社交网络中一种基于社区推荐的信任模型

张 丰[1] 王 箭[1] 赵燕飞[2] 杜 贺[1]
(南京航空航天大学计算机科学与技术学院 南京 210016)[1]
(南京审计学院计算机科学与技术系 南京 211815)[2]

摘 要 信任度计算一直是社交网络中备受人们关注的问题,而对陌生节点的信任度计算更是其中的研究热点。目前多数的信任模型由于推荐证据的不完整使得对陌生节点信任度计算准确性不高。随着社区数量的不断增多,基于社区的社交网络成为当今社交网络发展的一种趋势,引入社区推荐模型替代原有的节点推荐模型来提高推荐证据的完整性和可靠性,进而提高陌生节点信任度计算的准确性;同时考虑友群信任度对社区信任度的影响,并给出社区关联度因子来解决社区推荐可能存在的合谋攻击。最后,通过仿真实验验证了该模型的合理性和有效性。

关键词 社交网络,社区推荐,社区关联,信任度,友群
中图法分类号 TP393 **文献标识码** A

Trust Model Based on Groups Recommendation in Social Network

ZHANG Feng[1] WANG Jian[1] ZHAO Yan-fei[2] DU He[1]
(School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)[1]
(Department of Computer Science and Technology, Nanjing Audit University, Nanjing 211815, China)[2]

Abstract In social networking, trust calculation have attracted more and more attention, especially between two unknown nodes. At present most of the trust models aren't accurate enough due to incomplete recommendation evidence. With the increasing of community, community becomes a development trend of social networks today. In this paper, we first proposed community recommendation model in substitution for the existing node recommendation model, to improve integrity and reliability of the recommend evidence, and consequently improve the accuracy of unknown nodes trust computation. Secondly friend group trust influence was considered and community correlation factor was presented to solve the community possible collusion attack. Finally, simulation results verified the rationality and effectiveness of the proposed method.

Keywords Social network, Community recommendation, Community correlation factor, Trust, Friend group

1 引言

近年来,随着社交网络的广泛流行和用户数量的急剧增多,社交网络中的安全问题引起了人们越来越多的关注,信任度计算便是重要的一项。

社交网络是指个人之间的关系网络[1],它是建立在人际关系基础上的。与其它一般网络不同,在基于关系和社区形成的社交网络中,来访用户被划分为"朋友"和"非朋友"两种关系,朋友关系依靠社会关系进行确认,通过向请求为朋友的人提出询问来验证朋友是否真实。对于非朋友关系的信任度计算是当前社交网络信任度研究的热点。目前社会性网络中信任的研究还处于起步阶段,研究成果较少。

Jennifer等人[2]利用FOAF在基于Web的社交网络中计算没有直接联系用户之间的信任度关系,其信任度仅有两种取值(0表示不信任,1表示信任),很难用于现实的环境中。文献[3]将博弈论引入社交网络信任机制,基于博弈论方法的基本思想是用户信任和用户行为收益的博弈问题,被访问用户根据自身的收益矩阵来决定是否对来访用户开放私有信息,最终目的是使其自身的收益最大化。Bhuiyan等人[4]提出了在基于地理位置的社会性网络中结合信任与社会声誉来决策推荐的机制,该机制没有给出社会声誉的具体计算方法。

现有社交网络中关于"非朋友"关系的信任度计算主要有3类方法。

1)基于关系及关系深度的信任度计算

基于社交网络中关系的这一特性,文献[5]给出了通过关系和关系深度来计算信任度的方法,将不同的关系对应不同的信任值,通过关系及关系深度得到对陌生用户的信任值。这种方法没有考虑到用户对于社交网络的需求,即通过寻找有共同爱好的用户来扩大自己的朋友圈子。

2)基于用户属性、兴趣爱好、年龄的信任度计算

到稿日期:2013-07-18 返修日期:2014-02-07 本文受江苏省普通高校研究生科研创新计划资助项目(CXZZ12_0161),中央高校基本科研业务费专项资金资助。

张 丰(1989—),女,硕士生,主要研究方向为信息安全、P2P网络中信任度计算,E-mail:ahfengz@sina.com;王 箭 男,教授,博士生导师,CCF会员,主要研究方向为应用密码学、系统安全分析与设计等;赵燕飞(1978—),女,讲师,主要研究方向为信息安全、信任计算;杜 贺(1984—),男,博士生,主要研究方向为传感网中的信任度计算、传感器网络的密钥管理等。

文献[6]给出了一种节点信任值计算方法，其信任值计算的基本数据为朋友数量、注册时间和发帖数量(注册时间长和发帖数量多，说明用户在社交网络中的时间较长，建立的关系比较广泛)、用户之间的相互回帖数量、语义 eb 数据隐含的信息(blog 之间的联系紧密程度、私下交互机密信息等)。文献[7]针对移动社交网络，考虑在移动社交网络中用户的位置信息(通过手机 GPS 或者移动网络定位获得)、用户的状态(Presence)信息(如在线、离线、开会等)、手机日历/日程信息、用户的偏好信息，将人们之间的信任度划分为熟悉性产生的信任度以及相似性产生的信任度两部分：更合理、更全面地体现现实社会中人们之间产生信任的过程，代表现实生活中用户之间真实的信任关系。

3)基于用户推荐的信任度计算

当一个人想要了解陌生的人时，通常他会向周围的人打听关于这个人的信息，为了避免有些人提供不诚实的信息，他通常会向多个人打听，然后综合推荐信息得到需要了解的信息。Li Xiong[8]等人提出的 PeerTrust 算法以及窦文等人提出的 Trust 模型[9]都是基于上述思想的，通过朋友推荐给出对陌生节点的信誉值。这些算法对恶意节点具有较好的抑制，但算法不适合大规模的网络环境，在大规模环境下收敛速度较慢，同时评价信息的稀疏使得可信度计算误差较大。

一般说来，人们加入社交网络，希望找到自己兴趣相投的人，扩大自己的朋友圈，因此社区成为社交网络中一个重要的组成元素[10]，近年来基于兴趣的各类 SNS 社区如雨后春笋般出现[11]。另外，由于社区形成原因的多样性，社交网络中的每个人还可以属于多个社区。文献[12]的统计结果表明，每个大学生手机社交网络用户平均拥有 3～4 个社区。它的作用在于能够找到更多有共同兴趣爱好的朋友，用户通过社区可以使得原本陌生的用户之间由于共同的爱好建立联系，产生信任，人们总是倾向于跟态度、兴趣、价值观相近的用户有更多的交流，因此社区中的其他用户对该用户的评价更为准确。

目前在对社区的研究中，文献[13]在 SNS 社区模型研究的基础上，给出了一种群体信任算法，更好地描述了社交网络中用户对社区、社区对其中用户、社区与社区之间的群体信任关系。文献[14,15]提出了基于主观逻辑的群体信任模型，它通过顺序、选择、循环以及并行这 4 种基本的约束模式及其彼此之间的嵌套来表达群体中的个体之间的约束，但该模型只适用于群体中个体之间的约束关系可以确定的情况。该模型对软件群体的信任关系提供了很好的支持，但网络中的群体中个体之间的约束关系往往很难确定。

本文改进上述基于用户推荐的信任度计算模型，引进社区推荐代替已有的个体推荐。给出了社区推荐信任度的计算方法，同时引入社区关联信任度抑制社区中可能存在的合谋攻击，进一步提高信任度计算的准确性和抗合谋攻击。

2 相关概念

目前社交网络中节点对陌生节点的信任计算主要采用基于推荐的信任度计算方法，采用与目标节点有过交易的朋友节点的推荐，由于社交网络的特殊性，节点和其朋友节点在兴趣爱好、交往范围上往往具有很高的相似度，因此来自朋友节点的推荐可能会受到了解程度的限制，相对不准确。因此本文提出一种基于社区推荐的方法，以提高推荐证据的准确性。下面给出社区信任以及信任相关的一些概念。

1. 社区(group)

在社交网络中，社区是指一些节点因为某些共同的兴趣组成的兴趣组，它可以由多个节点组成，特殊地，也可以仅由一个节点组成。

2. 信任计算方法

当前信任计算方法主要有信誉和信任两种方法。

信誉系统：这种方法是利用收集到的用户行为和其它信息来计算用户的信誉值。

信任：主要依靠用户的社会关系由用户来指定与自身的信任关系。

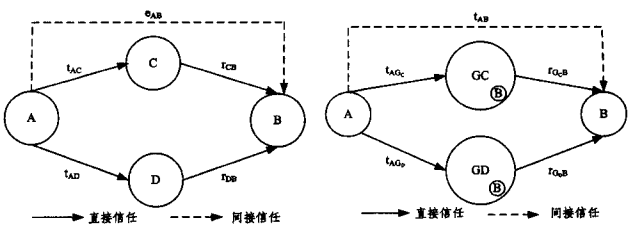
这两种方法各有优缺点，信誉值方法的优点是客观、容易分类，缺点是计算结果类似、不够灵活、用户无法干预、在用户很多的情况下计算复杂。信任值方法的优点是容易使用、更贴近信任的实际，缺点是用户提供的推荐信息可能误差较大，因此很难准确确定陌生人的信任值。

综合上面两种方法，本文提出了一种基于社区推荐的信任值计算方法，用局部信誉值的方法来计算节点在社区中的信任值，利用信誉系统在获得可信度方面较为全面的优势，提高了推荐信息的准确性，同时通过社区过滤用户的数量，降低信誉度计算的复杂度。用信任的方法表示节点对某一社区的信任度，弥补信誉值计算过程中的不够灵活、用户无法干预的问题，并增加社区关联度因子，有效地削弱了恶意节点合谋攻击的行为。

3 基于社区推荐信任模型

3.1 社区推荐模型

在社会网络中任一节点将其他节点分为“朋友”和“非朋友”两类。信任关系是人际关系的核心，朋友节点之间的信任容易建立，陌生节点间的信任度往往取决于其他节点的推荐。已有的推荐模型都是基于单个节点的推荐，推荐模型如图 1(a)所示，但基于单个节点的推荐可能会由于交易次数较少、了解程度局限而使推荐信息误差比较高；随着社区的发展，本文提出一种基于社区推荐的信任模型，推荐模型如图 1(b)所示，用目标节点所在社区的推荐代替单个节点的推荐，由于同一个社区内的用户相互了解程度较高，有效提高了推荐信息的准确性。



(a) 基于节点推荐的信任模型　(b) 基于群体推荐的信任模型

图 1　基于推荐的信任模型

图 1(a)是传统的推荐信任模型，节点 A 对节点 C 的直接信任度为 t_{AC}，节点 C 对节点 B 的直接信任度作为推荐信任度 r_{CB}，节点 A 与节点 B 之间存在两条信任路径，分别为 P_{ACB} 和 P_{ADB}，由这两条信任路径综合计算可得到节点 A 对节点 D 的间接信任度为 e_{AB}。

在图 1(b)中，G_C 和 G_D 代表 B 加入的社区，r_{G_CB} 表示社区 G_C 对节点 B 的推荐信任值，本文使用节点 B 在社区 G_C 中

的局部信誉值作为社区对节点 B 的推荐信任值。t_{AG_C} 代表社区外节点 A 对社区 G_C 的信任值，由节点 A 依靠与社区中节点的交互记录得到的直接信任值综合社区的关联信任值得到。最终 A 综合社区对目标节点的推荐值以及其对该社区的信任值，得到对节点 B 的间接信任值 e_{AB}。

3.2 基于社区推荐模型总体信任度计算方法

该算法使用推荐的方法计算陌生节点之间的信任度，用社区推荐替代传统的节点的推荐，使其具有更高的准确性和抗合谋攻击性。节点 A 对陌生节点 B 的总体信任度计算方法根据式(1)得到：

$$T(A,B)=\sum_{i\in G(B)} TNG(A,G_i)\times RGN(G_i,B) \tag{1}$$

式中，$T(A,B)$为节点 A 对目标节点 B 的总体信任度，$G(B)$为节点 B 加入的所有社区的集合，$TNG(A,G_i)$为节点 A 对 B 所在社区 G_i 的信任度，在节点对社区的信任研究中，人们常常依据节点自身对社区中节点的信任关系复合得到。$RGN(G_i,B)$为社区 G_i 对其中节点 B 的推荐信任度，采用社区中成员的评价计算节点 B 的局部信誉值作为社区 G_i 对节点 B 的信任值。

3.3 社区对其中节点的推荐信任度

本文使用节点在社区中的局部信誉值作为社区对其中节点的推荐信任度，该信誉值的计算基于社区中其他用户的直接信任值，通过直接信任值的迭代得到对应用户在社区中的信誉。一个节点在社区中的信誉为社区中其他节点对该节点直接信任值的加权平均，权重为对应节点在社区中的信誉。本文参考信誉值的计算方法，给出社区对节点进行推荐信任度计算的公式，如式(2)所示。

$$RGN(i,G)=\frac{1}{\sum_{j\in V(G),j\neq i} RGN(j,G)}\sum_{j\in V(G),j\neq i}(RGN(j,G)\times s_{ji}) \tag{2}$$

式中，$RGN(i,G)$表示节点 i 在社区 G 中的局部信誉度；$V(G)$表示社区 G 中节点的集合，s_{ji} 表示节点 j 对节点 i 的直接信任度，若节点 j 与节点 i 没有过直接交互，则 $s_{ji}=0$。

若社区 G 中有 n 个节点，则可列出 n 个类似于式(2)的方程，其中 $RGN(i,G)$、$RGN(j,G)$均为未知数。求解这个问题即是求解一个 n 元二次方程组，可采用下面的迭代算法来进行求解。

上述算法首先对群 G 内所有节点在社区中的可信度赋一个(0,1]之间的初值，然后根据式(2)不断进行迭代，最后的收敛结果即为社区内每个节点在社区内的可信度。

3.4 节点对社区的信任度

节点 A 对社区 G 的信任值产生于其与该社区中节点在以往交易中产生的信任度，同时考虑与该社区交互较多的社区可信度。因此节点对社区的信任度包括直接信任度和社区关联信任度两部分。直接信任度是 A 在与社区 G 中节点的交互行为中形成的对社区的信任度。社区关联信任度是 A 通过社区 G 友群的可信度及其与社区 G 的关联程度得到的对社区 G 的信任度。节点 A 对社区 G 的信任度计算方法如式(3)所示：

$$TNG(A,G)=\alpha e(A,G)+(1-\alpha)rel(A,G) \tag{3}$$

式中，$TNG(A,G)$为 A 对社区 G 的总体信任度，$e(A,G)$为节点 A 对社区 G 的直接信任度，$rel(G)$为社区 G 的关联信任度。α 为调节因子，当节点对社区较为陌生时，关联信任度对社区的总体信任度影响较大，当节点较为熟悉社区时，直接信任度对社区的整体信任度影响较大。当 A 和 B 处于同一个社区时，$TNG(A,G)=1$，认为 A 完全信任此社区时，节点 A 对 B 的信任值为 B 在社区中的局部信誉度。

文献[9]给出了一种群体信任算法，本文参考该方法，将其应用于基于社区的信任模型中，同时增加社区关联度因子来抑制社区合谋推荐，提出基于社区关联度的社区信任度计算方法。

3.4.1 直接可信度

节点对社区的直接可信度产生于节点与社区中节点的交易行为，一般认为当节点与社区的交易越多时，节点越信任该社区，当节点与社区每次的交互行为评价值越高时，节点认为此次交易越愉快，此时对社区的信任度也相应会增加。因此计算节点 A 对社区 G 的直接信任度时，节点 A 对社区中节点的直接信任度起到关键的作用，其通过节点 A 对社区 G 中有过直接交互的节点的信任值加权平均得到，另外考虑节点 A 与社区 G 中有过直接交互的节点数量对直接信任值产生影响。综合上述因素，式(4)给出直接信任值的计算方法：

$$e_{AG}=I(A,G)\times\frac{1}{n}\sum_{i\in V(A,G)} e_{Ai} \tag{4}$$

式中，$V(A,G)$为社区 G 中与节点 A 有过直接交互的节点的集合，e_{Ai} 为 A 对社区 G 中有过直接交互的节点 i 的信任值。n 为社区 G 中与节点 A 有过直接交互的节点的个数，$I(A,G)$为社区 G 中与 A 有过直接交互的节点的数量对直接信任度的影响，当社区 G 与节点 A 有过直接交互的节点的数量越多时，节点 A 应对社区 G 有着更多的了解，此时 e_{AG} 应该越大，具体 $I(A,G)$的计算如式(5)所示：

$$I(A,G)=1-\prod_{i\in v(A,G)} 1-e_{Ai} \tag{5}$$

3.4.2 社区关联信任度

社区推荐可以提高推荐的准确性，同时也可能存在合谋推荐攻击。引入社区关联信任度，考虑友群信任度对社区信任度的影响，进一步提高用户对社区信任度计算的准确性，抑制可能存在的合谋攻击。一般认为当一个社区的可信度较低时，与其具有较高关联度的社区的可信度也较低。社区关联度是指两个社区中节点的重合度及交互频率。具体来说，两个社区中节点重合度越高，交易的次数越多，它们的关联度越大，我们把这两个社区称为友群，友群之间的信任度应较接近。交易的次数可以通过记录的方式获得，节点重合度可能存在包含、被包含、有交集节点、无交集节点 4 种情况，如图 2 所示，式(6)给出这 4 种情况下节点重合度的计算方法。

$$\mathrm{sim}(g,k)=\frac{num(g,k)}{\min(num(g),num(k))} \tag{6}$$

式中，$\mathrm{sim}(g,k)$表示 g、k 两个社区的节点重合度，$num(g)$、$num(k)$分别表示社区 g 和社区 k 中的节点个数，$num(g,k)$表示同时属于两个社区的节点个数。当两个社区存在包含关系时，如图 2(a)、(b)所示，$\mathrm{sim}(g,k)=1$。

根据实验结果，我们把节点重合度达到一定比率或者成员数均为 n、交易次数达到 $n^2/4$ 次的两个社区称为友群，即平均两个社区间一半的节点间有过直接交互。按照上述对交易次数的限制和对节点重合度的划分，进而把友群分为交易友群、节点重合友群两类，式(7)考虑交易友群和节点重合友群，给出了社区关联信任度的计算方法。

$$rel(A,g)=\beta_1\sum_{i\in G_1(g)}\frac{1}{n}TNG(A,i)+\beta_2\frac{1}{\sum_{j\in G_2(g)}\mathrm{sim}(g,j)}\sum_{j\in G_2(g)}(\mathrm{sim}(g,j)\times TNG(A,j)) \tag{7}$$

式中，$rel(A,g)$表示节点 A 对社区 g 计算出的社区关联信任度，G_1、G_2 分别为交易友群、节点重合友群集合，n 为交易友群包含的友群数量，$TNG(A,i)$、$TNG(A,j)$分别代表节点 A 对社区 i、j 的信任度。$\mathrm{sim}(g,k)$代表两个友群的节点重合度。β_i 为调节因子，调节交易友群及节点重合友群在社区的关联信任度计算上的影响。本文更加看重交易友群对关联信任度的影响，当一对友群同属两个友群范畴、$sim(g,k)$不为 1 时，我们认为其属于交易友群，反之认为是节点重合友群。因此我们选取 $\beta_1>\beta_2$。

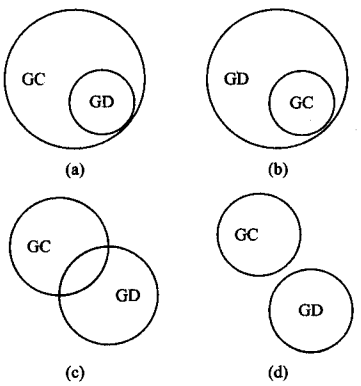


图 2　节点重合友群划分

4　实验结果及分析

本节从算法的准确性和抗攻击性这两方面对给出的基于社区推荐的信任模型进行仿真。仿真使用 VS 2010 仿真软件，硬件环境为 Intel Core 双核处理器，4GB 内存，64 位操作系统，仿真规模包括 10000 个节点、1000 个社区，每个节点平均加入 3 个社区。

4.1　交易友群的最优划分次数

本文通过友群的信任度来抑制恶意节点的合谋推荐，目前没有对交易友群划分标准的研究。本文针对交易友群划分标准进行了实验，根据不同交易次数划分交易友群对交易成功率的影响，图 3 给出了实验结果。

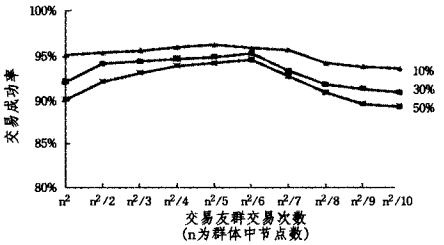


图 3　交易友群的交易次数选择

图 3 选取节点数均为 n 的两个社区，给出在恶意节点比率为 10%、30%、50%的情况下，交易友群的次数划分选择为 n^2、$n^2/2$、…、$n^2/10$ 的实验结果。从图中可以看出，该模型在恶意节点率增加的情况下性能仍较稳定，即使恶意节点占到一半时，在第一次交易时也能够对节点的信任度进行准确的预判，使得交易成功率仍处在较高的水平上；当划分交易友群的次数选择较高或较少时，交易成功率均有下降，当交易次数选择为$[n^2/4, n^2/6]$时，即社区中平均有一半的节点之间有过交互，此时交易成功率最高。

4.2　基于社区推荐模型信任计算的准确性

在仿真的社交网络系统中有两种类型的节点：一类是友好节点，这些节点在系统中具有良好的行为，因此这类节点的推荐较为可信。另一类是恶意节点，这些节点在系统中有不良行为，进行恶意推荐或提供虚假信息。在一个健康的社交网络中大部分节点应该都是可信的。同时应该能够降低恶意节点的信任度，抑制恶意节点的欺骗行为。表 1 给出在恶意节点比率为 10%、20%、30%的情况下，基于单个节点推荐和基于社区推荐的节点信任值的实验结果。

表 1　健康网络中节点推荐与社区推荐信任值比较

名称	10 个恶意节点				20 个恶意节点				30 个恶意节点			
	peertrust		本文算法		peertrust		本文算法		peertrust		本文算法	
	恶意	非恶意	恶意	非恶意	恶意	非恶意	恶意	非恶意	恶意	非恶意	恶意	非恶意
(0—0.2)	8	0	9	0	17	0	19	0	22	0	27	0
(0.2—0.4)	2	0	1	0	2	0	1	0	6	0	3	0
(0.4—0.6)	0	5	0	2	1	5	0	0	2	7	3	0
(0.6—0.8)	0	20	0	15	0	22	0	16	0	25	0	19
(0.8—1)	0	65	0	73	0	53	0	64	0	38	0	51

从表 1 中的实验结果可以看出：在网络中恶意节点率相对较低时，本文算法针对陌生节点的第一次交易时的信任评估优于基于单个节点的推荐算法，同时在恶意节点率相对较高为 30%时，该算法仍具有较好的性能，同时使得恶意节点的信任度稳定维持在较低的水平上。

4.3　基于社区推荐模型的抗合谋攻击性

针对社区推荐可能存在的合谋攻击，文中引入友群的概念抵制社区的合谋攻击，表 2 给出了基于社区推荐的信任度评估算法在抗合谋攻击方面的性能评估，同时给出了友群数对抗合谋攻击的影响对比。

表 2　友群数量对社区推荐中抗合谋攻击的影响

名称	每个群组有 2 个友群				每个群组有 3 个友群				每个群组有 4 个友群			
	10 个合谋群		20 个合谋群		10 个合谋群		20 个合谋群		10 个合谋群		20 个合谋群	
	合谋	非合谋	合谋	非合谋	合谋	非合谋	合谋	非合谋	合谋	非合谋	合谋	非合谋
(0—0.2)	7	0	17	0	8	0	17	0	9	0	19	0
(0.2—0.4)	3	0	3	0	2	0	3	0	1	0	1	0
(0.4—0.6)	0	10	0	11	0	7	0	9	0	3	0	4
(0.6—0.8)	0	15	0	17	0	12	0	15	0	5	0	8
(0.8—1)	0	65	0	52	0	71	0	56	0	82	0	68

从表2中的实验结果可以得出，当平均每个社区有2个友群时，合谋社区的信任度均未高于0.4，且多数分布于(0—0.2)的极低信任度等级上，同时随着平均社区友群数的增加，系统的抗合谋攻击能力也不断增强，当平均每个社区有4个友群时，90%以上的合谋社区的信任值均位于(0—0.2)等级上，同时，80%以上的非合谋社区信任分布在(0.8—1)的高信任等级上。

结束语 本文提出了一种计算陌生节点信任度的推荐模型，并给出了具体的计算方法。模型使用局部信誉大大提高了推荐证据的可靠性及准确性，同时通过社区域对节点个数进行隔离，有效地降低了算法的复杂度。进一步引入社区关联信任度解决社区推荐中可能存在的合谋攻击，很好地抑制了社区的合谋攻击，提高了对陌生节点的信任度计算准确性。

参 考 文 献

[1] 包昌火，谢新洲，申宁. 人际网络分析[J]. 情报学报，2003，22(3)：366-374

[2] Golbeck, Jennifer, Hendler, et al. Inferring binary trust relations hips in Web-based social networks[J]. ACM Transactions on Internet Technology(TOIT), 2006, 6(4): 497-529

[3] 张胜兵，蔡皖东，李勇军. 一种基于博弈论的社交网络访问控制方法[J]. 西北工业大学学报，2011，29(4)：652-657

[4] Bhuiyan T, Xu Y, Josang A. Integrating trust with public reputation in location-based social networks for recommendation making[C] // Proceedings of IEEE/W/IC/ACM International Conference on Web Intelligence and Intelligent Agent Technology. Sydeny, NSW, 2008: 107-110

[5] 陈庆余，刘建伟，刘靖. 半去中心化的社交网访问控制方案[J]. 计算机工程与应用，2011，47(20)：85-87，95

[6] Brickley D, Miller L. FOAF Vocabulary Specification 0.91. Namespace Document[OL]. http://xmlns.com/foaf/0

[7] 乔秀全，杨春，李晓峰，等. 社交网络服务中一种基于用户上下文的信任度计算方法[J]. 计算机学报，2011，34(12)：2403-2413

[8] Li Xiong, Ling Liu. A Reputation-Based Trust Model for Peer-to-Peer Ecommerce Communities[C] // Proceedings of IEEE Conference of E-Commerce. ACM Press, 2003: 275-284

[9] 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

[10] 刘耀庭. 社交网络结构研究[D]. 杭州：浙江大学计算机学院，2008

[11] Chou A Y. The analysis of online social networking; How technology is changing e-commerce purchasing decision[J]. International Journal of Information Systems and Change Management, 2010, 4(4): 353-365

[12] 乔歆新，朱吉虹，沈勇. 手机移动社交网络的用户研究[J]. 电信科学，2010，26(10)：109-113

[13] 鲍捷，程久军. 基于社交网络的群体信任算法[J]. 计算机科学，2012，39(2)：38-42

[14] 王勇，代桂平，侯亚荣，等. 基于模糊逻辑的群体信任模型[J]. 北京工业大学学报，2010，36(7)

[15] 王勇，代桂平，侯亚荣，等. 基于主观逻辑的群体信任模型[J]. 通信学报，2009，30(11)：8-14

(上接第154页)

[2] Zhao L Y, Liu F. Service-oriented Pricing and Resource Allocation in Grid Computing Environment[C] // 2011 International Conference on Electronic & Mechanical Engineering and Information Technology. 2011: 3927-3930

[3] Schneider S, Shabalin P, Bichler M. On the robustness of nonlinear personalized price combinatorial auctions[J]. European Journal of Operational Research, 2010(206): 248-259

[4] Christopher T, Parkes C. Cryptographic combinatorial securities exchanges[C] // The 13th International Conference on Financial Crypto-graphy and Data Security, Feb 2326, 2009. Accra Beach, Barbados: Springer Verlag, 2009: 285-304

[5] Xia M, Stallaert J, Whinston A B. Solving the combinatorial double problem[J]. European Journal of Operational Research, 2005, 164(1): 239-251

[6] Ma J, Orgun M A. Trust management and trust theory revision [J]. IEEE Trans on System, Man and Cybernetics Parta: System and Human, 2006, 36(3): 451-460

[7] Vijayakumar V, Wahidhabanu R S D. Trust and reputation aware security for resource selection in grid computing [C] // 2008 International Conference on Security Technology Proceedings. Sanya, China, Dec. 2008: 121-124

[8] Yuan L L, He Z J, Zeng G S. A Resource Trade Model Based on Trust Evaluation for Grid Computing[C] // IFIP International Conference on Network and Panallel Computing-Workshops. 2007: 506-511

[9] Li L, Liu Y A, Ma X L. Grid resource allocation based on the combinatorial double auction[J]. Acta Electronica Sinica, 2009, 37(1): 165-169

[10] Yang M, Liu Y A, Ma X L. Research on Grid Resource Allocation Based on Equivalent Price[C] // ISECS International Colloquium on computing, Communication, Control, and Management. 2009: 148-152

[11] Wang K, Li L, Hausheer D. A Trust-Incentive-based Combinatorial Double Auction Algorithm[C] // IEEE/IFIP Network Operations and Management Symposium NOMS 2010: Mini-conference. 2010: 209-215

[12] Gan Z B, Xiao X L, Li K. A Multi-dimension Trust Risk Evaluation for E-commerce systems[C] // IEEE, Eighth Web Information Systems and Applications Conference. 2011: 143-149

[13] Xu X Q, Yang L. A Multi-dimensional and Multi-directional Trust Model for Federated Identity Management[C] // International Conference on Instrumentation, Measurement, Computer, Communication and Control. 2011: 512-515

[14] Li X Y, Zhou F, Yang X D. A multi-dimensional trust evaluation model for large-scale P2P computing[J]. J. Parallel Distrib. Comput, 2011(71): 837-847