

一种 P2P 网络服务环境的信任度计算模型

刘凤鸣¹, 陆星家¹, 丁永生^{1,2}

(1. 东华大学 信息科学与技术学院, 上海 201620; 2. 东华大学 数字化纺织服装技术教育部工程研究中心, 上海 201620)

(liufm69@mail.dhu.edu.cn)

摘要:首先依据新实体能力属性给出了初始信任度计算算法,然后根据实体的直接交互满意度与其他信任实体的推荐信息,设计了直接信任度和推荐信任度计算算法。综合三种信任度,提出了信任度计算模型。该模型为网络实体间信任关系的建立和信任行为的决策提供了有力依据,从而减少实体交互风险,提高网络运行稳定性。

关键词:P2P 网络;信任;信任度;能力属性;满意度

中图分类号: TP309; TP393 **文献标志码:** A

Computation model for trustworthiness in P2P network service environment

LIU Feng-ming¹, LU Xing-jia¹, DING Yong-sheng^{1,2}

(1. College of Information Sciences and Technology, Donghua University, Shanghai 201620, China;

2. Engineering Research Center of Digitized Textile and Fashion Technology, Ministry of Education, Donghua University, Shanghai 201620, China)

Abstract: An algorithm to compute an initial trust value for the new entities based on its capability was presented, and then the computation algorithms of direct trustworthiness based on the degree of interaction satisfaction were designed. The recommendation trustworthiness based on the recommendation opinions came from trusted entities. Finally, the integrated trustworthiness computation model was given. Based on this model, the trust relationships can be built among entities in P2P network service environment and the decision of trust can be made based on the trustworthiness, and the risk can be reduced and the stability of network can be promoted.

Key words: P2P network; trust; trustworthiness; capabilities attribute; degree of satisfaction

0 引言

P2P 网络是一个分布的、动态的自组织系统,实体是自治的,可以自由地进入与退出网络,而且实体行为无权威中心或可信第三方进行管制^[1]。实体之间难以建立确定的信任关系。如何考查实体的可信性,实现共享、协作,控制恶意网络行为成为当前研究的热点问题。

文献[2]最早借鉴了社会学等学科对信任的研究,将信任进行了量化计算。文献[3]定义了信任量化框架,使实体之间的关系明确化^[3]。文献[4-8]分别建立了各自的实体信任度评估模型,将信任关系以信任度为标度进一步加以明确。

信任度评估主要涉及两个问题^[4]:1) 信任的表述和度量;2) 信任度推导和计算算法。

在文献[5]的信任度评估模型中,引入了经验的概念来表述和度量信任关系,经验被定义为对某个实体完成交互的情况记录,分为肯定经验和否定经验。文献[5]在其模型中对直接信任和推荐信任进行了详细的讨论,最后给出了信任度推导和计算模型。

在文献[6-8]的信任度评估模型中,引入了事实空间(Evidence Space)和观念空间(Opinion Space)的概念来描述和度量信任关系。事实空间由一系列实体产生的可观察到的事件组成,观念空间则由一系列对陈述的主观信任评估组成。实体产生的事件被简单地划分为肯定事件和否定事件。文献

[7]给出了一个由观察到的肯定事件数和否定事件数决定的概率确定性密度函数,并以此来计算实体产生某个事件的概率的可信度。主观信任度为陈述的信任程度、不信任程度和不确定程度之和。文献[8]的信任度评估模型提供了一套主观逻辑算子(合并、合意和推荐)用于信任度之间的运算。

文献[9]引入模糊集合论中隶属度的概念描述信任的模糊性,在概念树的基础上对信任综合评价获得信任值,在信任推导规则中考虑了信任关系的合成权重,但没有考虑信任值的更新。

文献[10]使用概率统计学中假设检验的思想,采用成功经验和失败经验对信任关系进行度量,并给出了直接信任度计算公式。用经验采纳系数来表示对推荐者所推荐的经验的不同采纳程度,并给出了一个符合一般事实的经验传递和综合计算公式。

在现有的信任度评估模型,几乎都忽略了新实体的信任度评估,也很少考虑恶意推荐或串谋推荐的安全风险,更没能很好地体现节点作为服务实体的个体特征。不仅使新实体难以很好地融入网络,也不能很好地满足动态服务环境的安全需求。

本文基于实体能力属性和交互满意度提出了一种信任度评估模型。首先考虑到新实体没有信任度可以获得已存在实体的认可,不能进行直接交互活动,定义了实体属性集,并对其进行了量化,给出了实体初始信任度的计算算法;对网络已存在实体,提出了交互满意度的概念,并以此计算实体的直接

收稿日期:2007-09-12; **修回日期:**2007-11-23。 **基金项目:**国家自然科学基金资助项目(60534020;60474037);教育部新世纪优秀人才支持计划(NCET-04-415);教育部科技创新工程重大项目培育资金项目;上海市国际科技合作基金项目(061307041)。

作者简介:刘凤鸣(1969-),男,山东胶州人,博士研究生,CCF 会员,主要研究方向:网络智能、信息安全; 陆星家(1979-),男,安徽芜湖人,博士研究生,主要研究方向:智能服装、无线网络; 丁永生(1967-),男,安徽怀宁人,教授,博士生导师,博士,主要研究方向:智能系统、网络智能、DNA 计算、人工免疫系统、生物网络结构。

信任度;为避免恶意推荐的风险,在计算推荐信任度时,通过建立信任路径来获取信任链上实体的推荐信息。依据信任度,实体之间可以通过信任认证、信任传播建立不同程度的信任关系,形成信任网络和信任社区,实现可信服务。

1 信任度计算模型

网络中实体用三元组 $E(A, R, T)$ 来表示。其中, A 为实体能力属性集, R 为交互记录集, T 为信任度集, 包括初始信任度、直接信任度和推荐信任度。实体的属性集根据实体提供的服务类型进行设定, 同类型服务的实体具有相同的能力属性集。

1.1 初始信任度

对于提供某类型服务的新实体, 如图 1 中所示 A, B, C, D, E 等, 设初始信任度为 0。

定义提供某类型服务的新实体的属性集为 $A(a_1, a_2, \dots, a_n)$, a_i 表示实体的第 i 个属性。对属性 a_i 分级, 设共分为 m_i 级, 每一级对应一数值 x_{ij} ($j = 1, \dots, m_i$), $x_{i1} = m_i, \dots, x_{im_i} = 1$ 。表 1 给出了某类服务实体的能力属性值表。

表 1 实体的能力属性值表

属性 a_1	值	属性 a_2	值	...	属性 a_n	值
标准 1	m_1	标准 1	m_2	...	标准 1	m_n
标准 2	$m_1 - 1$	标准 2	$m_2 - 1$...	标准 2	$m_n - 1$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
标准 m_1	1	标准 m_2	1	...	标准 m_n	1

相同服务类型的实体的每一属性都会在表中找到相对应级别的值 $x_{ij} = m_i - j + 1$ 。实体的不同属性对于实体信任度评估的影响是不同的, 所以对每一属性设权重值为 w_i ($0 < w_i < 1$), w_i 随属性对实体信任度的影响同向变化。综上所述, 新实体的初始信任度计算公式如下:

$$T_{\text{init}} = \sum_{i=1}^n w_i x_{ij} \quad (1)$$

其中, T_{init} 为初始信任度, $1 \leq j \leq m_i$ 。

依据初始信任度, 新实体可以较快地融入网络, 同其他实体建立初步的信任关系, 提供或消费服务。

1.2 直接信任度

对于网络中任意两个有直接交互的实体, 如图 1 中的 A, B , 定义实体 A 保存的与实体 B 交互的记录集合为 $R_{A \rightarrow B}(P, F)$, 其中, P 为成功记录集, F 为失败记录集。集合 P 为 $(p, (\alpha_i, t_i))$, 其中 p 为成功记录数, α_i 为第 i ($i = 1, \dots, p$) 条成功记录的满意度, t_i 为第 i ($i = 1, \dots, p$) 条成功记录的发生时间; 集合 F 为 $(f, (\beta_j, t_j))$, 其中 f 为失败记录数, β_j 为第 j ($j = 1, \dots, f$) 条失败记录的不满意度, t_j 为第 j ($j = 1, \dots, f$) 条失败记录的发生时间。首先考虑交互记录的时效问题, 也就是说距离当前时间越近交互记录越有参考性, 设第 i 条成功记录的时效值为 $\Delta t_i^{\text{succ}} = t_{\text{curr}} - t_i + 1 \dots (i = 1, \dots, p)$; 第 j 条失败记录的时效值为 $\Delta t_j^{\text{fail}} = t_{\text{curr}} - t_j + 1 \dots (j = 1, \dots, f)$, t_{curr} 为当前日期时间, 加 1 使当日的交互记录的时效值不为 0。对于满意度 α_i , 分为三级: 完全满意、较为满意、一般满意; 对于不满意度 β_j , 同样分为三级: 不满意、很不满意、完全不满意。 α_i 取值范围为 $[0, 1]$, β_j 取值范围为 $[-1, 0]$ 。不失一般性, α_i, β_j 取值如表 2 所示。

这样, A 对 B 的直接信任度 $T_{A \rightarrow B}$ 的计算公式如下:

$$T_{A \rightarrow B} = \sum_{i=1}^p \frac{\alpha_i}{\Delta t_i^{\text{succ}}} + \sum_{j=1}^f \frac{\beta_j}{\Delta t_j^{\text{fail}}} \quad (2)$$

信任度的值可能为正, 也可能为负。在一定的上下文环境下, 允许信任度值为负, 负值越大, 表示不满意的程度越小, 负

值越小, 不满意程度越大。

表 2 α_i, β_j 的取值参考表

满意度 α_i	不满意度 β_j
完全满意 $\alpha_i = 1$	不满意 $-0.5 < \beta_j \leq 0$
较为满意 $1 > \alpha_i \geq 0.5$	很不满意 $-1 < \beta_j \leq -0.5$
一般满意 $0.5 > \alpha_i \geq 0$	完全不满意 $\beta_j = -1$

依据实体间的直接交互记录, 可由公式 (2) 计算出实体的直接信任度。依据信任度值, 做出是否信任的决策, 通过实体间的信任决策进行信任认证, 又因实体信任的非对称性, 从而可用有向图来表示信任网络, 如图 1 所示。

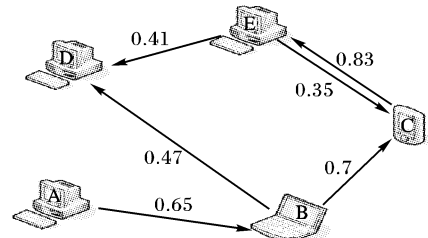


图 1 信任网络

1.3 推荐信任度

对于没有直接交互的实体, 如图 1 (线上标注为直接信任度) 中的 A 与 D , A 不能得到对于 D 的直接信任度。但 D 与网络中的 B, E 有直接交互。因此, A 在考查 D 时就可以参考 B, E 的推荐信息。这里, 为了避免恶意推荐, 只考虑通过信任路径上的实体的推荐信息。所谓信任路径指的是路径上的实体双方有直接交互, 并至少通过单方的信任认证而形成的一条同向信任链。如图 1 所示, A 要考查 D , 有两条信任路径, 分别为: $A \rightarrow B$ 和 $A \rightarrow B \rightarrow C \rightarrow E$ 。这里不考虑自己推荐自己的情况。因此, 在实际网络中, 对于同一个目标实体, 可能存在着多条信任路径上的推荐。这里先讨论单条信任路径上的推荐信任度的计算方法, 然后再对多条取其平均值即可。

假定一条推荐信任路径的长度 m ($m \leq l$), l 是允许的路径长度最大值。设实体 X 要考查目标实体 Y , 第 i ($i \leq m$) 个推荐者为 U , 第 $i-1$ 个推荐者为 V , 第 $i+1$ 个推荐者为 W 。设实体 V 给出的推荐信息为二元组 $(T_{V \rightarrow Y}, T_{V \rightarrow U})$, 实体 U 给出的推荐信息为 $(T_{U \rightarrow Y}, T_{U \rightarrow W})$ 。如果其中某个实体与目标实体没有交互记录, 也就不存在直接信任度, 那么二元组中的第一个元素设为 0。这里有一点需要说明, 推荐路径上最后一个实体的推荐信息二元组的第二个元素为空。二元组中的第二个元素作为采纳系数。这样, 推荐者 U 对 Y 的推荐信任度是 $T_{V \rightarrow U} \times T_{U \rightarrow Y}$ 。考虑到路径长度的影响, 即近距离实体的推荐信任度比远距离实体的推荐信任度更具有参考性, 设置距离影响因子 s 为路径长度的函数, 不失一般性, 可设 $s = 1/i^2$ 。这样, 一条路径上 X 对 Y 的推荐信任度 $t_{X \rightarrow Y}$ 的计算公式为:

$$t_{X \rightarrow Y} = \sum s(T_{V \rightarrow U} \times T_{U \rightarrow Y}) = \sum_{i=1}^m \frac{(T_{V \rightarrow U} \times T_{U \rightarrow Y})}{i^2} \quad (3)$$

假设存在 k 条推荐信任路径, 则推荐信任度 $T_{X \rightarrow Y}$ 为所在路径上推荐信任度和的平均值。

$$T_{X \rightarrow Y} = (\sum t_{X \rightarrow Y}) / k \quad (4)$$

1.4 信任度计算模型

综合初始信任度、直接信任度、推荐信任度, 实体的信任度计算模型:

$$T = \alpha T_{\text{init}} + \beta T_{A \rightarrow B} + \lambda T_{X \rightarrow Y} \quad (5)$$

式中, α, β, λ 分别表示初始信任度、直接信任度、推荐信任度

在实体信任度中所占比重,其中, $\alpha < \lambda < \beta$,且 $\alpha + \beta + \lambda = 1$ 。在有大量交互记录参考的情况下,可以适当降低初始信任度所占比重或不考虑,即可设 $\alpha = 0$;当然,如果需要,可向信任实体征询推荐信息,计算其推荐信任度;对没有直接交互的实体, $\beta = 0$,此时可以根据经验适当设置 α 、 λ 的比重。

系统初始,刚加入到系统内的实体因匿名性等特征彼此互不熟识,当一个节点提出服务请求时,查寻到若干提供同类服务的实体,可以依据实体初始信任度作出选择。假定在文件共享系统中,如Gnutella,当新实体加入时,系统征询其与服务相关的属性信息(如共享文件数、最大带宽、在线时间、最大下载线程……)。系统将这些信息按上述初始信任度算法,就可计算出实体的初始信任值,服务消费者可以依此进行选择。选定实体后,发出服务请求,建立连接,进行交互,并将交互信息保存。通过直接交互记录,可以计算直接信任度,通过直接信任度,可以建立稳定的信任关系,建立信任路径,形成信任网络。

2 仿真

基于实验室的多Agent生物网络仿真平台,我们实现了信任评估模型并进行了仿真实验。实验中的网络节点为平台中的智能生物Agent^[11]。首先,对模型在网络中的收敛性进行了仿真测试,结果如图2所示。结果显示评估算法在网络运行过程中受Agent的动态进入与退出等原因的影响有一定的波动,但总体的结果是趋向收敛稳定的。为了对比实验,我们将Agent分成了两类,一类在运行过程中采用信任评估算法时行服务选择;一类不加任何控制措施,选择服务时采用随机方法,结果如图3所示。随着实验的运行,生物Agent出现了两种不同的走向,采用信任评估的节点在网络中的活性逐渐提高,而另一类节点正好相反,活性逐渐降低,部分死亡而退出网络。图4是在实验中全部生物Agent都采用信任评估算法进行服务选择时,网络运行的稳定性的仿真实验结果,结果同样显示了网络运行的整体趋向是稳定的,性能也在逐步提高。

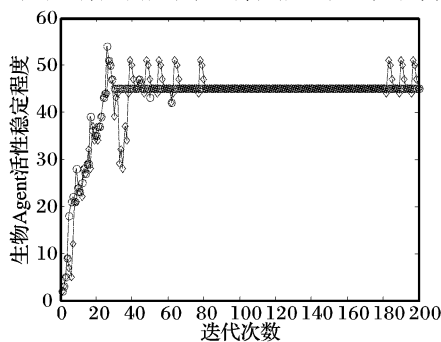


图2 节点信任度评估收敛性仿真结果

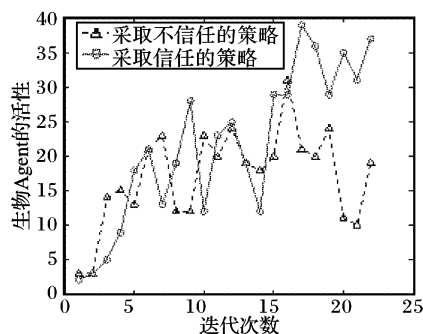


图3 两类节点的分离仿真结果

从实验的仿真结果中可以看出,在开放、分布、无中心控制的网络中,实体之间的交互关系的建立直接影响到网络的安全与稳定。在保证实体匿名性的情况下,信任管理显示出

传统安全措施无可替代的作用。信任评估模型的直接交互记录是实体本地存放,而且是对方的记录信息,因而也不存在修改的风险。对于推荐信任度的计算,采用是信任实体的推荐信息,也不会增加网络的负荷。总的实验结果分析显示信任评估模型对于网络的安全与运行性能起到了良好的作用。

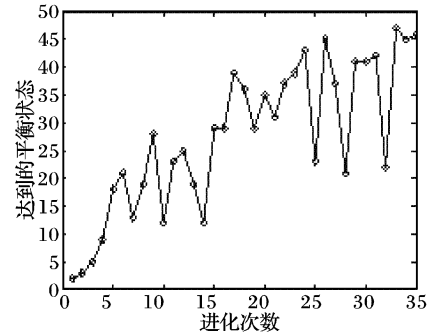


图4 采取信任模型的网络进化稳定性仿真结果

3 结语

本文在总结了多个信任评估模型的基础上,考虑到合理性、实用性、可比性、可操作性,以及实体的个性特征,对实体的服务能力和直接交互进行了量化计算,提出了一种适用于分布式网络服务环境的信任度评估模型。模型考虑了P2P网络动态分布的安全需求,为动态自治的实体进行了量化评估。即使恶意实体重新注册作为新实体加入网络,如果不能提供有效的服务,建立良好的直接交互关系,就不会获得足够的信任度,从而危害到网络安全与稳定。此举既遏止了实体的不良行为,又激励了诚信实体,为网络的安全运行提供了基础。在以后的工作中,还将进一步深入研究信任对于服务资源的可用性、可靠性以及访问控制等方面的应用,以最大限度地保证实体可信、服务可信、网络可信。

参考文献:

- [1] JØSANG A. Prospective for online trust management[J/OL]. [2007-09-02]. IEEE Transactions on Knowledge and Data Engineering, 2007, forthcoming, <http://sky.fit.qut.edu.au/~josang/publications.html>.
- [2] MARSH S. Formalizing trust as a computational Concept [D]. Stirling: University of Stirling, 1994.
- [3] MCKNIGHT D, CHERVANY N. The meanings of trust [R]. MIS-RC 96-04, University of Minnesota, Management Information Systems Research Center, University of Minnesota, 1996.
- [4] 徐锋, 吕建. Web安全中的信任管理研究与进展[J]. 软件学报, 2002, 13(11): 2057-2064.
- [5] BETH T H, BORCHERDING M, KLEIN B. Valuation of trust in open networks [C]// Proceedings of European Symposium on Research in Security (ESORICS). Brighton: Springer-Verlag, 1994: 3-18.
- [6] JØSANG A. The right type of trust for distributed systems [C]// Proceedings of the 1996 New Security Paradigms Workshop. Lake Arrowhead: ACM Press, 1996: 119-131.
- [7] JØSANG A, KNAPSKOG S J. A metric for trusted systems [J/OL]. [2007-09-15]. <http://csrc.nist.gov/nissc/1998/proceedings/paperA2.pdf>.
- [8] JØSANG A. A subjective metric of authentication [C]// Proceedings of ESORICS'98, Louvain-la-Neuve, Belgium: Springer-Verlag, 1998: 329-344.
- [9] 唐文, 陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报, 2003, 14(8): 1401-1408.
- [10] 徐锋, 吕建, 郑玮, 等. 一个软件服务协同中信任评估模型的设计[J]. 软件学报, 2003, 14(6): 1043-1051.
- [11] 张向锋, 任立红, 皋磊, 等. 生态网络仿真平台的能量服务管理[J]. 计算机工程与应用, 2003, 39(31): 145-148.