Poster: Your Heart Won't Lie: PPG-based Continuous Authentication on Wrist-worn Wearable Devices

Tianming Zhao*, Yan Wang*, Jian Liu†, Yingying Chen†
*SUNY at Binghamton University, Binghamton, NY 13902, USA
†Rutgers University, North Brunswick, NJ 08902, USA
{tzhao7,yanwang}@binghamton.edu,jianliu@winlab.rutgers.edu,yingying.chen@rutgers.edu

ABSTRACT

This paper presents a photoplethysmography (PPG)-based continuous user authentication (CA) system, which especially leverages the PPG sensors in wrist-worn wearable devices to identify users. We explore the uniqueness of the human cardiac system captured by the PPG sensing technology. Existing CA systems require either the dedicated sensing hardware or specific gestures, whereas our system does not require any users' interactions but only the wearable device, which has already been pervasively equipped with PPG sensors. Notably, we design a robust motion artifacts (MA) removal method to mitigate the impact of MA from wrist movements. Additionally, we explore the characteristic fiducial features from PPG measurements to efficiently distinguish the human cardiac system. Furthermore, we develop a cardiac-based classifier for user identification using the Gradient Boosting Tree (GBT). Experiments with the prototype of the wrist-worn PPG sensing platform and 10 participants in different scenarios demonstrate that our system can effectively remove MA and achieve a high average authentication success rate over 90%.

CCS CONCEPTS

• **Security and privacy** → **Biometrics**; **Multi-factor authentication**; • **Human-centered computing** → *Ubiquitous and mobile computing design and evaluation methods*;

KEYWORDS

Photoplethysmography (PPG); Continuous Authentication; Wearable Devices

MobiCom '18, October 29-November 2, 2018, New Delhi, India

ACM ISBN 978-1-4503-5903-0/18/10.
https://doi.org/10.1145/3241539.3267748

ACM Reference Format:
Tianming Zhao*, Yan Wang*, Jian Liu†, Yingying Chen†. 2018. Poster: Your Heart Won't Lie: PPG-based Continuous Authentication on Wrist-worn Wearable Devices. In *The 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18), October 29-November 2, 2018, New Delhi, India.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3241539.3267748

1 INTRODUCTION

The population of wrist-worn wearable devices has increased significantly since 2015 and is predicted to reach over 100 million in 2019. With the emerging use of the AI-enabled wearable devices, the user's privacy is becoming a significant concern as the wearable devices have the access to the user's most personal information. Traditional user authentication methods used by the wearable systems, such as passwords and graphic patterns, can only verify the user's identity at the time performing the authentication and are vulnerable to various knowledge-based attacks (e.g., shoulder attack [2] and smudge attack). Therefore, there is an essential demand to enable continuous authentication (CA) on wearable devices to automatically protect users' privacy.

We argue that a robust and efficient CA system should be able to automatically recognize the user's identity without the user's intervention in terms of the user's conscious involvement. To enable CA in wearable devices, existing approaches either use the user's unique behavioral pattern or biometrics to automatically determine the user's identity. For example, ZEBRA [3] leverages the motion sensors in the activity tracker on the user's wrist to perform CA automatically. However, it requires the user to perform certain gestures, which is inconvenient and difficult to control. Kang et al. [1] utilizes the ECG-based biometrics for CA. However, the user's ECG signals are only available in dedicated sensing devices, which are incompatible with most commodity wearable devices.

In this work, we devise an on-wrist CA system that leverages the unique biometric in the user's cardiac system to verify the user's identity automatically. Different from existing approaches, our system utilizes the photoplethysmography (PPG) sensors readily available in wearable devices to capture the user's cardiac features and perform CA. Since

most commodity wrist-worn wearable devices (e.g., smartwatches and activity trackers) have already equipped with the PPG sensors, our system can be easily deployed to the existing wearable devices without any hardware modification. To the best of our knowledge, we are the first to design and develop the CA system based on the PPG sensors in wrist-worn wearable devices. The insights are that 1) the coarse-grained pulsatile signals captured by the commodity PPG sensors in wrist-worn wearable devices can provide unique cardiac features, which are good for differentiating different people; 2) the motion artifacts resulted from human body movements can be effectively reduced by the motion artifact removal module, which improves the performance of our system significantly. The main contribution of our work are summarized as follows:

- We propose the first CA system that can identify the user by using the unique biometric information extracted from the PPG sensors in wrist-worn wearable devices regardless of motion artifacts. The proposed CA system can be easily deployed in any PPG-enabled wearable devices (e.g., smartwatches and activity trackers) without hardware modification.
- We develop a robust motion artifacts (MA) removal method that detects MA with various intensities and effectively improves the performance of the PPG-based CA system by eliminating the interference from the MA.
- We explore the fiducial features that can capture the uniqueness in the user's cardiac system and develop a gradient boosting tree (GBT)-based classifier to accurately authenticate the user.
- We build a prototype of our CA system using the commodity PPG sensors. Experimental results with 10 participants and our prototype demonstrate that our system can achieve a high CA accuracy over 91% and our MA removal method can improve the accuracy significantly.

2 APPROACH OVERVIEW

2.1 Attack Model

Because PPG sensors require the direct contact of the user's skin to measure the blood flow, such close-proximity nature makes the adversary very hard to obtain the user's PPG measurements and launch knowledge-based attacks (e.g., the replay attack and synthesis attack). In this work, we assume the adversary cannot compromise the user's wearable device. Therefore, the adversary can only launch the *Random Attack*, where the adversary may wear the user's wearable device and expect the PPG measurements on the adversary's wrist can pass the PPG-based user identification system.

2.2 System Overview

The architecture of our PPG-based user authentication system is shown in Figure 1. The system collects PPG measurements from the user's wearable device continuously. Due to

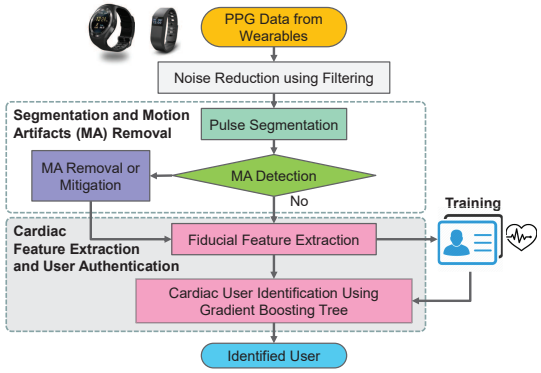
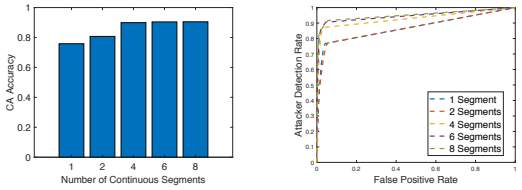


Figure 1: Architecture of the PPG-based user authentication system.

hardware imperfection and motion artifacts, the raw PPG measurements inevitably contain high-frequency interference and baseline drift. Therefore, our system first performs the *Noise Reduction using Filtering* to reduce such noise. Since the frequency of the pulsatile component in PPG measurements is between $0.5Hz$ and $4Hz$, we adopt a band-pass filter to reduce the noises. Additionally, the PPG measurements are processed by a center median filter, followed by a center moving-average filter with the same window size, to further smooth the PPG patterns. (The median filter may introduce edge jitters, and the moving-average filter reduces such edge jitters and enhances the smoothness of the waveform.) After filtering, the system conducts the *Pulse Segmentation* to determine the segment of PPG measurements that contain a complete cardiac cycle. The insight is that each cardiac cycle should include the *systolic peak* and the *dicrotic notch*, which could be identified in the PPG measurement with the consideration of the typical duration of the diastole and systole phases.

A significant component in our system is the *Motion Artifacts (MA) Removal*. In PPG measurements, motion artifacts (MA) are mainly caused by the tissue deformations and instantaneous local blood flow changes in the wrist area. While the pulsatile signals are repetitive waveforms in PPG measurements, most MA are burst signal. The system utilizes the statistical differences (e.g., kurtosis, skewness and standard deviation) in the PPG measurements to perform the *MA Detection*. If the system detects MA, depending on whether MA dominate the PPG segment or not, our system either removes the MA-related measurements from the segment or reduce MA by using a special moving average filter, which averages each MA segment with several pure-pulse PPG segments.

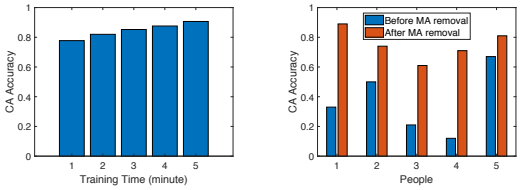
The fiducial features are considered the indicators for cardiovascular variables and the general status of the human heart, which could be the most common PPG indexes in the clinical assessment. After the MA Removal, our system performs the *Fiducial Feature Extraction* to extract the unique



(a) CA accuracy with different continuous segments

(b) ROC curves with different continuous segments

Figure 2: Performance of different number of continuous segments under 1 legitimate user and 9 attacker.



(a)Performance with different training size

(b)Performance with MA removal

Figure 3: Performance with MA removal.

cardiac features from the PPG segment and its second derivative. In total, we derive 29 fiducial features (e.g., systolic peak x, systolic peak time/crest time $t1$, dicrotic notch z) for each PPG segment. The extracted features are used to build the user's profile and train a binary classifier using the Gradient Boosting Tree (GBT) when the user enrolls the system. In the *Cardiac User Identification using Gradient Boosting* process, the extracted features of the incoming PPG segment are taken as the input to the GBT classifier to verify the user's identity.

3 PERFORMANCE EVALUATION

3.1 Experimental Methodology

We find that current operating systems of commodity wearable devices (e.g., Android and iOS) do not provide PPG raw readings. Therefore, we design a wrist-worn prototype, which mimics the layout of PPG sensors in commodity wearables, to demonstrate the feasibility of our system. Our prototype consists of two commodity green LED PPG sensors connected to an Arduino UNO (REV3) board, which continuously collects PPG raw readings at 300Hz and save them to a laptop (i.e., Dell Latitude E6430) to perform the proposed CA implemented in MATLAB.

We recruit 10 participants (i.e., 8 male and 2 female students) whose age are between 20 to 30 to collect PPG measurements under two different scenarios (i.e., *Static Scenario* and *Moving Scenario*) in a three-day time span. For each day, in the static scenario, the 10 participants are asked to sit for 10 mins, respectively. While in the moving scenario, five of the 10 participants are asked to pick up a cup and drink water repeatedly for 2 mins and sit still for 3 mins, respectively. In total, we collect 8000 PPG segments in the static scenario and 700 PPG segments in the moving scenario, respectively.

3.2 Performance of CA System

We first evaluate the performance of our PPG-based CA system by showing the CA accuracy. Figure 2(a) depicts the CA accuracy of our system in the static scenario when different numbers of PPG segments are available for testing. It is obvious that the performance of our system becomes stable at about 90% CA accuracy when four or more PPG segments (i.e., around 3 seconds) are used for CA. To study the performance of our PPG-based CA system when defending against the random attack, we derive the receiver operating characteristic (ROC) curves of using different numbers of PPG segments for testing as shown in Figure 2(b). We can see that our attacker detection rate reaches to over 87% with the false positive rate of around 3.5% when the system takes four PPG segments for testing. Our system can achieve over 90% detection rate and less than 4.5% false positive rate when six or more PPG segments are available. This indicates that our CA system can effectively identify the users and attackers with the good user experience.

We then evaluate the impact of the training data size. Figure 3(a) shows that our system can achieve around 90% CA accuracy among 10 participants with only five-minute training data, which is very practical in our daily use of the wrist-worn wearable devices. In addition, Figure 3(b) shows that the CA accuracy of our system reaches to around 76% after using the MA removal on the data collected from four participants in the moving scenario. Compared to the CA accuracy before using the MA removal, which is around 30%, the results indicate that our MA removal module can effectively mitigate the impacts of MAs and significantly improve the accuracy of our CA system. We notice that the PPG signals may drift from time to time even if they are from the same person [4]. We plan to develop an adaptive training approach to deal with the drift in our future work.

ACKNOWLEDGMENTS

This work was partially supported by the National Science Foundation Grants CNS-1566455, CNS-1814590, CNS-1820624, CNS-1826647 and ARO Grant W911NF-18-1-0221.

REFERENCES

[1] Shin Jae Kang, Seung Yong Lee, Hyo Il Cho, and Hyunggon Park. 2016. Ecg authentication system design based on signal analysis in mobile and wearable devices. *IEEE Signal Processing Letters* 23, 6 (2016), 805–808.

[2] Federico Maggi, Simone Gasparini, and Giacomo Boracchi. 2011. A fast eavesdropping attack against touchscreens. In *Information assurance and security (IAS), 2011 7th international conference on*. IEEE, 320–325.

[3] Shrirang Mare, Andrés Molina Markham, Cory Cornelius, Ronald Peterson, and David Kotz. 2014. Zebra: Zero-effort bilateral recurring authentication. In *Security and Privacy (SP), 2014 IEEE Symposium on*. IEEE, 705–720.

[4] Jorge Sancho, Álvaro Alesanco, and José García. 2018. Biometric Authentication Using the PPG: A Long-Term Feasibility Study. *Sensors* 18, 5 (2018), 1525.