第 38 卷 第 2 期
Vol.38 No.2

计 算 机 工 程
Computer Engineering

2012 年 1 月
January 2012

• 安全技术 •

文章编号：1000—3428(2012)02—0141—03 文献标识码：A 中图分类号：TP393

P2P 环境中基于信誉与云理论的信任模型

林 军，姜文君，王国军

(中南大学信息科学与工程学院，长沙 410083)

摘 要：在 P2P 环境中，现有信任模型不能完整地体现信任的主观性、模糊性和随机性。为此，提出一种针对 P2P 环境的信任模型(CloudBT)。在计算节点的全局信任值时引入时间权重函数，并结合云模型得到节点的信任值，该信任值包括信任的平均度量和信任的不确定信息。在做信任决策时，综合考虑节点信任值的大小及其行为的波动情况。模拟结果表明，CloudBT 在 P2P 电子商务环境中具有较高的成功交易率和较强的抗攻击能力。

关键词：P2P 环境；信任模型；主观性；云模型；信誉机制

Trust Model Based on Reputation and Cloud Theory in P2P Environment

LIN Jun, JIANG Wen-jun, WANG Guo-jun

(School of Information Science and Engineering, Central South University, Changsha 410083, China)

【Abstract】In P2P environment, most of the existing trust models can not reflect the subjectivity, fuzziness and uncertainty of trust. This paper presents a new trust model for P2P environment——CloudBT. In the calculation of the node global trust value, it introduces time weight function, and combines with cloud model to get the node trust value which integrates cloud model with reputation-based model to describe the measure and uncertainty of trust, and considers both the trust value of nodes and behavior of the fluctuations when making trust decisions. Simulation results show that the CloudBT model has the high success rate of trade and strong ability against the attack in P2P e-commerce environment.

【Key words】P2P environment; trust model; subjectivity; cloud model; reputation mechanism

DOI: 10.3969/j.issn.1000-3428.2012.02.045

1 概述

随着网络技术的发展，网络应用模型由相对集中的静态形式发展为开放的动态形式。P2P 网络作为一种动态、开放的分布式服务环境，是由大规模自由节点匿名参与而形成，因此，具有自组织、开放和可扩展等本质特点。分布式网络环境的异构性和动态性造成了节点之间缺乏足够的安全信任关系，从而对 P2P 系统安全提出了严峻的挑战。传统的安全技术如访问控制策略、公钥证书体系等由于依赖参与节点的正确安全操作而导致其不适合 P2P 环境，也无法解决对等网络应用中匿名节点之间合作所面临的信任和激励问题。因此，在节点之间建立一种信任机制，建设一个透明有序的交易环境，显得非常有意义。

目前，信任机制正逐渐被越来越多的专家学者所重视。信任本质上是基于信念的，具有很大的不确定性[1](主观性、模糊性和随机性)。信任还具有动态变化的本质，它可以随着经验、主体的心理状态、客体的周围环境、时间等因素而变化。信任很难用简单、确定性的数值加以描述。所以，有必要将信任的主观性、模糊性以及随机性综合考虑在信任模型中。

基于信誉的信任模型是指通过观察和收集实体在网络中的行为和表现评估其信任，因此，也称为基于行为的信任模型。EigenTrust[2]模型和基于 EigenTrust 改进的 SWRTrust[3]模型都是基于信誉的全局信任模型，它们能够在一定程度上解决恶意节点的协同作弊问题，但它们只考虑了信任的随机性，都没有综合考虑信任的模糊性。

现有的典型模型都试图用概率数学或模糊数学作为研究工具，解决信任模型中遇到的各种问题，但无法完整地描述信任的不确定性。研究发现云模型[4]能把定性概念的主观性、模糊性和随机性有机给合起来，实现概念的定性和定量之间的互相转换，因此，能为信任模型的研究提供有价值的方法。文献[5]将云模型引入到普适计算、电子商务系统等信任模型研究中。本文将云模型和基于信誉的模型相结合，提出一种新的信任模型 CloudBT，并将其引入到 P2P 电子商务的网络环境中。

2 云理论

20 世纪 90 年代初，李德毅院士开创的“云”理论[1,4,6]，是在传统的模糊数学和概率统计的基础上提出了定性与定量互换模型，主要反映 2 种不确定性：模糊性和随机性，它把模糊性和随机性有机结合在一起，构成定性和定量相互间的映射，为定性与定量相结合的信息处理提供了有力手段。

2.1 云的基本概念

定义 设 U 是一个用精确数值表示的定量论域(一维或多维)，C 是 U 上对应的定性概念，对于论域上的任意一个元素

基金项目：国家自然科学基金资助项目(61073037)；湖南省科技计划基金资助重点项目(2010GK2003)

作者简介：林 军(1986－)，男，硕士研究生，主研方向：可信计算，P2P 网络；姜文君，博士研究生；王国军，教授、博士生导师

收稿日期：2011-04-07 **E-mail：**linjunemail@gmail.com

x，都存在一个稳定倾向的随机数 $y=H_C(x)$，称为 x 对 C 的隶属度，x 在论域 U 上的分布称为云。

云是由许多个云滴组成，每个云滴就是 C 映射到数域空间的一个点，每个 x 就是一个云滴。某一个云滴也许无足轻重，但云的整体形状反映了定性概念的重要特性。

2.2 云的数字特征

云的 3 个数字特征用期望 E_x、熵 E_n 和超熵 H_e 表示，它们把模糊性和随机性完全集成在一起，反映了定性概念在整体上的定量特征，以下是这 3 个数字特征所代表的含义：

(1)期望 E_x：在数域空间中最能够代表定性概念 C 的点，它代表 C 的信息中心值。

(2)熵 E_n：是定性概念 C 的不确定性，代表概念 C 的粒度。反映数域空间中可被 C 接受的云滴范围大小，即 C 的模糊性，熵越大，定性概念越宏观，模糊性也越大。

(3)超熵 H_e：超熵是熵的不确定性度量，即熵的熵。它反映了定性概念 C 样本出现的随机性。

2.3 逆向云发生器

宇宙中的事物、人类知识概念和自然界中的大量模糊概念都可以用正态云刻画。正态云的期望曲线是一个正态曲线。正态云的特性如下：对于任何 $x\in U$，若 x 在定性概念的每次随机实现满足 $x\sim N(E_x,E_n'^2)$ 且 $E_n'^2\sim N(E_n,H_e^2)$，x 对 C 的隶属度满足 $y=\mathrm{e}^{\frac{(x-E_x)^2}{2(E_n'^2)^2}}$，则 x 在定量论域 U 上的分布称为正态云。下文中提到的云如果没有特别说明，则都是基于正态云。由云滴计算出云的 3 个数字特征 E_x、E_n、H_e 的过程叫做逆向云发生器。

算法 1 逆向云发生器算法

输入 N 个云滴 x_i

输出 N 个云滴表示定性概念的期望 E_x、熵 E_n 和超熵 H_e

Step1 根据 x_i 计算云滴的样本均值 $\bar{x}=\frac{1}{N}\sum_{i=1}^{N}x_i$，一阶样本绝对中心距 $B=\frac{1}{N}\sum_{i=1}^{N}|x_i-\bar{x}|$，样本方差 $S^2=\frac{1}{N}\sum_{i=1}^{N}(x_i-\bar{x})^2$。

Step2 E_x 的估计值为 $E\hat{x}=\bar{x}$。

Step3 E_n 的估计值为 $E\hat{n}=\sqrt{\frac{\pi}{2}}\times B$。

Step4 H_e 的估计值为 $H\hat{e}=\left(S^2-E\hat{n}^2\right)^{1/2}$。

3 基于信誉与云理论的信任模型 CloudBT

在 P2P 电子商务网络环境中，主体想要进行一次交易时，会面临很多选择，如何设计一种直观、简单、有效的信任评价辅助完成交易，从而提升交易的准确性和主体的满意度是本文的研究重点。目前，大多电子商务平台都采用计算平均值的方法进行信任评分，主体很难据此选择可信主体进行交易。统计的方法能够有效地反映主观评分的随机性，却不能表述主观的模糊性。对于主观的评分，不论是多级评分还是连续数值空间的评分都存在明显的模糊性。例如，对于综合评分都是 4 分的主体，是无法得到它们之间的明显的区别。针对这些问题，本文提出了 CloudBT 模型，该模型在 EigenTrust[2]模型的基础上进行了扩展：(1)引入时间权重函数计算节点的全局信任值；(2)结合云模型完整的得到节点的信任值，该信任值既包括信任的平均度量，又包含信任的不确定信息；(3)在做信任决策时，综合考虑节点信任值的大小及其行为的波动情况。

3.1 全局信任值计算

在全局信誉模型中任意节点 i 在网络中都有全局唯一的信任值，记作 T_i。

CloudBT 模型中 T_i 的计算方法见式(1)：

$$T_i=\sum_{k\in U_i}(L_{ki}\cdot C_{ki}\cdot T_k) \tag{1}$$

$$L_{ki}=\frac{\sum_{n=1}^{COU_{ki}}tr_{ki}(n)\cdot\omega_n}{COU_i} \tag{2}$$

$$C_{ki}=\frac{\sum_{j\in U_{ki}}L_{kj}\cdot L_{ij}}{\sqrt{\sum_{j\in U_{ki}}L_{kj}}\sqrt{\sum_{j\in U_{ki}}L_{ij}}} \tag{3}$$

$$w_n=\cos\left(\frac{\pi(t_r-t_n)}{2T_{\max}}\times\gamma\right) \tag{4}$$

在式(1)中，U_i 是所有与节点 i 进行过交易并给出评价的节点；L_{ki} 是节点 k 对节点 i 的信任评价；C_{ki} 是节点 k 与节点 i 的相似度。在式(2)中，COU_i 是网络中所有节点与节点 i 交易过的总次数；COU_{ki} 是节点 k 与节点 i 的交易总次数；$tr_{ki}(n)$ 是节点 k 第 n 次对节点 i 的交易评价。在式(3)中，U_{ki} 是同时与节点 k 和节点 i 交易过的节点集。在式(4)中，w_n 是时间权重函数；$T_{\max}$ 为节点所能容忍或记忆的最大时间；t_r 为当前时间；t_n 为交易时间；γ 为衰减速度，当 γ 为 0 时不衰减。引入时间权重主要是因为主体交易的时间对交易的评估具有重大影响，距离当前时刻越近的交易对信任的计算影响越大，将交易时间作为计算信任的因素，使模型具有时间衰减特性。在计算节点的信任值时采用余弦函数模拟节点对历史信任的遗忘过程。上述时间函数是可以调整的，如果不希望考虑时间权重，只要把 γ 设为 0 即可。

3.2 节点信任的不确定性计算

EigenTrust 模型仅通过信任值对节点的信任情况进行度量，忽略了信任的模糊性。云模型通过 3 个数字特征可以更全面地反映节点的信任情况，通过期望反映节点的平均信任情况，通过熵和超熵反映节点信任的模糊性。在一个节点数为 n 的网络中，节点 i 的全局信任值可以根据交易的历史记录，按式(1)~式(4)进行迭代计算得到，在计算过程中将每个 $L_{ki}\cdot C_{ki}\cdot T_k$ 作为逆向云算法的输入，可以得到该节点的信任云的 3 个数字特征。CloudBT 信任评价流程如图 1 所示。

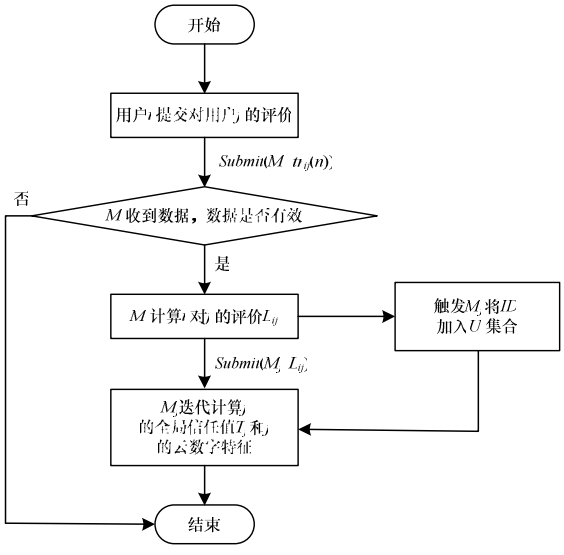

图 1 CloudBT 信任评价流程

算法 2 信任值及不确定性计算算法

Step1 节点 i 与节点 j 交易后向 i 的信任值管理者 M_i 提交数据：

$Submit(M_i, tr_{ij}(n))$。

Step2 i 的信任管理者 M_i 收到数据时，更新 L_{ij}，触发 M_j 将 ID_i 加入集合 U_j 和 M_j 计算节点 j 的全局信任过程：

(1)验证 $tr_{ij}(n)$ 的合法性；

(2)通过式(2)和式(4)计算 L_{ij}；

(3) $Submit(M_j, L_{ij})$。

Step3 M_j 迭代计算 j 的全局信任值并计算 j 的 3 个云参数：

For (every $k \in U_j (k \neq j)$； m: 1 to $length(U_j)$){

$Query(M_k, T_k, L_{kj})$；

按式(3)计算节点 k 与节点 j 的相似度 C_{kj}；

$T_j \leftarrow T_j + L_{kj} C_{kj} T_k$；

$num[] = L_{kj} C_{kj} T_k$； }

Step4 计算节点 j 的 3 个云参数：

将 $num[]$ 作为算法 1 的输入，计算节点 j 的 3 个云参数。

在算法中用到的 2 个原语含义分别如下：

(1) $Submit(M_i, data_{ik})$：将节点 i 对节点 k 的信任评价的数据 $data_{ik}$ 提交到 i 的信任值管理者节点 M_i [2-3](这里的信任值管理者节点的选取采用文献[3]的方法，M_i 保存节点 i 的所有交易记录)，数据 $data_{ik}$ 的具体含义由上下文决定。

(2) $Query(M_i, T_i, L_{ik})$：查询节点 i 的全局誉值 T_i 和 i 对 k 的局部信誉评价 L_{ik}。

值得注意的是，在信任值计算中样本总数 n 尽可能大，n 越大逆向云发生器产生的误差就越小。

3.3 信任决策

主体 A 是否与服务提供主体 B 进行交易，取决于主体 A 对主体 B 的信任程度。一般基于信誉的信任模型仅按信任值由高到低的顺序选取节点进行交易，在本文模型中综合考虑节点的信任值以及节点行为的波动性，更全面地判断节点的信任情况。

具体的信任决策如下：在本文模型中每个节点都有一个二元组属性<信任值，超熵>，在实际工程应用当中可以设置一个可接受的信任值阈值 δ 和超熵 H_e 的阈值 ε (本文设 δ 为 0.5，ε 值可以具体调整)。当节点 i 发起一个交易请求时，满足条件的节点做出反应，即如果服务提供主体中存在信任值大于 δ 且超熵小于 ε 的节点 $R' = \{P_i^{'}, P_i^{'} \in R \& T_i \geqslant \delta \& H_e \leqslant \varepsilon\}$，通常情况下，返回的 R' 中包含很多节点，此时并没有达到信任决策的目的，这时大部分简单的做法是按信任值的大小顺序选取节点进行交易。本文提出一种根据信任值的变化率情况进行信任决策，具体实现如下：

在本文模型中保存各节点在各时刻的信任值，即节点 i 历史信任记录为 $T_i = \{T_{t_0}, T_{t1}, \cdots, T_{t_n}\}$，节点 i 在 t_0 时刻到 t_1 时令的变化率为 $rate_{i_0} = \dfrac{T_{t_1} - T_{t_0}}{t_1 - t_0}$，同理可以计算节点 i 在 t_1 时刻到 t_2 的变化率，由此可以得到节点 i 的变化率为 $rate_i = \{rate_{i_0}, rate_{i_1}, \cdots, rate_{i_{n-1}}\}$。然后由 $rate_i$ 的各个元素根据算法 1 计算 $rate_i$ 的期望和超熵 $\{Ex_{rate_i}, He_{rate_i}\}$，$Ex_{rate_i}$=0 表示节点 i 信任值无变化；Ex_{rate_i}>0 表示节点 i 的信任值在提升，它的绝对值越大升得越快；Ex_{rate_i}<0 表示节点 i 的信任值在降低，同样绝对值越大降得越快，此时可以选取 Ex_{rate} 大且 He_{rate_i} 小的节点进行交易。

如果网络中不存在信任值大于 δ 且熵小于 ε 的节点，则说明该网络节点提供低质的服务且不稳定，如果要进行交易则需更加小心，只能选择信任值较高且超熵相对较小的节点。应该优先选择 R' 中的节点进行交易，因为这些节点能够提供稳定且质量较高的服务。

4 模拟实验及分析

为验证本文模型的效果，本文构建了一个仿真平台模拟 P2P 网络环境，该平台基于斯坦福大学开发的 Query Cycle Simulator 开发包[7]。在该开发包中，每次仿真由若干个周期组成，每个周期内网络中的某个节点随机地发出一个交易请求后等待，收到该请求信息并符合条件的节点对它做出响应，该节点按照上述的信任决策选择节点进行交易。本文网络节点数取 100 个，恶意节点和高可信节点的邻居节点数为 5，普通节点的邻居节点数为 3，拥有邻居节点数越多意味着越可能被查询到，进行交易的机会就越大。

在信任模型中最主要的 2 个性能指标就是成功交易率和对抗攻击能力，本文对这 2 个方面进行实验。

4.1 成功交易率验证

成功交易率是指正常节点的成功交易次数占节点总交易次数的比率，它是信任模型最主要的性能指标之一，在本次实验中主要验证存在恶意节点时的系统成功交易率，并与 EigenTrust、随机情况进行比较。为了简化实验，假设恶意节点提供的服务和评价是不真实的。图 2 给出了网络中恶意节点数占总节点数的 40%时成功交易率。可以看出即使存在大量的恶意节点，本文模型仍具有较高的成功交易率，而随机的成功交易率一直很差。

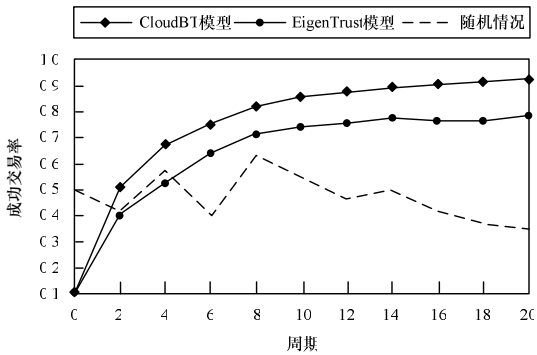

图 2 信任模型的成功交易率比较

4.2 抗攻击能力验证

系统在经过一定的交易后，正常节点将获得较高的信任值，因此被选作交易对象的可能性就增大，网络中的交易成功率可以维持在较高的水平。在本文实验中，用节点的失败交易次数随仿真周期的变化反映模型的抗攻击能力，因为在本文系统中如果恶意节点 i 的信任值小于正常节点 k 信任值以较大的概率出现，那么本文系统的抗攻击能力就能得到验证，因为节点首先会选择信任值高的节点为首选交易对象。如果经过较小的周期，网络的失败交易次数就接近 0，说明模型的抗攻击能力比较强。从图 3 可以看出，本文模型以较小的周期就可以遏制失败交易的发生。 (下转第 145 页)