

可信网络中基于多维决策属性的信任量化模型

李小勇 桂小林

(西安交通大学电子与信息工程学院 西安 710049)

摘 要 可信网络中的信任关系模型本质上是最复杂的社会关系之一,涉及假设、期望、行为和环境等多种因子,很难准确地定量表示和预测. 综合考虑影响信任关系的多种可能要素,提出了一个新的基于多维决策属性的信任关系量化模型,引入直接信任、风险函数、反馈信任、激励函数和实体活跃度等多个决策属性,从多个角度推理和评估信任关系的复杂性和不确定性,用来解决传统量化模型对环境的动态变化适应能力不足的问题;在多维决策属性的融合计算过程中,通过信息熵理论确立各决策属性的分类权重,克服了过去常用的确定权重的主观判断方法,并可以改善传统方法由于主观分配分类权重而导致的模型自适应性不强的问题. 模拟实验表明,与已有同类模型相比,该模型具有更稳健的动态适应性,在模型的安全性方面也有明显的优势.

关键词 可信网络;信任量化模型;信息熵;多维决策属性

中图法分类号 TP311

DOI号: 10.3724/SP.J.1016.2009.00405

Trust Quantitative Model with Multiple Decision Factors in Trusted Network

LI Xiao-Yong GUI Xiao-Lin

(School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049)

Abstract In a trustworthy network system, trust model is one of the most complex concepts in social relationships, and it also is an abstract psychological cognitive process, involving assumptions, expectations, behavior and the environment, and other factors. So, it is very difficult to quantify and forecast trust-ship accurately. In this paper, a novel dynamic trust quantization model with multiple decision factors based on information entropy is proposed, in which multiple decision factors, including direct trust, trust risk function, feedback trust, incentive function and active degree, are incorporated to reflect trust relationship's complexity and uncertainty in various angles. Also, the weight of classification is set up by information entropy theory for these decision factors, which overcomes the shortage of traditional method, in which the weight is set up by subjective manners, and makes the model has a better rationality and a higher practicability. Simulation's results show that, compared to the existing trust quantization metrics, the model in this paper is more robust on trust dynamic adaptability, has remarkable enhancements in the system's security.

Keywords trustworthy network; trust quantitative model; information entropy; multiple decision factors

1 引 言

随着以 Internet 为基础平台的、各种大规模分

布式应用(如网格计算、P2P 计算、电子商务、Ad hoc 和普适计算等)的深入研究,系统表现为由多个软件服务组成的动态协作模型. 在这些动态的和不确定的 Internet 环境下,传统的安全机制中基于

PKI(Pubic Key Infrastructure)的静态信任机制不能适应这些新的应用需求,因此,针对大规模分布式应用的可信网络技术成为一个待解决的热点问题^[1-2].网络可信技术是在原有网络安全技术的基础上增加行为可信的安全新方法,强化了对网络状态的动态处理,为实施智能自适应的网络安全和服务质量控制提供策略基础.然而,从信任关系的内涵来看,其本质上是最复杂的社会关系之一,具有不确定性、不对称性、部分传递性、异步性、上下文独立性和时空减性等一系列复杂的动态属性,是一个抽象的心理“认知”过程,涉及假设、期望、行为和环境等多种因子,很难定量表示和预测.另外,动态信任管理技术是近几年才发展起来的,仍然属于前瞻性研究课题,对很多相关理论和技术性问题都没有形成共识,仍缺乏系统明确的方法论指导,还无法完全解决互联网发展过程中对于信任关系准确度量与预测的需求.因此,系统而深入地开展动态信任关系量化机理的研究,具有重要的现实意义和广阔的应用前景.

信任关系的不确定性是信任评估和可信赖性预测的最大挑战^[2].毋庸置疑,现有的成果^[3-8]有效地推动了相关研究的发展和极大地丰富了人们对信任管理基本问题的理解,但也有本身存在的问题:

(1)大多数模型^[4,6-10]对影响信任量化的决策属性(Decision Factor,DF)考虑不全面,在计算总体信任度时只考虑直接信任与反馈信任的简单的加权平均,而对一些重要的环境上下文考虑不够,特别是影响这些上下文的细节考虑不全面,例如:大多文献没有考虑风险因素、激励因素和节点稳定性程度等因素.由于不注重信任值的环境上下文意义,模型不能很好地刻画信任关系的复杂性和不确定性.

(2)现有的信任评测模型在计算 OTD(Overall Trust Degree)时,主要采用直接信任与间接信任加权平均的方法,而且分类权重采用专家意见法或者平均权值法等主观的方法,致使预测结果带有较大的主观成分,影响了可信决策的科学性,而且缺少灵活性,一旦权值确定,将在实际应用中很难由系统动态的去调整它,致使预测模型缺少自适应性.

针对以上问题,在前期工作的基础上^[2,9,11-15],本文提出了一个多 DF 的动态信任关系量化模型,引入直接信任、信任风险函数、反馈信任、激励函数和实体活跃度等多个 DF 从多个角度刻画信任关系的复杂性和不确定性,对信任关系进行建模时,强调综合考察影响信任的多种 DF,针对信任关系的多

维属性进行更精细的建模.并通过信息熵理论确立各 DF 的分类权重,克服了过去常用的确定权重的主观判断方法,从而使该模型具有更好的科学性和更高的实际应用价值.最后,通过模拟实验对本文模型进行了分析,与其它典型模型相比:本文模型具有更稳健的动态适应性,在模型的安全性方面也有显著改善.

2 相关工作

1996 年,Blaze 为解决 Internet 上网络服务的安全问题,提出了“信任管理”概念,并首次将信任管理机制引入到分布式系统之中.随着以网络为基础的各种大规模分布式应用系统的相继出现和应用,信任关系、信任模型和信任管理的研究逐渐成为信息安全领域中的研究热点.文献[2]综合分析了动态信任的相关概念、主要问题和研究方法,并选取一些新的、典型的动态信任模型及其使用的数学方法进行了评述与比较.

近几年,有些学者研究了多种分布式应用中的动态信任关系,并使用不同的数学方法和数学工具,建立了信任关系度量与预测模型.文献[3]开发了一个具有鲁棒性和伸缩性的 P2P 声誉系统 Power-Trust,该系统利用了幂次法则收集本地节点反馈并将这些反馈聚合起来,生成全局声誉,通过一个“look-ahead”随机行走策略,Power-Trust 系统明显改善了全局声誉的精确性和聚合速度. Peer-Trust^[4]针对平均值算法不能很好地满足信任动态性需求,提出了基于自适应时间窗口的动态信任计算模型和基于个人相似度的信任信息聚合方法 PSM,虽然 PSM 算法在抑止恶意节点的恶意反馈方面有较好的适应能力,但由于自适应时间窗口相对简单,不能有效地反映信任关系的动态变化趋势,影响了信任评价的准确性. PET^[7]在对以前研究工作进行归纳总结的基础上,提出了一种 P2P 文件共享系统的信任关系评估模型,总体信任度(OTD)采取基于风险的直接信任和基于推荐的反馈信任耦合的方式得到,PET 模型首次将风险作为影响信任关系的要素之一引入可信性评估之中,但模型对信任随时间变化的动态属性也没有进行合理的建模.

在国内,文献[8]研究了 P2P 环境下的信任度量模型,通过数理统计方法,引入近期信任、长期信任、惩罚因子和推荐信任 4 个参数来反映节点的信

程度.文献[10]提出了可信网络中一种基于行为信任预测的博弈控制机制,论述了如何利用贝叶斯网络对用户的行为信任进行预测.文献[9]利用机器学习方法研究了动态信任评估模型,算法采用基于规则的机器学习方法,具有从大量输入数据中自学习以获取评估规则的能力.

3 信任关系模型的构建

3.1 相关问题的形式化定义

监控目标网络实体间所有交互的影响、获取和分析各种环境上下文信息是可信访问控制的关键任务之一,动态信任关系建模与评估的主要目标是信任关系的合理量化,而信任关系的量化又是由各种DF确定的,尽管信任是一个非常模糊和不确定心理认知,但是通过DF的获取和量化,可以进行总体信任度的预测、量化和推理^[2].

设 x_1, x_2, \dots, x_N 表示系统中的 N 个实体(节点或者资源), $X = \{x_1, x_2, \dots, x_N\}$, 称为实体域,根据担任角色的不同,实体分为3种类型:(1)服务提供者(Service Provider, SP);(2)服务请求者(Service Requester, SR);(3)反馈者(Feedback Rater, FR).

$\forall x_i$ 评估 $x_j (x_j \in X)$ 的信任程度有 M 项测量指标,分别表示为 $Y_1(x_i, x_j), Y_2(x_i, x_j), \dots, Y_M(x_i, x_j)$, 指标集合表示为 $Y = \{Y_1, Y_2, \dots, Y_M\}$, 其中每一个元素 $0 \leq Y_m(x_i, x_j) \leq 1 (m=1, 2, \dots, M)$ 称为一个决策属性(DF). 设 ω_m 表示第 m 个DF ($Y_m(x_i, x_j)$) 相对于其它DF的重要性程度,并且 ω_m 满足:

$$0 \leq \omega_m \leq 1, \sum_{m=1}^M \omega_m = 1 \quad (1)$$

则称 ω_m 为 $Y_m(x_i, x_j) (m=1, 2, \dots, M)$ 的分类权重.

定义 1. 设 $\Gamma(x_i, x_j, s, t)$ 表示实体 x_i 对实体 x_j 的总体信任评价,称为总体信任度. 令

$$\Gamma(x_i, x_j, s, t) = \sum_{m=1}^M \omega_m Y_m(x_i, x_j) \quad (2)$$

其中 s 是 x_i 提供的服务质量等级, x_j 可以得到的服务类别及质量由它的 $\Gamma(x_i, x_j, s, t)$ 值决定, $\Gamma(x_i, x_j, s, t)$ 的值越高,获得的服务质量也越高; t 是交互时间戳,为了提高信任评估的准确性和动态适应能力,把一段时间分为若干个时间戳,时间戳反映了某一个时刻的信任度,信任度具有随时间变化而衰减的特性.

定义 2. 设对总体信任度 $\Gamma(x_i, x_j, s, t)$ 有 P

个评估等级 c_1, c_2, \dots, c_P , 其中 $0 \leq c_p \leq 1 (p=1, 2, \dots, P)$. 评估等级空间记作 U , 表示为 $U = \{c_1, c_2, \dots, c_P\}$. 若评估等级空间 U 具有如下性质: $c_i \cap c_j = \emptyset (i \neq j)$, 且 $c_1 < c_2 < \dots < c_P$, 即 c_{k+1} 比 c_k 强, 则称 $U = \{c_1, c_2, \dots, c_P\}$ 为一个有序分割类.

设实体可提供 P 个级别的服务 $S = \{s_1, s_2, \dots, s_P\}$, 且 S 是一个有序分割类, S 和总体信任度 $\Gamma(x_i, x_j, s, t)$ 之间的映射函数 Ψ 表示为

$$\Psi(\Gamma(x_i, x_j, s, t)) = \begin{cases} s_K, & c_P \leq \Gamma(x_i, x_j, s, t) \leq 1 \\ s_{K-1}, & c_{b-1} \leq \Gamma(x_i, x_j, s, t) < c_P \\ \dots & \\ s_2, & c_1 \leq \Gamma(x_i, x_j, s, t) < c_2 \\ s_1, & 0 \leq \Gamma(x_i, x_j, s, t) < c_1 \end{cases} \quad (3)$$

分界点 c_1, c_2, \dots, c_P 由定义 2 确定, 当 x_i 向 x_j 请求某种质量的服务时, 首先要根据 x_j 的信任级别 $\Gamma(x_i, x_j, s, t)$ 决定它所能得到的服务质量, 这样既可以分级对不同的实体提供不同的服务, 也有利于降低系统可能存在的风险. 例如, 某 FTP 服务提供了 3 个等级的服务质量, $S = \{s_1, s_2, s_3\}$, s_1 表示拒绝服务, s_2 表示只读, s_3 表示既可以读也可以写. 相应的决策等级空间设定为 $\mathfrak{R} = \{c_1, c_2, c_3\} = \{0, 0.2, 0.5\}$, 则服务决策函数可表示为

$$\Psi(\Gamma(P_i, P_j)) = \begin{cases} s_3, & 0.5 < \Gamma(x_i, x_j, s, t) \leq 1 \\ s_2, & 0.2 \leq \Gamma(x_i, x_j, s, t) \leq 0.5 \\ s_1, & 0 \leq \Gamma(x_i, x_j, s, t) < 0.2 \end{cases}$$

设某实体 P_j 的 $\Gamma(x_i, x_j, s, t) = 0.19$, 则根据函数 Ψ , 决策过程为 $\Psi(\Gamma(x_i, x_j, s, t)) = \Psi(0.19) = s_1 =$ 拒绝服务.

3.2 多维决策属性的计算

文献[2]指出, 当实体之间的信任关系不能准确量化的时候, 它也就是不稳定的, 给信任的管理和评估带来了困难. 信任关系的合理量化是信任管理的关键问题之一. 为了准确量化动态信任关系, 在前期工作的基础上^[2, 11-15], 引入直接信任、信任风险函数、反馈信任、激励函数和实体活跃度等多个DF从多个角度刻画信任关系的动态性和不确定性, 对信任关系进行建模时, 强调综合考察影响信任的多种DF, 针对信任关系的多维属性进行更加详细的建模.

定义 3. 实体 x_i 与 x_j 在最近的 h 个直接交互中的信任满意度评价为 $E_{ij} = \{e_{ij}^{(1)}, e_{ij}^{(2)}, \dots, e_{ij}^{(h)}\}$, 其中 $0 \leq e_{ij}^{(k)} \leq 1, k \in [1, h], h < H, H$ 为最大的有效

历史记录数, E_{ij} 中的元素按照交互的时间顺序排列, $e_{ij}^{(1)}$ 表示离现在较久的一次交互, $e_{ij}^{(h)}$ 表示离现在最近的一次交互. 则 x_i 对 x_j 的直接信任为

$$Y_1(x_i, x_j) = \begin{cases} \sum_{k=1}^h e_{ij}^{(k)} \cdot \gamma(k) / h, & h \neq 0 \\ 0, & h = 0 \end{cases} \quad (4)$$

式中 $\gamma(k) \in [0, 1]$ 是衰减函数, 用来对发生在不同时刻的直接信任信息进行合理的加权, 根据人们的行为习惯, 对于新发生的交互行为应该给予更多的权重, 衰减函数定义为

$$\gamma(k) = \begin{cases} 1, & k = h \\ \gamma(k-1) = \gamma(k) - 1/h, & 1 \leq k \leq h \end{cases} \quad (5)$$

与其它模型^[4,7-8]相比, 基于衰减函数与时间戳相结合进行直接信任计算具有下列优点:

(1) 反映了信任关系随时间的变化而衰减的属性, 提高信任量化的准确度;

(2) 用时间戳 h 标示出信任的时间维度, 提高动态适应能力, 引入有效历史记录数 H , 可以删除陈旧的数据, 节约存储.

Nena Lim^[16]等人认为, 信任和风险密切相关, 信任只存在于具有不确定性的风险环境当中, 它们之间的关系是相互交织的. 如果商务交易、人际交往中没有风险, 即人的行为是确定的时候, 那么信任也没有存在的必要, 所以风险是信任产生的前提; 根据文献[2], 目前信任模型的一个主要缺陷是缺少风险要素的考虑, 虽然文献[7]也引入了风险机制, 但该机制并未考虑风险与服务质量的关系. 在开放系统中, 主要关注点是恶意实体对系统可能的破坏行为的风险, 依据经济学中风险投资的原理, 我们从服务的角度定义风险, 使用以下公式计算风险的大小:

$$R(x_i, x_j) = S_j(1 - \Gamma(x_i, x_j, s, t-1)) \\ = \Psi(\Gamma(x_i, x_j, s, t-1)) [1 - \Gamma(x_i, x_j, s, t-1)] \quad (6)$$

式中 S_j 表示 x_j 所请求的服务质量, 根据经验, S_j 值越大, 风险也越大, 所以风险与 S_j 成正比, $\Gamma(x_i, x_j, s, t-1)$ 表示 x_i 对 x_j 最近一个时间戳的信任评价, 信任度越高, 风险越小, 所以风险与 $1 - \Gamma(x_i, x_j, s, t-1)$ 成正比.

定义 4. 信任风险函数主要是指服务提供者对服务请求者行为的不确定性和自身服务行为不利结果的认知, 它与式(6)给出的风险有如下关系:

$$Y_2(x_i, x_j) = 1 - R(x_i, x_j) \quad (7)$$

由式(6)和式(7)可以看出, $Y_2(x_i, x_j)$ 有两个维度: (1) 服务请求者中恶意实体对服务提供者可能的攻击行为或者恶意推荐行为的概率, 若实体的信任级别高, 这种恶意行为的概率就低, 否则相反; (2) 与服务提供者所提供的服务的重要性有关, 所提供服务的级别越高, 可能的风险也就越大. 通过式(7)也可以看出, $Y_2(x_i, x_j)$ 与 $R(x_i, x_j)$ 是成反比的, 这主要是基于定义 1 计算总体信任度的需要决定的, 信任风险函数作为一个 DF, 应该是与 $R(x_i, x_j)$ 成反比的.

定义 5. 设反馈者的集合为 $\{W_1, W_2, \dots, W_L\}$, $Y_1(W_k, x_j)$ 表示第 k 个反馈者对 x_j 的直接信任. 则反馈信任为

$$Y_3(x_i, x_j) = \begin{cases} \frac{\sum_{k=1}^L (\varpi(W_k) \times Y_1(W_k, x_j))}{\sum_{k=1}^L \varpi(W_k)}, & L \neq 0 \\ 0, & L = 0 \end{cases} \quad (8)$$

式中 L 为反馈者的个数, 当没有反馈信息时, 根据文献[17]的结论, 取默认值 $Y_3(x_i, x_j) = 0$, 表示没有反馈者, 反馈信任值为零. $\varpi(W_k)$ 为反馈者加权函数:

$$\varpi(W_k) = \begin{cases} 1, & LEVEL = 1 \\ \prod_{d=0}^l Y_1(x_d, x_{succ}), & LEVEL > 1 \end{cases} \quad (9)$$

其中 $Y_1(x_d, x_{succ})$ 表示从 x_i 到 x_k 信任路径上实体 x_d 对它的后继实体 x_{succ} 的直接信任.

不同于其它模型, 我们认为反馈信任不能采取简单的算术平均的办法, 因为不同的反馈者所在的层级(网络中反馈者 x_k 距离 x_i 的跳数, 用 $LEVEL$ 表示)不同, 有些反馈者是 x_i 的邻居 ($LEVEL = 1$), 而有些不是 ($LEVEL > 1$). 根据人们的经验, 反馈者距离自己越近, 反馈的信息越可靠, 所以本文引入反馈者加权函数 $\varpi(W_k)$, 对每一个反馈信息根据它与决策者 SP 的距离 $LEVEL$ 进行加权. 例如在图 1 中, 对于服务提供者 P_0 的直接邻居节点(与 P_0 有直接交互历史的节点), 也就是 $LEVEL = 1$ 时, $\varpi(P_2) = 0.7$, 当 $LEVEL = 2$ 时, $\varpi(P_6) = 0.5 \times 0.7 = 0.35$, 当 $LEVEL = 3$ 时, $\varpi(P_9) = 0.5 \times 0.6 \times 0.8 = 0.24$.

开放的网络环境中存在着大量不可靠的服务质量以及欺诈行为. 例如, 在 P2P 文件共享系统中, 经常发生资源下载中途失效的情况. 因此, 要

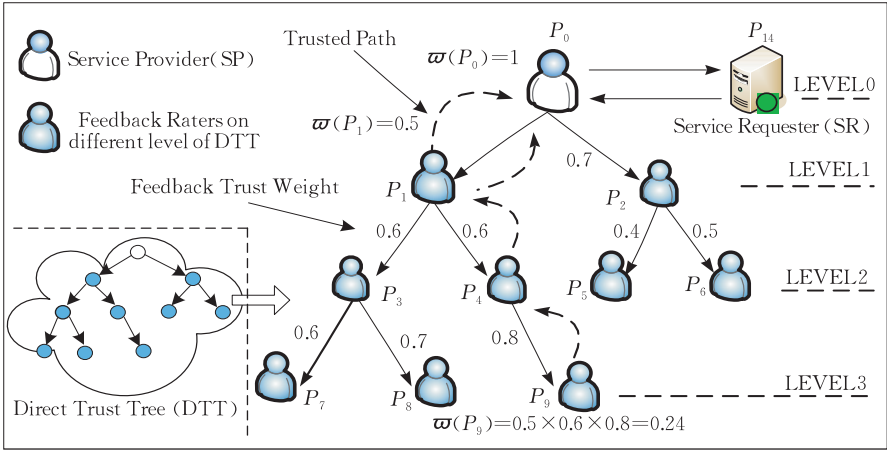


图 1 反馈加权函数的计算

提高网络的性能必须考虑实体的主动服务行为，激励节点之间有效合作并合理使用网络资源。本文引入激励函数到总体信任度评估的 DF 中，可以有效增强实体之间的主动服务意愿，增大交互成功的概率。

定义 6. 激励函数定义为

$$Y_4(x_i, x_j) = 1 - \frac{\sum_H F(x_i, x_j)}{H} \quad (10)$$

$\sum_H F(x_i, x_j)$ 表示在最大有效历史记录 H 中交互失败的次数，激励函数体现了系统对合作实体的激励性，因为合作的实体通常有较少的交易失败率，而恶意不合作实体经常中断服务或者拒绝服务，激励函数也体现出对恶意不合作实体的惩罚性，在有效的若干个交互中，失败的交互越多，意味着服务请求者可能是一个恶意不合作的实体。

定义 7. 实体活跃度反映了实体在网络中的活跃程度与稳定程度，反馈者个数越多，表示与实体有成功交互纪录的其它实体个数越多。活跃度越高，也说明实体有较高的可信度。

$$Y_5(x_i, x_j) = \frac{1}{2} [\Phi(L) + \Phi(n_{\text{total}})] \quad (11)$$

其中， $\Phi(x) = 1 - (1/x + \delta)$ ， L 为反馈者个数， n_{total} 为所有与 j 有交互行为的实体的个数， $\Phi(x)$ 的调节常数 δ 为一个大于 0 的任意常数，用于控制 $\Phi(x)$ 趋于 1 的速度， δ 值越大， $\Phi(x)$ 趋于 1 的速度越快，通过图 2 可以看出：实体活跃度 $Y_5(x_i, x_j)$ 由两个变量 L 和 n_{total} 共同决定，与实体交易的其它实体个数越多， $Y_5(x_i, x_j)$ 值越大，同时反馈者个数越多， $Y_5(x_i, x_j)$ 的值也越大，而变量 L 和 n_{total} 的数量确实反映了实体在网络中的活跃程度，例如， $L = 55$ ， $n_{\text{total}} = 15$ ， $\delta = 0.2$ ，那么 $Y_5(x_i, x_j) = 0.87$ 。

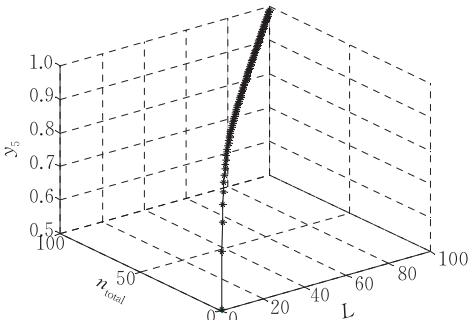


图 2 实体活跃度

3.3 基于信息熵的 DF 分类权重

第 2.2 节给出了多 DF 的计算方法，通过各个 $Y_m(x_i, x_j)$ 的定义，不难看出 $0 \leq Y_m(x_i, x_j) \leq 1$ ，且 $Y_m(x_i, x_j)$ 值的大小反映了该 DF 的可信程度，例如 $Y_1(x_i, x_j) = 0.5$ ，表示直接可信度就是 50%，但却还有 50% 的不可信成分，而这 50% 的不可信成分可能使系统面临 50% 的风险，而传统的信任模型对这一现象缺少考虑，例如：在采用直接信任与间接信任加权平均的算法中^[4,6-10]，节点更愿意相信自己的直接经验，赋予直接信任更多的权重，反而导致系统面临更多的风险。如某系统（直接信任，权重）=（0.4，0.6），（间接信任，权重）=（0.8，0.4），则总体信任 = $0.6 \times 0.4 + 0.4 \times 0.8 = 0.56$ ，这显然是不合理的，因为给 40% 的可信度赋予 60% 的权重，将必然导致可信决策的谬误。

信息熵是由香农(Shannon)将热力学熵引入信息论而提出的，其为不确定方法的一个重要概念，常被用于较粗略地给出不确定性的度量。信息熵在事件发生之前，它是结果不确定性的量度，在事件发生之后，它是我们从该事件中所得到的信息的量度(信息量)。因此，事件的信息熵，是一个事件的不确定性或

信息量的量度,也可以理解为包含在这个事件本身中的关于它自己的信息,因为事件发生后结果就完全确定了^[18].

定义 8. 第 m 个决策属性($Y_m(x_i, x_j)$)所确定的信息熵为

$$H(Y_m(x_i, x_j)) = -Y_m(x_i, x_j)\log Y_m(x_i, x_j) - (1 - Y_m(x_i, x_j))\log(1 - Y_m(x_i, x_j)) \quad (12)$$

其中 $Y_m(x_i, x_j)$ 意味着 DF 的可信度,而 $1 - Y_m(x_i, x_j)$ 表示 DF 的不可信程度.可见定义 8 只有两个信源,其概率分别为 $Y_m(x_i, x_j)$ 和 $1 - Y_m(x_i, x_j)$. 例如,两个 DF 的测量值分别为

$$\begin{bmatrix} Y_1(x_i, x_j) & 1 - Y_1(x_i, x_j) \\ 0.99 & 0.01 \end{bmatrix},$$
$$\begin{bmatrix} Y_2(x_i, x_j) & 1 - Y_2(x_i, x_j) \\ 0.5 & 0.5 \end{bmatrix},$$

则

$$H(Y_1(x_i, x_j)) = -0.99\log 0.99 - 0.11\log 0.11 = 0.08.$$
$$H(Y_2(x_i, x_j)) = -0.5\log 0.5 - 0.5\log 0.5 = 1.$$

$H(Y_2(x_i, x_j)) > H(Y_1(x_i, x_j))$,说明决策属性 $Y_2(x_i, x_j)$ 比 $Y_1(x_i, x_j)$ 的平均不确定性要大,若在事件发生之前,分析信源 $Y_2(x_i, x_j)$,由于事件是等概率的,难以猜测哪一个事件会发生;而 $Y_1(x_i, x_j)$ 虽然也存在不确定性,但大致可以知道 $Y_1(x_i, x_j)$ 出现的可能性要大.

图 3 是根据定义 8 得到的 DF 熵函数坐标图,可见,DF 的熵函数 $0 \leq H(Y_m(x_i, x_j)) \leq 1$,且熵函数以 $Y_m(x_i, x_j) = 0.5$ 为轴呈对称分布,物理意义是 $Y_m(x_i, x_j)$ 在区间 $[0, 0.5]$ 可能发生(不可信)和在区间 $[0.5, 1]$ 可能发生(可信)的不确定性程度大小相等.可信决策的期望是信息熵能唯一反映出事件可信的不确定性程度,熵函数的对称性显然不利于我们做出这样的唯一的判断,下面通过定义 9 对这一局限进行修正.

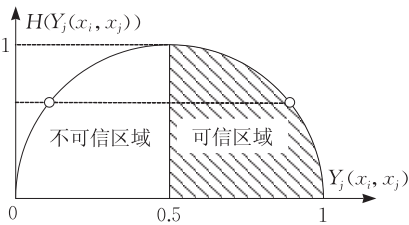


图 3 决策属性的熵函数

定义 9. 设 V_m 是 $Y_m(x_i, x_j)$ ($m = 1, 2, \dots, M$) 相对于其它 DF 的分类区分度,令

$$V_m = \begin{cases} 1 - \frac{1}{\log P} H(Y_m(x_i, x_j)), & Y_m(x_i, x_j) > 0.5 \\ 0, & Y_m(x_i, x_j) \leq 0.5 \end{cases} \quad (13)$$

令

$$\varpi_m = V_m / \sum_{m=1}^M V_m, \quad \varpi_m = (\varpi_1, \varpi_2, \dots, \varpi_M) \quad (14)$$

式(13)中 P 就是定义 1 中给出的评估等级的级数.根据式(14),显然有

$$0 \leq \varpi_m \leq 1 \text{ 且 } \sum_{m=1}^M \varpi_m = 1,$$

所以式(14)就是式(1)给出的分类权重,称 $\varpi_m = (\varpi_1, \varpi_2, \dots, \varpi_M)$ 为 DF 的分类权重向量,DF 分类权重是根据指标观测值计算得到的,说明它不需要主观拟定.当某一 DF 的值不大于 0.5 时,直接判定它的 V_m 为 0,进而根据式(14),它的分类权重为 0,这样可以有效减少系统的风险,提高系统抵御不确定性风险带来的威胁.

例如:设在某个交互过程中评估等级数 $P = 5$,某时刻计算得到的各 DF 为

$$Y_m(x_i, x_j) = \{0.6, 0.4, 0.8, 0.2, 0.8\},$$

则各个 DF 的分类权重计算如表 1 所示.

表 1 DF 分类权重的计算

m	$Y_m(x_i, x_j)$	$1 - Y_m(x_i, x_j)$	$H(Y_m(x_i, x_j))$	V_m	ϖ_m
1	0.6	0.4	0.9708	0.5818	0.2966
2	0.4	0.6	0.9708	0	0
3	0.8	0.2	0.7205	0.6896	0.3516
4	0.2	0.8	0.7205	0	0
5	0.8	0.2	0.7205	0.6896	0.3516

从表 1 可以看出, $Y_1(x_i, x_j)$ 和 $Y_2(x_i, x_j)$ 的 DF 信息熵相同,都是 0.9708,而 $Y_3(x_i, x_j)$ 、 $Y_4(x_i, x_j)$ 和 $Y_5(x_i, x_j)$ 的 DF 信息熵也相同,都是 0.7205.这反映出两点:(1) $Y_1(x_i, x_j)$ 和 $Y_2(x_i, x_j)$ 的不确定性比 $Y_3(x_i, x_j)$ 、 $Y_4(x_i, x_j)$ 和 $Y_5(x_i, x_j)$ 的不确定性要大;(2) 就某一个 DF 而言,反映出了信息熵的对称性(图 2),也就是 $Y_m(x_i, x_j)$ 和 $1 - Y_m(x_i, x_j)$ 顺序任意互换时,DF 熵函数的值不变,这也说明熵只与随机变量的总体结构有关,与信源个体的统计特性无关,同时也说明所定义的信息熵有其局限性,它不能描述事件本身的主观意义.而定义 9 给出的计算分类权重 ϖ_m 的方法却恰好能够弥补这一局限,从表 1 的计算的最终结果可以看出, $Y_3(x_i, x_j)$ 和 $Y_5(x_i, x_j)$ 的权重大于 $Y_1(x_i, x_j)$ 的权重,说明 $Y_3(x_i, x_j)$ 和 $Y_5(x_i, x_j)$ 的测量值对总体信任度的贡

献要大于 $Y_1(x_i, x_j)$ 的贡献,这也与 DF 输入值的大小关系相一致,而 $Y_2(x_i, x_j)$ 和 $Y_4(x_i, x_j)$ 的权值为 0,说明它们的测量值偏低,对总体信任度的评估不做出贡献。由此,根据定义 1 计算出总体信任度:

$$\begin{aligned}\Gamma(x_i, x_j, s, t) &= \sum_{m=1}^M \varpi_m Y_m(x_i, x_j) = \sum_{m=1}^5 \varpi_m Y_m(x_i, x_j) \\ &= 0.6 \times 0.2966 + 2 \times 0.3516 \times 0.8 \\ &= 0.74052.\end{aligned}$$

3.4 相关实现算法

x_j 向服务提供者 x_i 请求某种服务,但 x_i 本地数据库中并没有 x_j 的交互记录(或者有 x_j 的记录,但记录时间戳是比较早的,已经超过了系统设定的最低有效时间阈值,那么需要调用相关算法进行信任度的计算,然后根据计算结果决定是否提供 x_j 所请求的服务 s_j 。下面给出本文模型的总体实现流程。

算法 1. 总体信任度计算算法 OTDCA(Overall Trust Degree Calculated Algorithm)。

1. 输入: H, δ, P, M ; /* 输入最大有效历史记录数、实体活跃度函数调节常数、DF 数和总体信任评估等级等参数 */
2. 设 $FSET(x_j) = \{W_1, W_2, \dots, W_L\}$;
/* $FSET(x_j)$ 表示所有针对实体 x_j 的反馈实体的集合 */
3. 根据算法 2 计算 $FSET(x_j)$;
4. 计算 DF
 - 1) $Y_1(x_i, x_j) \leftarrow$ 计算式(4), (5); /* 直接信任 */
 - 2) $Y_2(x_i, x_j) \leftarrow$ 计算式(6), (7); /* 风险函数 */
 - 3) $Y_3(x_i, x_j) \leftarrow$ 计算式(8), (9); /* 反馈信任 */
 - 4) $Y_4(x_i, x_j) \leftarrow$ 计算式(10); /* 激励函数 */
 - 5) $Y_5(x_i, x_j) \leftarrow$ 计算式(11); /* 实体活跃度 */
5. 根据式(12)~(14)计算各个决策属性 DF 的分类权重 ϖ_m ;
6. $\Gamma(x_i, x_j, s, t) \leftarrow$ 计算式(2); /* 总体信任度计算 */
7. $\Psi(\Gamma(x_i, x_j, s, t)) \leftarrow$ 计算式(3); /* 求解服务请求者所请求的服务 s_j 是否和信任映射函数计算得到的服务相符合 */
8. IF ($\Psi(\Gamma(x_i, x_j, s, t)) \geq s_j$) THEN
对 x_j 提供服务 s_j ;
ELSE 拒绝提供服务.
9. END.

可信网络访问控制研究的一个关键问题是如何通过有效的方式获取反馈信任信息,定义 5 给出了当有 L 个反馈实体时如何进行反馈信任的聚合计算,但并没有给出如何获得这 L 个反馈实体,下面给出反馈实体的递归搜索算法。

算法 2. 反馈实体搜索算法 FESA(Feedback Entries Searching Algorithm)。

1. $RequestFeedbacks(x_i, x_j, \lambda, \eta)$;
/* 函数名,递归函数入口 */
2. IF ($LEVEL(x_k) > \lambda$) THEN 结束; /* 函数 $LEVEL(x_k)$ 表示第 k 个反馈者 x_k 距离 x_i 的跳数, λ 表示最大搜索深度, $\lambda \geq 1$, 用来控制反馈信任请求信息在网络中的传播深度,也用来控制递归搜索算法的结束 */
3. FOR (所有 $x_k \in NSET(x_i)$) DO
IF ($\Gamma(x_i, x_k, s, t) > \eta$) THEN
在 x_k 的本地数据库查询 $\Gamma(x_i, x_j, s, t)$;
IF ($\Gamma(x_i, x_j, s, t)$ 存在) THEN
1) 根据等式(1)计算 $Y_1(x_k, x_j)$; 根据等式(8)、(9)累加计算反馈信任 $Y_3(x_i, x_j)$;
2) $FSET(x_j) = FSET(x_j) + x_k$;
3) $RequestFeedbacks(x_k, x_j, \lambda, \eta)$;
/* 继续搜索 */
4. ENDFOR; /* 集合 $NSET(x_i)$ 表示实体 x_i 的所有邻居实体(邻居实体(Neighbor Entities)指与 x_i 有直接交互行为的实体); η 表示对反馈者信任级别的最小值, $\eta \in [0.5, 1]$, 只有反馈者的直接信任值 $\Gamma(x_i, x_k, s, t) > \eta$ 时,该反馈者的反馈信息才是可信的,通过 η 可以拒绝信任级别较低的反者 */
5. 输出 $FSET(x_j)$;
6. END.

4 模拟实验与性能分析

4.1 实验设置

模拟实验是目前采用最广泛的信任模型评测方法,通过计算机来模拟具体的应用场景及实体之间的交互行为,可以从多个角度评估信任模型在解决实际问题时的效果。随着分布式信任模型研究的增多,为了评估信任模型在 P2P 环境、Ad hoc 和普适计算环境中的效果,实验模拟已经成为信任模型的主要评估手段。

本文通过 NetLogo^① 平台实现了一个模拟的 Peer-to-Peer 网络环境来对本文的相关模型及其算法进行性能分析,NetLogo 平台是美国西北大学网络学习和计算机建模中心推出的可编程建模环境,采用 Java 语言编写,能够跨平台运行。它同时提供单机和网络环境两种版本,每个模型还可以保存为

① Tissue S. NetLogo. <http://ccl.northwestern.edu>

Java applets,可嵌入到网页上运行. NetLogo 提供一个开放的模拟平台,自身带有模型库,用户可以改变多种条件的设置,体验基于 Multi-Agent 复杂开放系统仿真建模的思想,进行探索性研究. 它对于研究人员是一种有力的工具,允许建模者对几千个“独立”的 Agent 下达指令进行并行运作,特别适合于研究随着时间演化的复杂系统. 作为参照,对本文模型和 PT1^[4] 和 PT2^[7] 进行比较,表 2 为部分实验参数.

表 2 模拟实验参数说明

	参数	缺省值	描述
运行参数	N	1000	实体总个数
	S	2000	模拟次数
	H	10	有效最大历史记录数
算法参数	λ	4	反馈者搜索深度
	δ	1	调节常数
	η	0.61	反馈者最小信任度

为了贴近实际网络环境,使用和文献[19]相同的环境设置,并在实验中对节点的类型做如下设定:

(1) 实验中实体的 3 种角色是相互独立的,一个实体即可以作为 SP 也可以作为 SR 和 FR,但几个身份相互独立,互不影响.

(2) FR 可以分为 4 种类型:① H 类实体,总能提供真实的反馈;② M 类实体,对其它实体总给出相反评价;③ E 类实体,根据扩大因子 Δ 对其它实体总是给出扩大的评价 $F + \Delta(1 - 0.5)$ (模拟实验中,取 $\Delta = 0.5$);④ C 类实体,对团伙内实体评价为 1,对其它实体评价为 0.

(3) SP 根据所提供服务的質量分为 3 种类型:① GS 总能提供可靠的服务;② BS 总拒绝提供服务;③ RS 根据时间的动态变化分别提供 GS 和 BS 服务.

(4) 评估等级 $U = \{c_1, c_2, \dots, c_P\} = \{0, 0.2, 0.4, 0.6, 0.8, 1\}$, 相应的信任级别映射如表 3 所示.

表 3 实体信任级别映射关系

序号	信任值	信任关系
1	$[0, 0.2)$	非常低
2	$[0.2, 0.4)$	低
3	$[0.4, 0.6)$	正常
4	$[0.6, 0.8)$	高
5	$[0.8, 1.0]$	非常高

4.2 有效性评估

可信网络管理的一个主要功能是进行实体各种恶意行为的检测. 信任机制应该具有较强的恶意行

为的检测能力. 我们用恶意反馈行为的检测率 (MDR) 和恶意实体的服务失败率 (MFR) 来反映信任模型的安全能力. MDR 主要反映了系统对恶意反馈行为的检测能力,而 MFR 反映了系统对恶意访问行为的检测与抵御能力.

设在时刻 t 共检测到 $G(t)$ 个诚实的反馈行为,检测到 $B(t)$ 个恶意的反馈行为,而设定的恶意反馈者所占的百分比为 α (注意 $\alpha = FR_M \times 100\% + FR_C \times 100\% + FR_E \times 100\%$),则 MDR (用 $\theta(t)$ 表示) 定义为

$$\theta(t) = \frac{B(t)/(B(t) + G(t))}{\alpha} = \frac{B(t)}{\alpha(B(t) + G(t))}$$

(15)

设在交互过程中某个时刻 t 检测到服务请求成功的次数为 $S(t)$,服务请求失败的次数 $F(t)$,而设定的恶意实体所占的百分比为 β ,则 MFR (用 $\varphi(t)$ 表示) 定义为

$$\varphi(t) = \frac{F(t)/(S(t) + F(t))}{\beta} = \frac{F(t)}{\beta(S(t) + F(t))}$$

(16)

图 4(a)~(c) 是不同百分比的恶意 FR 环境下 MDR 的比较. 实验中,所设定的恶意 FR 的比率分别为 20%、50%、80%. 从图 4(a) 可以看出,当网络中恶意 FR 比例为 20% 时,网络中大部分实体为 H 类实体 (80%),3 个模型都表现出较好的检测能力,MDR 都介于 90%~100% 之间. 当恶意 FR 达到 50% 时 (图 4(b)),系统中有一半的实体为恶意 FR,本文模型的 MDR 要明显优于 PT1 和 PT2 模型,当恶意 FR 达到 80% 时 (图 4(c)),系统中大部分实体都是恶意的 FR,本文模型仍然稳定可靠,而 PT1 的 MDR 下降了大约 5%,PT1 性能下降也达到 4% 左右.

图 4(d)~(f) 是不同百分比的恶意反馈节点环境下 MFR 的比较. 实验中,所设定的恶意 FR 的比率分别为 20%、50%、80%. 在图 4(d) 中,当恶意实体比例为 20% 时,本文模型和 PT1、PT2 都有介于 90%~100% 之间的 MFR. 在图 4(e) 中,当恶意实体达到 50% 时,3 个模型仍然都能提供稳定的服务. 但当恶意实体达到 80% 时,本文模型仍然表现较好,其 MFR 基本没有下降,PT1 算法虽然也有较高的 MFR,但从图 4(f) 可以看出,当恶意实体比率较大时,其性能有一些波动,PT2 随着模拟时间的增多,性能呈现明显下降趋势.

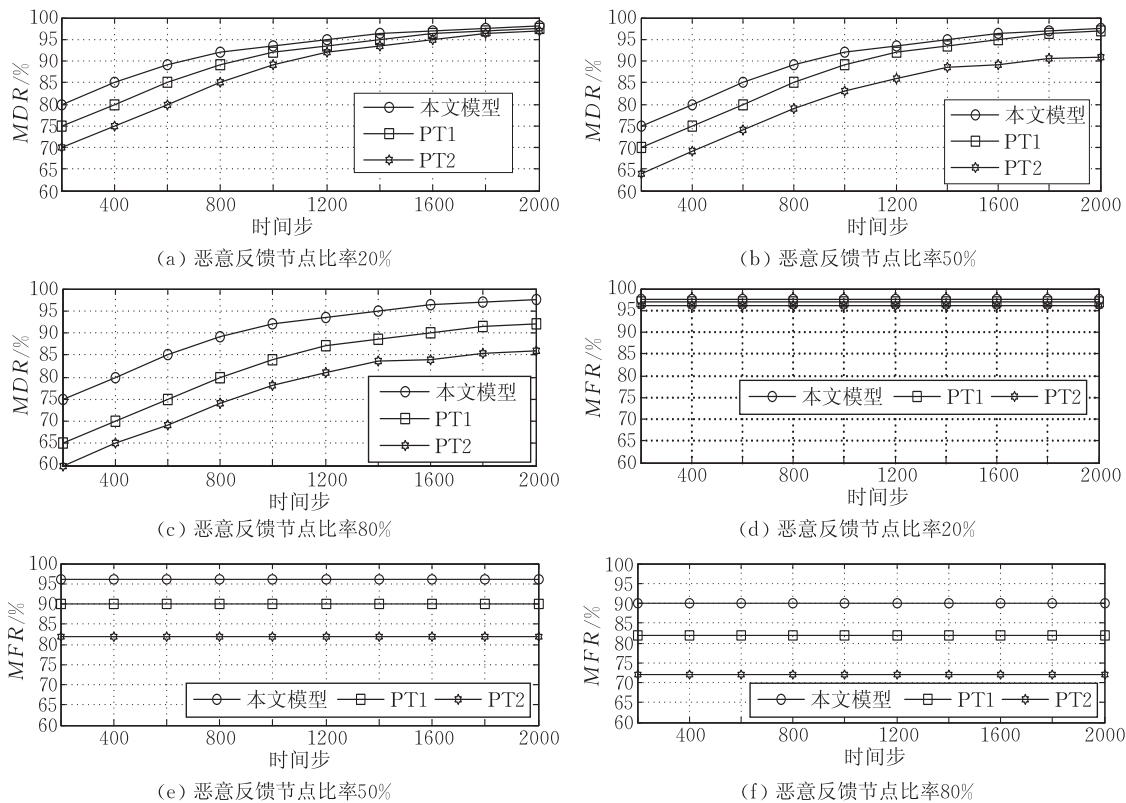


图4 MDR和MFR分析

4.3 动态适应性评估

动态适应性,就是系统在各种不确定因素的影响下提供可靠服务的能力,一个教好的信任模型能够在复杂的动态环境中继续提供稳定的服务. 系统的动态性主要反应在系统中的实体行为的动态性,例如:SP提供的服务可以在GS,BS,RS之间动态变化,FR可以动态地在4种身份之间变化,实体也可以随机地离开和加入. 实验通过3个参数来反映系统的动态性.

(1) 服务请求频度 $SRF(0 \leq SRF \leq 1)$,反映了系统的繁忙程度, SRF 的值越大,服务请求越频繁. 在实验中, SRF 是系统设定的一个常数.

(2) 服务动态频度 $SCF(0 \leq SCF \leq 1)$,反映了系统中服务提供者或者资源的不稳定性, SCF 的值越大,SP在GS,BS,RS之间频繁的动态切换. 在实验中, SCF 是系统设定的一个常数.

(3) 社群动态频度 $SDF(0 \leq SDF \leq 1)$,反映了网络社群的不确定性,在实验中, SDF 是系统设定的一个常数,表示系统中有 $SDF \times N$ 个实体是不稳定的,它们可以随时地离开或加入.

用交互的成功率(SSP)来说明模型的动态适应能力,高的访问成功率说明模型具有好的动态适应性. 计算方法为($A_g(t)$ 表示成功的交互次数, $B_{total}(t)$ 表示总交互次数)

$$\nabla(t) = \frac{A_g(t)}{B_{total}(t)} \quad (17)$$

实验中反馈实体FR的类型分别设置为 β_H : 80%, β_M : 10%, β_E : 5%, β_C : 5%, 这样的取值也基本符合一个实际网络的特点,因为在一个实际网络中大部分实体都是诚实的实体($\beta_H = 80\%$),只有少部分的实体是恶意实体($\beta_M + \beta_E + \beta_C = 20\%$). 首先观察在一个动态性变化较小的网络环境下模型的动态适应能力, SRF 分别为20%(图5(a))和80%(图5(b)), $SCF = 0\%$ (SP提供稳定的服务), $SDF = 0\%$ (系统中所有的实体都不能随意地离开). 从图5(a)~(b)的比较结果可以看出,在一个相对稳定的环境中,3个模型都表现出较好的动态适应能力,它们的SSP平均都在95%以上.

图5(c)~(d)中 $SCF = 0.4$, $SDF = 0.4$,说明网络是一个较不稳定的环境,从图5(c)~(d)的实验结果可以看出,随着系统交互业务量的增加,本文模型比PT1模型的服务成功率平均可提高5%左右. 图5(e)~(f)为在一个高度动态变化的环境下的观测结果,动态性参数分别取值 $SCF = 0.8$, $SDF = 0.8$,服务请求的频度分别为20%(图5(e))和80%(图5(f)),说明SP较频繁地在GS,BS,RS之间切换,有80%的实体可以随意地加入或者离开. 从图5(e)~(f)可以看出,3个模型的SSP都有所下降,

但三者下降的比率有明显的差别：本文模型平均下降 3%，PT1 平均下降 5%，而 PT2 下降比率达到 8%。可见，在一个恶意节点比率较高的网络社会环境下，本文模型的 SSP 性能最稳定，PT1 模型次之，而 PT2 模型最低。出现这种性能差异的原因也是显然的，本文模型采用多个 DF 从多个角度刻画

信任关系的复杂性和不确定性，对信任关系进行建模时，强调综合考察影响信任的多种决策属性，针对信任关系的多维决策属性进行更全面的建模，从而使该模型能更准确地反应信任关系的本质属性，并具有更好的合理性和更高的动态适应能力。

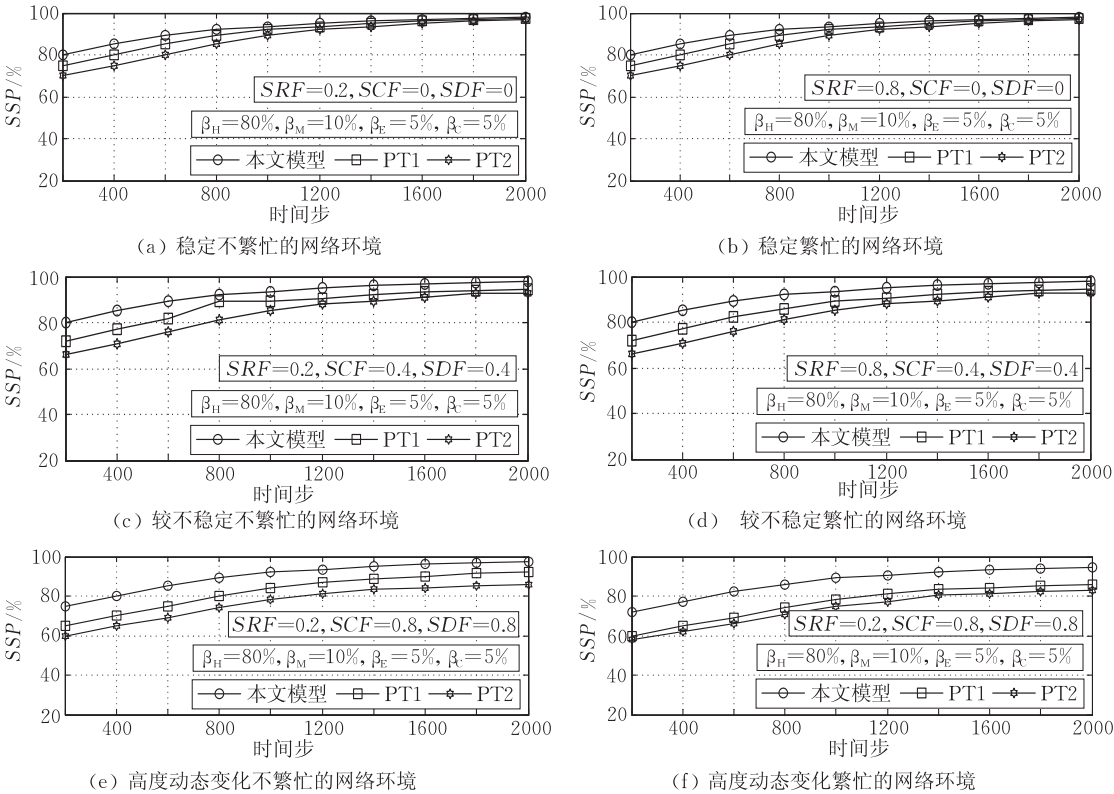


图 5 模型动态适应性分析

4.4 进一步讨论

(1) 模型的有效性问题的

动态信任理论的主要思想是，在对实体信任关系进行建模与管理时，强调综合考察影响实体可信性的多种因素（特别是行为上下文），针对实体行为可信的多个属性进行有侧重点的建模；强调动态地收集相关的主观因素和客观证据的变化，以一种及时的方式实现对实体可信性度测、管理和决策，并对实体的可信性进行动态更新与演化。开放系统引入动态信任管理的主要目标是降低风险，提高系统的安全性，而信任关系从内涵上来看，其本身属于一个心理学的范畴，是一个很难度量的抽象的心理“认知”，当一个实体之间的信任关系模型不符合人类心理认知习惯的时候，它肯定是不合理的，也是不稳定的，给信任的管理和评估带来了困难。通过图 5 和图 6 的实验结果可以看出，模型具有更稳健的动态适应性，在模型的安全性方面

也有明显的优势。

(2) 模型的普适性问题

在以互联网为基础平台的、各种复杂开放的分布式应用环境（如网格、P2P、电子商务、电子政务、Ad hoc 和普适计算等）中，系统表现为由多个软件服务组成的动态协作模型。在这种动态的和不确定的环境中，应用环境具有异构性、动态性、分布性和多管理域等特征，用户、应用程序、计算资源和计算环境等的管理方式不再是集中和封闭的，而是开放和动态的。从前面的讨论可以看出，本文的研究也正是基于准确刻画信任关系的动态性和不确定性这一主要目标。虽然本文仅仅通过 P2P 网络对算法进行了模拟实验，因为 P2P 系统是一个非常典型的开放系统，例如节点可以随意地加入和离开，服务提供者可以动态地改变它们的服务策略，因此，我们认为，本文模型是一个普适的信任关系量化模型，该模型也适合于其它的开放系统。

5 结论和下一步的工作

针对目前的信任模型输入因子简单,对行为和环境动态变化的适应能力支持不足等问题,本文提出了基于多维决策属性的信任关系量化模型,强调综合考察影响信任的多种决策属性,针对信任关系的多个属性进行有重点的建模.并通过信息熵理论确立各决策因子的分类权重,克服了过去常用的确定权重的主观判断方法,从而使该模型具有更高的实际应用价值.

下一步的工作重点是,基于人类对信任关系的认知过程深入研究信任关系的内涵、性质,并对本文模型做进一步的完善,并结合机器学习、人工智能等方法,继续探索适合描述动态信任关系的普适的量化模型.

参 考 文 献

- [1] Lin Chuang, Peng Xue-Hai. Research on trustworthy networks. *Chinese Journal of Computers*, 2005, 28(5): 751-758(in Chinese)
(林闯, 彭雪海. 可信网络研究. *计算机学报*, 2005, 28(5): 751-758)
- [2] Li Xiao-Yong, Gui Xiao-Lin. Research on dynamic trust model in large-scale distributed environment. *Journal of Software*, 2007, 18(6): 1510-1521(in Chinese)
(李小勇, 桂小林. 大规模分布式环境下动态信任模型研究. *软件学报*, 2007, 18(6): 1510-1521)
- [3] Zhou Rong-Fang, Hwang Kai. Power-Trust: A robust and scalable reputation system for trusted Peer-to-Peer computing. *IEEE Transactions on Parallel and Distributed Systems*, 2007, 18(4): 460-473
- [4] Li Xiong, Liu Lin. Peer-Trust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering*, 2004, 16(7): 843-857
- [5] Theodorakopoulos G, Baras J S. On trust models and trust evaluation metrics for ad-hoc networks. *IEEE Journal on Selected Areas in Communications*, 2006, 24(2): 318-328
- [6] Sun Y, Yu W, Han Z, Liu K J R. Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 2006, 24(2): 305-319
- [7] Liang Zheng-Qiang, Shi Wei-Song. Enforcing cooperative resource sharing in untrusted Peer-to-Peer environments. *Journal of Mobile Networks and Applications-Springer*, 2005, 10(6): 771-783
- [8] Chang Jun-Sheng, Wang Huai-Min, Yin Gang. DyTrust: A time-frame based dynamic trust model for P2P systems. *Chinese Journal of Computers*, 2006, 29(8): 1301-1307(in Chinese)
(常俊胜, 王怀民, 尹刚. DyTrust: 一种 P2P 系统中基于时间帧的动态信任模型. *计算机学报*, 2006, 29(8): 1301-1307)
- [9] Chen Fei-Fei, Gui Xiao-Lin. Research on dynamic trust-Level evaluation mechanism based on machine learning. *Journal of Computer Research and Development*, 2007, 44(2): 223-229(in Chinese)
(陈菲菲, 桂小林. 基于机器学习的动态信任评估模型研究. *计算机研究与发展*, 2007, 44(2): 223-229)
- [10] Lin Chuang, Wang Yuan-Zhuo et al. Research on network dependability analysis methods based on stochastic Petri net. *Acta Electronica Sinica*, 2006, 34(2): 322-332(in Chinese)
(林闯, 王元卓等. 基于随机 Petri 网的网络可信性分析方法研究. *电子学报*, 2006, 34(2): 322-332)
- [11] Li Xiao-Yong, Gui Xiao-Lin. Research on adaptive prediction model of dynamic trust relationship in Open distributed systems. *Journal of Computational Information Systems*, 2008, 4(4): 1427-1434
- [12] Li Xiao-Yong, Gui Xiao-Lin. Developing scalable reputation mechanism for large-scale P2P application. *DCDIS Series B*, 2007, 14(S2): 15-19
- [13] Li Xiao-Yong, Gui Xiao-Lin. Engineering trusted P2P system with fast reputation aggregating mechanism//Proceedings of the IEEE International Conference on Robotics and Biomimetics. Sanya, China, 2007: 2007-2012
- [14] Li Xiao-Yong, Gui Xiao-Lin. A comprehensive and adaptive trust model for large-scale P2P networks. *Journal of Computer Science and Technology*, Accepted
- [15] Li Xiao-Yong, Gui Xiao-Lin et al. Novel scalable aggregation algorithm of feedback trust information. *Journal of Xi'an Jiaotong University*, 2007, 41(8): 879-883(in Chinese)
(李小勇, 桂小林等. 基于 DDT 的反馈信任信息聚合算法. *西安交通大学学报*, 2007, 41(8): 879-883)
- [16] Nena Lim. Consumer's perceived risk: Source versus consequences. *Electronic Commerce Research and Application*, 2003, 2(3): 216-228
- [17] Ziegler C-N, Lausen G. Spreading activation models for trust propagation//Proceedings of the IEEE International Conference on e-Technology, e-Commerce, and e-Service (EEE-04). Taipei, China, 2004: 83-97
- [18] Yulmetyev R M, Emelyanova N A, Gafarov F M. Dynamical Shannon entropy and information Tsallis entropy in complex systems. *Physica A*, 2004, 341(11): 649-676
- [19] Liang Zheng-Qiang, Shi Wei-Song. Analysis of recommendations on trust inference in open environment. *Journal of Performance Evaluation*, 2008, 65(2): 99-128



LI Xiao-Yong, born in 1975, Ph. D. candidate. His current research interests include trusted network and dynamic trust management.

GUI Xiao-Lin, born in 1966, professor, Ph. D. supervisor. His research interests include grid computing, cloud computing and dynamic trust management.

Background

With the widespread applications of large-scale open environments, such as Grid computing, Ubiquitous computing, P2P computing, Ad hoc networks, etc., the technology of dynamic trust management has become a significant requirement from a network economics' point of view, and trust evaluating and predicting mechanism has become a determining factor for any given service's success. But the dynamic nature of trust creates the biggest challenge in measuring trust value and predicting trust relationship amongst peers. In recent years, many of state-of-the-art trust models have been proposed, and some of them are very innovative and elaborate, but most of the studies still have some limitations: (1) Many current trust models use simple or one-sided trust decision factors to quantify and predict trustworthiness of service providers or requesters, which may lead to inaccurate or unfair outcome of trust decision. When trust relationship between peers cannot be fairly defined, it is unstable, and difficult to manage and predict. (2) In many of previous studies, the subjective assigning method to weights of trust decision factors cannot reflect trust decision scientific and reasonable, and may lead to misjudgment of trust decision result.

Focusing on these problems, in this paper, a novel dynamic trust quantization model with multiple decision factors based on information entropy is proposed, in which multiple decision factors, including direct trust, trust risk function, feedback trust, incentive function and active degree, are incorporated to reflect trust relationship's complexity and uncertainty in various angles. Also, the weight of classification is set up by information entropy theory for these decision factors, which overcomes the shortage of traditional method, in which the weight is set up by subjective manners, and makes the model has a better rationality and a higher practicability. Simulation's results show that, compared to the existing trust quantization metrics, the model in this paper is more robust on trust dynamic adaptability, has remarkable enhancements in the system's security.

This work is supported by the National Nature Science Foundation of China (No. 60873071); the National High-Tech Research and Development Plan of China (863) (No. 2008AA01Z410); Program for New Century Excellent Talents in University of China (NCET No. 05-0829); Scientific and Technological Project in Shaanxi Province, China (No. 2007K04-05).