doi:10.11959/j.issn.1000-436x.2015012

基于动态分组的开放分布系统信任度量与管理研究

蒋黎明[1,2]，刘志明[1]，张琨[2]，徐建[2]，张宏[2]
(1. 南华大学 计算机科学与技术学院，湖南 衡阳 421001；2. 南京理工大学 计算机科学与技术学院，江苏 南京 210094)

摘 要：现有组信任模型在维护信任关系的稳定性与负载均衡能力方面存在局限性。为解决这些问题，提出一种稳定性增强的组信任模型 SEGTM（stability enhanced group based trust model），以动态组构造与管理为基础，划分同组及跨组节点间的信任关系并给予了各自的度量方法，较好地解决了信任模型因信任网络拓扑动态改变而难以有效维护信任关系度量的准确性问题。仿真实验结果表明，该模型在应对网络拓扑动态变化时具有较好的稳定性和负载均衡能力，同时也能有效抵抗恶意节点的攻击。

关键词：开放分布系统；信任网络；信任模型；局部信任度
中图分类号：TP391 **文献标识码**：A

Research on trust measure and management for open distributed systems based on dynamic grouping

JIANG Li-ming[1,2], LIU Zhi-ming[1], ZHANG Kun[2], XU Jian[2], ZHANG Hong[2]
(1. School of Computer Science and Technology, University of South China, Hengyang 421001, China;
2. School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract: A stability enhanced group-based trust model(denoted by SEGTM) for open distributed systems was presented to solve the problems of not sufficiently maintaining trust relation between peers due to the dynamic changes in trust network topology. First, the formation and dynamic management of peers' group were depicted in detail, including nodes gathered into the same group with similar interests, competition for group head and nodes within the group leave in active or passive ways. Then, the trust relation in proposed model was categorized into three kinds and subsequently each solution for these kinds was also put forward. So, the problems of decline in accuracy of computational trust degree between peers due to the difference of peers' interests and low probability of repeated transactions between them were addressed. Simulation results show that the model not only enhances the fairness and stability in response to dynamic changes in network topology, but also can effectively resist the attacks of malicious nodes.

Key words: open distributed systems; trust network; trust model; local trust degree

1 引言

近年来，随着计算机网络和通信技术的飞速发展，以电子商务、P2P、网格计算为代表的大规模开放分布系统得到了蓬勃发展。开放分布系统具有节点间对等自治、节点动态加入与离开以及网络灵活自组织性的特性，因而赢得了越来越多的 Internet 终端用户的青睐。也正是这些特性增加了开放分布系统中实体间交互安全和服务质量的不确定性，进一步阻碍了系统的广泛部署与应用。已有研究工作[1~3]表明，开放分布系统中通过建立实体之间的信任度量与评价模型，能够有效抑制开放分布系统服务质量的不确定性，增强实体交互安全，提高系统的可信性。

收稿日期：2013-12-12；**修回日期**：2014-03-12
基金项目：国家自然科学基金资助项目（61300234）；湖南省科技计划基金资助项目（2013GK3155）；南华大学博士科研启动基金资助项目（2012XQD09）；南华大学重点实验室建设基金资助项目
Foundation Items: The National Natural Science Foundation of China (61300234); The Project of Hunan Province Science and Technology Program(2013GK3155); The Scientific Research Starting Foundation for Doctors of China in University of South China (2012XQD09); The Construct Program of the Key Laboratory in University of South China

研究人员将分组机制引入到信任建模与评估研究中，节点基于相似的兴趣爱好聚类成组，且组内成员节点采用分布式管理，这样在增加组内节点重复交易次数的同时，又能在很大程度上将搜索信任信息引起的通信流量限制在局部范围内，这能够有效降低系统的通信开销，增强了系统的可扩展能力。但现有的组信任模型在评价模型性能时中多采用静态分组方式，即在系统初始化时完成组的构造和成员节点的确定，而在系统运行过程中不再考虑原有节点的退出和新节点的加入等引起的动态信任网络拓扑改变以及这种改变对模型的公平性和稳定性的影响。

1) 对于新加入节点，分组或分层信任模型通常为新节点设置较低的初始信任值，故新节点难以被其他节点选为服务提供者，自然也无法实现通过提供优质服务来提升自身的信任度，造成一个新加入节点总被“饿死”的恶性循环，这对新节点有失公平，而系统内原有的信任度最高的节点则会出现服务热点现象，因而系统的负载均衡能力较差。

2) 当一定数量的节点退出系统时，信任网络拓扑将发生变化，组内节点间信任度量的准确性下降，整个系统的交互成功率受到影响、无法快速恢复到较高水平，因而模型的自稳定性能力不强。

针对这些问题，本文将聚类思想与分层方法应用到信任关系度量与评估中，提出一种基于动态组的信任模型，克服了当前基于分组的信任模型在应对系统拓扑动态变化时模型的公平性和稳定性不足问题。首先，分析了开放计算系统中的信任特性，并提出一种新的组构造与动态管理方法；其次，给出了一种新的组信任度量模型 SEGTM（stability enhanced group based trust model），详细介绍了组内节点间和跨组节点间的信任度计算；并通过模拟实验对本文模型的准确性和有效性进行分析。

2　相关工作

现有的大多数信任模型都着力于为服务(资源)提供者计算信任度，比较有代表性的模型有集中式信任模型、全局信任模型以及局部推荐信任模型。eBay[4]，Amazon[5]等电子商务系统中均采用集中式信任模型，该类系统由少数中心节点负责整个网络的信任度量，而中心节点的身份是由 CA 颁发的证书予以确认，这种集中式信任模型应用于大规模开放系统中将存在中心节点性能瓶颈和单点失效问题。全局信任模型中节点间的信任度是通过邻居参与者之间局部信任度的迭代计算得到，此方法的计算和通信开销颇大，且对节点的能力要求较高。文献[6]对信任类型进行了划分，通过区别对待服务信任和反馈信任、直接信任和间接信任，增强了全局信任模型在复杂环境中的应用能力。在基于推荐的信任模型[4,7~15]中，服务请求节点通过询问其他节点（推荐者）来计算对服务提供节点的信任度。按照反馈推荐的聚合方式分为基于全局推荐的信任模型[4,7~9]和局部推荐的信任模型[11~14]。全局推荐信任模型充分利用其他所有节点的推荐信息来度量目标节点的信任度，因而每个节点只有一个全局信任度。虽然全局推荐信任模型可以克服信任系统中交互数据的稀疏性，但无法体现信任度量的多方面性与个体差异性等特征，而局部推荐信任模型有效地调和了这一矛盾，因此在大规模分布环境中具有更好的适用性。

随着研究的深入，不少研究人员将分组策略引入到信任建模工作中。文献[10]提出了基于全局信任的多层分组 P2P 信任模型，利用多层分组策略，通过各个层次间相互协作来对一个对等节点的信任度进行评价，避免了全局信任度模型中的全网无限迭代问题。但文献[10]中的分组是基于物理距离的减法聚类方法实现，而没有考虑同组节点间的兴趣相似性，因此，在开放分布系统中，这种分组的效率难以得到保证。

近年来提出的 SuperTrust[16]、GossipTrust[9]等模型是典型的基于分组的信任模型[9,10,13~18]。SuperTrust 依赖超级节点对群组进行划分和管理，并将节点的信任关系区分为超级节点间的信任关系、超级节点与普通节点的信任关系及普通节点间的信任关系 3 种类型。超级节点是预先指定的,且不会退出系统, 该假设条件在开放自组织计算环境中往往难以满足。基于组内推荐的信任度量机制计算组内普通节点间的信任值，通过计算群组内所有节点对此超级节点的全局信任度来计算超级节点的信任值。SuperTrust 模型下的系统结构如图 1 所示。如果服务提供节点（比如 P3）位于同一群组，则服务请求节点（P2）在本地存储对该服务提供节点的交易记录；如果

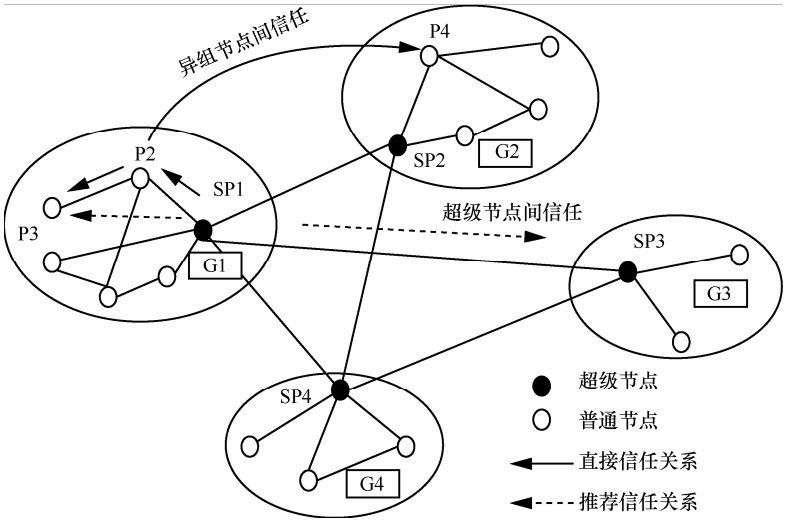


图 1 SuperTrust 模型下的系统结构

服务提供节点（比如 P4）位于其他群组，则服务请求节点（P2）将交易记录向其所在群组的组头节点（SP1）反馈，组头节点 SP1 根据节点 P2 的反馈建立对节点 P4 所在群组的组头节点 SP2 的信任关系。

以 GossipTrust[9]、SuperTrust[16]、StereoTrust[17] 为代表的众多基于分组的信任模型虽然解决了基于推荐信任模型中存在的交互数据稀疏及获取推荐信息引起的通信开销大等问题，但存在如引言中所指出的几个问题：1) 模型为加入新节点分配了较低的初始信任值，这使具有较强服务能力的新加入节点失去了向其他节点提供优质服务的机会，自然也无法通过提供高质量服务来提升自身的服务信任度；2）模型也没有针对组内节点的加入和离开给出有效的管理方法，即就组内信任信息的动态更新与共享过程给出具体实现方法，也没有评估大量组内节点退出系统所引起的网络拓扑变化对模型的稳定性带来的影响。

本文首先给出了一种基于节点的相似兴趣而聚集成组的组构造与动态管理方法，包括组初始化和新节点的准入控制、全局信任表的更新和组头节点的竞争，以及组内节点主动、被动离开的动态管理机制。在此基础上提出一种基于动态分组的组信任模型（SEGTM, stability enhanced group based trust model），详细描述了组内节点间以跨组节点间的信任度量方法。最后通过仿真节点动态加入和退出 2 种场景下模型的交互成功率和平均负载等性能指标变化来验证 SEGTM 的有效性及可靠性。

3 新的组构造与动态管理方法

本文提出一种基于相似兴趣聚集的组构造与动态管理方法。基于组的信任网络结构如图 2 所示。组内节点按照角色可以分为 3 种。

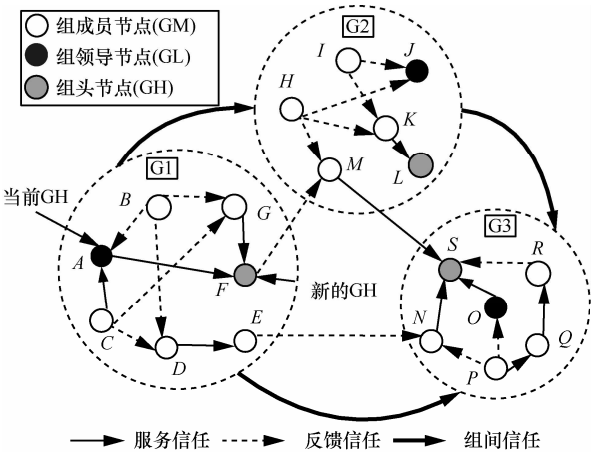


图 2 基于组的信任网络结构

1) 组成员节点，只能以服务请求者或者服务提供者身份参与交互；

2) 组头节点（兼有组成员节点身份），对新加入节点进行准入控制，向组成员节点广播全局信任表；

3) 组领导节点（兼有组成员节点身份），负责组头节点的竞争以及本组黑名单的维护和管理。

节点根据历史交易情况建立对目标节点的本地信任度。如果节点 G 与目标节点 F 位于同一分组，则节点 G 在本地存储对节点 F 的交易记录；如果目标节点 M 位于其他群组，则节点 F 将交易记录提

交给其所在组头节点 A，节点 A 根据组内所有节点与组 G2 内节点的所有交互经验建立对组 G2 的组信任关系。

本文中用到的符号统一说明如下：N_i 为非组内成员节点 i；N_i^g 为组 g 中的成员节点 i；ID_g 为组 g 的 ID 号；C_g 为组 g 的组中心；TV_i^F 为节点 i 的反馈信任度；TV_i^S 为节点 i 的服务信任度；GH_i^g 为组 g 的组头节点 i；NS_i^g 为组 g 中成员节点 i 的邻居集。

3.1　组初始化及构造算法

系统内任一节点 N_i 的服务兴趣均由一个 n 维向量表示，节点 N_i 的兴趣记为 $I_{N_i}=\{a_1,a_2,\cdots,a_n\}$ $(0\leqslant a_1,a_2,\cdots,a_n\leqslant 1)$，每个组都有一个组中心（某一类服务兴趣的参照值），也用一个 n 维矢量表示，记为 $\boldsymbol{C}=\{b_1,b_2,\cdots,b_n\}$ $(0\leqslant b_1,b_2,\cdots,b_n\leqslant 1)$。$I_{N_i}$ 和 C_g 的距离表示节点 N_i 的兴趣与组 g 的组中心的相似度（简记为节点 N_i 与组 g 的相似度），采用余弦相似度公式计算如下

$$S_{N_i,C_g}=\cos\alpha=\frac{\sum_{k=1}^{n}a_k b_k}{\sqrt{(\sum_{k=1}^{n}a_k{}^2)(\sum_{k=1}^{n}b_k{}^2)}} \tag{1}$$

每一个组都是由与组中心的距离（相似度）小于既定阈值 θ 的节点构成，若 $S_{N_i,C_g}\geqslant\theta$，则 N_i 被允许加入组 g。

组初始化及构造算法如下。

输入：网络初始节点集 Z，$|Z|=N$，Z_g 为组 g 中的节点集，Z_S 为非在组节点。

步骤 1　若 $Z_S\neq\Phi$，则从 Z_S 中随机选择一个节点 N_i 担任组头 GH_i^g，此时有 $Z_S=Z_S-N_i$，GH_i^g 创建全局信任表和组间交易表，并生成广告消息 $AdverticeMsg[ID_g,C_g,\theta,GH_i^g]$ 向全网节点广播。

步骤 2　$N_j(N_j\in Z_S)$ 接收到消息 $AdverticeMsg[ID_g,C_g,\theta,GH_i^g]$，若 N_j 的兴趣矢量与 C_g 的相似度值大于 θ，则 N_j 向 GH_i^g 发送新节点请求加入消息 $NewJointReq[N_j,IP_i]$。

步骤 3　如果 GH_i^g 收到的消息列表为空，则转而执行步骤 6，否则，GH_i^g 从 *NewJointReq* 列表中依次选择 N_j 的加入请求消息进行处理。

1) GH_i^g 检查节点 N_j 是否在其黑名单中，若是则向节点 N_j 发送 *JointRep*[*fialed*]，返回步骤 3，选择其他节点的 *NewJointReq* 进行处理。

2) GH_i^g 检查组规模与组最大容量 ξ，如果前者大于后者，则发送 $NewJointRep[GH_{N_i}^g,0]$，返回步骤 3，选择其他节点的 *NewJointReq* 进行处理。

3) 如果 GH_i^g 在其全局信任表中查找不到 N_j 的信任值，则初始化 $TV_j^S=1$，$TV_j^F=0.5$。

步骤 4　GH_i^g 向 N_j 发送成功加入消息 $JointRep[ID_g,GH_i^g,NS_j^g,TV_j^S,TV_j^F]$；// NS_j^g 为 N_j 在组 g 中的邻居集。

步骤 5　GH_i^g 向组内成员节点广播新成员节点 N_j 消息，组内成员节点更新自己的邻居集。

步骤 6　重复执行步骤 1，直到 $Z_S=\Phi$，此时，组的初始化与构造完成。

输出：所有的 Z_g。

当系统初始化完成后，组头节点定期向组内节点广播最新的全局信任表，同时，检查组规模是否已经达到组最大容量，若没有，则向全网节点广播广告消息 $AdverticeMsg[ID_g,C_g,\theta,GH_i^g]$。

全局信任表和组间交易表是由每个组的首任组头节点（也是本组的领导节点）负责创建，其中，全局信任表项包含节点名称和相应的全局信任值（服务信任）；组间交易表项包含源节点所在组名称、源节点、目的节点所在组名称、目的节点，交易评价。

3.2　组头节点的竞争过程

本文提出的组头竞争原则是组头由组内最大全局信任度者担任，而全局信任度又是汇聚所有成员节点的直接信任度，并采取加权处理得到。本节中采用 $TV_i^S(j)$ 表示 N_i^g，N_j^g 之间的服务信任度（成功交互次数/总服务交互次数），也称为直接信任度；$TV_m^F(i)$ 表示 N_i^g，N_j^g 之间的反馈信任度（成功推荐次数/总推荐次数）。间接信任度表示通过第三者的推荐形成的信任度，即声誉（reputation）。

定义 1　（全局信任度）实体 i 对实体 j 的直接信任度表示为 $TV_i^S(j)$，组 g 中与节点 j 有过服务交互的节点数为 $|S_g|$，与节点 i 有过反馈交互的节点数为 $|F_g|$，则节点 j 的全局信任度 $TV(j)$ 表示为

$$TV(j)=\frac{\frac{\sum_{m=1}^{|F_g|}TV_m^F(i)}{|F_g|}\sum_{i=1}^{|S_g|}TV_i^S(j)}{|S_g|} \tag{2}$$

组领导节点以固定间隔收集组内成员的局部信任表，通过加权平均各成员节点的局部信任值以获得组内各成员节点的全局信任表。组领导节点将选择全局信任度最高的节点作为新的组头节点，并与其共同执有全局信任表。如果在组头节点的选择过程中，如果出现多个成员节点的信任值相等的情况，则依据以下优先级规则进行竞争。

优先级 1：成员节点是组领导节点；

优先级 2：成员节点是当前的组头节点；

在确定了新的组头节点后，组领导节点向组内成员节点广播组头节点更换消息。以图 2 中的组 G1 为例，全局信任表的获取及组头节点竞争结果如图 3 所示。

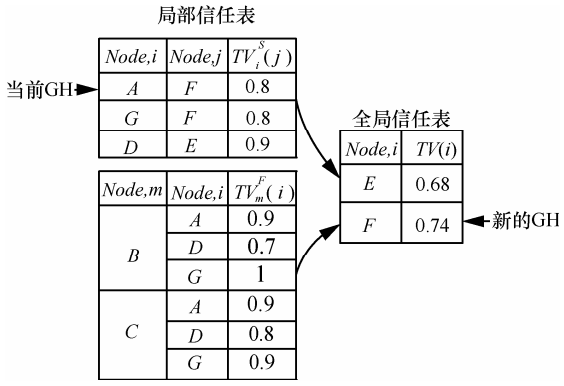


图 3 组头节点竞争

3.3 组内节点主动或被动离开

对于组内节点主动离开情况，分为 3 种情况。

1) 若组 g 内成员节点 N_j 要离开，首先，N_j 向组头节点 GH_i^g 发送离开消息，然后，GH_i^g 向节点 N_j 发确认消息，允许其离开，并向组内成员节点广播 N_j 已离开的消息，所有节点成员及时更新自己的邻居。

2) 若当前组头节点 GH_i^g 要离开，首先，GH_i^g 向组领导节点发送离开请求消息，并将其维护的组间交易信息移交给组领导节点。然后，组领导节点从全局信任表中选择信任度值次高节点作为新的组头节点，并向 GH_i^g 发确认消息允许其离开，同时向组内成员节点广播新的组头节点信息。

3) 若组领导节点要离开，则该组将不再存在。

假设在初始阶段加入网络的节点可以作为组领导节点，这是因为作为整个网络的构建者和最初的使用者，不应该也不会去破坏网络。同时，组领导节点除了承担成员节点的功能（参与交易，维护自身交易结果）外，还承担着维护本组成员节点和组头节点的管理。因而，本文假定在系统运行过程中，组领导节点不会离开组，只有在组内恶意节点操纵了组头节点竞争的时候，组领导节点才会离开。

若组领导节点检测到成员节点的恶意行为，则将该节点添加进本组黑名单中（被动离开），同时通报本组成员节点，所有成员节点更新邻居。节点被动离开本组的情况，分为 2 种情况。

1) 较低的全局信任值，即全局信任表中成员节点的信任值低于阈值 δ。

2) 虚假推荐，组领导节点接收到各节点提交的局部信任表后，很容易得到提交不一致推荐的节点（对同一节点的推荐值与推荐均值间的误差超过阈值 γ，则视为不一致推荐）。对于自身交互经验并不充分的推荐节点而言，也会给出错误推荐，但随着交互经验的积累，推荐值会变得准确可靠。因而本文设定，若组内某节点提供的不一致推荐所在的交互周期数超过阈值 ω，则视为虚假推荐节点。

4 基于组的信任模型 SEGTM

在 SEGTM 中，节点被划归到不同的组中，SEGTM 假定每个节点不能同时申请加入多个组（节点加入多个组可视为该节点拥有多个身份，但在每个组中只有一个独一无二的身份）。图 2 中表达了 3 种类型的信任关系：1) 同组节点间的信任关系，例如在组 G1 中，组内节点 A 与节点 E 之间为服务信任关系，B 与 F 之间为反馈信任关系；2) 跨组节点之间的信任关系，节点 F(G1)与 H(G2)之间的服务信任关系；3) 本文还刻画了组 G1 与 G2、G3 与 G2 之间的信任关系。上述 3 种类型信任关系的度量方式分别介绍如下。

4.1 同组节点间信任度量

在 SEGTM 中，基于本地交易记录和推荐信任信息加权计算同一组内的节点信任度计算，为此，首先给出局部信任度的定义。

定义 2 （局部信任度）如果在整个交易时期内节点 N_i^g,N_j^g 之间有 N_{ij} 次历史交互记录，则节点 N_i^g 对 N_j^g 的局部信任度可表示为

$$TV_i(j)=\begin{cases}\dfrac{N_{ij}^S-N_{ij}^F}{N_{ij}}, & N_{ij}=N_{ij}^S+N_{ij}^F \text{且} N_{ij}\neq 0\\ 0, & N_{ij}=N_{ij}^S+N_{ij}^F \text{且} N_{ij}=0\end{cases} \tag{3}$$

其中，N_{ij}^S 表示交易成功的次数，N_{ij}^F 表示交易失败的次数。本文规定如果两者没有交互记录，则局部信任度为 0。

由于同组内节点间的交易类型（分为服务交易和反馈交易）不同，信任关系被区分为服务信任与反馈信任，因而节点 N_i^g 、N_j^g 之间可能存在 2 种不同的局部信任度，即服务信任度 $TV_i^S(j)$ 和反馈信任度 $TV_i^F(j)$。

局部信任度只是 2 个节点之间直接交易之后有限的信任关系，不能以此作为一个节点的全局信任度，所以节点 i 评价节点 j 的信任度，还需要依靠节点 i 汇集推荐节点的信任信息（即节点 j 的推荐信任度）。

定义 3　（推荐信任度）请求节点 i 对各个推荐节点的反馈信任度来加权其推荐信息，合成后便得到被评价节点 j 的推荐信任度。因此，节点 i 计算出 j 的推荐信任度为

$$TRe_{ij}=\frac{\sum_{m\in I(j)} TV_i^F(m)TV_m^S(j)}{\sum_{m\in I(j)} TV_i^F(m)} \tag{4}$$

其中，$TV_m(j)$ 为推荐节点 m 对节点 j 的服务信任度，$TV_i^F(m)$ 为节点 i 对推荐节点 m 的反馈信任度，$I(j)$ 为节点 j 的推荐者集合。

综上，同一组内成员节点之间服务信任度为

$$TV_{ij}^S=\alpha TV_i^S(j)+(1-\alpha)TRe_{ij} \tag{5}$$

其中，α 是直接信任度的信心因子，α 的取值和交互的数目有关，交互的数目越多则 α 取值越大，$0\leqslant\alpha\leqslant 1$。本文取 $\alpha=\dfrac{N_{ij}}{H}$（当 $N_{ij}>H$ 时，$\alpha=1$），其中，N_{ij} 为节点 i 和节点 j 之间交互的数目，H 为设定的交互数目门限值，本文中取值为 10。

4.2　跨组节点间的信任度量

由于同组节点兴趣相似，相互之间积累了较多的交互经验，组内节点间往往能基于大量的交易评价信息得出较为准确的信任度量；跨组节点间的兴趣相差较大，交易数据存在稀疏性问题，因而服务请求节点需要通过分享组内其他节点的跨组的相似交易信息来计算与其他组节点间的信任度。

定义 4　组 G_x 对组 G_y 下节点 $N_j^{G_y}$ 的信任度表示为

$$TV_{G_x,N_j^{G_y}}=\frac{\sum_{N_i^{G_x}\in I(N_j^{G_y})}(N^S_{N_i^{G_x},N_j^{G_y}}-N^F_{N_i^{G_x},N_j^{G_y}})}{\sum_{N_i^{G_x}\in I(N_j^{G_y})} N_{N_i^{G_x},N_j^{G_y}}} \tag{6}$$

其中，$I(N_j^{G_y})$ 为所有与 $N_j^{G_y}$ 有过交互的节点，$N^S_{N_i^{G_x},N_j^{G_y}}$ 为节点 $N_i^{G_x}$ 与 $N_j^{G_y}$（G_y）成功交易的次数，$N^F_{N_i^{G_x},N_j^{G_y}}$ 为 $N_i^{G_x}$ 与 $N_j^{G_y}$ 失败交易的次数，$N_{N_i^{G_x},N_j^{G_y}}$ 为 $N_i^{G_x}$ 与 $N_j^{G_y}$ 的交易总次数。同样考虑到交易类型的不同，信任度 $TV_{G_x,N_j^{G_y}}$ 也区分为 $TV^S_{G_x,N_j^{G_y}}$（服务信任）和 $TV^F_{G_x,N_j^{G_y}}$（反馈信任）。

定义 5　组 G_x 对组 G_y 的信任度表示为

$$TV_{G_x,G_y}=\begin{cases}N^S_{G_x,G_y}-N^F_{G_x,G_y}\big/N_{G_x,G_y}, & N_{G_x,G_y}=N^S_{G_x,G_y}+N^F_{G_x,G_y}\neq 0\\ 0, & N_{G_x,G_y}=N^S_{G_x,G_y}+N^F_{G_x,G_y}=0\end{cases} \tag{7}$$

其中，$N^S_{G_xG_y}$ 为群组 G_x 中节点与群组 G_y 中节点交易成功的次数，$N^F_{G_xG_y}$ 为群组 G_x 中节点与 G_y 中节点交易失败的次数。根据交易类型的不同，信任度 TV_{G_x,G_y} 也区分为 $TV^S_{G_x,G_y}$（服务信任）和 $TV^F_{G_x,G_y}$（反馈信任）。

跨组节点 $N_i^{G_x}$ 和 $N_j^{G_y}$ 间的信任关系度量将会出现 3 类情形。

1)　$N_i^{G_x}$ 基于组内成员节点推荐得到对 $N_j^{G_y}$ 的信任度，即 G_x 内成员节点 $N_k^{G_x}$ 与 $N_j^{G_y}$（$G_x\neq G_y$）之间存在较充分的交易经验，因此，$N_i^{G_x}$ 采用式(4)、式(5)计算 $N_j^{G_y}$ 的信任度。

2)　$N_i^{G_x}$ 基于组 G_y 中节点 $N_{k,k\neq i,j}^{G_y}$ 推荐得到对 $N_j^{G_y}$ 的信任度，此时 $N_i^{G_x}$ 对 $N_j^{G_y}$ 的信任度计算如式(8)所示，若 G_x 对 $N_k^{G_y}$ 不存在反馈信任时，式(8)中的 $TV^F_{G_x,N_k^{G_y}}$ 将由 $TV^F_{G_x,G_y}$ 替代。

$$TV^S_{N_i^{G_x},N_j^{G_y}}=\frac{\sum_{N_k^{G_y}\in I(N_i^{G_x})} TV^F_{G_x,N_k^{G_y}}TV^S_{N_k^{G_y}}(j)}{\sum_{N_k^{G_y}\in I(N_i^{G_x})} TV^F_{G_x,N_k^{G_y}}} \tag{8}$$

3) $N_i^{G_x}$ 基于组 $G_{z,z\neq x,y}$ 中节点 $N_{k,k\neq i,j}^{G_z}$ 推荐得到对 $N_j^{G_y}$ 的信任度，则 $N_i^{G_x}$ 对 $N_j^{G_y}$ 的信任度计算如式（9）所示。若 G_x 对 $N_k^{G_z}$ 不存在反馈信任时，式（9）中的 $TV^F_{G_x,N_k^{G_z}}$ 将由 $TV^F_{G_x,G_z}$ 替代。

$$TV^S_{N_i^{G_x},N_j^{G_y}} = TV^F_{G_x,N_k^{G_z}} TV^F_{G_x,N_k^{G_y}} \tag{9}$$

情形 1)下节点间信任度计算结果可信度是最高的，而情形 3)下信任值的可信度最低。所以当 $N_i^{G_x}$ 和 $N_j^{G_y}$ 间信任度量同时存在 2 种或 3 种情形时，本文取可信度最高的计算结果作为跨组节点间的信任值。

5 实验结果与分析

本文仿真基于北卡罗拉州立大学开发的多 Agent 交互系统[19]，同时实现了 SuperTrust 方案[16]，基于局部推荐的信任模型（PRTrust）和基于全局推荐的信任模型（GRTrust），并对它们的优劣进行了比较分析。PRTrust 和 GRTrust 模型均采本文中的式(4)和式(5)计算节点间的信任值，不同之处在于，PRTrust 模型中节点是通过邻居的依次推荐来获得对目标节点的信任信息（即部分推荐），而 GRTrust 模型中，节点将聚合系统内所有与目标节点有过历史交互的节点的推荐信任值，并假定所有推荐节点的可信度相同。

5.1 实验设置

本文实验思想如下。1) 系统中有 N 个 Agent，用一个 4 维矢量来建模 Agent 的服务兴趣和服务能力，假定 Agent i 的服务兴趣用矢量 $\boldsymbol{I}$ 表示为 $\boldsymbol{I}_i=(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$，其中，$\alpha_k\in(0.5,1)(k=1,2,3,4)$；Agent j 的服务能力用矢量 $\boldsymbol{E}$ 表示为 $\boldsymbol{E}_j=(\beta_1,\beta_2,\beta_3,\beta_4)$，其中，$\beta_k\in(0,1)(k=1,2,3,4)$。本文定义 Agent i 的服务兴趣与 Agent j 的服务能力的相似度 $Sim(\boldsymbol{I}_i,\boldsymbol{E}_j)$ 作为标定 j 向 i 提供服务的 QoS 值，如式(10)所示。如果 $Sim(\boldsymbol{I}_i,\boldsymbol{E}_j)\geqslant 1$，则视为成功交互；如果 $Sim(\boldsymbol{I}_i,\boldsymbol{E}_j)<1$），则视为失败的交互。

$$(QoS)_{Sji}=Sim(\boldsymbol{I}_i,\boldsymbol{E}_j)=\frac{\sum_{k=1}^{4}\alpha_k\beta_k}{2\sqrt{\sum_{k=1}^{4}\alpha_k{}^2}} \tag{10}$$

2) 在每一个仿真周期中，网络中的每个节点都可以请求一次服务。当节点发起请求后，等待接受相应并从中选择节点进行交互，直到服务成功或者试过了所有的响应，请求结束并进行数据收集。这就是一个完整的仿真周期。在 SuperTrust 和 RBTrust 模型中，节点本地可保存 10 个节点的信任信息。本文中组内节点都有自己的邻居集(NS)，并保存与其邻居节点的交互。每一仿真周期结束后，所有的节点根据交互情况更新自己的邻居。

网络中的节点依据行为表现分为以下几种。

诚实 Agent。这类 Agent 无论是提供服务还是对其他节点的推荐都是真实的，简称为 HA。

恶意 Agent。这类 Agent 可以分为以下几种。

1) 概率欺骗 Agent，这类节点在其他 Agnet 请求服务时以一定概率可靠服务，记这类节点为 SA；

2) 虚假推荐 Agent，这类 Agent 对外提供可靠服务，但诋毁所有与之交互过的 HA，提交虚假评价信息，称这类 Agent 为 EA；

3) 共谋欺骗 Agent，SA 类与 EA 类 Agent 组成利益团体，夸大该团体内的同类 Agent，并与 HA 类 Agent 的交互时选择不合作，称这类 Agent 为 CA。

实验仿真了 100 个服务交互周期，每个 Agent 在每个周期会发起 1 轮服务请求，每个 Agent 在整个仿真过程中可完成 100 次服务交互。实验结果均取 10 次运行结果的平均值以提高实验数据的可靠性。表 1 为本文模型的参数设置。

表 1 实验参数设置

参数名	描述	值
N	系统中 Agent 总数	可变
NS	每个 Agent 的最大邻居数	5
K	系统初始化群组个数	20
θ	节点与组的相似度	0.15
ξ	组成员数上限值	50
δ	可信节点的全局信任值下限	0.4
γ	推荐信任值误差上限	0.2
ω	不一致推荐交互周期数上限	4
H	组内节点交互数目门限值	10

5.2 公平性与抗恶意节点攻击能力

本组实验中，本组实验中，初始节点总数设为 500 个。当系统稳定后，向系统中增加新节点，新节点的邻居为随机指派，且每个节点的邻居不超过 5 个。假设好节点以 96%的概率提供可信服务（考虑到实际应用环境中由于非自身原因导致的交互

失败情况发生）。仿真试验针对系统交互成功率变化（新节点加入后第一个交互周期）、节点的平均负载（诚实节点单位周期内平均提供的服务数）和对恶意节点的抵御能力指标对比分析 SEGTM、SuperTrust、PRTrust 和 GRTrust 4 种信任模型的优劣。

5.2.1　系统交互成功率及节点的平均负载

系统稳定后，分别以 10%~50%的比例向系统中增加新节点（均为诚实节点）。图 4 是增加新节点后的系统交互成功率变化情况。由图 4 可知，在新节点加入前，系统的交互成功率为 96%（节点加入前的一个仿真周期内的服务交互统计结果），新加入节点比例少于 25%时，系统的交互成功率变化并不明显，但随着新节点比例的增加，系统交互成功率下降速度加快，当新节点比例达到 50%时，系统性能最低的是 PRTrust 模型，交互成功率只有 88%左右。而 SEGTM 模型基本没有受到大的影响，因为新节点仍然是基于自身兴趣加入到原有组中，并且原有组中早已形成稳定的信任关系，所以，系统的交互成功率几乎不受影响，依然维持在 95%左右，这表明 SEGTM 模型对开放分布系统规模的持续增长能提供很好的支持。

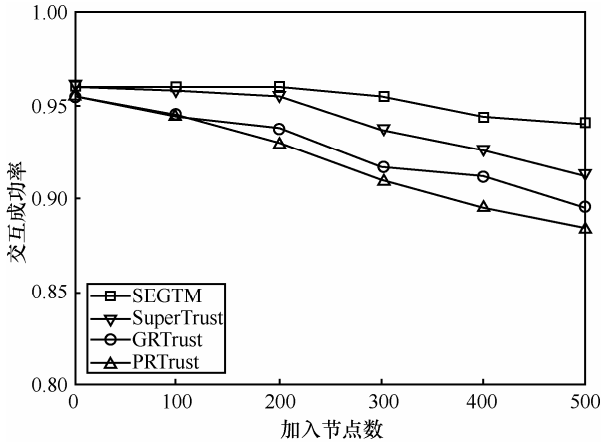


图 4　新节点加入后的系统交互成功率变化

图 5 反映了系统中加入新节点后节点的平均负载变化情况，由图 5 可以看出，随着新节点的加入，SuperTrust、PRTrust 和 GRTrust 3 模型中服务提供节点的平均负载也随之上升，这是因为新节点加入系统后，由于初始信任度较低，因而只能选择系统中信任度较高的节点来提供服务，使服务提供节点的提供的服务数增加。而本文模型中，由于新节点被赋予较高的初始信任值，新节点也同样有机会作为服务提供节点，因而服务提供节点的平均负载基本保持稳定。因此，本文模型有利于鼓励新节点积极参与到系统协作中来，并通过提供高质量的服务来提升节点的全局信任度。

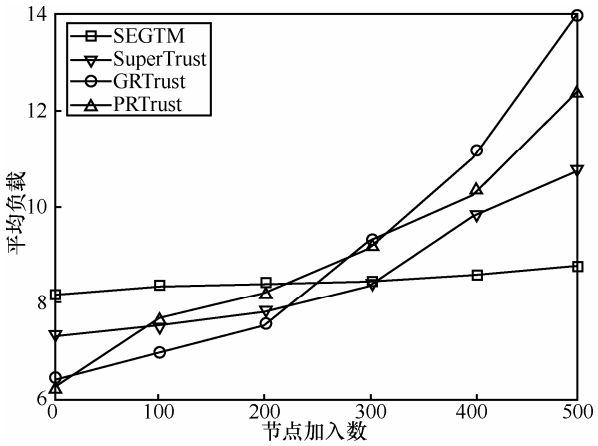


图 5　新节点加入后的服务提供节点的平均负载

5.2.2　对恶意节点的抵御

系统稳定后，分别以 10%~50%的比例向系统中增加新节点（恶意节点比例为 0~50%）。概率欺骗节点提供可信服务的几率为 40%，虚假推荐以 40%的几率提供诚实推荐，合谋节点对内部节点提供的都是可信服务，对外为不可信服务。

图 6(a)反映了系统交互成功率随 SA 类恶意节点比例增加而变化的情况。由于 SEGTM 和 SuperTrust 模型能够通过组内具有相似兴趣的节点获取推荐信任，因而在恶意节点比例较小时，SEGTM、SuperTrust 模型能够有效识别 SA 类恶意节点，所以系统交互成功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，SEGTM 模型的性能显示出较大的优势，因为 SEGTM 模型通过计算组内节点的全局信任度，将恶意节点排除在本组之外，大大降低了组内节点选择恶意节点作为服务提供方的概率。而 PRTrust 模型下系统的交互成功率随恶意节点比例的增加而大幅减小，这是因为恶意节点会隐藏其恶意行为而以一定概率（60%）提供可信服务，因此诚实节点会错误地评估其他节点的可信度，造成交互成功率下降。

图 6(b)反映了系统中存在虚假推荐节点时 4 种模型的交互成功率变化情况。可以看出，随着恶意节点比例的增大，SEGTM 和 SuperTrust 模型依然能够保持较高的交互成功率，这是因为这 2 种模型能够过滤掉虚假和不公平推荐信息，因而能识别出

虚假推荐节点；同时，充分利用组内反馈可信度高的节点的推荐，增强了信任度量的准确性，抵御了大多数恶意节点的攻击，即便是在恶意节点比例达到 50%时，系统的成功交易率仍然能维持在较高的水平。相比之下，随虚假推荐节点比例的增加，PRTrust 和 GRTrust 模型的交互成功率却下降得很快，这是因为 PRTrust 和 GRTrust 模型不能将推荐信息里不真实和误导性的信息区分开来，当虚假推荐节点多时，系统对节点的信任度计算误差较大，致使交互成功率不断下降。

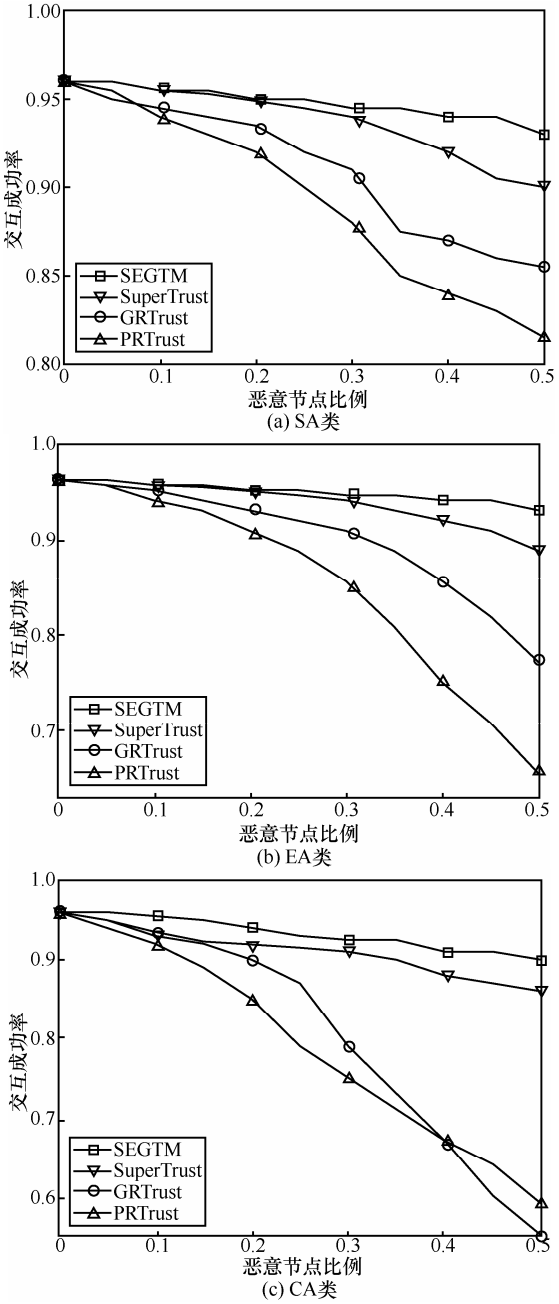


图 6 新节点中各类恶意节点对系统交互成功率的影响

图 6(c)是在恶意节点共谋欺骗攻击下 4 种模型的交互成功率对比情况。可以看出，随着恶意节点比例的增加，SEGTM 和 SuperTrust 模型的系统交互成功率下降缓慢，这是因为在 SEGTM 和 SuperTrust 模型中，具有相似兴趣的节点聚集成组，并且基于组内节点的反馈可信度过滤掉不公平的推荐信息。而 GRTrust 和 PRTrust 模型在恶意节点的共谋欺骗攻击下，节点不能准确评估另一个节点的信任值，因此，系统的成功交易率随恶意节点比例增加迅速下降。

5.3 节点退出情况下模型的稳定性

本组实验中，初始节点总数设为 1 000 个。在系统稳定后，系统内的节点按照比例（系统规模的 10%~50%）退出系统。图 7 是节点退出后系统交互成功率变化情况。由图 7 可知，在节点退出前，系统的交互成功率为 96%（仅指节点退出前的一个仿真周期内的统计结果），当退出节点比例少于 20%时，SEGTM 和 SuperTrust 模型下系统的交互成功率变化并不明显，但随着新加入节点比例的增加，系统交互成功率下降速度加快，当退出节点比例达到 50%时，SEGTM 模型下系统的交互成功率只有 60%左右，而 SuperTrust 模型下系统的交互成功率为 50%左右。系统性能最低的是 PRTrust 模型，当退出节点比例达到 50%时，交互成功率只有 40%。

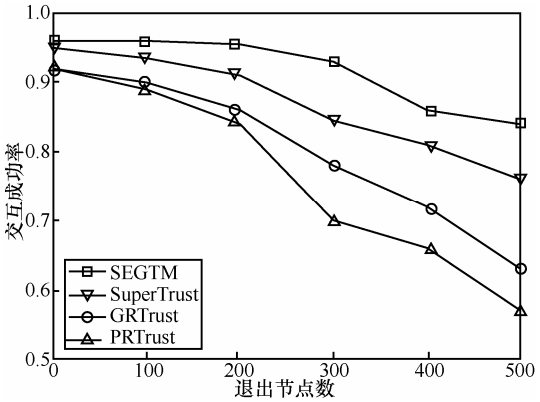


图 7 节点退出后系统交互成功率变化

图 8 所示为系统剩余节点（50%节点退出后）的交互成功率随仿真周期的变化情况。相对于 SuperTrust 模型而言，SEGTM 模型下节点的交互成功率下降得要少，且能够迅速恢复到较高水平。这是由于组内部分节点退出后，组领导节点通过更新全局信任表，从剩下节点中选择出新的组头节点，一定程度上保障了组内节点交互的成功率。PRTrust

模型的交互成功率下降最为严重，这是因为在 PRTrust 模型中，节点综合利用本地信任信息和邻居的推荐来计算目标节点的信任值，因此，当大量节点退出系统后，节点将难以有效获取所有节点的信任信息，导致信任度量的准确性迅速下降。

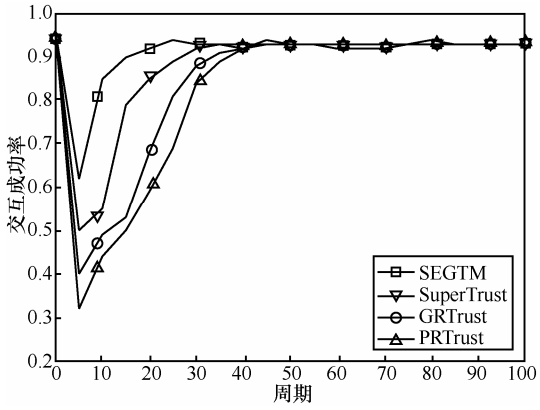


图 8　系统剩余节点交互成功率随仿真周期的变化

6　结束语

在大规模开放分布系统中，有效建立节点间信任关系度量是目前的研究焦点与热点问题。本文提出了一种自稳定性增强的组信任模型 SEGTM。首先，SEGTM 采用一种新的组构造与动态管理方法，在恶意节点被检测出并被加入组黑名单的同时，通过赋予新加入节点较高的初始信任值，鼓励新加入节点通过提供高质量服务来提升节点的全局信任度，在改善节点公平性的同时，降低了系统的平均负载。在大量节点退出系统时，组内成员节点及时更新各自的邻居集，同时组领导节点通过更新全局信任表选出新的组头节点，一定程度上维护了组内与组间的有效信任信息，增强了模型的稳定性。其次，SEGTM 将节点间的信任关系划分为同组节点和跨组节点间的信任度量，并给出了各自的计算方法，在节点间兴趣差异大、相互发生重复交易的可能性较小情况下增强了模型信任度量的准确性。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，对网络拓扑的动态变化具有很好的公平性和自稳定性，同时也能有效处理各类恶意节点不同程度的攻击，因而具有很好的应用前景。

参考文献：

[1] DU R Z, TIAN J F, WANG Z X, *et al*. A trust model of P2P network based on reputation and risk[A]. Proceedings of the 2009 WRI World Congress on Software Engineering(WCSE2009)[C]. Xiamen, China, 2009.382-386.

[2] 蒋黎明, 张琨, 徐建等. 证据信任模型中的信任传递与聚合研究[J]. 通信学报, 2011 32(8):91-100.
JIANG L M, ZHANG K, XU J, *et al*. Research on trust transitivity and aggregation in evidential trust model[J]. Journal on Communications, 2011 32(8):91-100.

[3] WAN K Y, ALAGAR V. A context-aware trust model for service-oriented multi-agent systems[A]. 1st International Workshop on Quality-of-Service Concerns in Service Oriented Architectures (QoSCSOA 2008)[C]. Sydney, Australia, 2008.221-236.

[4] eBay[EB/OL]. http://www.ebay.com.

[5] Amazon[EB/OL]. http://www.amazon.com.

[6] KAMVAR S, SCHLOSSER M. The eigentrust algorithm for reputation management in P2P networks[A]. Proceedings of the 12th International Conference on World Wide Web (WWW '03)[C]. Budapest, Hungary, 2003.

[7] LI X, LIU L. Peertrust: supporting reputation-based trust for peer-to-peer electronic communities[J]. IEEE Transactions on Knowledge and Data Engineering, 2004. 16(7): 843-857.

[8] SWAMYNATHAN G, ZHAO B Y, KEVIN C A, *et al*. Globally decoupled reputations for large distributed networks[J]. Advances in Multimedia, 2007, 2007(1): 1-14.

[9] ZHOU R F, HWANG K, CAI M. Gossiptrust for fast reputation aggregation in peer-to-peer networks[J]. IEEE Transactions on Knowledge and Data Engineering, 2008, 20(9):1282-1295.

[10] 孙知信, 唐益慰. 基于全局信任度的多层分组 P2P 信任模型[J]. 通信学报, 2007, 28(9): 133-140.
SUN Z X, TANG Y W. Multilayer and grouping P2P trust model based on Global reputation[J]. Journal on Communications, 2007, 28(9): 133-140.

[11] ZHOU R F, HWANG K. Powertrust: a robust and scalable reputation system for trusted peer-to-peer computing[J]. IEEE Transactions on Parallel and Distributed Systems, 2007. 18(4):460-473.

[12] SONG S, HWANG K, ZHOU R, *et al*. Trusted P2P transactions with fuzzy reputation aggregation[J]. Internet Computing, IEEE, 2005, 9(6):24-34.

[13] LEE S, SHERWOOD R, BHATTACHARJEE B. Cooperative peer groups in NICE[A]. Proc of Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies[C]. 2003.1272-1282.

[14] ZHAO H. Y, LI X. L. H-trust: a group trust management system for peer-to-peer desktop grid[J]. Journal of Computer Science and Technology 2009, 24(5):833-843.

[15] SONG S, HWANG K, ZHOU R E. Trusted P2P transactions with fuzzy reputation aggregation[J]. IEEE Internet Computing, 2005. 18-28.

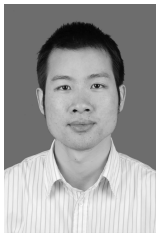
[16] XUE G T, YOU J. Y, JIA Z Q. An interest group model for content location in peer-to-peer systems[A]. Proceedings of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04)[C]. Beijing, China, 2004.306-309.

[17] LIU X, DATTA A, RZADCA K. StereoTrust: a group based personalized trust model[A]. 18th ACM Conference on Information and Knowledge Management[C]. Hongkong, China, 2009.7-16.

[18] ZHANG Y, ZHENG H, LIU Y, *et al*. A group trust model based on service similarity evaluation in P2P networks[J]. International Journal of Intelligent Systems, 2011, 26(1): 47-62.

[19] YU B, SINGH M P. Distributed reputation management for electronic commerce[J]. Computational Intelligence, 2002, 18(4):53-549.

作者简介：



蒋黎明（1983-），男，湖南永州人，南华大学讲师，主要研究方向为自组织网络安全隐私保护与动态信任建模。

刘志明（1972-），男，湖南浏阳人，南华大学教授，主要研究方向为云计算与大数据管理。

张琨（1978-），女，陕西西安人，南京理工大学副教授，主要研究方向为生物计算与信息安全。

徐建（1979-），男，江苏江阴人，南京理工大学副教授，主要研究方向为信息安全、人工智能。

张宏（1956-），男，江苏南京人，南京理工大学教授、博士生导师，主要研究方向为无线网络与网络安全。