一种新的基于改进型 D-S 证据理论的 P2P 信任模型

田春岐[①②] 邹仕洪[①] 王文东[①] 程时端[①]
[①](北京邮电大学网络与交换技术国家重点实验室宽带网研究中心 北京 100876)
[②](同济大学电子与信息工程学院计算机科学与技术系 上海 200092)

摘 要：在大规模对等网(P2P)文件共享环境中，节点之间信任问题亟需解决。该文提出一种基于改进型D-S证据理论的P2P信任模型，给出了该模型的数学分析和抑制各类恶意节点攻击的措施。实验证明该算法较已有的一些信任机制在系统成功交易率、模型的安全性等问题上有较大改进。

关键词：对等网；D-S证据理论；信任；局部信任度
中图分类号：TP393 **文献标识码**：A **文章编号**：1009-5896(2008)06-1480-05

A New Trust Model Based on Advanced D-S Evidence Theory for P2P Networks

Tian Chun-qi[①②] Zou Shi-hong[①] Wang Wen-dong[①] Cheng Shi-duan[①]
[①](*Broadband Network Research Center*, *State Key Lab of Networking and Switching Technology*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)
[②](*Department of Computer Science and Technology*, *College of Electronic and Information Engineering*, *Tongji University*, *Shanghai* 20092, *China*)

Abstract: Trust relationship between participants is indispensable to set up in a large-scale distributed P2P file-sharing system. A novel trust model for P2P system based on advanced D-S theory of evidence is proposed in this paper to solve this problem, in which mathematic analysis and some measures are presented to defense against several malicious attacks. The experimental results show that, compared to the current some trust models, the proposed model is more robust on trust security problems and more advanced in successful transaction rate.

Key words: P2P; D-S theory of evidence; Trust; Local trust value

1 引言

P2P网络中节点之间信任问题是现在研究的热点。目前对其研究主要集中在为系统建立可靠的信任管理模型。基于共享信息的局部信任模型[1−5]与人际社会网络(social network)有很大的相似性，由于其在信誉度计算方式上的灵活性，得到了广泛的研究。然而，已有的这些机制还存在诸多不足之处，如没有给出矛盾推荐信息融合的可靠方法，在汇聚推荐信息时不能有效处理信息不确定性问题等等。

本文提出一种基于改进 D-S 证据理论 P2P 信任模型(a Advanced Dempster-Shafer Evidence Theory based Trust Model, AET^{2}M)，通过将节点的局部信任度表示为交易节点对其行为特征支持的证据，结合 P2P 文件共享系统的特性利用置信度对推荐证据建立数学模型，并对不同推荐证据的可靠性予以量化区分，给出了对信任不确定性判决的依据，然后利用改进的 D-S 证据合成准则实施融合，得出节点在全网范围内的可信度。实验证明了 AET^{2}M 具有抑制各类恶意节点攻击的有效性和健壮性，同时能较好评估 P2P 系统节点的信任度，在开放网络环境中具有很好的效果。

2006-11-13 收到，2007-05-21 改回
国家 973 项目(2003CB314806)和国家自然科学基金(60603060, 60502037, 90604019)资助课题

2 改进的证据合成规则

D-S 证据理论可以看作是有限域上对经典概率推理理论的一般化扩展，其主要特性是支持描述不同等级的精确度和直接引入了对未知不确定性的描述。基本 D-S 证据理论相关知识由于篇幅所限，此处不再赘述。

基本 D-S 证据合成规则能够融合多个证据源提供的证据，但是，Yager[6]指出：基本 D-S 合成公式在证据间没有冲突或低冲突时，证据的推理基本正常；但当证据间高度冲突时，合成的结果往往有悖常理。Yager 因此提出了一种新的合成公式，然而此公式也被证实当其应用于两个证据源时效果较好，当证据源多于两个时，合成结果却并不理想。主要原因：在基本 D-S 合成规则归一化过程中，将冲突信息完全抛弃，在数学结果上就引出不合常理问题；而后者是当两个证据高度冲突时，将冲突信息全部划分给全域，也就是未知项，以等待新的证据再作判断。 针对 Yager 公式新引入的问题，一种很自然的想法是不全部将冲突信息分配给未知

项，认为冲突信息部分可以利用。基于这一思想，文献[7,8]提出了各自的证据合成规则，各有优缺点。

我们认为，在组合规则中，即使证据之间存在冲突，它们也是部分可用的；冲突信息不能简单地被抛弃，而应该把支持证据冲突的概率分配给各个命题，从而提出改进的证据理论合成规则。通过把支持证据冲突的概率按各个命题的平均支持程度加权进行分配，提高了合成结果的可靠性与合理性，即使对于高度冲突的证据，也能够取得理想的合成结果。

$$\begin{cases} m(\Phi)=0 \\ m(A)=\sum\limits_{\cap A=A_i}\prod\limits_{1\le i\le n} m_i(A_i)+k\cdot f(A),\ \forall A\ne\Phi \end{cases} \tag{1}$$

式中 $k=\sum\limits_{\cap A_i=\Phi}\prod\limits_{0\le i\le n} m_i(A_i)=1-\sum\limits_{\cap A_i\ne\Phi}\prod\limits_{0\le i\le n} m_i(A_i)$，$f(A)=\sum\limits_{1\le i\le n} m_i(A)\Big/S_e$，$S_e=\sum\limits_{1\le i\le n} m_i(X)$，$X$ 是 n 个证据所有的焦元。

3　基于证据理论的 P2P 系统信任模型 AET^{2}M

P2P 网络是由许多节点组成的覆盖(overlay)网络，为了描述方便，本文以文件共享系统为例。假设节点在下载完成之后，按照下载的文件质量状况分为以下 4 类情况，(见表 1)。

表 1 下载文件种类描述

文件种类 (Category)	文件描述(Describe)
G(Good)	文件为所请求的且质量好
C(Common)	文件为所请求的但质量一般(保证对)
I(Inauthentic)	文件为不真实文件
M(Malicious)	文件为恶意文件(木马、病毒等)

3.1 基于推荐的 P2P 系统信任模型

P2P 系统中，两个节点直接发生交易的次数有限，甚至从未有过交易，因此要评价一个节点的可信程度，只靠自身直接交互经验是不充分的，所以基于推荐的信任模型得到了广泛的研究。下面先引入置信度的概念。

置信度　我们知道，节点的信任度是一个暂态值，因为节点的行为是随时间动态变化的，过去的信任度就不能代表一个节点目前的品质。为解决这个问题，引入与交易时间相关的时间窗口来刻画节点行为。时间窗口，实际上就是一段时间区间(窗口大小等同于区间长度)，用来表征节点在这段时间内的交易行为变化情况。窗口是随时间推进向前顺次滑移的，即上一个窗口结束的时间就是下一个窗口开始的时间。

在 AET^{2}M 中，节点本地存储的是从与之有过交易的节点上下载的不同质量状况文件的比例列表 $\{r_G,r_C,r_I,r_M\}$ (当然存储的还有关于推荐者的相关经验信息等，但是此处只关心前者)。如果节点 i 和 j 发生交易的时期为 $[t_{\text{start}},t_{\text{end}}]=[W_1,W_2,\cdots,W_n]$，其中 W_k $(1\le k\le n)$表示第 k 个时间窗口(发生的交易)，首次交易一定位于 W_1 窗口内，当前交易一定位于 W_n 内，令在时间窗口 W_k 内 i 节点与 j 节点交易后的结果记为 $\{r_{ij}^k(G),r_{ij}^k(C),r_{ij}^k(I),r_{ij}^k(M)\}$。

目前的信任模型中都区分不同时期交易对计算信任度的影响，且比较一致的做法是为不同时期的交易按距离当前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。在本模型中，我们提出一种衰减函数，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。

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

利用衰减函数 f，对应于每个时间窗口都有一个相应的衰减因子(函数值)，如对应于时间窗口 W_k 的衰减因子为 f_k。假设在最近的时间窗口 W_n 内 i 节点与 j 节点交易后的结果为 $\{r_{ij}^n(G),r_{ij}^n(C),r_{ij}^n(I),r_{ij}^n(M)\}$，如果在 W_{n-1} 窗口内两者交易的结果是 $\{r_{ij}^{n-1}(G),r_{ij}^{n-1}(C),r_{ij}^{n-1}(I),r_{ij}^{n-1}(M)\}$，使用衰减因子合成这两个窗口内交易后的结果是 $\{(r_{ij}^n+f_{n-1}r_{ij}^{n-1})(G),(r_{ij}^n+f_{n-1}r_{ij}^{n-1})(C),(r_{ij}^n+(1/f_{n-1})r_{ij}^{n-1})(I),(r_{ij}^n+(1/f_{n-1})r_{ij}^{n-1})(M)\}$。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 和 M 两种结果的叠加上使用衰减因子的倒数 $1/f_{n-1}$ (>1)。同理，所有时间窗口内交易的结果则为 $\left\{\left(\sum\limits_{k=1}^n f_k r_{ij}^k\right)(G),\left(\sum\limits_{k=1}^n f_k r_{ij}^k\right)(C),\left(\sum\limits_{k=1}^n (1/f_k) r_{ij}^k\right)(I),\left(\sum\limits_{k=1}^n (1/f_k) r_{ij}^k\right)(M)\right\}$。

定义 2　置信度　整个交易时间区间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。如上例，节点 i 与 j 交易的结果对 G,C,I,M 的置信度分别为 $\left(\sum\limits_{k=1}^n f_k r_{ij}^k\right)(G)\Big/S_{\text{GCIM}}$，$\left(\sum\limits_{k=1}^n f_k r_{ij}^k\right)(C)\Big/S_{\text{GCIM}}$，$\left(\sum\limits_{k=1}^n (1/f_k) r_{ij}^k\right)(I)\Big/S_{\text{GCIM}}$，和 $\left(\sum\limits_{k=1}^n (1/f_k) r_{ij}^k\right)(M)\Big/S_{\text{GCIM}}$，其中 $S_{\text{GCIM}}=\left(\sum\limits_{\substack{k=1\\T=G,C}}^n f_k r_{ij}^k\right)(T)+\left(\sum\limits_{\substack{k=1\\T=I,M}}^n 1/f_k r_{ij}^k\right)(T)$。

在 AET^{2}M 中，置信度只有在本地节点收到网络中某个节点关于另一节点在征求推荐信息时才计算的，而且在当前的窗口内如果还有其他节点欲获取该节点对同一节点的推荐信息，此计算出的置信度有效。

计算出节点 i 对节点 j 关于 G,C,I,M 的置信度后，就可以利用它来建立基本概率分配函数模型。

3.2 节点的基本概率分配(BPA)函数建模

我们知道，局部信任度来自于两个节点的直接交互历

史，是由下载的文件质量状况决定的。依据质量状况将下载文件分成了 4 类：G,C,I,M，所以识别框架就为 $\Theta=\{G,C,I,M\}$。节点 i 与节点 j 直接交互后，i 对 $\theta_j\in\Theta$ ($j=1,2,3,4$) 的置信度假如为 α_{ij}，满足条件 $\sum_{j=1}^{4}\alpha_{ij}=1$，我们就借助这个置信度建立节点 i 对 θ_j 的支持强度 $m(\{\theta_j\}|R_i)$，且后者应该是前者的一个单调增加函数(这个道理是显然的)，本文把这种关系简单取作一个线性函数：

$$m(\{\theta_j\}|R_i)=\lambda\alpha_{ij},\ j=1,2,3,4 \tag{2}$$

其中系数 λ 为区间 (0,1] 上的一个常系数。由于 α_{ij} 满足 $\sum_{j=1}^{4}\alpha_{ij}=1$ 式，因此可得

$$\sum_{j=1}^{4}m(\{\theta_j\}|R_i)\le 1 \tag{3}$$

为使m成为基本概率分配函数，补充定义

$$m(\Theta|R_i)=1-\sum_{j=1}^{4}m(\{\theta_j\}|R_i) \tag{4}$$

此时，由式(2)和式(4)定义的函数 $m(\bullet|R_i)$ 是一个基本概率分配函数，它的焦元至多包括 $\{\theta_j\}$ ($j=1,2,3,4$)和整个识别框架 Θ，这个函数就是节点的基本概率分配函数。它具有如下性质：当 $\forall A\subset\Theta$ 且 $|A|>1$ 或 $|A|=0$ 时，满足 $m(A)=0$。节点的基本概率分配函数模型得到之后，就可以计算节点的信任度了。

3.3 局部信任度的计算及推荐证据的合成

基于推荐的 P2P 网络信任模型在计算节点信任度时，分为两个步骤：一是计算局部信任度，局部信任度是在两节点交互结束后，发起请求的节点为响应的节点依据后者提供的文件质量给出的评价；二是聚合局部信任度，由发起请求的节点汇聚网络中与响应节点有过交易的节点的推荐信息而得。

局部信任度的计算 在 AET^{2}M 中，节点局部信任度被表示为与之有过交易的节点对该节点上传的不同质量状况的文件支持的证据。如节点 i 对节点 j 的局部信任度为 $R_{ij}=m_{ij}=\{m_{ij}(G),m_{ij}(C),m_{ij}(I),m_{ij}(M),m_{ij}(\Theta)\}$，式中 m 为框架 $\Theta=\{G,C,I,M\}$ 上的基本概率分配函数，具体 $m_{ij}(T),T=G,C,I,M,\Theta$ 的计算直接利用式(2)和式(4)。

推荐证据的合成及信任度评价方法 当节点 i 接收到关于对节点 j 的所有推荐信息时(推荐信息是推荐节点与 j 交互后对 G,C,I,M 支持的证据，所以也称推荐证据)，节点 i 就要对这些证据进行融合，融合方式采用的是我们改进的 D-S 证据理论合成规则。但是有一个实际的问题是，在 P2P 系统中，节点信誉度有高有低，信誉高的节点的推荐比信誉度低的推荐更应该值得信赖，所以也应该对节点的推荐区别对待，给予不同的权重。本方案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，他们没有动机破坏自己构造的网络，我们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。则我们对这些节点的基本概率分配函数定义为

$$\left.\begin{aligned} m(\{\theta_j\}|R_i)&=\frac{w_i}{w_k}\lambda\alpha_{ij},\ j=1,2,3,4,\\ m(\Theta|R_i)&=1-\sum_{j=1}^{4}m(\{\theta_j\}|R_i)\end{aligned}\right\} \tag{5}$$

在得到各个推荐的 BPA 函数后，节点 i 便利用式(1)对这些证据进行合成。

合成后的证据是一个统一的对 G,C,I,M,Θ 支持的比例列表，而不是一个具体的数值，而且我们通过做大量试验，发现合成证据中对 Θ 的支持强度已经很小，说明了汇聚各方推荐后已经能明确判断出被评价节点的可信程度。在我们信任模型中，判断一个节点信任度的方法是根据证据对各类结果(G,C,I,M,Θ)支持比例的相对强度，具体为(假设汇聚后证据对 G,C,I,M 的支持比例分别为 a,b,c,d)：

(1)若证据支持 I 和 M 类文件的比例不超过一定门限(两者门限值不同，$\text{Threshold}_I>\text{Threshold}_M$)，则可认为该节点是可信节点。这两个比例任一比例超过各自门限都视该节点为不可信节点。在文件共享系统中，不可信节点不应被选择为下载源，所以步骤到此为止；如果有多个节点都为不可信节点，需要判定节点信任度高低，则按 $c+\gamma d$ ($\gamma>1$)进行判决，$c+\gamma d$ 值越大，信任度越低；

(2)如果两个都为可信节点，则主要比较证据对 G 和 C 文件的联合支持强度，本方案用 $a+b/\eta$ ($\eta>1$)来表示该强度，$a+b/\eta$ 值越大，信任度越高；

(3)如果两个节点均为可信节点且证据对 G、C 联合支持强度相同，则按 $c+\gamma d$ ($\gamma>1$)比较证据对 I、M 的联合支持强度，$c+\gamma d$ 值越小越可信。

可以看出，本方案评定节点信任度的方法是柔性的、多尺度的，不同于一般信任机制仅仅是单一数值大小的比较，这是本方案的一个很大特点。

4 仿真及结果分析

本文仿真基于斯坦福大学开发的查询周期仿真器[10, 11]，同时，我们实现了 YuBin 方案[4]和 EigenRep[9]机制，并在简单恶意攻击、诋毁、合谋欺诈和复杂策略 4 种攻击模式下，分别对系统成功交易率(Successful Transaction Rate, STR)进行对比分析，即整个网络成功交易次数在所有交易次数中所占的比例。

仿真网络环境为：节点总数为 1000 个，其中恶意节点比例为[0.1–0.5]，好节点的度数为 4，恶意节点度数为 6，TTL 为 4。假设简单恶意节点以 40%比例提供可信文件。文件个数为 10000 个，文件种类为 100 个，文件在各节点均匀随机分布。其他参数设置见表 2。

表 2 仿真参数及其取值

参数	η	γ	ρ	λ	ξ	ζ	ε	δ	σ
数值	3	5	0.8	0.8	0.15	0.1	0.05	0.03	0.6

网络中恶意节点依据行为表现分为以下 4 种：简单恶意节点，此类节点只提供不真实的服务；诋毁节点，此类节点为与之有过交易的节点提供不真实的负面评价；合谋恶意节点(collusive)，即恶意节点互相勾结，诋毁好节点、夸大同类节点；具有策略的节点(strategy)，这类节点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，信誉度低时又以较高比例提供可信文件。

4.1 简单恶意节点(SM)及诋毁节点(DM)

图 1 和图 2 分别给出了在 SM 和 DM 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。

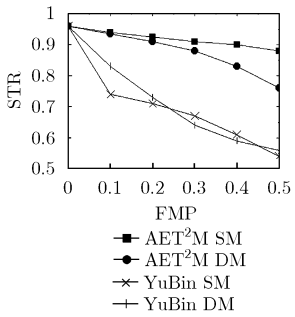

图 1 与 YuBin 方案成功交易率对比

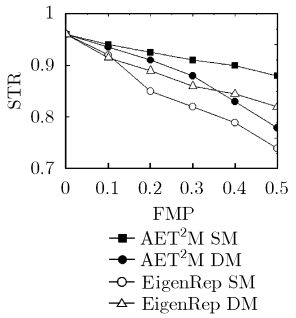

图 2 与 EigenRep 成功交易率对比

当系统中没有恶意节点时，成功交易率均为 96%。随着恶意节点比例的增加，3 种方案的成功交易率均呈下降趋势，但相比较而言本方案下降最为缓慢。YuBin 方案下降得最快，当系统中恶意节点比例达到 50%时，成功交易率只有 55%左右，这是因为 YuBin 方案没有区分不同时期的交易对计算信任度的影响，并且其直接采用了原始 D-S 证据合成法则，而该法则在合成冲突证据时有它本身的缺陷，从而造成节点信任计算误差大，故而会误将不可信节点作为下载源，导致无效交易增多，因此成功交易率下降最快。在 SM 类节点下，AET^{2}M 即使系统中恶意节点比例达到 50%时，系统成功交易率也在 85%左右；由于 EigenRep 模型对这种以一定比例随机提供真实服务的恶意节点(仿真中 SM 类节点对每个服务请求以 40%概率提供可信文件)欠缺惩罚机制，所以成功交易率也有较大的下降。

在DM类节点下，同样由于EigenRep 模型没有惩罚机制，因此诋毁这种攻击方式对其影响不大。而AET^{2}M能够有效地抑制诋毁攻击的影响，在系统节点中50%都为诋毁恶意节点的情况下，仍然具有80%左右的交易成功率。

4.2 合谋欺诈节点

图3是在Collusive类节点下3种机制成功交易率情况对比。由图可知，AET^{2}M在不同恶意节点比例下比EigenRep与YuBin方案均有较大优势。由于 EigenRep 模型对合谋作弊这类攻击未作任何处理，因此，随着此类节点比例的增加，恶意节点之间通过相互夸大可信度，从而吸引大量的交易，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。YuBin方案的成功交易率随恶意节点比例基本直线下降，也就是说该信任机制在合谋欺诈下性能很差。与之相反，AET^{2}M则明显抑制了合谋攻击，显示出强鲁棒性。

4.3 复杂策略节点

本文对这 3 种机制在具有复杂策略的恶意节点攻击下进行了成功交易率比较。仿真中假设 Strategy 节点信任度低于 0.5 则为不可信节点，同时假设该类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。从图 4 可以看出，由于 EigenRep 与 YuBin 方案均未对此类情况作任何处理，对节点的欺骗行为没有惩罚体制，因此系统的成功交易率随恶意节点比例的增大有较大幅度的下降。而 AET^{2}M 在不同恶意节点比例下相比较此两者有很大优势，这是因为 AET^{2}M 对由节点性能下降引起的无效交易增多现象给出明确的惩罚，同时体现在此节点信任度的计算上，有利于节点选择下载源，故而减少了有害或无效交易。

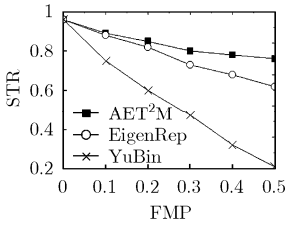

图3 Collusive下成功交易率对比

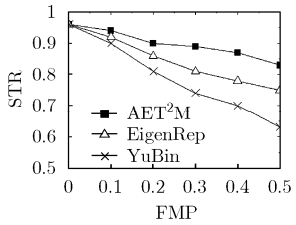

图4 Strategy下成功交易率对比

5 结束语

D-S 证据理论作为一种新兴的不确定性推理理论，已经被用于多个领域，本文探讨了其在 P2P 网络节点信任模型中的应用。本文提出了基于推荐机制的 P2P 信任管理模型 AET^{2}M，该模型克服了已有一些模型的若干局限性，仿真结果表明，该模型较相关研究工作在各类恶意节点不同程度地攻击强度下具有相当的优势，在大规模的开放网络环境中具有很好的效果。

参 考 文 献

[1] Damiani E, Vimercati D C, and Paraboschi S, *et al*.. Managing and sharing servants' reputation in p2p systems [J]. *IEEE Trans. on Knowledge and Data Engineering*, 2003, 15(4): 840–854.

[2] Cornelli F, Damiani E, and Vimercati D C, *et al*.. Choosing reputable servents in a P2P network. In Proceedings of the 11th International Conference of World Wide Web, Hawaii:

2002: 441–449.

[3] Xiong L and Liu L. Peertrust: Supporting reputation based trust for P2P electronic communities [J]. *IEEE Trans. on Knowledge and Data Engineering*, 2004, 16(7): 843–857.

[4] Yu B and Singh M P. An evidential model of distributed reputation management. Proceedings of the First International Conference on Autonomous Agents & Multiagent Systems (AAMAS), Bologna, Italy, July 2002: 82–93.

[5] Song S, Hwang K, and Zhou R F. Trusted P2P transactions with fuzzy reputation aggregation [J]. *IEEE Internet Computing*, 2005, 11(3): 18–28.

[6] Yager R R. On the Dempster-Shafer framework and new combination rules. *Information Science,* 1989, 41(2): 93–137.

[7] Xu H and Semt P. Some strategies for explanations in evidence reasoning [J]. *IEEE Trans. on System, Man and Cybern. Part A: Systems Human*, 1996, 26(5): 599–607.

[8] Takahiko H. Decision rule for pattern classification by integrating interval feature values [J]. *Pattern Analysis and Machine Intelligence*, 1998, 20(4): 440–447.

[9] 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: 123–134.

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

[11] Schlosser M, Condie T, and Kamvar S. Simulating a file-sharing P2P network. In First Workshop on Semantics in P2P and Grid Computing, California, December, 2003: 113–121.

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，副教授，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.

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.