基于多维决策属性的网络用户行为可信度评估

蒋 泽, 李双庆, 尹程果
(重庆大学 计算机学院, 重庆 400044)

摘 要: 针对已有模型在动态适应性、主观分类权重、决策属性建模粗糙等方面的不足, 提出了一种新的网络用户行为可信评估模型。采用更完善的决策属性来衡量用户行为可信性, 基于 AHP原理计算直接可信度, 运用信息熵理论客观的分类方法, 确定各个决策属性的权重, 并通过加权几何平均融合各决策属性。实验结果表明, 该模型能够准确评价网络用户行为的可信性, 反映网络用户行为可信性的动态变化特性。与传统模型相比, 在准确度和安全性方面有了很大提高。

关键词: 多维决策属性; 权重; 用户行为可信; 用户行为评估
中图分类号: TP393 文献标志码: A 文章编号: 1001-3695(2011)06-2289-05
doi:10.3969/j.issn.1001-3695.2011.06.078

Evaluating network user behavior trust based on multiple decisions attributes

JIANG Ze, LI Shuang-qing, YIN Cheng-guo
(College of Computer Science, Chongqing University, Chongqing 400044, China)

Abstract: Aiming at solving the problems of the bad dynamic adaptability, subjective classification weighting and the roughness of decision attributes modeling, this paper brought out the concept of a new evaluating model of the user behavior trust. With adopting more comprehensive decision attributes to evaluate the user behavior trust and also founding on the AHP principle to calculate the direct reliability, introduced the objective classification method from the information entropy theory to ensure each decision attribute weight and syncretism each decision attribute by weighted geometric mean. The experiment shows that user behavior trust can be proved correctly and its dynamic adaptability also can be validated. Comparing with traditional models, dynamic adaptability of this model have been largely improved by performing a simulated experiment.

Key words: multiple decision attributes; weight; user behavior trust; evaluation of user behavior

引言

网络用户行为可信评估是一个复杂的分析推理过程, 它是与上下文和时间相关的一个动态过程, 可信性的动态性和模糊性将是评估的最大挑战, 随着时间的变化, 用户之间的行为上下文可能会动态地变化, 并且具有时间滞后性的特点[1]。对网络用户行为进行可信度评估, 依赖于行为上下文和时间。在这个评估过程中, 对某一时间段采样得到行为证据值, 是一个相对静态和稳定的量, 采样的时间粒度影响评估结果的准确程度。所以, 网络用户行为可信尽管是动态变化且是模糊的, 同时也是可以量化的。其技术关键在于选取合理的网络用户行为证据、建立有效的评估模型以及对评估结果进行动态更新。通过直接或者间接的方式获取行为可信证据, 建立可信度评估模型, 根据上下文和时间动态地进行可信度更新。每次交互过程中, 在时间和获取的行为证据上下文的触发下, 都会对可信度进行调整。即使用户没有发生网络行为, 其网络行为可信度的评估结果也会随着时间变化而改变。因此, 在对网络用户行为进行可信度评估时, 需要从多个角度综合考虑影响评估的决策因子, 注重可信度的上下文和时间, 从而更准确地反映网络用户行为可信性。

已有模型对比分析

现有的理论成果有效地推动了相关研究的发展, 主要有以下几种网络用户行为可信评估模型:

a)基于模糊理论的行为可信评估。Song等人提出了一种网格环境下的实体之间基于模糊逻辑的动态可信模型(fuzzy-trust model); 唐文提出了一种基于模糊集合理论的可信管理机制; 耿延军等人发表了基于模糊理论的行为可信评估研究等[2]。

b)基于贝叶斯网络和行为日志挖掘。根据交互的历史经验, 计算出各属性可信等级的先验概率, 选择最大的先验概率计算本次交互的条件概率, 最后选择条件概率最大的可信等级作为本次评估的结果。

c)基于 BP神经网络行为可信分析方法。即误差回归神经网络, 它是一种无反馈的前向网络, 网络中的神经元分层排列, 是目前应用较为广泛的神经网络之一。

d) PTM(pervasive trust management model based on D-S theory)模型。主要采用改进的证据理论(D-S theory)的方法进行建模, 可信度的评估采用概率加权平均的方法。

这些理论成果推动了相关的研究工作, 但也存在一些不足

收稿日期: 2010-10-10; 修回日期: 2010-12-07

作者简介: 蒋泽(1985-), 男, 湖南长沙人, 硕士研究生, 主要研究方向为可信计算、计算机网络(jiangze_cqu@sina.com); 李双庆(1969-), 男, 重庆人, 副教授, 硕导, 主要研究方向为嵌入式系统开发、SOA/SOC、可信计算、计算机网络; 尹程果(1986-), 男, 重庆人, 硕士研究生, 主要研究方向为嵌入式系统开发、计算机网络.

之处:

a)对影响可信性量化的决策因子考虑不全面。大多数模型对影响可信量化的决策属性考虑比较片面,特别是对有些影响上下文的细节考虑不全面,模型不能很好地刻画可信关系的复杂性和不确定性。

b)设定分类权重的方法偏于主观。各个可信属性权重分配大多采用简单的平均值法或者专家推荐法,往往不能反映客观实际情况。

c)缺少对风险因素考虑。可信与风险密切相关,可信只存在于不确定性的风险环境当中,它们之间的关系是相互的。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,那么可信也没有存在的必要,所以风险是可信产生的前提。

针对以上问题,对网络用户行为可信进行建模时,需要强调综合考察影响行为可信的多种决策属性,针对可信性的多维属性进行更精细的建模,并且在确立各决策属性的分类权重时,需要对常用的主观判断方法进行改进,使该模型具有客观性和更高的实用性。

用户行为可信评估模型的构建

. 模型相关术语定义

本文结合已有理论成果和相关课题研究,考虑计算机科学领域可信性的研究特点,对于网络用户行为可信模型及文章中涉及的主要概念定义如下:

定义 1 行为(behavior)用户的一次行为是指该用户对于某项程序、数据或者应用的一次操作情况。

定义 2 用户行为可信(user behavior trust)在两个或多个用户之间交易时,根据用户在交易过程中所表现的行为作出评价。

定义 3 用户行为可信评估模型(user behavior trust evaluating model)研究在特定网络环境和特定时间内,根据过去直接的或间接的行为接触经验,对双方事务中客体用户的行为,评估其符合主体期望的主观认定的一种模型。它包括可信的定义、可信的评价、可信关系的形式化表示和推导、可信度的计算和存储等。

定义 4 可信度 trust(X, Y) 可信度用一个三元组(X, Y, trust)来表示。对某个用户行为的信任程度大小,是用户行为可信的量化评价指标。其中:X是对客体进行可信评估主体的集合;Y是被可信主体评估的客体集合;trust表示 A、B之间的可信度,且 trust(X, Y)∈[0, 1]。

定义 5 用户类型(user type)描述网络中不同用户担任的角色。根据担任角色的不同,用户分为三种类型:服务提供者(SP)、服务请求者(SQ)和推荐者(FD)。

定义 6 决策属性(decision attribute)用户行为可信关系量化的一个组成部分,行为可信通过各个决策属性根据不同的权重比合成来体现。模型根据具体网络环境特点,选取合适的决策属性数目,计算出各个决策属性的可信度,确定权重比例,综合成用户行为总体可信度,评估用户行为可信性,为可信管理决策提供基础。

. 用户行为可信评估建模的分析

建立用户行为可信评估模型,首先要分析行为可信性的特点,明确行为可信评估需要注意的问题。本文通过对行为可信性的研究,分析了建模过程中需要解决的关键问题:

a)主客观的有机统一。可信性是一个主观概念,即可信评估的评价是主观的,但是评估所依赖的内容必须是客观的,兼顾可信性主客观的特点。

b)可信关系的合理量化。可信是模糊和不确定的,通过各个决策属性对其进行量化,将其转换为对各个决策属性的计算。

c)可信评估的动态性。主要体现在上下文和时间的变化,用户的行为可信与特定的网络环境和应用有关,同时也要考虑近期评估的重要性和远期行为的衰减性等时间特性。

d)可信是有条件传递。A信任 B,B信任 C,那么,A通过 B的推荐也可以信任 C,但是这种推荐是有条件的,呈现出逐步递减的特点。

e)行为可信的风险评估。可信和风险是一对矛盾统一体,在可信评估的同时需要进行风险分析。

f)可信评估的防欺骗和欺骗惩罚。可信性的"慢升快降"特点为有效控制欺骗行为提供了思路,建立可信关系时,采取保守的"慢升"可信度方法来防范欺骗,而采取"快降"的方式来惩罚欺骗。

g)行为评估的规模性和有效性。用户行为的可信评估应该基于用户长期大量的行为,用户行为必须体现一定的活跃程度,这样才有稳定性和代表性,才能作为用户可信决策的依据。

针对建模分析过程提出的几个关键问题,本文将会引入直接可信度、间接可信度、可信风险系数、行为活跃度、行为奖惩因子等决策属性,从多个角度量化用户行为可信关系,并进行总体可信度的量化、计算,建立用户行为可信评估模型,为用户行为可信的预测、控制和管理提供基础。

. 各个决策属性的计算

2.3.1 直接可信度(direct trust degree)

直接可信度表示在给定的上下文中,用户根据直接交互行为的历史记录而得出的对另外一个用户的信任程度。直接可信度可以通过软硬件直接测量得到的数据,经过规范化处理等步骤来得到。

本文采用基于 AHP(层次分析方法)的原理来计算直接可信度。其方法是:将用户行为可信逐层分解、细化为可以直接测量的原始数据,从而计算得到直接可信度值。AHP方法一般分为五个步骤:建立层次结构模型、构造判断矩阵、层次单排序及一致性检验、层次总排序、层次总排序的一致性检验等。如果问题只需要相邻两层次之间的因素排序,只需前三步即可[3]。

设 n为用户行为可信所包含的可信属性的数目总和,m为所有可信属性中包含可信度证据项数的最大值,如果没有达到最大值,则设对应的权重值为 0。e_{ij}为第 i个可信属性的第 j个证据值,ω_{ij}表示对应证据值的权重,且 $e_{ij}\in[0,1]$,$\omega_{ij}\in[0,1]$,e_{ij}为经过规范化处理的证据值。所有的异构证据经过归一化处理,得到可信度计算所能利用的数值。

在获得了底层证据值并对其规范化后,利用规范化后的证据值和用 AHP方法确定的各证据的权重对各用户行为特性进行评估,评估公式为

$$E * W E^{T}=\begin{bmatrix} e_{11} & e_{1k} & \cdots & e_{1m} \\ \vdots & \vdots & & \vdots \\ e_{i1} & e_{kk} & \cdots & e_{im} \\ e_{n1} & e_{nk} & \cdots & e_{nm} \end{bmatrix}\begin{bmatrix} w_{11} & w_{1k} & \cdots & w_{1m} \\ \vdots & \vdots & & \vdots \\ w_{i1} & w_{ik} & \cdots & w_{im} \\ w_{n1} & w_{nk} & \cdots & w_{nm} \end{bmatrix}^{T}$$

其中: E为证据矩阵, W E为权重矩阵, 结果取主对角线元素值或者计算主对角线的值即为各可信属性值, 在获得了各个可信属性的评估值之后, 再利用属性评估值和各属性的权重, 就可以对整体用户行为进行评估, 从而最终得到直接可信度的计算公式为

$$T_1(x_i, x_j) = P^T * WP = (p_1 \cdots p_i \cdots p_n)(wp_1 \cdots wp_i \cdots wp_n)^T = \sum_{i=1}^{n} p_i w_i \quad (1)$$

其中: P为用户行为属性评估值向量, WP为行为属性的权重向量。对于得到的权重, 还要进行层次排序和一致性检验, 以符合要求。如果没有通过检验, 则需要重新调整和修正矩阵, 使其满足需求。

2.3.2 间接可信度 (indirect trust degree)

间接可信度表示用户间通过第三者的间接推荐形成的可信度。引入间接可信度的目的是在特定的上下文中, 可以直接获取的行为证据不足, 或者从未与待评估用户发生过直接交互行为情况下, 需要通过第三方为桥梁来获取可信度, 且第三方与这两者之间均有直接可信关系, 第三方可以是单个节点, 也可以是一条信任链。

假定有 n个推荐者, 设为推荐者集合 $\{R_1, R_2, \cdots, R_n\}$, $T_1(R_k, x_j)$表示第 k个用户推荐者对用户 x_j的直接可信度。x_i对 x_j的间接可信度为 $T_2(x_i, x_j)$, L为推荐者所在的层数, 即网络中推荐者距离用户评估者的跳数, λ_k为第 k个推荐者的推荐因子, 则间接可信度的计算公式为

$$T_2(x_i, x_j) = \begin{cases} \dfrac{\sum_{k=1}^{n} (\lambda_k \cdot T_1(x_k, x_j))}{\sum_{k=1}^{n} \lambda_k} & n > 0 \\ 0 & n = 0 \end{cases} \quad (2)$$

由于推荐者与评估者之间的距离不同, 间接可信度也不一样, 不能简单进行算术平均, 所以引入了推荐因子。离评估者距离越近, 推荐的信息也越可靠, 推荐因子也越大。当不存在推荐者时, 则间接可信度值为 0。推荐因子定义为

$$\lambda_k = \begin{cases} 1 & l = 0 \\ \prod_{m=0}^{l} T_1(x_m, x_{next}) & l > 0 \end{cases}$$

其中: l为推荐者距离评估者的跳数, $T_1(x_m, x_{next})$表示从 x_i对 x_j的可信路径上推荐者 x_m对后继的用户节点 x_{next}的直接可信度值。当 l = 0时, 表示评估者对自己的可信; 当 l = 1时, 表示评估者的所有邻居推荐者。

. . 可信风险系数

Lim等人认为, 可信与风险密切相关, 可信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影响的。如果商务交易、交互行为中没有风险, 即用户的行为是确定的, 那么可信关系也没有存在的必要, 风险是用户行为可信产生的前提[4,5]。

可信风险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。其来源主要有两个方面: 一是用户实体之间进行直接交互而产生的直接可信风险; 二是在没有历史交易记录的情况下, 其他推荐者的间接推荐带来的可信风险。在计算可信风险系数时, 需要构造一个风险评估函数来量化不同情况下的风险。定义如下:

$$R(s_{ij}, f_{ij}, \omega) = \omega^{\sum f_{ij}} \omega \in (0, 1)$$

其中: s_{ij}和 f_{ij}分别表示用户 x_i与 x_j交互过程中, x_i用户认为交互成功和失败的次数, ω 表示可信度值。进一步可以得到总体可信风险系数公式如下:

$$R(x_i, x_j) = \alpha \cdot R_{直}(s_{ij}, f_{ij}, \omega) + (1-\alpha) \cdot R_{间}(s_{ij}, f_{ij}, \omega)$$

其中: α∈ (0, 1)表示权重, 称为风险对可信度的调节因子。$R(x_i, x_j)$可信风险系数值取决于直接可信风险和间接可信风险。可信和风险有这样的反比关系: 可信度越高, 风险就越低; 反之, 可信度越低, 风险就越高, 本文中近似地认为: 可信度值 + 可信风险值 ≈ 1。所以, 最终得到的可信风险系数计算公式如下:

$$T_3(x_i, x_j) = 1 - R(x_i, x_j) \quad (3)$$

通过式 (3)也可以得出, 用户的可信级别高, 发生恶意行为的概率就低, 否则相反; 所提供服务的级别越高, 可能的风险也就越大。

. . 行为活跃度

行为活跃度是指用户在网络中与其他用户发生交互行为的活跃程度与稳定程度。推荐者用户个数越多, 表示与用户有成功交互记录的其他用户个数越多, 活跃度越高, 也说明该用户具有较高的可信度, 其他用户愿意与该用户进行交互。活跃度也作为一个决策属性引入到行为可信度的计算当中。

$$\theta(x) = 1 - \left(\frac{1}{x} + \Omega\right), \quad T_4(x_i, x_j) = \frac{1}{2} \times (\theta(x_j) + \theta(total)) \quad (4)$$

其中: θ(x)表示活跃度函数; x代表活跃用户的个数; Ω 为一个属于 [0, 1]的任意常数。设 R为推荐者用户的个数, total为所有与 x_j交互行为的用户的个数, 行为活跃度与 x_j这两者呈正比关系, 推荐者用户和与 x_j有交互行为用户的个数越多, 活跃度值也就越大。

. . 行为奖惩因子

行为奖惩因子是指为了防范恶意用户的欺骗行为和鼓励正常用户提供高的服务质量而引入的一个决策属性。网络环境的开放性使得网络中可能存在着大量不可靠的服务以及欺骗、伪造等行为。例如文件共享系统的资源下载中途失效; 电子交易中的会话劫持和伪造信息等。本文引入奖惩因子体现出对失败交易的惩罚性, 可以有效避免恶意用户对系统的攻击, 减少用户随意改变服务质量而导致的交易失败, 降低或者避免网络中的欺诈行为。奖惩因子函数如式 (5)所示:

$$T_5(x_i, x_j) = \frac{\alpha \times S(x_i, x_j) + \beta \times F(x_i, x_j)}{H_{total}}, \quad \alpha, \beta \in [0, 1] \quad (5)$$

其中: $S(x_i, x_j)$表示 x_i与 x_j的交互成功的次数; $F(x_i, x_j)$表示 x_i与 x_j的交互失败的次数; H_{total}为总的交互次数, 通常情况下, H_{total}为成功与失败次数的总和。α 和 β 为激励和惩罚调节因子, 可信关系是具有缓慢增加、快速减少的特点, 因此在陌生或者危险的环境时, α 和 β 两者的比值较小; 当处于高可信环境时, α 和 β 的比值较大, 以适应环境的动态变化和更新。

. 基于信息熵的客观权重分类

传统的可信评估模型采用算术加权平均或者专家推荐法来分配决策属性权重, 方法简单易算, 但是使得评估结果会有较大的主观成分, 权值一旦确定便不可变动, 不能适时动态调整, 缺少自适应性, 有时还会出现决策失误。基于信息熵的权重分类方法, 以客观实验数据为基础, 根据每次获得的可信度动态更新变化, 能够很好地反映出不同上下文和时间段、各个决策属性的变化情况。

根据信息熵的定义和计算公式，对于有 n个可能取值的信源 a，其信息熵定义为

$$H(a)=-\sum_{i=1}^{n}P_i\log_2 P_i,\quad P_i=\frac{T_i}{\sum_{i=1}^{n}T_i}\quad i=1,2,3,\cdots,n$$

其中：a为信息源，P_i为 a中第 i个可能结果发生的概率值。在本文中各个决策属性的信息源为两个，分别为第 i个决策属性的可信度和不可信度，它们的概率为 $T_i(x_i,x_j)$和 $1-T_i(x_i,x_j)$。设 T_i表示第 i个决策属性的可信度，ω_i表示对应的决策属性可信度的权重值，根据信息熵的基本性质，熵函数是以横坐标为 0.5的直线轴对称分布，决策属性在两个区间发生的不确定性程度一样，不利于作出唯一的可信决策判断，同时 ω_i与 $H(T_i)$具有负向性关系，即呈反比的对应关系。因此，需要对原来公式经过适当变换和修正，本文采用式(6)来确定权重系数 ω_i：

$$\begin{cases}\omega_j=\begin{cases}\log_2 M-H(T_j) & T_j\geqslant 0.5\\ \dfrac{H(1-T_j)}{\log_2 M} & T_j\leqslant 0.5\end{cases}\\ \omega_i=\dfrac{\omega_j}{\sum_{j=1}^{m}\omega_j}\quad i=1,2,3,\cdots,m\\ 0\leqslant\omega_i\leqslant 1,\ \sum_{i=1}^{m}\omega_i=1\end{cases}\tag{6}$$

其中：M表示评估等级空间的层数；m表示决策属性的数目；w_i表示经过归一化处理后的决策属性 X_j的权重系数，结果保留小数点后两位数。

. 加权几何平均对各个决策属性进行综合

设 I_i表示第 i个决策属性可信度值，W_i是其对应的权重值，则用户行为可信综合评估结果值为

$$T_{总和}=\prod_{i=1}^{n}I_i^{W_i}\tag{7}$$

其中：$i=1,2,3,\cdots,n$，$\sum_{i=1}^{n}W_i=1$。与加权算术平均相比，加权几何平均更能够体现各个决策属性的作用，因此使得最后得到的评估效果也更加接近真实情况。在具体的评估过程中，还可以将两者进行综合，即采用混合平均的方法。

建立用户行为可信评估等级空间

建立用户行为可信评估等级空间，目的是将获得的用户行为可信度与服务级别相对应，根据不同的可信度级别提供相应等级的服务质量，从而实现用户行为可信的评估、预测和控制。

定性评估项的结果通常是以等级的形式给出，最简单的定性评估结果为“是”或“不是”，最常见的定性指标结果的表现形式通常是一个有序的名称集，如“很差”“差”“一般”“好”。在用户行为评估方面，对于定性的评估项，就可以采取这些表示方式。对于定性评估项的最简单的定性评估结果，即评估结果为“是”或者“否”的情况，归一化处理可以采用直接法，即分别对应为“1”或者“0”。当定性指标采用“很差”“差”“一般”“好”的方式进行描述时，可以根据它们的次序粗略地分别分配一个整数来实现结果的量化，具体取什么样的值可以根据指标的测量结果而定。

模拟实验

目前应用比较广泛的可信模型评测方法是通过计算机模拟实验，来对具体的应用场景以及不同用户之间的交互行为进行模拟评估和性能分析，这样可以从多个角度分析可信模型在解决实际问题时的效果。本文以 P2P网络文件共享和下载作为研究内容，探讨在该网络环境下，通过建立用户行为可信评估模型，服务提供者对用户评定可信等级，对于不同敏感度等级的用户，采取不同强度的控制措施和提供不同等级的服务质量。

. 实验环境设置

本文设想的应用场景为文件共享和下载服务，即用户的目标是下载其所需的文件，服务提供者即评估者的目标是根据不同可信度等级的用户提供相应的服务。在这里考虑到实验的可操作性和有效性，本文对 P2P网络文件共享进行了简化，假定文件共享网络是理想的，所有用户的身份都已得到可信认证，用户的行为定义为从所有拥有其所需文件的用户中，选择满足可信要求的用户，完成交互(下载)。

模拟实验参数设置为：规模为 1 000个用户节点的模拟网络，拥有的文件总数为 5 000个，将这些文件随机地分配到所有用户中，并保证每个用户至少拥有一个文件，每个用户完成至少一次交互行为，模拟的次数为 100次。

a)实验中用户角色的设定：用户分为三种角色，即服务提供者、服务请求者和反馈者。这三者是相互独立的，也就是说一个用户可以包含多种角色身份，但几个身份相互独立、互不影响。

b)实验中用户的设定：主要分为三种类型，第一类为正常用户 NU，无论是提供上传文件服务还是对其他用户的评价上，都是可信的；第二类是恶意用户 BU，这类用户能提供正常的服务，但是总是存在夸大、冒名、诋毁其他用户的行为；第三类是失效用户 LU，这类用户没有恶意的反馈行为，但是提供的服务不能满足服务请求者要求。

c)实验中服务提供者所提供的服务质量分为三种类型：第一类是总能提供可靠的服务；第二类总是拒绝提供服务；第三类则是根据时间和可信等级的变化动态地提供前两种服务。

d)建立用户行为可信度评估等级 $T=\{t_1,t_2,t_3,t_4,t_5\}=\{0.0,0.2,0.4,0.6,0.8,1\}$，相应的可信级别—服务映射如表 1所示。

表 1 可信级别—服务映射表

序号	可信度	可信关系级别	服务级别
1	[0.0,0.2)	很低	拒绝
2	[0.2,0.4)	低	拒绝(只读)
3	[0.4,0.6)	正常	允许下载
4	[0.6,0.8)	高	快速、可靠
5	[0.8,1]	很高	快速、安全、可靠

. 实验过程

根据本文的算法流程和计算公式，在用户行为可信评估过程中，需要计算各个决策属性的可信度，得到相应的权重值并最终综合成行为总体可信度。

以对某个用户进行行为可信度评估为例，实验中本文根据 AHP原理来计算用户行为的直接可信度，通过软硬件工具获得了直接行为可信证据，总共有 16种，如表 2所示。然后采用 Yaahp软件来建立层次结构模型，构造判断矩阵并计算出结果。

表 2　用户行为证据表

代号	证据名称	可信属性分类
I_1	IP包传输时延	性能属性
I_2	IP包吞吐量	性能属性
I_3	IP包响应时间	性能属性
I_4	IP包延迟抖动时间	性能属性
U_1	用户 IP包丢失率	可用性属性
U_2	无故障服务次数	可用性属性
U_3	连接建立成功率	可用性属性
U_4	IP包误码率	可用性属性
S_1	非法连接次数	安全性属性
S_2	感染病毒数目	安全性属性
S_3	尝试越权次数	安全性属性

对测得的该用户行为证据值进行规范化后，小数点保留两位，得到如表 3所示的值。

表 3　用户行为证据规范化处理

名称	I_1	I_2	I_3	I_4	U_1	U_2	U_3	U_4	S_1	S_2	S_3
数值	0.13	0.25	0.38	0.24	0.35	0.26	0.11	0.28	0.36	0.34	0.30

利用 YaahP软件建立层次结构模型，确定各证据的权重值，并计算直接可信度的值。其具体过程如图 1～3所示。

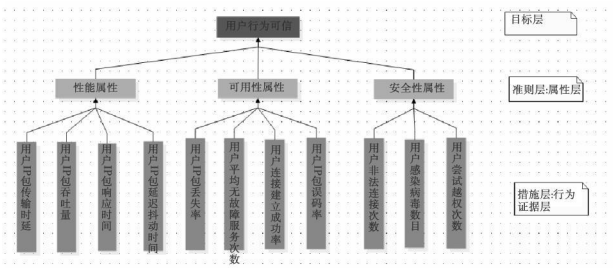

图1　建立层次结构模型

图2　计算行为证据的权重

图3　计算直接可信度

最终得到该用户的直接可信度为 0.2412。同时，该用户有三个推荐者，一个是邻居节点，另外两个距离该用户的跳数分别为 2和 3，推荐因子为 0.5、0.2和 0.1，对该用户的直接可信度为 0.35、0.25、0.15，根据式（2）可以得到间接可信度为 0.30。该用户在 100次的交互行为中，成功次数和失败次数分别为 80次和 20次。在该网络环境中，该用户的直接可信度和间接可信度值均低于 0.5，说明可信风险较大，设定风险调节因子为 0.5，根据式（3）计算得到可信风险系数值为 0.26。该用户的推荐用户为三个，根据式（4）计算得到行为活跃度为 0.11，最后根据式（5）得出该用户的行为奖惩因子为 0.16。评估等级空间的层数设置为五层，各个层的阈值分别是 0.2、0.4、0.6、0.8和 1，根据式（6）得到各个决策属性的权重比为 0.24、0.24、0.21、0.14、0.17，最后根据式（7）对各个决策属性的可信度进行综合得到总体可信度为 0.23。查询评估等级空间和可信级别—服务映射表，该用户可信度等级为低，所能获得的服务级别为拒绝服务（只读）。

. 性能分析

对网络用户行为可信进行评估，可信决策的准确性和动态适应性是衡量一个可信评估系统性能的主要指标。在各种不确定因素的动态影响下，能够提供准确、可靠、高效的服务与否是衡量服务提供者好坏的主要参考依据。实验以用户交互成功率作为准确性和动态适应性衡量标准，高的交互成功率说明模型具有高的准确性和动态适应能力。实验性能分析如图 4和 5所示。

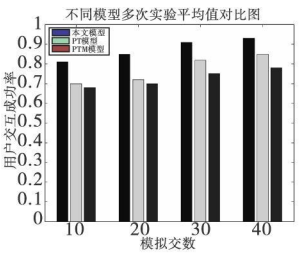

图4　不同模型准确性比较

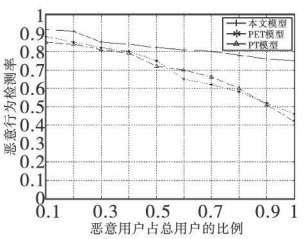

图5　不同模型安全性能比较

实验中用户的类型分别设置为：正常用户占 80%，恶意用户占 10%，失效用户占 10%。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用户都是诚实的用户，只有少部分的用户是恶意用户或者失效用户。在相对稳定的网络环境下，经过不同次数的模拟实验发现，各个模型的结果的平均值，随着运行实验次数的增多，用户交互成功率都呈现上升趋势，说明用户交互经验和活跃度越高，对于用户交互成功的帮助越大，模型能够更好地提供服务，其准确性和动态适应能力越强；同时本文模型相比其他两个模型，具有更好的准确度，性能也更稳定。

本文用恶意行为的检测率来反映模型的安全性。设在时刻 共检测到 T( )个诚实的行为，检测到 B( )个恶意的行为，而设定的恶意用户所占的百分比为 ，则恶意行为检测率表示为 β= B( )/a×（B( )+T( )）。实验结果如图 5所示。

从实验中可以看出，当网络中大部分用户为正常用户的时候，模型都具有良好的检测能力，随着网络中恶意用户比例的增加，PTM和 PT模型的性能下降得比较明显，波动比较大，而本文模型仍然有较高的检测率，说明本文模型对恶意行为的检测和抵御能力较两者高。

结束语

本文提出了一个基于多维属性的网络用户行为可信评估模型。通过引入多个决策属性来量化行为可信关系，从多个角度更精细地刻画可信性的复杂性和不确定性，基于信息熵理论确立各决策因子的分类权重，克服了常用的主观判断的确定权重方法，各个决策属性的合成也基于加权几何评估价的方法，从而使该模型具有更好的科学性和更高的实际应用价值。

（下转第 2320页）

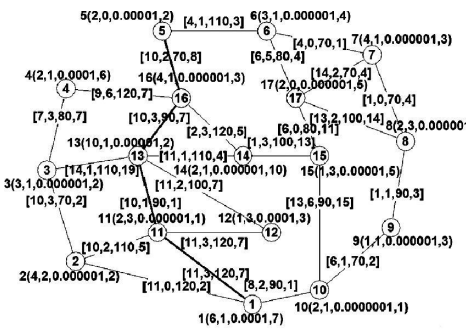

图3 采用蚁群算法发现局部路由

当采用 QoS混沌蚁群算法融合全局寻优结果如图 4所示。

图4 AC²OA_QoS发现全局路由

QoS混沌蚁群优化算法全局和局部寻优结果如表 2所示。

表 2 QoS混沌蚁群优化算法最短路由表

连接请求	路由	延时	延时抖动	丢包率	费用开销	最小带宽
1→5	1→11→13→16→5	56	14	0.000022	28	80
1→5	1→10→9→8→7→6→5	36	12	0.000014	28	70

. 算法对比实验

将混沌蚁群优化算法(AC² OA_ QoS)和一般蚁群算法 ACO 粒子群算法 PSO作对比，收敛程度比率(%)与进化代数之间的关系如图 5所示。

图 5中将 AC²OA_ QoS算法和基本 ACO PSO进行比较. 通过实验发现：一般的基本 ACO PSO分别在 79 89代才完全收敛，而 AC² OA_ QoS算法仅用 58代左右就完全收敛，且优化后得到的系统稳定性远大于基本 ACO PSO得到的系统稳定性。因此，AC² OA_ QoS算法比其他优化算法简单、优化效果好、收敛速度快，得到全局最优点的能力更强。

图 6为用 AC²OA_ QoS算法、基本 ACO PSO逐次迭代时路径传输时延的变化情况。从图中可以看出，本文中 AC² OA_ QoS算法传输延时较小，可以快速有效地搜索到系统最优解，其他算法执行时间相对较长。

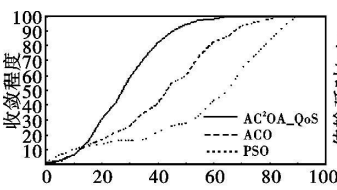

图5 算法收敛过程

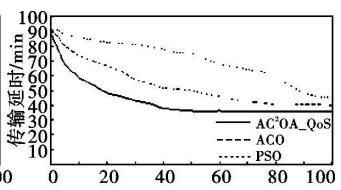

图6 传输延时的变化曲线

结束语

本文提出一种多约束 QoS混沌算法与蚁群算法融合的算法(AC² OA_ QoS)，将混沌算法融入到蚁群算法的具体过程中，利用混沌优化提高蚁群算法搜索的效率，避免蚁群算法在局部最优化，同时拓展了蚁群算法的求解范围。首先将混合算法应用到求解包含延迟、延迟抖动、带宽、丢包率和最小花费等约束条件在内的 QoS路由问题，解决了在多约束条件下查找网络系统最佳路由的方法。其次设计使不同条件所占的比重各有侧重。利用混沌算法结果设计蚁群算法信息素，并将约束条件引入，提高了算法的可靠性和准确性。通过实验表明，融合后的算法的收敛速度和求解全局最优解的效果均得到了提高，有效地克服了基本算法可能陷入局部最优解的缺陷，并通过对比实验可以看出，经过较少的迭代就可以找到全局最优路径，具有较好的收敛性和自适应性。

参考文献：

[1] WHITE T, PAGUREK B, OPPACHER F. ASGA: improving the ant system by integration with genetic algorithms[C] // Proc of the 3rd Conference on Genetic Programming (GP/SGA'98). Wisconsin: University of Wisconsin Madision, 1998: 610-617.

[2] GELENBE E, GHANWANI A, SRINIVASON V. Improved neural heuristics for multicast routing[J]. IEEE Journal on Selected Areas in Communications, 1997, 15(2): 147-155.

[3] COLORNI A, DORIGO M, MANIEZZO V. Distributed optimization by ant colonies[C] // Proc of the European Conference of Artificial Life. Paris: Elsevier, 1991: 134-144.

[4] MOFFAT J. Complexity theory and network centric warfare[M]. Washington DC: DoD CCRP, 2003.

[5] 李兵，蒋慰孙. 混沌优化方法及其应用[J]. 控制理论及其应用，1997, 14(4): 613-615.

[6] 张彤，王宏伟，王子才. 变尺度混沌优化方法及其应用[J]. 控制与决策，1999, 14(3): 285-287.

[7] 高尚. 解旅行商问题的混沌蚁群算法[J]. 系统工程理论与实践，2005, 25(9): 100-104.

[8] 王子才，张彤，王宏伟. 基于混沌变量的模拟退火优化方法[J]. 控制与决策，1999, 14(4): 381-384.

[9] 李亚东，李少远. 一种新的遗传混沌优化组合方法[J]. 控制理论与应用，2002, 19(1): 143-145.

[10] 王灵，俞金寿. 混沌耗散离散粒子群算法及其在故障诊断中的应用[J]. 控制与决策，2007, 22(10): 1197-1200.

(上接第 2293页)

参考文献：

[1] 李小勇，桂小林. 大规模分布式环境下动态信任模型研究[J]. 软件学报，2007, 18(6): 2-10.

[2] 林闯，彭雪海. 可信网络研究[J]. 计算机学报，2005, 28(5): 749-752.

[3] 冀铁果，田立勤，胡志兴. 可信网络中一种基于 AHP的用户行为评估方法[J]. 计算机工程与应用，2007, 43(19): 120-125, 151.

[4] 林闯，田立勤. 可信网络中用户行为可信的研究[J]. 计算机研究与发展，2008, 45(12): 3-5.

[5] 陈菲菲，桂小林. 基于机器学习的动态信任评估模型研究[J]. 计算机研究与发展，2007, 44(2): 220-229.

[6] THEODORAKOPOULOS G, BARAS J S. On trust models and trust evaluation metrics for Ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 318-328.

[7] ZHOU Run-fang, HWANG K. PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing[J]. IEEE Trans on Parallel and Distributed Systems, 2007, 18(4): 460-473.

[8] 林齐宁. 决策分析[M]. 北京：北京邮电大学出版社，2003.

[9] Trust in cyberspace[EB/OL]. [2006-07-08]. http://www.nap.edu/catalog/6161.html.

[10] The 3rd China trusted computing and information security 2008[C/OL]. [2008-10-09]. http://www.tc2008.org/zwtz.htm.