基于行为流图的可信交互检测方法

易树平†, 李嘉佳, 易 茜

(重庆大学 机械工程学院，重庆 400044)

摘 要: 为保障人-网站交互的可靠性和可信性,以探寻交互行为模式的独特性为出发点,采用行为流图描述用户与网站的交互活动,通过分析可信交互行为模式提取与用户生理及心理特性相关的交互行为特征,提出一种以可信行为特征作为度量的可信交互检测方法,并基于某网站真实日志数据验证所提可信行为特征的功效. 将用户一次会话作为记录单元,描绘出用户与交互环境、工具、会话行为和所在页面4个维度相结合的行为流图;然后,依据数据分析,提取可信行为特征参数并使用SMOTE算法平衡数据集;最后,利用决策树和随机森林算法完成用于检测交互可信性的模型训练与测试. 通过实验对实际数据进行检测,所提出方法在决策树模型中对用户不可信行为的错误接受率为0.44 %,随机森林算法中则低至0.31 %. 研究结果表明,可信行为特征的组合具有用户可辨别性和独特性,证明了人-网站交互行为模式具有个体特性,与他人存在差异性,可用于检测交互行为发起者与账户真实所有者间身份的一致性.

关键词: 人-网站交互；可信交互；行为流图；可信行为；机器学习；决策树；随机森林

中图分类号: TP181 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2018.1618 **开放科学(资源服务)标识码(OSID):**

引用格式: 易树平,李嘉佳,易茜. 基于行为流图的可信交互检测方法[J]. 控制与决策, 2020, 35(11): 2715-2722.

Trustworthy interaction detection method based on user behavior flow diagram

YI Shu-ping†, LI Jia-jia, YI Qian

(College of Mechanical Engineering，Chongqing University，Chongqing 400044，China)

Abstract: A trustworthy interaction detection method based on user behavior flows is proposed to ensure the dependability and trustworthiness of human-web interaction. Firstly, the behavior flow diagram is used to capture the all relevant factors of user behavior from web log, in which the uniqueness is taken as the starting point of this. The behavior units are recorded as “one session”. The behavior flow diagram describes the interactions in four dimensions, namely interactive environment, interactive tool, session behavior, and the current page. Then, the behavior features related to individual psychology and physiology are extracted as trustworthiness measures on the basis of data analysis. After balancing the data set through synthetic minority over-sampling technique (SMOTE), the training and testing trustworthy interaction detection model are completed by the aid of the decision tree and random forest algorithm. Finally, an instance is given to illustrate that the false accept rate (FAR) of the untrustworthy behavior of the proposed method in decision tree model is 0.44 %, while it is as low as 0.31 % in random forest. The results indicate that the combination of trustworthy behavior features has differentiation and uniqueness among users, which proves that the behavior patterns of human-web interaction have personality and distinguishable otherness with someone else. It can be used to detect identity consistency between the dominator of interactive behavior and the real owner of an account.

Keywords: human-web interaction；trustworthy interaction；behavior flow diagram；trustworthy behavior；machine learning；decision tree；random forest

0 引 言

可信交互是指网站注册账户的真实所有者与网站间发生的交互,该账户被他人使用的过程不具有可信性. 账户是在网络上用来证明用户身份的一串符号,被划分为一次性账户、常规账户、敏感账户、发言人账户和高价值交易账户[1],除一次性账户以外的账户类型都与用户个人信息、业务工作和财产利益相关联.

收稿日期: 2018-11-23；**修回日期:** 2019-04-15.

基金项目: 国家自然科学基金项目(71671020)；重庆市技术创新与应用发展专项重点项目(cstc2019jscx-mbdxX0049).

†通讯作者. E-mail: yshuping@cqu.edu.cn.

为有序开展在线活动,第三方网络要求用户上传的相关个人信息以数据组合形式表示用户在线身份. Hille等[2]认为随着网络犯罪份子窃取用户身份进行恶意操作的意图上升,用户对于在线身份被盗窃的恐惧也越发增涨. 盗用者操纵他人账户的过程是不被信任的交互过程,将导致账户所有者蒙受各类损失,如何及时判别和阻遏这种不可信交互、保障用户不受损是一个亟需解决的问题.

Andrew[3]采用地理定位检测账户是否处于可被信任的常在位置,但位置信息易伪造,发生误判的可能性很高. Aljawarneh等[4]尝试通过检查账户登录者拥有的标识物体判断登录凭证的可信性,例如带有嵌入式芯片的智能卡,然而添加额外的硬件设备既增加成本投入,又具有较高遗失风险. Malathi等[5]基于生物特征(如指纹、虹膜等)识别登录者身份可信性,但当这些特征发生伤损或老化时将影响识别准确率.

行为认证方法将不易被他人模仿的个人行为模式作为用户数字指纹[6],若当前行为与用户行为库中的模式不一致,则推断当前用户身份不可信. 在人机交互领域,大多针对用户在某一种操作中的行为表现进行研究,如网站访问浏览模式[7]、社交消息发布模式[8]、击键行为模式[9]、鼠标使用模式[10]等. Ruan等[8]通过检测正在发生的社交行为与账户历史行为模式的匹配性判断帐户是否被盗,Barbon等[11]提出了一种纯文本挖掘方法用于检查发布内容是否存在不可信风险,这两种方法依赖于社交网络的特有属性,在其他类型网站上适用性不强. 用户对计算机的常见输入行为——键盘敲击[12]和鼠标操作[10]也可被用于检测操作行为的可信性. Ho等[9]将用户在特定按键上具有的不同打字速度作为基本行为模式,以此区分真正用户与盗用者. Shen等[10]建立了一种鼠标使用行为模型进行用户身份验证,所提出方法的错误接受率为1.38%. 键盘和鼠标行为数据的采集与系统日志不同,需要添加单独代码并与现有系统集成. 目前,利用日志中行为信息的可信交互检测尚无量化结果,也暂未发现将人-网站交互行为模式用于检测交互可信性的研究.

基于此,本文提出采用行为流图描述服务器日志中反映人-网站交互行为的客观信息,从4个维度再现用户会话交互过程,作为交互行为模式的表征. 应用统计分析发现行为流图中指示个体一致性或差异性有4大类行为表现,与这些表现相关的14个行为特征可用于可信交互检测. 借助机器学习方法的决策树和随机森林算法,基于真实数据构建可信交互检测模型,测试验证其检测效果. 通过实例表明,所提出方法在随机森林模型中的不可信行为错误接受率为0.31%,在决策树中也较低,为0.44%,对不可信行为的检测力较强. 可信交互检测追踪的是网络用户实体,关注个体与网站间交互行为模式,探究带有个体特性的行为表现,将其定义为用户可信交互行为模式. 本文研究结果证明了以可信行为特征构建的组合是属于个体的,具有独特性,在人-网站交互中可用于检测交互行为的可信性,为保障网络交互安全的可信性检测方法提供了新的思路.

1 可信检测

对于注册账户而言,只有由所有者发起的行为才被视作可信,其他非本人的所有行为均不可信,通过对交互行为可信性的判断即可检测人-网站交互可信性.

1.1 交互行为

网站系统产生大量日志信息,其中包含人-网站交互数据,但日志记录庞杂,涉及许多无关交互行为的信息,且数据格式刻板,无法直接展现有意义的信息. 通过对原始日志数据进行清洗、用户标记、会话标记及格式化处理后,提取出用户交互行为信息,以网络行为流图再现式地呈现人-网站交互过程,作为用户交互行为模式的可视化表达形式. 4个一级行为要素包括:用户对交互环境与工具的选择行为(I、II)、会话过程行为(III)以及页面访问行为(IV).

用户X某日内一次会话交互行为流和页面操作流如图1和图2所示. 同一用户在一天内产生一次或多次会话,同一会话中用户所选择交互环境与工具不发生改变,但不同会话间可能发生变化. 用户访问常见来源(III. iv)有4种:直接输入网址、点击收藏夹中网址、点击外部预留链接、搜索关键词或相关信息. “时间戳”信息从多个维度分解:当前会话发生星期(III. i)、会话请求开始时间整点(III. ii)和此次会话持续时间(III. iii),这些均与个人偏好习惯和行为选择相关. 人-网站交互均带有目的性,交互过程访问的页面(IV)是对总目标的分解. 以访问页面作为行为流图中间节点,将交互过程分解为若干步骤,中间节点上负载若干行为信息,所涉及的操作事件信息见图2. 通过行为流图描述交互行为模式有助于发现日志记录中潜在有用的客观信息,为构建可信行为特征组合提供更全面的选择.

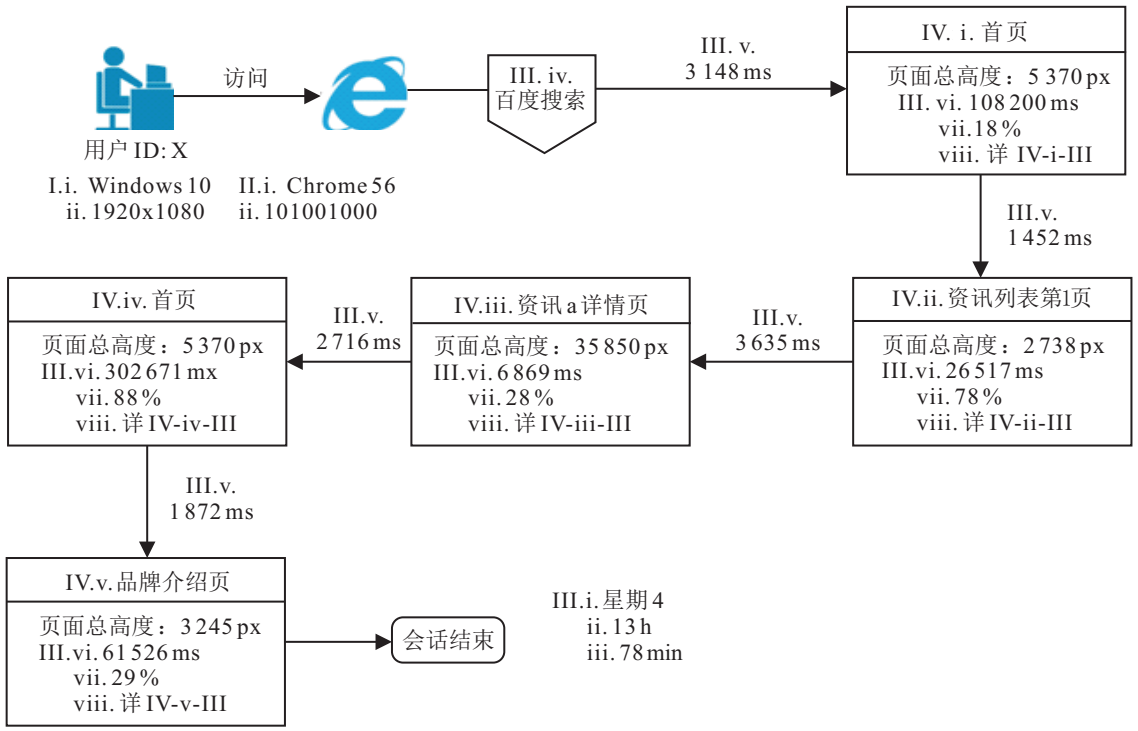

图 1　用户X行为流

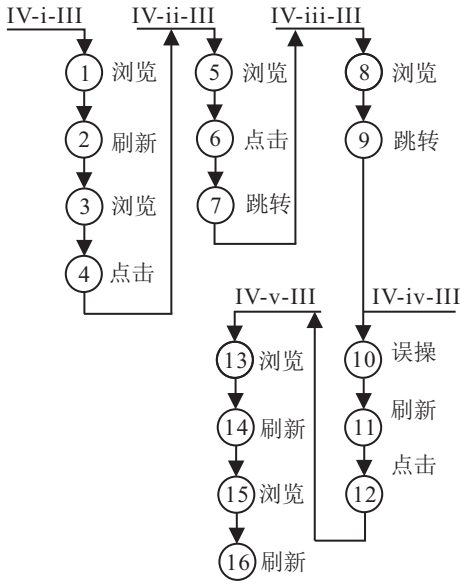

图 2　用户X操作事件流

1.2　可信交互

可信交互是对交互过程的研究,强调过程中的可靠性和可信任性,即由当前登录者使用此账户的过程是安全的,允许授予交互权限. 交互过程会产生一系列交互行为,要保证交互过程可信必须先保证交互行为可信. 如果行为是可信的,则它是可以被预期的,总与用户惯性不相悖,并带有个性特征. 本文采用可信交互行为作为可信交互检测的特征度量,在当前主体获得账户控制权前,判断该主体行为表现是否由账户真实所有者发出,为网站决定是否继续授权于该主体提供决策参考,从而达到提高网络交互可靠性和安全性的目的.

2　可信交互行为模式与度量

以个体为中心,关注个体用户的交互行为,发现行为流图中能凸显个体一致性和差异性的可信交互行为模式,所涉及的更细粒的行为即可信交互行为特征是可信交互检测的度量.

以国内某旅行资讯网站服务日志为数据源,对随机抽取的5名用户的数据记录进行分析. 通过量化、无量纲化、数据规范化等处理方法,采用SPSS进行相关统计分析,研究个体用户与交互行为模式的相关或互异关系,下面将逐一论述.

2.1　交互工具与环境

浏览器是用户与网页承载信息交互的直接工具. 用户在其设备配置环境下,根据自我需求选择交互体验最佳的一种或多种浏览器. 对浏览器的选择是一种对交互工具的选择行为,受用户所处交互环境及其需求特性影响. 在本文数据集中,用户不局限在相同操作系统下进行交互,当操作系统发生变化时有可能选择不同浏览器,也可能一直使用同一款浏览器;也有在同样系统下更换浏览器类型的情况发生;还存在操作系统与浏览器均未发生改变的情况.

2.2　会话行为

个体的外显动作是人与环境相互作用的产物和表现,人的心理、生理、思维等内在要素对行为的可能性和趋向具有决定作用,行为科学研究表明每个人

都有其独特的行为模式[13]. 鉴于此,推论在网络环境下,人的会话交互行为模式也同样具有个体差异,下面围绕行为流图中会话行为的8个二级要素从5个方面展开分析研究.

2.2.1 单次会话操作频率

通过对一次会话(30 min内)持续时长及该次会话内总操作量的统计,计算用户操作频率,以此衡量用户动作跳转快慢.

首先,根据用户id与会话id间的对应关系归总属于各个用户的会话记录,分别统计各个会话的持续时长和操作总量,计算每名用户每次会话的操作频率. 在用户操作频率的Levene检验中sig. = 0.013 < 0.05,总体样本不满足方差齐性,故选用独立样本中位数和Kruskal-Wallis检验. 零假设1(在用户类别上,会话操作频率的中位数相同)的sig. = 0.027 < 0.05,零假设2(在用户类别上,会话操作频率的分布相同)的sig. = 0.039 < 0.05,故拒绝零假设1和零假设2. 检验结果表明用户在会话操作频率上表现出个体差异.

2.2.2 页面操作事件

对5名用户页面操作量及其类型进行占比分析后发现,用户共同的最常用操作是点击事件,但对其他操作类型的偏好各不相同.

图3为用户页面操作变化时序图,15种操作类型分别由不同颜色表示,用户在操作类型间的跳转有较大区别. 用户A会话过程中连续点击事件发生可能性更大,几乎不发生误操作;用户B对事件操作类型的选择更广,在一次会话中共进行了12种不同操作,但较易出现错误操作;用户C更倾向于“点击-浏览-查看详情-跳转”的操作组合,过程中偶尔出现操作错误;用户D和用户E所进行的操作类型相同,但用户E操作间跳跃性较强,与用户D相比,连续重复操作比例较低.

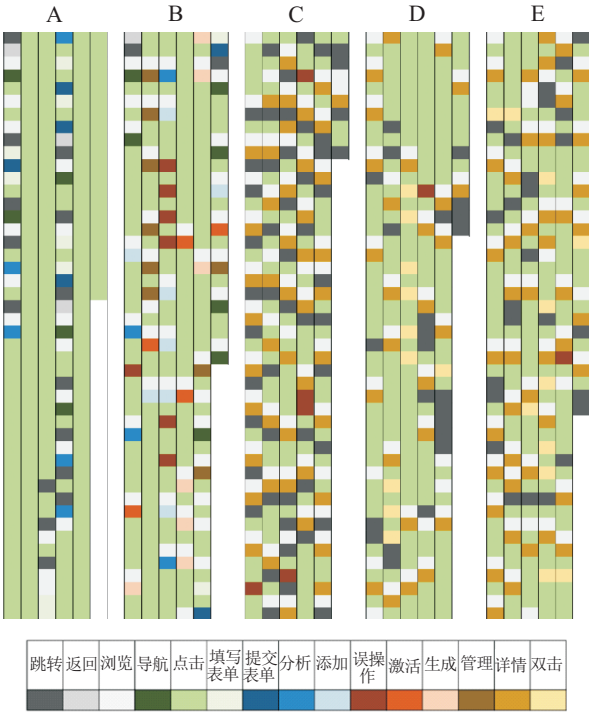

图3 页面操作时序变化

2.2.3 页面浏览与鼠标滑动

用户所浏览完成的页面高度与页面总高度间的比值称作页面浏览百分比,浏览百分比与页面总内容量的乘积被视为用户在该页面的信息浏览量. 用户向下拉动网页时产生窗口滑块滚动事件,向下滚动窗口的次数与页面内容浏览量综合反映出用户对信息的接受速度,该速度受个体理解能力和阅读速度限制.

2.2.4 页面等待

用户在网页打开前的等待时间是外部对用户个体系统的输入变量,若所需等待时间超过用户耐心阈值,则有改变原有行为轨迹的可能性. 数字性能管理平台Dynatrace发现,有将近一半人页面等待的耐心阈值为3 s,若等待时长大于其阈值则会选择离开当前页面.

2.2.5 交互界面

浏览器窗口是人与网页信息交互时直接的可视界面,用户可以自由调整窗口大小与形状,对用户进行访问调查发现交互界面形状与大小的设置因个人情况而异. 用户A偏向于直接使用浏览器自带的分屏功能,不再手动调整窗口大小与形状;用户B和用户C会根据页面内容和任务实际情况进行手动调整,以实现最佳浏览状态;由于缩小浏览页面存在着视觉障碍,用户D无论何时均会选择开启全屏浏览;用户E则会根据网页所提供信息的内容和类型进行调整;用户L只在必要时才打开全屏模式,通常会进行重置窗口大小的操作.

另外,用户在线设备的屏幕配置是交互体验的直接影响因素,也是影响可视窗口大小和鼠标点击位置的相关变量,属于用户对交互外部输入的选择.

2.3 页面访问

当前访问页面和页面停留时间与用户信息需求相关,反映用户对页面内容的兴趣程度,也间接反映用户阅读习惯倾向. 页面布局结构、导航菜单设置与个体偏好间的吻合度决定用户进一步探索当前页面的可能性. 若用户对页面内容更感兴趣或当前页面布置更符合其浏览习惯,则停留时间更长,反之会很快离开.

通过当前所在页面和跳转页面找到用户浏览页面之间的路径关系,代表着用户对访问目标的分解模式,例如:用户 A 在修改个人资料时最有可能的行为路径为“首页-信息详情页-功能页面1-功能页面2-信息详情页”.

2.4　用户活跃周期

用户在相同时期内产生操作量越多表明其越活跃. 以7日作为周期分析各用户的活动水平,单个用户每日活动水平值最高为100,5名注册用户日活跃度趋势如图4所示. 用户B和用户D分别在周二、周三出现明显活跃高峰,两名用户在其高度活跃日的活跃值均超过50;但用户B在周六时活跃值转为0,而用户D则在周二与周六出现0操作量. 用户C和用户E的高度活跃日分别为周一和周日,两人均未出现0活跃值. 用户A的日活跃度在一周内变化相对平缓,未出现日操作量激增的情况. 另外,5名用户在周五和周六的活跃度均偏低.

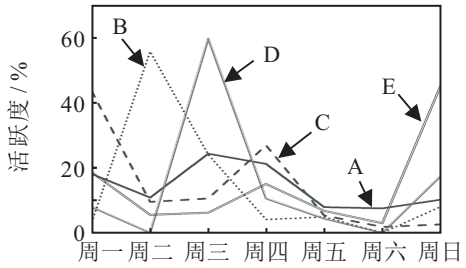

图 4　日活跃度变化趋势

下面以24小时为周期分析各用户活跃度. 考虑人的作息规律,将24小时归类为等间隔的8个时间段. 时段内活跃值为因变量,用户与时间段为自变量,使用SPSS进行方差分析,得到时间段和用户 * 时间段(交互效应)的显著性水平均小于0.01,即不同用户在不同时间段内的活跃度有差异. 图5为5名用户在同一时间段中活跃表现差异曲线,只有用户A在深夜时访问网站并产生页面事件,并且没有用户在凌晨和早晨有活跃现象;在其他6个时间段中用户的活跃水平均表现出差异性. 图6为用户活跃水平随着时间组的变化情况. 用户活跃高峰多数集中在下午,但用户之间的活跃波动曲线均不一致.

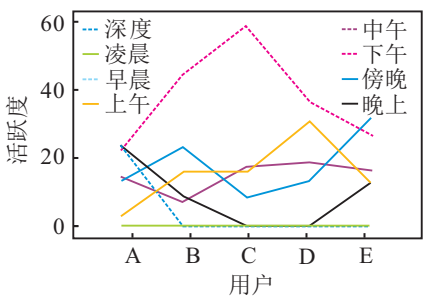

图 5　时间段中活跃水平的用户差异

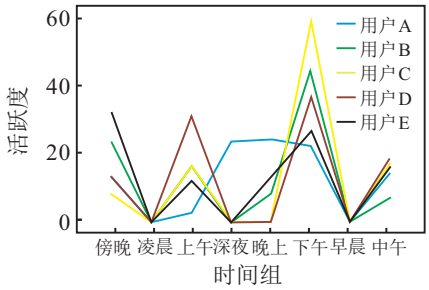

图 6　用户活跃水平的时间变化

通过时间维的用户活跃水平分析,发现用户的周内活跃度变化存在个体差异,并且用户的日间活动表现出明显昼夜节律,同时因为受个体作息规律和模式的影响也同样存在用户间差异.

3　可信检测建模与评估方法

机器学习中的分类预测模型可以帮助实现通过人-网页交互行为检测交互可信性的任务,过程框架如图7所示.

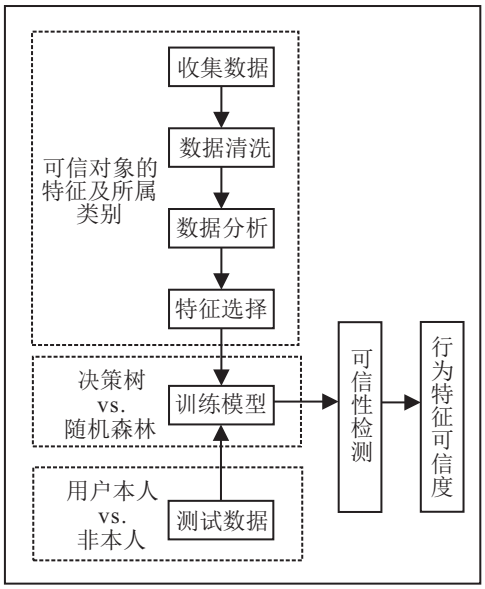

图 7　判断交互可信性的基本框架

3.1　机器学习中的树模型

相比于线性模型,树模型对特征分别进行处理,比较接近人类思维方式,模型具有可解释性,擅长于处理分类问题. 本文选择构建基于决策树和随机森林算法的树型模型完成可信检测. 决策树[14]和随机森林[15]等方法被广泛应用于各种科学领域解决数据处理与分析问题,它们都属于非线性有监督分类模型.

3.2　评估指标

可信交互检测是二分类问题,即账户由拥有者本人登录操作是可信的,若被其他人使用则是不可信的. 数据样本标签的实际取值只有正类(positive)和

负类(negative)之分,正类为属于账户拥有者的样本,负类为不属于该账户拥有者的数据样本. 首先引入交互可信性检测中的4个名词概念:

1) 真正类(true positive, TP),真正属于预测对象的交互行为也被预测为属于该对象;

2) 假正类(false positive, FP),原本不属于预测对象的交互行为被预测为是属于该对象;

3) 真负类(true negative, TN),真正不属于预测对象的交互行为也被预测为不属于该对象;

4) 假负类(false negative, FN),原本属于预测对象的交互行为被预测为不属于该对象.

对于检验交互可信性而言,测试模型将输入行为特征正确预测给所属用户的几率越高表明检测交互可信性的效果越佳. 另外,各个行为特征在模型生成过程中的贡献大小即为特征用于检测时的作用强度,检测力越强代表该交互行为特征在用户类别上可区分性越高,可信性越高.

本文选用精确率(precision, P)、错误接受率(false acceptance rate, FAR)和F_1-score(F_1)评估可信检测的效果.

3.2.1 精确率(P)

精确率是指在被模型匹配为可信交互行为的样本中真正可信的比例. 取值区间为[0, 1],越接近1表明对用户可信行为的识别精确度越高,有

$$P = \mathrm{TP}/(\mathrm{TP}+\mathrm{FP}). \tag{1}$$

3.2.2 错误接受率(FAR)

错误接受率是指将原本非可信的交互行为匹配成可信行为的样本数在真正非可信样本中所占比例. 取值区间为[0, 1],$\mathrm{FAR}=0$代表未出现将不可信行为错误判断为可信行为的情况,有

$$\mathrm{FAR} = \mathrm{FP}/(\mathrm{FP}+\mathrm{TN}). \tag{2}$$

3.2.3 F_1 score(F_1)

召回率(recall, R)是在用户可信行为的所有样本中被判断为确实是该用户可信行为的样本所占比例,与精确率的加权调和平均则为F_1. F_1是对R和P的综合考量,取值越接近1代表验证交互可信性的检测方法越好,有

$$R = \mathrm{TP}/(\mathrm{TP}+\mathrm{FN}), \tag{3}$$

$$F_1 = 2\mathrm{PR}/(P+R) = 2\mathrm{TP}/(\mathrm{TP}+\mathrm{FP}+\mathrm{FN}). \tag{4}$$

4 可信交互检测实例

为验证本文所提出方法的效果,通过采集现实数据进行实证分析. 从某旅游资讯类网站收集201名用户的网络行为数据,为避免出现涉及用户信息而导致的隐私问题,已对数据源进行脱敏处理. 按照用户ID所对应的样本容量大小,由高到低依次选取17名用户作为实例验证对象,在为期两周的时间内,17名用户总共产生32 669条行为记录数据,包含40个记录维度. 通过异常样本清洗、数据变换、组合迭代、分裂衍生等方法,最终得到各行为表现涉及到的14个与用户个体生理及心理相关的交互行为特征数据集.

现实数据随机性较强,实例数据集中样本类别分布不均衡. 本文选择SMOTE算法[16]实现数据平衡,消除类别非均衡数据集对机器学习效果可能带来的负面影响. 平衡后,样本集中共有129 421条数据记录,其中每名用户样本数为7 613条.

4.1 可信交互检测效果

使用Python调用scikit-learn决策树和随机森林类库构建可信检测模型,按8:2将数据集随机划分为训练集和测试集,对模型参数进行调整,得到最终实证结果. 采用混淆矩阵和指标P、FAR、F_1评估可信交互检测效果. 决策树与随机森林模型输出的混淆矩阵如图8和图9所示.

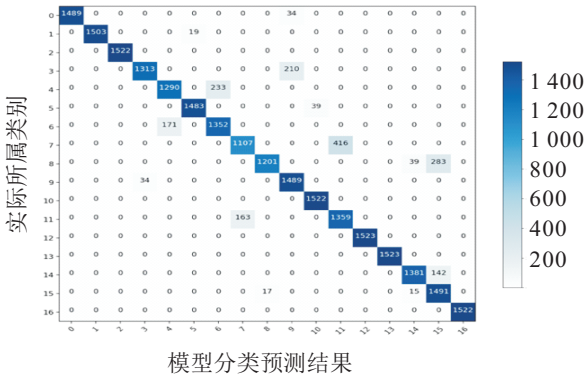

图8 决策树输出混淆矩阵

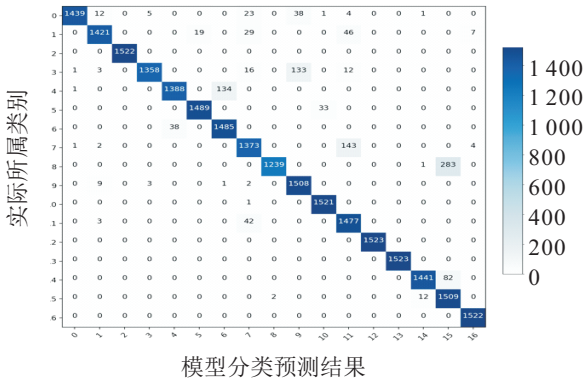

图9 随机森林模型输出混淆矩阵

在决策树算法中,用户2、10、12、13、16的所有行为样本都被正确判别给了本人. 用户7与用户11的交互行为易被混淆(用户7有416个行为被错误地

识别为用户 11 所有,用户 11 的 163 个行为被错认为用户 7 所有). 另外,用户 4 和 6、用户 3 和 9 的交互行为也存在被相互错认的情况. 用户 8、14、15 三者的交互行为具有相似性,易发生两两混认现象. 其可信检测效果的评估指标为: $P^{\mathrm{DTC}} = 92.99\,\%, F_1^{\mathrm{DTC}} = 92.99\,\%, \mathrm{FAR}^{\mathrm{DTC}} = 0.44\,\%$.

在随机森林算法中,用户 2、12、13、16 的交互行为都准确地被识别为实际类别. 此算法下两者间相互混淆的情况减弱,两两相互被错认的程度也没有双向对等. 虽然用户 8 有 283 条行为被错认为用户 15,但用户 15 只有 2 个行为被误判给用户 8,与之相似的情况还发生在用户 3 与 9、用户 4 与 6、用户 7 与 11 之间. 基于随机森林的可信检测效果评估 $P^{\mathrm{RF}} = 95.06\,\%, F_1^{\mathrm{RF}} = 95.06\,\%$,均比决策树算法提升 2.07 个百分点; $\mathrm{FAR}^{\mathrm{RF}} = 0.31\,\%$,在决策树算法的基础上降低了 0.13 %.

通过个体网络行为模式保障用户交互可信性的重点是控制非本人操作时被错误识别为账户所有者的几率,即尽可能降低接受非授权人员操作账户的几率,所以,错误接受率 (FAR) 是评价检测效果的重要指标. 决策树的 FAR 为 0.44 %,随机森林为 0.31 %. 举例说明,在他人盗用用户 A 的账户所产生的 10 000 条交互行为记录中,有 44 条会被决策树模型误认为是 A 本人产生的,随机森林则只会将其中 31 条误判为属于 A.

4.2　可信行为特征重要度

行为特征在用户类别 (本人与非本人) 上的区分能力越强,重要度越高,即该特征在用户类别上个体效应明显,具有可信性,对可信检测起正面推进作用. 图 10 为本文所选用可信行为特征的重要度排序, 14 个特征均具有一定的可信水平,共有 7 个特征的重要度超过 5,有 2 个特征的重要度在 1 ~ 5 之间,其余 5 个特征的可信水平不足 1. 其中,用户对交互工具的选择行为、页面停留行为、页面跳转行为以及日活跃度这 4 个可信行为特征的重要度在 10 以上,而页面停留时间,页面等待时间、页面浏览内容量、页面下滑次数和页面操作事件类型这 5 个可信行为特征在判断用户类别上较弱.

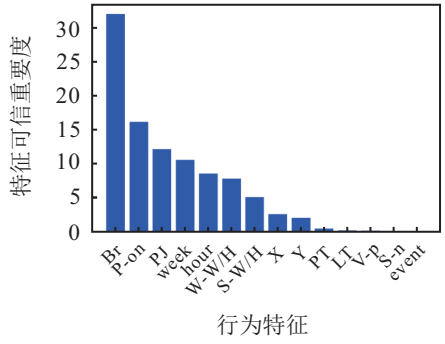

图 10　特征可信重要度

5　结　论

本文所提出的行为流图可复现地描述网页上的用户交互活动,其中涉及的一系列可信交互行为特征可以有效地检测网站交互可信性,所使用的随机森林算法能够很好地拒绝接受不可信行为,在区分用户类别时不易发生混淆. 虽然决策树算法错误接受不可信行为的概率也较低,但易出现用户互混的情况. 使用本文结果与其他涉及用户网络行为模式的相关研究进行比较,结果见表 1. 不同的是本文用于可信交互检测的交互行为特征与用户个体的心理和生理相关联,不局限于某一种操作,是人-网站交互过程中各种行为的集合,同时也取得了较优的检测结果.

表 1　与其他相关研究对比

文献	特征	算法	FAR / %	Precision / %
[10]	鼠标移动方向与类型	nearest neighbor + SVM	0.92	–
[17]	键盘敲击频率	neural network	4.1	–
[18]	在线交流行为	DTC	–	85
本文	网页交互行为	DTC RF	0.44 0.31	92.99 95.06

本文用于检测交互可信性的行为特征均具有一定的可信重要度,超半数特征的重要度较高,表明这些行为特征参数值在用户类别间具有较高的可区分性,对交互可信性的检测力较强.

目前,验证本文所提出方法时只使用了一个数据源,未能验证在多种数据源上的普适性,也未研究行为流图中涉及到的所有行为信息在不同数据源中是否有差别,未来将采用不同来源和维度的数据集验证方法的普适性.

参考文献 (References)

[1] Grosse E, Upadhyay M. Authentication at scale[J]. IEEE Security & Privacy, 2013, 11(1): 15-22.

[2] Hille P, Walsh G, Cleveland M. Consumer fear of online identity theft: Scale development and validation[J]. Journal of Interactive Marketing, 2015, 30(2): 1-19.

[3] Andrew M. Facebook tracks the location of logins for better security[DB/OL]. [2010-11-24]. http://www.

zdnet. com / blog / weblife/facebook-adds-better-security-tracks - the - location-of-your-slogins / 2010. accessedSep. 2013.

[4] Aljawarneh S, Debabneh M, Masadeh S, et al. Deploying a web client authentication system using smart card for E-systems[J]. Research Journal of Applied Sciences Engineering & Technology, 2011, 3(9): 948-952.

[5] Malathi R, Jeberson R. An integrated approach of physical biometric authentication system[J]. Procedia Computer Science, 2016, 85: 820-826.

[6] Howard S, David L S, Alex P. “CHAPTER 12 behavioral biometrics” in new solutions for cybersecurity[M]. Cambridge: MIT, 2018: 367-377.

[7] Olejnik L, Castelluccia C, Janc A. On the uniqueness of Web browsing history patterns[J]. Annals of Telecommunications — Annales Des Télécommunications, 2014, 69(1/2): 63-74

[8] Ruan X, Wu Z Y, Wang H, et al. Profiling online social behaviors for compromised account detection[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(1): 176-187.

[9] Ho J, Kang D K. One-class naïve Bayes with duration feature ranking for accurate user authentication using keystroke dynamics[J]. Applied Intelligence, 2018, 48(6): 1547-1564.

[10] Shen C, Cai Z, Liu X, et al. MouseIdentity: Modeling mouse-interaction behavior for a user verification system[J]. IEEE Transactions on Human-Machine Systems, 2016, 46(5): 734-748.

[11] Barbon S, Igawa R A, Bogaz Z B. Authorship verification applied to detection of compromised accounts on online social networks[J]. Multimedia Tools and Applications, 2017, 76(3): 3213-3233.

[12] Monrose F, Rubin A D. Keystroke dynamics as a biometric for authentication[J]. Future Generation Computer Systems, 2000, 16(4): 351-359.

[13] Hu Zhiyan. Behavior management[M]. Beijing: Economic Science Press, 2006: 28.

[14] 程幼明, 姚丽, 何惠妍, 等. 一种考虑DMU间交叉竞争的博弈效率DEA评价方法[J]. 控制与决策, 2018, 33(9): 1677-1685.
(Cheng Y M, Yao L, He H Y, et al. An evaluation method for DEA game efficiency considering cross-competition game of DMUs[J]. Control and Decision, 2018, 33(9): 1677-1685.)

[15] 吴成东, 卢紫微, 于晓升. 基于加权随机森林的图像超分辨率算法研究[J]. 控制与决策, 2019, 34(10): 2243-2248.
(Wu C D, Lu Z W, Yu X S. Image super resolution reconstruction algorithm based on weighted random forest[J]. Control and Decision, 2019, 34(10): 2243-2248.)

[16] Nitesh V C, Kevin W B, Lawrence O, et al. SMOTE: Synthetic minority over-sampling technique[J]. Journal of Artificial Intelligence Research, 2002, 16(1): 321-357.

[17] Alpar O. Frequency spectrograms for biometric keystroke authentication using neural network based classifier[J]. Knowledge-Based Systems, 2017, 116: 163-171.

[18] Adeyemi I R, Razak S A, Salleh M, et al. Observing consistency in online communication patterns for user re-identification[J]. PLoS, 2016, 11(12): e0166930.

作者简介

易树平(1960–), 男, 教授, 博士生导师, 从事工业工程理论与技术等研究, E-mail: yshuping@cqu.edu.cn;

李嘉佳(1992–), 女, 硕士生, 从事人机交互的研究, E-mail: lijiajia@cqu.edu.cn;

易茜(1986–), 女, 讲师, 博士, 从事绿色制造等研究, E-mail: yiqian@cqu.edu.cn.

(责任编辑：郑晓蕾)