第35卷 第10期 计 算 机 工 程 2009年5月
Vol.35 No.10 Computer Engineering May 2009
·安全技术· 文章编号：1000—3428(2009)10—0129—03 文献标识码：A 中图分类号：TP393.08

电子商务系统的信任建模与评估

王 亮[1]，郭亚军[1,2]
(1. 华中师范大学计算机科学系，武汉 430079；2. 武汉生物工程学院计算机科学系，武汉 430415)

摘 要：针对P2P电子商务系统的安全问题，提出一种基于声誉的信任模型。通过引入影响信任度的信任因素改进局部声誉与全局声誉的计算方法，准确地反映出节点的信任度，降低信任度计算的时间复杂度。实验结果表明，该模型相比现有的信任模型，能提高系统交易成功率，并有效用于P2P电子商务系统中。

关键词：P2P系统；电子商务；信任模型；声誉

Trust Modeling and Evaluation in E-commerce System

WANG Liang[1], GUO Ya-jun[1,2]
(1. Department of Computer Science, Huazhong Normal University, Wuhan 430079;
2. Department of Computer Science, Wuhan Bioengineering Institute, Wuhan 430415)

【Abstract】 For the problem of security in P2P e-commerce system, this paper provides a novel reputation-based trust model. By introducing many comprehensive trust factors in computing trust level and improving the calculation methods of the local reputation and global reputation, this model can not only accurately reflect the node's trust level, but also reduce the time complexity in computing trust level. Experimental results show that the trust model can improve the rate of successful transaction compared to the existing trust models, and can be effectively applied to the P2P e-commerce system.

【Key words】 P2P system; e-commerce; trust model; reputation

1 概述

在P2P系统中，节点既是消费者也是服务者，它能匿名地进行直接交互，并随时加入和离开系统。在P2P电子商务系统中，由于用户常与陌生的用户进行交易，很有可能遇到恶意用户，从而蒙受巨大的损失，因此如何在P2P电子商务系统中提供一个有效的信任机制(模型)，帮助在用户之间建立起信任，让买卖双方互相知晓，并且评估他们在参加交易中的风险，以便能安全地进行交易，是目前P2P电子商务技术研究的一个热点。

信任模型为P2P电子商务系统安全问题的解决提供了方案。信任模型是一个用于建立和管理信任关系的框架，其主要功能是对实体之间的信任关系进行评估，提供信任值的计算或根据服务请求提供合适的引用链。文献[1]提出在P2P环境下基于全局声誉的信任模型EigenRep。EigenRep通过邻居节点间的满意度的迭代来获取节点的可信度。在无恶意节点的网络中，该模型可较好地反映出节点的真实行为，但该模型存在收敛性的问题，且具有较高的计算和通信代价。文献[2]提出基于模糊逻辑推理规则来计算节点的全局声誉的FuzzyTrust信任模型。该模型具有较高的恶意节点检测率，但计算代价和通信代价比较高，而且该模型未考虑影响信任评价的各种信任因素，也未对模型的收敛性进行论证。文献[3]提出一种基于局部声誉的信任模型HBDTM，但该模型未给出交易时间影响因子的确定方法且模型本身抗攻击能力较差。文献[4]使用DS证据理论来表达信任(声誉)值，模型中假定了2个可能的结果，若信任为$m(T_A)$，不信任为$m(\neg T_A)$，则信任值为$\Gamma(A)=m(T_A)-m(\neg T_A)$，$\{m(T_A),\ m(\neg T_A)\}\in[0,\ 1]$，$\Gamma(A)\in[-1,\ 1]$。根据其行为历史记录进行信任评估以及预定义的可信和不可信行为的门限值，使用Dempster规则即可计算出$m(T_A)$和$m(\neg T_A)$，进而得出信任值，但该模型抗攻击能力较差。

目前的信任模型存在如下问题：(1)信任度计算的时间复杂度比较高。(2)抗攻击能力有待提高。本文基于上述问题提出一种新的在P2P电子商务系统中基于声誉的信任模型。

2 基于声誉的信任模型

2.1 局部声誉

局部声誉(直接信任度)是节点i对节点j历史行为的观察或评价信息而得出的对节点j未来行为的期望。信任是缓慢增加的，一旦交易失败，信任就会迅速减少，这种机制根源于人类社会，人们之间的信任是通过长期积累而形成的，即信任是动态的、累积的。为体现信任动态性和累积性的特点以及更准确和客观地反映局部声誉，在局部声誉的计算中，本文引入以下4个重要参数：

(1)交易金额：交易金额的大小直接反映了此次交易的重要程度，交易金额越大，则对局部声誉的影响越大，这样可防止一些恶意节点通过小金额的成功交易来抬升局部声誉，然后在大金额交易时进行欺骗。

(2)交易次数：买卖双方交易的次数越多，则双方越熟悉，就越容易在双方之间建立起信任。

基金项目：中国博士后基金资助项目(20070410953)；湖北省教育厅科技基金资助项目(B20084002)；武汉市教育局科研基金资助项目(200765)

作者简介：王 亮(1982－)，男，硕士研究生，主研方向：信息安全，可信网络；郭亚军，副教授、博士后

收稿日期：2008-09-09 **E-mail：**wangliang@mails.ccnu.edu.cn

(3)交易满意度：是一个人为主观参数，即在一次交易完成之后，买卖双方各自给出对此次交易的满意程度。

(4)交易时间：距离当前时刻越近的交易越能比较真实地反映出节点的近期行为，从而对声誉影响就越大；反之，交易时间距离当前时刻越远，对声誉的影响就越小[5]。

节点 i 在当前时刻 t 时对节点 j 的直接信任度(节点 j 相对于节点 i 的局部声誉)$D(i, j, t)$的计算公式为

$$D(i,j,t)=\sum_{k=1}^{B(k)}\frac{S_k(i,j,t_k)M_k(i,j,t_k)\varphi(t_k)}{\sum_{k=1}^{B(k)}M_k(i,j,t_k)\varphi(t_k)}+\sum_{k=1}^{B(k)}(f(k)-1)\mathrm{e}^{-\frac{1}{n+1}}+\sum_{k=1}^{B(k)}f(k)\varphi(t_k)\mathrm{e}^{-\frac{1}{MP_k(i,j,t_k)}}$$

$B(k)$：节点 i 与节点 j 在时间段 t 内的交易总次数。

$S_k(i,j,t_k)$：节点 i 在时刻 t_k 时对节点 j 的第 k 次交易的交易满意度，其取值区间为[-1, 1]。

$M_k(i,j,t_k)$：节点 i, j 在时刻 t_k 时第 k 次交易的金额。

$MP_k(i,j,t_k)$：节点 i, j 在时刻 t_k 时第 k 次交易的金额所占的比重

$$MP_k(i,j,t_k)=\frac{\text{第}k\text{次交易金额}}{\text{总交易金额}}=\frac{M_k(i,j,t_k)}{\sum_{k=1}^{B(k)}M_k(i,j,t_k)}$$

其中，$\varphi(t_k)$ 表示时间衰减函数；$\varphi(t_k)=\mathrm{e}^{-\lambda(t-t_k)}$，$\lambda>0,\ \lambda\in R$，$\lambda$ 为衰减系数，其值可根据用户所需的具体策略而制定。

$(f(k)-1)\mathrm{e}^{-\frac{1}{n+1}}$：交易失败后的惩罚项

$f(k)=\begin{cases}0 & \text{第}k\text{次交易失败}\\ 1 & \text{第}k\text{次交易成功}\end{cases}$，$\mathrm{e}^{-\frac{1}{n+1}}$ 为惩罚因子，n 是失败的次数，它随着 n 的增大而增大。

$f(k)\varphi(t_k)\mathrm{e}^{-\frac{1}{MPk(i,j,t_k)}}$：交易成功后的奖励项，其中，$\varphi(t_k)\mathrm{e}^{-\frac{1}{MP_k(i,j,t_k)}}$ 是奖励因子，交易金额所占的比重越大且交易时刻距离当前交易时刻越近，奖励因子就越大，这样就会提高节点进行成功交易的积极性。

为防止恶意节点通过振荡的交易来抬升自己的声誉，惩罚的力度必须大于奖励的力度，即以下的命题必须成立：

当 $n\geq 1,\ 0<MP_k(i,\ j,\ t_k)\leq 1,\ 0<\varphi(t_k)\leq 1$ 时，

$\mathrm{e}^{-\frac{1}{n+1}}>\varphi(t_k)\mathrm{e}^{-\frac{1}{MP_k(i,\ j,\ t_k)}}$，证明如下：

设 $g(x)=\mathrm{e}^{-\frac{1}{x}},\ x>0$

$\because 0<MPk(i,j,tk)\leq 1<n+1$，$g(x)$ 为单调递增函数

$\therefore \mathrm{e}^{-\frac{1}{n+1}}>\mathrm{e}^{-\frac{1}{MP_k(i,j,t_k)}}$

又 $\because 0<\varphi(t_k)\leq 1$

$\therefore \mathrm{e}^{-\frac{1}{n+1}}>\varphi(t_k)\mathrm{e}^{-\frac{1}{MP_k(i,\ j,\ t_k)}}$

故该命题正确，证毕。

由上述证明可知，惩罚的力度要大于奖励力度，从而当恶意节点进行振荡的交易时，节点的局部声誉值是呈下降趋势的，从而能防止恶意节点通过振荡交易来抬升自己的声誉。

2.2 全局声誉

节点 j 的全局声誉是根据节点 j 的邻居节点在当前时刻 t 时给出的对 j 的综合信任，即 j 的全局声誉，记为 $R(j, t)$。

节点 j 的全局声誉与下列因素有关：

(1)节点 j 的邻居节点数目：邻居节点的数目越多，则 j 的全局声誉越准确，但如果邻居节点与全局声誉的计算无关，则不能准确地反映 j 的全局声誉，并很有可能有一些恶意节点会通过共谋来抬升彼此的声誉，从而欺骗用户，使用户遭受损失[6]。

(2)节点 j 的邻居节点对 j 的直接信任度(j 相对于 j 的邻居节点的局部声誉)：节点 j 的邻居节点对 j 的直接信任度越大，则对 j 的全局声誉影响就越大。

(3)节点 j 的邻居节点对 j 的信任评价权重：邻居节点对节点 j 的信任评价权重越高，则节点 j 越可信；反之，则节点 j 越不可信。

节点 j 在当前时刻 t 时的全局声誉 $R(j, t)$计算公式为

$$R(j,\ t)=\frac{\sum_{r\in I(j)}w_r\times D(r,\ j,\ t)}{\sum_{r\in I(j)}w_r}$$

其中，$I(j)$为所有与 j 有交易经历的邻居节点的集合；R 为 j 的一个邻居节点；w_r 为 r 对 j 的信任评价权重，影响 w_r 的因素有邻居节点与 j 的交易金额和交易时间，其变化规则如下：

(1)如果交易金额很大且交易时间很新，则权值就很大。

(2)如果交易金额很小且交易时间很旧，则权值就很小。

因此，取

$$w_r=\mathrm{e}^{-\frac{1}{\sum_{k=1}^{B(k)}M_k(r,j,t_k)\varphi(t_k)}}$$

其中，$\sum_{k=1}^{B(k)}M_k(r,\ j,\ t_k)\varphi(t_k)$ 是通过时间衰减因子对历次交易的交易金额进行衰减后得到的交易金额期望。

本文之所以选取邻居节点来计算节点的全局声誉是基于以下 2 个原因：

(1)防止与节点 j 无关的节点进入到节点 j 的全局声誉的计算中，从而避免一些恶意节点对节点 j 进行诋毁、夸大或共谋行为。

(2)降低计算全局声誉的复杂度，在一些模型中，节点的全局声誉是通过多个节点传递推荐来得到的，这势必会增加计算的时间复杂度，但本计算方法不考虑中间节点的传递，从而使计算的复杂度要小得多。

2.3 信任度

节点 i 对节点 j 的信任度是通过局部声誉权重系数和全局声誉权重系数来综合节点 j 的局部声誉和节点 j 的全局声誉，从而得出的 i 对 j 的信任程度。节点 i 在当前时刻 t 时对节点 j 的信任度 $T(i, j, t)$的定义如下：

$$T(i,\ j,\ t)=\alpha D(i,\ j,\ t)+\beta R(j,\ t),\text{且}\alpha+\beta=1,\ \alpha,\ \beta\geq 0$$

其中，a 和 β 分别是局部声誉权重系数和全局声誉权重系数，其值可根据用户所需的具体策略而制定。在计算出节点 j 的信任度后，节点 i 须设置一个信任阈值 δ，当 $T(i, j, t)\geq\delta$ 时，则在最近的时间段 t 内节点 i 信任节点 j；反之，当 $T(i, j, t)<\delta$ 时，则在最近的时间段 t 内节点 i 不信任节点 j，用户可根据自己的信任策略来制定信任阈值。

3 实验仿真结果及分析

通过实验考察本文的信任模型在计算信任度的时间负载和交易成功率上与 EigenRep 模型和 Beta 模型的对比情况。实验的硬件环境为：CPU 为 Intel Pentium 820D，内存为 2 GB，仿真软件为 Matlab7.1。

3.1 计算信任度的时间负载

将本文所提出的信任模型简称为 RTM，图 1 为 3 种模型

的运行时间对比，可见，本文提出的信任模型具有较低的计算负载，这是因为本文并没有通过多个中间节点的传递推荐来计算全局声誉，所以能具有较低的时间负载。

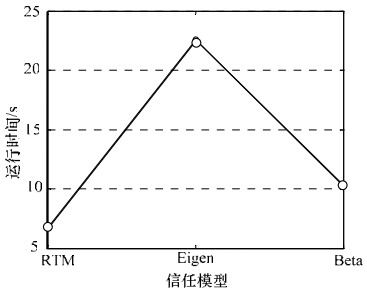

图 1　运行时间对比

3.2　交易成功率

在 P2P 电子商务系统中有 2 种类型的节点：(1)诚信节点，能提供诚信交易，在系统中具有良好的行为，其信任度和交易成功率都比较高；(2)恶意节点，在电子商务系统中进行共谋、诋毁、振荡等一些破坏系统安全性的不良行为，严重地影响了系统的性能，其信任度和交易成功率都很低。

本实验设定所有新加入系统的节点的初始信任度为 0，观察的节点总数为 100。本文的信任模型 RTM 与 EigenRep 和 Beta 在恶意节点比例增多时，各自交易成功率变化对比如图 2 所示。

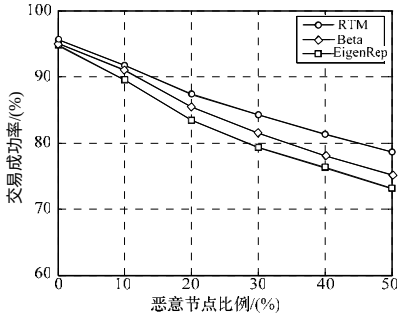

图 2　交易成功率对比

可见，当系统存在恶意节点时，本文的信任模型具有较高的交易成功率，并且当恶意节点较多时仍然具有较高的交易成功率，从而说明本文的信任模型与现有的一些信任模型相比具有较好的抗攻击能力。

4　结束语

本文针对 P2P 电子商务系统提出一种新的基于声誉的信任模型，全面考虑影响局部声誉和全局声誉的因素并改进其计算方法，在计算节点局部声誉中引入惩罚因子和奖励因子，不仅使声誉的计算更人性化，符合人们的交往逻辑，而且还有效地防止了恶意节点通过小金额交易和振荡交易来抬升自己的声誉。实验结果表明，本文提出的信任模型能准确地反映节点的信任度，降低信任度计算的时间复杂度，与现有的一些信任模型相比较大程度地提高了系统交易成功率，具有较好的抗攻击能力。但本模型未引入风险机制，逻辑比较简单，将做进一步改进。

参考文献

[1] Kamvar S D, Schlosser M T. EigenRep: Reputation Management in P2P Networks[C]//Proc. of the 12th Int'l World Wide Web Conference. Budapest, Hungary: ACM Press, 2003: 123-134.

[2] Song S, Hwang K, Zhou R F, et al. Trusted P2P Transactions with Fuzzy Reputation Aggregation[J]. IEEE Internet Computing, 2005, 9(6): 24-34.

[3] 袁　巍, 李津生, 洪佩琳. 一种 P2P 网络分布式信任模型及仿真[J]. 系统仿真学报, 2006, 18(4): 938-942.

[4] Yu Bin, Singh M P. An Evidential Model of Distributed Reputation Management[C]//Proc. of the 1st International Joint Conference on Autonomous Agents and Multiagent Systems. Bologna, Italy: ACM Press, 2002: 294-301.

[5] Jøsang A, Ismail R. The Beta Reputation System[C]//Proc. of the 15th Bled Electronic Commerce Conference. Bled, Slovenia: EC Press, 2002: 324-337.

[6] 姜守旭, 李建中. 一种在 P2P 电子商务系统中基于声誉的信任机制[J]. 软件学报, 2007, 18(10): 2551-2563.

编辑　金胡考

(上接第 128 页)

展，使其具有对 IEEE802.11i 中 4 步握手协议的机密性和认证正确性进行形式化分析的能力。4 步握手协议能实现安全协议对于机密性和认证正确性的要求。下一步将继续对串空间模型进行分析，使其具有对协议可用性进行形式化分析的能力。

参考文献

[1] Fabrega F, Herzog J, Guttman J. Strand Space: Why Is a Security Protocol Correct[C]//Proceedings of the IEEE Symposium on Security and Privacy. [S. l.]: IEEE Computer Society Press, 1998.

[2] Fabrega F, Herzog J, Guttman J. Honest Ideals on Strand Space[C]// Proceedings of the IEEE Computer Security Foundations Workshop. [S. l.]: IEEE Computer Society Press, 1998.

[3] Fabrega F, Herzog J, Guttman J. Strand Spaces: Proving Security Protocols Correct[J]. Journal of Computer Security, 1999, 7(2/3): 191-230.

[4] Dolev D, Yao A C. On the Security of Public Key Protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.

[5] ISO/IEC. IEEE Standard 802.11-2007 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications[S]. 2007.

[6] ISO/IEC. IEEE Standard 802.11i-2004 IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control(MAC) Security Enhancements[S]. 2004.

编辑　顾姣健