G-PPG: A Gesture-related PPG-based Two-Factor Authentication for Wearable Devices

Jiaqi Pan¹, Xinyan Zhou¹*, Zenan Zhang¹, Xiaoyu Ji², Haiming Chen¹
¹Ningbo University, Ningbo, Zhejiang, China
²Zhejiang University, Hangzhou, Zhejiang, China
zhouxinyan@nbu.edu.cn

Abstract—Verifying the user identity of wearable devices is crucial for system security, especially before sensitive operations like making financial payments. A PPG-based two-factor authentication can be a promising solution with widely deployed PPG (Photoplethysmography) sensors within wearable devices. Our observations find PPG readings reveal a significant relevance to the user’s hand motions, i.e., gestures, while the user’s heartbeat characteristics and wearing habits are also implicitly related, which can be utilized for user authentication. In this paper, we design G-PPG, a gesture-related PPG-based two-factor authentication mechanism that can non-intrusively validate the user’s identity. In G-PPG, gesture detection and segmentation and a specific feature set are proposed for accurate gesture-related PPG characteristic extraction. Moreover, an adaptive update scheme is proposed for the high accuracy of long-term authentication. Our experiments among 15 participants demonstrate that G-PPG can achieve a 90% accuracy in the long-term study.

Index Terms—Wearable Security, Internet of Things, Two-factor Authentication, PPG sensors

I. INTRODUCTION

In recent years, wearable devices have drawn great attention in the IoT (Internet of Things) market and play essential roles in daily human life. With various embedded sensors, wearable devices like smartwatches reveal broad application scenarios for healthcare monitoring, navigation, fitness tracking, etc. With the enhancement of functionality, wearable devices are even utilized in sensitive scenarios (financial payment, etc.) and regarded as a trustworthy party with advanced authority that can access other smart devices, which are vulnerable in some unexpected cases. For example, an attacker can use the smartwatch to unlock the smart locker that has been prepared directly without further authentication. Without further protection, users usually get anxious when their wearable devices are stolen or lost, and their sensitive data or application account could be leakages by attackers.

In order to prevent the misuse of wearable devices, a continuous or two-factor authentication mechanism is necessary, especially when sensitive authorities are asked for it. A common solution to validate the user’s identity is asking the user to input a password or PIN, which usually lasts for seconds. However, weak password problems and credential stuffing attacks make password-based authentication risky and user-unfriendly.

To solve this problem, sensors that can extract users’ biometric features or behavior patterns are leveraged for continuous authentication yet face challenges. To be specific, fingerprint sensors can be fooled by fake fingerprints [1], and camera-based face recognition can be compromised by dedicated designed images [2]. To enhance the security of biometric-based authentication, a physiological feature that is hard to clone and observe should be applied. PPG (Photoplethysmography) sensor that captures the user’s heartbeat at the wrist-side becomes a promising candidate.

PPG is a non-intrusive optical biomonitoring technique that can measure the blood volume in vascular tissue under the skin in the wrist or fingertip area by receiving the reflected light rays. The received signal is related to the cardiac cycle’s systole and diastole, which can be utilized for heartbeat monitoring. Due to its reliable performance and low price, almost all current smart bands and watches are equipped with PPG sensors for health monitoring and sport detection, which makes it possible to use PPG for authentication.

Previous research demonstrates that PPG readings reveal unique and unclonable characteristics, and it is feasible to use PPG readings for user authentication [3]–[6]. However, PPG-based authentication still faces challenges. First, the PPG measurements are susceptible to movements, such as walking and riding, which may impact the authentication accuracy and utility, and a motion artifacts removal algorithm is also required. Besides, compared to fingertip-PPG, the wrist-PPG readings are typically weak and noisy. Therefore, existing methods usually need users to wear the device tightly to collect sufficient PPG signals for authentication. However, in practice, there is always a gap between the wristband and skin, and the gap even changes according to the user’s hand motion, which also reduces the accuracy and practicability of heartbeat-based PPG authentication.

Different from existing work, we propose G-PPG, which extracts gesture-related PPG readings for user authentication. Specifically, we find that PPG readings reveal unique and strong patterns when a user performs a specific gesture. Moreover, different users and gestures will show discriminative differences. With a thorough analysis of the above observations, we conclude that the gesture brings rhythmic changes to the gap between the PPG sensor and the skin, which reflect the user’s behavior pattern and the wearing habits. Furthermore, the heartbeat itself also introduces unique signals

* Xinyan Zhou is the corresponding author.
to the PPG measurements. As a joint result of the above two reasons, the gesture-related PPG shows great potential for user authentication. Besides common advantages of PPG-based authentications (non-intrusive, secure, and etc.), G-PPG has the following advantages: 1) **Anti-movement interference:** G-PPG derives features from gesture-related PPG signals, and hand movements are no noises but crucial patterns that should be carefully extracted. 2) **High accuracy:** both heartbeat characteristics and personal behavior habits are utilized for authentication, and sufficient individual features make it possible for accurate authentication. 3) **High robustness:** our platform enables reliable authentication during user movement. We validate the performance of G-PPG with a prototype among 15 candidates, and the results demonstrate that G-PPG can provide reliable two-factor authentication with a PPG sensor only. The main contributions of G-PPG are summarized in the following:

- We evaluate the feasibility of gesture-related PPG authentication, and gesture-dependence, user-dependence, and PPG sensor sensitivity are validated.
- We design G-PPG, which comprises a data acquisition and preprocessing module, a feature extraction module, a training phase, and the authentication module. A specific feature set is designed to extract gesture-related features. Moreover, an adaptive update mechanism is proposed for better user experience and long-term authentication.
- We build a prototype using a commodity PPG sensor, and we evaluate the performance of G-PPG with 15 candidates (11 males and 4 females). Experimental results prove the security and efficiency of our mechanism.
- We verify the performance of G-PPG with different daily activities (sitting and walking), and the results demonstrate that G-PPG can keep a high precision even with the interference of walking vibrations.

II. **RELATED WORK**

Extensive research has been proposed for continuous authentication or 2-factor authentication. According to the authentication objects (network, device, and user), we can divide authentication methods into proximity-based authentications, device-fingerprint-based authentications, and biometric-based authentications.

**Proximity-based Authentications:** Such methods authenticate devices by validating the device in a legitimate area or sharing common network connections. RSI (received signal indicator) [7]–[10] and CSI (channel state information) [11], [12] are two physical layer information that can be utilized to extract proximity-based keys for device authentication. For example, Xi et al. propose TDS (The Dancing Signals) which puts two devices into physical proximity and utilizes the common radio environment as a proof of identity, and generates a common key for device authentication. However, RSI-based mechanisms suffer from coarse-grained signal measurement, while CSI-based methods typically require dedicated hardware for signal measurements (an Intel 5300 Wi-Fi card). Besides radio signals, other types of signals like acoustic, vibration, and light [13]–[15] are also utilized for proximity-based authentication. However, the above methods usually involve multiple devices with various sensors, which show more hardware requirements and system environments.

**Device-fingerprint-based Authentications:** With the recognition of the device hardware imperfections, devices can be authenticated with their embedded hardware modules, which have been studied theoretically and experimentally [16]. Due to the naturally uncountable and unique characteristics, hardware modules like CPU [17], RF (radio frequency) front-ends [18], cameras [19], microphones [20], accelerometers [21], and gyroscopes [22] are widely utilized for device authentication and paring. By validating the identity of the registered device, the above methods show high authentication accuracy and consistency with the assumption that both the device and the device-holder are legitimate parties. Unfortunately, this assumption makes such mechanisms insecure when the attacker physically compromises the device, i.e., the attacker may utilize a legitimate device fingerprint to pass the authentication mechanism and log in to the system illegally.

**Biometric-based Authentications:** Compared to the above two authentication mechanisms, biometric-based ones authenticate users’ identities directly, which reveals natural reliability and can guarantee the legitimacy of the access behavior. For instance, human fingerprinting matching and face recognition have been used commercially (smartphones, smart lockers, etc.) due to their easy collection and long-term consistency characteristics. However, replay attacks, spoofing attacks, and synthesis attacks [23] that target on above mechanisms are reported frequently, and real-time or liveness user authentication mechanisms have been studied in recent years. Yan et al. [24] propose CaFiled. This text-independent speaker verification method can detect voice-spoofing attacks by constructing a “field print” with the acoustic biometrics embedded in the sound field.

**Wearable-based Authentications:** With the prevalence of wearable devices, PPG (photoplethysmography) and ECG (electrocardiogram) -based authentication methods are also studied. CardicCam [25] extracts unique cardiac futures from the cardiac motion patterns in fingerprints by asking users to press on a built-in camera, and Yang et al. [26] authenticate users via ECG data while preserving sensitive healthy data from being exposed to adversaries. As for the PPG sensors, Zhao et al. propose Trueheart [3], which is a continuous authentication (CA) mechanism that collects users’ heartbeats via PPG sensors. Cao et al. propose PPGPass [4], a non-intrusive and secure two-factor authentication system, and Bastos et al. [5] combine PPG and ECG for identity authentication. Both Trueheart [3] and PPGPass [4] can achieve a high authentication accuracy. However, due to the sensitivity of PPG sensors, motion artifacts removal algorithms are required to obtain clean heartbeat signals efficiently. Unlike the above methods, G-PPG leverages such sensitivity for user authentication. Specifically, G-PPG requires users to perform gestures and extracts gesture-related PPG features for authentication.
with the observation that PPG readings reveal both gesture-dependency and user-dependency.

III. G-PPG OVERVIEW

A. Feasibility Study

In G-PPG, we utilize the PPG measurements when users are required to operate designated gestures for authentication, based on the observations that different users reveal marked differences in PPG measurements with hand motions. We validate the feasibility of G-PPG with coarse-grained experiments in a PPG data collection platform, and details of the platform are illustrated in Sec. V.

User Consistency and Dependence. We first examine the user consistency and dependence of the PPG measurements with different gestures, which are fundamental characteristics of G-PPG. We capture PPG measurements from 4 users with the same gesture, and the sampling rate of the PPG is 100Hz. We plot 15 samples for each user directly in Fig. 1(a), which reveals significant consistency among samples. To further evaluate the user dependence, as shown in Fig 1(b), we find samples from different users can be simply separated in a two-dimension plane (i.e., skewness as the X-axis and standard deviation as the Y-axis). The above findings demonstrate that PPG measurements with gestures show great potential for user authentication.

Gesture dependence. For better user experience during the authentication, we further explore the gesture dependence, i.e., the PPG measurements could be distinguishable with different gestures. We utilize the same platform to collect PPG measurements from the same user with 3 different gestures, and 15 samples are collected for each gesture. Fig. 1(c) reveals the variance (X-axis) and skewness (Y-axis) of each sample, and we find different gestures are clearly clustered, which provides more choices for users and expands the data space for authentication.

Gesture Robustness. Users’ daily activities can impact the performance of PPG-based authentication [3], [4], and we validate the robustness of G-PPG in two different daily scenarios, including sitting and walking cases. As shown in Fig.1(d), gesture-related PPG signals can be clearly observed from PPG readings, while the motion artifacts may cover the original cardiac signals. Therefore, utilizing cardiac PPG signals alone for authentication requires an extra motion artifacts removal algorithm, while the gesture-related PPG signals show a great potential for a robust authentication performance.

B. System Overview

The basic idea of G-PPG is utilizing the PPG measurements changes during the gestures to authenticate the user’s identity. The fundamental principle is that PPG measurements reveal unique characteristics when users conduct hand gestures derived from the user’s wrist physiological features and the wearing habits of the wearable devices. Specifically, the gap between the wearable device and the user’s wrist skin is irregular among users, and the gap changes significantly when the user is conducting near-wrist gestures. By measuring the light reflections, PPG measurements are hypersensitive to user gestures, which can be utilized for authentication.

The architecture of our G-PPG is shown in Fig.2, G-PPG requires the user to follow a pre-defined gesture and collects PPG data in real-time to authenticate the user’s identity.

Data Acquisition and Preprocessing. With a dedicated gesture, we collect PPG measurements for further user authentication. Raw PPG sensor data inevitably contain disturbances from heart rate and other movements. Therefore, a basic noise reduction mechanism and a low pass filtering are necessary at the beginning of the data acquisition. Besides, gesture detection and segmentation are applied to extract gesture segments from continuous PPG measurements.

Feature Extraction. We try to extract features that can efficiently classify user identities with segmented PPG measurements. Previous work provides fiducial features for PPG-based authentication, which are critical landmarks in PPG pulse waveform [3]. However, our work is based on gesture-related PPG measurements, and previous features are not applicable. In G-PPG, we propose a set of customized features related to user wearing habits and physiological characteristics. In addition, we also select general signal features in time, frequency, and time-frequency domains as a supplementary.

Training Module. The training module is operated in the enrollment phase, the initialization process of G-PPG. With several labeled legitimate user training samples and pre-stored negative samples, we train a binary classifier for G-PPG. In the design of G-PPG, we compare the performance of 5 classifiers, which include Random Forest (RF), Support Vector Machine
(SVM), Decision Tree (DT), Gradient Boosting (GB), and K-Nearest Neighbor (K-NN). With careful consideration of the complexity and accuracy, we select a random forest in G-PPG. In addition, the classifier is continuously updated with labeled samples in the authentication module.

**Authentication Module.** This module utilizes the trained classifier to authenticate user’s identity. Attackers that cannot pass the G-PPG will be denied for further services. Moreover, the labeled samples will be pushed to the training module for adaptive updates to the classifier.

**C. Challenges**

To achieve an accurate authentication performance, G-PPG faces the following challenges.

**Re-using PPG sensors for gesture-related authentication.** PPG sensors are designed to sense the pulse rate. Specifically, PPG sensors emit red or green light, and the blood will absorb the light. By measuring the reflected light changes, PPG can evaluate the user’s pulse conditions. In G-PPG, we re-use the PPG sensor to indirectly sense the gesture movement, which is out of the scope of the PPG applications.

**Accurate authentication with low-cost sensors.** PPG sensors in wearable devices are typical low-cost commodity modules with a low sampling rate and resolutions, which makes accurate authentication difficult.

**Customized features for authentication.** G-PPG authenticates users with gesture-PPG, and universal pulse characteristics are not applicable. Selecting efficient features that imply the user’s gesture characteristics should be carefully studied.

**Limited training data size for better user experience.** While providing more gesture choices for authentication, the overhead of the enrollment phase may reduce user experience. Therefore, to have a better user experience, the training data size should be reduced to a certain level.

**IV. G-PPG SYSTEM DESIGN**

In this section, we describe the four modules in G-PPG in detail, which include data acquisition and preprocess module, feature extraction module, training module and authentication module.

**A. Data Acquisition and Preprocessing**

1) **Noise Reduction and Filtering:** PPG sensors measure pulses continuously, and we try to extract gestures from PPG measurements. Besides, due to the low accuracy of the PPG sensor, the data collected by the PPG sensor may include power drift and measurement noises. Considering that the frequency of heartbeats is usually less than 3Hz, we utilized a low-pass filter (LPF) to reduce signal noises with a cut-off frequency of 20Hz, which can not only retain heart rate information and gesture information but also remove high-frequency noises.

2) **Gesture Detection and Segmentation:** As shown in Fig. 1(d), a series of PPG readings typically contains multiple heartbeats, motion noises, and “gesture” signals. In order to extract gesture-related PPG signals for user authentication, we need to determine the starting point and the segment length.

**Segment Length:** Our preliminary study of the duration of gestures of 15 participants finds that the duration of a gesture is typically between 0.7s and 1s. Therefore, we empirically set the length of the segment to 1 second to ensure that all gesture-related data can be completely extracted. With a sampling rate of 100Hz, we have the number of sampling points in a segment τ as 100 in a gesture-related PPG signal.

**Starting Point:** From the PPG data we collected in Fig. 1(d), we find that gesture-related PPG signals typically show a pronounced fluctuation when compared with heartbeats and noises. With the above observation, we can utilize the energy accumulation to detect the starting point of a segment.

Considering a discrete-time series of PPG readings \( x(t) \) with \( T \) samples containing multiple gestures, we need to extract each gesture. We first calculate the energy accumulation \( E_t \) that starts at \( x(t) \) with a sliding window with the length of \( \tau \):

\[
E_t = \sum_{t}^{t+\tau-1} |x(t) - \bar{X}|
\]  

(1)

Here, \( \bar{X} \) is the average strength of the PPG signal that is measured in a static state (with only heartbeat and noises), which can be regarded as the noise floor of the gesture extraction. The first starting point detection problem can be formulated as the following function:

\[
\arg\min_{g_1} E_{g_1} > \theta E_{\text{max}}
\]  

(2)

\( E_{\text{max}} \) is the maximum energy accumulation segment in the entire data set, and \( \theta \) is a tolerance coefficient that shows deviation among gestures. Empirically, we select \( \theta \) as 0.8. Considering there could be multiple gestures, we repeat Eq. 2 within the new data set \( [x(g_1 + \tau), x(T)] \) to find the second starting point, and so on.
B. Feature Extraction

In G-PPG, we authenticate users with gesture-related PPG signals, which means traditional PPG features are not applicable [3], [4]. We design a specific feature set and a general feature set for further authentication to better extract features with user gesture habits and wearing habits.

1) Specific Feature Set: Our observations of 15 participants’ different gesture-related PPG signals demonstrate that over 80% of the gesture segment contains at least one pair of peak and trough. To make G-PPG applicable for all gestures and users, we elaborate design 6 features extracted from a single pair of peak and trough and 2 global features related to the overall shape of the signals. Fig. 3 illustrates how the first 6 gesture-specific features are derived from the critical landmarks in the PPG pulse waveform. It is worth mentioning that all features are strongly related to users’ wearing habits and gesture habits.

Taking the systolic amplitude \( h \) as an example, we define the \( h \) as the distance between the peak and the trough, related to the user wearing the wearable device’s habit. Specifically, if the user wears the device tightly, the variable space between the PPG sensor and the skin will be limited, which means lower amplitudes of both the peak and the trough. Another feature, crest width \( m \), reveals the speed of the user to release the gesture, while the trough width \( n \) represents the duration of the gesture retraction. The descriptions of 8 specific features and their physiological meanings are summarized in Tab. I.

2) General Feature Set: We also extract a set of general features from the gesture-related PPG signals in three domains: time domain, frequency domain, and time-frequency domain. In the time domain, we consider the mean value, standard deviation, average deviation, skewness, etc. features, widely used for data feature extraction. We perform Fast Fourier Transform and extract 6 frequency-domain features, and we perform Discrete Wavelet Transform with Harr wavelet to obtain the other 6 features in the time-frequency domain. We also summarize the general feature set in Tab. II as reference.

C. Training Phase

Given a sample \( \langle F(s)_i, F(g)_i, Z_i \rangle \), we have \( F(s)_i, F(g)_i \) that represents gesture-related specific features and general features, and \( Z_i \) indicates identity label (i.e. \( z_i = 1 \) means \( F(s)_i, F(g)_i \) is a legitimate user, \( z_i = 0 \) means \( F(s)_i, F(g)_i \) corresponds to an attacker).

We evaluate the performance of five binary classifiers (RF, SVM, DT, GB, and K-NN) to find which can provide a better authentication accuracy in G-PPG. As a result, we select the random forest (RF) classifier that performs the best with joint consideration of the accuracy and F1-score. The details will be discussed in Sec. V.

D. Authentication Mechanism

In the authentication stage, G-PPG randomly selects one gesture for the user and requires him/ her to follow the gesture. We extract the gesture feature set \( \langle F(s)_i, F(g)_i \rangle \) from the segmented PPG measurements and utilize the pre-trained classifier to validate the user’s identity. If the sample can pass the classifier, G-PPG authenticates the sample as a legitimate user. Otherwise, G-PPG determines the sample as a stranger and denies further processes.

Adaptive Update: Due to the repeated wearing on-off, we find the user’s wearing habits and gesture habits may change slightly over some time, and the corresponding gesture features may also change. Therefore, G-PPG collects the user-authenticated gesture segments and retrains the classifier regularly. Specifically, G-PPG periodically adds users’ latest PPG gesture feature sets and removes old gesture feature sets.
to keep the classifier up to date. The long-term performance of G-PPG will also be evaluated in Sec. V.

V. PERFORMANCE EVALUATION

A. Experiment Settings

1) Hardware design: We find commercial devices usually do not provide access permissions to the raw PPG data, and only processed heart-beat results can be acquired. Based on this, we build a data collection prototype with an off-the-shelf PPG module and connect it to an Arduino UNO (REV3) board. It is worth mentioning that the motion sensor (MPU-6050) that was utilized for the feasibility study is also connected to the UNO board. To imitate the wearing process of a wearable device, we fix the PPG sensor to a wristband and let users wear it as a wearable device. Fig 4 shows the prototype and settings of the experiments. Considering the sampling rate of commercial sensor modules can reach up to at least 100 Hz, we set the sampling rate of PPG sensor as 100 Hz in experiments.

2) Data Collection: We recruit 15 participants (11 males and 4 females) to collect gesture data with PPG sensor using our wearable prototype. For each participant, we collect 5 gestures that are shown in Fig. 2. Each gesture we collect 40 samples. For long-term evaluation, we keep tracking 6 participants (5 males and 1 female) in one week to evaluate the performance of G-PPG in long-term authentication. Specifically, we collect data from each participant 4 times a day, and participants should take off the device after each sampling round. Each gesture we collect 40 samples.

B. Metrics

We evaluate the performance of G-PPG with the following metrics:

- Accuracy: Accuracy is the ratio of correctly labeled samples (users and attackers) to the number of samples for test.
- Precision: Precision is the ratio of correctly labeled positive samples to the total predicted positive samples.
- Recall: Recall is the ratio of correctly predicted positive samples to the number of actual positive samples.
- F1-score: F1-score is the harmonic average of the precision and recall, which can be represented as: $F1 = \frac{2 \times \text{precision} \times \text{recall}}{\text{precision} + \text{recall}}$. F1-score can reveal the system’s overall performance, even with unbalanced sample distribution cases.

C. Overall Performances

We first evaluate the overall performance of G-PPG by checking the authentication accuracy. Specifically, we collect samples from 15 participants with 5 gestures. In particular, we set that each participant acts as a legal user once, while the rest 14 participants act as attackers. To guarantee the balance of the test samples, we randomly select 2 samples from each participant (attacker) as negative samples for each gesture. Fig. 5(a) shows that each participant can achieve an accuracy that is higher than 90% (only one participant has an accuracy of 89%), and males and females reveal similar results.

Secondly, we also evaluate the authentication accuracy of each gesture, and Fig. 5(b) reveals the average results of 15 participants. Considering G-PPG will randomly require users to perform a designated gesture in practice scenarios, we only use the same type of gestures from attackers as negative samples in test samples. As shown in Fig. 5(b), the accuracy of five gestures can exceed 90%, while F1-score exceeds 88%. All 5 gestures show good performance on authentication, and we also notice Gesture 3 may show a slightly lower accuracy when compared with the rest 4 gestures. In G-PPG, we can turn down the probability of Gesture 3 in real cases.

The above two experiments demonstrate G-PPG as a promising authentication mechanism practical with a single wrist-PPG sensor. In the following, we conduct several experiments to further evaluate the micro-benchmark in G-PPG.

D. The Impact of Classifiers

We compare the performance of G-PPG with different classifiers, which include decision tree (DT), gradient boost (GB), K-nearest neighbor (K-NN), random forest (RF), and support vector machine (SVM). These 5 models are widely used in binary classification problems, and we show the average accuracy and F1-score of each gesture and participant in Fig. 6. We find that RF reveals the best performance in both accuracy and F1-score compared with other classifiers. RF is adopted in G-PPG as the default classifier for further analysis in the following.

E. Impact of Feature Selection

We elaborately design a specific feature set to extract the gesture-related characteristic for authentication, and we evaluate the impact of feature selection by utilizing different feature
sets for authentication. Fig. 7 reveals the accuracy (Fig. 7(a)) and F1-score (Fig. 7(b)) of 5 gestures with the following three feature sets: 1) only use the specific feature set with 8 features, 2) only use the general feature set with 20 features, and 3) use all 28 features. Results demonstrate that utilizing all features shows the best authentication performance while using only 8 specific features reveals a remarkable performance. It is worth mentioning that the specific feature set overcomes the general feature set with only 8 features. Therefore, we consider the specific feature set can well extract the key characteristics from samples and make contributions to the classification results.

**F. Impact of Training Data Size**

The training data size reflects the user experience to some extent. Specifically, more training data means the user should spend more time on the system initialization, which may discourage users willing to use G-PPG. On the other hand, the accuracy may not be high enough for authentication with a few training samples. We take $K$ samples from legitimate users and train the model with an additional $2K$ negative samples in the experiment. The negative samples can be pre-stored in the system. We analyze the accuracy and F1-score for the different number of positive training samples ($K = 4, 8, 12, 16, 20, 24, 28, 32$), and the results are shown in Fig. 8. We find that even with 4 positive samples, G-PPG can reach an accuracy of 87.75%, and with 8 samples, the accuracy can reach up to 90.23%. Recall that each sample lasts for 1 second, G-PPG needs 8 s to train a gesture. Though one gesture can also be utilized for authentication, we still suggest users train at least 2 gestures for authentication, which lasts 16 s for the initialization phase. Considering the training phase of a user-fingerprint authentication may last for 30 s and Trueheart [3] requires a 2-minute-training to reach a 90% accuracy, we consider the time duration of the training phase in G-PPG is acceptable.

**G. Practical Analysis**

To further analyze the performance of G-PPG in practice, we evaluate the long-term performance of G-PPG and estimate the impact on the user’s daily activities. The user-defined security level proposed in the authentication mechanism is also evaluated.

**Long-term Authentication:** One may argue that the gesture-related PPG samples may change when the user takes on/off the wearable devices. Therefore, we keep tracking the gesture data of 6 participants (5 males and 1 female) for a week and analyze the performance of G-PPG each day. Participants will take off the wearable device after each sampling round to simulate the user’s daily usage habits. It is worth mentioning that we utilize the adaptive update mechanism after each authentication round, and the model is updated each day. The results in Fig. 9 demonstrate that the accuracy and F1-score are relatively stable, and the indicators (accuracy and F1-score) even increase a little bit after a few days with the adaptive update mechanism, which reveals a promising characteristic for long-term authentication.

**The Impact of Daily Activities:** We also study the impact of daily activities on G-PPG to validate the system robustness. In most wearable-based authentication methods [3]–[5], [25], [26], users are required to perform the authentication in a relatively stationary case, however, the moving scenario should also be considered in the daily life. We collect samples from 6
participants in two typical activities: sitting and walking, representing static and moving scenarios accordingly. As shown in Fig. 10, G-PPG demonstrates a similar precision in both cases, while the F1-score reaches up to 84.77% even in the walking scenario. We also notice the recall in the walking case is lower than the sitting case. In such cases, users can still pass the authentication by launching a second attempt.

VI. CONCLUSION

In this paper, we design G-PPG, a gesture-related PPG-based two-factor authentication mechanism for wearable devices. With an embedded PPG sensor, G-PPG can authenticate the user’s identity through dedicated gestures, which is based on the observation that gesture-related PPG readings can imply users’ heartbeat, wearing habits, and behavior habits. Specifically, we design a gesture detection and segmentation algorithm to extract gesture-related PPG measurements, and a specific feature set is proposed according to the empirical observations. We validate the performance and security of G-PPG among 15 participants, and the results demonstrate that G-PPG can achieve high accuracy of over 90% in long-term evaluations.

ACKNOWLEDGMENT

This work was supported in part by the following foundations: National Natural Science Foundation of China under Grant No. 62002183, and in part by Zhejiang Provincial Natural Science Foundation of China under Grant LQ20F020012, in part by the Natural Science Foundation of Ningbo under Grant 202003N4087. The Natural Science Foundation of Ningbo City under Grant No. 2021J090 and Ningbo Municipal Commonweal S&T Project under Grant No. 2022S005.

REFERENCES