一种新的基于概率统计论的 P2P 网络信任模型

徐海湄*①② 齐守青② 卢显良① 韩 宏①
①(电子科技大学计算机科学与工程学院 成都 610054)
②(解放军重庆通信学院 重庆 400035)

摘 要：经典的 P2P 网络信任模型采用迭代方法由局部信任值推算出全局信任值，每次交易都要引起整个网络节点的迭代运算，导致计算复杂，通信流量大，并且面临交易数据过于稀疏，计算不够精确从而容易陷于恶意节点的共谋、诋毁和睡眠等攻击问题。为了保证数据的稠密性与计算结果的精确性，论文基于概率统计理论，提出了一种新的全局信任模型。该模型根据节点的历史交易情况，运用最大似然估计，假设检验等方法计算出节点的信任度，节点选择与可信度高的节点进行交易。数学分析与仿真实验表明该模型能有效地抵抗恶意节点的攻击，与经典信任模型 Eigentrust 相比，较大程度地提高了整个 P2P 网络的成功交易率。

关键词：对等网络；概率统计论信任模型；最大似然估计；假设检验；交易历史记录
中图分类号：TP393 **文献标识码**： A **文章编号**：1009-5896(2011)06-1314-05
DOI: 10.3724/SP.J.1146.2010.00179

A Novel Trust Model of P2P Networks Based on Theory of Probability and Statistics

Xu Hai-mei①② Qi Shou-qing② Lu Xian-liang① Han Hong①
①(*School of Computer Science & Engineering*, *University of Electronic Science & Technology of China*, *Chengdu* 610054, *China*)
②(*College of Chongqing Communication*, *Chongqing* 400035, *China*)

Abstract: Classical trust model of P2P networks calculates the global trust value by iteration of local trust value. Every transaction will cause iteration throughout the whole networks resulting in computational complexity, huge communication traffic. These also face collusion attack, smear attack, sleeping attack and so on that caused by sparse transaction data and inaccurate computing result. To ensure the density of transaction data and the accuracy of computing result, a novel P2P global Probability and Statistics based trust (PStrust) model is presented. The history records of transaction are used to figure out the trust value of every peer by methods of the maximum likelihood estimation and hypothesis testing. Every peer trades with the peer with high credibility. Mathematical analysis and simulation show PStrust can resist attacks of malicious peers and improve the successful download rate of the whole P2P system compared with traditional model Eigentrust.

Key words: P2P network; Probability and Statistics based trust (PStrust) model; Maximum likelihood estimation; Hypothesis testing; History records of transactions

1 引言

对等网络技术因为其开放、匿名、自治等特点得到了广泛的应用，但是由此带来的安全问题、搭便车[1–3]等问题使系统的服务质量(QoS)严重下降。例如，一些节点利用 P2P 网络扩散病毒与伪造文件；70%的用户从来不共享任何文件，50%的文件查询响应依靠 1%的共享用户。解决上述问题的有效途径是建立信任机制，信任值高的节点获取到优质的 QoS，文献[4]提出的 Eigentrust 和文献[5]提出的 Peertrust 是比较经典的信任模型。

文献[6–12]在 Eigentrust 与 Peertrust 的基础上做了局部改进，但是没有克服两种算法的固有缺陷，依然采用迭代方法由局部信任值推算出全局信任值，每次交易要引起整个网络节点的迭代运算，导致计算复杂，通信流量大，并且容易陷于恶意节点的冒名、诋毁和共谋攻击。

网络规模巨大使任意两个节点之间的重复交易不容易发生，而对一个节点的反馈意见越多，越容

2010-03-01 收到，2011-04-06 改回
国家 973 计划项目(2009CB320403)和重庆市重点自然科学基金(CSTC, 2007ba2017)资助课题
*通信作者：徐海湄 xuhaimei@uestc.edu.cn

易把错误的偏见评价驱逐出去。如何汇聚所有节点的直接经验求出节点的全局信任值呢？为了保证数据的稠密性与计算结果的精确性，本文基于概率统计论[13−16]提出了一种新的 P2P 全局信任模型 PStrust(Probability and Statistics based trust model)，该模型克服了基于迭代方法的信任模型的计算复杂性，使全局信任值可以精确表示节点的可信程度，并且对恶意节点的攻击等安全问题进行了综合考虑。

2　全局信任模型 PStrust

2.1 全局信任值的计算

定义 1　节点的全局信任值

在当前时间周期 $T(t)$ 内，根据网络中所有节点与节点 i 的交易历史评估出节点 i 愿意提供服务的概率，称为节点 i 的全局信任值 $\theta_i, 0 \le \theta_i \le 1$，任意节点具有全局唯一的信任值。

$\theta_i = 1$ 表示无私节点 AN (Altruistic Nodes)，任何时候都以 100% 的概率为其他节点提供良好服务。$\theta_i = 0$ 表示自私节点 SN (Selfish Nodes)，任何时候都不提供服务或者提供虚假的恶意服务。$0 < \theta_i < 1$ 表示节点是混合节点 MN (Mixed Nodes)，自私行为获利大时则自私，无私行为获利大时则无私。

定义 2　交易记录

网络中两个节点每发生一次交易行为，接受服务的一方会给提供服务的一方做交易行为记录，简称交易记录。节点 i 对节点 j 的交易记录 $x_{ij} = \{s_{ij}, f_{ij}\}$，其中 s_{ij} 表示节点 j 提供给节点 i 的服务成功的次数，f_{ij} 表示节点 j 提供给节点 i 的服务失败的次数。

最大似然估计方法的原理[13−16]是根据从离散型随机变量 X 得到的样本 $X_1, X_2, \cdots, X_n$，取得联合分布率 $\prod_{i=1}^{n} P(x_i;\theta)$，构造出样本似然函数 $L(\theta)$，然后适当选取 $\hat{\theta}_i$，使 $L(\theta)$ 的值达到最大，也就是使实验得出结果 $X_1 = x_1, X_2 = x_2, \cdots, X_n = x_n$ 的概率最大。

汇聚网络中所有节点对节点 i 的交易记录 $x_{ji}(j = 1,2,\cdots,n)$，用最大似然估计方法求出节点 i 的全局信任值 θ_i。θ_i 的似然函数为

$$L(\theta_i, x_{1i}, x_{2i}, \cdots, x_{ni}) = \prod_{j=1,j\neq i}^{n} \theta_i^{s_{ji}} (1-\theta_i)^{f_{ji}} = \theta_i^{\sum_{j=1,j\neq i}^{n} s_{ji}} (1-\theta_i)^{\sum_{j=1,j\neq i}^{n} f_{ji}} \quad (1)$$

对数似然函数为

$$\phi(\theta_i) = \ln L(\theta_i) = \sum_{j=1,j\neq i}^{n} s_{ji} \ln \theta_i + \sum_{j=1,j\neq i}^{n} f_{ji} \ln(1-\theta_i) \quad (2)$$

似然方程为

$$\frac{d\phi(\theta_i)}{d\theta_i} = \frac{\sum_{j=1,j\neq i}^{n} s_{ji}}{\theta_i} - \frac{\sum_{j=1,j\neq i}^{n} f_{ji}}{1-\theta_i} = 0 \quad (3)$$

解得 θ_i 的最大似然估计值 $\hat{\theta}_i$ 为节点 i 的全局信任值。

2.2 全局信任值的估计误差

用最大似然估计方法给出节点 i 的全局信任值的估计量 $\hat{\theta}_i$，对了解 θ_i 的大小有一定的参考价值，如果给出 $\hat{\theta}_i$ 的精度和可信程度，则在工程上的可用性更强。

定义 3　节点 i 的信任值 θ_i 的置信区间与置信度

给定任意节点 i 的信任估计值 $\underline{\theta}_i$ 与 $\overline{\theta}_i$ ($\underline{\theta}_i < \overline{\theta}_i$)，构成随机区间 $(\underline{\theta}_i, \overline{\theta}_i)$，使此区间包含信任值 θ_i 的概率不小于设定的常数 $1-\alpha (0 < \alpha < 1)$，$(\underline{\theta}_i, \overline{\theta}_i)$ 称为信任值 θ_i 的置信区间[15]，$1-\alpha$ 称为 θ_i 的置信度[16]。

置信区间 $(\underline{\theta}_i, \overline{\theta}_i)$ 的长度 $L = \overline{\theta}_i - \underline{\theta}_i$ 越短，θ_i 的估计值 $\hat{\theta}_i$ 的精度就越高，$1-\alpha$ 越大，$\hat{\theta}_i$ 的可信程度就越大[16]。

定义 4　节点 j 的交易样本数量 $n = \sum_{i=1}^{N} (s_{ij} + f_{ij})$，其中 N 表示 P2P 网络中节点的总数量。

定理 1　当节点 j 的交易记录样本数量 n 很大 $(n \ge 30)$ 时，则节点 j 的信任评估值 $\hat{\theta}_j$ 近似服从正态分布 $\hat{\theta}_j \to N(\theta_j, \theta_j(1-\theta_j)/n)$，以 $\hat{\theta}_j$ 代替 θ_j，得到 θ_j 的置信度为 $1-\alpha$ 的近似置信区间为

$$(\hat{\theta}_j - Z_{\alpha/2}\sqrt{\hat{\theta}_j(1-\hat{\theta}_j)/n}, \hat{\theta}_j + Z_{\alpha/2}\sqrt{\hat{\theta}_j(1-\hat{\theta}_j)/n})$$

证明　令节点 j 的任意一个交易记录 $X = \begin{cases} 1, & \text{交易成功} \\ 0, & \text{交易失败} \end{cases}$，则 X 服从 Bernoulli 分布 $B(1,\theta_j)$，其中 θ_j 未知，$0 < \theta_j < 1$。根据中心极限定理[14,15]，当交易记录样本数量 n 很大 $(n \ge 30)$ 时，样本均值 $\overline{X}$ 近似服从正态分布 $N(\theta_j, \theta_j(1-\theta_j)/n)$，于是有 $(\overline{X} - \theta_j)/\sqrt{\theta_j(1-\theta_j)/n}$ 近似服从标准正态分布 $N(0,1)$，所以 $p\{|\overline{X} - \theta_j|/\sqrt{\theta_j(1-\theta_j)/n} < Z_{\alpha/2}\} = 1-\alpha$，为方便起见，可以写成

$$(\overline{X} - \theta_j)/\sqrt{\theta_j(1-\theta_j)/n} = (\overline{X} - \theta_j)\sqrt{n}/\sqrt{\theta_j(1-\theta_j)}$$

从而 θ_j 的置信度为 $1-\alpha$ 的置信区间为

$$(\hat{\theta}_j - Z_{\alpha/2}\sqrt{\hat{\theta}_j(1-\hat{\theta}_j)/n}, \hat{\theta}_j + Z_{\alpha/2}\sqrt{\hat{\theta}_j(1-\hat{\theta}_j)/n}) \quad (4)$$

证毕

定理 2　当节点 j 的信任值估计量为 $\hat{\theta}_j$，置信区间长度为 L，置信度为 $1-\alpha$，则样本容量 n 应该满足：$n \ge \hat{\theta}_j(1-\hat{\theta}_j)(2Z_{\alpha/2}/L)^2$。

证明　由定理 1 知 $(\overline{X} - \theta_j)/\sqrt{\theta_j(1-\theta_j)/n}$ 近似服从标准正态分布 $N(0,1)$，所以

$$p\{|\overline{X}-\theta_j|/\sqrt{\theta_j(1-\theta_j)/n}<Z_{\alpha/2}\}=1-\alpha \quad (5)$$

故 θ_j 的置信区间为 $(\overline{X}\pm Z_{\alpha/2}\sqrt{\theta_j(1-\theta_j)/n})$，置信区间长度为 $L=2Z_{\alpha/2}\sqrt{\theta_j(1-\theta_j)/n}$，因为样本数量越大则 $\hat{\theta}_j$ 的可信度越大[15,16]，因此令 $L\geq 2Z_{\alpha/2}\cdot\sqrt{\theta_j(1-\theta_j)/n}$，用估计值 $\hat{\theta}_j$ 代替 θ_j 求出 $n\geq\hat{\theta}_j(1-\hat{\theta}_j)(2Z_{\alpha/2}/L)^2$。 证毕

3 信任模型的安全性

3.1 诋毁与共谋攻击的抑制

诋毁指的是恶意节点故意给与之交易过的节点提供负面的评价，例如成功的交易被记录为不成功。

共谋攻击，即恶意节点相互勾结，诋毁团伙外的节点，抬高对同伙的评价。

根据节点的反馈行为将节点分为两大类：诚实节点与恶意节点。

诚实节点总是如实记录之交易过的节点行为。

恶意节点分为简单恶意节点，恶意集体，策略恶意节点 3 类。

简单恶意节点 SM(Simple Malicious)随机分布在网络中，通过反馈对正常交易行为进行诋毁。

恶意集体 CM(Collective Malicious)则是多个恶意节点形成联盟通过反馈行为对团伙外的节点进行诋毁，而对团伙内的节点提高反馈评价。

策略恶意节点 SM(Strategic Malicious)：这类节点先是以无私节点的身份提供良好服务，等信誉值升高以后，便诋毁无私节点，同时极力夸大自私节点，并且开始提供恶意服务。

值得注意的是一个交易行为可信的节点并不总是如实评价其他节点，例如以 100%的概率提供良好服务的无私节点并不一定是诚实节点，这在以往的经典模型 Eigentrust, Peertrust 中总是混为一谈。

本文采取假设检验方法将恶意节点筛选出来，用诚实节点的反馈评价评估出节点真实的信任值。

假设检验法的原理[14−17]如下：关于节点 j 的当前信任值 θ_j 的检验：令节点 j 的任意一个交易记录 $X=\begin{cases}1,\text{交易成功}\\0,\text{交易失败}\end{cases}$，则 X 服从 Bernoulli 分布 $B(1,\theta_j)$。

检验假设：$H_0:\theta_j=\theta_0$, $H_1:\theta_j\neq\theta_0$ 其中 θ_0 为已知常数；

当原假设 H_0 为真时，当交易记录样本数量 $n\geq 30$，检验统计量 $Z=\dfrac{\overline{X}-\theta_0}{\sqrt{\theta_0(1-\theta_0)/n}}$ 近似服从标准正态分布 $N(0,1)$，其中 $\overline{X}$ 表示样本均值；

给定显著水平 α，使 $P(|Z|\geq z_{\alpha/2})=\alpha$，则拒绝域为 $|Z|\geq z_{\alpha/2}$，计算检验统计量 Z 的观察值，根据该值是否落在拒绝域中，推断拒绝原假设或者接受原假设。

通过上述方法将恶意节点的反馈评价剔除，使利用最大似然估计得到的节点信任值更加精确。

3.2 睡眠攻击的抑制

睡眠攻击指的是一个节点通过连续提供优质服务给其他节点获取到了较高的信任值后，便不再提供服务，但是如果它利用高信任值索取太多的服务，即收益/贡献>>1，对于系统来说是不公平的。因此必须考虑每个时间周期内的交易次数，在越短的时间段内提供的服务次数越多，说明节点越活跃。

按照定理 1 与定理 2，根据置信度 1−α，置信区间 L，求出当前时间周期内计算节点 j 的信任值所需要的交易次数 N_{need}，而实际的可信交易次数用 N_{fact} 表示，如果 $N_{\text{need}}\leq N_{\text{fact}}$，根据最大似然估计方法计算出 $\theta_j(t)$，否则 $\theta_j(t-1)$ 按照指数衰减：

$$\theta_j(t)=\theta_j(t-1)(1-e^{-N_{\text{fact}}/N_{\text{need}}}) \quad (6)$$

由式(6)可以看出，信任值随着交易次数呈现负指数增长趋势，在交易次数较少时，信任值下降比较快，只有持续的给系统提供优质服务，才能维持较高的信任值。因此如果一个节点采取睡眠攻击时，它的信任值会很快下降。

4 仿真实验

为分析信任模型 PStrust，本文在 PeerSim[17]的基础上，基于 Java 编程建立了仿真环境。程序在配置为 Pentium Dual-Core E5300 2.6 GHz CPU, 2 GB Memory 的单机上运行。仿真的应用背景是文件共享，每次仿真由若干个周期 T 组成，每个周期内，节点通过一定的策略查找所需文件，并从所有拥有该文件的节点中选择信任值高的节点下载该文件，同理，节点选择信任值高的节点上传文件。每个节点在每个周期内进行 50 次查询，每次查询引起一次交易。每个周期结束时收集数据，进行计算后进入下一个周期，每个实验做 10 次，取平均值。第一个周期开始时候，每个节点的信任值为 $1/n$，n 为 P2P 规模。取其为 1500 个节点，其中无私节点与自私节点比例各占 35%，混合节点占 30%。在简单恶意节点攻击，恶意集体攻击，策略恶意节点攻击 3 种情形下，将 PStrust 与经典的信任模型 Eigentrust 进行了比较。

实验评估标准：下载成功率SDR(Successful Download Rate), SDR＝下载成功次数/要求下载的总次数。PStrust与Eigentrust作对比的时候，采取无私节点的SDR做对比，因为无私节点的SDR的变化直观地反映了信任模型的效果。

实验1　比较不同比例的简单恶意节点对信任模型PStrust和Eigentrust中无私节点的SDR的影响。

实验结果如图1所示，两种算法在恶意节点比例较小时候，整个网络中无私节点的SDR都比较高，但是随着恶意节点的增加，PStrust相对Eigentrust有所提高。这是因为恶意节点大幅增加时候，Eigentrust依然认为信任值高的节点反馈行为必然真实，导致节点的信誉度计算受到恶意节点的影响，而PStrust 只考虑诚实节点的反馈信息，即使恶意节点比例达到50%，使信任值的可信度依然维持在83%，而Eigentrust此时下降到60%。

实验2　简单恶意节点固定在30%，比较信任模型PStrust中3类节点的SDR的变化情况。

由图2中看出，随着时间推移，无私节点的SDR开始时候稍低，后逐渐升高，自私节点的SDR先维持在高水平，后急剧下降，而混合节点的SDR则先降低，后逐渐升高。这是因为在PStrust中，信任系统刚开始建立时，自私节点可以从无私节点处成功下载到文件，而随着时间推移，信任系统建立起来后，无私节点的信誉值越来越高，并保持在一个较高水平，自私节点的信任值则急速下降，无法继续从无私节点处得到服务。而混合策略节点看到自私行为无法获利，则终止自私行为，使信任值提高，从而使得SDR逐渐升高。这说明PStrust具有良好的激励无私行为，遏制自私行为的能力。

实验3　恶意集体的共谋攻击，比较此种情况下，两种系统中无私节点的SDR的变化情况。

从图 3 中看出，在恶意集体的共谋攻击下，Eigentrust 中无私节点 的 SDR 明显低于 PStrust, 这是因为在 Eigentrust 中，共谋攻击使恶意集体的信任值升高，无私节点被信任值高的恶意集体诋毁成功，信任值下降，而 PStrust 中利用假设检验方法将诚实集体与恶意集体分开，利用诚实集体的反馈信息求出节点的信任值，即使恶意集体比例达到50%，无私节点 SDR 保持在 81%，而此时的 Eigentrust 中，无私节点的 SDR 已经下降到 47%。

实验4　将策略恶意节点固定在35%，比较此种情况下两种系统中无私节点与自私节点策略恶意节点的SDR变化情况。

Eigentrust认为信任值高的节点的反馈信息的权重越高，随着策略恶意节点的活动，无私节点的信任值渐渐降低，SDR相应降低。而策略恶意节点由于提供恶意服务，信任值逐渐下降。在6个周期后，无私节点的声誉逐渐上升，由图4可以看出SDR也逐渐上升。而PStrust中，无私节点的声誉始终维持在较高的水平，这是因为信任值的计算只考虑诚实节点的反馈信息，并不受策略恶意节点的影响。

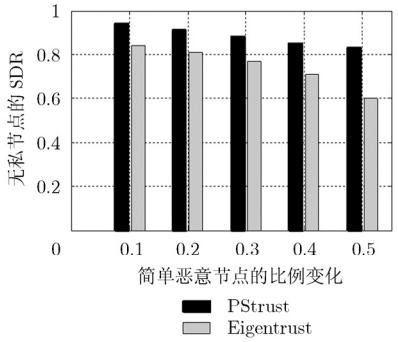

图1 SDR随简单恶意节点的变化情况

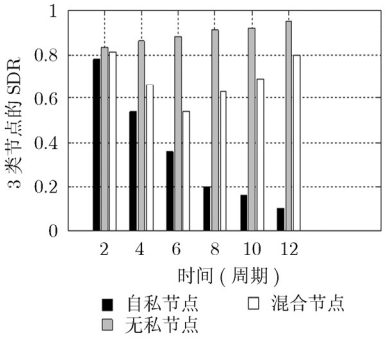

图2 3类节点的SDR随时间的变化情况

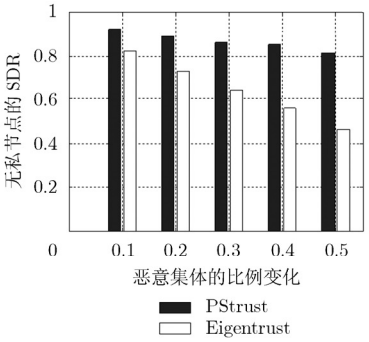

图3 SDR随恶意集体比例的变化情况

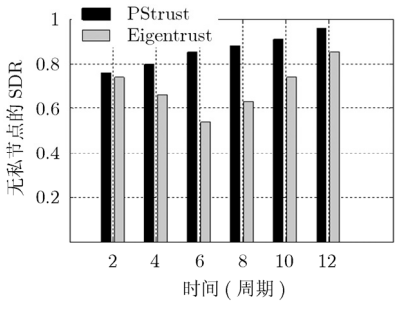

图 4 无私节点的 SDR 随时间的变化情况

5　结束语

本文针对 P2P 网络中的信任问题提出了基于概率统计理论的信任模型，根据最大似然估计方法计算出节点的全局信任值，并利用置信度与区间估计等方法求出信任值的精度与可信程度，使其在工程上更具实用性。而恶意节点通过假设检验的方法被剔除，使信任系统具有了抗诋毁和共谋攻击的能力，睡眠攻击则通过信任值在睡眠期间呈现指数衰减的

方法得到抑制。与 Eigentrust 对比，本文模型克服了迭代算法的复杂性，并有效地提高了交易成功率。但是实际的网络环境比较复杂，恶意节点的种类具有多样性与并发性，统计分析节点的行为特性比较复杂，如何在大规模分布式网络环境中进行全局信任值的计算与存储都需要考虑，因此使 PStrust 在工程上更容易实施，是下一步研究的重点。

参 考 文 献

[1] Feldman M and Chuang J. Overcoming free-riding behavior in Peer-to-Peer systems[J]. *ACM SIGecom Exchanges*, 2005, 5(4): 41–50.

[2] Kudtarkar A M and Umamaheswari S. Avoiding white washing in P2P networks [C]. The First International Conference on Communication Systems and Networks, Bangalore, India, 2009: 1–4.

[3] Ganesh Kumar M, Arun Ram K, and Ananya A R. Controling free riders in Peer to Peer networks by intelligent mining [C]. International Conference on Computer Engineering and Technology, Singapore, 2009, Vol. 1: 267–271.

[4] Kamvar S D and Schlosser M T. EigenRep: Reputation Management in P2P Networks [C]. The 12th International World Wide Web Conference, Budapest, Hungary, ACM Press, 2003: 123–134.

[5] Li Xiong and Ling Liu. PeerTrust: supporting reputation-based trust for Peer-to-Peer electronic communities [J]. *IEEE Transactions on Knowledge and Data Engineering*, 2004, 16(7): 843–857.

[6] 彭东生, 林闯, 刘卫东. 一种直接评价节点诚信度的分布式信任机制 [J]. 软件学报, 2008, 19(4): 946–955.
Peng Dong-sheng, Lin Chuang, and Liu Wei-dong. A distributed trust mechanism directly evaluating reputation of nodes[J]. *Journal of Software*, 2008, 19(4): 946–955.

[7] Wang Y F, Hori Y, and Sakurai K. Characterizing and reputation economic and social properties of trust and reputation systems in P2P environment [J]. *Journal of Computer Science and Technology*, 2008, 23(1): 129–140.

[8] 李景涛, 荆一楠, 肖晓春, 王雪平, 张根度. 基于相似度加权推荐的 P2P 环境下的信任模型[J]. 软件学报, 2007, 18(1): 157–167.
Li Jing-tao, Jing Yi-nan, Xiao Xiao-chun, Wang Xue-ping, and Zhang Gen-du. A trust model based on similarity-weighted recommendation for P2P enviroments[J]. *Journal of Software*, 2007, 18(1): 157–167.

[9] 张骞, 张霞, 文志学, 刘积仁, Ting Shan. Peer-to-Peer multiple-grain trust model [J]. 软件学报, 2006, 17(1): 96–107.
Zhang Qian, Zhang Xia, Wen Zhi-xue, Liu Ji-ren, and Ting Shan. Peer-to-Peer multiple-grain trust model [J]. *Journal of Software*, 2006, 17(1): 96–107.

[10] Zhou Run fang, Hwang Kai, and Cai Min. Gossips trust for fast reputation aggregation in peer-to-peer networks [J]. *IEEE Transactions on Knowledge and Data Engineering*, 2008, 20(9): 1282–1295.

[11] Zhou R and Hwang K. Powertrust: a robust and scalable reputation system for trusted P2P computing [J]. *IEEE Transactions on Parallel and Distributed Systems*, 2007, 18(4): 460–473.

[12] Niu Chang-yong, Luo Heng, Fan Ming, and Shen Rui-min. On feedback similarity measurement in web of trust [C]. IEEE Global Congress on Intelligent Systems, Xiamen, China, 2009, Vol. 3: 33–37.

[13] 滕素珍, 任玉杰, 斯琴. 概率论与数理统计大讲堂提高冲刺版 [M]. 2005, 大连: 大连理工大学出版社, 2005: 301–368.

[14] 孙清华, 孙昊. 概率论与数理统计内容、方法与技巧[M]. 武汉: 华中科技大学出版社, 2006: 201–290.

[15] 茆诗松, 周纪芗. 概率论与数理统计[M]. 北京: 中国统计出版社, 2007.12.

[16] Davison A. Statistical Models [M]. Cambridge: Cambridge University Press, 2003: 35–79.

[17] The PEERSIM website, http://peersim. sourceforge.net/ 2009-4-22.

徐海湄： 女，1974年生，博士生，研究方向为对等网络技术、分布式计算技术、P2P资源定位技术.

齐守青： 男，1974年生，讲师，研究方向为网络通信技术与通信对抗技术.

卢显良： 男，1943年生，教授，博士生导师，研究方向为分布式计算技术、网络通信技术、对等网络技术.

韩 宏： 女，1973年生，博士，副教授，研究方向为网络安全、软件工程.