鼠标行为 HHT 变换的工业互联网用户身份认证

张一弓[1,2]，易茜[1]，李剑[2]，李聪波[1]，尹爱军[1]，易树平[1]
（1. 重庆大学机械传动国家重点实验室，重庆 400044；
2. 重庆大学输配电装备及系统安全与新技术国家重点实验室，重庆 400044）

摘 要：工业互联网的快速发展引发了对网络安全的广泛关注，终端用户身份认证技术成为研究热点。根据工业互联网人机交互特点，设计了实验网站，收集了该网站 24 名用户两年半的非受控环境下鼠标行为数据作实例，采用希尔伯特黄变换（HHT, Hilbert-Huang transform）提取鼠标行为信号频域特征，结合时域特征，形成 163 维时频域联合特征矩阵，用于表征用户鼠标行为模式特征。使用 Bagged tree、支持向量机（SVM, support vector machine）、Boost tree 和 *K* 最邻近（*K*NN, *K*-nearest neighbor）算法构建网络用户身份认证模型，对比数据测试结果表明，Bagged tree 算法在本案例中内部检测效果最佳，平均错误接受率（FAR, false acceptance rate）为 0.12%、平均错误拒绝率（FRR, false rejection rate）为 0.28%；外部检测中，平均 FAR 为 1.47%。相较于传统鼠标动力学方法，使用 HHT 提取鼠标行为频域信息能更好地实现终端用户身份认证，为保障工业互联网安全提供有效的技术支撑。

关键词：工业互联网；身份认证；鼠标行为；希尔伯特黄变换；Bagged tree
中图分类号：TP273
文献标志码：A
doi: 10.11959/j.issn.2096−3750.2022.00268

User authentication of industrial internet based on HHT transform of mouse behavior

ZHANG Yigong[1,2], YI Qian[1], LI Jian[2], LI Congbo[1], YIN Aijun[1], YI Shuping[1]
1. State Key Laboratory of Mechanical Transmission, Chongqing University, Chongqing 400044, China
2. State Key Laboratory of Power Transmission Equipment and System Security and New Technology, Chongqing University, Chongqing 400044, China

Abstract: The rapid development of the industrial internet had caused widespread concern about the network security, and the end-user authentication technology was considered a research hotspot. According to the characteristics of human-computer interaction in industrial internet, an experimental website was designed. 24 users' mouse behavior data in an uncontrolled environment were collected within 2.5 years to conduct case studies. Hilbert-Huang transform (HHT) was used to extract frequency domain features of mouse behavior signals, combined with time domain features to form a time-frequency joint domain feature matrix of 163-dimensional to characterize user mouse behavior patterns. Bagged tree, support vector machine (SVM), Boost tree and *K*-nearest neighbor (*K*NN) were used to build a user authentication model, and the comparison result showed that the Bagged tree had the best internal detection effect in this case, with an average false acceptance rate (FAR) of 0.12% and an average false rejection rate (FRR) of 0.28%. In external detection, the FAR was 1.47%. Compared with the traditional mouse dynamics method, the frequency domain information of mouse behavior extracted by HHT can better realize the user authentication, and provide technical support the security of the industrial internet.

Key words: industrial internet, identity authentication, mouse behavior, Hilbert-Huang transform, Bagged tree

收稿日期：2022−01−05 ；**修回日期：**2022−04−24
通信作者：易茜，yiqian@cqu.edu.cn
基金项目：国家自然科学基金资助项目（No.71671020）；中央高校基本科研业务费资助项目（No.2021CDJKYJH 022）
Foundation Items: The National Natural Science Foundation of China (No.71671020), The Fundamental Research Funds for the Central Universities (No.2021CDJKYJH 022)

0 引言

工业互联网作为新一代信息技术与制造业深度融合的产物，日益成为新工业革命的关键支撑和深化“互联网+先进制造业”的重要基石，对未来工业发展产生全方位、深层次、革命性影响[1]。加快建设和发展工业互联网，对发展先进制造业、支持传统产业优化升级具有重要意义。然而，我国工业互联网仍处于发展初期，技术和安全等方面存在瓶颈和短板[2]。《工业互联网安全总体要求》中指出，用户身份鉴别、访问控制等是工业互联网安全防护的重要内容[3]。

截至 2018 年 12 月，我国国家信息安全漏洞库新增漏洞 18 780 个，其中工业终端缺乏身份认证、访问控制等安全机制是一类重要问题[4]。在云企业资源计划（ERP, enterprise resource planning）中，云的按需服务和多租户特性使得身份认证过程易受到攻击，引发后续访问过程的不安全问题[5]。因此，探索一种新型有效的用户身份认证技术是保障工业互联网安全的有效途径。

计算机是访问工业互联网最常用的终端之一。用户一般通过静态身份认证登录账户，然后发生交互行为，但常用的密码认证、令牌认证、生物认证等静态身份认证方法仍存在被破解的风险[6-7]，因而人们提出基于生物特征的认证方法作为身份认证的重要补充。生物行为特征认证，采用不易被他人模仿的个人行为特征作为用户独特的身份辨识，能够在交互过程中持续进行身份辨识，保护账户安全。鼠标在人机交互过程中使用频繁，其行为数据记录简单、数据量大，是一种典型的具有时间序列性质的生物行为数据。基于鼠标动力学的生物特征身份认证方法开始受到学者的关注。

Pusara 等[8]对使用鼠标行为数据的身份认证进行了研究。Ahmed 等[9]发展并提出了鼠标动力学方法，设计实验收集鼠标操作中时间戳、坐标等数据，将低级的鼠标行为组合成为高级动作。鼠标移动速度、加速度等 19 维运动特征被用于训练基于神经网络的用户身份识别模型，获得了 2.464 9%的错误接受率（FAR, false accept rate）和 2.461 4%的错误拒绝率（FRR, false reject rate）。Feher[10]提出划分鼠标行为层次结构并探究新的行为特征，得到了 10%的等错误率（EER, equal error rate）。Zheng 等[11]计算了曲率距离等基于角度的指标，并用支持向量机（SVM, support vector machine）建模识别，所得 EER 为 1.3%。沈超等[12]从人机交互和生理层面上对用户鼠标行为进行研究，将鼠标行为分为对话层和生理层，使用基于顺序前进贪婪搜索和 SVM 构建身份认证模型，在 20 名用户鼠标数据实验中得到 FAR 为 1.67%、FRR 为 3.68%。徐剑等[13]采用层次化方法对用户鼠标行为进行定义，采用随机森林分类器构建身份认证模型，得到 FAR 为 3.96%、FRR 为 11.63%。Yi 等[14]基于鼠标动力学方法，设计实验探究了不同情绪下的鼠标行为，发现虽然用户鼠标行为特征在不同情绪下会有所不同，但在身份认证结果上没有显著差异。Chong 等[15]在研究中首次尝试使用卷积神经网络（CNN, convolutional neural network）、长短期记忆（LSTM, long short-term memory）网络以及 CNN-LSTM 混合模型等深度学习框架简化鼠标行为特征提取过程，进行身份认证。这些研究均表明，用户鼠标行为模式在时域表现出独特性，可用于身份认证。

在前期利用鼠标行为时域特征进行身份认证基础上，人们开始关注其他生物行为的频域特征。Noy 等[16]通过一项手臂追踪实验发现，人们进行手臂运动时的平均抖动频率存在个体间差异。这种个体间差异能够表现出个人独有的特点，并且已经被用于身份认证。O.Alpar[17]在击键动力学研究中使用加窗傅里叶变换探究不同用户输入相同密码时敲击键盘的频率信息和频谱分布差异，训练高斯−牛顿神经网络进行身份认证，得到 4.1%的 EER。在进一步的研究中，O.Alpar[18]使用了一种改进的短时傅里叶变换来探索频域信息，并训练 SVM 分类器进行身份认证，得到 1.40%～2.12%的 EER。相关研究表明，频域信息也能表征用户行为模式的独特性，可用于用户身份认证。

目前，仅见笔者团队前期研究[19]分析了鼠标行为的频域特征，其所设计的单因素对比实验结果证明了相比于仅使用时域分析，对鼠标行为进行时频联合分析提取特征并建模，能够获得更好的身份识别效果。在该研究以及笔者团队对基于网络用户行为的身份认证研究的基础[6,14,19]上，本文从生理运动角度更加深入地分析了鼠标行为的运动学特点，针对文献[19]中所使用的小波包变换特征提取方法对小波基选择的主观性、对瞬时频率等特征捕捉不精确的两处短板，提出运用希尔伯特黄变换

（HHT, Hilbert-Huang transform）更准确地探究鼠标行为频域的瞬时特征、描述频域信息随时间的变化过程，更好地表征用户鼠标行为模式，提高身份认证精度。

Bagged tree 算法因其对多棵决策树的集成而能有效地降低机器学习模型的方差[20]，已经被用于输电线路故障识别[21]、非入侵负载监控[22]等场景，获得了优秀的效果。本文尝试将其应用于身份认证的问题中。

综上，本文提出一种基于鼠标行为信号时频域联合分析的用户动态身份认证方法，利用 HHT 对工业互联网用户鼠标行为信号进行时频变换，形成时频域联合特征矩阵，以表征用户鼠标行为模式的特征。使用 Bagged tree 机器学习算法构建数据模型，用于表征每个用户独特的行为模式，实现用户身份认证检测。该方法可对鼠标行为信号进行实时监控，判断交互行为是否可信并终止异常的交互操作，为工业互联网网络安全管理提供一种动态身份认证的重要补充方法。

1　工业互联网鼠标行为数据特点与采集

1.1　工业互联网人机交互终端鼠标行为数据特点

工业互联网的本质是在传统云平台基础上叠加大数据、人工智能等新兴技术，构建数据采集体系，建设包括存储、集成、访问、分析、管理等功能的使能平台，实现工业技术、经验知识的模型化、软件化和复用化[23]。

在使用工业互联网时，任务引导人机交互过程，进而影响鼠标行为。用户登录后，会进行数据查找、资料下载、本地上传、在线通信等交互操作。在这些操作中，用户控制鼠标移动并单击交互界面上的功能按键，完成一次有效的交互过程。此外，用户还会浏览界面信息、使用键盘键入信息，这些操作将鼠标行为分割成很多间隔的运动段。一般，一次有目的地移动鼠标的操作在数秒之内完成。因此，从工程信号角度来看，工业互联网鼠标行为因任务变化而产生随机性和断续性，这使得鼠标行为信号表现出非线性、非稳态的特点。

此外，在一次有效的鼠标操作中，用户首先寻找屏幕上的目标按键，然后控制鼠标移动到目标位置，单击交互按键，产生交互结果。其中的移动过程是由手腕控制完成的精准到达运动。在人体运动控制领域，人们普遍认为平滑性是受控肢体运动的典型特征[24-25]。Morasso 等[24]用钟形分布的单峰速度曲线表现出手臂自由到达运动的平滑性，然而需要精准控制到达位置的手部运动的速度曲线会表现出基于钟形的叠加的多峰分布状态[26-27]。由于大脑算力的限制，人类无法实现绝对实时的信息处理，因此在运动中采取前馈、串行的信息处理过程，即根据该时刻运动状态对下一时刻进行预判，做出有效运动。这些研究表明，为了完成一次准确的鼠标点击操作，人们会将点击前的移动到达过程分解为一个主任务和若干子任务的连接。基于钟形的多峰分布的鼠标行为速度曲线如图 1 所示，呈现出基于钟形的多峰分布的特点，体现了对到达运动的分解过程。其中，横轴时间单位为采样频率 f 的倒数，纵轴速度单位为像素点/时间。

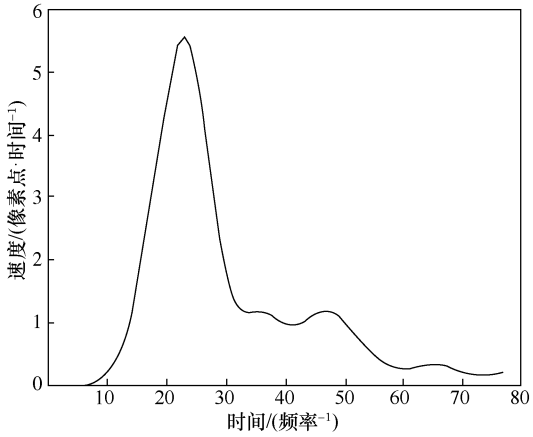

图 1　基于钟形的多峰分布的鼠标行为速度曲线

虽然人体运动采取相同的策略，但运动过程并非完全一致。运动过程频域特征已经被用于步态识别的研究中[28]。本文提出使用鼠标行为频域特征随时间的变化来描述用户鼠标行为模式特点。

综上，基于鼠标行为数据信号的非线性、非稳态特性，以及探究鼠标行为频域信息随时间的变化的需要，选用 HHT 对鼠标行为时域信号进行时频变换，探索用户鼠标行为模式特征，表征用户鼠标行为模式独特性。

1.2　鼠标行为数据采集

根据工业互联网人机交互过程鼠标行为特点，设计构建实验网站，模拟工业互联网交互环境。使用 html 和 JavaScript 开发前端网页，编写鼠标行为数据采集程序，通过嵌入式代码技术来记录。

在实验网站中，注册用户可以进行信息浏览、数据查找、资料下载、在线联络等任务，这些任务

都需要通过鼠标的移动、单击来完成。因此，该网站上的交互环境可以被视为非受控环境，且能够良好模拟工业互联网的鼠标交互行为。

浏览实验网站时的鼠标行为数据会被记录为 csv 文件并存储在阿里云服务器中，作为本研究的原始数据。原始数据包含 5 个维度：鼠标行为类型、时间戳（ms）、X 轴坐标（pix）、Y 轴坐标（pix）、用户名（已经脱敏），采样频率为 60 Hz。其中，鼠标行为类型包括：移动（slide）、左键按下（left down）、右键按下（right down）、左键抬起（left up）、右键抬起（right up）。这些基本的鼠标行为与时间戳和位置相结合构成了连续的鼠标操作行为序列。

2 基于 HHT 的时频域联合特征提取方法

2.1 希尔伯特黄变换

NE Huang[29]在 1998 年基于 Hilbert 变换提出的 HHT 方法是一种分析非平稳、非线性信号的分析方法。HHT 摆脱了线性时频分析方法中海森堡测不准原理的限制，通过经验模式分解（EMD, empirical mode decomposition），将输入信号自适应地分解为多个固有模态函数（IMF, intrinsic modal function），这些 IMF 经过 Hilbert 变换后能得到能表征用户鼠标行为模式特征的频域信息。

EMD 分解思想认为，原始信号由一系列本征 IMF 组成，每个 IMF 分量含有信号的内在振动模式。其中，IMF 需要满足两个基本条件：对于一信号，其极值点和过零点的数目必须相等或至多相差一个点；在任意点，由局部极大值和局部极小值构成的上、下两条包络线的平均值为 0。EMD 算法将一个复杂非稳态信号分解为若干本征模态函数之和，实际上就是对非平稳信号进行平稳化处理。并在分解过程中保留原始信号的特性。这种分解是自适应的，因而能够更好地反映信号中震颤处的本质信息。

Hilbert 变换定义瞬时频率为：设 $x(t)$ 为一实信号，$\hat{x}$ 是 $x(t)$ 的 Hilbert 变换，Hilbert 变换构成 $x(t)$ 的解析信号 $z(t)$

$$z(t)=x(t)+\mathrm{j}\hat{x}(t)=a(t)\mathrm{e}^{\mathrm{j}\theta(t)} \tag{1}$$

其中，

$$a(t)=\sqrt{u^2(t)+v^2(t)}=\left|x(t)\right| \tag{2}$$

$$\theta(t)=\arctan\left[\frac{v(t)}{\mathrm{u}(t)}\right] \tag{3}$$

定义瞬时频率 f_i 为

$$f_i=\frac{1}{2\pi}\cdot\frac{\mathrm{d}\theta}{\mathrm{d}t} \tag{4}$$

即实信号 $x(t)$ 的瞬时频率被定义为相应解析信号 $z(t)$ 的相位的导数。

定义固有模态函数 $c_i(t)$ 相应的瞬时能量分布为

$$E_i(t)=\frac{1}{2}a_i^2(t) \tag{5}$$

$$E(t)=\sum E_i(t) \tag{6}$$

其中，$E(t)$ 表示信号在任意 t 时刻的瞬时能量值，其数值是 Hilbert 变换下幅值的模方。它描述了信号在不同时刻下的能量转移和波动历程。

2.2 时域特征提取

使用 Python 清洗原始数据，删除重复值、空值，并按照时间顺序排序。根据鼠标位置与时间的关系计算每位用户 X 轴速度、Y 轴速度、切向速度等 14 项鼠标运动行为时域特征，见表 1。

表 1 鼠标运动行为时域特征

时域特征	计算方法
X 轴坐标	X
Y 轴坐标	Y
X 轴速度	$v_x=\delta x/\delta t$
Y 轴速度	$v_y=\delta y/\delta t$
切向速度	$v=\sqrt{v_x^2+v_y^2}$
切向加速度	$a=\delta v/\delta t$
速度二阶导数	$j=\delta a/\delta t$
速度三阶导数	$s=\delta j/\delta t$
速度四阶导数	$d=\delta s/\delta t$
角度	$\theta=\arctan(\delta y/\delta x)$
角度变化率	$v_\theta=\delta\theta/\delta t$
曲率	$c=\delta\theta/\delta s$
曲率变化率	$v_{\mathrm{cur}}=\delta c/\delta t$
曲率距离[11]	cd

2.3 频域特征提取

选取时域特征中与时间相关的 9 项特征作为输

入信号，在 MATLAB 中调用“emd()”模块对输入信号执行 EMD。用户 A 鼠标加速度信号 EMD 分解过程如图 2 所示。第一行是加速度信号，向下依次为 EMD 后的 IMF1 到 IMF5，残差项略去。

在这些 IMF 中，不是每一项都包含用户使用鼠标时个人所独有的行为特点，需要筛选选出合适的、能体现信号本质特征的 IMF。Ayenu-Prah[30]在研究中针对机械振动信号，计算每个 IMF 与原始信号的相关系数得到判定阈值来筛选 IMF。然而，上述方法在本研究中表现不佳，常常保留 IMF1 这样的高频噪声分量，舍去与人体生理运动相关的低频信息。

为了专注于探究鼠标数据中反映用户行为的信息和因人而异的特点，本文基于人体生理运动的频率分布来筛选 IMF。人类受控运动的频率上限不超过 12.46 Hz[31]，文中主要关注 13 Hz 以内的频域信息。不同于小波变换等方法的正交分解过程，EMD 是自适应分解过程，所以各 IMF 带宽不确定，通过 Hilbert 变换求出每个 IMF 的瞬时频率，根据人类运动频率上限筛选 IMF。

最后将保留的各 IMF 的瞬时频率、瞬时能量相加，得到输入信号的频域特征。

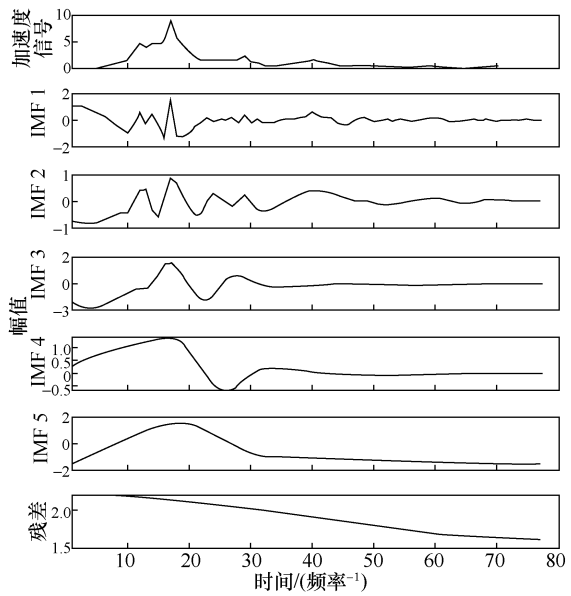

图 2　用户 A 鼠标加速度信号 EMD 分解过程

2.4　运动段划分

用户操作鼠标的特征特点往往表现在一段连续的操作当中，即蕴藏在一段信号序列中。Ahemd[9]提取鼠标移动、鼠标单击拖拽、两次单击间的移动、鼠标静默 4 种运动的数据构建直方图作为特征；Feher 等[10]将鼠标操作行为划分为 3 个层级分别计算运动特征。徐剑等[13]采用层次划分法对用户鼠标行为进行定义并提取特征值。本文根据鼠标运动过程划分运动段，鼠标事件名称与记号见表 2。

表 2　鼠标事件名称与记号

鼠标事件	原始数据中的名称	记号
鼠标移动	slide	m_{t_i}
按键按下	left down/right down	d_{t_i}
按键弹起	left up/right up	u_{t_i}

定义的运动段如下。

1) 无点击的运动段 $M0$：鼠标移动序列内两个按时间顺序发生的鼠标移动事件之间的时间间隔小于 τ，且整个运动段的持续时间超过 δ，选为一个运动段。

$$M0_{t_1}^{t_n}=\left\langle m_{t_1},m_{t_2},\cdots,m_{t_n}\left|t_n-t_1\geqslant\delta\right.\right| \\ \forall k:1\leqslant k\leqslant n-1,t_{k+1}-t_k\leqslant\tau\rangle$$

2) 以按键弹起开始并以按键按下结束的运动段 $M1$：

$$M1_{t_1}^{t_n}=\left\langle u_{t_1},[m_{t_2},\cdots,m_{t_{n-1}}],d_{t_n}\left|t_{n-1}-t_2\geqslant\delta\right.\right| \\ \forall k:2\leqslant k\leqslant n-2,t_{k+1}-t_k\leqslant\tau\rangle$$

3) 以鼠标静默开始并以按键按下结束的运动段 $M2$：

$$M2_{t_1}^{t_n}=\left\langle[m_{t_1},m_{t_2},\cdots,m_{t_{n-1}}],d_{t_n}\left|t_{n-1}-t_2\geqslant\delta\right.\right| \\ \forall k:2\leqslant k\leqslant n-2,t_{k+1}-t_k\leqslant\tau\rangle$$

4) 以按键弹起开始并以鼠标静默结束的运动段 $M3$：

$$M3_{t_1}^{t_n}=\left\langle u_{t_1},[m_{t_2},\cdots,m_{t_{n-1}},m_{t_n}]\left|t_{n-1}-t_2\geqslant\delta\right.\right| \\ \forall k:2\leqslant k\leqslant n-2,t_{k+1}-t_k\leqslant\tau\rangle$$

对于每一个划分出来的运动段，计算表 2 中 14 维时域特征和 18 维频域瞬时特征的最大值、最小值、平均值、标准差、极差，形成 160 项时频域特征。然后，计算每个运动段的运动段距离 s_n、运动段持续时间 t_n、路径抖动率 J 共 3 个特征，如式(7)～

式(9)所示。鼠标运动行为时频域特征见表 3。

$$s_n = \sum_{i=1}^{i=n} s_i \tag{7}$$

$$t_n = \sum_{i=1}^{i=n} t_i \tag{8}$$

$$J = \frac{\sqrt{(x_1 - x_n)^2 + (y_1 - y_n)^2}}{s_n} \tag{9}$$

表 3　鼠标运动行为时频域特征

类型	特征名称					特征数
与时间无关	v_x v_x v a v'' v''' v'''' v_θ v_{cur}	×	特征本身 瞬时频率 瞬时能量	×	最小值 最大值 平均值 标准差 极差	135
与时间无关	X Y θ c cd	×	最小值 最大值 平均值 标准差 极差			25
其他	s_n t_n J					3

3　身份认证模型构建

时频联合域特征描述了不同用户独特的鼠标行为模式，表征了不同用户鼠标行为模式特征。使用机器学习分类算法，构建数据模型，表征用户行为模式，实现身份认证。本文基于 Baggedtree 算法构建身份认证模型，检测用户身份。

3.1　基于 Bagged tree 的身份认证模型构建

Breiman 的“装袋”算法是最早的基于集成的算法之一[20]。这是一种通过在原始数据集中有放回地抽样重新选取出 S 个新的数据集来训练分类器的集成技术。Bagged tree 算法原理如图 4 所示。

单一决策树的算法存在方差高的问题。如果训练模式发生变化，则生成的新的决策树可能与原始决策树完全不同，预测精度也会发生较大的变化。也就是说单个决策树可能导致过拟合的情况。为了克服决策树算法的这一问题，Bagged tree 算法通过对所有决策树的表决结果进行综合来得到预测结果，降低了方差，减少了过拟合问题并增强了每一棵决策树的适用性。

3.2　身份认证的评价指标

身份认证是一个二分类问题。样本标签只有正类和负类之分，正类是账户真实所有者，负类不是账户真实所有者[6]。因而所有的判定结果可分为以下 4 类：

真正类（TP, true positive），正样本被判为正样本；

假正类（FP, false positive），负样本被判为正样本；

真负类（TN, true negative），负样本被判为负

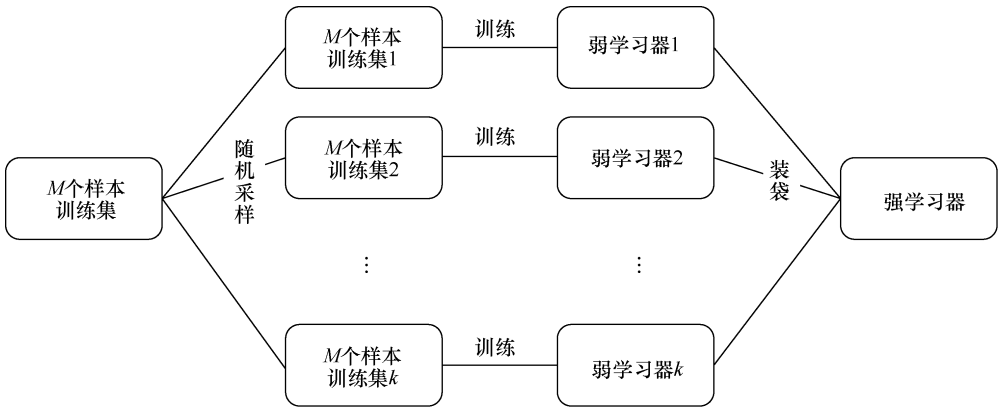

图 4　Bagged tree 算法原理

样本；

假负类（FN, false negative），正样本被判为负样本。

理想情况下，FAR 和 FRR 应均为 0，但这并不现实，因为 FAR 与 FRR 相互矛盾、此消彼长，有时会用 EER（FAR 等于 FRR 时的值）来评价安全检测系统的整体效果。对于本文所研究的身份认证系统而言，尽可能多地检测出非法用户，同时较好地避免误将合法的真实用户认为非法入侵用户的情况是最需要关注的。因此，本文选用 FAR、FRR 作为评价指标。

1) FAR

FAR 是指在所有负类样本中，被误判为正类的负类样本所占的比例。FAR 越接近 0，则表明模型对非法入侵用户的检测能力越强。

$$\mathrm{FAR}=\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}} \tag{10}$$

2) FRR

FRR 是指在所有正类样本中，被误判为负类的正类样本所占的比例。FRR 越接近 0，则表明模型将真实用户判定为非法入侵者的可能性越低。

$$\mathrm{FRR}=\frac{\mathrm{FN}}{\mathrm{TP}+\mathrm{FN}} \tag{11}$$

4　身份认证模型检测实例

4.1　基于鼠标行为数据的身份认证

本研究关注用户日常的、非受控的鼠标操作行为。公开数据集，如 TWOS[32]，由“短期、受控”环境来模拟用户使用网络的场景采集数据，与本研究所设定的“长期、非受控”的真实场景存在较大不同。为此，笔者团队自建了 AML 网站，从中采集 24 名用户（19 名男性和 5 名女性，年龄为 22～45 岁）在非受控环境下两年半的鼠标行为数据用于研究。数据收集过程得到了受试者的准许。

笔者团队提出了两种检测情景，一种是内部检测，例如公司系统内部对员工冒用他人账户登录系统进行操作的检测；另一种是外部检测，例如非公司人员非法入侵公司内部系统进行操作的检测。需要指出，在内部检测情景中，所有用户行为数据都被采集并建模，但在外部检测中，入侵用户的行为对身份认证模型来说是未知的。

4.1.1　内部检测

为了验证所提方法在内部检测情景中的性能，从 24 名用户数据中随机选出 18 名用户的数据作为本节研究数据集，该数据集记录了他们 2017 年 7 月−2019 年 10 月历次合法登录的非受控环境下的鼠标行为数据。为保护用户隐私，进行了用户信息脱敏处理。对每一位用户的鼠标数据进行数据清洗、按时间排序，然后计算时域瞬时特征，并选择与时间相关的时域特征进行 HHT 得到频域瞬时特征，最后划分为运动段并计算运动段内所有特征的最小值、最大值、平均值、标准差、极差。

经过上述处理，对每一位用户形成具有 163 维特征的鼠标运动行为特征矩阵。A 用户的时频域联合特征矩阵如式(12)所示。A 用户的鼠标运动行为 $N\times164$ 矩阵的第一列表示脱敏处理后的用户名；其余列表示使用本文所提方法计算的 163 维特征；每一行是一个样本，表示该用户的一个运动段中所计算的 163 维特征。

$$\begin{pmatrix} A & -12 & 28 & \cdots & 0.4 \\ A & -73 & 122 & \cdots & 0.1 \\ A & -37 & 579 & \cdots & 0.4 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A & -83 & 115 & \cdots & 0.9 \end{pmatrix} \tag{12}$$

依次将 18 名用户中的每一名作为真实用户，其他 17 名作为冒用者，形成 18 份数据集。由于数据集中正负用户的样本量差异较大，为了排除样本不平衡的因素对身份认证效果的影响，在训练模型前使用 Borderline SMOTE 算法[33]，平衡样本集。

使用 Bagged tree 算法构建身份认证模型。采用 5 折交叉验证，将样本划分训练集和测试集，决策树数量为 200。使用 FAR、FRR 两项评价指标来评估身份认证效果，18 名用户的身份认证结果见表 4，FAR 平均值为 0.12%、FRR 平均值为 0.28%。

4.1.2　外部检测

在这 18 名用户之外，本节将其余的 6 名用户视为外部入侵者，进行外部检测，来验证该身份认证模型的泛化能力。

表 4 18 名用户的身份认证结果

真实用户	FAR	FRR
A	0.05%	0.65%
B	0.18%	0.13%
C	0.09%	0.06%
D	0%	0%
E	0.15%	0.26%
F	0.25%	0.19%
G	0%	0.34%
H	0.06%	0.15%
I	0.09%	0.39%
J	0.24%	0.33%
K	0.36%	0.71%
L	0.08%	0.24%
M	0.06%	0.56%
N	0.03%	0.09%
O	0.06%	0.36%
P	0%	0.03%
Q	0.19%	0.22%
R	0.22%	0.26%
平均	0.12%	0.28%

对这 6 名用户采用相同的数据处理方法计算特征，但不用他们的数据训练模型。依次在上述 18 个模型中检测，由于检测样本只有负类，所以只使用 FAR 作为评价指标，外部检测结果见表 5。外部入侵者检测 FAR 最高值为 2.57%，最低值为 0.72%，平均值为 1.47%。这表明，只有 1.47%的入侵行为没有被检测出来。

表 5 外部检测结果

外部入侵者	样本数量	FAR
入侵者 1	470	0.72%
入侵者 2	49	1.53%
入侵者 3	124	1.41%
入侵者 4	97	2.57%
入侵者 5	162	1.77%
入侵者 6	101	0.80%
平均	167.17	1.47%

4.2 与其他分类算法的对比

不同算法的身份认证结果见表 6，结果表明本文所用 Bagged tree 算法能达到更好的身份认证效果。

表 6 不同算法的身份认证结果

分类器	FAR	FRR
Bagged tree（本文）	0.12%	0.28%
Boost trees	0.29%	0.64%
高斯核 SVM	0.38%	0.89%
*K*NN	0.66%	1.83%

4.3 与以前研究的对比

本文方法与其他鼠标行为身份认证方法效果对比见表 7，被用来对比的研究都是该研究领域被认可的成果。对比结果表明，使用 HHT 提

表 7 本文方法与其他鼠标行为身份认证方法效果对比

研究	方法	实验设计	结果
Ahmed 等[9]	MD-NN	22 名被试者，短期非受控环境	FAR=2.464 9%
			FRR=2.461 4%
Gamboa 等[34]	Weibull 分布	50 名被试者，15 min 短期受控游戏环境	EER=0.5%
Shen 等[35]	SVM（单核）	28 名被试者，30 min 短期非受控环境	FAR=0.37%
			FRR=1.12%
Feher 等[10]	MD	25 名被试者，短期受控环境	EER=10%
Zheng 等[36]	MD-SVM	14 名被试者，短期受控环境	FAR=2.96%
			FRR=0.86%
本文（内部检测）	HHT-BT	4 名被试者，超过两年的长期非受控环境	FAR=0.12%
			FRR=0.28%
本文（外部检测）			FAR=1.47%

取鼠标行为频域特征，构成时频域特征矩阵，采用 Bagged tree 算法训练身份认证模型，能够得到更好的效果。

5　结束语

本研究面向工业互联网安全问题，基于网络用户行为模式具有独特性的假设，使用鼠标行为进行用户身份认证。本文提出发掘鼠标行为信号频域信息，使用 HHT 计算瞬时频率和瞬时能量，构建时频域特征矩阵，以更好地表征用户鼠标行为模式特点，最后使用 Bagged tree 算法建立用户鼠标行为身份认证模型。在对实验网站 24 名用户近两年半的非受控环境下鼠标行为数据的内部检测实例研究中，18 名用户内部检测 FAR 为 0.12%、FRR 为 0.28%优于现有研究；6 名用户的外部检测中，FAR 为 1.47%。

在未来的研究中，将进一步探究网络行为可信度的评价方法，探索设计可信交互[37]机制，提出基于过程的认证方法，对用户进行持续身份认证，更好地保障工业互联网安全。

参考文献：

[1] 中国国务院. 国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见[EB]. 2017.
The Chinese State Council. Guiding opinions on deepening the "Internet plus advanced manufacturing industry" to develop industrial Internet[EB]. 2017.

[2] 人民政协报.深入实施工业互联网创新发展战略为建设制造强国和现代化经济体系提供有力支撑: 全国政协“加快推进工业互联网建设”双周协商座谈会发言摘登(上)[N]. 人民政协报, 2020-05-07(4).
People's Political Consultative Conference. In-depth implementation of the Industrial Internet innovation development strategy provides strong support for the construction of a strong manufacturing country and a modern economic system-The CPPCC National Committee "accelerate the promotion of industrial Internet construction" bi-weekly consultation forum to replace the excerpt[N].CPPCC Daily, 2020.

[3] 工业互联网产业联盟. 工业互联网安全总体要求[EB]. 2018.
Alliance of Industrial Internet. General requirements for industrial Internet security[EB]. 2018.

[4] 互联网产业联盟. 中国工业互联网安全态势报告(2018)[EB]. 2019.
Alliance of Industry Internet. China industrial internet security situation report（2018）[EB]. 2019.

[5] KUMAR R, GOYAL R. On cloud security requirements, threats, vulnerabilities and countermeasures: a survey[J]. Computer Science Review, 2019(33): 1-48.

[6] 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.
YI S P, LI J J, YI Q. Trustworthy interaction detection method based onuser behavior flow diagram[J]. Control and Decision, 2020, 35(11): 2715-2722.

[7] MALATHI R, JEBERSON RETNARAJ R. An integrated approach of physical biometric authentication system[J]. Procedia Computer Science, 2016(85): 820-826.

[8] PUSARA M, BRODLEY C E. User re-authentication via mouse movements[C]//Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security-VizSEC/DMSEC '04. NewYork: ACM Press, 2004: 1-8.

[9] AHMED A A E, TRAORE I. A new biometric technology based on mouse dynamics[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(3): 165-179.

[10] FEHER C, ELOVICI Y, MOSKOVITCH R, et al. User identity verification via mouse dynamics[J]. Information Sciences, 2012, 201: 19-36.

[11] ZHENG N, PALOSKI A, WANG H N. An efficient user verification system using angle-based mouse movement biometrics[J]. ACM Transactions on Information and System Security, 2016, 18(3): 1-27.

[12] 沈超,蔡忠闽, 管晓宏, 等. 基于鼠标行为特征的用户身份认证与监控[J]. 通信学报, 2010, 31(7): 68-75.
SHEN C, CAI Z M, GUAN X H, et al. User authentication and monitoring based on mouse behavioral features[J]. Journal on Communications, 2010, 31(7): 68-75.

[13] 徐剑, 李明洁, 周福才, 等. 基于用户鼠标行为的身份认证方法[J]. 计算机科学, 2016, 43(2): 148-154.
XU J, LI M J, ZHOU F C, et al. Identity authentication method based on user's mouse behavior[J]. Computer Science, 2016, 43(2): 148-154.

[14] YI Q, XIONG S Q, WANG B, et al. Identification of trusted interactive behavior based on mouse behavior considering Web user's emotions[J]. International Journal of Industrial Ergonomics, 2020(76): 102903.

[15] CHONG P, ELOVICI Y, BINDER A. User authentication based on mouse dynamics using deep neural networks: a comprehensive study[J]. IEEE Transactions on Information Forensics and Security, 2020(15): 1086-1101.

[16] NOY L, ALON U, FRIEDMAN J. Corrective jitter motion shows similar individual frequencies for the arm and the finger[J]. Experimental Brain Research, 2015, 233(4): 1307-1320.

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

[18] ALPAR O. TAPSTROKE: a novel intelligent authentication system using tap frequencies[J]. Expert Systems With Applications, 2019(136): 426-438.

[19] 易茜, 黎伟, 易树平,等. 基于鼠标行为时频联合分析的用户可信认证[J]. 北京邮电大学学报, 2021, 44(4): 121-128.
YI Q, LI W, YI S P, et al. Trustworthy identity authentication based on joint time-frequency analysis of mouse behavior[J]. Journal of Beijing University of Posts and Telecommunications, 2021, 44(4): 121-128.

[20] BREIMAN L. Bagging predictors[J]. Machine Learning, 1996, 24(2): 123-140.

[21] MISHRA P K, YADAV A, PAZOKI M. A novel fault classification scheme for series capacitor compensated transmission line based on bagged tree ensemble classifier[J]. IEEE Access, 2018(6): 27373-27382.

[22] LE TT H, KANG H, KIM H. Household appliance classification using lower odd-numbered harmonics and the bagging decision tree[J]. IEEE Access, 2020(8): 55937-55952.

[23] 工业互联网产业联盟. 工业互联网平台白皮书（2017）[EB]. 2017.
Alliance of Industrial Internet Industrial internet platform white paper (2017) [EB]. 2017.

[24] MORASSO P, MUSSA IVALDI F A. Trajectory formation and handwriting: a computational model[J]. Biological Cybernetics, 1982, 45(2): 131-142.

[25] UNO Y, KAWATO M, SUZUKI R. Formation and control of optimal trajectory in human multijoint arm movement[J]. Biological Cybernetics, 1989, 61(2): 89-101.

[26] LEE D, PORT N L, GEORGOPOULOS A P. Manual interception of moving targets. II. On-line control of overlapping submovements[J]. Experimental Brain Research, 1997, 116(3): 421-433.

[27] NOVAK K E, MILLER L E, HOUK J C. The use of overlapping submovements in the control of rapid hand movements[J]. Experimental Brain Research, 2002, 144(3): 351-364.

[28] 郇战, 陈学杰, 吕士云,等. 基于多分类器融合的步态识别方法[J]. 计算机应用, 2019, 39(3): 712-718.
HUAN Z, CHEN X J, LYU S Y, et al. Gait recognition method based on multiple classifier fusion[J]. Journal of Computer Applications, 2019, 39(3): 712-718.

[29] HUANG N E, SHEN Z, LONG S R, et al. The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis[J]. Proceedings of the Royal Society of London Series A: Mathematical, Physical and Engineering Sciences, 1998, 454(1971): 903-995.

[30] AYENU-PRAH A, ATTOH-OKINE N. A criterion for selecting relevant intrinsic mode functions in empirical mode decomposition[J]. Advances in Adaptive Data Analysis, 2010, 2(1): 1-24.

[31] MANN K A, WERNERE F W, PALMER A K. Frequency spectrum analysis of wrist motion for activities of daily living[J]. Journal of Orthopaedic Research, 1989, 7(2): 304-306.

[32] HARILAL A, TOFFALINI F, CASTELLANOS J, et al. TWOS: adataset of malicious insider threat behavior based on a gamified competition[C]//Proceedings of the 2017 International Workshop on Managing Insider Security Threats. New York: ACM, 2017: 45-56.

[33] HAN H, WANG W Y, MAO B H. Borderline-SMOTE: anew over-sampling method in imbalanced data sets learning[C]//Advances in Intelligent Computing, 2005: 878-887.

[34] GAMBOA H, FRED A L N, JAIN A K. Webbiometrics: user verification via web interaction[C]//Proceedings of 2007 Biometrics Symposium. Piscataway: IEEE Press, 2007: 1-6.

[35] SHEN C, CAI Z M, GUAN X H. Continuous authentication for mouse dynamics: a pattern-growth approach[C]//Proceedings of IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012). Piscataway: IEEE Press, 2012: 1-12.

[36] ZHENG N, PALOSKI A, WANG H N. An efficient user verification system via mouse movements[C]//CCS '11: Proceedings of the 18th ACM Conference on Computer and Communications Security. 2011: 139-150.

[37] LINZ. Research on agent-based human-information system trusted interaction in distributed cooperative work environment[J]. The Open Automation and Control Systems Journal, 2011, 3(1): 1-7.

[作者简介]

张一弓（1996− ），男，重庆大学电气学院博士生，主要研究方向为网络用户行为模式与可信交互、电力物联网。

易茜（1986−），女，博士，重庆大学讲师、硕士生导师，主要研究方向为网络用户行为模式与可信交互、智能制造系统、绿色制造等。

李剑（1971− ），男，博士，重庆大学教授、博士生导师，国家杰出青年科学基金获得者，主要研究方向为电工绝缘新材料、电力装备智能化、物联网等。

尹爱军（1978− ），男，博士，重庆大学教授、博士生导师，主要研究方向为智能测试仪器、工业大数据智能运维系统、设备故障诊断与预测、高端装备等。

李聪波（1981− ），男，博士，重庆大学教授、博士生导师，主要研究方向为绿色制造、智能制造系统、制造系统工程等。

易树平（1960− ），男，博士，重庆大学教授、博士生导师，主要研究方向为工业工程理论与技术、数字化背景下的人因工程、智能制造等。