一种个性化域名信誉评价机制

孟绪颖[1,2] 王 淼[1] 张玉军[1]

[1](中国科学院计算技术研究所 北京 100190)
[2](中国科学院大学 北京 100049)

摘 要 域名解析是互联网信息服务的前提，但目前关于域名信誉评价的相关研究却尚不成熟。针对域名服务的复杂性、恶意攻击的普遍性以及用户需求的多样性等问题，提出了一种个性化域名信誉评价机制。主要贡献在于：(1)提出了基于多元指标的域名信誉评价框架；(2)设计了抵御恶意攻击的信誉计算模型，提高了计算精度和适应能力；(3)参考用户个人偏好区分域名类型，为用户选择偏好域名提供依据，优化用户体验。实验结果表明，该机制能准确反映域名的信誉状况，排除恶意评价的影响，并根据域名信誉值和用户个人偏好选择个性化域名服务，提升用户满意度。

关键词 域名；信誉评价；多元指标；抵御恶意攻击；个性化
中图分类号 TP 393 **文献标志码** A

A Customized Reputation Evaluation Mechanism for Domain Names

MENG Xuying[1,2] WANG Miao[1] ZHANG Yujun[1]

[1](*Institute of Computing Technology*, *Chinese Academy of Sciences*, *Beijing* 100190, *China*)
[2](*University of Chinese Academy of Sciences*, *Beijing* 100049, *China*)

Abstract Domain name resolution is a foundation of the Internet, yet there is still no appropriate reputation evaluation mechanism for it. Considering the complexity of domain name service and the pervasiveness of malicious attacks, a customized reputation evaluation mechanism for domain names was presented. The main contributions are: (1) a domain reputation evaluation framework based on multi-index evaluation; (2) a variety of mechanisms that resist malicious attacks and improve the precision and adaptability of the reputation computation model; (3) theoretical support for users to choose their desired service with improved experience, taking into account the users' personal preferences. Results show that the proposed customized mechanism can accurately reflect the reputation of domain names, fight against malicious evaluation attacks and improve user satisfaction.

Keywords domain name; reputation evaluation; multi-index evaluation; resistance against malicious attacks; customization

收稿日期：2015-12-28 **修回日期**：2016-01-20
基金项目：国家 973 计划项目(2012CB315804)；国家自然科学基金(61402446、61572474)；国家科技支持项目(2012BAH45B02)；中国科学院科研装备研制项目(YZ201426)；江苏省未来网络前瞻性研究项目(BY2013095-5-01)
作者简介：孟绪颖，博士研究生，研究方向为可信计算；王淼，博士，副研究员，研究方向为可信计算；张玉军(通讯作者)，博士，研究员，博士生导师，研究方向为网络安全，E-mail：zhmj@ict.ac.cn。

1 引　言

域名系统不仅用于解决地址对应问题，也是各种应用和网站建设的基础，域名是寻址访问的必备条件，是互联网各种应用的核心。一旦域名系统被恶意利用，将会给整个互联网造成无法估量的损失[1-3]，域名系统亟需一个能够如实反映域名信誉状况的评价机制[4-8]。设计良好的域名信誉评价机制能够起到三方面的作用：(1)域名信誉评价可以加深用户对域名应用和企业网站诚信度的认识，并根据用户偏好提供可靠性等服务质量信息，优化用户体验；(2)域名信誉评价可以有效地体现域名的使用情况以及企业的信誉情况，使得满足用户偏好的优质企业脱颖而出，促进企业信息化发展；(3)域名信誉评价也能根据用户偏好提供个性化服务，帮助用户过滤不感兴趣的信息、筛选出感兴趣的内容，为网络信息过滤、不良应用防范、网络搜索等提供又一个重要的参考指标，提高用户满意度。

虽然信誉评价在多种应用场景中已经得到成功应用[6-9]，但这些领域中的信誉评价机制并不完全适用于域名，域名信誉评价面临新的挑战：单一指标无法反应网页的信誉状况，针对其复杂性，需要综合考虑多元指标；针对信誉计算模型可能面临多种恶意攻击，如摇摆攻击、诋毁攻击、消极反馈及合谋攻击等[5]，需要在信誉计算模型中引入相关因素抵御攻击；用户的个人偏好千差万别，对各评价指标的偏好程度不同，需要针对不同的用户定制个人偏好。

针对域名信誉评价面临的挑战，本文提出了一种个性化域名信誉评价机制(A Customized Reputation Evaluation Mechanism of Domain Name，简称 CREMech)。该机制建立多元指标的信誉评价框架，设计抵御攻击的信誉计算模型，并参考用户个人偏好区分域名类型，为用户选择偏好域名提供依据。实验结果表明，CREMech 能合理反映域名的信誉状况，显著减少各种恶意攻击对信誉评价的影响，提升用户满意度。

本文后续章节按如下方式组织：第 2 节对相关工作进行了回顾，第 3 节描述了域名信誉评价机制，第 4 节给出了模拟实验结果，最后第 5 节对全文进行了总结。

2 相关工作

目前通过用户评价体现服务端信誉状况的方式已经较为成熟，比如用于 P2P 网络的信誉评价机制[5]、基于信誉评价的 Web Service 选择机制[6]等。虽然域名是各种应用和网站建设的基础，但目前却没有针对域名的成熟的信誉评价机制。

研究领域中，用户评价主要集中在判断域名是否为恶意网站上，评价指标单一、且抵御攻击机制不完善。Mao 等[4]提出由第三方专家对部分页面进行评估，并在优质网页不会提供恶意链接的前提下，计算出其他域名的可信度。该评价机制没有考虑专家意见的公正性、评价指标单一，而且没有建立对某些攻击的抵御机制，导致信誉评价机制可能在一定条件下失效，如当服务质量突然改变时，信誉值并不会迅速发生改变。WOT[13]提出用户对域名的可信程度、儿童安全性两项指标评分，指标仍较单一。Ronda 等[14]和 Ma 等[15]将用户行为和自动分类结合起来得到域名的可信度，但是只能区分出域名的可信度，指标依旧单一，而且没有建立对某些攻击的抵御机制，比如不区分恶意的点击事件，反而可能提高了恶意网址的可信度。

目前的域名信誉评价机制没有考虑个人偏好的差异，如 Geng 等[12]虽提出各种评价网页内容的指标，但对各域名信誉值的计算却采取相同的标准。Fouliras 等[7]提出了购物网页内具体商品的信誉评价框架，但也没有考虑个人偏好的不同。也有研究者[8-11]提出对新兴网络应用如社交

网络、微博中用户的信誉评价机制，却对不同用户采用相同的评判标准。

综上，当前针对域名信誉评价的解决方案存在评价指标单一、抵御攻击机制不完善、忽视个人偏好差异等问题，需要引入多元指标、进一步完善抵御攻击机制并参考个人偏好，最终建立个性化域名信誉评价机制。

3 个性化域名信誉评价机制

3.1 域名信誉评价框架

论文提出了如图 1 所示的域名信誉评价框架。首先收集用户对多元指标的信誉评价，通过恶意检测、合谋检测抵御恶意攻击模型筛选出正常信誉评价，计算出基于正常信誉评价的各指标信誉值；在此基础上，结合个人偏好加权求得域名总信誉值；最后结合总信誉值和个人偏好区分域名类型，对不同类型的域名进行区分操作。

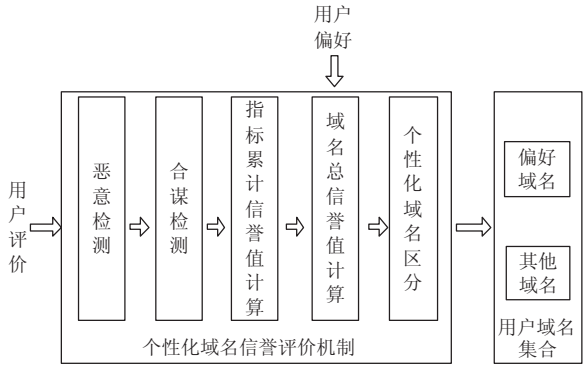


图 1 域名信誉评价框架

Fig. 1 The reputation evaluation framework of domain name

3.2 恶意检测

评价域名有多项指标，如可信度、专业度等。在一个评价周期内，用户可以对一个域名的各项指标进行评价。域名指标信誉值是指所有正常用户对一个域名某一指标的信誉评价的平均值，分为当前指标信誉值和累积指标信誉值。其中，当前指标信誉值是指在当前评价周期内的域名指标信誉值；累积指标信誉值是指当前指标信誉值和上个评价周期后的累积指标信誉值的加权和。在评价域名时，恶意节点往往提供和大多数正常用户节点相反的信誉评价，从而影响指标信誉值的公正性。计算指标信誉值的关键在于通过模糊等价矩阵动态聚类的方法识别恶意节点，从而得出能够反映域名真实信誉状况的指标信誉值。

假设在第 $t+1$ 个评价周期，集合 U_i^p 中的用户提交了对域名 i 的信誉评价。下面以域名 i 的第 m（$1\leqslant m\leqslant n$）个指标的当前信誉值 $v_{i_m}^{t+1}$ 和累计信誉值 V_{i_m} 计算过程为例进行说明。

在计算指标信誉值时，首先需要找出异常评价节点。恶意节点往往提供和大多数正常用户相反的信誉评价，根据评价差异度筛选异常评价节点，缩小恶意节点筛选范围。具体来讲，对于 $\forall k\in U_i^p$，若用户 k 对于其他用户 l 满足

$$\frac{1}{n}\sum_{m=1}^{n}\sqrt{\frac{\sum_{l\in U_i^p,l\neq k}(v_{ki_m}^{t+1}-v_{li_m}^{t+1})^2}{h}}>\zeta \tag{1}$$

则称用户 k 的评价异常。其中，$\left|U_i^p\right|=h$；$v_{ki_m}^{t+1}$（$1\leqslant k\leqslant h$）表示第 k 个用户对域名 i 的第 m 个指标的信誉评价；ζ 为异常检测阈值。评价异常的节点组成异常节点集合 U_i^u 。

3.3 合谋检测

在异常节点集合 U_i^u 中，采用模糊等价矩阵动态聚类的方法识别合谋攻击节点，进一步筛选恶意节点。合谋检测过程如下。

(1) 计算用户的评价相似度：对集合 U_i^u 中的任意两个用户，用距离法计算它们在当前评价周期的评价相似度。对 $\forall e,f\in U_i^u$，假设 e、f 共同对 x 个域名的 y 个指标进行了评价，则 e、f 的评价相似度为

$$sim_{ef}=1-\sqrt{\frac{\sum_{i=1}^{x}\sum_{m=1}^{y}(v_{ei_m}^{t+1}-v_{fi_m}^{t+1})^2}{xy}} \tag{2}$$

(2) 构造模糊相似矩阵：对集合 U_i^u 中的节

点按照公式(2)计算建立相似模糊矩阵 $\boldsymbol{R}$，$\boldsymbol{R}$ 满足自反性和对称性，采用平方法求 $\boldsymbol{R}$ 传递闭包 $t(\boldsymbol{R})$，$\boldsymbol{R}^*=t(\boldsymbol{R})$为模糊等价矩阵，$r_{ef}^*$ 为 $\boldsymbol{R}^*$ 中的第 e 行第 f 列的值。

(3)剪边聚类：取 $\lambda\in[0,1]$，构建不同的等价矩阵 $\boldsymbol{R}_\lambda^*$，将矩阵 $\boldsymbol{R}_\lambda^*$ 中的第 e 行第 f 列的值 $r_{\lambda ef}^*$ 定义为：

$$r_{\lambda ef}^*=\begin{cases}1, & r_{ef}^*\geqslant\lambda\\ 0, & \text{其他}\end{cases} \tag{3}$$

若 e、f 行中的每列的值都相同，则 e、f 为同一类，将符合该条件的节点聚为同一类，其中数量最大的一组为合谋节点集合 U_i^c，异常节点集合 U_i^u 中的其他节点为正常节点。

3.4　指标累计信誉值计算

筛选出正常节点后，定义域名 i 的第 m 个指标在评价周期 $t+1$ 的当前信誉值 $v_{i_m}^{t+1}$ 为：

$$v_{i_m}^{t+1}=\frac{\sum\limits_{k\in U_i^f}v_{ki_m}^{t+1}}{d} \tag{4}$$

其中，$U_i^f=U_i^p-U_i^c$ 为筛选出的正常节点集合，$\left|U_i^f\right|=d$。

定义域名 i 的第 m 个指标在 $t+1$ 个评价周期后的累计信誉值 $V_{i_m}^{t+1}$ 为：

$$V_{i_m}^{t+1}=\begin{cases}\mu\times v_{i_m}^{t+1}, & t=0\\ (1-\mu)\times V_{i_m}^{t}+\mu\times v_{i_m}^{t+1}, & t>0\end{cases} \tag{5}$$

其中，μ（$0<\mu\leqslant1$）为信誉学习因子，μ 越大，先前的经验就越容易被遗忘。人类社会信誉是缓慢增加、快速减少的，也就是说信誉的增加和减少是不对称的，为了检测和惩罚节点的摇摆攻击行为，引入自适应的信誉学习因子：

$$\mu=\begin{cases}\alpha, & v_{i_m}^{t+1}-V_{i_m}^{t}\geqslant-\varepsilon\\ \beta, & \text{其他}\end{cases} \tag{6}$$

其中，$0\leqslant\alpha<\beta\leqslant1$，使得信誉降低的速度比增加的速度快。参数 ε 规定了评价时误差容忍范围。

3.5　域名总信誉值计算

不同类型的用户对域名的各项指标有不同的关注度，比如游戏爱好者更关心趣味性，金融业者更关心可信度，而学生家长则更关心文明健康度。对于域名的 n 个评价指标来讲，用户根据不同的需求可以设置不同的偏好程度，并用个人偏好向量表示。假设用户 k 的偏好向量为 ω_k，$\omega_k=(\omega_{k1}\ \ \omega_{k2}\ \cdots\ \omega_{km}\ \cdots\ \omega_{kn})$，其中 ω_{km} 表示用户 k 对指标 m 的偏好程度，且满足 $\sum\limits_{m=1}^{n}\omega_{km}=1$。

定义域名 i 对用户 k 在 $t+1$ 个评价周期后的总信誉值为：

$$SV_{ki}^{t+1}=\sum_{m=1}^{n}V_{i_m}^{t+1}\times\omega_{km} \tag{7}$$

3.6　个性化域名区分

由 3.5 中计算出域名总信誉值，在考虑个人偏好的同时进一步区分偏好域名和其他域名，提升用户满意度。根据各指标信誉值和总信誉值的范围，使用公式(8)识别域名 i 的类型，域名总信誉值和各指标信誉值都满足用户偏好的域名即为偏好域名，否则为其他域名。

$$i\in\begin{cases}U_k^g, & V_{i_m}^{t+1}\geqslant\delta\times\omega_{km}(m\in[1,n]),SV_{ki}^{t+1}\in[\delta,1]\\ U_k^b, & \text{其他}\end{cases} \tag{8}$$

其中，U_k^g 为用户 k 的偏好域名集合；U_k^b 为用户 k 的其他域名集合；δ 为偏好域名与其他域名的分界阈值。

大多数评价系统只是将评分供用户参考，没有根据其偏好进行相应的区分。CREMech 根据各指标信誉值及总信誉值区分出域名类型，为用户选择合适服务提供理论依据，如屏蔽所有不良域名等，有效优化了用户体验。

4　机制评价

本节通过模拟实验对 CREMech 的信誉反映

状况、抵御攻击的能力和服务满意度等指标进行评价。

4.1 实验环境

本节采用实验方法实现了 CREMech，并与 PeerTrust（PSM/DTC Basic 和 PSM/DTC Adaptive）[5]机制进行了对比分析。其中，PeerTust 基本时间窗口中的交易次数设为 100，自适应时间窗口中的交易次数设为 20。模拟实验部署在 Chrome 浏览器上，如图 2 所示。

图 2 模拟实验平台

Fig. 2 A sample scenario title

在模拟试验中，每个域名有 3 个评价指标，根据各指标信誉值将域名分为高质量、普通质量和低质量域名，各指标信誉值区间分别对应 [0.8, 1]、[0.4, 0.6]、[0, 0.2]。模拟 10 000 个用户，用户对域名指标的评分范围在 0～1。根据评分范围将用户划分为不相交的两类：正常用户和恶意用户，其中恶意用户又划分为合谋用户和消极反馈用户（始终占恶意节点的 10%）。其中，正常用户是指提供公正评价的用户；合谋用户是提供虚假评价、保持相同攻击行为的用户，即一致提供过低/高的评分；消极反馈用户是指对域名的各指标给予随机信誉值的用户。现实中，极少存在绝对诚实或绝对不诚实的用户。所以，正常用户有 90% 的可能提供公正评价；而合谋用户也是有 90% 的可能提供虚假评价，10% 的可能提供公正评价。

实验按照设定的参数完成初始化后，用户根据使用情况对域名进行评价。信誉计算模型定期对用户的评价进行收集，计算服务的信誉值。

其他的实验配置参数如表 1 所示。

表 1 实验配置参数表

Table 1 System parameters

参数	描述	值
ζ	异常检测阈值	0.55
λ	合谋检测阈值	0.60
α	信誉增长学习因子	0.10
β	信誉减少学习因子	0.35
ε	最大误差容忍范围	0.01
$\omega_{k1}:\omega_{k2}:\omega_{k3}$	用户 k 的个人偏好向量	2∶3∶5

4.2 实验结果

4.2.1 信誉反映状况

本节考察使用 CREMech 后域名的信誉反映状况，假设所有用户都属于正常节点，即所有用户对域名提供公正评价，实验结果如图 3 所示。从图 3 可以看出，CREMech 能够准确反映域名的信誉状况，使得高质量域名得到更高的信誉值。

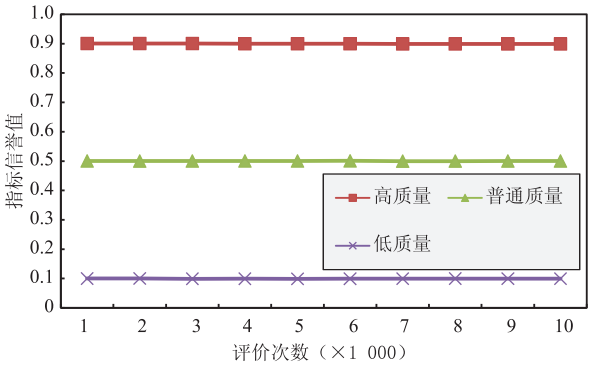


图 3 指标信誉值随评价次数的变化情况

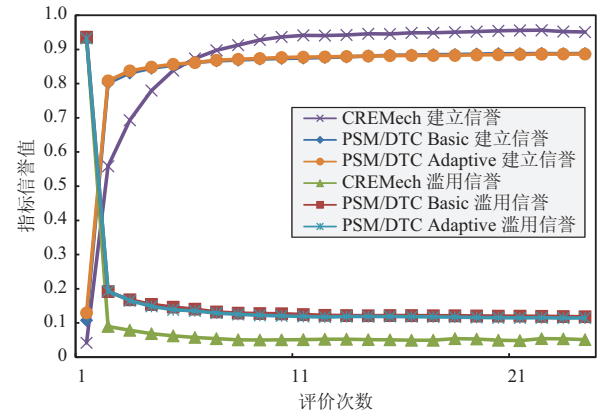
Fig. 3 Index reputation value with number of evaluations

4.2.2 抵御攻击的能力

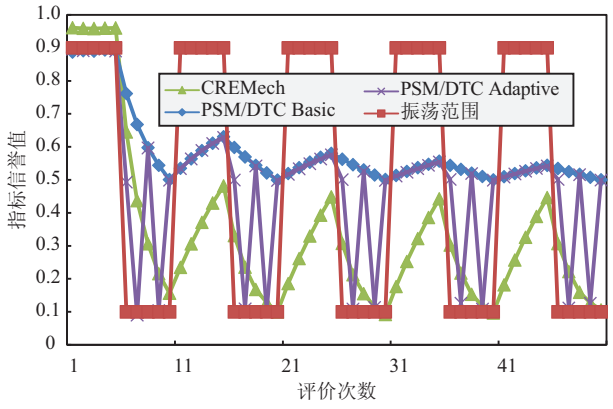
本节考察 CREMech 和 PeerTust 机制抵御摇摆攻击和合谋攻击的性能比较。

图 4 给出了不同场景下，通过 CREMech 和

PeerTrust 机制计算得到的指标信誉值。摇摆攻击中恶意服务节点的行为可以分为三种情况：高信誉域名提供低档服务，滥用信誉；低信誉域名提供高档服务，建立信誉；域名周期性的提供高低档服务，维持较高信誉。图 4(a)显示了在前两种情况下域名的指标信誉值变化曲线。当高信誉域名提供低档服务时，三种机制最终都导致信誉值下降，但是 CREMech 对域名行为的改变更敏感，能更快地下降信誉值并保持稳定；当低信誉域名恢复提供高档服务建立信誉时，三种机制最终都导致信誉值上升，但是 CREMech 需要更长的时间建立信誉值。图 4(b)显示了当域名在建立和滥用声誉之间摇摆时，该域名的信誉值变化曲线。同样，CREMech 对域名行为的改变更敏感，信誉值增加和减少不对称，有效惩罚了域名的摇摆行为。



(a) 建立、滥用信誉



(b) 周期振荡

图 4　对抗摇摆攻击的效果

Fig. 4　Effectiveness against aggregate feedback

由于信誉评价过程中存在着恶意用户和合谋团体干扰，信誉模型的结果可能会出现错误。设正常用户和恶意用户组成的集合分别是 X 和 Y，被信誉模型误判为恶意用户的正常用户组成集合 U_{FPR}，被信誉模型误判为正常用户的恶意用户组成集合 U_{FNR}，则误报率 FPR(False Positive Rate)为 $FPR=\frac{U_{FPR}}{|X|}$，漏报率 FNR(False Negative Rate)为 $FNR=\frac{U_{FNR}}{|Y|}$。图 5 给出了 CREMech 的误报率、漏报率随网络中恶意节点比率的变化情况。在恶意节点比率低于 50% 时，CREMech 能较准确地识别出恶意节点。实验表明，CREMech 对恶意攻击具有明显的抑制作用，可以有效地排除恶意节点的干扰，表现出更强的适应性。图 6 显示了高质量域名的信誉值随着恶意节点比率的变化情况，在恶意节点比率低于 50% 时，CREMech 能正确反映域名的信誉状况，不受恶意节点的干扰，而使用 PeerTrust 机制的信誉值随着合谋节点的增加而降低，无法有效抵御恶意攻击。

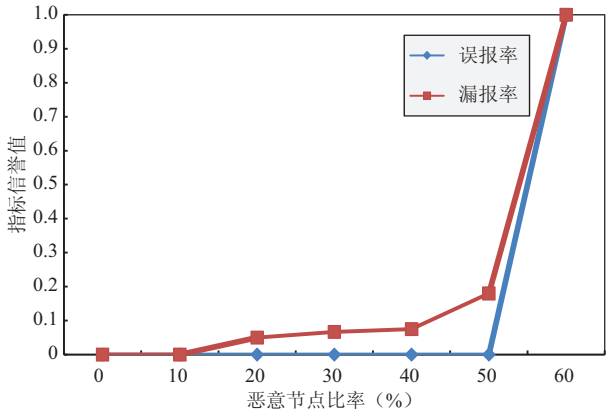


图 5　误报率和漏报率随恶意节点比率的变化情况

Fig. 5　FPR and FNR with malicious node ratio

4.2.3 服务满意度

本节考察 CREMech 和 PeerTrust 机制使用后

的用户体验的比较。

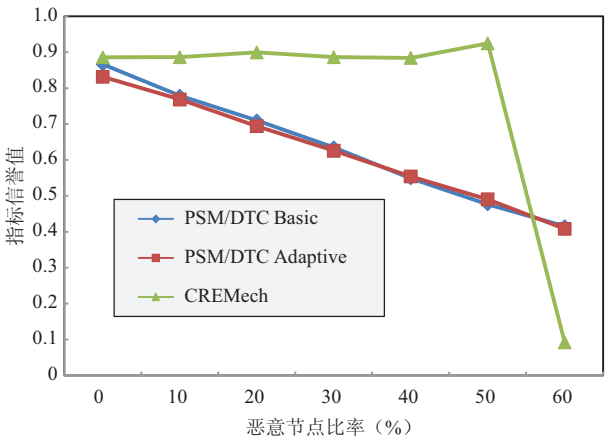


图 6 指标信誉值随恶意节点比率的变化情况

Fig. 6 Index reputation level with malicious node ratio

在评价周期内，用户成功访问域名的各指标信誉值比率和个人偏好向量的相似度越高，用户体验越好。设用户 k 在评价周期内访问的域名集合为 U_k，定义指标信誉比率 V_{km} 为域名集合 U_k 中第 m 个指标信誉值总数占所有指标信誉值总数的比率。

$$V_{km}=\frac{\sum_{i\in U_k} V_{ki_m}}{\sum_{i\in U_k}\sum_{x=1}^{n} V_{ki_x}} \tag{9}$$

各指标信誉比率构成指标信誉向量 $\left(\frac{\sum_{i\in U_k} V_{ki_1}}{\sum_{i\in U_k}\sum_{x=1}^{n} V_{ki_x}},\frac{\sum_{i\in U_k} V_{ki_2}}{\sum_{i\in U_k}\sum_{x=1}^{n} V_{ki_x}},\cdots,\frac{\sum_{i\in U_k} V_{ki_n}}{\sum_{i\in U_k}\sum_{x=1}^{n} V_{ki_x}}\right)$。计算用户 k 的指标信誉向量和个人偏好向量的相似度，定义用户满意度 ST_k 间接反映用户体验情况。

$$ST_k=1-\sqrt{\frac{\sum_{m=1}^{n}\left(\frac{V_{km}-\omega_{km}}{\omega_{km}}\right)^2}{n}} \tag{10}$$

从图 7 可以看出，随着偏好域名和不良域名的分界阈值 δ 的升高，用户满意度并不一定升高。当分界阈值 δ 为 0.6 时，更多的总信誉不高的用户偏好域名被划分为偏好域名，这些域名的各项指标的差异更明显；而当 δ 为 0.9 时，各项指标的值都比较高，各指标之间的差异不明显，用户满意度较低。但和 PeerTrust 机制相比，CREMech 更能优化用户体验、提升用户满意度。

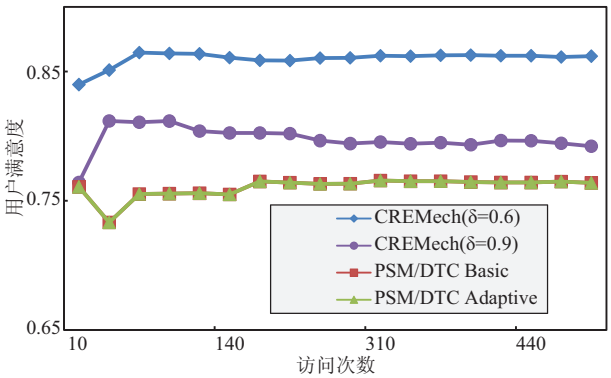


图 7 用户满意度随访问次数的变化情况

Fig. 7 Satisfaction level with number of evaluations

4.3 与其他方法的对比

目前关于域名的信誉评价研究主要是基于域名内容的，以 DUP(Dynamic User Profiles)[16]为例，表 2 显示了 CREMech 和基于域名内容的域名信誉评价机制 DUP 各方面能力的对比结果。

表 2 域名信誉评价机制功能对比

Table 2 Comparison between CREMech and DUP

功能	CREMech	DUP
域名信誉	动态获取域名信誉	动态获取域名信誉
多特征	支持	不支持
抵御攻击	支持	不支持
个性化服务	个人设置用户偏好	动态提取用户偏好

与基于域名内容的域名信誉评价机制 DUP 相比，CREMech 和 DUP 都能够动态获取域名信誉值，但 DUP 只支持词频这一类特征，而 CREMech 可以分别对多项特征进行分析。同时，DUP 也没有考虑域名信誉的摇摆攻击，而 CREMech 能检测和惩罚域名的摇摆攻击行为，并快速准确地反映域名信誉值的变化。由于 DUP 能根据用户历史点击的域名内容分析用户

偏好，所以能够更快速地反映用户偏好的变化，而 CREMech 的用户偏好是由个人设置的，无法实时反映用户偏好的变化。综上所述，CREMech 能够分析域名多特征的信誉值，并更准确快速地反映域名各指标信誉值的动态变化，但 DUP 能够更快速地反映用户偏好的变化。

5 结　论

本文从用户体验的角度提出基于多元指标的信誉计算模型，并在信誉计算模型中引入了多种机制抵御恶意攻击，提高了信誉计算模型的计算精度和适应能力，同时，在信誉计算模型中引入个人偏好，优化了用户体验。模拟实验表明，使用 CREMech 能准确反映域名的信誉状况，抵御恶意攻击，提升用户满意度。

由于域名服务对各种应用和网站建设极其重要，下一步需要重点研究的问题是如何将本文的个性化域名信誉评价机制应用到实际的系统中，如域名推荐系统、恶意网站拦截系统等。随着研究的进一步深入，个性化域名信誉评价机制将在更多合适的领域中发挥作用。

参 考 文 献

[1] Xiang G, Hong J, Rose CP, et al. CANTINA+: a feature-rich machine learning framework for detecting phishing web sites [J]. ACM Transactions on Information & System Security, 2011, 14(2): 613-613.

[2] Yadav S, Reddy AKK, Reddy ALN, et al. Detecting algorithmically generated malicious domain names [C] // Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement, 2010: 48-61.

[3] Labovitz C, Iekel-Johnson S, Mcpherson D, et al. Internet inter-domain traffic [J]. ACM Sigcomm Computer Communication Review, 2010, 40(4): 75-86.

[4] Mao J, Dong XS, Li P, et al. Rating web pages using page-transition evidence [M] // Information and Communications Security, Springer, 2013: 49-58.

[5] Xiong L, Liu L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities [J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857.

[6] Ye B, Pervez A, Ghavami M, et al. A trust-based model for quality of web service [C] // SERVICE COMPUTATION 2013, the 5th International Conferences on Advanced Service Computing, 2013: 39-45.

[7] Fouliras P. A novel reputation-based model for e-commerce [J]. Operational Research, 2013, 13(1): 113-138.

[8] Sherchan W, Nepal S, Paris C. A survey of trust in social networks [J]. ACM Computing Surveys, 2013, 45(4): 115-123.

[9] Shen H, Liu G. Harmony: integrated resource and reputation management for large-scale distributed systems [C] // Proceedings of the 20th International Conference on Computer Communications and Networks, 2011: 1-6.

[10] Nitti M, Girau R, Atzori L. Trustworthiness management in the social Internet of things [J]. IEEE Transactions on Knowledge & Data Engineering, 2014, 26(5): 1253-1266.

[11] Chai W, Xu W, Zuo MY, et al. ACQR: a novel framework to identify and predict influential users in micro-blogging [C] // Pacific Asia Conference on Information Systems, 2013: 1-15.

[12] Geng GG, Jin XB, Zhang XC, et al. Evaluating web content quality via multi-scale features [J]. Eprint Arxiv, 2013.

[13] WOT. WOT reputation data enhances user experience [OL]. [2015-12-28]. https://www.mywot.com/en/business.

[14] Ronda T, Saroiu S, Wolman A. Itrustpage: a user-assisted anti-phishing tool [C] // Proceedings of the 3rd ACM SIGOPS/EuroSys European Conference on Computer Systems, 2008: 261-272.

[15] Ma J, Saul LK, Savage S, et al. Beyond blacklists: learning to detect malicious web sites from suspicious URLs [C] // Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2009: 1245-1254.

[16] Hawalah A, Fasli M. Dynamic user profiles for web personalisation [J]. Expert Systems with Applications, 2015, 42(5): 2547-2569.