一种 P2P 网络信任模型 METrust

于 真[1],申贵成[1],刘丙午[1],李京春[2],王少杰[2]
(1. 北京物资学院信息学院,北京 101149;2. 国家信息技术安全研究中心,北京 100094)

摘 要: Peer-to-Peer(P2P)网络的异构性、匿名性、自治性等特点导致了一些安全问题,比如伪造、诋毁、协同作弊等,影响了服务质量.提出了一种基于推荐的 P2P 网络信任模型 METrust,节点在网络中拥有唯一的推荐可信度,引入了更新幅度和更新力度两个参数来更新推荐可信度.给出了节点推荐可信度的更新算法;节点根据评价标准的相似程度选择推荐,其中节点的评价标准通过 AHP(Analytic Hierarchy Process)方法确定.仿真实验表明,METrust 信任模型可以识别恶意节点,有效提高 P2P 网络的服务质量.

关键词: Peer-to-Peer; 信任; 推荐; 评价标准
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2010) 11-2600-06

METrust: A Trust Model in P2P Networks

YU Zhen[1], SHEN Gui-cheng[1], LIU Bing-wu[1], LI Jing-chun[2], WANG Shao-jie[2]
(1. *School of Information, Beijing Wuzi University, Beijing* 101149, *China*;
2. *National Research Center for Information Technology Security, Beijing* 100094, *China*)

Abstract: In Peer-to-Peer (P2P) networks, peers' features such as heterogeneity, anonymity and autonomy lead to some security problems, such as forging, slandering and collective cheating, which affect the quality of service a lot. A trust model METrust in P2P networks based on the recommendation is proposed, each peer in the network has a unique credibility of recommendation, two trust parameters for updating the credibility of recommendation are introduced, namely updating range and updating strength. The trust model METrust proposes an algorithm to update the credibility of recommendation; a peer selects recommendation peers whose evaluation criteria are similar, evaluation criteria of peers are determined through the AHP method(Analytic Hierarchy Process). Simulations show that, the trust model METrust can identify malicious peers, and improve the quality of service in P2P networks effectively.

Key words: Peer-to-Peer; trust; recommendation; evaluation criteria

1 引言

近年来,P2P(Peer-to-Peer)技术[1]由于其特有的优势,得到了广泛应用.然而,P2P 网络的匿名性、自治性等特点也导致了一些安全问题,比如伪造、诋毁、协同作弊等,影响了服务质量.一些信任评价模型[2~4]对节点的可信程度从各方面进行衡量,并说明了在 P2P 网络中引入信任可有效识别恶意节点,对于保障 P2P 网络的服务质量有重要意义.

目前 P2P 网络中基于推荐的信任模型[4~7]大多是通过自身的交互经验和来自其他节点的推荐信息这两方面来确定服务节点的可信程度.如何确定节点的推荐可信程度是获取推荐信息的关键.为了能够有效获取推荐,本文提出了一种基于推荐的 P2P 网络信任模型 METrust,节点在网络中拥有唯一的推荐可信度,是该节点历次所提供推荐的可信程度的综合.仿真实验表明,METrust 可以识别网络中的恶意节点,并能有效提高服务质量.

2 相关工作

基于推荐的信任模型现已得到广泛应用,如 eBay[8]、Amazon[9],根据计算方法的不同,可分为全局信任模型和局部信任模型[10].EigenTrust[4]预设了一个固定的亚可信节点集合,实际中较难操作.文献[7]取消了预设节点集合,并对一些不良行为引入了惩罚措施,减少了迭代开销,但没有考虑节点评价差异,也没有对不诚实推荐节点实施惩罚.SWRTrust[11]在全局信任值上加入了节点评分行为的相似因素来表示推荐能力,在一定

收稿日期:2009-03-13;修回日期:2010-08-01
基金项目:国家 863 高技术研究发展计划(No.2007AA012474);北京市教委科技面上项目(No.KM201010037002)

程度上遏制了联合欺诈.文献[12]给出了一个多粒度信任模型.文献[13]将节点直接经验和其他节点的推荐通过加权平均合并到一起进行信任计算,但由于各节点的权重难以确定,影响对服务结果的判定,易造成不公平评价.文献[14]提出了一个针对恶意推荐者的信任模型,评价针对的是服务节点所提供的文件.文献[15]定义了可疑交易来识别虚假反馈.文献[16]提出了一个基于概率统计解释的信任模型.文献[17]采用了集对分析方法来解决信任计算中的不确定性问题.PeerTrust[5]引入了更多的可信度评价因素,从多个角度构造可信度,但计算代价较高.文献[6]利用 Bayesian 网络来表示信任的多面性问题,实质上基于节点自身的主观判定,具有局部片面性.这类局部信任模型[5,6]中,访问节点不能参考其他节点对于该推荐节点提供推荐的看法,恶意推荐节点也没有得到应有的惩罚,通过这种方式来获取推荐可信度开销较大.

3　P2P 网络信任模型 METrust

3.1　节点评价标准的确定

节点评价标准的不一致性会导致对服务节点的不公平评价,针对这一问题,本文提出的信任模型 METrust 考虑了节点的评价标准差异.节点需要确定自身的评价标准,并提供给其他节点作为交互的参考依据,节点的评价标准通过权重 n 元组来实现:

定义 1　节点 i 的权重 n 元组 $(W_{i1}, W_{i2}, \cdots, W_{in})$, $W_{im} \in [0,1]$, $m \in [1,n]$, $\sum_{m=1}^{n} W_{im} = 1$.其中 W_{im} 表示的是节点 i 的评价标准的第 m 个方面所占的权重,比如下载速度,文件质量等,n 表示 P2P 网络中的评价标准种类,节点可以按照自身偏好来配置权重.

在 METrust 中,权重的设定会直接影响到节点相似度的判断.为了提高节点各方面权重设置的准确度,使用层次分析法 AHP(Analytic Hierarchy Process)[18]来确定各节点的权重,可以得到准则层中各元素对目标层的权重向量,即 P2P 网络中的每个节点得到一个评价标准的权重表 $(W_{i1}, W_{i2}, \cdots, W_{in})$. METrust 建立的层次结构模型如图 1 所示,其中第一层为目标层,即选择一个服务节点,中间的准则层表示影响目标实现的准则,在本文中为节点的多个评价标准,最后的措施层为服务节点列表.

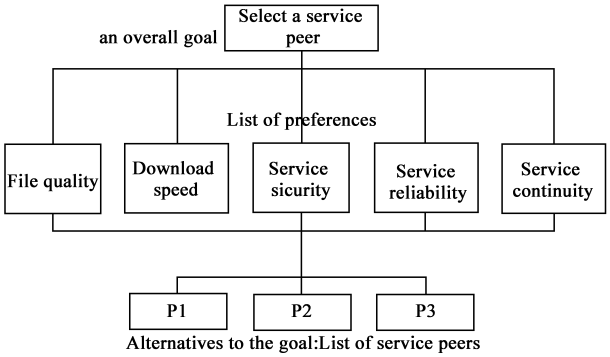

图1　层次结构模型图

3.2　信任值的度量

在 P2P 网络中,每个节点既可作为服务节点又可作为访问节点,同时为其它节点提供推荐.节点信任值通常可由公式(1)来计算[5,6]:

$$T_{ij} = \lambda \times D_{ij} + (1-\lambda) \times r_{ij}, \lambda \in [0,1] \quad (1)$$

其中,T_{ij} 表示在节点 i 看来服务节点 j 能提供服务的能力;D_{ij} 表示节点 i 对节点 j 的直接信任;r_{ij} 表示的是来自于各推荐节点的推荐信任;λ 表示节点自身对直接信任和推荐信任的侧重程度.

METrust 信任模型采用公式(1)进行信任值计算,选择信任值最高的服务节点.选择推荐节点的一个重要因素是节点评价标准的相似性.首先给出相关定义.

定义 2　交互满意度

$$S_{ij}^{k} = \sum_{n} W_{in} S_{ijn}^{k} \quad (2)$$

其中 S_{ij}^{k} 表示访问节点 i 在和服务节点 j 的第 k 次交互的综合满意度,$S_{ij}^{k} \in [0,1]$;S_{ijn}^{k} 表示该次交互中对第 n 个方面的满意度,$S_{ijn}^{k} \in [0,1]$.当 $S_{ij}^{k} \geqslant \alpha$ 时,表示交互成功,$\alpha \in [0,1]$,为满意度阈值.

定义 3　来自节点自身的直接信任

$$D_{ij} = \frac{\sum_{k=1}^{G_{ij}+B_{ij}} S_{ij}^{k}}{G_{ij} + B_{ij}}, D_{ij} \in [0,1] \quad (3)$$

其中 G_{ij} 表示节点 i 与节点 j 的成功交互次数,B_{ij} 表示失败交互次数.若两节点间没有直接交互经验,G_{ij} 与 B_{ij} 均为 0,则 D_{ij} 为 0.

定义 4　节点 i 与节点 j 的评价标准相似度

$$Sim_{ij} = \frac{\sum_{m=1}^{n} W_{im} \times W_{jm}}{\sqrt{\sum_{m=1}^{n} W_{im}^{2}} \times \sqrt{\sum_{m=1}^{n} W_{jm}^{2}}}, Sim_{ij} \in [0,1] \quad (4)$$

本文通过余弦相似度函数来刻画两节点的相似程度,比较的是两个节点间的评价标准.

定义 5　来自推荐节点的间接信任

$$r_{ij} = \frac{1}{\sum_{r \in I(j)} Sim_{ir}} \sum_{r \in I(j)} D_{rj} \times R_r \times Sim_{ir}; r_{ij} \in [0,1] \quad (5)$$

其中 $I(j)$ 为服务节点 j 的推荐节点集合.R_r 表示推荐节点 r 提供推荐的可信程度,即推荐可信度,在网络中有唯一值,来衡量该节点能否提供可信推荐,$R_r \in [0,1]$. METrust 在 $I(j)$ 中选择 $Sim_{ir} \geqslant \beta$ 的推荐节点,β

$\in[0,1]$,为相似度阈值,相似度较高的节点才有较大参考价值.

定义 6 节点 i 的更新幅度

$$U_c^i=\sqrt{2}^{5(c-Max_c)/Max_c},\ U_c^i\in(0,1] \tag{6}$$

节点在交互结束后,需要根据此次交互结果来更新其他推荐节点的推荐可信度. METrust 根据当前交互次数来确定更新幅度,更新幅度随着交互经验的增加而缓慢增长,当交互次数达到 Max_c 时,有足够经验后则可采取正常的更新幅度. 当交互次数较少时,更新幅度也较低,这样在一定程度上可避免恶意节点集团成员的恶意更新. c 为当前交互次数.

定义 7 针对服务节点 S,访问节点 i 成功下载后更新推荐节点的更新力度

$$P_i^s=\frac{\sum\limits_{k\in I(s)}G_{ks}}{\sum\limits_{k\in I(s)}G_{ks}+\sum\limits_{k\in I(s)}B_{ks}}\times R_i \tag{7}$$

失败下载后更新推荐节点的更新力度

$$P_i^s=\frac{\sum\limits_{k\in I(s)}B_{ks}}{\sum\limits_{k\in I(s)}G_{ks}+\sum\limits_{k\in I(s)}B_{ks}}\times R_i \tag{8}$$

其中,$I(s)$表示在服务节点 S 的所有推荐节点中与节点 i 评价标准相似的推荐节点集合. 更新力度通过集合 $I(s)$的主流次数占总交互次数的比率以及节点 i 的推荐可信度来确定.

3.3 推荐可信度更新算法

METrust 中每个节点都拥有唯一的推荐可信度,反映该节点在整个 P2P 网络中提供推荐的可信程度,体现了该节点的推荐"名声",并通过推荐可信度的更新来识别恶意推荐节点,保证网络的安全性.

METrust 中,节点需要对比直接信任之间的差异. 本文定义了节点 i 和节点 j 之间针对服务节点 S 的评价差异

$$diff_{ij}^s=|D_{is}-D_{js}|\times Sim_{ij} \tag{9}$$

METrust 中,针对服务节点 S,节点 i 使用以下公式更新节点 j 的推荐可信度:

(1)如果 $diff_{ij}^s<\theta$,推荐可信度更新公式为:

$$R_j=R_j+\left(P_i^s\times U_c^i\times(1-R_j)\times\frac{1-diff_{ij}^s/\theta}{2}\right)^{\frac{n}{1-R_j}} \tag{10}$$

(2)如果 $diff_{ij}^s\geqslant\theta$,推荐可信度更新公式为:

$$R_j=R_j\times\left(1-P_i^s\times\frac{U_c^i}{2}+P_i^s\times\frac{U_c^i}{2}\times\frac{\theta}{diff_{ij}^s}\right)^{\frac{R_j}{n}} \tag{11}$$

其中,n 为节点个数,各节点的初始推荐可信度为 1. 当评价差异小于容忍度时,节点 j 的推荐可信度增加,反之减小.

每个节点在作为服务节点时对应一个用于存放推荐节点信息的数据结构 RT,RT 及各节点的推荐可信度可通过分布式哈希表[19]放置于网络中;作为访问节点则对应一个存放本地服务节点信息的数据结构 LT. 访问节点在每次交互结束后,更新 LT 和服务节点对应的 RT,并执行推荐可信度更新算法,来更新各推荐节点的推荐可信度. 首先给出几个原语及其语义:

$I(i)$:节点 i 的推荐节点集合中与访问节点的评价标准相似的节点集合;

GetVal(ID_r, D_{rj}, R_r):从服务节点 j 的 RT 中读取 D_{rj} 并取得 R_r;

CalSim(ID_i, ID_r, Sim_{ir}):从服务节点 j 的 RT 中读取推荐节点 r 的权重,并计算 Sim_{ir};

CalDiff(ID_i, ID_r, D_{ij}, D_{rj}, Sim_{ir}):计算节点 i 和节点 r 之间的评价差异;

CalFactor(U_c^i, P_i^j):计算访问节点 i 针对服务节点 j 的各推荐节点的更新幅度和更新力度;

CalRecm($diff_{ir}^j$, θ, R_r):比较 $diff_{ir}^j$ 和 θ 的大小,并更新 R_r;

访问节点 i 更新服务节点 j 的各推荐节点的推荐可信度算法如下:

```
Procedure UpdateRecmTrust(ID_i, ID_j)
for (any r∈I(j) ! = i)
  GetVal(ID_r, D_rj, R_r);
  CalSim(ID_i, ID_r, Sim_ir);
  CalDiff(ID_i, ID_r, D_ij, D_rj, Sim_ir);
  CalFactor(U_c^i, P_i^j);
  With probability P_i^j, CalRecm(diff_ir^j, θ, R_r);
  endfor
end
```

3.4 信任模型开销

METrust 的主要开销在于推荐信任的更新,节点在更新推荐可信度时,仅需查询一轮该服务节点对应的推荐节点集合,并更新该集合中与自身相似的节点,消息复杂度为 $O(n)$,实际上,推荐节点集合中与自身相似的节点远小于网络规模,进一步减少了开销;网络中需要存储每个节点分别作为访问节点和服务节点的交互历史,并对每个节点记录一个推荐可信度.

4 仿真及结果分析

本文采用查询周期模型[20,21]进行仿真,构造了一个 P2P 文件共享网络. 仿真中,网络节点分为两类:正常节点和恶意节点. 仿真环境设置如表 1. 拓扑结构示例如图 2,白色区域内为正常节点;其他是恶意节点,比例为 10%.

表 1　仿真环境设置

网络	拓扑构造 节点规模 最少邻居数目 查询消息的 TTL		Power-law 100 个 3 4
服务	评价标准		下载速度 文件质量
节点	正常节点	活动状态 查询请求 进行响应 请求文件	100% 100% 匹配即响应 随机
	恶意节点	活动状态 查询请求 进行响应 请求文件	100% 100% 根据恶意行为响应 随机
内容	文件目录种类 节点共享的文件目录 节点共享的文件 在其目录中的分布		20 个 服从 Zipf 分布 均匀随机分布
仿真	仿真周期		500 次

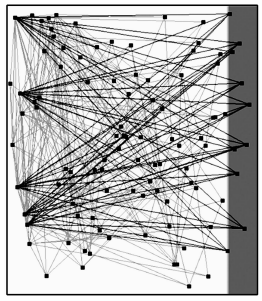

图2　仿真拓扑结构图

仿真实现了 EigenTrust 模型,采用 PSM 算法的 PeerTrust 模型,METrust 模型,及 Random 随机模型.性能评价指标为平均下载成功率,是正常节点的成功下载次数占其所有下载次数的比率.仿真包括了 4 类恶意行为,并分别在较复杂的 DM 类和 EM 类恶意行为时对四种模型进行了对比:

(1)简单恶意节点(IM 类):积极响应查询并提供虚假服务;

(2)恶意节点集团(CM 类):恶意节点形成集团进行联合欺诈,集合内成员除了具备 IM 类节点功能,还夸大同集合成员,诋毁其他正常节点;

(3)摇摆节点集团(DM 类):恶意节点除了构成 CM 类节点之外,还以概率 f 为其他节点提供可信文件和正常反馈,以便积累一些信任后进行其他恶意行为;

(4)伪装节点集团(EM 类):恶意节点不仅构成 CM,还有部分节点对外表现为正常节点,从而获得较高可信度,并给其他 CM 类恶意节点高评价.

4.1　DM 类节点

首先给出了各节点推荐可信度的变化情况.节点个数为 100,其中 1-90 为正常节点,其他为 DM 类节点.如图 3 所示,DM 类节点的推荐可信度随着交互周期的增加降低到一个较低值,而其他提供诚实推荐的节点的推荐可信度没有明显变化.

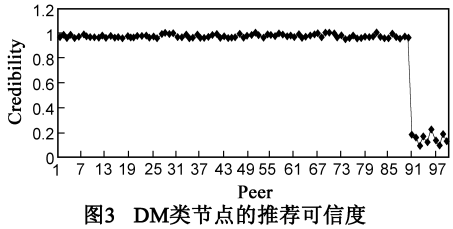

图3　DM类节点的推荐可信度

然后在恶意节点比例为 30%时,给出了概率 f 从 0 到 0.8 变化时的下载成功率.如图 4 所示,METrust 优于其他几类模型,对该类恶意节点具有抑制作用,由于恶意节点会以概率 f 来提供正常服务,因此随着概率 f 的增加,下载成功率不断升高.PeerTrust 可以识别部分 DM 类恶意节点,但是由于推荐可信度的判定基于双方的公共交互节点集合,当集合节点不足时难以判断.EigenTrust 在 DM 类节点存在时,效果较差,DM 类节点随着 f 的增加,恶意节点积累了部分信任值得以进行恶意行为,下载成功率降低,但是随着上载成本的增加,当概率 f 达到一定程度时,下载成功率缓慢增加,当 $f=0.3$附近时 DM 类节点恶意行为最强,DM 类节点可以破坏 EigenTrust.在 Random 中,由于其他节点提供正常服务的概率 f 逐渐增大,因此节点得到可信下载的机会也越多.

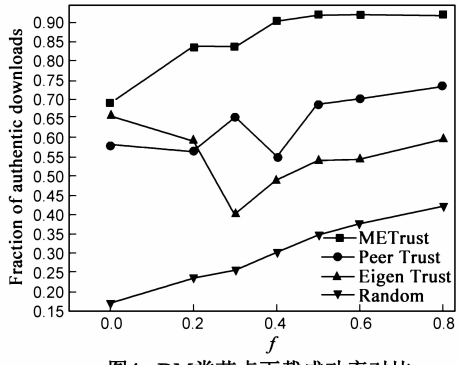

图4　DM类节点下载成功率对比

4.2　EM 类节点

首先给出了各节点推荐可信度的变化情况.节点个数为 100,其中 1 ~ 80 为正常节点;其余为恶意节点,50%即节点 85、86、87、89、91、94、95、96、98、100 组成 EM 类节点,剩余为 IM 类节点.从图 5 中可以看出 METrust 可以识别 EM 类恶意节点.

然后在恶意节点比例为 30%时,按照 EM 类节点所占的比例由 0%至 50%,对比了四种模型的下载成功率.如图 6 所示,METrust 较之其他几种模型,可以更好地抑制这种恶意行为,METrust 随着伪装节点占恶意节

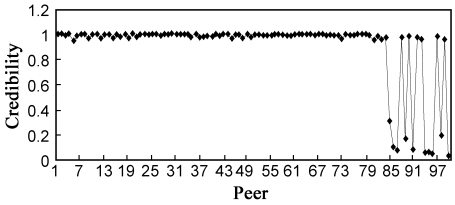

图5 EM类节点的推荐可信度

点比例的增大,下载成功率缓慢提高,这是由于伪装的恶意节点为了迅速取得较高的信任值,贡献了一部分成功的服务.PeerTrust 在一定程度上抑制了这种恶意行为,但是这种模型只依靠于双方的交互经验判断推荐节点的相似度,效果不太稳定.EigenTrust 的有效性较低,当 EM 类节点达到 20% 左右时,EigenTrust 有效性最低,此时恶意节点集团能够进行较多的恶意行为.该类节点对于 Random 没有影响.

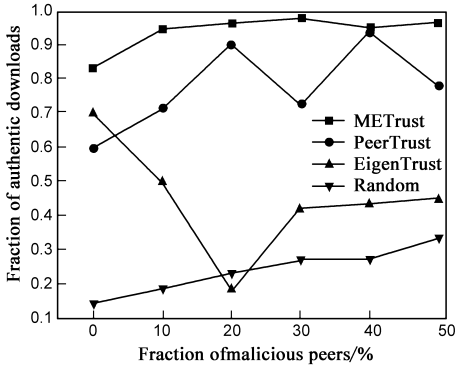

图6 EM类节点下载成功率对比

5 结论

本文提出了一种 P2P 网络信任模型 METrust,METrust 中每个节点被赋予了唯一的推荐可信度.分析和仿真实验表明,METrust 能以较小的开销评估节点的信任值,可以识别网络中的恶意节点,有效提高 P2P 网络的服务质量.

参考文献:

[1] A Oram. Peer-to-Peer: Harnessing the Power of Disruptive Technologies [M]. USA: O'Reilly and Associates, 2001.

[2] K Aberer, Z Despotovic. Managing Trust in a Peer-to-Peer Information System [A]. Proc. ACM Conf. Information and Knowledge Management (CIKM) [C]. USA: ACM Press, 2001.310 – 317.

[3] F Cornelli, E Damiani, S D C di Vimercati, et al. Choosing reputable systems in a P2P network [A]. Proc. 11th Int'l World Wide Web Conf [C]. Hawaii: ACM Press, 2002.441 – 449.

[4] S Kamvar, M Scholsser, H Garcia-Molina. The EigenTrust algorithm for reputation management in P2P networks [A]. Proc. 12th Int'l World Wide Web Conf [C]. NewYork: ACM Press, 2003.640 – 651.

[5] Y Wang, J Vassileva. Bayesian network-based trust model in peer-to-peer networks [A]. Proceedings of the Workshop on "Deception, Fraud and Trust in Agent Societies" at the Autonomous Agents and Multi Agent Systems 2003 (AAMAS-03) [C]. Berlin: Springer-Verlag, 2003.23 – 34.

[6] Li Xiong, Ling Liu. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities [J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 6(7): 843 – 857.

[7] 窦文,王怀民,贾焰,等.构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型[J].软件学报,2004,15(4):571 – 583.
Dou Wen, Wang Huai-Min, Jia Yan, et al. A recommendation-based peer-to-peer trust model [J]. Journal of Software, 2004, 15(4): 571 – 583. (in Chinese)

[8] eBay Web Site [OL]. http://www.ebay.com, 2009-03-10.

[9] Amazon.com [OL]. http://www.amazon.com, 2009-03-10.

[10] 张宇,陈华钧,姜晓红,盛浩,等.电子商务系统信任管理研究综述[J].电子学报,2008,36(10):2011 – 2020.
ZHANG Yu, CHEN Hua-jun, JIANG Xiao-hong, SHENG Hao, et al. A survey of trust management for e-commerce systems [J]. Acta Electronica Sinica, 2008, 36 (10): 2011 – 2012. (in Chinese)

[11] 李景涛,荆一楠,肖晓春,王雪平,等.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, et al. A trust model based on similarity-weighted recommendation for P2P environments [J]. JournalofSoftware, 2007, 18(1): 157 – 167. (in Chinese)

[12] 张骞,张霞,文学志,刘积仁,等.Peer-to-Peer 环境下多粒度 Trust 模型构造[J].软件学报,2006,17(1):96 – 107.
Zhang Qian, Zhang Xia, WenXue-zhi, Liu Ji-ren, et al. Construction of peer-to-peer multiple-grain trust model [J]. Journal of Software, 2006, 17(1): 96 – 107. (in Chinese)

[13] A Abdul-Rahman, S Hailes. Supporting trust in virtual communities [A]. In Proc. of the 33rd Hawaii International Conference on System Sciences [C]. Los Alamitos: IEEE Computer Society Press, 2000.132 – 141.

[14] S Y Lee, O H Kown, J Kim, S J Hong. Mitigating the impact of liars by reflecting peer's credibility on P2P file reputation systems [A]. Lecture Notes in Computer Science, Agents and Peer-to-Peer Computing [C]. Heidelberg: Springer, 2008.111 – 122.

[15] L Mekouar, Y Iraqi, R Boutaba. Detecting malicious peers in a reputation-based peer-to-peer system [OL]. http://bcr2.uwaterloo.ca/~iraqi/Papers/Conferences/CCNC2005.pdf, 2005-01-03.

[16] 徐锋,吕建,郑玮,曹春.一个软件服务协同中信任评估模型的设计[J].软件学报,2003,14(6):1043-1051.

Xu Feng, Lü Jian, Zheng Wei, Cao Cun. Design of a trust valuation model in software service coordination [J]. Journal of Software, 2003, 14(6): 1043 – 1051. (in Chinese)

[17] 胡波,王汝传,王海燕.基于集对分析的 P2P 网络安全中的信誉度改进算法[J].电子学报.2007,35(2):244 – 247. Hu Bo, WANG Ru-chuan, Wang Hai-yan. A modified security solution based on SPA for servents' reputations in P2P systems [J]. Acta Electronica Sinica, 2007, 35(2): 244 – 247. (in Chinese)

[18] Analytic Hierarchy Process [OL]. http://en.wikipedia.org/wiki/Analytic-Hierarchy_Process, 2010-08-01.

[19] Ratnasamy S. Routing algorithms for DHTs: Some open questions [A]. Kaashoek F, ed. Proc. of the 1st Int'l Workshop on Peer-to-Peer Systems [C]. Cambridge: Springer-Verlag, 2002. 45 – 52.

[20] QueryCycleSimulator [OL]. http://p2p.stanford.edu/www/demos.htm, 2009-03-10.

[21] M Schlosser, T Condie, S Kamvar. Simulating a File-Sharing P2P Network [OL]. http://nlp.stanford.edu/pubs/simulator.pdf, 2009-03-10.

作者简介:

于　真　女,1983 年生于山东聊城.北京物资学院教师,博士.研究方向为 P2P 技术、网络信息安全.
E-mail: yuzhenhappy@163.com

申贵成　男,1966 年生于江苏建湖.北京物资学院教授,博士.研究方向为信息安全、管理信息系统.