P2P 电子商务环境下的动态安全信任管理模型

李致远[1]，王汝传[1, 2, 3]

（1. 南京邮电大学 计算机学院，江苏 南京 210003；2. 江苏省无线传感网高技术研究重点实验室，江苏 南京 210003；
3. 南京邮电大学 计算机研究所，江苏 南京 210003）

摘 要：针对 P2P 电子商务中的信任评估问题，提出一种基于信任云的动态安全信任管理模型(TCDSTM)。TCDSTM 利用云理论来刻画信任及信任等级，然后给出具有抗攻击能力的全局信任度融合算法、节点的类型识别和拓扑重构机制。理论分析和仿真实验一致表明，TCDSTM 不仅可以抵御共谋、振荡等恶意攻击，而且大大提高了交易成功率。此外，该模型具有较低的通信开销。

关键词：对等网络；电子商务；信任；云理论

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2011)03-0050-10

Dynamic secure trust management model for P2P e-commerce environments

LI Zhi-yuan[1], WANG Ru-chuan[1, 2, 3]

(1. College of Computer，Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China;
3. Institute of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: For the trust evaluation problem in P2P e-commerce, a trust cloud-based dynamic secure trust management model (TCDSTM) was proposed. Cloud theory was used to describe the trust and the trust level in TCDSTM. Then an anti-attack global trust aggregation algorithm, the node type identification and topology reconstruction mechanisms were presented. Both theoretical analysis and simulation results show that TCDSTM not only can resist collusion attack, on-off attack and other malicious attacks, but also can improve the success rate of transactions. In addition, TCDSTM has low communication overhead.

Key words: peer to peer networks; electronic commerce; trust; cloud theory

---

收稿日期：2009-02-13；**修回日期**：2010-08-18

基金项目：国家自然科学基金资助项目（60973139，60773041，61003039，61003236）；江苏省科技支撑计划（工业）项目（BE 2010197，BE 2010198）；江苏省级现代服务业发展专项基金资助项目；江苏省高校自然科学基础研究基金资助项目（10KJB520013）；高校科研成果产业化推进工程项目（JH10-14）；国家和江苏省博士后基金资助项目（20100471353，20100471355）；江苏高校科技创新计划基金资助项目（CX10B-196Z，CX10B-197Z，CX10B-198Z，CX10B-199Z）；江苏省六大高峰人才基金资助项目（2008118）

Foundation Items: The National Natural Science Foundation of China (60973139, 60773041, 61003039, 61003236); Scientific & Technological Support Project (Industry) of Jiangsu Province (BE 2010197, BE 2010198); The Special Foundation for the Development of Modern Service Industry of Jiangsu Province; Jiangsu Provincial Research Scheme of Natural Science for Higher Education Institutions (10KJB520013); Scientific Research & Industry Promotion Project for Higher Education Institutions(JH10-14); The Postdoctoral Foundation of China and Jiangsu Province (20100471353, 20100471355); The Science & Technology Innovation Fund for Higher Education Institutions of Jiangsu Province (CX10B-196Z, CX10B-197Z, CX10B-198Z, CX10B-199Z,); The Six Kinds of Top Talent of Jiangsu Province (2008118)

1　引言

电子商务是伴随着互联网成长起来的一种商业模式。在电子商务经历了 B2B（business-to-business）、B2C（business-to-consumer）等传统的 C/S 模式之后，迎来了一种新的模式——P2P 电子商务。在 P2P 电子商务系统中，参与交易的节点既是买方，同时又是卖方。据 Netguide 2008 年的中国互联网调查报告显示，P2P 电子商务已经成为一种主要的在线交易方式，并预测未来几年这种模式的收益将大幅增长。国内外主要的电子商务公司（Taobao、eBay、Amazon 等）都开设了自己的 P2P 电子商务平台，数据统计显示在 P2P 电子商务平台上的成交量正在急速上升。但由于在该平台上交易的双方大都是陌生的，在交易前如何使买卖双方了解对方的信息一直是 P2P 电子商务亟待解决的关键问题之一。目前，国内外的学术界以及 Taobao、eBay、Amazon 等公司都通过建立信任管理模型来解决这一问题，但是他们建立的信任模型在某种程度上都存在着一定的不足。学术界提出的信任管理模型大都是针对全分布式环境的，在这种环境下建立起来的信任管理模型容易受到共谋、振荡等恶意攻击，致使信任评估系统出现错误。尽管国内外学者提出了各种解决方案，但是始终无法彻底地解决这一问题，其主要原因是系统中缺少一个或多个永久可信的参考点。Taobao、eBay、Amazon 等公司建立的信任管理模型存在的共同缺陷如下：①模型过于简单致使信任值计算不准确、更新不及时；②不考虑环境变化对信任的影响，比如对不同时间、不同地点的信息反馈做同等处理。

鉴于此，本文提出一种基于信任云的 P2P 网络动态安全信任管理模型 TCDSTM (trust cloud-based dynamic secure trust management for P2P network)。该模型利用云理论来刻画信任及信任等级评判标准，然后给出具有防御恶意攻击能力的全局信任度融合算法、节点的类型识别以及拓扑重构机制。理论分析和仿真实验一致表明，TCDSTM 不仅可以抵御共谋、振荡等恶意攻击，而且大大提高了交易成功率。此外，该模型具有较低的通信开销。

2　相关工作

文献[1]对现有的 P2P 电子商务环境下的信任模型进行了总结，把其分为基于 PKI 的信任模型、自动信任协商模型和基于声誉的信任模型 3 种，然后给出了 P2P 电子商务下信任模型的设计原则。文献[2~5]提出了多种 P2P 电子商务环境下的信任模型，这些模型与 P2P 环境下的信任模型研究思路是一致的，都是首先给出信任度量标准，然后给出全局信任度融合算法。但是，上述模型只是针对纯 P2P 网络环境，而当前的 P2P 应用系统大都采用基于超级节点的混合 P2P 架构，这样，现有的信任模型不能够直接应用于 P2P 电子商务系统中。

下面给出近年来 P2P 环境下的信任模型的研究状况。

文献[6]提出了一种基于概率统计方法的信任评价模型，该模型能够更有效地抑制策略性欺骗和不诚实推荐的威胁，特别是复杂的协同作弊方式对系统的攻击。文献[7]提出基于改进 D-S 证据理论的信任模型，模型解决了汇聚推荐信息时无法处理不确定性以及强行组合矛盾推荐信息引起的性能下降问题。文献[8]提出了一种基于集对分析的信任模型，模型采用集对分析方法解决了信誉值计算中存在的不确定性问题。文献[9]提出了一种 P2P 环境下基于 Gossip 的信任值快速融合模型以提高信任模型的性能。通过上述信任模型的研究基本解决了信任表示、信任值的快速融合等问题。但是，这些模型均没有考虑与 P2P 应用系统的结合。当前的 P2P 应用系统大都采用基于超级节点的双层拓扑架构，比如，KaZaA、ARES、Skype 等。自 2008 年起，开始有学者对该领域进行研究，他们提出了一些具有抗攻击能力的信任管理模型[10~12]。实验表明上述基于超级节点的信任管理模型与分布式信任管理模型相比，在性能方面有了较大的提高。但上述模型仅能在有限程度上防御共谋、振荡等恶意攻击。对于与经济效益关联较弱的 P2P 应用（P2P 文件共享、P2P 流媒体等），恶意攻击带来的后果是可以接受的。但对于 P2P 电子商务系统，则要求信任管理模型必须能够抵御各类攻击。

3　动态安全信任管理模型

3.1　网络拓扑结构和假设

1) 网络拓扑及工作流程说明

P2P 网络拓扑分为集中式、非结构化和结构化 3 种。其中，集中式拓扑容易出现单点失效；非结构化拓扑资源定位效率低、广播消耗的带宽大；结构化拓扑则不适用于 P2P 电子商务。因此，本文采

用了目前使用最广泛的基于超级节点的双层 P2P 网络拓扑结构，如图 1 所示。其中，超级节点通过 KAD 协议组成异或 DHT 网络；永久可信节点为电子商务公司部署的服务器；一般可信节点是从普通 P2P 节点中挑选出来的能力强、在线时间长、信任值高的节点；一般可信节点与普通 P2P 节点之间存在角色转换。下面对 P2P 电子商务在该拓扑结构上的工作流程进行说明。

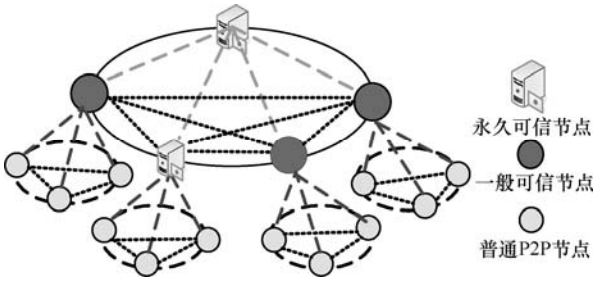

图 1　TCDSTM 部署的拓扑结构

① 普通 P2P 节点利用存在本地的超级节点列表接入网络，它可以同时连接多个超级节点。此外，Peer 节点会周期性地收到超级节点的更新列表。

② 卖方 Peer 节点发布商务信息列表给其所连接的超级节点。列表中的每条商务信息主要包含：商品信息的描述、用户 ID 的散列值。其中，用户 ID 能够唯一地标识用户身份，它是在用户注册 P2P 电子商务平台时，由平台随机分配的。

③ 买方 Peer 节点发起所需商品的关键词搜索请求给其所连接的超级节点。

④ 超级节点通过模糊查询将与关键词搜索请求相关的商品信息列表返回给买方 Peer 节点。商品信息列表包括对商品信息的描述和用户 ID 的散列值。

⑤ 买方 Peer 节点从商品信息列表中选择所需的商品，然后选择卖方 Peer 节点。此时，会触发以用户 ID 的散列值为主键的散列搜索请求到超级节点。

⑥ 超级节点将用户信息列表返回买方 Peer 节点，用户信息列表包含拥有买方 Peer 节点所需商品的用户信息（IP 地址+Port）。列表是按照用户的信任度由高到低排列的。

⑦ 买方 Peer 节点选择信任度高的节点建立连接，进行商务谈判和交易。

2) 模型假设

① 用户在交易完成后，必须将评价结果上报给其连接的超级节点。

② 信任值的传输、全局信任度计算及全局信任度差异化向量计算期间，数据是加密的、无法篡改。

上述假设是为了便于信任研究的开展而设置的，也是大量信任研究[2~12]所共同使用假设条件。

3.2　符号描述和相关定义

1) 符号描述

假设网络是一个由节点集合 V 、边集合 E 和权值 W 组成的带权有向图 $G=(V,E,W)$，权值 W 表示相邻节点的信任推荐度。表 1 列出了本文常用到的符号。

表 1　　**符号描述**

符号	描述
T	信任
V	节点
V_{ij}	从 V_i 到 V_j 的一条边
W	节点信任推荐度
Tr^i	第 i 个信任等级
$T_v / T_{V_{ij}}^{(k)}$	信任值/V_i 对 V_j 直接信任值
T_{online}	节点在线时长
θ_{ij}	i 对 j 的诚信评价，默认值 60
$T_{v_{ij}}^{(t)}$	V_i 对 V_j 间接信任值
T_{v_i}	节点 V_i 的全局信任值
G	可信节点集合
B	不可信节点集合

2) 相关定义

定义 1　如果 Peer B 能够严格地按照 Peer A 所期望的行为进行活动，则称为 A 直接信任 B，记为 $A \xrightarrow{Trust} B$。

定义 2　如果 Peer A 信任 Peer C，Peer C 信任 Peer B，则 A 推荐信任 B。记为 $(A \xrightarrow{Trust} C) \bigcap (C \xrightarrow{Trust} B) \Rightarrow (A \xrightarrow{Trust} B)$。

信任具有以下几个性质。

① 信任具有主观性、随机不确定性以及模糊不确定性。

② 信任具有自反性。即 V_i 可以相信其自身。

③ 信任是可传递的(transitivity)，即信任可以在交互的节点间进行传递。

$(A \xrightarrow{Trust} B) \bigcap (B \xrightarrow{Trust} C) \Rightarrow (A \xrightarrow{Trust} C)$。

④ 信任具有不对称性，即若有 A 信任 B，则 B 不一定信任 A。

$(A \xrightarrow{Trust} B) \neq (B \xrightarrow{Trust} A)$。

⑤ 时间衰减性：随着时间的变化，节点历史行为的评估对当前信任评估的影响会逐渐变小。

⑥ 信任是有大小、有方向的矢量。

定义 3　设网络中任意 2 个信任向量 T_x 和 T_y，它们之间的夹角定义见式(1)。

$$\cos\delta = \cos(T_x, T_y) = \frac{T_x^t T_y}{\|T_x\|\|T_y\|} \tag{1}$$

其中，T_x^t 是向量 T_x 的转置，$\|T_x\|$ 和 $\|T_y\|$ 分别为向量 T_x 和 T_y 的欧几里得范数。

定义 4　（全局信任度差异化矩阵）全局信任度差异化矩阵 $\boldsymbol{T}_{\text{matrix}}$ 刻画了各节点在不同的周期里全局信任度的波动情况，见式(2)。

$$\boldsymbol{T}_{\text{matrix}} = \begin{pmatrix} t_{\text{matrix}}\left(\dfrac{\left|t_{v_1}^{(q)} - t_{v_1}^{(q-1)}\right|}{t_{v_1}^{(q-1)}}\right) & \cdots & t_{\text{matrix}}\left(\dfrac{\left|t_{v_1}^{(p)} - t_{v_1}^{(p-1)}\right|}{t_{v_1}^{(p-1)}}\right) \\ \vdots & \ddots & \vdots \\ t_{\text{matrix}}\left(\dfrac{\left|t_{v_n}^{(q)} - t_{v_n}^{(q-1)}\right|}{t_{v_n}^{(q-1)}}\right) & \cdots & t_{\text{matrix}}\left(\dfrac{\left|t_{v_1}^{(p)} - t_{v_1}^{(p-1)}\right|}{t_{v_1}^{(p-1)}}\right) \end{pmatrix}, \quad 1 \leqslant p \leqslant q \tag{2}$$

其中，$t_{v_1}^{(q)}$ 表示节点 i 在第 q 次迭代后的全局信任度；$t_{\text{matrix}}\left(\dfrac{\left|t_{v_1}^{(q)} - t_{v_1}^{(q-1)}\right|}{t_{v_1}^{(q-1)}}\right)$ 表示节点 i 在第 q 次迭代后的全局信任度波动因子，当 $\dfrac{\left|t_{v_1}^{(q)} - t_{v_1}^{(q-1)}\right|}{t_{v_1}^{(q-1)}} \geqslant \varepsilon$（$\varepsilon$为预先设定的阈值）时，$t_{\text{matrix}}\left(\dfrac{\left|t_{v_1}^{(q)} - t_{v_1}^{(q-1)}\right|}{t_{v_1}^{(q-1)}}\right)$ 的函数值为 1，反之为 0；q 是当前的迭代周期，p 是 q 之前的迭代周期。$\boldsymbol{T}_{\text{matrix}}$ 初始化为一个零矩阵，一个迭代周期结束后，删除矩阵最右边一列，同时，从右边倒数第二列开始至最左边一列元素，依次向右移动一列，并将最新得到的全局信任度波动因子插入左边一列中。以此保证在矩阵 $\boldsymbol{T}_{\text{matrix}}$ 中，从右到左的波动因子对模型的影响力逐渐增大。

全局信任度差异化矩阵 $\boldsymbol{T}_{\text{matrix}}$ 只是一个理论意义上的矩阵，而在本文的网络结构下，对于普通 Peer 节点在 $q-p+1$ 次迭代周期中，其全局信任度差异化向量是由其隶属的超级节点统计得到的；对于一般可信节点的全局信任度差异化向量是由永久可信节点统计得到的。

3.3　基于云理论的信任模型构建

定义 5　设 U 是一个用数值表示的定量论域，T 是 U 上的定性概念，T_v 属于论域空间 U，T_r 为信任等级的语言值，对于 $\forall T_v \in U$，存在映射关系 $\mu_T: U \to [0,100]$，$T_v \mapsto \mu_{T_r}(T_v) \in [0,1]$，称 $\mu_{T_r}(T_v)$ 为 T_v 对 T_r 的信任度隶属函数。$\mu_{T_r}(T_v)$ 在论域 U 上的分布称为主体在属性 T_v 上的信任云。

根据中心极限理论，如果决定某一随机变量结果的是大量微小的、独立的随机因素之和，并且每一因素的单独作用相对均匀得小，没有一种因素可起到压倒一切的主导作用，那么这个随机变量近似于正态分布。对于相邻节点评价的随机变量，单个主体的评价作用相对较小，不能起到压倒一切的主导作用，由此可判定信任云是一种正态云模型，记作 $T_r(E_x, E_n, H_e)$。其中，E_x 表示 T_v 的中心值，中心值处的信任隶属度为 100%，E_n 表示信任的模糊性，H_e 表示 E_n 的不确定性。

定义 6　设 T_{v_i} 为 V_i 的一个信任值，$U=[a,b]$ 为该属性的取值论域，$U' = \{U_i \mid \bigcup_{i=1}^{k} U_i = U, \bigcap_{i=1}^{k} U_i = \phi, \forall T_{v_i} \in U_i, \forall T_{v_j} \in U_j, i < j, T_{v_i} < T_{v_j}\}$，$U'$ 是 U 上的一个划分，信任度隶属函数在划分论域 U_i 上的正态信任云，称之为信任等级云，记为 $T_r = \{T_r^i(E_{x_i}, E_{n_i}, H_{e_i})\}, i \in [1,k]$。

设 U_i 的上、下限为 $\alpha_{\max}^i$ 和 $\alpha_{\min}^i$ 根据云模型的 $3E_n$ 规则，可由以下公式计算信任等级云的 3 个参数。

对于 $Tr^i, i \in [1,\omega]$，有 $E_{x_\omega} = (\alpha_{\max}^i + \alpha_{\min}^i)/2$　(3)

$$E_{n_\omega} = (\alpha_{\max}^i - \alpha_{\min}^i)/6 \tag{4}$$

$$H_{e_\omega} = \sigma \tag{5}$$

其中，σ 为一常数，可根据属性值的不确定性和模糊性的程度来具体调整。

下面根据信任云和信任等级云的定义，建立一个信任等级云的评判标准。

首先以百分制的形式，把信任定义为 6 个等级，如式（6）所示。

$$Tr^i=\begin{cases}\text{完全信任}, & i=1, T_v=100\\ \text{非常信任}, & i=2, 90\leqslant T_v<100\\ \text{比较信任}, & i=3, 80\leqslant T_v<90\\ \text{基本信任}, & i=4, 70\leqslant T_v<80\\ \text{可疑}, & i=5, 60\leqslant T_v<70\\ \text{不信任}, & i=6, T_v<60\end{cases} \tag{6}$$

令取值论域$U=[0,100]$，根据式(6)定义的自变量变化范围划分为 6 个区间。依照信任云和信任等级云的定义以及云模型的$3E_n$规则，得到每个信任等级云的 3 个数字特征期望值E_x、熵E_n和超熵H_e，把其作为输入，云滴N是 2 000，采用正向云算法[13]得到如图 2 所示的信任等级云的实现。图中的每一个云表示一个信任等级，除T_r^1的完全信任为一个点状云，其余的均为正态云。

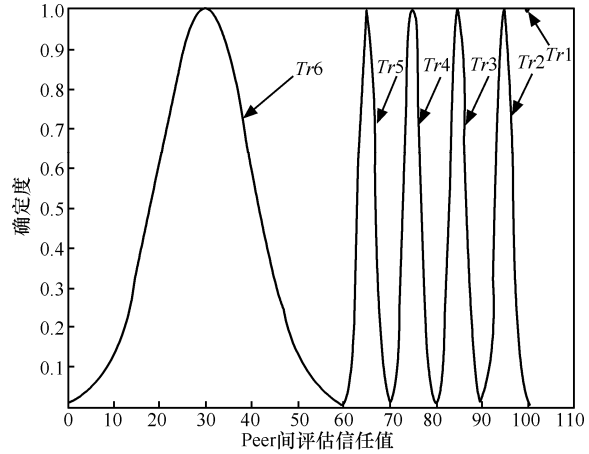

图 2　信任等级云图

3.4　防攻击的全局信任值融合算法

全局信任值融合算法主要由 3 个因素决定：节点间相互评估的信任值、节点的信任推荐度和信任值随时间变化的函数关系。

1) 节点间相互评估的信任值计算方法

节点间的信任度是评价一个节点能力的标准，也是评价一个节点声誉的标准。它主要是依据 2 个 Peer 节点的交互记录。信任度是动态变化的，每一次交互总会得到不同的信任值。以 P2P 电子商务为场景，对节点的信任度计算需要考虑以下 2 个因素，买卖方的诚信统计和节点在线时长。

获取信任度算法如下步骤。

① 假设买方节点 i (Peer i)和卖方节点 j(Peer j)已经完成商务谈判。

② 如果 Peer j 向 Peer i 提供所需商品为正品，令$\theta_{ij}=\theta_{ij}+1$，否则令$\theta_{ij}=\theta_{ij}-1$。

③ 如果 Peer i 按照协议向 Peer j 付款，令$\theta_{ji}=\theta_{ji}+1$，否则令$\theta_{ji}=\theta_{ji}-1$。

Peer i 对 Peer j 的信任评价见式(7)。

$$T_{V_{ij}}=100\left|\arctan[(\alpha\ \ \beta)(\theta_{ij}\ \ T_{\text{online}})^{\mathrm{T}}]\right|, \alpha+\beta=1 \tag{7}$$

Peer i 对 Peer j 的信任值更新见式(8)。

$$T_{V_{ij}}^{(k)}=(1-\rho)\times T_{V_{ij}}^{(k-1)}+\rho\times T_{V_{ij}}^{(k)} \tag{8}$$

$T_{V_{ij}}^{(k)}$表示第 k 时刻V_i对V_j的信任值，$T_{V_{ij}}^{(k-1)}$表示第$k-1$时刻的信任值，ρ为权重。

节点间相互评估的信任值$T_{V_{ij}}^{(k)}$是一个随时间衰减的函数，即离交易评估时间越近，信任值就越可信；反之，就不可信。因此，用负指数模型来描述其函数关系，见式(9)。

$$T_{V_{ij}}(t)=T_{V_{ij}}^{(k)}e^{-c(t-k)} \tag{9}$$

$T_{V_{ij}}(t)$ $T_{V_{ij}}(t)$表示$T_{V_{ij}}^{(k)}$在$(t-k)$时刻后的信任值，c是一个常数($c\geqslant 1$)。

2) 节点的推荐度

为了抑制共谋攻击（大量恶意节点故意抬高某一节点的信任值），需要建立信任等级和信任推荐度的映射表。信任等级越高，推荐度越高；信任等级越低，推荐度越低。这样，即便存在恶意节点发起共谋攻击，故意抬高对某一节点的信任评估值，但在全局信任值融合计算时，由于恶意节点的权值较小，对全局信任值计算的影响不大，恶意攻击的影响程度就大大削弱，见表 2。

表 2　　信任等级和推荐度的映射

信任等级 Tr	推荐度 W
完全信任	1
非常信任	0.8
比较信任	0.4
基本信任	0.1
可疑	0.025
不信任	0.006 25

3) 全局信任值计算方法

① Peer i 对 Peer j 的间接信任值计算，见式(10)。

$$T_{V_{ij}}^{(t)}=\frac{1}{\|N(j)\|}\sum_{s\in N(j)}\prod_{i\in S(i\to j)}W_{is}T_{V_{sj}}(t)$$

$$= \frac{1}{\|N(j)\|} \sum_{s \in N(j)} \prod_{i \in S(i \to j)} W_{is} T_{v_{sj}}^{(k)} e^{-c(t-k)} \quad (10)$$

其中，W_{is} 表示 V_i 对 V_s 的推荐度 W，$N(j)$ 表示与 Peer j 有过交易的节点集合，$\|N(j)\|$ 表示与 Peer j 有过交易的节点数目，$S(i \to j)$ 表示 Peer i 与 Peer j 可达路径上的节点集合。

网络中 Peer i 的全局信任值等于全网节点对 Peer i 的直接信任向量和间接信任向量的合向量，为此采用平行四边形法则求解 Peer i 的全局信任值 T_{v_i}。

② 全局信任值 T_{v_i} 的求解算法如下。

为了便于说明，无论直接信任值或推荐信任值统一用 $T_{v_{ji}}^{(k)}$ 表示。

Input $T_{v_{ji}}^{(k)}$ $j \in [1,n], i \neq j$ Output $T_{V_i}^{(k+1)}$

Procedure

Begin

$T_{V_i}^{(k)} = \sqrt{(T_{v_{ji}}^{(k)})^2 + (T_{v_{(j+1)i}}^{(k)})^2 - 2T_{v_{ji}}^{(k)} T_{v_{(j+1)i}}^{(k)} \cos\delta}$

$j = 0, \cos\delta$ 是两个信任矢量夹角的余弦值。

for (j=2;j<n-1;j++)

{

$T_{V_i}^{(k+1)} = \sqrt{(T_{v_{ji}}^{(k)})^2 + (T_{V_i}^{(k)})^2 - 2T_{v_{ji}}^{(k)} T_{V_i}^{(k)} \cos\delta}$

$T_{V_i}^{(k)} = T_{V_i}^{(k+1)}$

}

End

3.5 节点的类型识别及拓扑重构机制

1) 节点类型识别机制

① 对 $q-p+1$ 次迭代周期内的 Peer i 的信任值进行分析，对于序列 $\{t_{v_i}^{(p)}, \cdots, t_{v_i}^{(q-1)}, t_{v_i}^{(q)}\}$ 存在 3 种情况：序列为减序列、振荡序列和增序列。如果节点的信任值序列满足减序列或振荡序列，则把其列入 B 集合。如果节点的信任值序列满足增序列的条件，转入步骤②。

② 计算出 Peer i 的全局信任度差异化向量 $\left(t_{\text{matrix}}\left(\frac{|t_{v_i}^{(q)} - t_{v_i}^{(q-1)}|}{t_{v_i}^{(q-1)}}\right) \cdots t_{\text{matrix}}\left(\frac{|t_{v_i}^{(p)} - t_{v_i}^{(p-1)}|}{t_{v_i}^{(p-1)}}\right)\right)$。如果向量为零向量，则将 Peer i 记入 G 集合；反之，如果向量中存在多个波动因子为 1 的全局信任度，则表明 Peer i 很可能已经成为共谋集合中的一员，将该节点列入 B 集合。

2) 拓扑重构机制

根据节点类型识别机制可以识别出节点当前的状态和类型。如果一般可信节点发现连接到其上的普通节点属于 G 集合且该节点的全局信任值隶属于 Tr^1 或者 Tr^2（要求信任值的隶属度大于 80%），此时，将这个节点升级为一般可信超级节点，并将节点添加到超级节点列表中。永久可信节点周期性地根据节点类型识别机制检测一般可信节点的状态，一旦发现有一般可信节点加入到 B 集合中，则立即从超级节点列表中删除该节点。

当超级节点列表改变时，永久可信超级节点将更新后的超级节点列表发给一般可信超级节点，这些超级节点再将节点列表发送给普通 Peer 节点。普通 Peer 节点在下次登录网络时，就从更新后的超级节点列表中选择一定数量的可信超级节点进行连接，从而实现双层 P2P 网络拓扑的更新。

4 TCDSTM 模型的理论分析和仿真实验

4.1 TCDSTM 模型的全局信任度收敛性和复杂度分析

定理 1　对于 $\forall T_{V_{ji}}$ $j \in [1,n], i \neq j$，$\exists T_{V_i}^{(k+1)} = \sqrt{T_{V_{ji}}^2 + (T_{V_i}^{(k)})^2 - 2T_{V_{ji}} T_{V_i}^{(k)} \cos\delta}$ 收敛。

证明　因为 $0 \leqslant \cos\delta \leqslant 1$，有

$$T_{V_i}^{(k+1)} = \sqrt{T_{V_{ji}}^2 + (T_{V_i}^{(k)})^2 - 2T_{V_{ji}} T_{V_i}^{(k)} \cos\delta} \leqslant \sqrt{(T_{V_{ji}} + T_{V_i}^{(k)})^2} = T_{V_{ji}} + T_{V_i}^{(k)}$$

又因为 $T_{V_i}^{(k)}$ 的收敛性也取决于直接或间接信任向量 $T_{V_{ji}}$，所以只要向量 $T_{V_{ji}}$ 是收敛的，则全局信任度 T_{V_i} 必收敛。

由式 (10) 知，间接信任向量 $T_{v_{ij}}^{(t)} = \frac{1}{\|N(j)\|} \cdot \sum_{s \in N(j)} \prod_{i \in S(i \to j)} W_{is} T_{v_{sj}}^{(k)} e^{-c(t-k)}$。

那么，$T_{v_{ij}}^{(k+1)} = \frac{1}{\|N(j)\|} \cdot \sum_{s \in N(j)} \prod_{i \in S(i \to j)} W_{is} e^{-c} T_{v_{sj}}^{(k)}$，该式收敛的充分条件是 $\|We^{-c}\| < 1$，其中 $W = \{W_{is}, i \in S(i \to j)\}$。

又因为 $W \leqslant 1$，所以必有 $\|We^{-c}\| < 1$。因此，间接信任向量 $T_{V_{ji}}$ 是收敛的。

同理直接信任向量也是收敛的。

命题得证。

定理 2　设网络中的节点数为 n，超级节点个数为 m，节点 i 的全局信任值为 T_{V_i}，与 i 直接交易

过的节点数记为$\|N(i)\|$，与i间接交易过的节点记为j，i与j可达路径上的节点数记为$\|S(j\to i)\|$，则全局信任值融合算法的时间复杂度为$O(n)$，空间复杂度也为$O(n)$。

证明 显然，节点间相互评估的信任值算法的时间复杂度为$O(1)$，间接信任值算法的时间复杂度为$O(\|N(i)\|\|S(j\to i)\|)$，全局信任值融合算法的时间复杂度$T(n)=O(3n-12+1)=O(n)$，因此具有抗攻击能力的全局信任值融合算法的时间复杂度为$T(n)=O(n+\|N(i)\|\|S(j\to i)\|+1)=O(n)$。

同理可得，节点间相互评估的信任值算法的空间复杂度为$O(1)$，间接信任值算法的空间复杂度为$O\left(\sum_{\|N(i)\|}\|S(j\to i)\|\right)$，全局信任值融合算法的空间复杂度$O\left(\frac{m-1}{m}n\right)$，因此具有抗攻击能力的全局信任值融合算法的空间复杂度为

$$T(n)=O\left(\frac{m-1}{m}n+\sum_{\|N(i)\|}\|S(j\to i)\|+1\right)=O(n)$$

4.2 仿真实验

4.2.1 仿真参数设置

本文选择与 TCDSTM 采用相同网络环境的文献[10]和文献[12]所提出的信任模型，从信任计算差错率、交易成功率和控制开销 3 个方面进行对比分析，以验证 TCDSTM 模型的性能和抗攻击性。此外，还验证了网络中存在不同比例的恶意节点情况下，节点的全局信任度变化规律。

把网络中的节点分为 2 类：可信节点（包括完全信任和非常信任等级的节点）和恶意节点（包括其他等级的节点）。可信节点无论是提供服务还是对交易节点的评价都是真实可信的，称这类节点为t类，它所占的比例为P_t。恶意节点不提供可靠的服务，对交易节点常提供虚假的评价信息，称这类节点为Z类，比例为P_z。根据恶意程度不同，将恶意节点进一步分成以下 4 类。

① 非恶意情况下产生的攻击由比较信任等级的节点组成，只是偶尔提供有误差的评价，并不诋毁与之交易的节点，称这类节点为Z_A类。

② 个体诋毁由基本信任等级的节点组成，这类节点不参与任何共谋团体，只是有时会自发地故意提供不可信评价，以达到诋毁与之交易节点的目的，称这类节点为Z_B类。

③ 偶尔共谋诋毁由受怀疑等级的节点组成。这些节点组成一个协同作弊的团伙，在交易中偶尔互相提交虚假的推荐信息，偶尔对团伙外的节点进行诋毁，称这类节点为Z_C类。

④ 共谋诋毁由不信任等级的节点组成。这类节点也组成一个协同作弊的团伙，在交易中总是对团伙内的成员互相提交虚假的推荐信息，而对团伙外的节点进行诋毁，称这类节点为Z_D类。

采用 J-Sim[14~16]仿真平台进行仿真，J-Sim 是一种基于 Java 和 Tcl 脚本的、开源的、实时进程驱动的网络仿真平台。J-Sim 可以很好地对 Internet、无线网络、对等网络等不同体系结构的网络进行各个层面上的实时仿真。本文的硬件支撑环境为 1.73GHz 双核处理器和 2GB 内存。每项仿真均采用执行 10 次后取平均值，仿真参数设置见表 3，其余表中未列出的参数在具体章节中已经明确定义。

表 3 仿真实验参数

符号	描述	默认值
N	总节点数	1 000
M	超级节点的个数(其中永久可信节点 3 个)	10
n/m	每个簇中平均包含节点的个数	100
Pt	可信节点的比例	80%
$P_z(P_{Z_A},P_{Z_B},P_{Z_C},P_{Z_D})$	各类恶意节点的比例(2:1:1:1)	20%
$mrate$	恶意节点进行攻击的概率	100%
P	迭代窗口的大小	10
α	权重	0.6
ρ	权重	0.8
C	常数	1.75

4.2.2 性能评估

如图 3 所示为恶意节点发起攻击的概率为100%的条件下，随着恶意节点比例的增加，信任值计算错误率仿真。当恶意节点比例为 0 时，3 种模型的信任计算错误率是由计算误差导致的。之后，随着恶意节点比例的增加，TCDSTM、Hybrid Model[10]和 Hybrid Model[12]模型的信任值出错率小幅增长，3 种模型的抗攻击性初步体现出来。当恶意节点的比例增长到 50%时，Hybrid Model[10]和 Hybrid Model[12]信任值出错率有所增加，这主要是由大量恶意节点发起共谋攻击造成的。此时，TCDSTM 模型出错率仍然小幅增长，这表明 TCDSTM 模型具有更强地防御共谋攻击的能力。当网络中恶意节点比例达到 80%时，Hybrid

Model[10]和 Hybrid Model[12]的信任计算出错率分别为 59%和 64%，而 TCDSTM 模型的出错率仅为 40%。

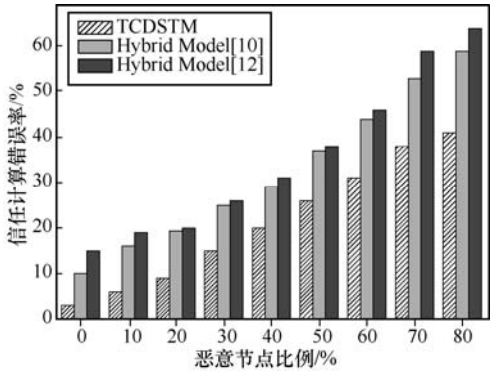

图 3　信任计算错误率—恶意节点比例

如图 4 所示为恶意节点比例为 20%，随着恶意节点攻击概率的增长，信任值计算错误率的仿真。起初，Hybrid Model[10]和 Hybrid Model[12]随着 *mrate* 的增加，信任值出错率迅速增长。在 *mrate* 达到 40%之后，Hybrid Model[10]和 Hybrid Model[12]的信任值出错率缓慢增长，最后收敛于 20%附近。对于 TCDSTM 模型随着 *mrate* 的增加，信任值出错率平缓上升，最后收敛于 9%。这就表明 TCDSTM 模型比 Hybrid Model[10]和 Hybrid Model[12]模型的抗攻击能力更强。同时也表明 TCDSTM 模型中防攻击的全局信任值融合机制、节点识别以及惩罚机制具有较强的抗攻击性和适应性。

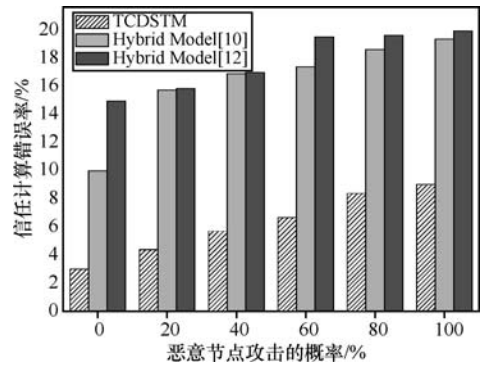

图 4　信任计算错误率—恶意节点发起攻击概率

如图 5 所示为交易成功率随着恶意节点比例增长的仿真，交易总次数为 1000。随着网络中恶意节点比例的增加，3 种模型的交易成功率都有不同程度的下降，其中 Hybrid Model[12]最为明显，当恶意节点数达到 80%后，交易成功率仅有 50%。TCDSTM 和 Hybrid Model[10]比 Hybrid Model[12]下降缓慢，当网络中恶意节点数达到 80%后，交易成功率分别为 60%和 54%。这就表明 TCDSTM 比其他 2 种混合模型的抗攻击能力要强，并且提高了节点的交易成功率。

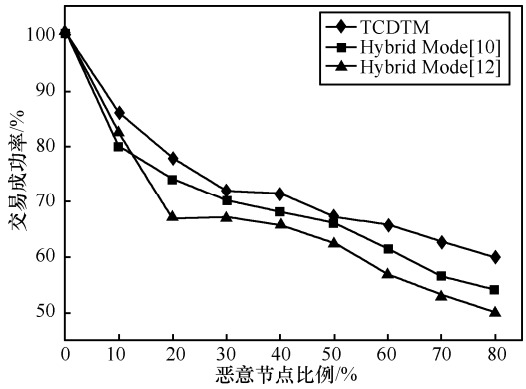

图 5　交易成功率—恶意节点的比例

如图 6 所示为网络中恶意节点的数量为 20%时，交易成功率随交易次数增加的仿真。随着交易次数的增加，TCDSTM 以 89%的交易成功率上下波动、Hybrid Model[10]以 81%的交易成功率上下波动、Hybrid Model[12]以 76.8%的交易成功率上下波动。实验结果表明 TCDSTM 可以明显地提高交易成功率。通过对网络中恶意节点数量为其他比例时的仿真，发现交易次数与交易成功率同样呈现这种规律性。

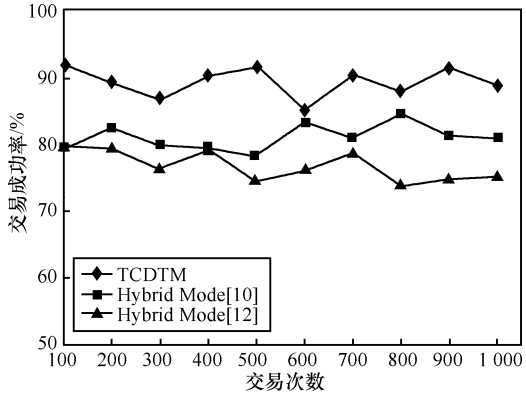

图 6　交易成功率—交易次数

如图 7 所示为网络的通信开销随网络规模增大的仿真。从图中不难发现，当网络规模为 100 时，Hybrid Model[10]、Hybrid Model[12] 和 TCDSTM 3 个模型所产生的消息数大致相等。当网络规模增长到 1 000 时，Hybrid Model[10]比 TCDSTM 多产生 10500 多条控制消息，Hybrid Model[12]比 TCDSTM 多产生 1 668 686 条控制消息，Hybrid Model[12]比

TCDSTM 多产生的控制消息数是 Hybrid Model[10]比 TCDSTM 多产生的控制消息数的 159 倍。当网络规模增长到10 000时，Hybrid Model[10]比 TCDSTM 多产生 115 000 多条控制消息，Hybrid Model[12]比 TCDSTM 多产生 37 219 600 条控制消息，Hybrid Model[12]比 TCDSTM 多产生的控制消息数是 Hybrid Model[10]比 TCDSTM 多产生的控制消息数的 323 倍。从整体上看，随着网络规模的增大，TCDSTM 和 Hybrid Model[10]所产生的通信开销数相差较小，而 Hybrid Model[12]显然与 TCDSTM 和 Hybrid Model[10]模型所产生的控制消息数的差越来越大。这就表明 TCDSTM 模型不仅能够抵御各种恶意攻击，与同类混合 P2P 模型相比，TCDSTM 模型的通信开销更低。

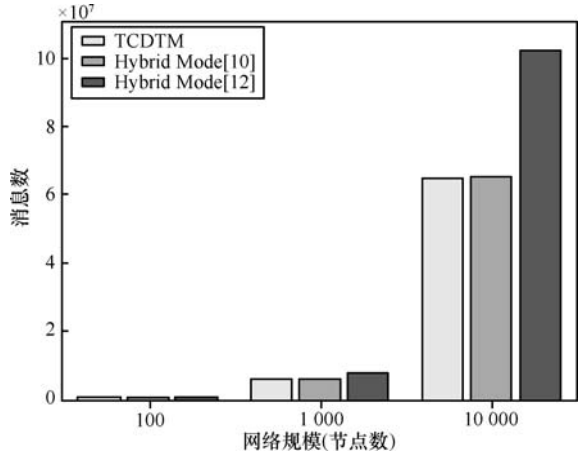

图 7 网络的通信开销(消息数)—网络规模

如图 8 所示为网络中节点的全局信任值的平均值在恶意节点比例不同情况下的仿真。设定恶意节点比例分别为 20%、40%和 60%，从图中不难发现，节点的全局信任度均值都能在较短的时间内收敛于一个稳定值。恶意节点的共谋行为起初对节点的全局信任值影响较大，尤其是在恶意节点比例较高时，但在其后的时间内，由于 TCDSTM 模型的节点识别机制和惩罚机制发挥作用，节点的全局信任值迅速收敛到其真实的信任值。实验结果表明即便发生了共谋攻击，对网络中节点的全局信任值影响不大，同时也表明了 TCDSTM 模型具有较强的抗攻击能力。

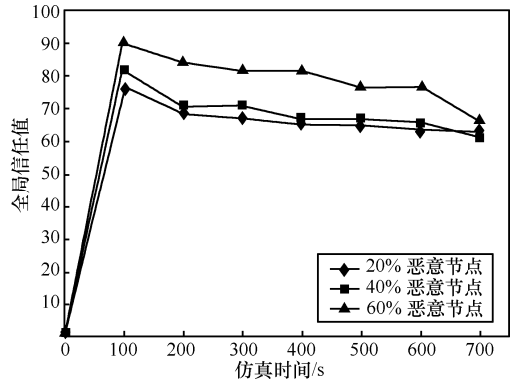

图 8 全局信任值—仿真时间

5 结束语

本文提出一种基于信任云的 P2P 网络动态安全信任管理模型 TCDSTM。该模型首先利用云理论构建一种新的信任模型，其中包括信任及信任等级评判标准的建立。然后，基于信任云理论提出具有防御恶意攻击能力的全局信任度融合模型及其求解算法。之后给出 Peer 节点的类型识别方法和拓扑重构机制。最后对全局信任值融合算法的收敛性和复杂度进行理论分析，并对不同网络环境下的信任计算错误率、交易成功率等指标进行仿真。理论分析和实验结果一致表明，TCDSTM 利用信任云理论可以更加准确地获取局部信任评价信息；通过全局信任值融合算法不仅可以抵御共谋、振荡等恶意攻击，而且大大提高了交易成功率。此外，模型具有较低的通信开销。这为 TCDSTM 模型向 P2P 电子商务系统中移植的可行性提供了理论依据和实验数据参考。但在实际应用中，TCDSTM 模型的具体表现如何，还需与 P2P 电子商务系统相结合并在真实的网络环境下进行测试，看是否存在有待改进之处，这将在以后的工作中进行深入研究。

参考文献：

[1] LIN Y. Study of security problems in P2P e-commerce[A]. Proceedings of the 2nd International Conference on e-Business and Information System Security[C]. Wuhan, China, 2010.1-4.

[2] LI C, WANG Y, YANG D. A trust evaluation model for future peer-to-peer e-commerce environments[A]. Proceedings of the Workshops on GLOBECOM[C]. Honolulu, HI, 2009.1-6.

[3] ZHANG S, ZHANG X, WANG B. History and future information based trust model in C2C E-commerce[A]. Proceedings of the Fifth International Conference on Information Assurance and Security[C]. Xian, China, 2009. 491-494.

[4] DONG P, WANG H, ZHANG H. Probability-based trust management model for distributed e-commerce[A]. Proceedings of the IEEE International Conference on Network Infrastructure and Digital Content[C]. Beijing, China, 2009. 419-423.

[5] ZHANG J, GUO X. Trust evaluation model based on fuzzy logic for

C2C e-commerce[A]. Proceedings of the International Symposium on Information Engineering and Electronic Commerce[C]. Ternopil, 2009. 403-407.

[6] 吴鹏, 吴国新, 方群. 一种基于概率统计方法的 P2P 系统信任评价模型[J]. 计算机研究与发展, 2008, 45(3):408-416.
WU P, WU G X, FANG Q. A reputation-based trust model based on probability and statistics for P2P systems[J]. Journal of Computer Research and Development, 2008, 45(3): 408-416.

[7] ZHANG Z, WANG X M, WANG Y X. A scheme for solving D-S theory based ignorant evidence fusion in P2P network[A]. Proceedings of the Fifth International Conference on Machine Learning and Cybernetics[C]. Dalian, China, 2006. 4531-4535.

[8] 胡波, 王汝传, 王海艳. 基于集对分析的 P2P 网络安全中的信誉度改进算法[J]. 电子学报, 2007, 35(2): 244-247.
HU B, WANG R C, WANG H Y. A modified security solution based on SPA for servants' reputations in P2P systems[J]. Acta Electronica Sinica, 2007, 35(2): 244-247.

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

[10] KARAME G, CHRISTOU I T, DIMITRIOU T. A secure hybrid reputation management system for super-peer networks[A]. Proceedings of the 5th IEEE International Conference on Consumer Communications and Networking[C]. Las Vegas, NV, 2008. 495-499.

[11] GAO L, LI Z M. A trust model for the superpeer-based P2P files sharing system[A]. Proceedings of the Second International Symposium on Electronic Commerce and Security[C]. Nanchang, China, 2009. 12-15.

[12] LIANG B B, GU L Z, SUN B, *et al*. A scheme of trust management system for P2P network[A]. Proceedings of the 12th International Conference on Advanced Communication Technology[C]. Phoenix Park, 2010. 1453-1458.

[13] 李德毅, 杜鹢. 不确定性人工智能[M]. 北京:国防工业出版社, 2005. 171-177.
LI D Y, DU Y. Artificial Intelligence with Uncertainty[M]. Beijing: National Defence Industry Press, 2005. 171-177.

[14] TYAN H Y. Design, Realization and Evaluation of a Component-Based Compositional Software Architecture for Network Simulation[D]. USA: the Ohio State University, 2002.

[15] HAMADA T, CHUJO K, CHUJO T, *et al*. Peer-to-peer traffic in metro networks: analysis, modeling, and policies[A]. Proceedings of the IEEE/IFIP Symposium on Network Operations and Management[C]. Seoul, South Korea, 2004. 425-438.

[16] SOBEIH A, HOU J C, KUNG L C, *et al*. J-Sim: a simulation and emulation environment for wireless sensor networks[J]. IEEE Wireless Communications, 2006, 13(4): 104-119.

作者简介：

李致远（1981-），男，河南开封人，南京邮电大学博士生，主要研究方向为无线传感器网络、P2P 网络安全。

王汝传（1943-），男，安徽合肥人，南京邮电大学教授、博士生导师，主要研究方向为计算机软件、计算机通信、信息安全、无线传感器网络、移动 Agent 等。

（上接第 49 页）

[13] 哈米德 • 贾法哈尼著，任品毅译. 空时编码的理论与实践[M]. 陕西：西安交通大学出版社，2007.
JAFARKHANI H. Space-Time Coding: Theory and Practice[M]. Xi'an: Xi'an Jiaotong University Press,2007.

[14] SIMON M. K. Evaluation of average bit error probability for space-time coding based on a simpler exact evaluation of pairwise error probability[J]. Int Jour Commun and Networks, 2001, 3(3): 257 -64.

[15] CRAIG J W. A new simple and exact result for calculating the probability of error for two-dimensional signal constellations[A]. Military Communications Conference[C]. USA, 1991.

[16] TELATAR E. Capacity of multi-antenna Gaussian channels[J]. European Transactions on Telecommunications, 1999, 10: 585-95.

作者简介：

李正权（1976-），男，湖北利川人，东南大学移动通信国家重点实验室博士后、中国计量学院副教授、硕士生导师，主要研究方向为空时编码和空时自适应信号处理。

沈连丰（1952-），男，江苏邳州人，东南大学教授、博士生导师，主要研究方向为宽带移动通信、短距离无线通信与泛在网络等。

郭永亮（1977-），男，甘肃灵台人，东南大学讲师，主要研究方向为无线通信中的空时处理、相干和非相干空时编码的设计与分析、多入多出系统的容量计算。