Hand in Motion: Enhanced Authentication Through Wrist and Mouse Movement

Borui Li[1], Wei Wang[2], Yang Gao[2], Vir V. Phoha[3], and Zhanpeng Jin[2]
[1]Binghamton University, SUNY, Binghamton, NY 13902
[2]University at Buffalo, SUNY, Buffalo, NY 14260
[3]Syracuse University, Syracuse, NY 13244
bli28@binghamton.edu, {wwang49,ygao36,zjin}@buffalo.edu, vvphoha@syr.edu

Abstract

Behavioral biometrics have been long used as a complementary method to the traditional one-time authentication system. Mouse dynamics, representing an individual's unique patterns of mouse operations, possess a great potential to bridge the security gap between two one-time authentications on the computer. In this paper, we propose a continuous authentication approach by combining the device-independent, angle-based mouse movement features and the wrist motion features. Based on a Random Forest Ensemble Classifier (RFEC) and the Sequential Sampling Analysis (SSA), the identity of the user can be continuously verified. Experimental results, based on 26 subjects, show that the proposed approach can reach the False Accept Rate (FAR) of 1.46% and 4.69% for impostors and intruders respectively and a False Reject Rate (FRR) of 0%. Moreover, the proposed approach is proven to be more effective in timely authentication (i.e., making an authentication decision within only 9 to 12 mouse clicks), compared with conventional methods solely based on the mouse geometry and locomotion features.

1. Introduction

Traditional one-time authentication approaches, like password and fingerprint biometrics, have been extensively studied and proven to be effective in preventing unauthorized access to the system. However, given the fact that these authentication processes take place only once before granting access, they lack the capability of monitoring the system on the fly to protect against an adversary's access in the middle of computer operations. So there is a profound need for an authentication system which can continuously monitor, evaluate, and verify the identity of the current user. Specifically, continuous authentication takes place both before granting access and continuously through the entire duration of the user's operation to maintain the granted access.

Generally, there are three types of biometrics that can provide solutions for the continuous authentication — soft biometrics, bio-signal biometrics, and behavioral biometrics. Soft biometrics, which is defined as human characteristics providing individually classifiable information, such as body weight, skin color, and facial marks [2, 7], is a popular method for continuous authentication. However, it "lacks the distinctiveness and permanence to sufficiently differentiate any two individuals" [7]. Moreover, most of the soft biometric feature acquisition processes require real-time camera monitoring, which is more intrusive to the users and may result in privacy concerns. Bio-signals, such as electrocardiograph (ECG), represent another type of biometrics that can be naturally used for continuous authentication. However, most bio-signal biometric systems need tedious perpetual wire connections with the sensors and the conductive gel applied onto the skin, which are inconvenient and less user-friendly. The third category — behavioral biometrics — involves an individual's uniquely measurable behavioral patterns such as gait, voice and signature. When accessing and securing a computer system, mouse and keystroke dynamics are the two most suitable behavioral traits for continuous authentication, which are non-intrusive and hassle-free, in terms that people can use their computers as usual. Recently, many research efforts have explored the intrinsic characteristic patterns of mouse operations for continuous authentication [17, 18, 28, 29].

In this paper, we propose and develop an enhanced mouse-based continuous authentication system by incorporating the dynamics of wrist motions. With the increasing advances and popularity of wearable devices, such as wristbands and smartwatches, human wrist motion behaviors [11] can be recorded and associated with the corresponding mouse operation activities. Compared with the

978-1-5386-7180-1/18/$31.00

traditional mouse-based authentication, our wrist motion enhanced, pattern-free mouse operation approach can provide higher efficiency and accuracy for continuous authentication, without sacrificing user experience or involving extra overhead. In addition to the non-intrusiveness and low cost, the proposed method has the following characteristics:

- Most prior research on mouse-based continuous authentication collects mouse dynamics data from different computers or even different mice [17, 28], which however, may diminish their validity due to the potential electrical and physical differences among different mouse units and different computer configurations. In this study, our mouse dynamics data are solely collected from the same mouse and the same computer.
- Leveraging the one-vs-all Random Forest Ensemble Classifier (RFEC), the proposed system can effectively detect both the *imposters* (a subject who belongs to the training database and whose identity is labeled as the attacker) and the *intruders* (a subject of other cases who does not belong to the database).
- Instead of using fixed, empirical thresholds, we propose to use the Sequential Sampling Analysis (SSA) to allow continuous monitoring and real-time evaluation of the mouse dynamics of the user based upon a dynamically evolving threshold setting.
- The wrist motion behavioral patterns captured by the wrist-worn smart devices (e.g., smartwatches or wristbands) can significantly improve the detection accuracy of imposters and intruders and also reduce the detection latency (i.e., the number of mouse clicks required to verify the identity of a user).
- Personalization on the feature sets by RFEC can boost the detection performance for unauthorized users and significantly reduce the computation overhead.

The remainder of this paper is organized as follows. Section 2 introduces the state of the art of mouse dynamics based authentication. Section 3 formulates the threat models and research problems. In Section 4, technical details including the angle-based mouse dynamics features, wrist motion features, feature fusion, RFEC classification, and SSA method are well described. Section 5 presents the experimental setting and protocol. A comprehensive analysis on experimental results is discussed in Section 6. Section 7 concludes this research and foresees the future work.

2. Related Work

Mouse dynamics have been extensively studied and used as a behavioral biometric approach. Most of the related research have relied on the distance or speed related features of mouse dynamics [1, 12, 15, 18, 23, 24]. For instance, features were extracted from the perspectives of geometry and locomotion, such as travel distance of pixels, elapsed time during actions, movement speed, acceleration and direction of movement [1]. With a definition of action types of move & click, regular move, and drag & drop, Lin *et al.* [12] implemented a distance-based feature extraction on file-related mouse operations and tested the system using the support vector machine SVM, decision trees and k-nearest neighbor (kNN) classifiers. Mondal *et al.* [18] also utilized the distance-based features and evaluated the mouse-based continuous authentication with multiple machine learning algorithms and a dynamic score model on the database containing 49 subjects [1].

Although the geometry- and locomotion-based features have been proven to be effective in representing the mouse operational behaviors, they are all subject to the device-dependent limitations. That is, the mouse dynamics may be affected by the inherent physical differences among various mouse units or among the different computer configurations. For example, either optical resolutions or pointer speeds could significantly influence the extracted features.

Another popular feature extraction approach is to use device-independent, angle-based measures [5, 29]. Hinbarji *et al.* [5] used the curvature features with a back propagation neural network as the classifier to reach an EER of 5.3% on 10 subjects. Such fine-grained (point-by-point) angle-based metrics of mouse movements were unique enough for distinguishing the mouse operators and independent from the specific hardware. However, these angle-based metrics were based on statistical distributions, resulting in a sliding window of 20 move&click for every authentication decision. Such fixed-window size approaches are not optimal for continuous authentication purpose, and not adaptable towards the user's own behaviors.

Furthermore, as the recent advances of wearable sensors and smart devices, many studies have explored the use of wearable sensor data for authentication and security purpose. For example, similar to the techniques that utilize mouse dynamics for static authentication [20, 22, 25], researchers have used the motion sensor data from the smartwatches to access computers through some pre-defined arm movement gestures [19, 27]. Other researchers have also used the motion sensor data from the smartwatches to infer the specific keystroke actions and even what the user is typing [13, 21, 26]. Mare *et al.* [16] explored how to utilize the motion sensor built in the bracelet to analyze people's typing characteristics for continuous authentication purpose. All related work above have shown the significance and usability of wrist motion behaviors in characterizing a specific individual. However, to the best of our knowledge, there appears to be little existing work that has explored the use of wearable sensors to enhance the mouse dynamics based continuous authentication.

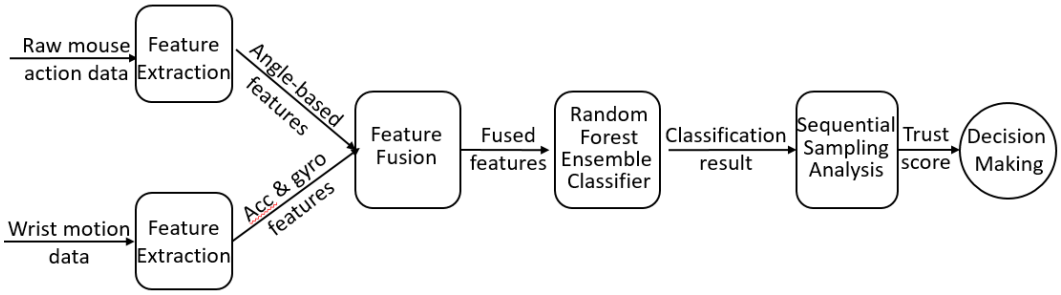


Figure 1. Flow digraph of the wrist motion enhanced, mouse dynamics based continuous authentication.

3. Threat Model

We consider an adversary who aims to gain unauthorized (and extended) access to the target system when the legitimate user is away from the computer while leaving the terminal open. Most existing computer systems typically do not possess any mechanism to verify that the user originally authenticated is the user still in control of the computer. It is a common scenario in which the user does not exercise adequate vigilance after initially authenticating at the console, such as forgetting to log-out when stepping away or staying nearby while focusing on other tasks (e.g., talking to someone or grabbing a coffee). Given this security threat, we propose a system that can continuously validating the identity of the user based on mouse dynamics and wrist motion behaviors when the user is operating the system.

3.1. Assumptions

For the threat model and our proposed defense scheme discussed above, we make the following assumptions:

Assumption 1: We assume that each individual user (including the legitimate users and the attackers) will wear a wearable smart device (e.g., a wristband or a smart-watch) on the wrist that has been paired to the computer system during the operation of dragging and moving the mouse.

Assumption 2: The wrist-worn device must contain the accelerometer and the gyroscope which are the most common built-in sensors for wearable devices.

3.2. Objectives

As an effective user authentication system, we consider three different roles of users, which are defined as follows:

- ***Genuine User***: The only authorized person who can access the system. Each time only one subject is randomly chosen as the genuine user to train the classifier.
- ***Impostors***: The people who attempts to illegally access the system and whose data has been partially known by the classifier.
- ***Intruders***: The people who attempts to illegally access the system but whose data is entirely unknown by the classifier.

Also, in this paper, we aim to address the following desired objectives:

Continuity: The proposed system can monitor the user's mouse operations and wrist motion behaviors continuously, unless the user involuntarily stop the mouse movement during the course of operating the computer.

Real-time: The proposed system can evaluate every mouse moving and clicking action and thus verify the identity of the current user in a near real-time manner, according to the dynamically evolving thresholds reflecting the user's accumulated performance.

Non-intrusiveness: The proposed system does not interrupt or interfere with the user's regular computer operation tasks. All data recordings and authentication analysis will be performed in the background.

Accuracy: The proposed system should be capable of capturing the most distinguishable features in mouse dynamics and wrist motion behaviors and correctly accepting or rejecting an individual identity with rather low matching errors (e.g., false acceptance rate and false rejection rate).

4. Continuous Authentication Using Mouse Dynamics

The general structure of the proposed continuous authentication system mainly consists of four parts as shown in Figure 1. The collected raw mouse action data and wrist motion data were first fed into the feature extraction module to obtain the angle-based mouse movement features and the acceleration & gyroscope features. Through a feature fusion model, two kinds of features are fused together. Then the RFEC uses these features to generate confidence scores. Based on these confidence scores, SSA calculates the trust scores and corresponding thresholds for acceptance or denial. A final authentication decision will be made if the current trust score is beyond any of the two thresholds.

4.1. Feature Extractions

4.1.1 Angle-based Feature Extraction

The adopted features in the proposed system are based on three types of angle metrics, as shown in Figure 2. The first metric is the *direction*, which is the angle x between $\overrightarrow{BC}$ and the horizontal. The second metric is the *angle*

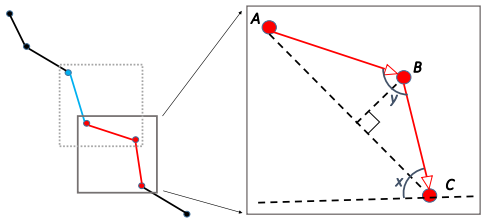


Figure 2. Example of angle metrics

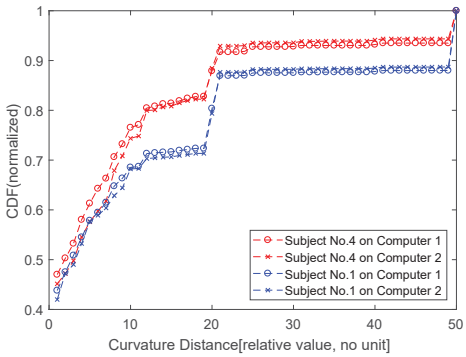


Figure 3. Example of curvature distance cumulative distribution

of curvature which is the angle between $\overrightarrow{AB}$ and $\overrightarrow{BC}$ denoted as $\angle ABC$. The last metric is the *curvature distance*, representing the ratio between the distance from point B to $\overrightarrow{AC}$ and the length of $\overrightarrow{AC}$. These three types of metrics are inter-related and complementary to shape a triangle. Probability distributions were further calculated for these three metrics respectively. For the *direction*, 360 features were extracted on the probability distribution among 1 to 360 degree. For the *curvature angle*, 180 features were extracted on the probability distribution from 1 to 180 degrees. 35 features were extracted on the probability distribution for the *curvature distance* with a range from 0 to 0.35.

As the extracted features should represent the distinctiveness of the different mouse operation behaviors from each individual, not the uniqueness resulted from settings such like pointer speed or hardware configurations. Compared with the traditional distance-based features, angle-based features are more robust and less sensitive to the specific model or setting of the device. Figure 3 depicts the cumulative distributions of the *curvature distance* of two subjects on different configurations. Both subjects operate the mouse to click on the same points randomly displayed on the screen repeatedly. It is observed that, this feature can precisely distinguish the difference between different individuals instead of different environmental settings.

This preliminary study showed that the angle-based probability distribution features are device-independent and thus can represent the uniqueness of mouse operational behaviors among different people, on the same device.

In order to achieve real-time monitoring and authentication, probability distributions are calculated upon each move & click trajectory, instead of being extracted for every 20 move & click trajectories, as implemented in [29].

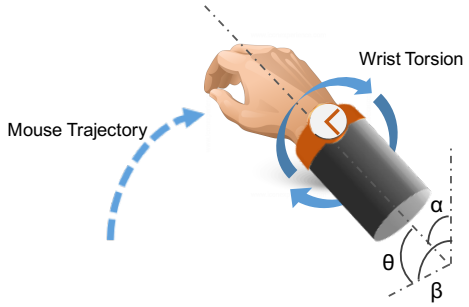


Figure 4. Overview of the two observations combining the mouse trajectory and the wrist torsion. Rotation angel α, β, and θ are pitch, roll, and jaw respectively.

The interval to separate two different trajectories was set to 100 ms [6, 8]. The software we used to record mouse trajectories can output the pointer location in the plane (horizontal and vertical dimensions) with the corresponding time stamp in ms and its action type as "move" or "click". In this way, the data can be divided into a lot of trajectory segments with two action types - regular move (all data points in this trajectory are labeled as the "move" actions) or move & click (i.e., the last data point of this trajectory segment is "click," while all previous data points are "move"). Because the "move" action's curvature characteristics could be quite arbitrary and thus are not representative in describing an individual's mouse operational behaviors. Therefore, in our study, we only use the move & click trajectories to extract the features. After segmentation, the entire angle-based feature set $\mathcal{F}_a$for the ith move & click trajectory can be depicted as follows:

$$\mathcal{F}_a(i) = \{PDF_{direction}(i), PDF_{distance}(i), PDF_{angle}(i)\} \quad (1)$$

where $PDF_{direction}$, $PDF_{distance}$, and PDF_{angle} denote the probability density functions (PDF) of the three angle metrics discussed above, *direction*, *curvature distance*, and the *curvature angle*, respectively.

4.1.2 Wrist Motion Feature Extraction and Fusion

In addition to the differences reflected in the angle-based features of mouse dynamics, differences may also exist in the wrist motion patterns. It has been demonstrated that the statistical distributions of acceleration and angular acceleration features captured by a smartwatch are individually unique [10] when the user is performing gesture-based operations on smartphones. As illustrated in Figure 4, given the observation that different individuals have their own habits and preferences of moving and rotating hands when they are operating the mouse. It is argued that the uniqueness of each individual also exists in their wrist motion behaviors when operating a mouse. Moreover, it is worthy to note that, the shape and size of the hands can effect and influence the wrist motion behaviors.

In this study, we use the built-in motion sensors in a smartwatch (i.e., SONY Smartwatch 3 SWR50) to capture the acceleration and angular acceleration data. We use the same start and end points of click segmentations for both angle-based features and wrist motion features. We extract the probability distribution features of acceleration

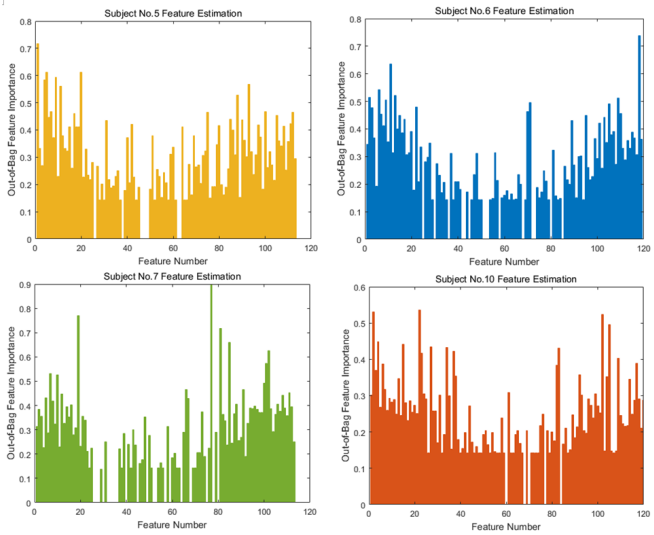


Figure 5. Estimated feature importance of two subjects

and angular acceleration data for each click action, according to their amplitudes computed from the three axises as $m = \sqrt{x^2 + y^2 + z^2}$. The distribution features obtained from the two motion sensors on the ith click segment is annotated as:

$$\mathcal{F}_w(i) = \{PDF_{acc}(i), PDF_{gyr}(i)\} \quad (2)$$

Finally, the angle-based feature set $\mathcal{F}_a(i)$ and the wrist motion feature set $\mathcal{F}_w(i)$ of the ith click action can be concatenated and fused as:

$$\mathcal{F}(i) = \{\mathcal{F}_a(i), \mathcal{F}_w(i)\} \quad (3)$$

Apparently, not all the features extracted are significant and useful for all subjects. An example of feature importance estimation of 4 different users is shown in Figure 5, it indicates that different subjects have their own optimal feature sets. To find the optimal features for all users, we utilize the filtering and retraining model for Random Forest Ensemble classifier similar to the gene selection in [4].

4.2. Random Forest Ensemble Classifier

Due to the large variance and high feature dimensionality associated with mouse dynamics and wrist motions, classifiers adopted need to be able to handle the high variance data, be resistant to over-fitting and automatically select the most important and suitable features. In this study, the Random Forest Ensemble Classifier (RFEC) is used. It is an aggregation of a number of base classifiers $h(X, \Theta_k), (k = 1, 2, ..., K)$. Θ_k is the parameter set for each individual decision tree, and K represents the number of trees. Under the condition that input data X is given, majority voting over all base classifiers can be realized by function h.

The fully growing of each decision tree makes RFEC capable of processing high dimensional features and the majority voting with w_k aggregation method makes it resistant to over-fitting and effective in handling high variance data. Based on the importance estimation of the random

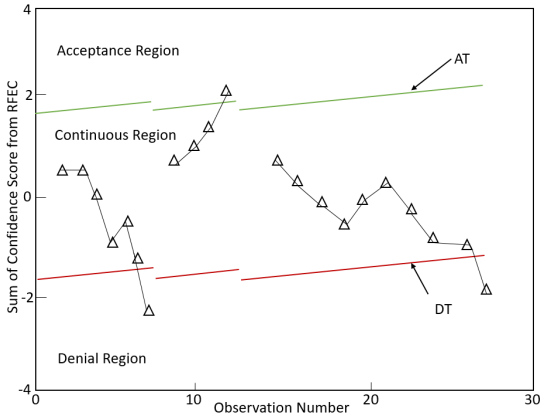


Figure 6. Example of Sequential Sampling Analysis

forest, the RFEC is iteratively trained. In each iteration, part of the less important feature cells are discarded and then a new RFEC is trained with the updated feature set. Through the returned Out of Bag (OOB) error of each iteration, the RFEC which performs the best and the corresponding feature set are kept as the optimal one for this specific user.

4.3. Sequential Sampling Analysis

With the goal of realizing dynamic thresholding on the returned confidence results from RFEC, Sequential Sampling Analysis (SSA) [14] is adopted and optimized to improve the efficiency and stability of intrusion detection in the proposed authentication system.

It is well recognized that the selection of proper thresholds has significant influence on the performance of a biometric authentication system. Especially for continuous authentication, the threshold settings will affect not only the authentication accuracy, but also the required time to identify the current user. For instance, a rather low rejection threshold would not deny an attacker's access until detecting too many mismatched mouse activity patterns, while a higher rejection threshold may result in frequent false rejections if the genuine user shows a few variant activity patterns. To this end, the proposed SSA can dynamically determine and update the thresholds for acceptance and rejection, based on the statistical analysis of all incoming data.

As shown in Figure 6, usually three regions are defined in SSA: *acceptance region*, *continuous region* and *denial region*, divided by the Acceptance Threshold (AT) and the Denial Threshold (DT). The region above the AT is defined as the acceptance region, the region between AT and DT is the continuous region and that beneath DT is the denial region. The sum of confidence scores is denoted as $S_n = \sum_{i=1}^{n} s(i)$, where $s(i)$ represents the confidence score returned by RFEC for the ith click. The system will accept the current user when his/her sum of scores reaches the acceptance region and deny the user once it drops into the denial region. When S_n fluctuates in the continuous region, the SSA will keep watching new click actions by ac-

cumulating the incoming click score $s(n+1)$ into S_{n+1} and updating the AT and DT with a slope b. In order to properly set the thresholds AT and DT, their climbing slope b and initial threshold l are calculated based on the distribution mean μ and standard deviation δ of the training data's confidential scores. The AT and DT can therefore be calculated and updated as follows:

$$AT = bn + l1, \quad DT = bn + l2 \tag{4}$$

where slope b and initial thresholds $l1$, $l2$ are defined as:

$$b = \frac{\mu_1 + \mu_2}{2}, \quad l1 = \frac{B\delta_1^2}{\mu_1 - \mu_2}, \quad l2 = \frac{A\delta_2^2}{\mu_2 - \mu_1} \tag{5}$$

The parameters A and B are defined as:

$$A = log\frac{1-\alpha}{\beta}, \quad B = log\frac{1-\beta}{\alpha} \tag{6}$$

where α and β represent the error tolerances of false rejection and false acceptance in SSA (for a balanced FAR and FRR, usually set $\alpha = \beta$). A higher tolerance will result in a wider continuous region, which will potentially lead to higher decision accuracy, while demanding more mouse clicks to identity the current user.

Leveraging this improved SSA mechanism, our proposed system can continuously evaluate the operational behaviors of the current user based upon each mouse move & click action. Consecutive "good (matching)" or "bad (mismatching)" mouse operations can expedite the decision making and thus accept or reject the user in a more timely manner. In real-world scenarios, the proposed technique can immediately lock out the system if the accumulated score drops below DT. Otherwise, the continuous authentication process will keep running in the background, if the score remains in the continuous or acceptance regions.

5. Experimental Setup

5.1. Experimental Protocol

In the experiments, subjects were instructed to seat on a chair in a natural and comfortable position and use the mouse to click on a red block icon (100 px $\times$ 100 px) that randomly showed up on the screen using a web-page-style software. The target block icons would show up one after another with the clicking behavior as the triggering condition. Clicking mistakes were allowed, which meant the subjects were free to retry if they hit the wrong place. The Recording User Input (RUI) software [9] was used for mouse data collection. Specific type of actions (i.e., clicking or moving) and the 2-dimensional mouse locations were recorded along with timestamps. The sampling rate of RUI was up to 100 Hz.

During the experimental sessions, all the subjects were required to wear the same smartwatch (i.e., SONY SWR50 SmartWatch 3) on the wrist of their dominant hand (the hand they use to operate the mouse) to record the accelerometer and gyroscope readings. All subjects involved in the experiments were of right-handedness. The subjects were seated on the same model of office chairs with a fixed height (40 cm) during all the experimental sessions. To demonstrate that our system is actually authenticating for different people rather than different mouse/pointer settings or computers, all the subjects were required to use exactly the same mouse (i.e., Dell MS116p optical mouse) connected to the same computer (with the screen resolution as 3440*1440). The clicking speed of mouse and the tracking speed of pointer were set as the default values.

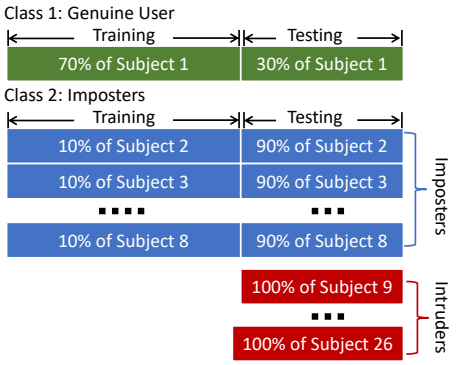


Figure 7. Data Structure

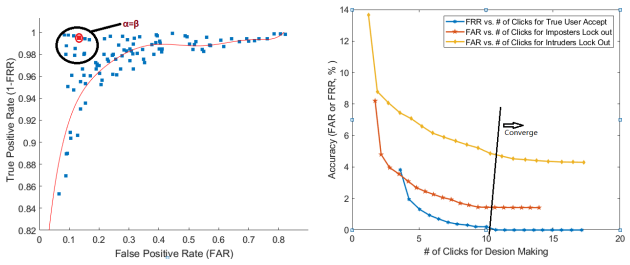
5.2. Data Structure

26 subjects (7 female, 19 male) of age from 23 to 33 were recruited to voluntarily participate in the experiments. To mimic the real-world environment, which means that the authentication system has limited training dataset compared with many unknown adversaries' attempts, in this work, we assigned 8 out of 26 subjects as the genuine user or the impostors, and the rest 18 subjects were considered as the intruders. Each time, to train the classifier, one of 8 subjects was randomly designated as the genuine user, and the rest 7 subjects were designated as the impostors. For the genuine user and the impostors, the data collected from each subject contained 1000 mouse clicks on average from five sessions during a period of two weeks (1000 clicks are sufficient to profile a user's mouse behaviors well, according to [29]). For each intruder, an average of 200 clicks were collected from one session. The detailed training and testing dataset allocation is shown in Figure 7.

6. Results

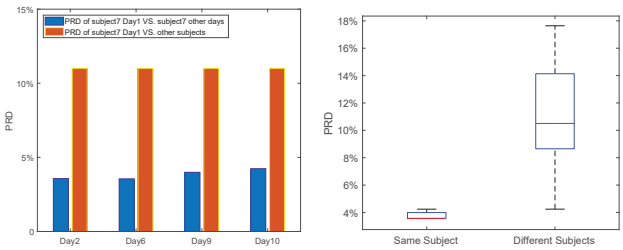
6.1. Metrics

Three performance indicators are used in the evaluation, including the False Acceptance Rate (FAR), the False Rejection Rate (FRR), and the average number of clicks required for evaluation of the current user's identity and make the authentication decisions (i.e., accep-



(a) (b)

Figure 8. (a):Scatter plot of the pairs of FAR and FRR given different α and β parameter settings;(b):Trade off of accuracy and efficiency given different α and β parameter settings.



(a) (b)

Figure 9. Permanence of the proposed wrist+mouse continuous authentication approach.

tance/rejection). Specifically, in this study, FRR refers to the percentage ratio between the mouse click samples of the genuine user that are falsely classified and labeled as the 'attacker' against the total number of click samples from the genuine user. FAR is defined as the percentage ratio between the click samples of the imposters/intruders that are falsely classified and accepted as the "true user" against the total number of click samples from the imposters and intruders who intend to access the system. Based on the implemented SSA mechanism which locks out any unauthorized user access or accept an authorized user when the accumulated score drops below the denial threshold or above the acceptance threshold, the number of clicks required for making the decision is recorded as an indicator of the efficiency of the proposed approach. It is manifest that less number of required clicks will result in a much faster and more timely acceptance of the genuine user or detection of malicious attackers, which however, will potentially degrade the authentication accuracy in terms of FRR and FAR.

6.2. Parameter Settings

It was reported that [14] the reasonable value range of parameters α and β in SSA should be from $10e-20$ to $10e-1$. Smaller α and β will give the SSA higher tolerance on FAR and FRR. To investigate the influence of parameter settings, in this study we divided α and β into 20 levels. Due to the reason that tuning α and β will not only affect FRR and FAR but also change the efficiency of continuous authentication (i.e., how many mouse clicks required for one acceptance or denial decision), the scatter plot for the pairs of FAR and FRR in Figure 8(a) is not as same as the regular ROC curve for binary classification which has a one-to-one correspondence between FRR and FAR. However, it can be observed that, based on the general trend of FAR and TPR (True Positive Rate which also equals to 1-FRR) which is plotted by the red line through the 7th-order polynomial curve fitting, there is still clear trade-off between FAR and FRR when we tune the parameters α and β. Through brute-force search among all the combinations of α and β with the 20 pre-defined levels, it is found that, when $\alpha = \beta$, the pairs of FAR and FRR are located close to the upper left corner (circled) and the system will yield the best performance (i.e., low FAR and high TPR).

In addition to considering the accuracy performance, efficiency is another important metric we need to assess when we tune the parameters. Based on the assumption of $\alpha = \beta$, Figure 8(b) presents how FRR, FAR and the corresponding number of mouse clicks needed for each authentication decision vary along with the increasing error tolerance (i.e., the decreasing parameters α and β). Unsurprisingly, the authentication accuracy improves (i.e., FRR and FAR), and the efficiency is degrading (i.e., more mouse clicks are needed for each decision). In order to achieve an optimal performance balance, in this study we chose $\alpha = \beta = 10^{-12}$ as the parameter settings (the red spot in Figure 8(a)) for our SSA process, which can generate relatively low FRR and FAR with only 9 to 12 mouse clicks for continuous authentication decision-making.

6.3. Performance

Tables 1 and 2 present the performance of the two different continuous approaches — the wrist motion enhanced method and the mouse-only method — when randomly selecting and assigning one subject (out of Subjects 1-8) as the genuine user.

It is observed that from Table 3, the wrist+mouse approach can achieve an FRR of 0%, FAR (imposters) of 1.46% and FAR (intruders) of 4.69% on average, while demanding only 9-12 mouse clicks to make an authentication decision. Under the same parameter setting, very similar accuracy levels can still be achieved by the mouse-only approach, which however, requires much more mouse clicks in order to make an authentication decision and thus results in a degraded time efficiency. A comparison of these two approaches shows that, our proposed wrist motion and mouse dynamics based feature fusion approach can reach nearly the same accuracy, while with a significantly improved authentication efficiency: 24.4% for detection of the genuine user detection, 31% for detection of the imposters, and 49% for detection of the intruders. Compared with the performance reported in [29], both of our approaches (i.e., wrist+mouse and mouse-only) can reach a similar accuracy

Table 1. Performance of the wrist motion enhanced, mouse dynamics based continuous authentication

Genuine Users	FRR	FAR			Avg # of Clicks for Detection of Attacks			
		Imposters	Intruders	All	True User	Imposters	Intruders	All
Subject1	0.00%	1.56%	3.05%	1.95%	14.0	6.8	8.1	7.5
Subject2	0.00%	3.01%	2.60%	2.90%	8.9	7.1	8.1	7.5
Subject3	0.00%	1.29%	6.93%	2.77%	12.9	10.6	13.0	11.3
Subject4	0.00%	0.19%	1.84%	0.67%	9.9	5.7	6.0	6.0
Subject5	0.00%	0.37%	4.39%	2.51%	11.8	8.0	9.9	8.7
Subject6	0.00%	1.24%	1.10%	1.20%	17.4	10.2	13.0	11.3
Subject7	0.00%	2.59%	6.05%	3.54%	11.6	12.3	14.2	12.7
Subject8	0.00%	1.45%	11.53%	4.27%	10.0	9.2	10.4	9.6
Avg	0.00%	1.46%	4.69%	2.48%	12.1	8.7	10.3	9.3

Table 2. Performance of the mouse-only continuous authentication

Genuine Users	FRR	FAR			Avg # of Clicks for Detection of Attacks			
		Imposters	Intruders	All	True User	Imposters	Intruders	All
Subject1	0.24%	1.74%	5.02%	2.24%	18.5	8.9	22.8	14.7
Subject2	0.00%	4.53%	3.37%	4.21%	12.9	11.8	18.9	16.8
Subject3	0.00%	2.21%	7.62%	3.48%	15.6	13.9	22.6	18.8
Subject4	0.00%	0.15%	3.90%	1.35%	12.3	9.6	16.6	12.3
Subject5	0.07%	0.92%	4.29%	2.76%	14.9	12.5	18.9	14.8
Subject6	0.00%	2.89%	3.62%	3.06%	22.8	19.9	25.7	22.6
Subject7	0.00%	4.66%	8.60%	5.48%	15.5	12.7	17.4	15.7
Subject8	0.53%	5.54%	14.11%	7.72%	15.8	11.2	19.0	15.6
Avg	0.11%	2.83%	6.32%	3.79%	16.0	12.6	20.2	16.4

Table 3. Performance comparisons of the proposed wrist+mouse approach and the mouse-only scheme

Features	FRR (Avg. # of Clicks)	FAR (Avg. # of Clicks)	
		Impostors	Intruders
Wrist + Mouse	0% (12.1)	1.46% (8.7)	4.69% (10.3)
Mouse Only	0.11% (16)	2.83% (12.6)	6.32% (20.2)

level with much better time efficiency.

6.4. Permanence

For biometric traits, the stability and invariability over time (commonly called "permanence") represent a critical requirement. To demonstrate the permanence of the chosen wrist motion and mouse dynamics features for continuous authentication, we evaluated the behaviors of one genuine user (Subject 7) in five different days and calculated the similarity across those days. The experimental data recordings of Subject 7 spanned over 10 days, and specifically we recorded the data on Day 1, Day 2, Day 6, Day 9 and Day 10 respectively). In this study, Percent Residual Difference (PRD) metric is used to gauge such similarity. PRD is a common quantitative measure that is used for the evaluation of differences between two distributions, which has been widely used in the research of other biometric modalities [3]. The formulation of PRD is defined as:

$$PRD = \sqrt{\frac{\sum_{i=1}^{N}(s_0(i) - s_n(i))^2}{\sum_{j=1}^{N}(s_0(i) - \bar{s_0})^2}} \times 100\% \qquad (7)$$

where s_n is the enrolled distribution, which has N data points. s_0 is the test distribution. Lower PRD represents a higher similarity between the enrolled distribution and the test distribution. Figure 9(a) presents the PRD values (in blue) between the distribution of Day 1 for Subject 7 and the distributions of the other 4 days. Similarly, Figure 9(a) also describes the PRD values (in red) between the distribution of Day 1 for Subject 7 and the averaged distributions of all other subjects in the same day. It is shown that, Subject 7's PRDs (in blue) slightly grows over time, which however, are still much smaller than the PRDs under different subjects (in red). To further demonstrate the permanence of wrist motion behaviors and mouse dynamics, for all the subjects who participated in the experiments, PRDs of the same subject (Subjects 1-8) cross different days and PRDs of different subjects are calculated and represented in box plot format in Figure 9(b). From this figure, we can see that there is a clear and distinguishable separation between those two groups of data, which further demonstrates the permanence and stability of the proposed approach over time.

7. Conclusions

Given the increasing demands on continuous authentication in order to properly secure the system during the course of operation, this study seeks to propose and investigate an effective approach capable of verifying the identity of the current user based on their wrist motion behaviors and mouse dynamics. Specifically, leveraging the Random Forest Ensemble Classifier (RFEC) and the Sequential Sampling Analysis (SSA), our wrist motion enhanced, pattern-free mouse operation approach can provide higher efficiency and accuracy for continuous authentication, without sacrificing user experience or involving extra overhead.

On the other side, this research is still in its early stage. Future work will focus on combining this proposed approach with other behavioral biometric modalities such as keystrokes to realize a comprehensive multi-modal continuous authentication solution. Furthermore, the evaluations

of accuracy, efficiency, and permanence demand a larger subject population and a longer long experimental duration.

Acknowledgment

This work was supported in part by the National Science Foundation (NSF) under grants SaTC-1422417, SaTC-1527795, and SaTC-1564046.

References

[1] A. A. E. Ahmed and I. Traore. A new biometric technology based on mouse dynamics. *IEEE Trans. Dependable Sec. Comput.*, 4(3):165, 2007.

[2] H. Ailisto, E. Vildjiounaite, M. Lindholm, S.-M. Mäkelä, and J. Peltola. Soft biometrics — combining body weight and fat measurements with fingerprint biometrics. *Pattern Recognition Letters*, 27(5):325–334, 2006.

[3] A. D. Chan, M. M. Hamdy, A. Badre, and V. Badee. Wavelet distance measure for person identification using electrocardiograms. *IEEE Trans. Instrum. Meas.*, 57(2):248–253, 2008.

[4] R. Díaz-Uriarte and S. A. De Andres. Gene selection and classification of microarray data using random forest. *BMC Bioinformatics*, 7(1):1, 2006.

[5] Z. Hinbarji, R. Albatal, and C. Gurrin. Dynamic user authentication based on mouse movements curves. In *Int'l Conf. on Multimedia Modeling*, pages 111–122. Springer, 2015.

[6] F. Hwang, S. Keates, P. Langdon, and J. Clarkson. A submovement analysis of cursor trajectories. *Behaviour & Information Technology*, 24(3):205–217, 2005.

[7] A. K. Jain, S. C. Dass, and K. Nandakumar. Soft biometric traits for personal recognition systems. In *Biometric authentication*, pages 731–738. Springer, 2004.

[8] S. Keates and S. Trewin. Effect of age and parkinson's disease on cursor positioning using a mouse. In *Proc. the 7th int'l ACM SIGACCESS Conf. on Computers and accessibility*, pages 68–75. ACM, 2005.

[9] U. Kukreja, W. E. Stevenson, and F. E. Ritter. RUI: Rec.ing user input from interfaces under Windows and Mac OS X. *Behavior Research Methods*, 38(4):656–659, 2006.

[10] W.-H. Lee and R. Lee. Implicit sensor-based authentication of smartphone users with smartwatch. In *Proc. the ACM 2016 Hardware and Architectural Support for Security and Privacy*, pages 1–8, 2016.

[11] B. Li, H. Sun, Y. Gao, V. V. Phoha, and Z. Jin. Enhanced free-text keystroke continuous authentication based on dynamics of wrist motion. In *Proc. IEEE Int'l Workshop Inf. Forensics and Security (WIFS)*, pages 1–6. IEEE, 2017.

[12] C.-C. Lin, C.-C. Chang, and D. Liang. A new non-intrusive authentication approach for data protection based on mouse dynamics. In *Proc. 2012 Int'l Symposium on Biometrics and Security Technologies*, pages 9–14. IEEE, 2012.

[13] X. Liu, Z. Zhou, W. Diao, Z. Li, and K. Zhang. When good becomes evil: Keystroke inference with smartwatch. In *Proc. 22nd ACM Conf. Comp. Comm. Security (CCS)*, pages 1273–1285, 2015.

[14] W. Louis, M. Komeili, and D. Hatzinakos. Continuous authentication using one-dimensional multi-resolution local binary patterns (1DMRLBP) in ECG biometrics. *IEEE Trans. Inf. Forensics Security*, 11(12):2818–2832, 2016.

[15] L. Ma, C. Yan, P. Zhao, and M. Wang. A kind of mouse behavior authentication method on dynamic soft keyboard. In *Proc. IEEE Int'l Conf. Syst., Man, Cybern.*, pages 211–216. IEEE, 2016.

[16] S. Mare, A. M. Markham, C. Cornelius, R. Peterson, and D. Kotz. Zebra: Zero-effort bilateral recurring authentication. In *Proc. IEEE Symposium Security and Privacy*, pages 705–720, 2014.

[17] S. Mondal and P. Bours. Continuous authentication using mouse dynamics. In *Proc. IEEE 2013 Int'l Conf. of the Biometrics Special Interest Group*, pages 1–12. IEEE, 2013.

[18] S. Mondal and P. Bours. A computational approach to the continuous authentication biometric system. *Information Sciences*, 304:28–53, 2015.

[19] M. A. S. Mondol, I. A. Emi, S. M. Preum, and J. A. Stankovic. User authentication using wrist mounted inertial sensors. In *Proc. 16th ACM/IEEE Int'l Conf. on Information Processing in Sensor Networks*, pages 309–310, 2017.

[20] R. Muda, N. A. Hamid, S. D. M. Satar, M. Mohamad, N. A. Mahadi, and F. Ghazali. Mouse movement behavioral biometric for static user authentication. *Advanced Science Letters*, 23(6):5050–5053, 2017.

[21] A. Sarkisyan, R. Debbiny, and A. Nahapetian. Wristsnoop: Smartphone PINs prediction using smartwatch motion sensors. In *Proc. IEEE Int'l Workshop Inf. Forensics and Security (WIFS)*, pages 1–6, Nov 2015.

[22] B. Sayed, I. Traore, I. Woungang, and M. S. Obaidat. Biometric authentication using mouse gesture dynamics. *IEEE Systems Journal*, 7(2):262–274, 2013.

[23] C. Shen, Z. Cai, and X. Guan. Can it be more practical? : Improving mouse dynamics biometric performance. In *Proc. 18th ACM Conf. Computer and Comm. Security (CCS)*, pages 853–856. ACM, 2011.

[24] C. Shen, Z. Cai, X. Guan, H. Sha, and J. Du. Feature analysis of mouse dynamics in identity authentication and monitoring. In *Proc. Int'l Conf. Comm.*, pages 1–5. IEEE, 2009.

[25] C. Shen, Z. Cai, X. Guan, and J. Wang. On the effectiveness and applicability of mouse dynamics biometric for static authentication: A benchmark study. In *Proc. 5th IAPR Int'l Conf. on Biometrics*, pages 378–383. IEEE, 2012.

[26] C. Wang, X. Guo, Y. Wang, Y. Chen, and B. Liu. Friend or foe?: Your wearable devices reveal your personal pin. In *Proc. 11th ACM Asia Conf. Comput. Commun. Security*, pages 189–200, 2016.

[27] J. Yang, Y. Li, and M. Xie. Motionauth: Motion-based authentication for wrist worn smart devices. In *Proc. IEEE Int'l Conf. on Pervasive Comp. Comm. Workshops*, pages 550–555. IEEE, 2015.

[28] N. Zheng, A. Paloski, and H. Wang. An efficient user verification system via mouse movements. In *Proc. 18th ACM Conf. Comp. Comm. Security (CCS)*, pages 139–150, 2011.

[29] N. Zheng, A. Paloski, and H. Wang. An efficient user verification system using angle-based mouse movement biometrics. *ACM Trans. Inf. Syst. Secur.*, 18(3):11, 2016.