

## 基于拓扑势的 P2P 社区推荐信任模型

韩祺祎\* 任梦吟 文红

(电子科技大学通信抗干扰技术国家级重点实验室 成都 611731)

**摘要:** 对等网(P2P)系统因其开放性和匿名性等特点易受到恶意攻击和非法滥用, 建立基于社区的信任模型是一个行之有效的解决途径。而现有的模型忽略了节点的动态性、活跃度及影响范围。该文在分析了 P2P 用户模型后, 提出一种基于拓扑势的 P2P 社区推荐信任模型, 综合评估了节点的影响力、交易量及信任度。在该模型中, 分别建立了社区内部和跨社区信任度计算机制, 给出了超级节点评选算法。最后的仿真实验结果验证了该信任模型的有效性和鲁棒性。

**关键词:** 对等网(P2P); 信任; 拓扑势; 社区; 超级节点

**中图分类号:** TP393

**文献标识码:** A

**文章编号:** 1009-5896(2015)06-1279-06

**DOI:** 10.11999/JEIT141303

## Topological Potential Based Recommendation Trust Model for P2P Communities System

Han Qi-yi Ren Meng-yin Wen Hong

(National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China)

**Abstract:** The features of autonomy, anonymity and distribution make the P2P system vulnerable to malicious attack and abuse. A feasible resolution in such an open environment is to exploit a community-based trust model to build trust relationship between peers. However, the existing model ignores the dynamic feature, the scope of activity and the influence of peers. After analyzing the P2P user model, a topological potential based recommendation trust model is proposed to integrate the influences, transactions, and reputations of nodes. In this model, the trust metrics are divided into intra- and inter-community computing mechanism. Moreover, the algorithm of selecting super node is presented. Simulation results show that the proposed trust model is effective and robust.

**Key words:** P2P; Trust; Topological potential; Community; Super node

### 1 引言

开放性、匿名性以及分布式等本质使 P2P 得到广泛应用与蓬勃发展, 同时也为恶意用户恣意散播非法内容、滥用网络资源提供便利<sup>[1-4]</sup>。同时, 分布性与动态性使 P2P 用户之间难以维持熟悉、稳定和持久的交流共享。因此如何迅捷而安全地完成交流共享为 P2P 提出了挑战。

建立信任模型是解决这些问题的有效方案, 在信任模型中, 通过相互评价交易结果的社交管理方式来建立一套没有可信第三方和中心服务器的信任体系, 使用户通过选取可信度高的节点来完成交易。文献[5]提出了经典的全局信任模型, 用全局节点迭

代计算信任值的方法解决了 P2P 信任安全问题, 其中提出了先验信任节点(pre-trust node)的概念, 假设网络初始建立阶段参与的节点都是先验可信的, 没有考虑网络中各节点可信程度的动态变化和节点的相互作用。文献[6]改进 EigenRep 的信任模型, 取消了网络初始阶段参与节点的先验可信性。文献[7]及文献[8]提出了节点重要程度同样影响信任评价。文献[9]提出了基于概率和统计理论的信任模型, 降低了网络开销。文献[10]提出了基于相似度的信任模型, 加强了对恶意团体及诋毁节点的识别。文献[11,12]建立了分簇的信任模型, 提出在 P2P 网络中选取簇头节点作为推荐信任节点, 但忽略了节点的动态性, 没有提出合理的簇头选取方法。

已有的工作都是建立在信任值高的节点其反馈也更可信, 而忽略了节点的动态性、不同影响范围和活跃程度。因为其在线时间、参与交互的范围、

2014-10-11 收到, 2015-01-04 改回

国家自然科学基金(61032003, 61271172)和教育部博士点基金(20120185110030, 20130185130002, 20120185110025)资助课题

\*通信作者: 韩祺祎 Alex\_han@163.com

活跃程度和网络拓扑等的不同，一个节点可能因为短期内响应很局限的一些节点的请求而获得很高的信任评价，该节点的反馈的参考价值就不如一个在线时间长，响应范围很广，共享文件很多的较高信任评价的节点。

本文提出一种基于拓扑势的 P2P 社区推荐信任模型(TPRTrust)，将节点的信任度计算划分为社区内和跨社区分别进行讨论。社区内由于节点间更紧密的互动交易，采用基于相似度的推荐信任计算机制；跨社区的节点由于稀疏的交流互相并不熟悉，采用基于拓扑势的推荐信任计算机制。此外，本文采用拓扑势方法分析描述了节点的信任度和对社区内其他节点的影响，并且通过对节点的拓扑势进行排序，给出了超级节点的评选算法。最后给出仿真实验来验证有效性和鲁棒性。

## 2 P2P 用户分析

P2P 是自组织并且以客户为导向的网络，网络规模会根据实际节点的加入和退出动态地扩大和收缩。因此，大部分节点倾向于短期和直接的资源共享。

P2P 是一个开放的分布式网络，然而如图 1 所示，我们却发现一个无标度网络现象，用户遵循幂律分布<sup>[2]</sup>，即大量的用户只间断地贡献了少量的交易，而少量的活跃用户主导了大部分的交易所。而且新加入的用户也倾向与这些少量的活跃用户建立交易。这样交易贡献的不平衡导致了节点地位的不平等，使得 P2P 网络趋于部分分布式。此外，用户倾向于通过相似的兴趣、需求以及亲疏关系等结成小团体来交流和分享，由此产生了聚集成组群的社区划分现象<sup>[13]</sup>。其中可靠而活跃拥有大量朋友的中心节点(图中颜色较深的节点)将会影响和主导整个社区乃至整个网络的交易内容及行为模式。

因此，在基于社区的 P2P 网络中，稳定可靠又

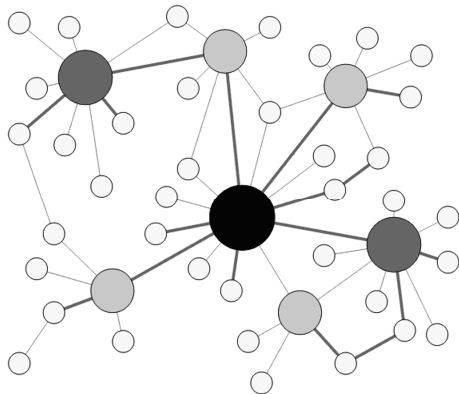


图 1 P2P 节点互动特征

愿意提供文件分享的中心节点成为代表自身社区的超级节点，赋予这些节点加权的可信度和更大的权利，可以保持 P2P 系统持续高效稳定的运行。

## 3 TPRTrust 信任模型

尽管 P2P 是分布式的网络架构，节点却倾向于小范围性的联合形成社区使得交流更加方便和可靠。本文采用基于社区的 P2P 网络结构，节点以相似的内容及兴趣聚集形成多个社区，这样交易主要在社区内部完成，信任管理的网络开销也很大程度上限制在局部范围内。

本文的 P2P 网络采用类似于 KaZaA 的社区结构，如图 2 所示，每个社区中，会有一个超级节点担负起类似于服务器的功能去实现路由、搜索以及信任管理等任务。这些超级节点成为局部的中心服务器以改善 P2P 缺乏中心协调和全局视野的情况。

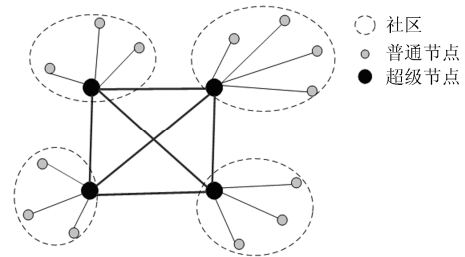


图 2 P2P 社区结构图

在 P2P 社区结构的基础上，我们将节点的信任度计算分为社区内部节点之间、超级节点信任度以及跨社区节点之间 3 种情况进行讨论。

### 3.1 社区内的信任度

我们先研究位于同一社区的节点之间的信任度计算问题。TPRTrust 中，同一社区内的节点信任度计算是按照基于相似度加权推荐的信任计算机制来进行的。社区内任意节点  $i$  具有唯一的信任度。

**定义 1 直接信任度** 直接信任度是节点  $i$  根据直接交易历史对节点  $j$  作出的信任评价，具体定义如下：

$$S(i, j) = \frac{\text{Sat}(i, j)}{\text{Sat}(i, j) + \text{Unsat}(i, j)} \quad (1)$$

式中  $\text{Sat}(i, j)$  表示满意的交易次数， $\text{Unsat}(i, j)$  表示不满意的交易次数，若没有交易历史，则直接信任度为 0。

**定义 2 相似度** 相似度描述了节点  $i$  与节点  $j$  之间信任评价的相似程度。相似度越高，则节点  $j$  与节点  $i$  对网络中其他节点的看法越一致。相似度有多种方式可以描述<sup>[14]</sup>，本文采用余弦相似度函数刻画相似度<sup>[15]</sup>，定义如下：

$$\text{Sim}(i, j) = \frac{\sum_k S(i, k)S(j, k)}{\sqrt{\sum_k S^2(i, k)}\sqrt{\sum_k S^2(j, k)}} \quad (2)$$

其中,  $S(i, k)$  由式(1)给出, 是直接信任度;  $k$  是与节点  $i$  和节点  $j$  都交易过的节点。若  $S(i, k)=0$ , 则  $\text{Sim}(i, j)$  取默认值 0.5。

用相似度去衡量自己与推荐节点之间的差异, 可以辨识出诋毁的节点。因此, 相似度加权的信任计算机制能让系统的公正性得到维护, 降低潜在的信任安全风险。

**定义 3** 社区内的节点信任度 在社区内部, 节点  $j$  表示与节点  $i$  有交易记录的节点; 共有  $N(j)$  个节点与节点  $i$  发生了数据交易;  $S(j, i)$  由式(1)给出, 表示节点  $j$  对节点  $i$  的直接信任度;  $\text{Sim}(j, i)$  由式(2)给出。那么, 社区内节点的信任度  $\text{Cr}(i)$  的计算如式(3):

$$\text{Cr}(i) = \sum_{j=1}^{N(j)} S(j, i)\text{Sim}(j, i)\text{Cr}(j) \quad (3)$$

式(3)中给出的信任度, 将由社区内全部节点迭代来计算, 其收敛性证明和网络开销可参考文献[5,6,8], 本文不再详述。

### 3.2 基于拓扑势的信任度

每个社区中, 超级节点不仅参与交易, 维护社区内的节点管理, 同时还存储节点跨社区交易的信任信息。因此, 需要综合评价节点的能力来推举超级节点。本文提出基于拓扑势的信任计算机制, 综合评估节点的影响力、交易量及信任度, 反映了节点的交易活跃度、在线稳定性及诚实的行为, 在开放和动态的 P2P 环境中保持信任的有效性和鲁棒性。

**3.2.1 拓扑势的引入** 网络中每个节点周围都存在一个虚拟的作用场, 节点之间都受到其它节点的联合作用<sup>[16]</sup>, 节点在网络结构中的拓扑位置确定了节点所处的位势和它影响相邻节点的能力。为刻画节点间相互作用的局域性以及影响随着网络距离而快速衰减的特性, 采用代表短程场作用的高斯势函数来描述节点间相互作用, 称相应的场为拓扑势场<sup>[17]</sup>。

**定义 4** 拓扑势 给定网络  $G = (V, E)$ , 其中  $V = \{v_1, v_2, \dots, v_n\}$  表示网络  $G$  中节点的集合,  $E \subseteq V \times V$  为边的集合且  $|E| = m$  为网络中边的数目。任意节点  $v_i \in V$  的拓扑势定义为

$$\varphi(v_i) = \sum_{j=1}^n \left( m_j \times e^{-\left(\frac{d_{ij}}{\sigma}\right)^2} \right) \quad (4)$$

其中  $d_{ij}$  表示节点  $v_i$  和  $v_j$  间的距离, 以最短路径来度量; 影响因子  $\sigma$  用于控制每个节点的影响范围, 每

个节点的影响范围近似为  $[3\sigma/\sqrt{2}]$  跳的局部区域, 当距离大于  $[3\sigma/\sqrt{2}]$  跳时, 势函数迅速衰减为 0。  $m_i \geq 0$  表示节点  $v_i$  ( $i = 1, 2, \dots, n$ ) 的质量, 用以描述每个节点的固有属性。在真实网络中,  $m_i$  用来描述社会网络中个体的活跃度以及通信网络中节点的软硬件资源等<sup>[18]</sup>。

**3.2.2 拓扑势理论改进的信任度** 在 P2P 信任安全模型中, 我们将节点间进行交易并相互信任的关系也用拓扑势的方式进行描述。在本文中对 P2P 节点的综合可信度考虑 3 个属性: 节点之间在交易关系网络中的最短跳数, 交易次数以及信任度。

**定义 5** 基于拓扑势的信任度 节点  $i$  的基于拓扑势的信任度计算公式定义为

$$P(i) = \sum_{j=1}^l \text{Cr}(j) \times e^{-\left(\frac{d(i, j)}{\sigma}\right)^2} \quad (5)$$

其中,  $\text{Cr}(j)$  是节点  $j$  的信任度, 由式(3)给出;  $d(i, j)$  是节点  $j$  到节点  $i$  的最短跳数; 影响因子  $\sigma = \lambda(1 - 1/e^{n_j/3})$ , 系数  $\lambda$  由社区规模决定,  $n_j$  是节点  $j$  的历史交易次数, 一个交易次数较多的节点影响因子越大影响范围也越远。

节点  $j$  的信任度越高, 历史交易次数越多, 到节点  $i$  的跳数越少, 则该节点对节点  $i$  的作用越大, 反之亦然。节点  $i$  的拓扑势为所有节点对它作用的总和。由式(5)分析可知, 在 P2P 网络中, 交易密集区的节点具有较高的拓扑势。拓扑势既体现了 P2P 节点信任评价的属性信息, 也定量反映了节点的交易对象和交易量。

因为 P2P 是分布式网络, 其中的节点不清楚全局网络的具体拓扑结构, 难以察觉哪些节点地位更重要。但在基于社区的 P2P 中, 超级节点成为局部的中心服务器。超级节点的拓扑势计算将局限在社区内部, 并不辐射整个网络拓扑结构, 既利用了超级节点的功能的同时也限制了网络开销。

**3.2.3 超级节点的评选** 超级节点需要管理和维护一个社区的查询请求和信任信息, 评选超级节点要根据节点的硬件性能、信任度、在线时间及邻居数目等能力综合量化和排序, 本文将节点的基于拓扑势的信任度作为量化标准, 综合考虑节点的信任度、交易数量及拓扑影响力进行评选。具体算法如下。

#### 算法 1 超级节点评选算法

输入: 数据交易关系矩阵  $G = (V, E)$ , 信任度向量  $\text{Cr}(V)$

输出: 备选超级节点  $\text{Sp}'$

for each  $v_i \in V$

$d(i, j), n_j, \text{Cr}(j) \leftarrow G(V, E), \text{Cr}(V)$

$P(v_i) \leftarrow$  计算式(5);

$\text{Rank}(P(v_i))$ ;

end for

return  $\text{Sp}' \leftarrow v_i = \arg \max(P(v_i))$

由于 P2P 节点的动态性, 社区拓扑及节点信任度都是动态变化的。当超级节点的基于拓扑势的信任度低于一定门限或离线失效时, 则运行算法 1 得到的备选超级节点接替超级节点的位置, 此外整个社区也会周期性地(本文中设置为 10 min)运行算法 1, 评选超级节点。

### 3.3 跨社区的信任度

当不属于同一社区的两个节点  $i$  与  $j$  发生交易时, 需要跨社区的信任度来参考是否执行交易。而跨社区的交易比社区内部的交易稀疏, 节点对另一个社区不了解, 两个节点之间也几乎没有共同的交易伙伴, 相似度没有参考价值。因此, 用社区信任度来描述节点  $j$  所在社区的整体可信度, 以及该社区内其他节点的推荐来计算跨社区节点之间的信任度。

**3.3.1 社区信任度** 在基于社区的 P2P 网络架构中, 注意到社区中的超级节点连接到多个其它的社区, 且超级节点内保存有跨社区的交易记录, 所以超级节点还能起到监督相邻社区的作用。

$S(C_j, C_i)$  由式(1)给出, 代表社区  $j$  内所有节点对社区  $i$  内所有节点的交易历史总和;  $N(C_i)$  代表与社区  $i$  发生过数据交易的社区数;  $P(\text{Sp}_j)$  由式(5)给出, 代表社区  $j$  的超级节点基于拓扑势的信任度。那么社区  $i$  的信任度为

$$\text{Cm}(C_i) = \frac{\sum_{j=1}^{N(C_i)} S(C_j, C_i) P(\text{Sp}_j)}{\sum_{j=1}^{N(C_i)} P(\text{Sp}_j)} \quad (6)$$

社区信任度由超级节点来管理, 超级节点虽然处于不同的社区, 可是由于它们之间的直连性保证了超级节点之间的相互监督, 最终制约社区中恶意节点的不良行为。

**3.3.2 跨社区节点之间的信任度计算** 节点  $i$  对跨社区的节点  $j$  的信任度  $R(i, j)$  为

$$R(i, j) = \sum_{k=1}^{N(k)} S(k, j) \text{Cm}(j) \text{Cr}(k) \quad (7)$$

节点  $k$  表示与节点  $j$  在同一个社区并且有交易记录的节点;  $N(k)$  代表节点  $k$  的个数;  $S(k, j)$  由式(1)给出;  $\text{Cm}(j)$  由式(6)给出;  $\text{Cr}(k)$  由式(3)给出。

式(7)中, 用社区信任度加权推荐信任来计算跨社区节点之间的信任度。在跨社区交易稀疏的情况下, 用社区内节点总体的信任度来规范跨社区的交易行为。

## 4 仿真实验与分析

### 4.1 仿真设置

本文在 OVERSIM<sup>[19]</sup>平台上仿真 P2P 文件共享系统, 实现了 TPRTrust 模型, 并与 GossipTrust<sup>[8]</sup>模型进行了比较。全网 1000 个节点随机分布在 20 个社区中。仿真运行了 60 min。其中, 平均每分钟每个节点发生且完成了 2 次数据交易。

网络中节点分为以下类型:

(1)正常节点(NN): 正常节点无论在提供服务上还是在对其他节点的反馈评价上都是真实的。

(2)简单恶意节点(SM): 这类恶意节点不仅提供恶意服务, 同时也诋毁信任评价。

(3)策略恶意节点(TM): 这类节点在未评选上超级节点时扮演正常节点, 等到信任度提高评选上超级节点后就转变为恶意团体节点。

(4)恶意团体(CM): 这类节点相互串通, 对与之交易的正常节点提供恶意服务, 并且相互合作夸大同类, 诋毁正常节点。

在仿真中, 我们通过预先设定节点恶意率来规定节点的恶意倾向。这个比率称为恶意节点率 MNR(Malicious Node Ratio)。我们定义如下一些性能评估参数:

(1)识别率 IR(Identifying Ratio): IR=由信任模型检测出来的恶意节点数/总的恶意节点数, 信任度低于门限值 0.3 即被判定为恶意节点;

(2)下载成功率 SDR(Successful Download Rate): SDR=下载成功次数/下载的总次数。

### 4.2 仿真结果分析

#### 实验 1 节点的动态性对网络的下载成功率影响

如图 3 所示, 在 TPRTrust 模型下, 我们仿真了超级节点(SP)和普通节点(NP)不同生存时间的下载成功率。结果表明在简单恶意节点的攻击以及节点加入离开的动态干扰下, TPRTrust 模型依然保持了较高的下载成功率。此外, 我们发现超级节点的在线时间越长, 下载成功率越高。而普通节点的在线时间对下载成功率影响也符合这个规律, 只是相对超级节点没有那么明显。由此可见, 一个稳定在线的超级节点对网络鲁棒性的重要作用。在 TPRTrust 模型中, 超级节点的评选算法保证了超级节点的稳定性, 因此网络的鲁棒性也得到了提高。

#### 实验 2 策略恶意节点的影响

本场景在一个社区内进行了仿真, 固定存在 20%的恶意团体节点和 1 个策略恶意节点, 图 4 和图 5 分别展示了 GossipTrust 模型和 TPRTrust 模型

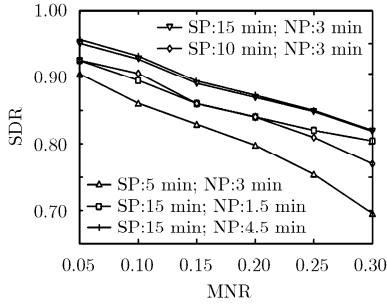


图 3 节点动态性的影响

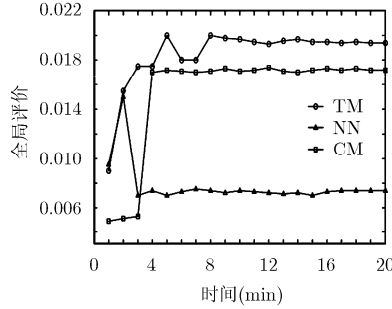


图 4 GossipTrust 中的节点信任度

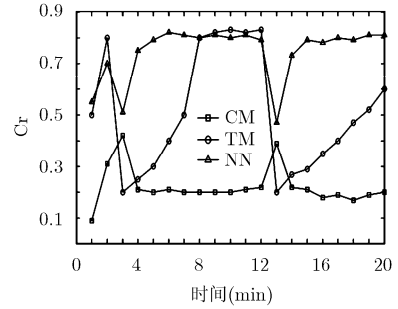


图 5 TPRTrust 中的节点信任度

下恶意节点、策略恶意节点及正常节点的信任度的变化。其中全局评价跟 Cr 都是表示节点的信任度，只是全局评价在 GossipTrust 模型中不是以归一化的方式来计算的。在 GossipTrust 模型中，在第 2 min 超级节点被策略恶意节点夺取后，恶意团体节点的信任度得到了极大提高，正常节点的信任度反而降低，并且一直维持，整个信任系统被破坏。而在 TPRTrust 模型中，在第 2 min 和 12 min，尽管策略恶意节点一时得逞，但是由于其超级节点信任度在恶意行为后迅速降低，并触及拓扑势门限，所以社区启动超级节点的更替和评选机制，策略恶意节点的超级节点地位随之被取代，信任度回复正常。而策略恶意节点则需要再一次经过长期的积累，并且等待超级节点更替周期才能评选上。总的来看，策略恶意节点长时间的积极活跃只能在短时间内肆意妄为，其对整个 P2P 系统的贡献比损坏还大。因此，在策略恶意节点的存在下，TPRTrust 模型比 GossipTrust 模型有效而鲁棒。

### 实验 3 恶意团体节点的识别率

在图 6 中，比较了 TPRTrust 模型和 GossipTrust 模型对恶意团体节点的识别率。随着恶意团体节点比例的增高，恶意节点相互间的合作更加密切，恶意节点识别率也相应降低。而 TPRTrust 模型比 GossipTrust 模型仍然保持较高的恶意节点识别率。这是因为在社区内，恶意团体节点相互合作夸大彼此的信任评价，而又诋毁与之交易的正常节点，不真实和误导性的推荐信息增多，GossipTrust 模型不能有效区分这些信息，对节点的信任度判断不准确。而 TPRTrust 模型通过相似度区分了恶意团体节点虚假的信任评价，同时超级节点监督制约了社区整体信任评价。在跨社区的情况下，随着恶意节点率的升高，一个社区很可能充斥着大量的恶意团体相互掩护相互推荐甚至取得超级节点主导权，导致 GossipTrust 模型下其他跨社区的节点很难辨识。而 TPRTrust 模型通过基于拓扑势的信任度加权的社

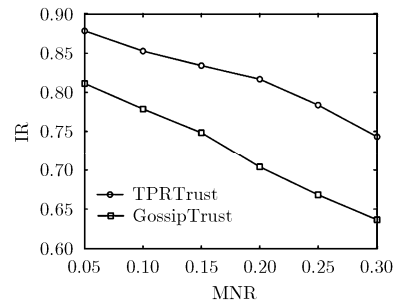


图 6 恶意节点识别率

区信任度可以描述该社区与其他社区交易的整体可信程度，从而从整体的角度判断该社区内的节点是否可信，限制了恶意行为的跨社区扩散。

## 5 结束语

信任模型的建立是 P2P 网络安全保障的关键问题，本文在一种 P2P 社区架构上部署了 TPRTrust 信任模型。信任度计算方式被划分为社区内和跨社区两种，在具体给出各种信任度计算方式的同时，还给出超级节点的评选算法。通过实验验证了 TPRTrust 信任模型在动态场景下的有效性和鲁棒性。仿真实验说明，本文提出的模型克服了现有模型如 GossipTrust 等模型的缺乏对超级节点监督管理的局限性，能够有效限制简单恶意节点、策略恶意节点、恶意团体等各类节点不同程度的攻击方式，因而具有广泛的应用场景及较好的可实现性。

## 参考文献

- [1] Feldman M, Padimitriou C, Chuang J, et al. Free-riding and whitewashing in peer-to-peer systems[J]. *IEEE Selected Areas in Communications*, 2006, 24(5): 1010-1019.
- [2] Saroiu S, Gummadi P K, and Gribble S D. A measurement study of peer-to-peer file sharing systems[C]. *SPIE International Conference on Multimedia Computing and Networking*, San Jose, USA, 2002: 156-170.
- [3] Huang Kun and Wang Lu. Research of trust model based on peer-to-peer network security[C]. *IEEE International Conference on Information Technology and Applications*,

- Chengdu, China, 2013: 126–129.
- [4] Ahmet C and Bharat B. SORT: a self-organizing trust model for peer-to-peer systems[J]. *IEEE Transactions on Dependable and Secure Computing*, 2013, 10(1): 14–27.
- [5] Kamvar D and Schlosser T. EigenRep: reputation management in P2P networks[C]. The 12th ACM International World Wide Web Conference, Budapest, Hungary, 2003: 123–134.
- [6] 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.
- [7] Han Qi-yi, Wen Hong, Ren Meng-yin, *et al.* A topological potential weighted community-based recommendation trust model for P2P networks[OL]. <http://link.springer.com/article/10.1007/s12083-014-0288-9>. 2014.6.
- [8] Zhou Run-fang, Hwang Kai, and Cai Min. GossipsTrust for fast reputation aggregation in peer-to-peer networks[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2008, 20(9): 1282–1295.
- [9] Xu Hai-mei, Liu Yu-lin, Qi Shou-qing, *et al.* A novel trust model based on probability and statistics for peer to peer networks[C]. IEEE International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering, Chengdu, China, 2013: 2047–2050.
- [10] Wang Guo-jun, Felix M, Guo Song, *et al.* Neighbor similarity trust against sybil attack in P2P e-commerce[J]. *IEEE Transactions on Parallel and Distributed Systems*, DOI: 10.1109/TPDS.2014.2312932.
- [11] 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.
- [12] 田春岐, 江建慧, 胡治国, 等. 一种基于聚集超级节点的 P2P 网络信任模型[J]. *计算机学报*, 2010, 33(2): 345–355.
- Tian Chun-qi, Jiang Jian-hui, Hu Zhi-guo, *et al.* A novel super peer based trust model for peer to peer networks[J]. *Chinese Journal of Computers*, 2010, 33(2): 345–355.
- [13] Adele J, Rameez R, Tamas V, *et al.* Systemic risk and user-level performance in private P2P communities[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2013, 24(12): 2503–2512.
- [14] Niu Chang-yong, Luo Heng, Fan Ming, *et al.* On feedback similarity measurement in web of trust[C]. IEEE Global Congress on Intelligent Systems, Xiamen, China, 2009, 3: 33–37.
- [15] Wang Jun-she, Li Xiao-long, and Zhang Yun. Research of P2P network trust model[C]. IEEE International Conference on Intelligent Human-Machine Systems and Cybernetics, Hangzhou, China, 2013: 70–73.
- [16] 张健沛, 李泓波, 杨静, 等. 基于拓扑势的网络社区结点重要度排序算法[J]. *哈尔滨工程大学学报*, 2012, 33(6): 745–752.
- Zhang Jian-pei, Li Hong-bo, Yang Jing, *et al.* An importance-sorting algorithm of network community nodes based on topological potential[J]. *Journal of Harbin Engineering University*, 2012, 33(6): 745–752.
- [17] 淦文燕, 赫南, 李德毅, 等. 一种基于拓扑势的网络社区发现方法[J]. *软件学报*, 2009, 20(8): 2241–2254.
- Gan Wen-yan, He Nan, Li De-yi, *et al.* Community discovery method in networks based on topological potential[J]. *Journal of Software*, 2009, 20(8): 2241–2254.
- [18] 王子厚, 韩言妮, 林涛, 等. 可重构网络中基于中心度与拓扑势排序的资源分配算法[J]. *通信学报*, 2012, 33(8): 10–20.
- Wang Zi-hou, Han Yan-ni, Lin Tao, *et al.* Resource allocation algorithms in the reconfigurable network based on network centrality and topology potential[J]. *Journal on Communications*, 2012, 33(8): 10–20.
- [19] Oversim[OL]. <http://www.oversim.org/wiki>. 2013.10.
- 韩祺祎: 男, 1987 年生, 博士生, 研究方向为对等网技术、分布式计算技术、网络安全.
- 任梦吟: 女, 1989 年生, 硕士生, 研究方向为分布式计算技术、智能计算技术.
- 文红: 女, 1969 年生, 教授, 博士生导师, 研究方向为通信与信息安全.