P2P 网络环境下基于推荐的信任模型*

雷月菊，陈光喜
（桂林电子科技大学 数学与计算科学学院，广西 桂林 541004）

摘　要：基于网络中节点之间不仅仅局限于直接交易建立起来的信任关系，还包括了第三方推荐信任的事实，提出了在 P2P 网络环境下基于推荐的信任模型。该模型用成功次数与失败次数在总交易数目中的比例作为直接信任度，将交易信誉与推荐信誉明确区分出来，引入了偏移因子计算推荐节点的可信性，通过惩罚因子和风险因素动态平衡节点直接信任度和其他节点的推荐信任度，得到目标节点的综合信任值，并给出仿真实验验证。实验结果证明，模型计算的综合信任值更趋近其真实值，并且能抵抗恶意节点的诋毁、协同作弊等威胁。

关键词：P2P 网络；交易信誉；推荐信誉；推荐；偏移因子
中图分类号：TP393.01　　**文献标志码**：A　　**文章编号**：1001-3695(2012)11-4320-03
doi:10.3969/j.issn.1001-3695.2012.11.082

Trust model based on recommended in P2P network environment

LEI Yue-ju, CHEN Guang-xi
(*School of Mathematics & Computational Science, Guilin University of Electronic Technology, Guilin Guangxi* 541004, *China*)

Abstract: The nodes in network are not only confined the trust relationship which established by trading directly, but also including the third party's recommended trust. This paper presented a trust model based on recommended in P2P environment. It used the proportion of success and failure in the trade total number as direct trust value, the model distinguish between transaction reputation and recommendation reputation definitely. Besides it introduced the credibility of the recommended node with offset factor to calculate, and had got the integrated trust value of target node by the directly trust of dynamic equilibrium node with the punishment factors and the risk factors, and recommended trust other nodes. Finally, it gare the simulation experiments. The experimental results show that the integrated trust value is more close to real value, and can resist threats such as slandered by malicious node, collaborative cheating and so on.

Key words: peer-to-peer network; transaction reputation; recommendation reputation; recommend; offset factor

0　引言

社会网络中，人际网络关系中核心的部分是信任关系。实体之间的信任关系往往取决于实体本身对被信任者的直接经验或者是其他个体的推荐经验，这种相互交流、相互信赖的关系就组成了一个信任网络[1]。在信任网络中，任何个体的可信度都不是完全绝对的，但是可以作为其他个体决定与其是否交易的依据。

在开放式的 peer-to-peer 网络环境中，所有实体（节点）之间的关系都是对等的，可以通过直接交易或者信息互换共享网络中的资源，这与传统的网络是有很大区别的。因为 P2P 网络的开放性、动态性、异构性，使得网络中的实体可以自由加入或者离开，因此，网络中节点之间的关系时刻处于动态变化中。由于在网络中实体之间的信任关系是通过相互进行交易获取服务建立起来的，用户通常要与一些不熟悉或者不认识的节点进行交易，若没有可信第三方推荐或者是信任权威参与的情况下，可能导致实体之间的信任关系很难建立。因此，在 P2P 网络中建立一种信任机制来衡量节点的可信度是很有必要的。在传统的网络环境或者应用中，推荐信任关系的建立是依靠可信的第三方，如认证中心（CA），如果实体持有认证中心颁发的证书，那它就被认为是可信的。但是这种传统的认证经常会伴随着一些额外的开销和费用，而在 P2P 网络中不宜普遍应用，因为在 P2P 环境中追寻的是零开销[2]。所以，有必要建立一种新的分布式信任机制，可以使用户对 P2P 网络中的资源进行有效使用。

国内外的学者和相关研究人员对信任模型也作了一系列的研究，从主观信任到基于推荐的信任模型数不胜数[3~5]。对于推荐信任模型，Aberer 等人[6]最先提出了 P2P 环境下基于信誉的监督方法，他们对节点的评价进行简单综合。文献[7]建立了 TRAVOS 信任模型，他们对节点的评价是通过实体之间直接交互建立的信任关系，产生历史信誉，若实体间没有直接交易则采用第三方推荐的历史信誉指数计算实体的信任值。Kamvar 等人[8]提出了 EigenTrust 模型，通过计算节点的局部信任值来定义节点全局信任值的计算方法。EigenTrust 模型算法稍微有点复杂，对于交易信誉与推荐信誉没有明确区分开，并且使用全局信任值迭代的方法作为推荐可信度。文献[9]提出了一种基于推荐的信任机制，对信任度进行概率分析来评估节点的可靠性。Xiong 等人[10]提出的 PeerTrust 信任模型，虽然区分了节点的推荐信誉与交易信誉，但是在参考他人推荐来判断对方信誉时，并没有考虑节点自身的信任度。

现阶段 P2P 网络中的信任模型仍存在一些问题和风险，

收稿日期：2012-03-26；**修回日期**：2012-05-08　　**基金项目**：广西可信软件重点实验室开放基金项目(200910595R06)

作者简介：雷月菊(1986-)，女，陕西渭南人，硕士研究生，主要研究方向为信息安全、可信计算；陈光喜(1971-)，男，四川金堂人，教授，博士，主要研究方向为信息安全与计算机代数(chgx@guet.edu.cn)。

本文针对上述问题在该网络环境下提出了一种基于推荐的信任模型,根据节点本身的交易信息得到的直接信任值并结合其他节点对其反馈信息信任值计算出目标节点的综合信任值,使得计算出的信任度更接近真实的信任值。

1　信任模型

定义 1　综合信任值。如果节点 i 通过与节点 j 在某一固定时间段$[t_{start},t_{end}]$内有过多次交易记录,那么节点 i 可以根据自身与 j 的历史交易经验,然后结合其他节点关于 j 的推荐反馈信息,计算出节点 j 的整体信任度。

1.1　EigenTrust 模型

在 EigenTrust[11] 信任模型中给出了节点计算局部信任度和全局信任度的方法:

a)节点 i 通过与节点 j 之间直接进行交易,对节点 j 产生了一个局部信任度,即定义为

$$D_{ij}=S_{ij}/N_{ij} \tag{1}$$

其中:N_{ij}表示在某个固定时间段$[t_{start},t_{end}]$内节点 i 与 j 的交易总次数;S_{ij}表示在节点 i 看来交易成功的次数;F_{ij}表示在节点 i 看来交易失败的次数。因为节点 i 与 j 对交易的成功与否看法不同,i 认为成功的交易记录在 j 看来并一定是成功的,所以这里取的是信任者对交易的态度值。假若 $N_{ij}=0$,则令$D_{ij}=0$。

b)任意节点 x 对 j 的交易反馈信息设为 $R_{x\to j}$,作为推荐的信任值反馈给其他节点,令

$$R_{x\to j}=(S_{xj}-F_{xj})/(\sum_k S_{kj}) \tag{2}$$

如果$(\sum_k S_{kj})=0$ 或者 $S_{xj}-F_{xj}<0$,则 $R_{x\to j}=0$。

c)在 EigenRep 模型中利用节点自身的全局信任值经过迭代作为它的推荐信任度[11,12],即

$$T_j=\sum_x (R_{x\to j}T_x) \tag{3}$$

在这个模型中,计算节点的信任值时主要存在两个问题:a)没有考虑到交易的风险性,所以计算的全局信任度可能与实际情况有偏离;b)直接用节点的全局信任值 T_j 迭代作为它的推荐信任度,没有考虑到可能会发生协同作弊、诋毁事件,如一些交易信任度高的节点对其他节点进行夸大事实、恶意诋毁或者提供虚假信息等。

本文针对这两个问题作了改进,重新定义了全局信任值的计算。

1.2　直接信任度计算

定义 2　由于节点之间的局部信任值的计算是根据自身直接交易经验而得到的对其他节点可信性程度的量化表示,因此令局部信任值为节点本身的直接信任度。以节点 i 为例,直接信任度计算为

$$D_{ij}=\alpha S_{ij}/N_{ij}+\beta P(x) \tag{4}$$

其中:α、β 都是权重因子,$0\leqslant\alpha,\beta\leqslant 1$,它们的取值决定于这次交易的重要性(如交易额大小、历史信誉度等),是随着交易而动态变化的;$P(x)$为交易的惩罚因子,令

$$P(x)=\begin{cases}0 & \text{正常交易}\\ -1 & \text{欺诈等恶意行为}\end{cases} \tag{5}$$

直接信任度是交易双方根据自身的直接经验得到的,当直接信任度 D_{ij}和 N_{ij}均大于设定的阈值时,系统可认定该节点是可信的,不用计算推荐信任度便可进行直接交易。

1.3　推荐信任度的计算

推荐信任度是当前节点没有直接交易,或者是交易次数过低或者是直接信任度没有达到系统设定的阈值时所用的一种方法。

定义 3　推荐节点自身的可信度称为节点的准确性因子 $A(x)$,则节点 j 的推荐信任度计算式为

$$R_j=\sum_x R_{x\to j}\times A(x) \tag{6}$$

其中:$R_{x\to j}$为节点 x 向节点 i 反馈的关于节点 j 的推荐信息,其计算参见式(2);$R_{x\to j}$为所有与节点 j 有过交易记录的节点推荐信息的集合;$A(x)$为推荐节点的准确性因子,其计算式引入节点的偏移因子 d_x。

定义 4　在某个固定时间段$[t_{start},t_{end}]$内节点 x 向节点 i 的反馈信息中,偏移因子 d_x 计算式为

$$d_x=[\sum_{n\in IS(i)\cap IS(x)}|S_{iu}/N_{iu}-S_{xu}/N_{xu}|]/[IS_{iu}\cap IS_{xu}] \tag{7}$$

其中:IS_{iu}表示为所有与 i 交易过的节点集合;IS_{xu}表示为所有与 x 交易过的节点集合;$IS_{iu}\cap IS_{xu}$表示为与节点 i 和 x 的共同节点进行交易的节点集合,根据节点 i 自身的评价与节点 x 提交的反馈评价作一比较,计算得到偏移因子 d_x($0\leqslant d_x\leqslant 1$)。如果 $IS_{iu}\cap IS_{xu}=0$,则意味着节点 x 与推荐节点 i 没有共同的交易节点,设初始值 $d_x=0.5$。

定义 5　如果偏移因子 d_x 已经得到,那么反馈节点 x 的准确性因子计算式为

$$A(x)=1-d_x^{1/s} \tag{8}$$

其中:$A(x)\leqslant 1$,$s=1,2,3,\cdots$。

这样推荐节点的推荐信任度就可以计算出来,得到的反馈信息才更真实,同时又可以防止一些潜在的恶意节点的合谋攻击和诋毁。但是若是推荐节点的准确性因子很低的话,那么它的信任度也会大打折扣。由式(8)的计算中可以得到,这样计算出来的准确性因子的值随着 d_x 的增大而减小,若是准确性因子的值很小,那么推荐节点自身的可信度就待考量。因此,设定边界值,若是 $A(x)\leqslant 1$ 的话,那么该推荐节点的推荐信任度可以忽略不计,则认为节点提供的信息不作为这次交易的参考内容。

1.4　风险值的计算

在网络交易中,实体(节点)之间进行交易都是在虚拟环境中进行的,每一次的信息交互都会伴随有一定的风险性。若忽略风险的作用,则节点容易受到攻击者的攻击,如一些诈欺行为或者是提供不可靠的服务等。因此定义风险值的计算为

$$R(x)=\xi D_{ij}+(1-\xi)\sum_x R_{x\to j}\times A(x) \tag{9}$$

其中:ξ 为设定的权重因子,取值应为一个较小的值。因为 P2P 网络中节点的动态性、异构性等特性的影响,对于找寻可信的第三方是有一定困难的。所以,相信第三方推荐信任信息的风险要比根据历史自身交易的风险大很多,设定的权重因子为一个比较小的值。

1.5　综合信任值的计算

定义 6　节点 i 在根据自身的历史交易经验结合向其他节点对节点 j 的反馈信息后,对节点 j 的综合信任度计算可表示为

$$G_j=\mu D_{ij}+(1-\mu)R_j-R(x) \tag{10}$$

其中:D_{ij}为节点 i 自己与节点 j 交易历史而累计的直接信任度;

R_j 表示由网络中其他节点对节点 j 的反馈信息而得到的推荐信任度，$R_j \leqslant 1$；μ 表示为节点 i 根据自身交易经验而设定的权重因子，在这里分为三种情况进行讨论。

a）若 $\mu = 0$，表示节点本身没有任何主见，仅仅依赖于其他节点的推荐反馈而与交易节点进行信息互动。

b）若 $\mu = 1$，表示节点自身只相信自己与交易节点以往的历史经验，对推荐信任度持有怀疑态度，不肯也不愿去相信反馈节点的推荐信息。

c）若 $0 < \mu < 1$，当节点 i 第一次与节点 j 进行交易时，由于直接信任度是由历史交易经验决定的，所以信任值是有限的，它更依赖于其他节点的推荐信任度，所以权重因子 μ 的比重会比较大；但是随着交易次数的不断累积，节点更愿意相信根据自身的交易经验来衡量节点的信任度，其他节点的推荐信息作为参考，因此权重因子 μ 的比重会随之下降，随着交易次数的增加而逐步加大。因此，权重因子是处于动态变化的过程中，即

$$\mu = 1 - \sigma^{k/n} \tag{11}$$

其中：σ 的取值是 $0.5 < \sigma < 1$；k 为节点 i 与 j 在某固定时间段 $[t_{start}, t_{end}]$ 内的第 k 次交易；n 为交易的总次数，取值是 $n \in \{1, 2, 3\cdots\}$。由式(11)看出，随着交易次数的增加，k 越大，μ 的值也会越大。这样得到的权重因子更符合实际交易中的情况和模式。

因此，可以得到关于节点 j 的综合信任度的计算式为

$$G_j = \mu D_{ij} + (1 - \mu) \sum_x R_{x \to j} \times A(x) - R(x) \tag{12}$$

最后根据得到的综合信任值与系统设定的阈值 G_{j0} 作比较。若是 $G_j > G_{j0}$，则表示节点是可信的，可以进行交易；若是 $G_j < G_{j0}$，则意味着节点的信任度有待商酌，这次交易暂不进行，为下次交易留作参考。

2 仿真实验与分析

2.1 仿真实验

通过仿真实验来检测该信任模型。为了更清晰地分析实验结果，将 EigenTrust、PeerTrust 模型与本文的信任模型放在同一个实验环境中进行比较。本文使用的场景以文件下载共享应用为例，用户的最终目标是下载所需文件，判断本次交易成功与否的唯一标准就是——下载文件的真实性。

实验环境设置为：模拟网络中的节点数是 100 个，文件总数是 1 000。将 1 000 份文件随机分配到 100 个节点中，保证每个节点至少拥有一份文件。每次交易时节点会从从不拥有的文件中任意选取其中一个进行下载。若下载成功，则节点拥有该文件，交易成功；若下载失败，则节点的文件拥有数不会增加，意味着交易失败。假设在模拟网络中诚实节点的数目多于恶意节点的数目，并且一次交易请求是由诚实节点发起的。实验结果如图 1 和 2 所示。

2.2 实验分析

图 1 所示为交易次数对目标节点综合信任值的影响。由于 EigenTrust 模型对推荐节点本身的准确性未加考虑，所以前 500 次的交易信任度没有很高，只是随着交易次数的增加使得直接信任度比重增大，从而增加信任度。PeerTrust 模型则完全依赖其他节点的推荐评价来判断目标节点的信任度，没有参考个人交互历史经验，开始交易时由于依赖推荐信任，比重较大，信任值较高；之后随着交易次数的累积，直接信任度的主要作用导致综合信任值涨幅不是很大。本文模型通过节点自身的交易记录作参考，并结合其他节点的推荐信息，引入偏移因子和随机数，可以忽略推荐信任度较低的节点推荐，这样计算出的节点信任值更能接近其真实值。实验验证了该模型的准确性和有效性。

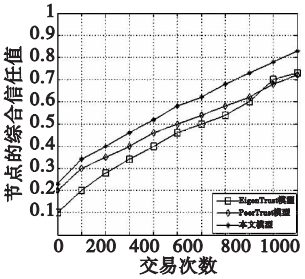

图1 交易次数对信任度的影响

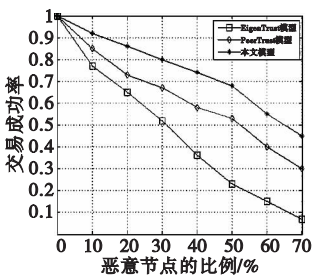

图2 不同恶意节点比例下的交易成功率

图 2 所示为不同恶意节点下交易成功率的情况。本文设置平均每个节点作 100 次交易后进行节点之间的互相评价，由诚实节点对其他节点进行信任度的评价。从结果中可以看出，随着恶意节点比例的逐渐增加，各个模型的交易成功率都有不同程度的下降。由于 EigenTrust 模型对恶意节点缺乏惩治措施，当恶意节点比例超过 40% 时，EigenTrust 模型计算错误率高，交易成功率随之下降迅速，若在恶意节点数目很多的环境下几乎难以运行；而无论恶意节点比例的大小，PeerTrust 和本文模型还能保持相对较高的交易成功率，证实该模型具有一定的安全性，在实际应用中更能发挥作用。

2.3 时效性和开销性分析

在 EigenTrust 模型中，由于缺乏对一些恶意节点的惩治机制，对协同作弊、提供虚假信息的合谋节点没有具体的惩罚措施，因此模型的时效性不是很明显，模型中在计算节点的全局可信值时要经过连续两次的迭代，其复杂度是 $O(n^2)$。在 PeerTrust 模型中，因为忽略了交易节点自身的历史经验，只是依赖于推荐节点的反馈信息，所以计算得到的综合信任值不是很合理，时效性不能真实地反映节点的信任程度，其计算的复杂度是 $O(n)$。在本文模型中，不仅增加惩罚机制对恶意节点的不实交易进行惩罚，同时注重交易双方的历史交互经验和推荐节点的反馈信息，随时都能更为准确真实地反映目标节点的综合信任值，因此时效性相对 EigenTrust、EigenTrust 模型来讲更为优越一些，并且计算的复杂度是 $O(n)$。

3 结束语

本文针对 EigenTrust 信任模型中存在的问题作了一些改进，提出了在 P2P 网络环境下基于推荐的信任模型。该模型通过惩罚因子来调节历史信任度作为以后进行交易的依据，使得直接信任值更接近其交易的真实值；在计算推荐信任度时，考虑了推荐节点本身的可信性，利用生成的随机数来判断节点的可信程度，可以有效防止恶意节点的协同作弊；最后计算目标节点的综合信任值时参考风险因子的影响，来决定这次交易是否可行。文中用仿真实验来验证推荐信任模型的可行性，得到较好的仿真结果，证明了该模型的有效性和 （下转第 4326 页）

特点,可对低频奇异值进行修改,也可应用到中高频中。

b)在大多数小波域的水印算法中,通常不会利用低频子带完成水印的嵌入,因为这样会造成水印系统的透明性下降。在本文的DWT-SVD算法中,尽管修改了低频子带的系数,但是水印化图像仍能维持较好的视觉效果,说明本算法较好地协调了不可感知性和鲁棒性。

c)本文还做了单独提取两个子带中的水印的实验。实验结果表明,嵌入在低频子带的水印在应对如高斯噪声、压缩等处理时具有较强的鲁棒性,而中频子带的水印则对旋转、剪切攻击具有很强的鲁棒性。

d)本算法对两种形式的水印均适用,尽管在灰度图像水印的鲁棒性上稍差于二值水印,但相比其他算法来讲,仍然有其可取之处。

表2 本文与文献[8]鲁棒性实验结果对比

攻击方式	*NC*	
	本文	文献[8]
未受攻击	1	1
0.05 椒盐噪声	0.959 75	0.945 63
0.08 椒盐噪声	0.923 68	–
0.01 高斯噪声	0.985 28	0.889 07
0.02 高斯噪声	0.960 5	–
中值滤波 5×5	0.886 5	0.992 14
平移 5×5	0.808 17	0.816 05
剪切	0.878 17	0.829 9
旋转 30°	0.501 26	0.481 42
JPEG90%	0.998 32	–
JPEG80%	0.995 65	0.982 45
JPEG50%	0.989 1	–
JPEG20%	0.975 82	–
亮度增强 50%	0.975 31	–

5 结束语

本文提出一种基于DWT-SVD域的自适应彩色图像水印算法。该算法先对原始图像进行三级离散小波变换;然后对得到的R、G、B三通道的各子带以及用Arnold置乱后的水印图像进行奇异值分解,利用人类视觉系统(HSV)特性自适应地调整水印嵌入强度,将水印的奇异值加入到原始图像子带的奇异值上。人类视觉系统模型的应用保证了水印的隐蔽性。仿真实验结果表明,本文提出的算法具有较强的鲁棒性,在经受了压缩、噪声、剪切等常见的信号处理后,仍能提取出较完整的水印。在今后的研究中,应该加强对盲水印算法的研究,使算法更具实用性。

参考文献:

[1] 林旭亮,孙燮华,万里红. 一种基于DWT和SVD图像水印的新算法[J]. 微计算机信息,2010,26(6):96-97.

[2] AL-HAJ A. Non-invertible copyright protection of digital images using DWT and SVD[J]. Proc of the 2nd International Conference on Digital Information Management. 2007:448-453.

[3] 徐慈蓉,樊锁海. 一种新的基于奇异值分解的图像数字水印算法[J]. 计算机仿真,2011,28(5):291-341.

[4] SANTHI V,Dr THANGAVELU A. DWT-SVD combined full band robust watermarking technique for color image in YUV color space[J]. International Journal of Computer Theory and Engineering,2009,1(4):424-429.

[5] 阮波. 一种基于DWT-SVD的数字水印算法研究[D]. 成都:西南交通大学,2008.

[6] BARNI M,BARTOLINI F,PIVA A. Improved wavelet-based watermarking through pixel-wise masking [J]. IEEE Trans on Image Processing,2001,10(5):783-791.

[7] 杨卫民,谭骏珊,金正. 基于奇异值分解的彩色图像水印算法[J]. 计算机工程与设计,2008,29(23):6152-6153.

[8] 徐国荣,王礼平. 基于奇异值与提升小波的彩色图像水印算法[J]. 计算机应用研究,2011,28(5):1981-1986.

(上接第4322页)实用性。但是,文中对节点信任值的计算在系统中的开销、时效性等没有深入研究,只是作了简单的一些分析和说明,对分布式环境下协同决策[13,14]、信任衰减[15]等问题研究不是很透彻,希望在今后的工作中作进一步改进。

参考文献:

[1] CARONNI G. Walking the Web of trust[C]//Proc of the 9th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. Washington DC: IEEE Computer Society, 2000:153-159.

[2] CHEN R,YEAGER W. Poblano:a distributed trust model for P2P networks TR-I4-02-08[R]. Palo Alto: Sun Microsystem,2002.

[3] YU Ding-guo, CHEN Nan, TAN Cheng-xiang. Research on trust cloud-based subjective trust management model under open network environment[J]. Information Technology,2011,10(4):759-768.

[4] LI Xiao-yong, ZHOU Feng, YANG Xu-dong. A multi-dimensional trust evaluation model for large-scale P2P computing[J]. Journal of Parallel and Distributed Computing,2011,71(6):837-847.

[5] 胡智,尹继元,鲁军. P2P网络中基于推荐与用户行为的信任模型研究[J]. Computer Knowledge and Technology,2011,12(7):2787-2788.

[6] ABERER K, DESPOTOVIC Z. Managing trust in a peer-to-peer information system [C]//Proc of the 10th International Conference on Information and Knowledge Management. New York: ACM Press, 2001:310-317.

[7] TEACY W T,JIGAR P,JENNINGS N R. TRAVOS: trust and reputation in the context of inaccurate information sources[J]. Autonomous Agents and Multi-agent Systems,2006, 12(2): 183-198.

[8] KAMVAR S D, SCHLOSSER M T. EigenRep: reputation management in P2P networks [C]//Proc of the 12th International World Wide Web Conference. New York: ACM Press,2003:123-134.

[9] 郭成,李明楚,姚红岩,等. P2P网络下基于推荐的信任模型[J]. 计算机工程,2008,34(24):157-159.

[10] XIONG Li,LIU Ling. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities [J]. IEEE Trans on Knowledge and Data Engineering,2004,16(7):843-857.

[11] 窦文. 信任敏感的P2P拓扑构造及其相关技术研究[D]. 长沙:国防科技大学,2003:53-70.

[12] 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.

[13] 朱友文,黄刘生,陈国良,等. 分布式计算环境下的动态可信度评估模型[J]. 计算机学报,2011,34(1):55-64.

[14] 彭涛,窦万峰,曲永花. 协同决策支持系统中的信任模型研究[J]. 计算机工程,2011,37(7):136-138.

[15] 李季,李刚. 一种基于信任衰减向量的P2P网络信誉模型[J]. 计算机工程与应用,2011,47(9):86-88.