一种基于主观逻辑理论的 P2P 网络信任模型*)

姚寒冰　胡和平　卢正鼎　黄保华　李瑞轩
(华中科技大学计算机学院　武汉 430074)

摘　要　由于 P2P 系统的开放、匿名等特点,使得 P2P 系统对节点缺乏约束机制,节点间缺乏信任。针对以上问题本文提出了一种基于主观逻辑理论的 P2P 网络信任模型,并在信任的计算中引入风险的机制,有效防止协同作弊和诋毁的安全隐患。实验和分析结果表明,这种信任模型能更加精确地评估节点的信任度,从而能更加有效地解决 P2P 网络环境中存在的安全问题。

关键词　P2P,信任,主观逻辑,声誉,风险

A Trust Model Based on the Subjective Logic Theory for P2P Network

YAO Han-Bing　HU He-Ping　LU Zheng-Ding　HUANG Bao-Huang　LI Rui-Xuan
(College of Computer Science, Huazhong University of Science and Technology, Wuhan 430074)

Abstract　Trust manage is new and important for security in peer-to-peer system. However, the feature of the peer-to-peer system such as user anonymity, open nature makes that peers are not responsible for their irresponsible bartering history. In order to resolve the security problems of P2P network, in this paper we develop a trust model based on the subjective logic theory, and a definition of risk is presented. By doing this, we can evaluate the trust relationships between peers more precisely, thus can resolve security problems exist in P2P network more effectively, which can be verified by simulated experiments.

Keywords　P2P, Trust, Subjective logic, Reputation, Risk

1　引言

P2P 技术是一种新兴的不依赖服务器的分布式网络模型,在对等计算、信息共享、分布式搜索等领域有着广泛的应用前景。它通过系统间对等点的直接交换实现网络信息和资源的共享,在这种网络中所有的节点都是对等的,真正实现了网络间的平等沟通[1]。虽然目前的 P2P 应用日益广泛,但仍然缺乏有效的机制以提高系统整体的可用性,这非常显著地表现为应用中大量欺诈行为的存在以及不可靠的服务质量[1]。

对于 P2P 应用来说,由于平台的灵活性和自由性,实体加入和离开的自由性,导致 P2P 应用无法要求实体提供关键认证信息,只能对实体进行注册登记而无法进行严格的认证。P2P 应用不适合使用基于 PKI 和数字证书的认证技术,在无法通过证书认证确定实体是否可信任的情况下,需要其他方式提供同样的功能[2]。一种普遍被采用的方法是对实体评定信任等级,通过信任的传递和传播,实体可以获得目标实体先前的历史经验,据此选择可靠的交易对象,或选择更安全的资源服务对象。

分析现有的信任模型,大多模拟社会学、心理学中的信任关系[3]。在社会网络中,信任关系是人际关系的核心,个体间的信任度往往取决于其他个体的推荐,同时,作为推荐者的可信度也决定其推荐个体的可信度。这种互相依赖的信任关系组成了信任网络[4]。在这样的信任网络中,任何实体的可信度都不是绝对可靠的,但可以作为其他实体决定其交互行为的依据。这类信任模型实际上是基于实体声誉的,反映一个实体过去长期的行为,能为没有直接接触的实体提供信任值[5,6]。它存在两个明显的弱点:第一,不能有效防止协同作弊和诋毁的安全隐患。协同作弊是指多个实体互相为对方提供过高的推荐值,从而破坏整个系统的可用性;诋毁是指恶意实体通过给予其他实体不真实的较低评价从而对系统造成间接损害。这种安全隐患在 P2P 网络环境下尤为突出。第二,声誉是一个长期积累的值,它的改变需要一段时间,不能快速反映实体近期的行为。针对以上问题,我们提出了一个新的信任模型,在该模型中,实体利用自己的交易经验和系统中其它实体的推荐,对和自己将要交易的实体进行信任度评估,并在信任的评估中引入风险的机制,使节点的信任度能反映其近期行为,同时有效防范协同作弊和诋毁的安全隐患。

本文第 2 节介绍 Jϕsang 主观逻辑理论;第 3 节对我们提出的信任模型作了详细描述,给出了信任值的计算方法;第 4 节对该模型进行了实验模拟,同时对实验结果作了分析说明;最后是结论和将来需要进一步的研究工作。

2　主观逻辑理论

Jϕsang 提出的主观逻辑(Subjective Logic)理论[7],其实质利用了证据理论(Dempster-Shafer 理论)[8],但传统证据理

*)本课题得到国家自然科学基金(60403027)资助。姚寒冰　博士研究生,主要研究方向为分布式系统安全,网格计算。胡和平　教授,主要研究方向为软件工程,数据挖掘,网络安全等。卢正鼎　教授,博士生导师,主要研究方向为软件工程,工程数据库,系统集成。黄保华　博士研究生,主要研究方向为分布式系统安全,对等计算。李瑞轩　副教授,主要研究方向为系统集成,分布式系统安全,Web 数据管理,语义网,对等计算,边缘计算。

论在信任传递与合成时，会得出与人们的常识推理相悖的结论[9]，主观逻辑克服了这一缺陷。Jϕsang 在主观逻辑理论的基础上对信任管理进行了研究，提出了证据空间（Evidence Space）和观念空间（Opinion Space）的概念来描述和度量信任关系，以描述二项事件的后验概率的 Beta 分布函数为基础，给出了一个由观察到肯定事件数和否定事件数来确定概率确定性密度函数，并以此为基础计算节点之间产生的每个事件的概率的可信度，提供了一套主观逻辑运算子用于信任度的推导和综合计算。Jϕsang 模型也无法有效地消除大规模的 P2P 应用中协同作弊和诋毁的安全隐患。

证据空间由一系列节点产生的可观察到的事件组成，节点产生的事件被简单地划分为肯定事件（positive event）和否定事件（negative event）。观念空间则由一系列对陈述的主观信任评估组成，主观信任度由三元组 $\omega_B^A = \{b_B^A, d_B^A, u_B^A\}$ 描述，该三元组满足：

$$b_B^A + d_B^A + u_B^A = 1, b_B^A, d_B^A, u_B^A \in [0,1]$$

其中 ω_B^A 即为节点 A 对 B 的主观观念，b_B^A, d_B^A, u_B^A 分别描述节点 A 对 B 的信任程度、不信任程度和不确定程度，Jϕsang 使用如下公式将 ω 定义为事实空间中肯定事件数 r 和否定事件数 s 的函数：

$$\begin{cases} b_B^A = r/(r+s+2) \\ d_B^A = s/(r+s+2) \\ u_B^A = 2/(r+s+2) \end{cases} \quad (1)$$

该函数称为证据映射函数（Evidence Mapping），Jϕsang 在文[7]中给出了该公式的合理性证明。

推荐算子⊗：设 $\omega_B^A = \{b_B^A, d_B^A, u_B^A\}$，$\omega_C^B = \{b_C^B, d_C^B, u_C^B\}$

则 $\omega_C^{AB} = \{b_C^{AB}, d_C^{AB}, u_C^{AB}\}$，$\begin{cases} b_C^{AB} = b_B^A * b_C^B \\ d_C^{AB} = b_B^A * d_C^B \\ u_C^{AB} = d_B^A + u_B^A + b_B^A * u_C^B \end{cases}$ (2)

记为 $\omega_C^{AB} \equiv \omega_B^A \otimes \omega_C^B$，推荐算子可用来计算信任的传递。

合意算子⊕：设 $\omega_C^A = \{b_C^A, d_C^A, u_C^A\}$，$\omega_C^B = \{b_C^B, d_C^B, u_C^B\}$，$k = u_C^A + u_C^B - u_C^A * u_C^B$，$\gamma = u_C^B / u_C^A$

则 $\omega_C^{A,B} = \{b_C^{A,B}, d_C^{A,B}, u_C^{A,B}\}$

$$\begin{cases} b_C^{A,B} = (b_C^A * u_C^B + b_C^B * u_C^A)/k \\ d_C^{A,B} = (d_C^A * u_C^B + d_C^B * u_C^A)/k \quad k \neq 0 \\ u_C^{A,B} = (u_C^A * u_C^B)/k \end{cases}$$

$$\begin{cases} b_C^{A,B} = (\gamma * b_C^A + b_C^B)/(\gamma+1) \\ d_C^{A,B} = (\gamma * d_C^A + d_C^B)/(\gamma+1) \quad k = 0 \\ u_C^{A,B} = 0 \end{cases} \quad (3)$$

记为 $\omega_C^{A,B} \equiv \omega_C^A \oplus \omega_C^B$，在信任推荐时，可能存在多条推荐路径，通过合意算子融合多个推荐信任值，综合评价节点的信任度。

3 信任模型

针对第 2 节中提到的基于节点声誉的信任模型弱点，本文引入风险的概念，风险反映节点近期的一个时间段不可靠的程度，如图 1 所示，信任由声誉与风险两部分构成，声誉由推荐信任和直接信任构成。图 1 中 α、β 代表权重，根据应用的要求和实际的运行情况，通过调整声誉与风险的权重，使信任度侧重节点长期行为或短期行为，通过增加风险的权重，信任值就能快速反映节点近期的行为，由于风险来源于直接交往行为，从而也能防止协同作弊和诋毁。首先介绍本文用到的几个概念：

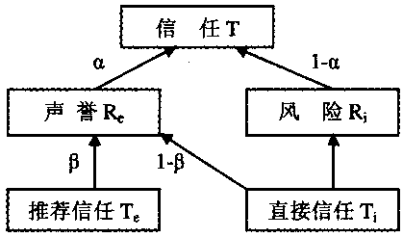

图 1 信任的结构

信任 T：是对一个节点行为的可信度的评估，与这个节点的可靠性、诚信和性能有关，信任是一个主观概念，取决于经验，用信任值来表示信任等级的高低，信任值随节点的行为而动态变化。

直接信任 T_i：指两个节点间根据近期相互间发生的直接交往行为而得出的信任等级关系，信任值来源于根据双方的交易情况得出的直接经验。

推荐信任 T_e：指两个节点之间没有进行过直接的交易，而是根据其他节点的推荐建立的一种信任关系，它们之间的信任值是根据其他节点的评估得出的结果。

声誉 R_e：反映节点长期的行为，由直接信任和推荐信任来计算。

风险 R_i：反映节点近期的不可靠程度，源于节点间直接交往的经验，本文简单地根据直接信任来计算。

3.1 信任模型定义

定义 1 信任关系 TR：$TR = (A, B, C, V, r, s, t)$，$A, B$ 是 P2P 网络中的两个节点，C 是信任关系的分类，根据实际应用的需求而定，V 是信任度，r 是节点交互经历中肯定事件的数量，s 是节点交互经历中否定事件的数量，t 是信任关系的时间约束。TR 表示节点 A 对节点 B 关于信任关系 C 的信任度为 V。

3.2 信任值的计算

直接信任度 T_i 与风险 R_i：设 $\omega_B^A = \{b_B^A, d_B^A, u_B^A\}$ 代表节点 A 对 B 的主观看法，该主观看法来自于节点 A 与 B 的直接交互历史，设 r 为节点 A 与 B 在最近某个固定时间 t 内（t 随具体应用而定）交易成功的次数，s 为交易失败的次数。按公式（1）计算 ω_B^A，如果节点 A 与 B 没有直接交互，则 $\omega_B^A = \{0, 0, 1\}$。取节点 A 对 B 的观念空间中的信任程度为直接信任度，即 $T_i = b_B^A$，风险 $R_i = 1 - b_B^A$。

推荐信任度 T_e：是其它节点对目标节点的一种综合评价，可通过公式（2）、（3）计算任意复杂结构的推荐信任，图 2 显示两种计算推荐信任的基本结构：信任传递与信任合成。取合成后的观念空间的信任程度为推荐信任度。

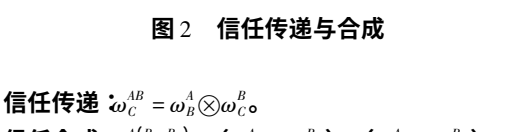

图 2 信任传递与合成

信任传递：$\omega_C^{AB} = \omega_B^A \otimes \omega_C^B$。

信任合成：$\omega_C^{A(B_1,B_2)} = (\omega_{B_1}^A \otimes \omega_C^{B_1}) \oplus (\omega_{B_2}^A \otimes \omega_C^{B_2})$。

在 P2P 网络中计算推荐信任度时，可能存在多条到目标节点的推荐路径，这些推荐路径最终组成一个推荐网络，通过信任传递与信任合成能计算任意复杂的推荐网络的推荐度，计算时先将网状的推荐路径转化为并行结构的推荐路径，考

虑到性能问题，可以在路径转换时作一些优化处理。图 3 显示网状的推荐路径向并行结构推荐路径的转换，信任合成表达式为：

$$\omega_C^{A(B_1B_4,B_2B_4,B_2B_5,B_3)} = (\omega_{B_1}^{A} \otimes \omega_{B_4}^{B_1} \otimes \omega_C^{B_4}) \oplus (\omega_{B_2}^{A} \otimes \omega_{B_4}^{B_2} \otimes \omega_C^{B_4}) \oplus (\omega_{B_2}^{A} \otimes \omega_{B_5}^{B_2} \otimes \omega_C^{B_5}) \oplus (\omega_{B_3}^{A} \otimes \omega_C^{B_3})$$

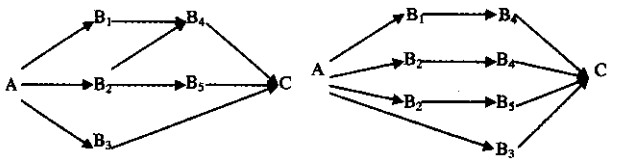

图 3　推荐网络的转化

声誉 R_e：$R_e = \beta T_e + (1-\beta) T_i$，$0 \leqslant \beta \leqslant 1$。

声誉值是目标节点长期行为的积累，在 P2P 网络环境下，β 应设为一个较低的值，因为节点的动态性和不确定性，不能过于依靠其它节点的推荐信任值，另外，过于依赖推荐信任值，将很难防止协同作弊和诋毁的安全隐患。

信任 T：$T = \alpha R_e + (1-\alpha) R_i$，$0 \leqslant \alpha \leqslant 1$。

增加 α 的值，信任侧重反映节点长期行为，$\alpha = 1$ 即为基于声誉的信任模型。仿真试验表明，风险在动态变化的 P2P 网络环境中非常重要，能有效防止协同作弊和诋毁的安全隐患，在 P2P 网络环境中 α 应设为一个较大的值。

4　仿真试验及结果分析

本文提出的信任模型引入了风险的概念，有效地解决了 P2P 网络环境的信任模型中存在的协同作弊和诋毁的安全隐患。为了验证该模型的有效性，我们进行了模拟实验。

4.1　实验场景

在实验中，P2P 网络提供文件共享服务，即用户从节点上下载共享的文件，下载文件的真实性是其判断一次交互是否成功的惟一标准。假设节点有两类：一类是诚实的节点，即它提供真实可信的文件下载服务；一类是不诚实的节点，即它有可能提供一个假文件下载服务，也有可能根本就不提供文件下载服务，也可能在下载的文件中含有恶意代码（例如病毒）。

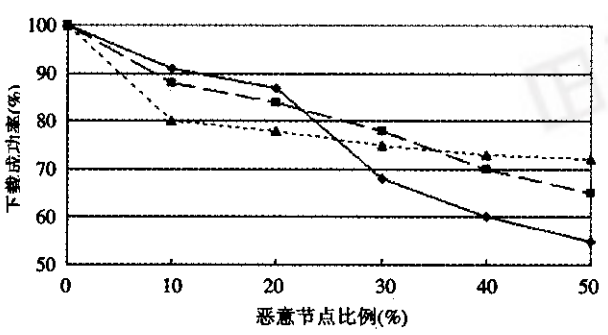

图 4　α，β 不同权重对信任值的影响

4.2　实验设计与结果

实验表明完全忽略风险的作用容易受到攻击者的攻击，因为任何一个非法用户都可以提交一个错误的评估来影响整个评估系统的准确性。本文所采用的计算方法不容易受这种攻击的影响并且能更准确地反映节点之间的信任关系。实验结果如图 4 所示，分为 3 种情况进行实验，情况 1：$\alpha = 1$，$\beta = 0.2$，该情况下忽略风险 R_i，侧重直接信任度 T_i，相当于完全基于声誉的信任系统；情形 2：$\alpha = 0.7$，$\beta = 0.2$，考虑风险 R_i 影响，侧重直接信任度 T_i；情形 3：$\alpha = 0.3$，$\beta = 0.2$，侧重风险 R_i 与直接信任度 T_i。

4.3　结果分析

从如图 4 所示的实验结果可以看出，P2P 网络环境中，不诚实用户的比例小于 20% 的情况下，情况 1 的下载成功率较高，由于没有考虑风险的影响，信任值能更快地趋于稳定，在不诚实节点所占比例小较小的情况下，信任值比较真实，能获得较高的下载成功率；而不诚实节点的比例超过 20% 时，情况 1 的下载成功率下降很快，而情况 2、3 的成功率相对稳定，因为随着不诚实节点的增加，情况 1 取得的节点信任值不太真实，而情况 2、3 中考虑了风险的影响，能反映节点近期行为，在节点近期出现恶意行为的情况下，快速调整其信任值，保证维持较高的下载率。比较情况 2、3，情况 2 考虑风险的影响，但赋予风险比较低的权重，情况 3 则侧重风险，赋予风险很高的权重，在不诚实节点低于 30% 时，情况 2 取得较高的成功率，情况 3 的信任值波动较大，下载成功率较低；不诚实节点较高时，情况 3 能取得可靠的信任值，取得了较高的下载成功率。

从实验分析可以看出，在 P2P 网络环境中，风险机制的引入，对防范协同作弊和诋毁的安全隐患起到较好的效果，考虑到信任值的稳定性，应赋予风险较低的权重。

结论　安全问题是 P2P 网络中被关注的一个重点，研究 P2P 中的信任关系具有非常大的现实意义。本文提出基于主观逻辑的 P2P 网络信任模型，利用主观逻辑理论来计算信任的传递与合成，在信任评估中引入了风险的机制，有效防止协同作弊和诋毁的安全隐患。本文的风险机制过于简单，在下一步研究工作中拟引入更复杂的风险机制，更好地解决 P2P 中的信任问题。

参 考 文 献

1　Ramaswamy, Freeriding Liu L. A new challenge for peer-to-peer file sharing systems. In：36th Annual Hawaii International Conference on System Sciences (HICSS236), 2003

2　Chen R, Poblano Y W. A distributed trust model for P2P networks：[Technical Report, TR-I4-02-08]. Palo Alto：Sun Microsystem, 2002

3　Khare R1. Rifkin A. Weaving a Web of trust. World Wide Web, 1997, 2(3)：77～112

4　Scott J. Social Network Analysis：A Handbook. 2th ed. SAGE Press, 2000. 87～236

5　Resnick P, Zeckhauser R, et al. Reputation systems. Communications of the ACM, 2000, 43(12)

6　Kamvar S D, Schlosser M T. EigenRep：Reputation management in P2P networks. In：Lawrence S, ed. Proc. of the 12th Int 'l World Wide Web Conf. Budapest：ACM Press, 123～134

7　Josang A. A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001, 9(3)：279～311

8　Zadeh L A. Review of Books：A Mathematical Theory of Evidence. AI magazine, 1984, 5(3)：81～83

9　Mui L, Mohtashemi M, Halberstadt A. A Computational Model for Trust and Reputation. 35th Hawaii International Conference on System Sciences