# 一种基于聚集超级节点的 P2P 网络信任模型

田春岐 江建慧 胡治国 李 峰

(同济大学嵌入式系统与服务计算教育部重点实验室 上海 201804)

(同济大学电子与信息工程学院计算机系 上海 201804)

**摘 要** 针对对等网(Peer-to-Peer,P2P)中节点之间由于兴趣爱好差异大、相互发生重复交易的可能性较小从而难以有效建立信任关系的现状,文中提出一种新的基于超级节点的 P2P 网络信任模型.该模型中节点以兴趣相似而聚簇,节点之间信任关系被划分为 3 种类型并被给予了各自的解决方案.同时,对于推荐信任信息中存在的虚假的、误导性的和不公正反馈的问题,文中还提出基于节点相似性的反馈信息过滤算法予以有效解决.最后的仿真实验结果表明,该信任模型不但具有抗恶意节点攻击的强壮性,同时在资源查询时具有较低的查询开销和失败率.

**关键词** 对等网;信任;信誉;超级节点;局部信任度

**中图法分类号** TP393 **DOI 号**: 10.3724/SP.J.1016.2010.00345

## A Novel Super-Peer Based Trust Model for Peer-to-Peer Networks

TIAN Chun-Qi JIANG Jian-Hui HU Zhi-Guo LI Feng

(*Key Laboratory of Embedded System and Service Computing, Ministry of Education, Tongji University, Shanghai* 201804)

(*Department of Computer Science, College of Electronics and Information Engineering, Tongji University, Shanghai* 201804)

**Abstract** A super-peer based trust model for Peer-to-Peer (P2P) networks is presented in this paper to solve the problems of not sufficiently building trust relation between peers due to the difference of peers' interests and low probability of repeated transactions between them. In the model peers gather in a group according to their interest similarity. Trust relation is categorized into three kinds and subsequently each solution for these kinds is also put forward. Moreover, a feedback filtering algorithm based on peers' similarity is proposed to effectively filter the fake, misleading and unfair feedbacks in the referrals. Subsequent experimental results show that the proposed model is not only robust on trust security, but also has low costs and failure rate when resource search happens.

**Keywords** P2P; trust; reputation; super-peer; local trust value

## 1 引 言

P2P 网络提供了真实生活中人与人直接进行交流的网络环境,它的开放、匿名以及节点之间松耦合的关系等特性使其赢得了越来越多的 Internet 终端用户的青睐进而促使了 P2P 业务的蓬勃发展.然而,也正是这些特性使得 P2P 中的节点在网上可恣意散布非法内容,滥用网络资源,同时,节点动态性又可造成网络带宽和信息存在的不稳定,这大大破

收稿日期:2008-05-03;最终修改稿收到日期:2009-07-04.本课题得到国家自然科学基金(60903194)、教育部博士点基金(200802471060)、通信与信息系统北京市重点实验室(北京交通大学)开放课题、国家大学生创新性实践计划及同济大学青年优秀人才培养行动计划资助.**田春岐**,男,1975 年生,博士,讲师,主要研究方向为 P2P 网络、信任管理.E-mail: tianchunqi@163.com. **江建慧**,男,1964 年生,教授,博士生导师,主要研究领域为分布式系统、可信计算、嵌入式系统等. **胡治国**,男,1978 年生,博士研究生,主要研究方向为计算机网络服务质量. **李 峰**,男,1989 年生,研究兴趣为计算机网络、信息安全等.

坏了正常的网络环境,降低了用户使用 P2P 网络的积极性.

事实证明,节点之间的信任问题是制约 P2P 网络应用进一步发展的主要障碍.信任问题亟需解决.国内外众多的科研工作者也为此做出了各自不懈的努力.基于共享信息的局部信任模型[1-6]使得节点可以彼此共享本地对其他节点的评价信息,并据此确定给定节点的信任度.虽然这种机制被证明能够较好地建立 P2P 中节点之间的信任关系,而且部分信任模型[6]还有较好的抗攻击性.但是一个现实的问题是,在这些信任模型中,共享信息的查找是一个难题,虽然有的机制[7]使用了类似 Chord 结构化的放置方式,但一般而言,共享信息是通过向朋友节点洪泛信任请求消息来获得的.在大规模 P2P 网络中,洪泛机制引起的冗余流量是相当大的,而且可扩展性差,Gnutella0.4① 网络已经证明这个事实.此外,这类基于共享信息的局部信任模型也不适合于部分分布式的 P2P 网络(例如 KaZaa②),因为在这类网络中节点之间不能进行管理信息的直接交互.

为此,本文提出了基于超级节点的 P2P 网络信任模型 SuperTrust(Super-peer based Trust model for P2P networks).在 SuperTrust 中,信任关系被划分为 3 种类型:超级节点之间的信任关系、超级节点与普通节点之间的信任关系及普通节点之间的信任关系.对于同组内普通节点的信任度计算,我们采用的是群组内基于推荐的信任计算机制,即该节点利用本地信任信息与所属群组的推荐信任信息确定目标节点的信任值.超级节点的信任度评价我们采用的是计算群组内所有节点对此超级节点的全局信任度方式.同时我们提出了 noisy 反馈信息过滤算法来过滤恶意节点提供的虚假的或不公正的评价.最后我们给出大量仿真实验来验证 SuperTrust 的有效性和可靠性.

本文第 2 节介绍相关工作;第 3 节描述基于超级节点的信任系统 SuperTrust;第 4 节对仿真及分析工作进行说明;最后一节对本文进行总结.

## 2 相关工作

随着新的网络应用模式的出现,P2P 网络领域的信任机制研究取得了很多的研究成果,其中大部分是基于反馈信息的信任模型,例如全局信任模型 EigenTrust[8]、Pagerank[9]等,局部信任模型 NICE[5]、XREP[1]、PeerTrust[6]、RETM[10],基于 Bayesian Networks[11]的信任模型等等.

全局信任模型[8-9]的特点是系统根据每个节点上传文件的历史行为为该节点计算一个全局的信任值,请求节点根据全局信任值来选择下载源.由于全局信任模型忽略了信任的私人化特征,对于某个特定的节点,其他节点对他的信任值都是相同的.因此,在大规模的 P2P 网络中是否有必要为每个节点计算全局信任值仍有待进一步研究.

在增强信任模型的动态适应能力方面,Lee[5]提出了一种全分布式的方式来存储用户的信誉信息.与其他信任系统不同的是,在 NICE 系统中,节点 $i$ 存储的信任信息是其他节点对 $i$ 所提供服务的满意反馈,因此节点有动机存储信任信息.在基于共享信息的局部信任模型中,共享信息的获取一般是通过向其他节点洪泛信任请求获得的,如 XREP[1],在大规模 P2P 网络中可扩展性较差.此外,这类基于共享信息的局部信任模型也不适合于部分分布式的 P2P 网络.

Xiong[6]提出了基于反馈的信任系统.为了更有效地评估节点的可信度以及描述 P2P 社区中各种恶意行为,不仅将对交易满意程度的反馈作为评估信任的参数,同时考虑了交易的总数目、反馈的可信程度、交易的上下文因子,而且给出了该模型在结构化 P2P 网络中的分布式实现.该文的主要贡献是给出了计算节点信任度的 5 个因子,并提出了一种基于反馈的计算信任度的有效方法.

Mekouar[12]提出了部分分布式(partially-decentralized) P2P 网络的信任管理机制(记为 PDTrust).超级节点传递节点之间的信任评价,使每个超级节点能够记录其叶节点对系统的有效贡献并作为叶节点的可信度.但 PDTrust 直接利用所有节点的反馈信息,容易受到恶意节点的联合欺诈攻击.

Wang[11]提出了 P2P 环境下基于贝叶斯网络的信任模型,它通过对贝塔($\beta$)概率密度函数的统计更新来计算节点信任度.该信任模型主要关注于描述信任的不同方面,使得节点可以根据不同的场景来按需获取节点不同方面的性能.当节点无法确定文件提供者的可信度时,利用其他节点的推荐信息来建立信任关系.该信任模型能够适应于规模较小的 Gnutella 网络,或具有 small-world 特性的大规模 Gnutella 网络.

① http://www.gnutella.com
② http://www.Kazaa.com

在基于组结构(Group based)的 P2P 网络拓扑结构方面,组的划分方式也是多样的,例如,有根据地理位置划分的[13]、有根据内容兴趣关联进行划分的[14-15]等;同时组内成员可以采用分布式的方式进行组织,也可以采用层次化的方式[16]. 在 SuperTrust 信任模型中,节点以内容兴趣相似而聚集成组,而且组成员采用了分布式的组织方式,这样同组内节点重复交易的次数大大增加,获取信任信息引起的流量也很大程度上限制在了局部范围内.

## 3　基于超级节点的信任模型 SuperTrust

在 SuperTrust 中,将所有节点以群组为单位进行划分,每个群组只有一个超级节点. 简单起见,SuperTrust 假定每个节点(如不特殊声明,本文中"节点"均指普通节点)只属于一个组(对于一个节点属于多个组的情况,可以看作是该节点在每个组中有不同的身份). 图 1 是具有超级节点的 P2P 网络结构图,图中给出了 4 个群组之间的连接关系,$SP$ 代表超级节点. 图中表示了 3 种信任类型,在群组 $G_1$ 中,超级节点 $SP_1$ 与节点 $P_2$ 之间、$P_2$ 与 $P_3$ 之间设为直接信任关系, $SP_1$ 与 $P_3$ 之间为推荐信任关系. 节点 $P_2$ 与 $P_4$ 之间表示的是位于不同群组的普通节点之间的信任关系,同时,我们还刻画了超级节点 $SP_1$ 与 $SP_3$ 之间的信任关系.

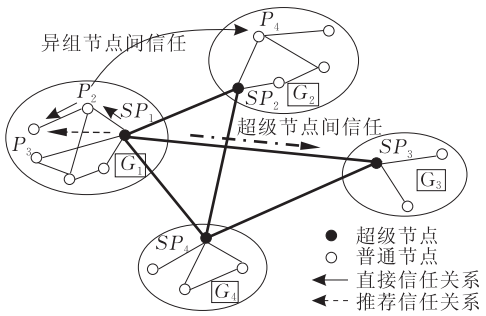


图 1　具有超级节点的 P2P 网络结构图

SuperTrust 的基本思想是节点根据交易建立对目标节点的本地信任关系:如果目标节点(比如 $P_3$)位于同一群组,则节点($P_2$)在本地存储对该目标节点的交易记录;如果目标节点(比如 $P_4$)位于其他群组,则节点($P_2$)将交易结果向其所在群组超级节点($SP_1$)反馈,超级节点 $SP_1$ 根据节点 $P_2$ 的反馈建立对节点 $P_4$ 所在群组的超级节点 $SP_2$ 的信任关系. 节点要评估同一群组内其他节点的信任度时,按照组内基于信誉的信任机制计算该节点的信任度;超级节点的信任度则按照该群组内所有节点对其的全局信任度来计算. 下面先介绍同组内节点之间信任度的计算方式.

### 3.1　同组内节点信任度计算

我们先研究位于同一组的普通节点之间的信任度计算问题. 在 SuperTrust 中,同一组内的节点信任度计算是按照基于信誉的信任计算机制来进行的,为此,我们首先给出局部信任度的定义.

**定义 1.**　如果在整个交易时期内节点 $P_m$,$P_j$ 之间交易了 $N_{mj}$ 次,则节点 $P_m$ 对 $P_j$ 的局部信任度(直接信任度)为

$$R_{mj}=R(P_m,P_j)=\begin{cases}\dfrac{Sat_{mj}-UnSat_{mj}}{N_{mj}}, & N_{mj}=Sat_{mj}+UnSat_{mj}\neq 0\\ 0, & N_{mj}=Sat_{mj}+UnSat_{mj}=0\end{cases} \tag{1}$$

式中 $Sat_{mj}$ 表示满意的交易次数,$UnSat_{mj}$ 表示不满意的交易次数. 我们规定如果两者没有交互历史,则局部信任度为 0.

#### 3.1.1　信誉度

局部信任度只是两个节点之间直接交易之后有限的信任关系,不足以全面准确评价一个节点,基于信誉的信任机制目前被证实能够很好地反映 P2P 网络中节点之间的信任关系. 因为我们建立群组时是按照节点兴趣爱好相似而聚集的,则同组内节点之间的交互会比普通的网络拓扑结构中节点之间交互更为频繁,所以也能够快速建立起信誉,依靠信誉就可以有效地评价一个节点.

在节点信誉度计算上有各种不同的方法[1,4,6,17-18],我们提出用可信度(credibility)来评价推荐节点信任信息的方法.

**定义 2.**　可信度. 节点 $m$ 的可信度是指节点 $i$ 对其所推荐信息的信赖程度,用 $Cr_{im}$ 表示. 可信度具有两大特点:动态变化和私人特征,动态变化是指可信度随该节点 $m$ 向节点 $i$ 提交对其他节点评价的次数的增加而变化(增加或者降低),私人特征即此可信度为该评价节点 $i$ 专有而不与其它节点共享.

节点 $i$ 汇集推荐节点的信任信息即可得到节点 $j$ 的信誉度,信誉度是所有与 $j$ 交互过的节点对其交互事实累积的主观评价,反映了 $j$ 长期历史行为的品质状况. 在 SuperTrust 中,我们利用请求节点 $i$ 对各个推荐节点的可信度来加权其推荐信息,合成后便得到被评价节点 $j$ 的信誉值. 因此,节点 $i$ 计算出的 $j$ 的信誉度为

$$Re_{ij}=\sum_{m\in I(j)}\frac{R_{mj}Cr_{im}}{\sum_{m\in I(j)}Cr_{im}} \tag{2}$$

式中,$Re_{ij}$为节点$i$汇聚推荐信息后的节点$j$的信誉度,$R_{mj}$为推荐节点$m$对节点$j$的局部信任度,$Cr_{im}$为节点$i$对推荐节点$m$的可信度,$I(j)$为节点$j$的推荐者集合.从式(2)可以看出,节点$i$对来自可信度高的节点的局部评价给予了较高的权重.

3.1.2 可信度计算

在SuperTrust中,请求节点依据其对推荐节点的可信度加权该推荐节点的局部评价.具体为:在节点$i$计算出节点$j$的信誉度后,对节点$m$的推荐作如下判断:如果此节点提供的评价与其他节点提供的综合评价(即$j$的信誉度)在一定程度上一致,即认为是正确评价,则它的可信度就在原来基础上有所增加;反之,如果它给出的评价与其他节点的综合评价不一致,则它的可信度就在原有基础上有所降低,它随后的推荐就会对被评价者的信誉度有一个减弱的影响.

我们首先定义信任偏差为

$$Diff_{im}=\sum_{m\in I(j)}|Re_{ij}-R_{mj}|/|I(j)| \tag{3}$$

式中$Re_{ij}$为节点$i$计算出的节点$j$的信誉度,$R_{mj}$为推荐节点$m$对节点$j$的局部信任度,$I(j)$为节点$j$的推荐者集合,$|I(j)|$为该集合的势.

定义相对信任偏差为

$$RTD_{im}=Diff_{im}/STD_j \tag{4}$$

式中$RTD_{im}$为节点$i$对$m$的相对信任偏差,$STD_j$为所有推荐节点对节点$j$的局部信任度的标准偏差.

我们按照节点提供的评价与其他节点提供的综合评价(即$j$的信誉度)的一致性程度,提出了该节点可信度更新的公式,计算方式如式(5).

$$Cr_{im}^{k+1}=\begin{cases}Cr_{im}^{k}+\delta(1-Cr_{im}^{k})(1-RTD_{im}), & 0\le RTD_{im}\le 1,\ k>0\\ Cr_{im}^{k}-\gamma Cr_{im}^{k}\left(1-\dfrac{1}{RTD_{im}}\right), & RTD_{im}>1,\ k>0\\ 0.5, & k=0\end{cases} \tag{5}$$

式中,参数$0<\delta<\gamma<1$,$k$为整数,$Cr_{im}^{k}$为第$k$次推荐后节点$i$对节点$m$的可信度.式(5)表达的意思是,当推荐节点$m$对被评价节点$j$的局部信任度与节点$j$的信誉度的逼近程度小于所有推荐节点提供的反馈信息的平均偏差时,则认为它的推荐是可信的,更新后的可信度是在原来的基础上有一个较小幅度的增加(具体幅度为$\delta(1-Cr_{im}^{k})(1-RTD_{im})$);反之,如果两者的逼近程度大于所有推荐节点提供的反馈信息的平均偏差时,则认为它的推荐是不可信的,可信度则在原来基础上有一个较大幅度的下降(具体幅度为$\gamma Cr_{im}^{k}\left(1-\dfrac{1}{RTD_{im}}\right)$,与目前的可信度$Cr_{im}^{k}$及$\gamma$有关).同时,我们假设节点初次推荐的节点可信度为0.5,文献[19]指出对新节点的部分信任可以提高系统整体性能,直至它被证实是不可信为止.

3.1.3 节点信任度计算

我们先给出同一群组内普通节点之间的信任度计算方法.我们有

同一群组内普通节点之间的信任度:

$$Tr_{ij}=\lambda\times R_{ij}+(1-\lambda)Re_{ij} \tag{6}$$

其中$\lambda$是直接信任度的信心因子,$\lambda$的取值和交互的数目有关,交互的数目越多则$\lambda$取值越大,$0\le\lambda\le 1$.我们可以取$\lambda=h/H_{Lmt}$,其中$h$为节点$i$和节点$j$之间交互的数目,$H_{Lmt}$为设定的交互数目门限值.本文中取值为20.

### 3.2 超级节点信任度计算

在SuperTrust中,在网络初始阶段我们假设初始加入P2P网络的节点是可信的,可以作为超级节点,因为作为整个P2P网络的构建者和最初的使用者,没有不良动机破坏此网络.同时,我们赋予超级节点以下功能:参与交易,维护自身交易结果;维护群组的节点管理;另外,超级节点还存储着节点跨群组交易的信任信息.

节点对本群组的超级节点的信任度是变化的.在SuperTrust中节点对该组超级节点的信任度计算按照全局信任度计算(与EigenRep类似),即

$$Tr_{SP_i}=\sum_{k\in I(G_i)}(R_{ik}R_{kSP_i}) \tag{7}$$

式中$Tr_{SP_i}$表示超级节点$SP_i$的信任度,$I(G_i)$为$SP_i$所在组的节点集合,$R_{ik}$表示节点$i$对$k$的局部信任度.

由此可见,在某时刻对整个群组而言,超级节点的信任度都是唯一的,而不是某个特定节点自身的评价.由于信任是由交互结果决定并受其影响的,在经过一定的时期后,节点信任度就有变化.于是,整个群组的节点都可以周期性地参与考核该超级节点的信任度,对信任度低于一定门限的超级节点可以进行更换,用备份超级节点替换此超级节点,这样就可避免恶意节点伪装身份进行欺骗.备份超级节点

选取是组内所有成员依据其信任度、稳定性以及整体性能共同决定的.

对于新加入的普通节点来说，我们规定在开始是完全信任该组内的超级节点的，随着自己不断深入的交互，逐渐调整对此超级节点的信任关系. 于是，在 SuperTrust 中，节点 $i$ 对超级节点 $SP_i$ 的信任度为

$$Tr_{iSP_i}=\begin{cases}1, & n=1\\ \theta Tr_{iSP_i}, & n>1\end{cases} \tag{8}$$

其中 $n$ 为交易次数，$\theta$ 的变化区间如下：

$$\psi^{|R_{iSP_i}-s|}\leq\theta\leq 1-(1-\psi)|R_{iSP_i}-s| \tag{9}$$

上式中 $\psi$ 为一常数，且 $0<\psi<1$，$R_{iSP_i}$ 为节点 $i$ 对超级节点 $SP_i$ 的直接信任度，$s$ 为组内节点对超级节点信任评价标准偏差. 本文仿真中取 $\theta=1-(1-\psi)\cdot|R_{iSP_i}-s|$.

超级节点 $SP_i$ 与 $SP_j$ 之间的信任度是依靠 $SP_i$ 群组内节点对 $SP_j$ 群组内节点的总体信任评价来建立的. 定义如下.

**定义 3.**　超级节点 $SP_i$ 对超级节点 $SP_j$ 的信任度为

$$Tr_{SP_iSP_j}=\begin{cases}Sat_{G_iG_j}-UnSat_{G_iG_j}/N_{G_iG_j}, & N_{G_iG_j}=Sat_{G_iG_j}+UnSat_{G_iG_j}\neq 0\\ Tr^{ref}_{SP_iSP_j}, & N_{G_iG_j}=Sat_{G_iG_j}+UnSat_{G_iG_j}=0\\ & \text{且存在 } TrustPath_{SP_iSP_j}\\ 0, & \text{其它}\end{cases} \tag{10}$$

式中 $Sat_{G_iG_j}$ 为群组 $G_i$（超级节点 $SP_i$ 所在的群组）中节点与群组 $G_j$ 中节点成功交易的次数，$UnSat_{G_iG_j}$ 为群组 $G_i$ 中节点与 $G_j$ 中节点失败交易的次数.

当 $Sat_{G_iG_j}+UnSat_{G_iG_j}=0$ 时，如果 $SP_i$ 与 $SP_j$ 间存在信任路径，则根据最强路径原则计算 $SP_i$ 对 $SP_j$ 的推荐信任值 $Tr^{ref}_{SP_iSP_j}$.

超级节点 $SP_i$ 对 $SP_j$ 的信任度 $Tr_{SP_iSP_j}$ 存储在 $SP_i$ 本地缓存中（本地还保存有跨组交易记录），且具有明显时效性，因为 $Tr_{SP_iSP_j}$ 是根据组间节点的交易数目变化的，只要交易数目发生变化，则 $Tr_{SP_iSP_j}$ 一定变化；且按照式(10)进行更新.

对于超级节点 $SP_i$ 与 $SP_j$ 间的一组信任路径，最强信任路径指经由 $SP_i$ 最信任群组到达 $SP_j$ 的信任路径. 令路径上的最小信任值为通过该信任路径确定的 $SP_i$ 对 $SP_j$ 的推荐信任值，则 $Tr^{ref}_{SP_iSP_j}$ 为最强信任路径上的推荐信任值. 如果有多条最强信任路径，则 $Tr^{ref}_{SP_iSP_j}$ 为这些推荐信任值的平均值. 如图 2 所示，群组 $A$ 到 $B$ 的最强信任路径有两条，为“$A->E->D->B$”和“$A->G->H->B$”，其推荐信任值分别为 0.4 和 0.2，因此，群组 $A$ 对 $B$ 的信任值 $Tr^{ref}_{SP_iSP_j}$ 为 0.3.

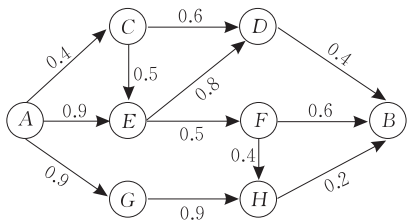


图 2　最强信任路径示例图

### 3.3　节点之间的信任度计算

令 $Tr_{ij}$ 为节点 $i$ 对 $j$ 的信任值，如果 $i$ 与 $j$ 属于同一组，则 $Tr_{ij}$ 按照式(6)计算，无论 $i$ 是普通节点还是超级节点，因为超级节点与其它节点一样也参与交易，也是组内一节点.

如果 $i$ 与 $j$ 不属于同一组，则我们规定节点 $i$ 对 $j$ 的信任值 $Tr_{ij}$ 为

$$Tr_{ij}=\min\{Tr_{iSP_i},Tr_{SP_iSP_j},Tr_{SP_jj}\} \tag{11}$$

即为三者中的最小值，式中 $Tr_{SP_jj}$ 为节点 $j$ 所在群组的超级节点 $SP_j$ 对 $j$ 的信任度. 由以上定义可知，信任值取值范围为$[-1,1]$. 以 0 为分界点，信任值越大节点越值得信赖，信任值越小节点越不可信.

节点 $i$ 对节点 $j$ 的信任计算可以用算法 1 实现.

**算法 1.**

```
TrustComputing (i,j)   //节点信任度计算算法
 //输入:j,  输出:Trij
 Feedback⇐retrieveFeedback(j);
 FSet⇐Feedback 中的反馈源节点集合;
 for m∈FSet do
   Rmj⇐计算等式(1);
   从缓冲 Cache_Cr 中得到节点 m 的反馈可信度 Cr_im;
   根据等式(5)更新 Cr_im;
 end for
 if j 与 i 属于同一个群组
   Trij⇐计算等式(6);
 else
   Tr_SPiSPj,Tr_SPjj⇐计算等式(10)及(6);
 Trij⇐计算等式(11);
 end if
end
```

### 3.4　Noisy 信息过滤机制

在基于信誉的信任机制中，反馈信息的过滤是一个重要的过程，因为反馈信息中不可避免地存在一些无用的、虚假的或者误导性的推荐信息（我们称这些信息为 noisy 信息），有效剔出 noisy 信息将大

大提高反馈信息融和的准确性和可靠性.

文献[8]把推荐信任等同于服务信任,但该方法不能有效抑制高信任度的节点提供不诚实的反馈.文献[17]提出了一个基于向量相似性度量的方法,对 PSM 方法进行了改进,能够过滤掉不诚实的反馈信息.文献[4]提出了一个加权多数算法 WMA,该算法的思想是对不同推荐者的推荐分配不同的权重,根据权重来聚合相应的权重,并根据交互的结果来动态地调整相应权重.这些方法没有考虑复杂的合谋节点联合欺骗的方式,未能有效抑制动态策略性的欺骗行为.

我们的算法基于节点给出反馈的重要性的相似性以及个体相似性来过滤不可信反馈.当节点反馈的重要性相似性和个体相似性都相似时,节点是相似的.这些属于同一群组的节点由相似关系形成了簇,本文假设属于群组中最大的簇(用 $TC$ 表示,称之为信任簇)的节点提交的信任信息是公正的.

我们定义了两种相似性:

(1)节点 $i$ 与 $j$ 所给出的反馈重要性的相似性.考虑在恶意节点合谋欺诈且存在伪装的合作节点的攻击下,伪装的合作节点对恶意集团外的其他节点给出公正的评价以增加与其他节点的个体相似性,同时选择性地对其同伙给出很高的评价来夸大其通过的信誉值.节点所给出反馈重要性的相似性通过对相同节点给出的评价的相对重要性的差异来评估,如式(12)所示.

$$FISim(i,j)=\begin{cases}\left|1-\dfrac{\sum_{k\in CSet(i,j)}|R_{ik}-R_{jk}|}{|CSet(i,j)|}\Big/\xi\right|, & CSet(i,j)\neq\varnothing\\ 0, & CSet(i,j)=\varnothing\end{cases}\tag{12}$$

其中,$R_{ik}$ 与 $R_{jk}$ 分别是节点 $i$ 和 $j$ 对节点 $k$ 的信任评价,$CSet(i,j)$ 指在最近观察窗口内与节点 $k$ 有交互的节点集 $Set(i)$ 与 $Set(j)$ 的交集,$\xi$ 为与 $k$ 交易过的所有节点对 $k$ 评价的标准偏差.如果 $FISim(i,j)>FISim_{\text{threshold}}$,则节点 $i$ 与节点 $j$ 所给出的评价具有相似的重要性,其中 $FISim_{\text{threshold}}$ 是判断节点所给出评价的重要性是否相似的门限值.

(2)节点 $i$ 与 $j$ 的个体相似性.通过节点 $i$ 与 $j$ 对相同节点给出的评价的均方根来评估,如式(13)所示

$$PSim(i,j)=\begin{cases}1-\sqrt{\sum_{k\in CSet(i,j)}(Tr_{ik}-Tr_{jk})^2/|CSet(i,j)|}, & CSet(i,j)\neq\varnothing\\ 0, & CSet(i,j)=\varnothing\end{cases}\tag{13}$$

其中 $CSet(i,j)$ 意义同反馈重要性相似性定义.如果 $PSim(i,j)$ 大于预定的门限(此门限是决定节点是否个体相似),节点 $i$ 与节点 $j$ 是个体相似的.

我们根据节点的反馈重要性相似性和个体相似性,给出 noisy 信息过滤算法如下.

**算法 2.**

$TrustCLSTsFiltering(N_G)$ //Noisy 信息过滤算法
//$N_G$ 是群组 $G$ 的节点集
//输入:$N_G$, 输出:$TC$
1. 初始化簇列表 $CList_G$
2. 获取群组 $G$ 中的簇
for $i\in N_G$ do
if $i$ 与 $CList_G$ 中任何节点不相似
$i$ 作为新的簇添加到 $CList_G$;
else 找出所有与 $i$ 有 $\varepsilon$ 个相似节点的簇,合并为一个簇并插入 $i$;
end if
找出 $CList_G$ 中最大的簇作为信任簇 $TC$ 并输出;
end for
end

在网络初始化阶段,由于系统中没有足够的评价信息来得到信任簇,超级节点 $SP_i$ 根据给出反馈信息的节点的可信度来加权更新信任信息.当系统中累计了足够的反馈信息后,则在每个观察窗口结束后,群组运行信任簇过滤算法 TrustCLSTsFiltering 得到信任簇 $TC$,并根据 $TC$ 结果来过滤 noisy 信息.

### 3.5 信任评估的计算与通信开销分析

利用 SuperTrust 进行信任评估的开销依赖于 SuperTrust 的具体实现,本节只讨论在分布式 P2P 网络中所实现 SuperTrust 的信任评估开销,具体针对计算开销和通信开销.在分布式 P2P 网络中,群组可以通过 CAN、Chord 或 P-Grid 的 DHT 机制来组织,该机制将节点映射到逻辑的坐标空间,保证每一个查询请求都能在复杂度 $\log M$($M$ 是群组大小)内得到响应.

计算开销方面.节点 $i$ 计算与其有共同交易节点的其他节点的相似性,通过运行 TrustCLSTsFiltering 算法可以得出信任簇.此过滤算法复杂度为 $O(rM)$,其中 $r$ 是与 $CList_G$ 相关的数值.

通信开销方面.为了计算节点之间的相似性,节点 $i$ 发起多个查询请求来得到节点 $j$(与节点 $i$ 有共

同的交易节点）给出的反馈信息，这些请求在 $O(\log M)$ 跳内获得信息. 当节点 $i$ 没有关于节点 $j$ 的本地信任信息时，为了获取节点 $j$ 的信任值，在节点 $i$ 与 $j$ 属于同一群组和不同群组的情况下节点 $i$ 分别需要 $O(\log M)$ 和 $O(\log N/M)+2O(\log M)$ 跳，其中 $N$ 为整个 P2P 网络的规模. 因此，SuperTrust 的通信开销具有较好的扩展性.

基于以上分析可知，SuperTrust 可以较好地扩展到大规模的 P2P 网络中，使得节点在有限的时间内评估其他节点的信任值.

## 4　仿真实验与分析

本文仿真基于斯坦福大学开发的查询周期仿真器（QueryCycleSimulator）①[20]，同时，我们实现了部分分布式（Partially-Decentralized）P2P 网络的信任机制（记为 PDTrust）和传统的基于信誉的信任（Reputation Based Trust，RBTrust）系统. 在 RBTrust 中，节点根据本地信任信息和其他节点的推荐信任来计算给定节点的信任值. 在每一个查询周期 QueryCycle（即仿真周期）中，网络中的节点可能处于积极状态或者离线状态，在积极状态每个节点都可以进行一次交易. 当节点发起请求后，等待接受响应并从中选择节点进行文件下载，直到下载了有效的文件或者试过了所有的响应，然后一个查询周期结束，并进行数据收集. 这就是一个完整的仿真周期.

在本文实现的基于信誉的信任系统 RBTrust 中，节点 $i$ 按如下公式计算节点 $j$ 的信任值 $Tr_{ij}$.

$$Tr_{ij}=\alpha\times R_{ij}+(1-\alpha)\times Re_{ij} \tag{14}$$

其中 $\alpha$ 为直接信任度 $R_{ij}$ 权重，依据 $i$ 对自己交易的信心程度来经验分配；$Re_{ij}$ 为节点 $i$ 对节点 $j$ 的信誉度，且 $Re_{ij}=\sum_{s\in I(j)} w_{is}\times R_{sj}\Big/\sum_{s\in I(j)} w_{is}$，上式中 $s$ 表示节点 $s$，$I(j)$ 是节点 $j$ 的推荐者集合，$w_{is}$ 是节点 $i$ 对节点 $s$ 的信任权重，在本文仿真中，$w_{is}$ 与节点 $i$ 对 $s$ 的直接信任度成正比，$\alpha=0.5$.

网络中的节点依据行为表现分为以下几种：

（1）好节点. 这类节点无论在提供服务上（上载）还是在对其他节点的评价上（提交对其他节点的评价），都是真实的，我们称这类节点为好节点，或者称为合作节点.

（2）恶意节点. 这类节点可进一步分为以下几个子类：

① 简单恶意节点. 这类节点在其他节点请求下载时提供不真实的文件，记这类节点为 SM 类.

② 诋毁节点. 这类节点在被询问到对其他节点的信任评价时，为与之有过交易的节点提供不真实的负面评价，记这类节点为 DM 类.

③ 合谋欺诈恶意节点. 恶意节点联合起来形成恶意集团，诋毁好节点并夸大同类节点，记这类合谋欺诈的恶意节点为 CM 类. CM 类的一个子集——具有前端节点的合谋欺诈，即合谋节点内存在一部分节点作为前端节点，它们提供真实可信的文件，同时对合作节点给予公正的评价. 这些前端节点的存在试图来掩饰恶意节点的行为，记具有前端节点的合谋欺诈为 CF 类.

事实上，恶意节点的情况要复杂得多，几乎各种类型恶意节点的组合都可以产生一类新的恶意节点，考虑到实验的可操作性，我们仅对以上类型进行了仿真实验. 我们仿真了 100 个查询周期，每个节点在整个仿真过程中可完成 100 次下载交易，每次交易目标为从其不曾拥有的文件中选择一个并试图进行下载. 交易的成功使得该用户拥有该文件，失败的交易不会增加该用户拥有的文件.

### 4.1　仿真环境

为了与 PDTrust 进行比较，仿真网络采用部分分布式的结构. 在 SuperTrust 和 RBTrust 系统中，节点本地可保存 10 个节点的信任信息，节点或群组发送的信任请求消息的 TTL 为 5. 在本仿真中，假设系统中每一个文件都至少被某个合作节点拥有.

我们仿真的网络环境为：节点总数为 1000 个，其中恶意节点比例为[0.1～0.5]，群组个数为 20 个，节点随机分布于各个群组中，每个组的邻居组个数为 3～6 个. 好节点和各类恶意节点均 100％处于积极状态，并在积极状态 100％发送文件请求. 假设简单恶意节点以 40％比例提供可信文件，合谋节点对内部节点 100％提供可信文件，对外 100％为不可信文件. 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. 仿真周期为 100 次，仿真次数为 3 次，仿真实验结果为平均值. 同时，假设能对系统中的所有文件成功定位，并且系统中每一个文件都至少被一个好节点拥有. 其他参数设置见表 1.

① The Stanford P2P Sociology Project. http://p2p.stanford.edu/www/demos.htm

**表 1 仿真参数表**

| 参数 | 值 |
|---|---|
| $\delta$ | 0.4 |
| $\gamma$ | 0.8 |
| $\psi$ | 0.5 |
| $\lambda$ | 0.6 |
| $\epsilon$ | 3 |

仿真实验首先对模型抗攻击性进行检测.我们对比了在 SM、DM、CM 以及 CF 4 种场景下 SuperTrust、PDTrust 和 RBTrust 3 种信任机制成功交易率(The successful Transaction Rate,STR)情况.成功交易率 STR 即整个网络中成功交易次数在所有交易次数中所占的比例.成功交易是指请求节点从响应节点准确无误地下载到所需要的文件;否则为一次失败交易.

## 4.2 抗攻击能力测试

### 4.2.1 简单恶意节点(SM)

在仿真中,我们假设合作节点以 0.96 的概率提供可信文件.因此,当系统中没有恶意节点时,合作节点的成功请求率为 0.96.由图 3 可知,当恶意节点仅仅提供不可信文件时,SuperTrust 和 PDTrust 在恶意节点比例较小时能够有效识别恶意节点,所以合作节点的成功交易率随着恶意节点比例的增加而减小缓慢.但随着恶意节点比例的增大,SuperTrust 系统的性能显示出较大的优势.RBTrust 系统的成功请求率随着恶意节点比例的增加而大幅减小,这是因为在 RBTrust 系统中,节点利用本地信任信息或可信的朋友和朋友的朋友的推荐来确定给定节点的信任值,因此并不能有效获取所有节点的信任信息.此外,在我们的仿真中,合作节点可能因为出现错误而提供不可信的文件,而恶意节点会为了隐藏其恶意行为而以一定概率提供可信文件,因此,在 RBTrust 中,节点可能错误地评估其他节点的可信度,造成成功交易率下降.

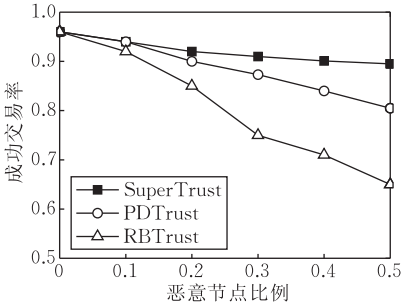


图 3 SM 下成功交易率对比

图 4 是在简单恶意节点下,恶意节点比例为 0.5 时,SuperTrust、PDTrust 和 RBTrust 3 种系统成功交易率随仿真周期的变化情况,可以看出,SuperTrust 的系统性能最优,PDTrust 次之,RBTrust 最差,说明了 SuperTrust 有较强的抵抗恶意节点攻击的能力.

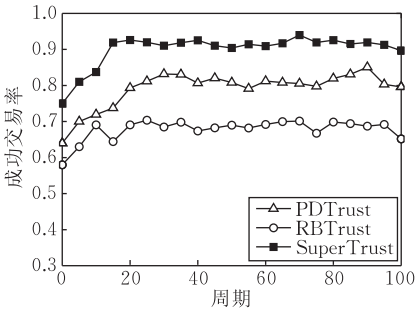


图 4 SM 下成功交易率随周期变化情况

### 4.2.2 诋毁节点(DM)

图 5 是在恶意节点诋毁攻击下 SuperTrust、PDTrust 和 RBTrust 3 种系统的成功交易率对比情况.

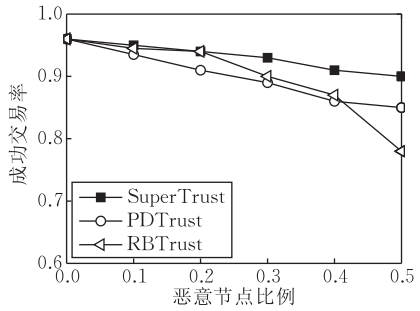


图 5 DM 下成功交易率对比

由图 5 可以看出,当系统中恶意节点比例较小时,3 种机制的系统成功交易率相差不大.但随着恶意节点比例的增大,SuperTrust 系统的性能显示出较大的优势,这是因为我们提出的反馈信息过滤算法能够过滤掉诋毁节点对合作节点发布的不公正信息,使得 SuperTrust 能够有效识别诋毁节点,而使大多数的攻击无效,因此在恶意节点比例达到 0.5 时,也能具有较高的成功交易率.RBTrust 系统的成功交易率随诋毁恶意节点比例的增加降低很快,这是因为当诋毁节点多时,推荐信息里不真实和误导性的信息增多,系统不能有效区分这些信息,对节点的信任度判断误差较大,故而不能有效选择下载源致使成功交易率下降.

图 6 是在诋毁攻击情况下,恶意节点比例为 0.5 时,SuperTrust、PDTrust 和 RBTrust 3 种系统成功交易率随仿真周期的变化情况.可以看出,SuperTrust 的系统成功交易率随着仿真周期的进行快速增加,最终保持相对稳定,而且在整个交易周期

内始终高于其他两者，显示了 SuperTrust 较强的对抗诋毁攻击的有效性.

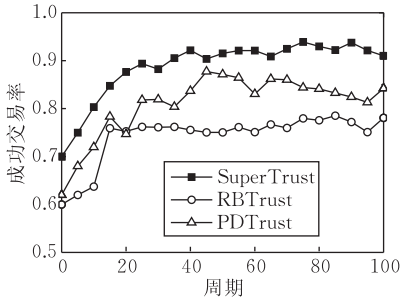


图 6　DM 下成功交易率随周期变化情况

### 4.2.3　合谋欺诈(CM)

图 7 是在恶意节点合谋欺诈下 SuperTrust、PDTrust 和 RBTrust 3 种系统的成功交易率对比情况.

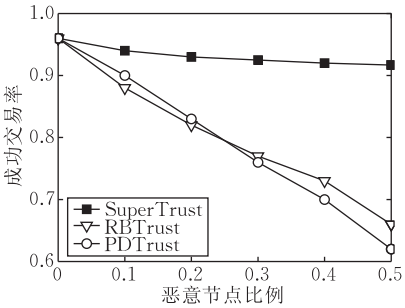


图 7　合谋欺诈下成功请求率对比

在 SuperTrust 和 PDTrust 系统中，恶意节点为与之有过交易的合作节点提供负面反馈，而对与之有过交易的同类节点提供高的正面反馈. 此外，恶意节点可能彼此串通频繁提交对彼此的高的正面评价. 在 RBTrust 中，假设恶意节点收到其他节点的推荐信任请求后，如果询问的是同类恶意节点，则给出推荐信任值为 1；否则，为－1.

由图可以看出，随着恶意节点比例的增加，SuperTrust 中合作节点的成功交易率远远高于 PDTrust 和 RBTrust 系统，这是因为在 SuperTrust 中，反馈信息过滤算法可以过滤大多数不公正的反馈，从而使得当恶意节点比例达到 0.5 时，系统的成功交易率仍能保持在 0.9 附近. 而在 PDTrust 中，信任信息的直接更新使得恶意节点通过彼此给出高的正面评价而有高的信任值. 因此，在 PDTrust 中，随着恶意节点比例的增加，成功请求率急剧下降. 在 RBTrust 中，节点不能准确评估另一个节点的信任值，而这种评估的不准确性在恶意节点的合谋欺诈攻击下更为严重. 因此，在 RBTrust 中，节点不能识别合作节点与恶意节点，因此系统的成功交易率随恶意节点比例增加迅速下降.

图 8 所示是在合谋欺诈情况下，恶意节点比例为 0.5 时，3 种系统的成功交易率随仿真周期的变化情况，可以看出，SuperTrust 的系统成功交易率随着仿真周期的进行快速增加且最终保持相对稳定，而 PDTrust 和 RBTrust 系统随着仿真周期的增加系统性能都有所下降，且整体上 PDTrust 的性能劣于 RBTrust，这是因为 PDTrust 直接对反馈信息进行简单加和为系统中每个节点计算全局信任值，当恶意节点比例高时，系统性能完全被恶意节点控制. 而对 RBTrust 而言，节点可以根据本地信誉信息确定给定节点的可信度，因此性能好于 PDTrust.

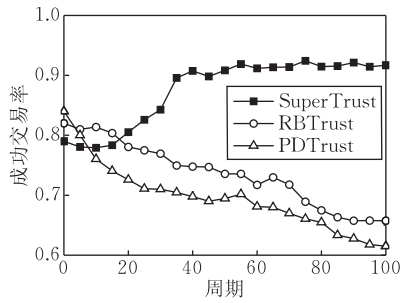


图 8　合谋欺诈下成功交易率随周期变化情况

### 4.2.4　具有前端节点的合谋欺诈(CF)

在仿真实验中，假设前端节点是整个恶意节点比例的 20%. 图 9 我们给出了具有前端节点的合谋欺诈攻击下 SuperTrust、PDTrust 和 RBTrust 系统中合作节点的成功交易率，同时与各个系统在恶意节点合谋欺诈攻击下的情况进行了比较.

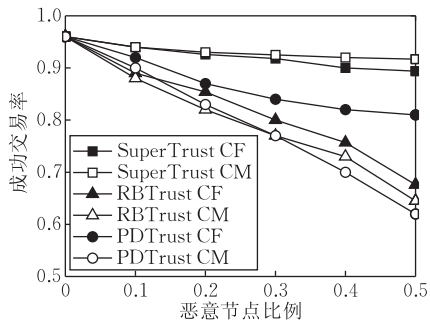


图 9　CF 下成功交易率对比

在具有前端节点的合谋欺诈攻击下，正如在恶意节点的合谋欺诈攻击下一样，SuperTrust 的成功交易率优于 PDTrust 和 RBTrust. 但是不同的是，在 SuperTrust 系统中，系统成功交易率在 CM 攻击下比在 CF 攻击下具有更好的性能. 而在 PDTrust 和 RBTrust 系统中正好相反. 这是因为在 SuperTrust 仿真中我们设置节点只要与簇中的若干节点相似，则认为与整个簇中所有节点相似，在 CF 攻击下，前

端节点的隐蔽性恶意行为使得其与合作节点相似的可能性增大,而成为评价簇中成员,从而提交了对恶意节点的高的正面评价.在 PDTrust 和 RBTrust 系统中,在恶意节点比例相同的情况下,CF 攻击比 CM 攻击时系统中有更多的节点提供有效文件,因此系统成功交易率在 CF 攻击时更高.

图 10 是恶意节点比例 0.5 时,SuperTrust、PDTrust 和 RBTrust 3 种机制的成功交易率在具有前端节点的合谋欺诈下和合谋欺诈攻击下的对比.对 SuperTrust 而言,系统性能在合谋攻击下优于具有前端节点的合谋欺诈,原因如前所述.但是,PDTrust 和 RBTrust 两种机制正好相反,系统成功交易率在具有前端节点的合谋欺诈下都高于合谋欺诈下,这是因为前端节点在提供有效文件的缘故,而且 PDTrust 在合谋攻击时,系统中前端节点的信誉值最高,且随着仿真周期的增加,前端节点提供服务的能力增强,因此出现了由开始无法有效识别恶意节点到前端节点能力的提高,系统性能出现上升的趋势.

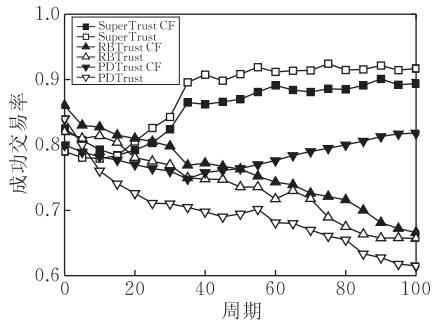


图 10 CF 下成功交易率随周期变化情况

## 5 结束语

在大规模 P2P 网络环境中,节点之间的信任关系建立是目前一个研究热点.本文提出了一种新的基于超级节点的 P2P 网络信任管理模型 SuperTrust.在 SuperTrust 中,信任关系被划分为 3 种:超级节点之间的信任关系、超级节点对普通节点的信任关系以及普通节点之间的信任关系,在具体给出各种信任度计算方式的同时,本文还提出基于节点相似性的反馈信息过滤算法以有效过滤掉信任信息里虚假的、误导性的和不公正的反馈.本文还通过大量的实验验证了信任模型的有效性和健壮性.仿真实验说明,本文提出的模型克服了已有模型的部分局限性,能够有效处理简单恶意攻击、诋毁、合谋欺诈及具有前端节点的合谋欺诈等各类恶意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工程可行性.

## 参 考 文 献

[1] Cornelli F, Damiani E, Vimercati D C. Choosing reputable servents in a P2P network//Proceedings of the 11th International Conference on World Wide Web(WWW'02). Hawaii, USA, 2002: 441-449

[2] Almenarez F, Marin A, Diaz D. Developing a model for trust management in pervasive devices//Proceedings of the 3rd IEEE International Workshop on Pervasive Computing and Communication Security(PerSec 2006). Washington, USA, 2006: 1-5

[3] Marti S, Garcia-Molina H. Limited reputation sharing in P2P systems//Proceedings of the 5th ACM Conference on Electronic Commerce. New York, NY, USA, 2005: 91-101

[4] Jordi S M, Paolucci M. On representation and aggregation of social evaluations in computational trust and reputation models. International Journal of Approximate Reasoning (Elsevier), 2007, 46: 458-483

[5] Lee S, Sherwood R, Bhattacharjee B. Cooperative peer groups in NICE//Proceedings of the IEEE Infocom. San Francisco, USA, 2003: 216-228

[6] Xiong L, Liu L. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857

[7] Song S S, Hwang K, Zhou R F. Trusted P2P transactions with fuzzy reputation aggregation. IEEE Internet Computing, 2005, 9(6): 18-28

[8] Kamvar S, Schlosser M. The EigenTrust algorithm for reputation management in P2P networks//Proceedings of the 12th International Conference on World Wide Web (WWW'03). Budapest, Hungary, 2003: 123-134

[9] Yamamoto A, Asahara D, Itao T. Distributed Pagerank: A distributed reputation model for open P2P networks//Proceedings of the International Symposium on Applications and the Internet Workshops (SAINTW'04). Tokyo, Japan, 2004: 389-396

[10] Tian Chun-Qi, Zou Shi-Hong, Wang Wen-Dong, Cheng Shi-Duan. A new trust model based on recommendation evidence for P2P networks. Chinese Journal of Computers, 2008, 31(2): 270-281(in Chinese)
(田春岐,邹仕洪,王文东,程时端. 基于推荐证据的有效抗攻击 P2P 网络信任模型. 计算机学报, 2008, 31(2): 270-281)

[11] Wang Y, Vassileva J. Trust and reputation model in peer-to-peer networks//Proceedings of the 3th International Conference on Peer-to-Peer Computing (P2P'03). Washington, DC, USA, 2003: 150-157

[12] Mekouar L, Iraqi Y, Boutaba R. A reputation management and selection advisor schemes for peer-to-peer systems//Proceedings of the 15th IFIP/IEEE International Workshop on Distributed Systems: Operations & Management. CA, USA, 2005: 208-219

[13] Zhang X Y, Zhang Q, Zhang Z S, Song G. A construction of locality-aware overlay network: Overlay and its performance. IEEE Journal on Selected Areas in Communications, 2004, 22(1): 18-28

[14] Zhang R M, Charlie Hu. Assisted peer-to-peer search with partial indexing. IEEE Transactions on Parallel and Distributed Systems, 2007, 18(8): 1146-1158

[15] Xue G T, You J Y, Jia Z Q. An interest group model for content location in peer-to-peer systems//Proceedings of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04). Beijing, China, 2004: 306-309

[16] Asvanund A, Bagla S, Kapadia M H, Krishnan R. Intelligent club management in peer-to-peer networks//Proceedings of the International Workshop on Economics of Peer-to-Peer Systems. California, USA, 2003: 52-60

[17] Guo L T, Yang S B, Wang J. Trust model based on similarity measure of vectors in P2P networks//Proceedings of the 4th International Conference on Grid and Cooperative Computing. Beijing, China, 2005: 836-847

[18] Hassana M, McClatchey R, Willers I. A scalable evidence based self-managing framework for trust management. Electronic Notes in Theoretical Computer Science (Elsevier), 2007, 179: 59-73

[19] Friedman E, Resnick P. The social cost of cheap pseudonyms. Journal of Economics and Management Strategy, 2001, 10(2): 173-199

[20] Schlosser M, Condie T, Kamvar S. Simulating a file-sharing P2P network//Proceedings of the 1st Workshop on Semantics in P2P and Grid Computing. California, USA, 2003: 113-121

**TIAN Chun-Qi**, born in 1975, Ph.D., lecturer. His research interests include peer-to-peer networks, trust management and quality of service (QoS).

**JIANG Jian-Hui**, born in 1964, Ph. D., professor, Ph. D. supervisor. His research interests include distributed system, trustworthy computing, embedded system and so on.

**HU Zhi-Guo**, born in 1978, Ph. D. candidate. His research interests include QoS of computer network, next generation network (NGN).

**LI Feng**, born in 1989, bachelor. His research interests include computer network, information security.

**Background**

P2P networks have already influenced and changed the style of our works and lives. Building trust relationship between peers in a large-scale distributed P2P system is a fundamental and challenging research topic. A novel trust model SuperTrust based on super peer is presented in this paper to solve some problems, for instance, noisy information filtering, loose trust relation between peers due to the difference of peers' interests and low probability of repeated transactions between them etc.. Experimental results show that SuperTrust has advantages in modeling dynamic trust relationship and filtering recommendation information, moreover, is more robust on trust security problems and more advanced in successful transaction rate.

This work is supported by the National Natural Science Foundation of China (grant No. 60903194), the National Research Foundation for the Doctoral Program of Ministry of Education (grant No. 200802471060), Open Foundation of Key Laboratory of Communication and Information System (Beijing Jiaotong University), and the National College Students Innovation Experiment Program. The authors have studied on network performance and service management since 2002. They focus on performance evaluation and improvement in Next Generation Internet, peer-to-peer (P2P) networks and wireless sensor networks. They have dozens of papers published in high level academic journals and international conference, including IEEE IPCCC, LNCS, JCST, Chinese Journal of Computers, Journal of Telecommunication, Chinese Journal of Electronics etc.