

# A Reputation and Risk Model of P2P Network Based on Subjective Logic

MA Xiaoxue<sup>1</sup>, WANG Zixian<sup>2</sup>

1. Computing Center, Hebei University, Baoding, China

2. Modern Education Technical Center, The Central Institute for Correctional Police, Baoding, China

e-mail: snow@hbu.cn, bd\_wzx@126.com

**Abstract:** As P2P system is a dynamic open and anonymous system, and these seriously restrict P2P system of cooperation between the users and system reliability and availability. To improve the above problems, a trust model of P2P network based on reputation and risk is presented in this paper. Taking into account the influence on the calculation of confidence at different periods of trading, time decay function which different weight is distributed in accordance with the trading range of different periods has been introduced into this model. And at the same time, taking into account uncertainty that the dynamic behavior of the nodes effects the calculation of confidence, the risk factors have been introduced, which makes the impact of node trust by the malicious acts more sensitive through adjusting weight of credibility of the value and risk value appropriately. The simulation experiments and analysis shows that the model is able to identify malicious nodes effectively to a certain extent, and increase the successful proportion of transactions of the system.

**Keywords:** P2P; reputation; risk; subjective logic

## 基于主观逻辑的 P2P 风险信誉模型

马晓雪<sup>1</sup>, 王子贤<sup>2</sup>

1. 河北大学计算中心, 保定, 中国, 071002;

2. 中央司法警官学院, 现代教育技术中心, 保定, 中国, 071000

e-mail: snow@hbu.cn, bd\_wzx@126.com

**【摘要】** P2P 系统是一个动态、开放、匿名的系统, 为改善由于 P2P 系统特点带来的节点缺乏信任的问题, 提高 P2P 系统中用户行为的可靠性及成功交易比例, 本文给出了一种基于主观逻辑的 P2P 风险信誉模型, 引入风险因素, 通过调节信誉值和风险值来减小由于 P2P 系统中的动态行为引起的对信任度计算的不确定性, 使节点的信任度受各种行为的影响更灵敏。最后给出了仿真实验, 通过对实验结果的分析, 该模型对恶意行为有较好的抵抗性, 能提高系统交易成功的比例。

**【关键词】** P2P; 信誉; 风险; 主观逻辑

### 1 引言

由于 P2P 网络具有动态性、开放性和匿名性[1]等特点, 使得 P2P 网络应用中存在大量的欺诈行为以及不可靠的服务质量, 成为制约 P2P 网络进一步发展的主要原因。

信任反映的是一个实体对另一个实体行为以及能力的综合评价, 目前节点之间的信任问题主要靠建立信

任模型来解决[2-4]。在基于 PKI(Public Key Infrastructure) 的信任模型中存在少数领袖节点, 领袖节点的合法性由 CA 颁发证书加以保证, 领袖节点对其它节点的行为加以监督, 这类模型[5]存在着单点失效, 可扩展性差等问题。基于信誉 (Reputation Based) 的信任模型[5-7]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的情况下, 可以通过询

问朋友节点,依靠朋友节点的推荐来确定资源提供者可信度,由于这种机制在信誉度上的计算方式灵活,目前得到广泛的研究。

但现存的P2P信任管理模型普遍存两个弱点:

(1) 信誉值的计算主要依据节点的历史行为进行,但大多数模型将用户的历史行为作为一种离散信息进行考虑,对节点行为的持续性考虑不足,这样对那些长时间保持真实可信行为的节点用户缺乏激励机制。

(2) 不能有效防止恶意节点的协同作弊及策略节点的恶意行为。协同作弊是指多个恶意节点相互勾结,诋毁好节点,夸大同类节点的恶意行为,从而破坏整个系统的可用性;诋毁是指恶意节点通过给予其他节点不真实的较低评价从而对系统造成间接损害。

针对以上问题,本文提出了一种基于主观逻辑的P2P风险信誉模型RRMS (A Reputation and Risk Model of P2P Network Based on Subjective logic),在该模型中,节点依据主观逻辑理论,利用自己的交易经验和系统中其它节点的推荐,对和自己将要交易的节点进行信任度评估;考虑到不同类型恶意节点的攻击,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,通过适当设定信誉值和风险值的权重大小,调整节点的信任度受恶意行为的影响的灵敏度,在一定程度上达到惩罚节点恶意行为,增强系统可用性的目的。

## 2 主观逻辑

Jøsang 提出了主观逻辑(Subjective Logic)理论<sup>[8,91]</sup>并在此基础上对信任管理进行了研究,提出了证据空间(Evidence Space)和观念空间(Opinion Space)的概念来描述和度量信任关系。

### 2.1. Beta函数

概率论中的贝塔( $\beta$ , beta)分布的概率密度分布函数的数学形式为:

$$f(x) = \frac{1}{\text{beta}(\alpha, \beta)} x^{\alpha-1} (1-x)^{\beta-1} \quad (0 < x < 1, \alpha > 0, \beta > 0) \quad (1)$$

基金项目: 本文受河北省自然科学基金(F2008 000646); 河北省教育厅自然科学基金重点项目(ZH2 006006); 河北大学自然科学基金(2008Q51)资助

这样, 参数  $\text{beta}(\alpha, \beta)$  的含义为:

$$\text{bate}(\alpha, \beta) = \int_0^1 x^{\alpha-1} (1-x)^{\beta-1} dx \quad (2)$$

Bate分布变量 $x$ 只能出现在 $[0,1]$ 区间,符合信任概率的取值范围。

主观逻辑中的事实空间由肯定事件和否定事件组成,通过考察交易者的历史交易信息资料,交易执行成功次数用 $r$ 表示,交易执行失败次数用 $s$ 表示,用历史信息预测未来交易的可能性,可以基于Beta分布函数表述二项事件(Binary event)后验概率的思想来,构造概率确定性密度函数 $f(p|\alpha, \beta)$ , 其中

$$\alpha = r + 1 \quad \beta = s + 1 \quad (3)$$

参数 $p$ 是个概率参数,任意给定的 $p$ ,概率密度函数 $f(p|\alpha, \beta)$ 代表了一个后验概率,在本文中含义是:在系统已有历史交易信息中,交易成功的次数为 $\alpha - 1$ 次,交易失败的次数为 $\beta - 1$ 次,在此基础上,用来评估下一次交易成功的概率。

### 2.2. 主观逻辑

观念空间由一系列对陈述语句或命题的主观信任评估组成,主观信任度由三元组 $\omega_B^A = \{b_B^A, d_B^A, u_B^A\}$ 表示,该三元满足 $b_B^A + d_B^A + u_B^A = 1, b_B^A, d_B^A, u_B^A \in [0,1]$ ,其中 $\omega_B^A$ 表示节点A对B的主观信任, $b_B^A, d_B^A, u_B^A$ 分别描述节点A对节点B的信任程度、不信任程度和不确定程度。Jøsang 将 $\omega$ 定义为事实空间中肯定事件数 $r$ 和否定事件数 $s$ 的函数:

$$\begin{cases} b_B^A = r / (r + s + 2) \\ d_B^A = s / (r + s + 2) \\ u_B^A = 2 / (r + s + 2) \end{cases} \quad (4)$$

该函数称为证据映射函数(Evidence Mapping), Jøsang 在文献[10]中给出了该公式的合理性证明。

主观逻辑提供了推荐算子(Recommendation Operator)和合意算子(Consensus Operator),分别用于信任度的推导计算和对多个相同信任内容的独立信任观念进行综合计算。

推荐算子 $\otimes$ : 设 $\omega_B^A = \{b_B^A, d_B^A, u_B^A\}$ ,  $\omega_C^B = \{b_C^B, d_C^B, u_C^B\}$ , 则 $\omega_C^A = \{b_C^A, d_C^A, u_C^A\}$ , 其中

$$\begin{cases} b_C^{AB} = b_B^A * b_C^B \\ d_C^{AB} = d_B^A * d_C^B \\ u_C^{AB} = d_B^A + u_B^A + b_B^A * u_C^B \end{cases} \quad (5)$$

记为  $\omega_C^{AB} \equiv \omega_B^A \otimes \omega_C^B$ , 推荐算子可用来计算信任的传递。

合意算子  $\oplus$ : 设  $\omega_C^A = \{b_C^A, d_C^A, u_C^A\}$ ,  $\omega_C^B = \{b_C^B, d_C^B, u_C^B\}$  分别表示节点 A 和 B 对节点 C 的信任观念, 则节点 A 和 B 对节点 C 的综合信任观念  $\omega_C^{A,B} = \{b_C^{A,B}, d_C^{A,B}, u_C^{A,B}\}$  为:

$$\begin{cases} b_C^{A,B} = (b_C^A * u_C^B + b_C^B * u_C^A) / k \\ d_C^{A,B} = (d_C^A * u_C^B + d_C^B * u_C^A) / k \\ u_C^{A,B} = (u_C^A * u_C^B) / k \end{cases} \quad (6)$$

其中  $k = u_C^A + u_C^B - u_C^A * u_C^B$ ,  $k \neq 0$ , 记为

$\omega_C^{A,B} \equiv \omega_C^A \oplus \omega_C^B$ , 在信任推荐时, 可能存在多条推荐路径, 通过合意算子融合多个推荐信任值, 形成综合推荐信任度。

### 3 TMRR模型

#### 3.1 模型的建立

为了使讨论更具针对性, 本文以 P2P 文件下载环境为讨论对象, 在 TMRR 模型中涉及到的以下几个概念:

**定义 1: 直接信任  $T_d$** , 根据两个节点直接历史交易情况得出的信任值。

**定义 2: 推荐信任  $T_r$** , 根据其他节点的推荐得到的信任值。

**定义 3: 信誉  $R_e$** , 反映节点的长期行为, 本文由直接信任和推荐信任求的。

**定义 4: 风险  $R_i$** , 本文结合文献[14]将风险定义为在 P2P 系统文件下载过程中, 出现的和预期相反的结果的可能性, 以及在此情况下造成危害的程度的一种反映。

**定义 5: 信任度  $T_{ij}$** , 节点  $i$  对节点  $j$  行为的可信度评估, 通过在信誉  $R_e$  的基础上对风险  $R_i$  的追加求得, 与

节点  $j$  的可靠性、品质和性能等相关, 其值随节点的行为而动态变化。

该模型的节点交易过程如下:

在模型中, 每个节点都有一个信任计算引擎和一个交易管理器, 当一个节点需要某个资源时, 过程如下:

**Step1:** 服务请求者向其它所有用户发出服务查询, 查询具有自己需要的资源的节点。

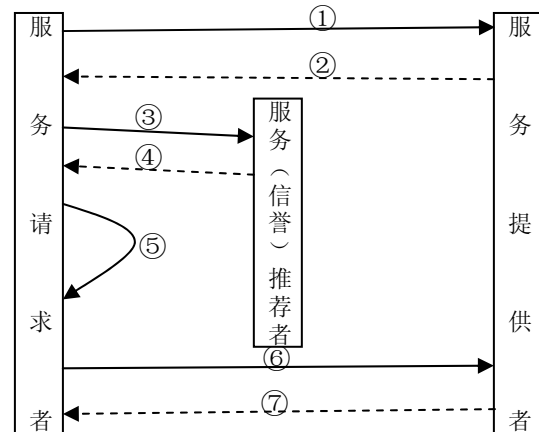


图 1. 系统节点交易过程

Figure 1. The transactions process among nodes

**Step2:** 拥有该资源的节点向服务请求者给出回应。

**Step3:** 服务请求者从这些回应者当中选择一个节点向信誉推荐者发出信誉查询。

**Step4:** 信誉推荐者收到查询信息后, 将自己了解的该节点的信誉值回应给服务请求者。

**Step5:** 服务请求者收到推荐信誉后综合自己的所掌握的信息采用一定的策略决定是否该信任这个服务提供者。如果可信进行 Step6, 否则返回 Step3。

**Step6:** 服务请求者向服务提供者发出执行服务的请求信息。

**Step7:** 服务提供者提供服务。

#### 3.2 信誉值的计算

##### 1、时间因素对信任计算的影响

由于信任具有动态性, 不同的历史信息对信任更新所产生的影响是不同的, 越近的历史信息所产生的影响应该越大, 当历史信息衰减到一定程度时, 所代表的历史信息对于节点的评估将失去指导意义。因此, 有必要引入时间衰减因子来反映历史信息的重要程度。在文献<sup>[10]</sup>中直接将时间衰减因子定义为一个常数显然不太合

理。本文先以当前时间为基准，按照一定的时间刻度向前划分不同的时间区间，按照不同时期的交易所属时间区间距离当前时间的远近程度，利用时间衰减函数，分配不同的权重。距离当前越近，赋予的权重越高；反之则越低。

**定义6: 时间衰减函数** $f$ ，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时间衰减函数，表示为

$$f(x) = f_k = \rho^{n-k} \quad (0 < \rho < 1, 1 \leq k \leq n) \quad (7)$$

这样利用定义好的时间衰减函数 $f$ ，对应于每个时间区间都有一个相应的时间衰减因子，如对应于时间区间 $t_k$ 的时间衰减因子为 $f_k$ ，同样可以得出，当前时间区间内发生的交易其时间衰减因子为 $f_n=1$ ，表示没有衰减；而首次交易相对于当前时间的衰减因子为 $f_1=\rho^{n-1}$ ，是衰减幅度最大的交易，位于相近的同一时间区间内的交易拥有相同的时间衰减因子。当 $\rho=1$ 时，表示历史信息不受时间衰减影响，当 $\rho=0$ 时，表示仅考虑最近一次的历史交易。

为了在 Beta 密度函数中引入时间衰减函数，引入变量  $q$ ，如果交易成功  $q=1$ ，否则  $q=0$ 。加入时间衰减因子后的 Beta 密度函数构造如下：

$$\begin{cases} r = f_k q_k \\ s = f_k (1 - q_k) \\ \alpha = r + 1 \\ \beta = s + 1 \end{cases} \quad (1 \leq k \leq n) \quad (8)$$

将 (7) 式带入 (4) 式，可求得随时间衰减后的节点 A 对节点 B 的主观信任  $\omega_B^A$ 。

### 2. 直接信任 $T_d$

通过前面分析可知， $\omega_B^A = \{b_B^A, d_B^A, u_B^A\}$  表示节点 A 对节点 B 的主观信任，其中  $b_B^A, d_B^A, u_B^A$  分别描述节点 A 对节点 B 的信任程度、不信任程度和不确定程度。取节点 A 对节点 B 的主观信任  $\omega_B^A$  中的信任程度  $b_B^A$  为直接信任度，即  $T_d = b_B^A$ ，如果节点 A 与节点 B 之间没

有直接历史交易，本模型中  $b_B^A = 0.5, d_B^A = 0, u_B^A = 0.5$ 。

### 3. 推荐信任 $T_r$

P2P 系统中，两个节点发生交易的次数有限，甚至从未有过交互，因此要全面评价一个节点，只靠自身直接交互经验并不完善，因此很多信任模型都是基于信誉的，通过综合其他节点对目标节点的一种综合评价，主要有两种基本结构：信任专递和信任合成。可通过公式 (5)、(6) 计算任意复杂的推荐信任，取合成后的信任程度为推荐信任度  $T_r$ 。

在 P2P 系统中，节点信誉度又高有低，信誉度高的节点的推荐比信任度低的节点的推荐应该更值得信赖，所以也必须对节点的推荐区别对待，给予不同的权重。

**定义 7:** 设  $P = \{P_1, P_2, \dots, P_n\}$  是推荐者集合， $P_r \in P (1 \leq r \leq n)$  表示推荐者  $r$ ， $P_r$  的推荐权重为  $\omega_{P_r}$ ，则推荐信任值  $T_r$  为：

$$T_r = \sum_{j=1}^n \omega_{P_r} R(P_r, j) / \sum_{r=1}^n \omega_{P_r} (P_r \in P) \quad (9)$$

其中， $R(P_r, j)$  为推荐者  $r$  对节点  $j$  的局部信任度， $\omega_{P_r}$  为  $r$  的推荐权重，在本文中  $\omega_{P_r}$  取值为推荐节点的信任值。

### 3. 信誉 $R_e$

信誉是对目标节点过去行为的主观评价，反映了节点长期历史行为的品质状况。相对节点  $i$ ，节点  $j$  的信誉值就是与节点  $i$  直接交互信任  $T_d$  和推荐信任  $T_r$  加权

$$R_e = \beta T_d + (1 - \beta) T_r \quad (0 \leq \beta \leq 1) \quad (10)$$

### 3.3 风险 $R_i$ 的计算

已有的基于推荐的信任模型中，大多只考虑了信誉值。信誉反映的是一个实体长期行为的累积，可以等同于信任。但对于恶意欺诈节点缺少必要的敏感性，如某些节点，一开始伪装成一个好节点，提供真实文件，等骗取较高的信誉度后，便开始利用其较高的信誉值欺骗请求下载文件的节点，给其提供不可信文件或虚假的推荐，甚至恶意文件；有的节点，按照一定比例提供真实

文件,从而使自己的信誉度能始终维持在系统规定的某个可信阈值之内,试图长期行骗,已达到自己的目的。由于信誉值下降较慢,这类节点无疑会给用户带来很大的危害,而风险的引入有助于解决这类问题。

风险是经济学上的概念,在经济学上,风险指损失发生的不确定性;是对事物在执行过程中出现和预期相反的结果的可能性,以及在此情况下造成危害的程度的一种反映。为了简化模型和提高效率,本文只考虑节点A和节点B两者之间直接交互的风险值,并且取节点A对节点B的主观信任 $\omega_B^A$ 中的不信任程度 $d_B^A$ 和不确定 $u_B^A$ 的和为风险度。

### 3.4 信任度的计算

节点信任度由节点的信誉 $R_e$ 和风险 $R_i$ 两部分确定,其中信誉 $R_e$ 又由节点间直接交互和其他节点推荐确定。风险用 $R_i$ 表示, $\alpha, \gamma$ 分别是二者的权重,则节点*i*对节点*j*的信任度为:

$$T_{ij} = \alpha R_e - \gamma R_i \quad (0 \leq \alpha, \gamma \leq 1) \quad (11)$$

上式 $\alpha, \gamma$ 的取值可根据请求节点*i*对被评价节点*j*交互的乐观程度,对*j*的行为及交互越乐观,选择 $\alpha / \gamma$ 值可越大,这样信任度受风险的影响越小;反之,选择 $\alpha / \gamma$ 值越小,信任度对风险影响越大,越敏感。为防

止节点的恶意行为,在p2p网络环境中, $\alpha / \gamma$ 的值应该设一个较大值,这样可以使满意的交易信誉值增加相对较慢,但不满意的交易信誉值下降却很快,使得节点受恶意行为的影响更敏感。

## 4 模拟实验及结果分析

信誉模型的作用是帮助系统中的用户评估其交互对象的信誉度,并决定是否在后续的交互中是否信任对方。一个有效的信誉模型应该能够最大化的维护合法用户的利益而遏制非法用户的各种欺骗行为,因此信誉系统有效性的重要评估标准就是用户的交互成功率RST(ratio of successful transaction),即整个信誉系统成功交易次数在所有交易次数中所占的比例。

为了验证本文研究内容的有效性,设置了一个与实际相近的试验场景。实验环境为P4 2.93GHz, 1G内存,

仿真基于Matlab实现。

### 4.1 实验 1

假设有三个节点peer1, peer2, peer3, 初始信誉值分别为: 0.5, 0.6, 0.9, 假设peer1为诚实节点, 在每次交互中总是提供真实可信的服务; peer2为欺骗节点, 在自身信誉值低于某个阈值时将为其其它节点提供真实可信的服务, 通过这些服务为自己积累信誉值, 而当自己的信誉值高于某个阈值时就会提供非真实不可信的服务; peer3为恶意节点, 该类节点始终为其它节点提供非真实不可信服务。这三种实体别代表了P2P环境下不同类型的节点。

设 $\alpha = 0.8, \beta = 0.8, \gamma = 0.2$ , 当peer2的信誉值低于0.5时, 该节点提供可信服务, 高于0.7时提供非真实不可信服务。各节点的信誉度随交互次数变化趋势如图2所示。

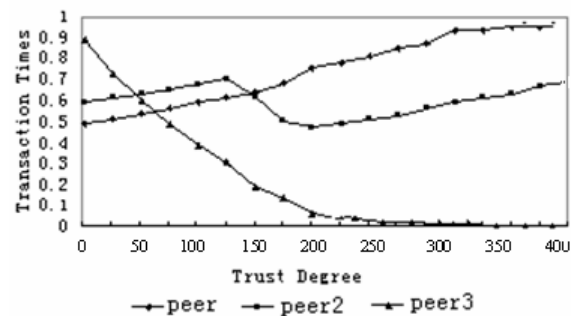


图2 模拟交互信任度

Figure 2. To simulate trustworthiness

从图1可以看出, 由于peer1节点一直提供诚实的服务, 虽然初始值为0.5, 但随着交互次数的增加, 其信任值也稳步增加。Peer2当信任值增加到0.7时, 开始提供非诚实服务, 信任值下降很快, 当信任值降到0.5以后, 又开始提供诚实服务, 信誉值增加缓慢, 其信任值增加和降低是不对称的, 可以有效减少恶意攻击的危害。Peer3一直提供非诚实服务, 其信任值下降最快。在该模型中, 可以通过调节参数 $\gamma$ 的取值来改变惩罚力度。

### 4.2 实验 2

图3是TMRR模型在 $\alpha, \beta, \gamma$ 在不同权重下系统成功交易对比(括号内分别为 $\alpha, \beta, \gamma$ 三者的权重, 为了简化

分析, 其中直接信任权重  $\beta$  取值为0.8), 其中 no-reputation system表示随机选择下载文件, TMRR (1, 0.8, 0) 表示忽略风险因素影响, 只采用信誉值作为交易选择要素。

从图3可以看出, 当系统中没有恶意节点时, 交易成功率都是100%, 随着恶意节点的增多, no reputation system 曲线下下降最快, 当系统中恶意节点增至50%时, 成功交易率只有50%左右。不考虑风险因素, 即

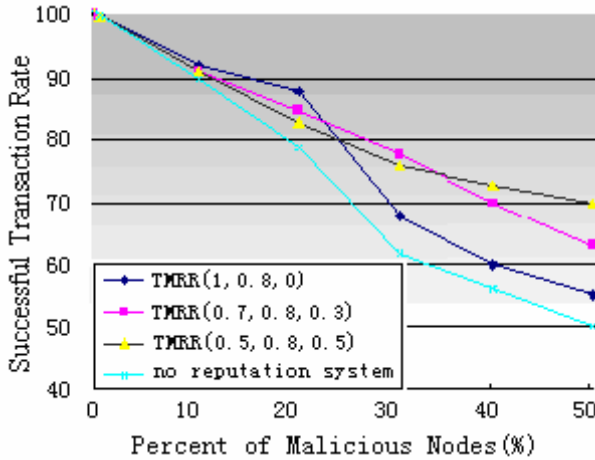


图 3.  $\alpha, \beta, \gamma$  不同权值对信任值的影响  
Figure 3. The affection of  $\alpha, \beta, \gamma$

$\alpha = 1, \lambda = 0$  时, 当恶意节点比例小于 20% 时, 成功交易率差别不大, 但随着恶意节点比例增大, 由于没有考虑惩罚机制, 曲线下下降也很快。

图 3 分别取 ( $\alpha = 0.7, \gamma = 0.3$ ) 和 ( $\alpha = 0.5, \gamma = 0.5$ ) 在不同权重下, 当系统中恶意节点比例较小时, 区别不大。但随着恶意节点的增多, ( $\alpha = 0.5, \gamma = 0.5$ ) 的优势更明显, 表明其风险权重分配更合适。通过实验表明, 在 P2P 系统中考虑风险因素非常必要, 并且当系统中恶意节点比例增多时, 适当增大风险权重系统仍然可以获得较高的成功交易比例。

## 5 结论与展望

在P2P系统中, 由于节点的动态行为影响信任度计算的不确定性, 本文引入风险因素, 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。通过仿真实验与分析, 表明该模型在一定程度上能够有效识别恶意节点。本文的风险机制过于简单, 在下一步研究工作中拟引入更复杂的风险机制, 更好地解决P2P中的信任问题。

## References (参考文献)

- [1] Wang Y, Vassileva J. Trust and reputation model in peer-to-peer networks. In: Proc of the 3rd Int'l Conf. on Peer-to-Peer Computing. IEEE Press, 2003. 150-157.
- [2] Zhu Junmao, Yang Shoubao, Fan Jianping, et al. A grid & P2P trust model based on recommendation evidence reasoning [J]. Journal of Computer Research and Development, 2005, 42(5): 797-803.
- [3] Jiang Shouxu, Li Jianzhong, et al. A novel Reputation-based mechanism for P2P Ecommerce systems[J]. Journal of software, 2007, 18(10): 2551-2563.
- [4] Z. Q. Liang, W. S. Shi. "PET: A Personalized trust model with reputation and risk evaluation for P2P resource sharing", the 38th Hawaii International Conference on System Science, 2005.
- [5] Altman J. PKI Security for JXTA overlay networks. Technical Report, TR-12-03-06, Palo Alto: Sun Microsystems, 2003.
- [6] 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.
- [7] Srivatsa M, Xiong L, Liu L. Trust guard: Countering vulnerabilities in reputation management for decentralized overlay networks. In: Ellis A, Hagino T, eds. Proc. of the 14th World Wide Web Conf. (WWW 2005). Chiba: ACM Press, 2005. 422-431.
- [8] Xiong L, Liu L. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans. on Knowledge and Data Engineering, 2004, 16(7): 843-857.
- [9] Jørgensen A. A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001, 9(3): 279-311.
- [10] Jørgensen A, Bhuiyan T. Optimal Trust Network Analysis with Subjective Logic. the 2nd International Conference on Emerging Security Information, Systems and Technologies. Cap Esterel, France, August 2008.