主观信任评估模型与决策方法的研究

杨玉丽[1,2] 彭新光[1] 王 峥[1]

(太原理工大学计算机科学与技术学院 太原 030024)[1] (运城学院公共计算机教学部 运城 044000)[2]

摘 要 在网上交易中,针对传统的信用度评估方法不能有效地描述商家信用度的时效性和风险性等特征的问题,提出基于多属性正态云的信任评估方法。首先生成包含5个等级的信任基云;然后引入时间衰减因子,分别从平均水平和变化率两个角度描述商家信用度历史信息,生成对应的声誉云和风险云;最后,由声誉云和风险云合成综合信任云,并计算其信任等级及信任分值。实验结果表明,该评估模型具有可行性和有效性,可为用户提供直观、有效的信任决策依据。

关键词 主观信任,信任决策,云模型,衰减因子,相似度

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.1.039

Research of Subjective Trust Evaluation Model and Decision-making

YANG Yu-li[1,2] PENG Xin-guang[1] WANG Zheng[1]

(College of Computer Science and Technology, Taiyuan University of Technology, Taiyuan 030024, China)[1]

(Department of Public Computer Teaching, Yuncheng University, Yuncheng 044000, China)[2]

Abstract Since traditional credit evaluation methods can not describe the business's creditworthiness characteristics of timeliness and risk effectively in electronic commerce transactions, a new subjective trust evaluation method based on multi-attribute normal cloud model was presented. Firstly, the standard trust cloud including five levels is generated. Then inducting time attenuation factor, the reputation cloud and risk cloud are designed to depict the average level and change rate about the credit history information respectively. Finally, the comprehensive trust cloud is synthesized with the reputation cloud and risk cloud, and its trust level and trust scores are calculated. Simulation result shows the feasibility and effectiveness of the evaluation model, which can assist people to finish trust decision-making intuitively and efficiently.

Keywords Subjective trust, Trust decision-making, Cloud model, Attenuation factor, Similarity

网上交易作为依赖于互联网技术的代表性应用,其交易模式主要包括用户和服务提供者(简称客体)两类角色。针对传统的网络安全技术不能有效地解决网上交易过程中存在的诸多安全隐患问题,研究学者尝试将主观信任机制引入到网上交易中,旨在帮助用户在面对大量提供不同服务或同类服务的客体时,可以快速、合理地选择交易客体。

近年来,信任的建模、推理规则等问题引起国内外众多学者的关注,并取得了一定的研究成果。文献[1]将模糊集合理论成功地引入主观信任模型中,运用模糊数学相关理论建模信任关系,由于所采用的隶属度函数将主观信任的模糊性精确化,因此存在模糊性不彻底的问题;文献[2]提出基于D-S证据理论的信任评估和推理方法,由于概率论不能反映主观信任模糊性的特点,因此其表现出"过度"形式化信任的趋势;考虑到主观信任的不确定性,文献[3]提出了基于主观逻辑的信任评估模型,其采用证据空间和观念空间量化信任关系,可以较恰当地描述信任的主观倾向;针对主观信任所具有的主观性、随机性和模糊性等特点,文献[4]提出基于主观信任云和信任变化云的评估方法,用于解决网上交易中用户对客体的主观评估问题;文献[5]设计了相似云算子,提出了由信任传递、合并、评估和更新算法构成的信任演化策略,并从理论上分析了各算法的时间复杂度和正确性;文献[6]提出复杂网络环境下的基于云模型的信任评估方法,针对不法分子的信用炒作和欺骗行为,设计了特殊属性的评估方法和信任惩罚方法;文献[7]提出基于云模型的信任评估方法,用于提高P2P网络的安全性。

上述文献侧重考虑主观信任的模糊性和随机性等特点,而忽略了其具有的风险性特征。本文在文献[4]的基础上,考虑了主观信任随时间衰减的特性,设计了涉及声誉和风险两个要素的细粒度的信任评估模型,试图提供一种简单、有效的信任决策方法,以有效地解决基于客体信用度信息的信任决策问题。

1 云模型简介

云模型[8]是李德毅院士在概率统计和模糊数学的基础

到稿日期:2014-02-27 返修日期:2014-04-30 本文受山西省留学基金项目(2009-28),山西自然科学基金项目(2009011022-2)资助。

杨玉丽(1979-),女,博士生,讲师,CCF会员,主要研究方向为计算机网络与安全、云计算,E-mail:yangyuliyyl@126.com;彭新光(1955-),男,博士,教授,主要研究方向为计算机网络与安全;王 峥(1974-),男,博士,讲师,主要研究方向为可信计算、云计算,E-mail:67687975@qq.com(通信作者)。

上，考虑随机性、模糊性及二者的关联性而建立的定性概念和定量数据间的互转模型，目前已在 Web 服务选择、智能算法和多准则决策等领域得到应用[9-11]。为了便于理解本文的研究思路，本节有针对性地介绍云模型的相关概念。

1.1 云的基本概念

定义 1（云和云滴[8]） 设 U 是用精确数值表示的定量论域，C 是 U 上的定性概念。若定量值 $x\in U$ 是定性概念 C 的一次随机实现，x 对 C 的确定度 $\mu(x)\in[0,1]$ 是有稳定倾向的随机数 $\mu:U\to[0,1]$，$\forall x\in U$，$x\to\mu(x)$，则 x 在论域 U 上的分布称为云，记为 $C(x)$，每个 x 称为一个云滴。

云模型采用期望 Ex、熵 En 和超熵 He 表征定性概念，并通过正向云发生器和逆向云发生器实现定性概念与定量数据间的相互转换。其中，正向云发生器根据云的数字特征 $\{Ex,En,He\}$ 产生云滴，实现定性概念到定量数据的转换，逆向云发生器将定量数据转换为定性语言值 $\{Ex,En,He\}$ 表示的概念，实现定量数据到定性概念的转换。

1.2 正态云

根据中心极限定理可以得知正态分布具有普适性，故本文以正态云为研究对象。

定义 2（一维正态云[8]） 设 $\Omega=[a,b]$ 为精确数值表示的定量论域，S 为 Ω 上的定性概念，定量值 $x\in\Omega$ 是定性概念 S 的一次随机实现，若 x 满足 $x\sim N(Ex,En'^2)$，$En'\sim N(En,He^2)$，且 x 对 S 的确定度满足 $\mu=e^{\frac{-(x-Ex)^2}{2(En)^2}}$，则 x 在论域 Ω 上的分布称为一维正态云。

2 基于云模型的信任评估框架

Huang[12]将主观信任定义为“根据对被信任方的能力和意愿的判定，信任方相信可以从被信任方获取所需服务，并愿意承担信任可能失败的风险”。由此可见，风险是主观信任的属性之一。故本文设计了包含声誉和风险两要素的信任评估模型，旨在为用户提供一种简单、有效的信任决策方法。

在网上交易过程中，简单、有效的信任决策方法可以提升用户的满意度。以 Amazon 为例，它目前采用 5 级评分机制，根据用户对客体信用度的历史评论信息，采用统计方法计算其平均信用度值，用于表征客体的可信度。表 1 列出了 7 个提供同类服务的客体的信用度评论信息。由于均值都为 4.1 分，因此用户很难合理、有效地进行信任决策。

表 1 Amazon 客体信用度评论信息

客体	★	★★	★★★	★★★★	★★★★★	均值
A	117	36	143	377	717	4.1
B	128	57	191	374	870	4.1
C	82	31	119	310	540	4.1
D	129	57	160	354	851	4.1
E	79	54	166	384	581	4.1
F	118	39	112	265	690	4.1
G	100	412	309	410	1643	4.1

考虑到 Amazon 所采用的统计方法只刻画了主观信任的随机性，却忽略其具有的模糊性和风险性等特征，本文试图采用云模型理论刻画主观信任：通过声誉云描述客体信用度的随机性、模糊性等；通过风险云量化客体信用度变化存在的风险性。基于云模型的主观信任评估过程如图 1 所示：(1)对信任等级进行划分，利用标准信任云生成器生成对应的信任基云；(2)根据客体信用度历史信息，采用改进的加权逆向云发生器生成声誉云和风险云；(3)将声誉云和风险云合成得到综合信任云；(4)确定综合信任云的信任等级；(5)根据综合信任云所属信任等级及对应的相似度值计算其信任分值，从而为用户提供合理、有效的信任决策依据。

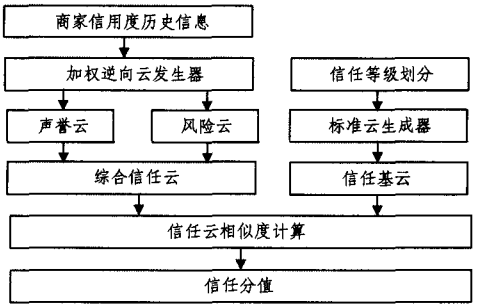

图 1 基于云模型的主观信任评估过程

3 基于云模型的信任评估

3.1 信任基云

信任等级体现信任关系的高低程度，从图 1 可以得知，它是主观信任评估模型的依据。下面通过信任基云描述不同的信任等级。

定义 3（信任基云） 对论域 $TD=[0,n]$ 进行划分，设 $TD'=\{TD_i\mid\bigcup_{i=1}^{n}TD_i=TD,\bigcap_{i=1}^{n}TD_i=\varnothing,\forall x_i,x_j\in TD_i,i<j,x_i<x_j\}$ 是 TD 的一个划分，信任确定度在 TD_i 上的分布称为信任基云，记为 $TBC=\{TBC_i(Ex_i,En_i,He_i)\}$。

由于 Amazon 采用 5 级评分机制，因此设论域 TD 的取值在[0,5]区间内，并将其分为 5 个子区间，其中第 i 个子区间为 $[R_i^{\min},R_i^{\max}](1\leqslant i\leqslant 5)$，$R_i^{\min}$ 和 $R_i^{\max}$ 分别表示区间的下限和上限。对应的信任等级、概念以及根据文献[6]的标准信任云生成器计算所得信任基云的 3 个数字特征值如表 2 所列。利用正向云发生器[8]生成的信任基云图如图 2 所示。

表 2 信任等级及信任基云

信任等级	概念	区间	信任基云
1	不信任	[0.0,1.0]	$TBC_1(0.0,0.33,0.1)$
2	低信任	[1.0,2.0]	$TBC_2(1.5,0.33,0.1)$
3	一般信任	[2.0,3.0]	$TBC_3(2.5,0.33,0.1)$
4	比较信任	[3.0,4.0]	$TBC_4(3.5,0.33,0.1)$
5	非常信任	[4.0,5.0]	$TBC_5(5.0,0.33,0.1)$

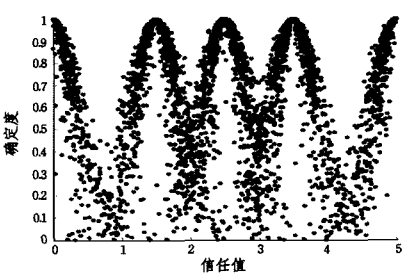

图 2 信任基云图

3.2 声誉云

定义 4（声誉云） 设 $RepD=[0,5]$ 是用精确数值表示的定量论域，$RepC$ 是 $RepD$ 上的定性概念。定量值 $x\in RepD$ 是定性概念 $RepC$ 的一次随机实现，若 x 满足 $x\sim N(Ex,En'^2)$，$En'\sim N(En,He^2)$，且 x 对 $RepC$ 的确定度满足 $\mu=e^{\frac{-(x-Ex)^2}{2(En)^2}}$，则 x 在论域 $RepD$ 上的分布称为声誉云，记为 $RepC(x)$，每个 x 称为一个云滴。

通常采用客体特定时间段内的信用度历史信息衡量该客

体的声誉。故客体的声誉与时间紧密关联，为了较为准确地描述客体的声誉，针对文献[4]中的加权逆向云生成算法采用等比率下降的方式计算时间权重，存在衰减过快的问题，本文提出改进的加权逆向云生成算法，如算法 1 所示。该算法选取余弦函数计算不同时刻的时间权重，以达到随着信用度评论时刻与当前信任决策时刻距离的增大，时间权值平缓衰减的目的。客体声誉云的生成过程如下：首先根据式(1)计算客体在不同时刻的信用度权值，然后根据算法 1 计算声誉云的 3 个数字特征值 Ex_{repu}，En_{repu} 和 He_{repu}。

$$w_i=\cos\left(\frac{\pi(t_c-t_i)}{2t_{\max}}\right) \tag{1}$$

式中，w_i 表示第 i 时刻客体信用度的时间权重，t_c 表示当前信任决策时刻，t_i 为客体信用度评论时刻，$t_{\max}$ 表示所考虑的距离当前信任决策时刻最长的时间段，超出 $t_{\max}$ 范围的信用度历史信息则不予考虑。

算法 1 改进的加权逆向云发生器

输入：客体在 t_{max} 时间段内的信用度历史信息向量 $V_{i,j}$（$V_{i,j}$ 表示在第 t_j 时刻，对客体的信用度评论为第 i 级），评论次数 K 及时间权重 w_j（$1\leqslant i\leqslant 5, 1\leqslant j\leqslant t_{max}$）

输出：声誉云 $RepC(Ex_{repu}, En_{repu}, He_{repu})$

①计算均值 $\overline{X}=\frac{1}{K}\sum_{i=1}^{5}\sum_{j=1}^{t_{max}}(V_{ij}*i*w_j)$

②计算一阶绝对中心距和方差

$$Fcm=\frac{1}{K}\sum_{i=1}^{5}\sum_{j=1}^{t_{max}}(w_j*|V_{ij}-\overline{X}|)$$

$$Var=\frac{1}{K-1}\sum_{i=1}^{5}\sum_{j=1}^{t_{max}}[w_j*|V_{ij}-\overline{X}|^2]$$

③计算 $Ex_{repu}=\overline{X}$

④计算 $En_{repu}=\sqrt{\frac{\pi}{2}}\times Fcm$

⑤计算 $He_{repu}=\sqrt{|Var-(En)^2|}$

3.3 风险云

文献[13]将风险定义为“对未来结果的不确定性”。针对用户根据客体历史信息预测其未来信任度值存在一定风险性[14]的问题，引入风险云量化其变化情况。

定义 5(风险云) 设 $RiskD=(-\infty,+\infty)$ 是用精确数值表示的定量论域，$RiskC$ 是 $RiskD$ 上的定性概念。定量值 $x\in RiskD$ 是定性概念 $RiskC$ 的一次随机实现，若 x 满足 $x\sim N(Ex,En'^2)$，$En'\sim N(En,He^2)$，且 x 对 $RiskC$ 的确定度满足 $\mu=e^{\frac{-(x-Ex)^2}{2(En')^2}}$，则 x 在论域 $RiskD$ 上的分布称为风险云，记为 $RiskC(x)$，每个 x 称为一个云滴。

风险云用于表征客体信用度变化率。本文将客体信用度变化率定义为：相邻时间窗口间客体平均信用度的变化情况，通过式(2)计算。

$$R_{rate}=\frac{\Delta V}{\Delta t}=\frac{AveV_{i+1}-AveV_i}{tw_{i+1}-tw_i} \tag{2}$$

式中，tw_{i+1} 和 tw_i 分别表示相邻的两个时间窗口，$AveV_{i+1}$ 和 $AveV_i$ 分别表示相邻时间窗口内客体的平均信用度。通过式(3)计算 tw_i 时间段内客体的平均信用度 $AveV_i$。

$$AveV_i=\frac{\sum_{j=1}^{5}[V_{i,j}*Num(V_{i,j})]}{L_i} \tag{3}$$

式中，L_i 表示 tw_i 时间段内的客体信用度评论条数；$Num(V_{i,j})$ 表示 $V_{i,j}$ 的条数。

为了量化客体信用度的变化趋势，把相邻时间窗口内客体平均信用度的变化率作为风险云的输入云滴数据。客体平均信用度变化率的生成过程如算法 2 所示。

算法 2 客体平均信用度变化率的生成过程

输入：N+1 个带时间标记的客体平均信用度值的集合 $SetV=\{AveV_0, AveV_1, \cdots, AveV_N\}$

输出：N 个在 $(-\infty,+\infty)$ 区间内的表示信用度变化率的云滴 $Drops=\{d_1, d_2, \cdots, d_N\}$

①low=0，sup=1；

②for i=1 to N do

③ $d_i=\frac{AveV_{sup}-AveV_{low}}{tw_{sup}-tw_{low}}$

④ low++，sup++；

⑤end for

在获取风险云的云滴集合 $Drops=\{d_1, d_2, \cdots, d_N\}$ 后，根据算法 1 计算风险云的 3 个数字特征值 Ex_{risk}，En_{risk} 和 He_{risk}。其中 $Ex_{risk}=0$ 表示客体平均信用度无变化；$Ex_{risk}<0$ 表示客体平均信用度下降，并且 Ex_{risk} 越小，表示下降越明显；反之，$Ex_{risk}>0$ 表示客体平均信用度提升，Ex_{risk} 越大表明提升越明显。En_{risk} 表示客体平均信用度变化的随机性和模糊性，En_{risk} 越大表明其变化越模糊。He_{risk} 表示客体平均信用度变化的稳定性，He_{risk} 越大表明其变化越不稳定。

3.4 综合信任云

通过声誉云和风险云以及用户的应用偏好权重计算综合信任云。综合信任云 $CompC(Ex_{Comp}, En_{Comp}, He_{Comp})$ 的数字特征值通过以下公式计算：

$$Ex_{Comp}=\lambda Ex_{Repu}+(1-\lambda)Ex_{Risk} \tag{4}$$

$$En_{Comp}=En_{Repu}+\frac{Ex_{Comp}-Ex_{Repu}}{Ex_{Risk}-Ex_{Repu}}(En_{Risk}-En_{Repu}) \tag{5}$$

$$He_{Comp}=He_{Repu}+\frac{Ex_{Comp}-Ex_{Repu}}{Ex_{Risk}-Ex_{Repu}}(He_{Risk}-He_{Repu}) \tag{6}$$

采用线性内插的方法计算综合信任云的数字特征值，用户可以根据不同的偏好需求给 λ 赋值，本文给 λ 赋值为 0.8。

3.5 信任决策

为了给用户提供简单、有效的信任决策方法，参考 Amazon 目前提供的 5 级评分机制，本文采用 5 分制的信任评分机制：首先通过客体信用度历史信息生成对应的综合信任云，然后通过信任云的相似度计算方法确定该综合信任云的信任等级，最后通过式(7)计算该客体的信任分值。

$$Score=R_i^{\min}+S_{Obj}*(R_i^{\max}-R_i^{\min}) \tag{7}$$

式中，S_{Obj} 表示综合信任云与信任基云的最大相似度值，可通过文献[15]中的信任云相似度计算算法得到。$R_i^{\min}$ 和 $R_i^{\max}$ 分别表示综合信任云所属信任区间的下限和上限。

4 仿真实验

仿真实验所使用 PC 机的基本配置：Intel® Core™ i5 CPU，3GB 内存，操作系统为 Microsoft Windows XP，所采用的编程语言为 Matlab。

4.1 实例分析

为了验证本文所提出的信任评估模型的有效性，从 Amazon 网站收集了来自亚洲、北美洲、欧洲和大洋洲 4 个不同地域的 50 个提供某种同类服务的客体，每个客体在一年之内（2013 年 1 月到 2014 年 1 月）的信用度评论累计次数大于 1000，且每条信用度评论记录中包括商品名称、评论时间和评论等级。

采用随机抽取的方法，从上述 50 个客体中随机抽取 7 个

来自不同地域的客体，编号分别为 A、B、C、D、E、F 和 G，其中 A 位于大洋洲，B 和 C 位于亚洲，D 和 E 和位于北美洲，F 和 G 位于欧洲。由于提供该类服务的客体受季节气候的影响，A 的信用度评论主要集中在 2013 年的第一个季度，B、C、D 和 E 的集中在第二、三季度，F 和 G 的则集中在第四季度。根据 Amazon 信任评分机制计算所抽取客体的信任分值的结果如表 1 所列。采用本文提出的主观信任评估方法对所抽取的客体的评估过程如下：

①根据客体信用度历史信息计算该客体的声誉云。本文考虑了一年之内的客体信用度评论信息，为方便计算，设 t_{max} 为 360 天。采用式(1)计算每条评论的时间权重，并通过算法 2 计算客体声誉云的数字特征值。

②根据客体信用度历史信息计算该客体的风险云。设单位时间窗口 tw_i 为 5 天，并将所有的信用度评论记录按单位时间窗口归类。根据式(1)计算单位时间窗口内信用度的时间权重，其中 $t_i=tw_i/2(1\leqslant i\leqslant 72)$。根据式(2)和式(3)计算单位时间窗口内客体的平均信用度，并采用算法 2 生成一定数量的云滴。通过算法 1 计算风险云的数字特征值。

③根据声誉云和风险云，采用式(4)－式(6)计算实体综合信任云的数字特征值，并计算综合信任云与信任基云的相似度，确定综合信任云的信任等级。表 3 列出表 1 中客体 C 的综合信任云与各信任基云的相似度，从中可以看出，C 的相似度与“低信任云”的相似度最大，所以其信任等级为 2。

④计算客体的信任值。对于不同信任等级的客体，根据表 2 确定信任区间，采用式(7)计算其信任分值。

表 3　综合信任云与信任基云的相似度

信任基云	相似度
不信任云	0.000
低信任云	0.461
一般信任云	0.211
比较信任云	0.090
非常信任云	0.030

根据上述的评估过程计算 7 个客体的信任值，如表 4 所列。从表 4 可以看出，由于 A 中距离当前决策时刻较远的信用度评论条数所占比例最大，致使其声誉云期望值最低，信任分值也低于其他 6 个客体，B、C、D 和 E 的声誉云期望值较高，F 和 G 的声誉云期望值最高；对于 B、C、D 和 E 而言，虽然 B 与 C 的声誉云，D 与 E 的声誉云相差不大，但由于 B、D 风险云的期望值 $Ex_{risk}<0$，而 C、E 的 $Ex_{risk}>0$，因此 C、E 的信任值是分别高于 B、D 的；对于 F 和 G 两个客体而言，二者的声誉云和风险云都比较相似，但由于 F 的综合信任云的熵和超熵值都较大，致使其与信任基云的相似度低于 G，因此 G 的信任分值最高。采用文献[4]的基于主观信任云和信任变化云的主观信任评估方法对表 1 中的 7 个客体进行信任决策时，一方面，用户需要对云模型的相关知识有一定了解，才能从 7 个客体中筛选出 F 和 G；另一方面，针对 F 和 G 的主观信任云和信任变化云都比较相似的情况，文献[4]通过正向云生成算法随机地为 F 和 G 的主观信任云生成 1 个云滴用于确定选择对象的方法具有一定的盲目性。由此可以验证本文所提出的信任评估模型的可行性和有效性，它可为用户提供简单有效的信任决策依据。

表 4　客体信任值

客体	Ex_{repu}	En_{repu}	He_{repu}	Ex_{risk}	En_{risk}	He_{risk}	Ex_{Comp}	En_{Comp}	He_{Comp}	相似度	信任等级	信任值
A	1.518	1.293	0.821	0.547	0.268	0.725	1.324	1.088	0.802	0.366	2	1.366
B	2.241	1.399	0.703	−0.778	0.439	0.678	1.638	1.208	0.698	0.419	2	1.419
C	2.231	1.384	0.668	0.489	0.192	0.765	1.882	1.146	0.687	0.461	2	1.444
D	3.523	0.979	0.972	−0.632	0.087	0.509	2.692	0.801	0.879	0.447	3	2.447
E	3.502	0.912	0.836	0.523	0.135	0.423	2.906	0.761	0.753	0.300	4	3.300
F	3.936	0.962	0.960	0.465	0.308	0.985	3.242	0.831	0.965	0.446	4	3.446
G	3.936	0.939	0.949	0.465	0.032	0.076	3.242	0.321	0.774	0.533	4	3.533

4.2　仿真实验

本实验数据来自 Amazon 网站上某商家 2013 年的商品评论记录(共 1988 条)，每条记录包括评论时间和评论等级。通过对 1998 条评论记录进行分析，发现该商家信任值的变化情况为：1 到 4 月份期间呈上升趋势；5 到 6 月份呈下降趋势，7 月份到 12 月份又呈上升趋势。分别采用本文和文献[6]的信任评估模型计算该商家一年内信任值的变化情况，如图 3 所示。其中，文献[6]的评估模型记为 TAV (Trust for Average Value)，本文的评估模型记为 TAVR (Trust for Average Value and Risk)。

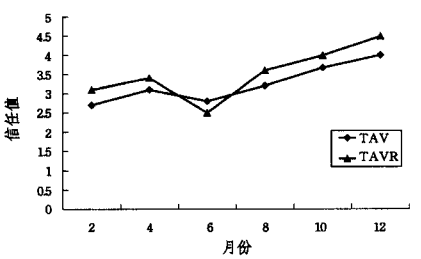

图 3　某商家的信任值

从图 3 中可以看出，两种方法都反映该商家在 5－6 月份的信任值呈下降趋势，但 TAVR 所描述的信任值下降梯度比 TAV 的大。这是因为 TAV 采用信任度的平均水平描述商家的信任值，而 TAVR 不仅考虑商家信任度的平均水平，同时也考虑其信任度变化潜在的风险，所以 TAVR 对商家信任值的描述粒度更细，致使其对商家信任值的变化情况具有更高的灵敏性，从而给用户提供更可信的决策依据。

结束语　本文以网上交易的主观信任评估问题为研究对象，在已有的工作基础之上，设计了基于云模型理论的信任评估过程，生成考虑声誉和风险两个要素的综合信任云，通过信任云相似度计算方法衡量其信任等级，计算客体的信任值，用于指导用户的信任决策。通过对真实数据的实验分析，表明本文提出的方法可以为用户提供简单、有效的信任决策依据。如何设计可以防范信任诋毁的信任评估模型是下一步的主要研究工作。

参 考 文 献

[1]　陈超，王汝传，张琳. 一种基于开放式网络环境的模糊主观信任模型研究[J]. 电子学报，2010，38(11)：2505-2509

[2]　张琳，刘婧文，王汝传，等. 基于改进 D-S 证据理论的信任评估模型[J]. 通信学报，2013，34(7)：167-173

[3] Jøsang A, O'Hara S. Multiplication of Multinomial Subjective Opinions[C]// Proceedings of the International Conference on Information Proceeding and Management of Uncertainty. Dortmund, Germany, 2010: 248-257
[4] 王守信，张莉，李鹤松. 一种基于云模型的主观信任评估方法[J]. 软件学报，2010，21(6)：1341-1352
[5] Du Wei, Cui Guo-hua, Liu Wei. An uncertainty trust evolution strategy for e-Science[J]. Journal of Computer Science and Technology, 2010, 25(6): 1225-1236
[6] 张仕斌，许春香. 基于云模型的信任评估方法研究[J]. 计算机学报，2013，36(2)：422-431
[7] 陆玲玲，徐建，张宏. 人类心理认知习惯与云模型相结合的 P2P 信任模型[J]. 计算机科学，2012，39(8)：38-41
[8] Li De-yi, Liu Chang-yu, Gan Wen-yan. A new cognitive model: cloud model[J]. Int J of Inteligent Systems, 2009, 24(3): 357-375
[9] 王尚广，孙其博，张光卫. 基于云模型的不确定性 QoS 感知的 Skyline 服务选择[J]. 软件学报，2012，23(6)：1397-1412
[10] 马颖，田维坚，樊养余. 基于云模型的自适应量子粒子群算法[J]. 模式识别与人工智能，2013，26(8)：787-793
[11] 任剑. 基于云模型的语言随机多准则决策方法[J]. 计算机集成制造系统，2012，18(12)：2792-2797
[12] Huang Jing-wei, Fox M. An ontology of trust: formal semantics and transitivity[C]// Proceedings of the 8th international conference on Electronic commerce. ACM, New York, NY, USA, 2006: 259-270
[13] Williams C A, Heins R M. Risk Management and Insurance [M]. New York: MC Graw Hill, 1985
[14] Wang Shou-xin, Zhang Li, Wang Shuai, et al. A Cloud-Based Trust Model for Evaluating Quality of Web Services[J]. Journal of Computer Science and Technology, 2010, 25(6): 1130-1142
[15] 杨玉丽，彭新光，付东来. 基于云模型的主观信任评估机制[J]. 计算机工程与设计，2013，34(12)：4151-4155

(上接第 143 页)

验中 Web 访问会话共有 7 个网络连接，会话字符熵平均为 0.256，TLSv1 加密会话字符熵为 0.737。可以看出，TLSv1 会话字符熵属于置信区间$[\mu-2\sigma,\mu+2\sigma]$，从而被检测为加密会话，http 会话字符熵值不属于上述区间，则被识别为一般应用。大量实验证明，$\mu=0.755$ 和 $\sigma=0.045$ 的设置对于所有实验会话具有最佳检测效果。被检测应用的会话信息熵在正态分布曲线上的位置如图 5 所示。

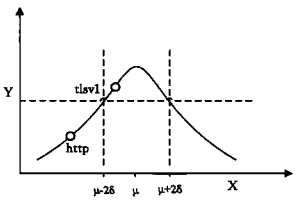

图 5 实验应用样本会话信息熵

本文选取了 48 个带加密功能的网络应用和 243 个一般网络应用，对加密应用和一般应用在真实网络环境中所产生的网络数据流进行加密会话检测。实验结果如表 1 所列。

表 1 检测结果统计

实验环境	网络状况	48 个加密网络应用			243 个一般网络应用		
		正确检测数(个)	错误检测数(个)	正确检测率(%)	正确检测数(个)	错误检测数(个)	错误检测率(%)
实验网	良好	46	2	95.8	238	5	2.05
公网	拥塞	44	4	91.7	234	9	3.7

经过大量样本实验，从正确检测率、错误检测率两个方面证明了该检测方法的可用性。在实验网环境下，由于网络状况良好、网络中丢包率低、重传包较少等原因，应用通信过程比较符合检测理想模型，因此正确检测率较高，错误检测率较低；在公网环境，拥塞的网络状况则会导致检测准确度有一定的降低。由表 1 中统计数据总体来看，该检测方法达到了比较高的正确检测率，将错误检测率降低在 5%以下，证明了该检测方法的可用性，对网络中加密会话的识别分析具有重要的意义，尤其对通过常规端口加密传输的泄密数据流检测，可从海量数据流中识别出可疑加密会话，有利于进一步针对性分析。

结束语 本文在对网络加密会话进行信息统计分析的基础上，提出基于信息熵的无指纹加密会话检测方法。该方法总结网络应用中常见字符和非常见字符在加密前后的出现规律，通过统计大量加密通信程序样本的会话信息熵并按正态分布特性训练出检测模型。检测中计算特定端口通信会话字符熵，以其熵值是否属于一定阈值范围来判断信息均匀度高低，从而进行加密会话检测。实验表明，该检测方法能够有效地检测出一般加密应用会话和加密木马会话，具有较高的正确检测率；同时，该方法高效地利用了处理器资源，在高速的网络环境中也能做到实时处理。此外，该方法已经被实际应用于网络入侵检测和木马行为监控等实时网络数据流分析当中，并取得了较好的效果，表明该方法具有很强的实用性。但是其仍存在一些不足，在时延较大的拥塞网络状况下，准确识别率略有降低，如何在拥塞网络环境下保证较高的准确识别率还有待提高。

参 考 文 献

[1] Lakhina A, Crovella M, Diot C. Characterization of Network-wide Anomalies in Traffic Flows[R]. Technical Report: BUCS-20040020. Boston University, 2004
[2] 高建明，龚亮亮，吕涛. 基于信息熵的目标平台识别方法[J]. 计算机应用与软件，2013，30(9)：171-184
[3] Kargupta H, Park B, Hershberger D, et al. Collective data mining: a new perspective toward distributed data mining[C]// Proceedings of Advances in Distributed and Parallel Knowledge Discovery. [S. l.]: AAAAI/ MIT Press, 2000: 128-175
[4] Sommer R, Paxson V. Outside the closed world: On using machine learing for network intrusion detection[C]// Proc. of 2010 IEEE Symposium on Secutiry and Privacy. 2010: 302-355
[5] 李文忠，左万利，赫枫龄. 一种基于信息熵的多维流数据噪声检测算法[J]. 计算机科学，2012，39(2)：123-144
[6] 王海龙，杨岳湘. 基于信息熵的大规模网络流量异常检测[J]. 计算机工程，2007，33 (18)：262-264
[7] Nehinbe J O. Automated technique for debugging network intrusion detection systems[C]// IEEE 2010 International Conference on Intelligent Systems, Modelling and Simulation (ISMS). Liverpool, 2010: 363-367
[8] 吴小叶，肖继民. 基于信息熵的网络异常流量的研究[J]. 广东通信技术，2008(4)：32-34
[9] Kim D S, Nguyen H N, Park J S. Genetic algorithm to improve SVM based network intrusion detection system[C]// Proc. of the 19th International Conference on Advanced Information Networking and Applications. 2005: 150-164
[10] 丁世飞，朱红，许新征，等. 基于熵的模糊信息测度研究[J]. 计算机学报，2012，30(8)：139-151