维普资讯 http://www.cqvip.com

一种改进的基于向量的 P2P 电子商务信任模型

汪丽芳　王　茜
（重庆大学计算机学院　重庆 400044）

摘　要　在交易之前通过信任模型帮助交易对象之间建立信任关系，是 P2P 电子商务发展的必要条件，也是近年来的研究热点。本文针对现有模型的不足，在基于投票协议的 P2P 电子商务安全信任模型[1]的基础上，引入了向量表示信任，并且在权限的确定、信任的表述和信任的评估等多方面做了改进。经过模拟实验和分析证明，改进后的模型不仅可以让用户根据各自的不同要求对交易对象做出更合理的信任评估，而且能快速识别和隔离恶意节点，从而降低了交易风险。

关键词　向量，P2P，电子商务，信任模型

Improved Vector-based Trust Model for P2P E-Commerce

WANG Li-fang　WANG Qian
(Department of Computer and Science, Chongqing University, Chongqing 400044, China)

Abstract　It is necessary for the P2P e-commerce to build up trust between two sides of business before transactions by trust model, which has been a hotpot recently. To improve the existent models and on the basic of polling protocol-based trust model, this paper uses vector to express trust, and takes some amelioration on privilege, expression of trust and evaluating trust. The result of simulative experiment shows that in the improved trust model a peer can not only evaluate other peers rationally according his various needs, but also identify and insulate vicious peers more quickly, consequently the transaction risk is reduced.

Keywords　Vector, Peer-to-peer, E-commerce, Trust model

1　引言

P2P 网络给电子商务带来了巨大的发展，但它的动态性和匿名性等特点使得交易之前的信任问题尤为突出。为了减小交易风险，营造诚信的交易氛围，需要用信任模型帮助用户在交易之前排除恶意节点，建立信任关系。为此，国内外研究者提出了一系列信任模型，如 BBK 信任模型[2]、Wang Yao 等提出的基于贝叶斯网络的模型[3]、Josang 等提出的一种主观信任模型[4]等，但这些模型存在一些不足，例如节点有恶意推荐时模型没有合理的奖惩机制，而且信任表述和计算过于简单，不能真实反映目标节点的信任度。针对这些不足，文献[1]提出了一种基于投票逻辑的 P2P 电子商务信任模型（本文中称为 V_1 模型），该模型建立在完全分布式的 P2P 体系结构上，更符合电子商务的现实意义，在计算信任时考虑了多种影响因素和奖惩机制，加入了权限限制。通过模拟实验证明，该模型能更加准确地评价交易对方，有效地识别和隔离恶意节点，制约了小规模积累信任值大规模攻击情况。但该模型仍然存在不少问题需要改进，主要有以下几点：(1)对不反馈意见的懒惰节点没有惩罚措施；(2)节点投票只能有好坏即 0,1 之分，没有考虑“不确定”；(3)从信任记录和反馈意见中获取信息较少，信任的主观性和多样性及各个节点的个性要求的体现上有待改进。为了解决这些问题，继续完善模型，本文引入向量表述信任（包含多方面信任信息）用历史交易金额为尺度确定交易权限，改变了历史情况记录策略，改进了各种信任的评估方法。最后，通过分析和实验验证了改进后的模型（本文中称为 V_2 模型）的优势。

2　信任、信任关系和信任模型

信任是一个主观概念，是一个节点对另一个节点能力、诚信和可靠性的一种信心[2]，它取决于经验，用信任值来表示信任程度，信任值随节点的行为而动态变化。本文中的信任关系分为三类：直接信任、间接信任和推荐信任。直接信任是两个有过直接交易的节点，根据交易情况对交易对方的一种直接经验。间接信任是指两个节点之间没有直接交易经验或是经验较少，通过其它节点的推荐而建立起来的信任。推荐信任是指在根据其它节点提供的推荐获取间接信任值的时候，对提供推荐的节点反馈意见的信任度。信任模型也被称为信任度评估模型，对信任关系进行表述、度量和评估，提供信任值的计算或者根据服务请求提供合适的引用链。

3　基于向量的 P2P 电子商务信任模型

本文对 V_1 模型做了多方面改进，本小节将从权限确定、信任表述和评估几个方面介绍 V_2 模型。

本文中假设 q 节点向 p 节点提出交易请求，o 节点等其他节点作为推荐节点。每个节点维护一张交易记录表，记录有其他节点的直接信任记录、恶意欺骗总金额、交易成功总金额、交易总金额、推荐信任记录。如表 1 为 p 节点的交易记录表，记录了和 n_1，n_2 等其他节点的交易经验。

汪丽芳　硕士研究生，研究方向为电子商务安全；王　茜　副教授，研究方向为电子商务、远程教育。

维普资讯 http://www.cqvip.com

表1 交易记录表

直接信任	恶意欺骗总额	交易成功总额	交易总额	记录时间	推荐信任记录
Td_{pn1}	Fl_{n1}	Fs_{n1}	F_{n1}	t_{n1}	Tr_{n1}
Td_{pn2}	Fl_{n2}	Fs_{n2}	F_{n2}	t_{n2}	Tr_{n2}
…	…	…	…	…	…

交易记录表按照“推荐信任记录”的值大小进行降序排序，此项初始值为0.5，前四项如果没有直接交易经验，值可为空。

3.1 信任的表述

为了体现信任的主观性和多样性，V_2 模型将直接信任和间接信任用向量表示，向量各分量的含义分别为交易速度满意度、商品可靠度、恶意欺骗率满意度、交易成功率满意度。交易速度满意度是 p 节点根据交易情况主观对 q 节点做出的评价；商品可靠度可包含商品质量和商品数量达到商家承诺的可靠度，也是 p 节点根据交易情况做出的主观评价；恶意欺骗率满意度是对恶意欺骗的一个衡量项；交易成功率中考虑商家是否有恶意欺骗外的中途毁约等情况。模型用 Td_{pq} 表示节点 p 对节点 q 的直接信任，T_{pxq} 表示节点 p 对节点 q 的间接信任。表2为 p 对 q 直接信任的表述。

表2 p 对 q 直接信任的表述

速度满意度	商品可靠度	恶意欺骗率满意度	交易成功率满意度
$Td_{pq}[0]$	$Td_{pq}[1]$	$Td_{pq}[2]$	$Td_{pq}[3]$

其中，每一项的值 $Td_{pq}[i]\in[-1,1]$。

如果 o 节点收到 p 节点的推荐请求，需要向 p 反馈意见，模型用向量 Tin_o 表示 o 节点反馈的信息，如表3所示。

表3 反馈信息的表述

速度满意度	商品可靠度	欺骗率满意度	成功率满意度	交易成功净额	计算时间	有无交易
$Tin_o[0]$	$Tin_o[1]$	$Tin_o[2]$	$Tin_o[3]$	$Tin_o[4]$	$Tin_o[5]$	$Tin_o[6]$

反馈信息中的交易净额信息用以帮助 p 节点确定交易权限，反馈上次计算信任时间，以便 p 节点用时间因子折算信任值。“有无交易”标志 o 节点是否有 q 节点的直接信任记录。如果此项为0，表示 o 节点没有和 q 节点交易的记录；如果为1，表示有记录，则反馈信息包括了信任记录信息。

p 节点对 q 的间接信任 T_{pxq} 表述类似直接信任。推荐信任仍然用一个简单的变量来表示，例如 p 节点对 o 节点的推荐信任用 Tr_{po} 表示，$Tr_{po}\in[0,1]$。

3.2 权限的确定

V_2 模型不再划分权限等级，而以交易金额作为尺度，默认交易上限 F_{max} 值为交易成功净额 $F_{成功净额}$，这里定义交易成功净额为

$$F_{成功净额}=F_{总成功金额}-F_{总失败金额}$$

如果没有直接交易经验，节点通过计算推荐信息里包含的金额信息计算平均成功净额，计算公式如下：

$$F_{平均成功净额}=\frac{\sum_{x=1}^{n}(Tin_x[4]\times Tr_{px})}{n} \tag{1}$$

根据表3可知，$Tin_x[4]$ 为节点 x 反馈信息中的成功净额信息，Tr_{px} 为 p 节点对节点 x 的推荐信任值，n 为“有无交易”不为0的反馈信息的个数。在默认情况下，交易金额上限为平均成功净额，即 $F_{max}=F_{平均成功净额}$

模型允许 p 节点自行更改交易金额上限 F_{max}。

3.3 信任的评估

3.3.1 直接信任的评估

如果节点 p 与节点 q 之间有直接交易的经验，则 p 的交易记录表里有直接信任 Td_{pq} 记录。为了便于和阈值比较，p 节点需要计算综合信任值，计算公式如下：

$$Td_{pq综合}=Y\times\sum_{i=0}^{3}(W_i\times Td_{pq}[i]) \tag{2}$$

其中，W_i 为各信任分量权重，体现本次交易对信任各个方面的不同重视程度。开始可设定默认值，之后可以更改，$W_i\in[0,1]$，$W_0+W_1+W_2+W_3=1$。加入时间衰退因子 Y，符合现实中的思想。随着时间推移，以前的行为对以后的交易影响越来越弱，Y 计算公式如下：

$$Y=\frac{1}{t_{当前时间}-t_{上次计算时间}+1} \tag{3}$$

计算出综合信任值后，节点 p 将其与设置好的阈值进行比较。节点在交易之前可进行阈值设置，此处有 Z_1 和 Z_2 两个阈值。当 $Td_{pq综合}\leqslant Z_1$ 时，q 节点完全不可信，p 节点决定不和 q 节点进行交易。如果 $Td_{pq综合}\geqslant Z_2$，p 节点认为 q 节点完全可信，且 q 请求交易金额 R 是在默认权限范围内，允许交易；如果 R 不在默认权限范围内，但 p 节点愿意冒险，则可以更改本次权限值进行交易，否则 p 节点拒绝与 q 进行交易。如果进行交易，交易结束(包括成功与不成功)后，p 先对交易记录表的其他项进行更新，再计算并更新直接信任值。直接信任的更新计算公式如下：

$$Td_{pq}[i]=\begin{cases}\lambda(\alpha\times Td_{pq}[i]+\beta\times td_{pq}[i])+\mu\dfrac{-1}{1+e^{-m}}, & \text{此次有欺诈}\\ \alpha\times Td_{pq}[i]+\beta\times td_{pq}[i], & \text{此次无欺诈}\end{cases} \tag{4}$$

其中，$\alpha+\beta=1$，$\lambda+\mu=1$。$\dfrac{1}{1+e^{-m}}$ 为恶意欺骗的惩罚项，随着欺骗次数 m 的增大，惩罚程度呈指数增长。$td_{pq}[i]$ 为对 q 本次交易表现的评价，$i=3$ 时 $td_{pq}[i]=-1+\dfrac{Fs_q}{F_q}\times 2$；当 $i=2$ 时，$td_{pq}[i]=1-\dfrac{Fl_q}{F_q}\times 2$。权重 α,β 由 p 根据需要设置；当 $i=1$ 或0时，$td_{pq}[i]$ 由 p 节点主观评估，权重 α,β 由本次交易的重要程度、距离上次记录时间等多种因素共同决定，模型默认计算，也允许节点更改。模型默认计算权重情况下，$\alpha=\dfrac{F_q-R}{F_q}\times Y$，其中 Y 为时间因子，$\beta=1-\alpha$。λ 和 μ 是影响惩罚程度的权重，由节点设置，μ 大则惩罚重。

3.3.2 间接信任的评估

虽然 p 节点有和 q 直接交易的经验，但信任程度不够确定。如 $Z_1<Td_{pq综合}<Z_2$ 时，p 需向其他节点请求推荐，通过综合计算其他节点给其反馈的信任信息来决定是否和 q 进行交易。另外，p 节点没有和 q 直接交易的经验时，也需要向其他节点请求推荐，具体工作流程如下：

(1) p 节点查询交易记录表，如果没有与 q 节点的直接交易记录，或者有与 q 节点的直接交易经验，但 $Z_1<Td_{pq综合}<Z_2$，转(2)。

(2) p 节点向排在列表前面的推荐信任值高的节点发送请求，要求回馈 q 节点的信任信息。

(3)其他节点收到请求信息后，查看交易记录表。如果有与 q 的直接交易记录，则向 p 节点反馈记录中的信任信息；如

维普资讯 http://www.cqvip.com

果没有交易记录，则置推荐信息中的“有无交易”项为0，表示不了解 q 节点。

(4) p 节点接收到各节点的反馈信息后，查看反馈信息的“有无交易”项。如果为0，说明此节点没有和 q 节点交易的经验，则丢弃此信息；如果为1，则将反馈信息保存到临时变量。如果 q 节点也反馈了信息，则 p 节点忽略 q 节点自身的反馈信息。设“有无交易”为1的反馈信息数为 n，p 节点计算 q 节点间接信任 T_{pxq} 的公式如下：

$$T_{pxq}[i]=\frac{\sum_{x=1}^{n}(Tin_x[i]\times Y_x\times Tr_{px})}{\sum_{x=1}^{n}Tr_{px}} \tag{5}$$

然后计算权限和综合间接信任值，综合间接信任值计算类似公式(2)：

$$T_{pxq综合}=\sum_{i=0}^{3}(W_i\times T_{pxq}[i])$$

将所得权限和综合间接信任值保存到临时变量。

(5)节点 p 根据计算出来的综合推荐信任值和权限来决定是否和 q 节点进行交易。一般情况下，节点对推荐信任的阈值要求比直接信任的要求高。根据交易的重要程度设定阈值 Z_3。当 $T_{pxq综合}\geqslant Z_3$ 且交易金额 $R\leqslant F_{max}$ 时，p 节点同意交易。否则，p 节点拒绝与 q 进行交易。

(6)交易结束后，p 节点更新与 q 节点交易的记录。直接信任值的更新公式如下：

$$Td_{pq}[i]=\begin{cases}\lambda(\rho\times T_{pxq}[i]+\delta\times td_{pq}[i])+\mu\times\dfrac{-1}{1+e^{-1}}, & \text{此次有欺诈}\\ \rho\times T_{pxq}[i]+\delta\times td_{pq}[i], & \text{此次无欺诈}\end{cases} \tag{6}$$

其中，$\rho+\delta=1$，$\lambda+\mu=1$，权值 ρ，δ，λ 和 μ 的大小由 p 节点自己根据需要设置，$td_{pq}[i]$ 的设置或计算如同公式(4)中所述。

如果所有反馈信息的“有无交易”都标为0，即 q 为新节点，则 p 节点赋予 q 初始信任值和最低交易金额权限。如果符合要求，则进行交易，交易之后更新交易记录表。此时直接信任值的更新公式为：

$$Td_{pq}[i]=\begin{cases}\lambda\times td_{pq}[i]+\mu\times\dfrac{-1}{1+e^{-1}} & \lambda+\mu=1,\text{此次有欺诈}\\ td_{pq}[i], & \text{此次无欺诈}\end{cases} \tag{7}$$

3.3.3 推荐信任的评估

在经过推荐而进行的交易结束时，p 节点需要对推荐节点的推荐进行评价，计算并且更新推荐信任值，交易记录表重新排序。p 节点对 o 的推荐信任值更新公式为

$$Tr_{po}=\phi\times Tr_{po}+\varphi\times tr_{po}\varphi+\phi=1 \tag{8}$$

其中，ϕ 和 φ 为权重，$\phi+\varphi=1$，权值由节点 p 自主设置。本次推荐信任 tr_{po} 是 p 节点对 o 本次推荐的评价，$tr_{po}\in[0,1]$，计算公式为

$$tr_{po}=1-\frac{\sum_{i=0}^{3}|Tin_o[i]-Td_{pq}[i]|}{8} \tag{9}$$

为了激励节点积极并且准确地推荐，在更新推荐信任值后，对相应节点的直接信任值也进行更新，更新公式如下：

$$Td_{po}[i]=\eta\times Td_{po}[i]+\gamma\times(-1+Tr_{po}\times 2) \tag{10}$$

其中，η 和 γ 为权重，$\eta+\gamma=1$，权值大小由 p 节点自主设置。

对于没有反馈意见的懒惰节点，本次推荐信任 tr_{po} 为0，反馈信息中“有无交易”为0的节点不更新其推荐信任值。

4 改进性能分析及模拟实验结果

V_2 模型对 V_1 模型做了多方面的改进，在 matlab 7.0.1 环境下验证了改进性能，并且将改进前后的模型进行了分析比较。

(1)更好地遏制共谋攻击和恶意推荐。在 V_2 模型中，节点的推荐信任值保存在交易记录表中，并且按照推荐信任值的大小降序排列。需要推荐时，p 节点选择排在前面的节点，向这些推荐信任值高的节点发送请求。沿用 V_1 模型思想，p 节点直接向各节点发送请求，各节点直接将信息反馈回来。但 V_2 模型并不广播请求，而只是有选择性地向自己信任的节点发送，不但减小了恶意推荐和共谋攻击的风险，而且减轻了网络负担。在模拟实验中，设有100个节点，其中有40个节点共同哄抬目标节点信任值。所有节点以前20次推荐均诚实，即实验开始时推荐信任值均为1。假设无恶意推荐时得到的目标节点的实际间接信任各项值均为0.1，图1为有恶意节点时 V_1 模型和 V_2 模型得到的间接信任值的比较。从图中可以看出，V_2 模型恶意节点的影响更小，间接信任值更快趋近于实际值。

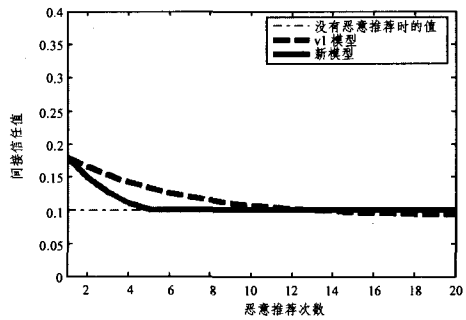

图1 间接信任值与恶意推荐次数关系

(2)有效防止小规模积累信任值和权限后进行大规模欺骗的攻击。V_1 模型对这个问题做了探讨，采取了权限的措施进行控制。但在该模型中，权限的升级是通过交易次数来决定，即使是小额交易，仍然可以增加交易成功次数，以促进权限的升高，恶意节点仍然可以进行大规模欺骗。例如，每次 q 和 p 交易，交易额为10元，而且每次表现都很好，10次后 j 的交易权限就相应升高，可以进行大规模交易，交易金额上限为1000元，这次 j 就进行了一次交易金额为1000的恶意欺骗，这样 p 节点和 q 的交易总体损失了900元。V_2 模型以成功净额为标准确定权限，交易金额不大于交易成功净额，q 节点即使进行了大规模欺诈，也得不偿失。因此 V_2 模型在很大程度上遏制了小规模积累信任值和权限后进行大规模欺骗的行为。当然，模型并不排除节点的冒险性心理，允许节点更改交易金额上限。模型不再设定下限，因为高权限的节点有权利进行小金额的交易。在模拟实验中，设 V_1 模型中每升级一个权限等级，需要10次成功交易，权限表为：

交易权限	下限值	上限值
1	0	100
2	11	1000
3	1001	10000
…	…	…

图2显示了改进前后 p 节点与 q 交易的最大损失可能，

维普资讯 http://www.cqvip.com

V_2 模型的最大损失不超过 0，相对 V_1 模型有了很大改进。

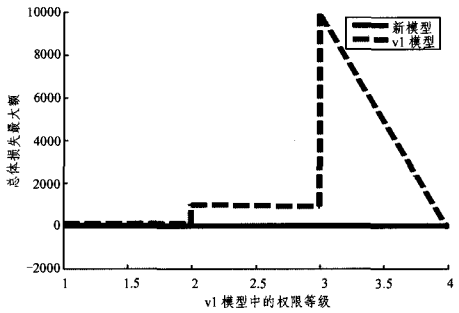

图 2　p 与 q 交易总体损失额最大值

(3)激励机制更完善。以前的模型中对收到请求没有反馈意见的节点基本没有惩罚措施，不能刺激这些节点积极推荐。在 V_2 模型中，p 节点按交易记录表选择节点发送请求并记录这些节点。如果有节点没有反馈意见，则将它此次推荐信任置为 0，加入推荐信任因子，更新直接信任值，以降低直接信任值。模拟实验中，开始 o 节点的推荐信任和直接信任值都为 1，公式(8)中 ϕ 设为 0.7，公式(10)中的 η 和 γ 分别设为 0.6 和 0.4，p 节点向 o 节点发送了请求，20 次 o 都没有反馈意见。没有反馈意见的次数和直接信任的关系如图 3。V_1 模型中直接信任值不受影响，而 V_2 模型中直接信任值随着未反馈意见次数的增加而减小。

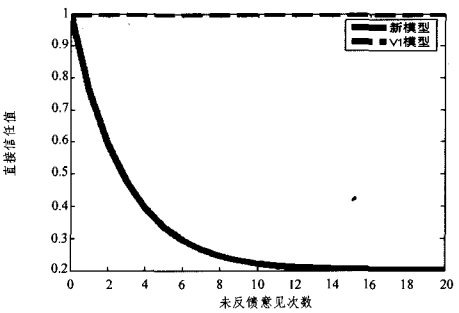

图 3　直接信任和未反馈意见次数的关系

(4)用向量表示信任，更能体现信任主观性。在 V_1 及其他模型中，信任都只用一个数字来度量，节点则根据这个数据来判断自己是否同意交易。虽然有少数模型在计算这个数值时考虑了几种因素，但结果和记录仍然只是一个数值。然而，实际电子商务中的信任并不这么简单，它包括了商品质量、处理速度等多种复杂因素，各个节点的要求不一样。即使是相同的节点，在不同的交易中，要求也不尽相同。例如上次交易只注重商品质量，这次则可能只关心交易对象是否会进行欺诈，但无法从信任值中获取详细的欺诈信息。V_2 模型采用向量表示信任，包含多方面信任，各节点可从信任记录中提取更多信息。如果本次只关心恶意欺骗方面的信任，则可从记录中查看“欺骗率满意度”，在计算综合直接信任值时，增大此项的权重，减小其他项权重。

(5)考虑了推荐不确定情况。在 V_1 模型中，其他节点的投票只有 0，1 之分，没有考虑“不确定”的情况，而且它们通过各自阈值确定 0 或 1，有同样的信任值可能会投出相反的票。在 V_2 模型中，节点直接反馈信任值，让请求节点统一评估，不会因为各节点阈值影响推荐值；如果不了解目标节点，可置“有无交易”为 0，不仅标识了“不确定”的情况，而且有利于识别新节点，即所有推荐信息里的“有无交易”都为 0 的情况。另外，请求节点能从反馈信息中获取足够详细的信息以供参考。

(6)V_2 模型在计算信任的时候多处用到交易金额作为尺度进行度量，例如用成功净额来确定权限，用金额大小来确定权重等，体现电子商务注重经济效益的特点。

(7)在 V_1 及其他一些模型中，为了更准确地评估信任，需要大量存储历史交易记录，占据了大量空间，而且难以维护。V_2 模型只存储上次交易后的更新信任值，标注上次计算信任的时间，节省了大量的空间，易于管理，方便计算。

结束语　本文对文献[1]中提出的模型在权限的确定、信任表述和信任评估等多方面做了改进，在 matlab7.0.1 环境下进行的模拟实验显示，改进后的模型体现了电子商务经济效益的特点和不同交易的个性化要求，解决了“懒惰节点”不反馈信息的问题，更有效地激励其他节点积极准确地推荐。在此模型中，交易双方能更加准确地评价对方，更快识别和排除恶意节点，有效防止恶意推荐以及小规模积累权限和信任值后进行大规模欺骗等攻击，从而在很大程度上降低了电子商务的交易风险。

参 考 文 献

[1] 王茜，杜瑾珺. 一种 P2P 电子商务安全信任模型. 计算机科学，2006：54-57

[2] Beth T，Borcherding M，KleinB. Valuation of trust in open networks. ESORICS 94，Brighton，UK，November 1994

[3] Wang Y，Vassileva J. Bayesian Network-based Trust Model[C]// Proceedings of the IEEE/WIC International Conference on WebIntelligence(WI'03). 2003

[4] Josang A. A Subjective Metric of Authentication// Quisquater J，ed. Proceedings of the ESORICS'98. Louvain- la-Neuve. Springer Verlag，1998：329-334