Demo: Toward Continuous User Authentication Using PPG in Commodity Wrist-worn Wearables

Tianming Zhao*, Yan Wang*, Jian Liu†, Yingying Chen†
*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

We present a photoplethysmography (PPG)-based continuous user authentication (CA) system leveraging the pervasively equipped PPG sensor in commodity wrist-worn wearables such as the smartwatch. Compared to existing approaches, our system does not require any users' interactions (e.g., performing specific gestures) and is applicable to practical scenarios where the user's daily activities cause motion artifacts (MA). Notably, we design a robust MA removal method to mitigate the impact of MA. Furthermore, we explore the uniqueness of the human cardiac system and extract the fiducial features in the PPG measurements to train the gradient boosting tree (GBT) classifier, which can effectively differentiate users continuously using low training effort. In particular, we build the prototype of our system using a commodity smartwatch and a WebSocket server running on a laptop for CA. In order to demonstrate the practical use of our system, we will demo our prototype under different scenarios (i.e., static and moving) to show it can effectively detect MA caused by daily activities and achieve a high authentication success rate.

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 '19, October 21–25, 2019, Los Cabos, Mexico

ACM ISBN 978-1-4503-6169-9/19/10.
https://doi.org/10.1145/3300061.3343375

ACM Reference Format:
Tianming Zhao, Yan Wang, Jian Liu, Yingying Chen. 2019. Demo: Toward Continuous User Authentication Using PPG in Commodity Wrist-worn Wearables. In *The 25th Annual International Conference on Mobile Computing and Networking (MobiCom '19), October 21–25, 2019, Los Cabos, Mexico.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3300061.3343375

1 INTRODUCTION

The significant advances in sensing and networking technology have boosted the development of wearable devices in the last decade. The wearable devices have been pervasively used since 2015, and its population is predicted to reach over 100 million by 2019. Considering the emerging use of artificial intelligence (AI) in the future, the user's account security and privacy are becoming significant concerns as the wearable devices have access to the user's most personal information. Traditional user authentication methods used by the wearable systems, such as passwords and graphic patterns, are vulnerable to various knowledge-based attacks (e.g., shoulder attack and smudge attack). More important, these one-time approaches only provide momentary identity verification, hence the user will have to re-pass the authentication system whenever the authentication is requested. Therefore, there is an essential need for a robust and convenient continuous user authentication (CA) solution for wearable devices.

Existing CA approaches usually focus on reducing or eliminating user involvement in the authentication process by leveraging the user's unique behavioral or physiological patterns. For example, ZEBRA [1] leverages the motion sensors in the activity tracker on the user's wrist to perform CA automatically. However, it requires the user to perform the particular activities (i.e., certain gestures), which is inconvenient and difficult to control. In addition, physiological patterns (i.e., heartbeat and breathing patterns) have been successfully used in CA systems. Recently, advanced sensing technology enables unobtrusive continuous user authentication based on the unique cardiac biometrics captured by the electrocardiogram (ECG) sensor [2]. However, all these systems require dedicated sensors, which are not readily available in commodity wearable devices.

In this work, we leverage the photoplethysmography (PPG) sensing technology that is pervasively enabled by the wrist-worn wearable devices (e.g., smartwatches and fitness trackers) to develop a CA system based on the uniqueness of human cardiac systems reflected by PPG signals. The advantage of using PPG for CA is obvious as the pulsatile signal always exists and does not require users' participation. Using the PPG signals from wearable devices to perform CA is a challenging task. First, PPG is a relatively coarse-grained sensing modality more susceptible to noise and interference especially when the measurements are from the wrist area. So, whether the PPG measurements from wrist-worn wearable devices are unique enough to identify users is unknown. Second, wrist-worn wearable devices usually involve in a lot of daily activities, which result in various motion artifacts (MAs) that could impact the quality of the PPG measurements significantly. To address these challenges, we extensively study the impact of different body movements and develop effective MA detection and mitigation/removal mechanisms that allow our CA system to perform CA accurately in daily lives. We summarize the major contributions of our work 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 practical prototype of our system using the commodity smartwatch and the WebSocket server implemented by JavaScript running on a laptop for better demonstration of our CA system under different scenarios.

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). Although the adversary may obtain the user's blood flow patterns through vision-based technology, there is no way to reproduce the PPG measurements that are similar to the users. 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.

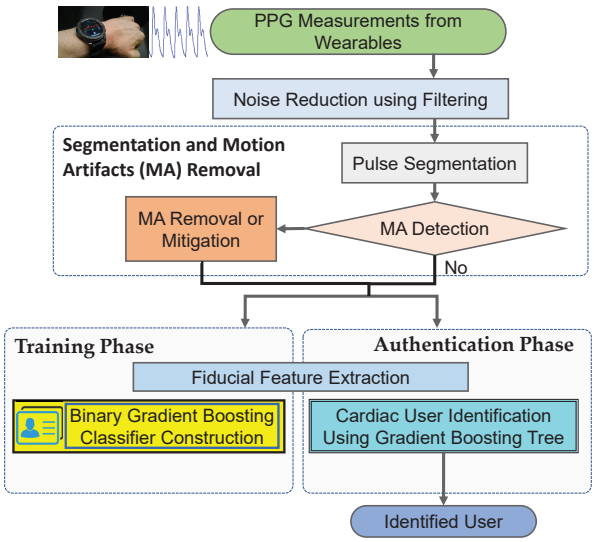

Figure 1: Architecture of the PPG-based user authentication system.

2.2 System Overview

The architecture of our PPG-based user authentication system is shown in Figure 1. The system continuously collects PPG measurements from the user's smartwatch as the input. Due to hardware imperfection and MA, the raw PPG measurements inevitably contain baseline drift and high-frequency interference. Therefore, our system first performs the *Noise Reduction using Filtering* to reduce such noise. A band-pass filter is used to extract the pulsatile components in PPG measurements. After filtering, the system conducts the *Pulse Segmentation* to determine the PPG segment that is likely to contain a complete cardiac cycle. The insight is that each cardiac cycle should include the systolic peak (i.e., the repetitively highest 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.

Next, we particularly design the *Motion Artifacts (MA) Removal* to mitigate the MA caused by daily activities. In PPG measurements, MA is 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) between the pulse waveform and MA signals to determine whether the PPG segment contains

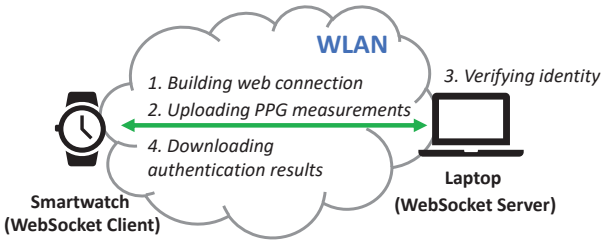

Figure 2: Demo setup.

a pulse or MA in the *MA Detection*. When MA is detected in multiple consecutive PPG segments, our system performs the MA Removal to eliminate the impacted PPG segments. Whereas if MA is detected in only a few consecutive PPG segments or scattered segments, our system performs the MA Mitigation to reconstruct the pulse waveform using a special moving average filter, which averages each MA segment with several pure-pulse PPG segments. After the *Motion Artifacts (MA) Removal*, our system will be separated into two phases: *Training Phase* and *Authentication Phase*.

In the *Training Phase*, our system extracts the unique cardiac features from the PPG segment using *Fiducial Feature Extraction*. Then in *Binary Gradient Boosting Classifier Construction*, the extracted features are used to train a binary classifier using the Gradient Boosting Tree (GBT) when the user enrolls the system. Finally, in the *Authentication Phase*, our system performs *Cardiac User Identification Using Gradient Boosting Tree* process where the extracted features of the incoming PPG segments are taken as the input to the GBT classifier to perform user authentication.

Implementation. We have implemented our CA system as shown in Figure 2, which is composed of a smartwatch for collecting the real-time PPG measurements, a laptop running the WebSocket server to receive the data and perform continuous authentication, and a WLAN enabling the communication between the smartwatch and the laptop via a WiFi access point. Before our CA system begins, the smartwatch and the laptop need to connect to the WLAN. Then our developed web application as the WebSocket client running on the smartwatch can initiate the connection to the WebSocket server running on the laptop. Once the connection is built, the smartwatch will transfer the real-time PPG measurements to the connected laptop via WLAN. Simultaneously, the laptop will process the incoming real-time PPG measurements and perform our CA system which is implemented using Matlab. As the CA goes, the CA results will be sent back to the smartwatch. In the end, either side of the connection (i.e., client or server) could terminate the connection when there's no need for CA. In particular, we do the experiment using a Samsung Gear S3 classic smartwatch with Tizen OS 4.0 which is equipped with two PPG sensors having a sampling rate of 20 Hz. The laptop is with Intel(R) Core(TM) i7-8550U @ 1.80 GHz CPU and 16 GB of RAM. For the evaluation, please refer to our poster [3] for details.

3 DEMONSTRATION

In this section, we summarize the detailed plan that we will conduct during the demo and provide the observation that the attendee will have. Then we list the facilities needed for our on-site demo.

3.1 Demo Plan

The demo will showcase our system under two different scenarios (i.e., static scenario and moving scenario) which cover various practical application scenarios.

Static Scenario. In the static scenario, we will wear the smartwatch and sit quietly for several mins which matches the major practical use case of continuous authentication. The attendee will observe the user's real-time PPG measurements from the screen of our laptop and the continuous authentication results of our system.

Moving Scenario. In the moving scenario, we will occasionally perform some daily actives (e.g., moving the forearms and grabbing up a cup) while we are sitting quietly which mimics the practical working office scenario. The attendee will observe how different kinds of gestures would impact the PPG measurements in terms of the motion artifacts. Moreover, they will also observe the performance of our *MA Detection* approach and the continuous authentication results while the gestures are being performed.

3.2 Facilities for the Demo

The facilities that are required by our demo include: (1) a table as mentioned in the default setup to deploy the equipment. (2) a chair for us to sit required by the demo scenarios as explained in the *Demo Plan*. (3) three power outlets for the laptop, the WiFi access point, and the smartwatch respectively. We do not need the special environments and tools, Internet access, physical space requirements. The estimated setup time required by our demo is about 15 minutes.

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] 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.

[2] João Ribeiro Pinto, Jaime S Cardoso, André Lourenço, and Carlos Carreiras. 2017. Towards a Continuous Biometric System Based on ECG Signals Acquired on the Steering Wheel. *Sensors* 17, 10 (2017), 2228.

[3] Tianming Zhao, Yan Wang, Jian Liu, and Yingying Chen. 2018. Your Heart Won't Lie: PPG-based Continuous Authentication on Wrist-worn Wearable Devices. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. ACM, 783–785.