+ (0.2 + 0.3 + 0.4 + 0.1 + 0 + 0.2 + 0.1 + 0.1 + 0.3 + 0.2)\, j/10 \\ &= 0.59 + 0.22 i + 0.19 j \end{aligned}$$

同理: $p(c_2) = 0.66 + 0.21 i + 0.13 j$.

显然, $p(c_2)$ 比 $p(c_1)$ 严格优先, 即 $p(c_2)$ 的信誉度比 $p(c_1)$ 好. 如果有多个节点的信誉度比较, 也是将其一一算出, 并最终给出完整的排序.

4.2 信誉度排序的改进机制

前面我们提过, 要搜索特定的文件时, 节点 p 向网络中其它节点发出查询信息的广播, 收到查询信息并且存有相应文件的节点 r 向 p 返回一个应答消息. 消息中包含了 r 自己申明的下载质量, 包括下载线程数、下载速度、文件匹配程度、版本更新时间等指标. 为了体现这些指标的差异, 信誉度的投票可以具体到这些指标.

在基本机制中, p 在计算出针对各个投票者的信誉度 p_k

(c_m)后,未对数据进行处理,直接聚合出 $p(c_m)$进行排序. 一种更简单有效的方法是先对 $p_k(c_m)$进行处理,将其定性为可信、不可信及不确定,再进行聚合和排序.

定义5　若实数 $u, v \in (0,1)$,节点信誉度 $p_k(c_m) = a + bi + cj$,$\max(a,b,c)$为 a,b,c 中的最大值. 如果 $\max(a,b,c) = a \geq u$,则称 $p_k(c_m)$为可信;如果 $\max(a,b,c) = c \geq v$,则称 $p_k(c_m)$为不可信;否则称 $p_k(c_m)$为不确定. 其中 u 为 P2P 网络中可信节点对应 a 的数学期望的经验值,v 为不可信节点的对应的数学期望的经验值.

结合以上两点,改进的排序算法如下:

设节点 $t_k(k = 0,1,\cdots,9)$对资源提供者 c 投票,投票内容包括下载质量的若干指标,p 已经计算出各项指标的信誉度,并将其定性为可信(用"○"表示)、不可信(用"×"表示)和不确定(用"—"表示). 其结果如表 3 所示:

表3　c 针对 t_k 下载质量各项指标的信誉度

下载质量指标	t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9
下载线程数	○	×	—	×	○	○	×	—	×	○
下载速度	—	○	○	×	—	○	—	○	○	○
匹配程度	—	—	×	○	×	—	○	○	—	×
版本更新	×	○	—	—	○	×	×	—	×	○

按照集对分析理论[6],由表 3 得出:集对 $H(C,T)$的基数 $\overline{\overline{H}} = mn = 40$,可信度 $H_f^+(X,Y)$的基数 $\overline{\overline{H_f^+}} = 16$,对立度 $H_f^-(X,Y)$的基数 $\overline{\overline{H_f^-}} = 12$,不确定度 $H_f(X,Y)$的基数 $\overline{\overline{H_f}} = 12$. 因此 c 的信誉度

$$p(c) = 16/40 + (12/40)\,i + (12/40)\,j = 0.4 + 0.3i + 0.3j$$

根据 p 对各指标的感兴趣程度,还可以为各项指标按照重要性赋权值,设权重向量

$$[\lambda_{线程数}, \lambda_{速度}, \lambda_{匹配}, \lambda_{版本}]^{\mathrm{T}} = [0.2, 0.3, 0.4, 0.1]^{\mathrm{T}}$$

则 $H_f^+(X,Y)$的等效基数 $= 4 \times (4 \times 0.2 + 6 \times 0.3 + 3 \times 0.4 + 3 \times 0.1) = 16.4$,同理 $H_f^-(X,Y)$的等效基数 $= 10.8$,$H_f(X,Y)$的等效基数 $= 12.8$. 此时 c 的信誉度

$$p(c) = 16.4/40 + (12.8/40)\,i + (10.8/40)\,j = 0.41 + 0.32i + 0.27j$$

在加权情况下,信誉度的排序可能会发生变化.

5　新算法与传统算法的比较

(1)传统算法的信誉度取值为离散的 0、1,而新算法的取值为$[0,1]$上的连续值. 设某次投票中针对资源提供者 c_1,投票者 $t_{1k}(k = 0,1,\cdots,9)$的信誉度同一性值分别如表 1,且该值构成一个样本空间. 则对于新算法,同一性值的数学期望 $E(X) = 0.59$,方差 $D(X) = [E(X - E(X))]^2 = 0.0289$. 对于传统算法,若定义信誉度同一性值不小于 0.5 时认为节点可信,则选票值为$\{1,1,0,1,1,0,1,1,1,1\}$,其数学期望 $E'(X) = 0.8$,方差 $D'(X) = 0.1600$. 由此可知,$D(X) < D'(X)$,说明新算法的稳定性优于传统算法.

(2)考察投票者的置信区间(可信度). 对于表 1 中数据同一性值所构成的样本空间,新算法中其数学期望 $E(X) = 0.59$,方差 $D(X) = 0.0289$. 计算其置信概率为 80 %的置信区间为$(0.59 - 0.08, 0.59 + 0.08)$,即$(0.51, 0.67)$. 传统算法中,其数学期望 $E'(X) = 0.8$,方差 $D'(X) = 0.1600$. 计算其置信概率为 80 %的置信区间为$(0.8 - 0.18, 0.8 + 0.18)$,即$(0.62, 0.98)$. 由此可知,新算法投票者的可信度更准确,比传统算法更能真实反应投票者的表现,从而在某种程度上能解决投票者的虚假作弊问题.

6　结束语

以往不考虑不确定性因素的传统信誉度聚合机制,节点在临界值附近的摆动会影响信誉度的参考价值,且不易定量反映出节点的具体可信程度. 本文提出的信誉度聚合与排序机制,能够比较准确地反映出节点的可信度,易于定量计算和比较,并能够较好地解决投票者的虚假作弊问题.

参考文献:

[1] K Aberer, Z Despotovic. Managing trust in a peer-to-peer information system[A]. Proc of the 10th Int'l ACM Conf. on Information and Knowledge Management[C]. New York: ACM Press, 2001. 310 - 317.

[2] F Cornelli. Choosing reputable servents in a P2P network[A]. Lassner D, ed. Proc of the 11th Int'l World Wide Web Conf[C]. Hawaii: ACM Press, 2002. 441 - 449.

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

[4] 赵克勤. 集对分析及其初步应用[M]. 杭州:浙江科学技术出版社, 2000.

[5] 张鹏,王光远. 新集对论[J]. 哈尔滨建筑大学学报, 2000, 33(3): 1 - 5.
Zhang Peng, Wang Guang-yuan. New theory of set pair[J]. Journal of Harbin University of Civil Engineering and Architecture, 2000, 33(3): 1 - 5. (in Chinese)

[6] 赵克勤,宣爱理. 集对论——一种新的不确定性理论方法与应用[J]. 系统工程, 1996, 14(1): 18 - 23.
Zhao Ke-qin, Xuan Ai-li. Set pair theory——a new theory method of non-define and its applications[J]. Systems Engineering, 1996, 14(1): 18 - 23. (in Chinese)

作者简介:

胡　波　男,1982 年生于河南信阳,南京邮电大学计算机科学与技术系硕士研究生,主要研究方向是计算机网络、计算机软件在通信中的应用和信息安全等.

王汝传　男,1943 年生于安徽合肥,教授、博士生导师. 主要研究方向是计算机软件、计算机网络和网格、信息安全、无线传感器网络、移动代理和虚拟现实技术等. E-mail: wangrc@njupt.edu.cn

王海艳　女,1974 年生于江苏扬州,南京邮电大学计算机系讲师,硕士,在读博士. 主要研究方向为计算机软件、计算机网络、信息安全、移动代理等.