Unlock with Your Heart: Heartbeat-based Authentication on Commercial Mobile Phones

LEI WANG, State Key Laboratory for Novel Software Technology, Nanjing University, China
KANG HUANG, State Key Laboratory for Novel Software Technology, Nanjing University, China
KE SUN, State Key Laboratory for Novel Software Technology, Nanjing University, China
WEI WANG, State Key Laboratory for Novel Software Technology, Nanjing University, China
CHEN TIAN, State Key Laboratory for Novel Software Technology, Nanjing University, China
LEI XIE, State Key Laboratory for Novel Software Technology, Nanjing University, China
QING GU, State Key Laboratory for Novel Software Technology, Nanjing University, China

In this paper, we propose to use the vibration of the chest in response to the heartbeat as a biometric feature to authenticate the user on mobile devices. We use the built-in accelerometer to capture the heartbeat signals on commercial mobile phones. The user only needs to press the phone on his/her chest, and the system can identify the user within a few heartbeats. To reliably extract heartbeat features, we design a two-step alignment scheme that can handle the natural variability in human heart rates. We further use an adaptive template selection scheme to authenticate the user under different body postures and body states. Based on heartbeat signals collected on twenty users, the experimental results show that our method can achieve an authentication accuracy of 96.49% and the heartbeat features are stable over a period of three months.

CCS Concepts: • **Security and privacy → Biometrics**;

Additional Key Words and Phrases: Biometrics-based Authentication, Mobile System

ACM Reference Format:
Lei Wang, Kang Huang, Ke Sun, Wei Wang, Chen Tian, Lei Xie, and Qing Gu. 2018. Unlock with Your Heart: Heartbeat-based Authentication on Commercial Mobile Phones. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 3, Article 140 (September 2018), 22 pages. https://doi.org/10.1145/3264950

1 INTRODUCTION

Biometric features, including fingerprints and faces, have been used as metrics for user authentication on commercial mobile devices. Biometrics-based user authentication systems identify the user based on "who you are", instead of "what you know" (passwords) or "what you have" (tokens) [47]. Since users often forget to carry their physical tokens and passwords are susceptible to leakage [5, 54], biometrics-based authentication systems

Authors' addresses: Lei Wang, State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu, China, wangl@smail.nju.edu.cn; Kang Huang, State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu, China, hkwany520@gmail.com; Ke Sun, State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu, China, kesun@smail.nju.edu.cn; Wei Wang, State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu, China, ww@nju.edu.cn; Chen Tian, State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu, China, tianchen@nju.edu.cn; Lei Xie, State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu, China, lxie@nju.edu.cn; Qing Gu, State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu, China, guq@nju.edu.cn.

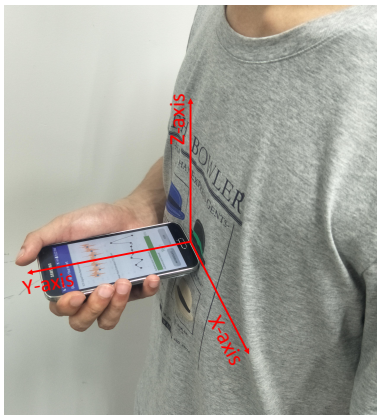
2474-9567/2018/9-ART140 $15.00
https://doi.org/10.1145/3264950

provide a convenient and secure way to unlock private mobile devices, *i.e.*, devices that often have a singular user, including smartphones and smartwatches. However, most biometric features, such as fingerprints, faces, and voices, are vulnerable to spoofing and replaying attacks [4, 13, 17, 43]. For example, with the widely available 3D-reconstruction and 3D-printing technologies, it is easy to bypass face recognition systems with 3D masks [17]. Therefore, we need to find a new biometric feature that is easily accessible on mobile devices and yet difficult to be reproduced by attackers.

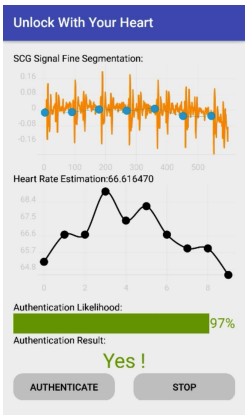
The vibration of the chest in response to the heartbeat, which is called seismocardiogram (SCG) [26], can be used as a biometric feature for user authentication. Firstly, the heartbeat pattern depends on the biological features and geometric structure of the heart, which is unique for each person. Secondly, SCG provides strong protection against spoofing attacks. To access the SCG, the adversaries have to attach a device to the chest of the user, which is considerably harder than taking photos of the user's face or recording the voices of the user. While there are contactless radar systems that can measure the heartbeat from a distance [39, 66], there is still no evidence that these signals are reliable enough for reconstructing the details of heartbeat dynamics. Furthermore, compared to replaying the heartbeat sound, it is harder for the adversaries to reproduce the small vibrations caused by heartbeats. Thirdly, the heartbeat pattern is closely linked to the "liveness" and the emotion of the user. By detecting the abnormality of the heartbeat pattern, the system can potentially reject the user when he/she is under threat. While SCG can serve as the biometric feature for user authentication, traditional SCG measurement schemes require specially designed devices and need to attach the device via chest bands [26]. This makes traditional SCG approaches not applicable to authentication on commercial mobile devices.

In this paper, we propose to use the built-in accelerometer to capture the heartbeat vibration and perform user authentication on commercial mobile devices. To unlock the device, the user only needs to press the device on his/her chest to collect heartbeat signals, and the system can identify the user within a few heartbeats, as shown in Figure 1(a). Our design is based on the observation that the detailed vibration patterns within one heartbeat cycle can serve as a unique identity for a person, and such patterns can be reliably captured by the accelerometers of commercial mobile phones. Using SCG collected from twenty volunteers, we find that different people have different heartbeat patterns even if their heart rates are similar. Moreover, these patterns are robust when the user slightly changes the position where the heartbeat is measured or the angle of the mobile phone. Therefore, this authentication scheme can be easily used in daily life. Heartbeat patterns can serve as the main authentication scheme for mobile devices, or as a supplementary authentication scheme in multi-factor authentication solutions. For example, a two-factor authentication system may ask the user to press the phone on his/her chest and put one finger on the fingerprint scanner at the same time. In this way, the system checks both the fingerprint and the heartbeat pattern to improve the security level of the authentication process.

When building heartbeat-based authentication system, we need to address the following technical challenges. First, human heartbeat patterns contain intrinsic Heart Rate Variability (HRV) [42]. Even for a healthy person, the standard deviation of the time between two normal heartbeats (SDNN) could be larger than one hundred milliseconds (one-tenth of the heartbeat cycle). This is because heartbeats are susceptible to variations in the inputs from the parasympathetic nervous system (PSNS) caused by multiple human factors, *e.g.*, respiration. The variability in heartbeat duration leads to challenges in dividing and aligning the heartbeat signals. To address this challenge, we propose a two-step segmentation and alignment scheme that can precisely align the key timing features of the heartbeat even if the durations of the heartbeats are slightly different. Second, extracting reliable features from heartbeat signals with different durations is challenging. On one hand, the heartbeat signals from different persons contain similar peak-and-valley sequences with slightly different amplitudes and time intervals. On the other hand, directly using the raw heartbeat signal and matching in the time domain often wrongly reject the authorized user due to the variation in the duration of a heartbeat cycle. To address this challenge, we propose to use wavelet transform to extract features from heartbeat signals. Our experimental results show that features extracted by wavelet transform outperform both the Dynamic Time Warping (DTW) and time domain matching



(a) Capturing the SCG signals using the mobile phone



(b) Interface of our Android APP

Fig. 1. Heartbeat-based authentication scenario

schemes. Third, human heartbeat patterns change under various conditions. For example, the heartbeat patterns captured after exercising are different to the pattern when the same user is in the resting state, even if these patterns are normalized in the time domain so that their heartbeat cycles are stretched to the same duration. To address this challenge, we propose a heartbeat pattern selection scheme that chooses the best heartbeat patterns for authentication based on the scenario information, which indicates the status of the user (*e.g.*, whether the user is in the exercising or the resting state) and the body posture (*e.g.*, whether the user is standing/sitting, lying down or leaning on the sofa).

We have implemented our heartbeat-based authentication scheme on the Android platform. We collected more than 110, 000 heartbeat samples from 35 volunteers. The implemented system achieves an Equal Error Rate (EER) of 3.51% for user authentication when using just five heartbeat cycles. Our experimental results also show that the system is robust against different ways of putting the mobile phone and different body postures.

In summary, we have made the following contributions in this paper:

- To our best knowledge, we are the first to perform heartbeat-based user authentication using the built-in accelerometer on commercial mobile phones.
- We propose a set of novel signal processing schemes designed for heartbeat-based user authentication, including template-based heartbeat alignment, wavelet-based feature extraction, and dynamic heartbeat pattern selection.
- We implement our authentication system on commercial smartphones and verify our design using heartbeat signals collected from twenty users.

2 RELATED WORK

Existing work on heartbeat measurement and authentication can be divided into three categories: special equipment based heartbeat measurement, commodity device based heartbeat measurement, and biometrics-based authentication.

Special Equipment based Heartbeat Measurement: Existing systems use specialized equipment to collect heartbeat signals, including electrocardiography (ECG), ballistocardiogram (BCG), seismocardiogram (SCG) and RF cardiac signals. ECG signal has been used for heart rate estimation [46, 58] and disease diagnosis [33, 37] for a long time. While ECG provides accurate heartbeat measurements, ECG systems have to attach electrodes

to the skin of the user, which is inconvenient for daily use. BCG measures the micro recoil movements of the body caused by the blood traveling along the vascular tree [8, 20, 41]. Such micro-movements can be captured by highly sensitive geophone mounted on the bed that the user is sleeping on [29, 30]. SCG measures the local vibration of the chest caused by the heartbeat and it has been used for heart rate estimation [9, 36, 52, 56]. SCG can also be used for assessments of the time interval of different mechanical events occurring during the systolic and diastolic phase [14–16]. However, most SCG systems require specifically designed chest belt to attach the sensor to the chest of the user [14]. Recently, RF-based systems provide a non-intrusive and contactless way for heartbeat measurement. Adib et al. [1] use Frequency Modulated Continuous Wave (FMCW) to monitor the heart rates with a median accuracy of 99%. Yang et al. [64] propose a system that uses 60GHz millimeter wave (mmWave) for heartbeat monitoring. However, most of these systems use expensive special hardware and only provide coarse heart rate estimations that are not applicable for user authentication.

Commodity Device based Heartbeat Measurement: Low-cost commodity devices, including Wi-Fi devices and smartphones, can also be used for heartbeat monitoring. With the Channel State Information (CSI) captured from commercial WI-Fi devices, it is possible to estimate the heart rate by either the amplitude of CSI [40] or the phase of CSI [63]. Furthermore, Zhao et al. [66] show that CSI provides enough details in heartbeat cycles so that it can be used for recognizing the emotional state of the user. Qian et al. [51] leverage inaudible acoustic signals emitted by commodity mobile phones to monitor the heart rates. However, these Wi-Fi and acoustic signal based measurements are sensitive to environmental changes, including the angle and the distance of the device to the target user.

There are systems that use the built-in accelerometers or gyroscopes in commodity mobile phone to capture the SCG signals [35, 44, 59]. Most of these systems only provide coarse measurements, such as heart rates or Heart Rate Variability (HRV) [35, 44]. In a recent system deployed on smartphones, Wang et al. [59] detect the detailed fiducial point of the SCG signals with the aid of photoplethysmogram (PPG) to measure the blood pressure of the user. In comparison, our system solely relies on the SCG signals captured by the built-in accelerometer to extract detailed heart movement pattern without help from other sensors.

Biometrics based Authentication: Biometrics-based authentication uses features, such as fingerprint [53, 55], face [18, 21], voice [7, 19, 31, 49], breath [11], iris [57], and heartbeat [12, 24], to authenticate the user. Among these features, the heartbeat pattern is a relatively new and hard-to-spoof biometric feature for authentication. Choudhary and Manikandan [12] propose a heartbeat extraction framework for authentication based on ECG signals. BreathLive [24] uses a heartbeat sound based authentication system, which relies on the inherent correlation between chest motion and sounds caused by deep respiration to protect the user from replay attacks. Auth'n'Scan [23] uses physiological information, including heart rates, HRV, and respiration rates, derived from PPG to authenticate the user. Cardiac Scan [39] uses a remote, high-resolution heartbeat monitoring system based on DC-coupled continuous-wave radar to achieve continuous user authentication. However, most of these heartbeat-based authentication systems use specially designed equipment and cannot be easily applied to current commodity mobile devices.

3 SYSTEM OVERVIEW

3.1 Authentication Model and System Components

Our heartbeat-based authentication system aims at identifying the owner of the mobile device. We assume that the mobile device only has one owner. However, our system can be extended to identify multiple users on the same device by updating our training and recognition process.

The first step of our system is the training process as shown in Figure 2. During the training process, the user needs to press the mobile device on his/her chest, more specifically, put the bottom of the phone perpendicularly on the lower portion of the sternum, to collect training heartbeat samples, as shown in Figure 1(a). The training

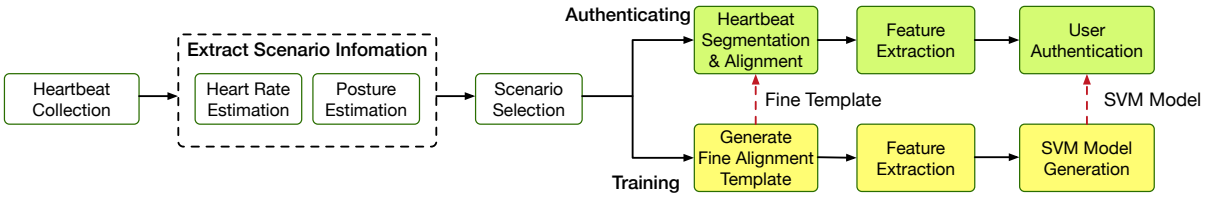


Fig. 2. Authentication System Components

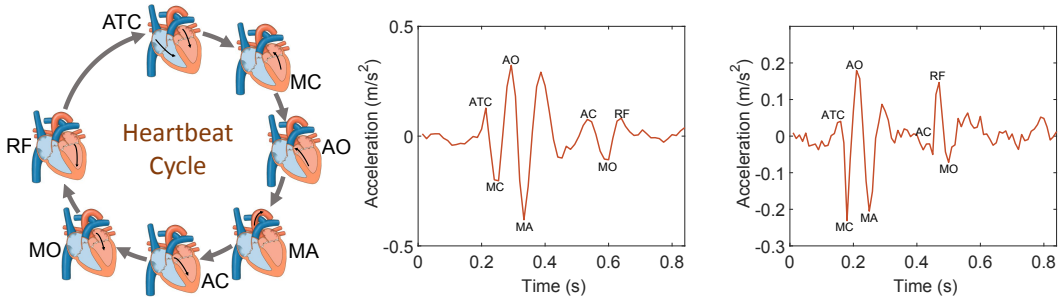
process normally takes less than two minutes (for collecting 60 heartbeats). Users may be instructed to change the position or the angle of the device during the training process to introduce more variations in the training samples. When collecting the training samples, our system records the built-in accelerometer readings at a sampling rate of 100~250 Hz (depending on the hardware support of the device). With the readings of the accelerometer, we first extract the heart rates and the body posture of the user. With this information, the collected training samples can be classified into one of the predefined scenarios, *e.g.*, the heart rates are in the range of 50 ~ 80 Beats per Minute (BPM) and the user is sitting on a chair. The training samples are then used for generating heartbeat patterns for that given scenario. Each heartbeat pattern includes one heartbeat template for signal alignment and one Support Vector Machine (SVM) model for identifying the owner of the device. The SVM model is a two-class classifier that is trained using the training heartbeats from the owner (as the positive samples) and the benchmark heartbeats from a global heartbeat database (as the negative samples). The SVM model can give the likelihood whether an unknown heartbeat signal belongs to the owner or not.

After the training process, our system uses the heartbeat patterns to perform user authentication. Similar to the training process, the authentication process first collects the heartbeat signals and then extracts the scenario information from the readings of the accelerometer. The scenario information is used for selecting one set of the heartbeat patterns, including both the template for signal alignment and the SVM model for authentication. If there is a matching heartbeat pattern in the database, the system first uses the template to segment the continuous SCG signals into individual heartbeat cycles and align the key features of each cycle. The system then extracts features using wavelet transform and applies the SVM model to classify the heartbeats. If there is no heartbeat pattern for the identified scenario, the system fallbacks to another authentication scheme, such as asking the user to input a PIN. If the user is authenticated through the PIN, the buffered heartbeat signals are used for generating the new heartbeat pattern (both the alignment template and the SVM model) for the identified scenario.

The key components of our system are described in the following sections:

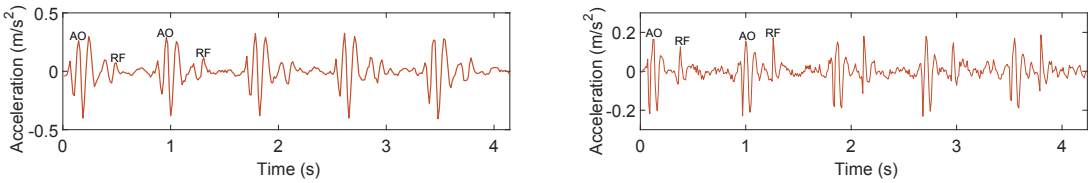
Heartbeat Segmentation and Alignment (Section 4): In the heartbeat segmentation component, we use a two-step segmentation algorithm to divide the continuous acceleration signals into individual heartbeat cycles. The first step is coarse heart rate estimation, which uses a coarse template to estimate the heart rates from the accelerometer readings. The estimated heart rates are used for selecting the heartbeat pattern which contains the template for fine-grained heartbeat alignment. In the second step of heartbeat segmentation, we use the fine template to perform a cross-correlation on the continuous heartbeat signals. By this way, we can precisely align the key features of each heartbeat cycle in the time domain.

Feature Extraction (Section 5): After the segmentation step, our system performs data preprocessing, *e.g.*, normalizing the amplitude of the heartbeat signals, before the feature extraction step. Then, we use Discrete Wavelet Transform (DWT) to extract features from the heartbeat. Each heartbeat cycle is decomposed into multiple levels of wavelet coefficients, and we choose the wavelet coefficients that are most closely related to the heartbeat patterns. This way, we reduce noises that come from different sources, including the respiration movements, small limb movements, and small variations in accelerometer readings.



(a) Heartbeat motion stages (b) Heartbeat pattern of volunteer A (c) Heartbeat pattern of volunteer B

Fig. 3. Heartbeat movement cycle and pattern



(a) Volunteer A (b) Volunteer B

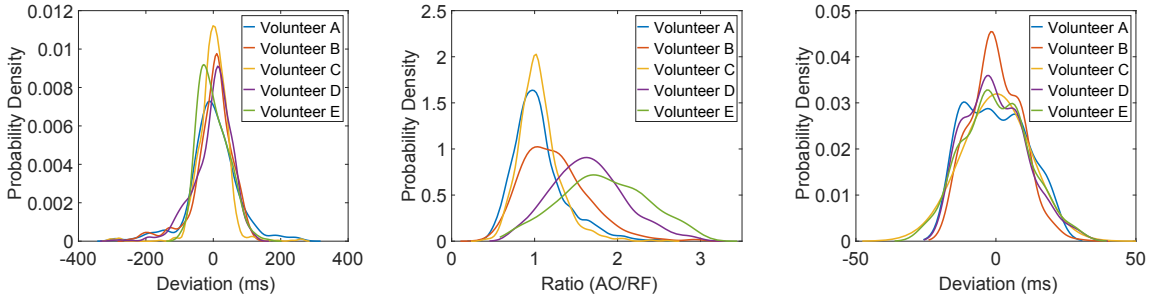
Fig. 4. Five consecutive heartbeat cycles for volunteer A and B

User Authentication (Section 6): Heartbeat authentication uses the SVM model for the heartbeat pattern of the given scenario. We first perform a per-heartbeat evaluation that gives the likelihood that the given heartbeat is from the authorized user. We then combine the likelihood of multiple consecutive heartbeats to improve the confidence in the decision. Our system dynamically determines the number of heartbeats that are required for the authentication process. For example, if the heartbeats have a consistently high likelihood of belonging to the authorized user, the authentication may only require as few as five heartbeats. If the system is not confident in the decision, it may instruct the user to press the phone on the chest for a longer time so that more heartbeat samples can be collected to improve the confidence.

3.2 Background of the SCG Signal

The seismocardiogram (SCG) signals collected by accelerometers capture the heartbeat motion of the user. Heartbeat motion is a 3D self-driving heart deformation arising from the stimulation of the cardiac muscle [22]. The human heart has two upper chambers (*i.e.* atria) and two bottom chambers (*i.e.* ventricles) [32]. The continuous contraction and relaxation of atria and ventricles cause the heartbeat motion. As shown in Fig.3(a), one heartbeat motion cycle consists of seven stages: (1) atrial contraction (ATC), (2) mitral valve closing (MC), (3) aortic valve opening (AO), (4) point of maximal acceleration in the aorta (MA), (5) aortic valve closure (AC), (6) mitral valve opening (MO), (7) rapid filling of left ventricle (RF) [16, 25].

The motion stages of the heartbeat cycle can be captured and identified using the accelerometer readings provided by mobile phones, see Figure 3(b). As the phone is pressed perpendicularly on the chest, we always use the readings of the y-axis of the accelerometer (pointing from the bottom to the top of the phone). Depending on the stage of the heartbeat cycle, the acceleration caused by the heart motion could be positive or negative. Therefore, each stage in the heartbeat cycle corresponds to one of the peaks or valleys in the SCG signal. Based on our measurements, the average amplitude of the AO peak is 0.2558 m/s^2 (SD= 0.0384 m/s^2). The background noise level of the accelerometer has a variance of 0.0104 m/s^2. Therefore, commercial mobile phones provide enough Signal-to-Noise Ratio (SNR) for measuring the details in SCG signals.



(a) Deviation of heartbeat interval from the mean value (b) Ratio of AO amplitude to RF Amplitude (c) Deviation of AO-RF interval from the mean value

Fig. 5. Variations in the SCG signal

3.3 Characteristics of the SCG Signal

By looking at the SCG waveforms, we have the following observations that lead to the possibility of using the SCG signal for authentication:

First, the SCG signals of different people go through the same seven stages, but have different signal patterns in terms of amplitudes of the corresponding peaks and intervals between peaks. Figure 3(b) and Figure 3(c) show two SCG samples of one heartbeat cycle from two volunteers. While both volunteers have similar heart rates (73 BPM and 71 BPM, respectively), the two SCG patterns have distinctive features. For example, the amplitudes of the AO peaks for the two volunteers are quite different. Such difference in heartbeat motion comes from the differences in the size, position and shape of the heart [38]. Therefore, the heartbeat motion patterns contain unique biometric features of the given user [22].

Second, the SCG signals of the same user are consistent over time. Figure 4 shows five consecutive heartbeat patterns of two volunteers. While there are small variations in the signals, we observe that the heartbeat patterns from the same person are consistent for consecutive heartbeat cycles. Furthermore, with heartbeat patterns collected across three months and with different clothes, we find that heartbeat patterns of the same user are quite stable. Therefore, the SCG signal can potentially serve as a consistent identity for the user.

4 HEARTBEAT SEGMENTATION AND ALIGNMENT

In this section, we describe the heartbeat segmentation and alignment process, in which the continuous heartbeat signals are divided into individual heartbeat cycles. High precision signal alignment is vital to heartbeat-based authentication systems. This is because a misaligned heartbeat signal will lead to incorrect positioning of the different heartbeat stages. Consequently, such incorrect positioning will lead to errors in user authentication. However, due to the variances in both the amplitude and timing of the SCG signals, it is challenging to precisely align the heartbeat signals.

4.1 Variations in the SCG Signal

While human heartbeats are repetitive motions, ECG-based experiments show that heartbeats are not perfectly periodical [2, 3, 27, 45]. Therefore, the SCG signals also have variations in both the amplitude and timing of the peaks corresponding to different heart motion stages.

First, human heartbeat rates are not stable. There are intrinsic Heartbeat Rate Variability (HRV) in SCG signals [42]. Figure 5(a) shows the Probability Density Function (PDF) of the deviation in time intervals between two normal heartbeats for five volunteers sitting on the chair. The ground truth values are obtained by manually selecting the auto-correlation peaks in the SCG signals. We observe that the standard deviation of heartbeat interval is 46ms, which is consistent with results from ECG signals [42]. Thus, the duration of heartbeat cycle

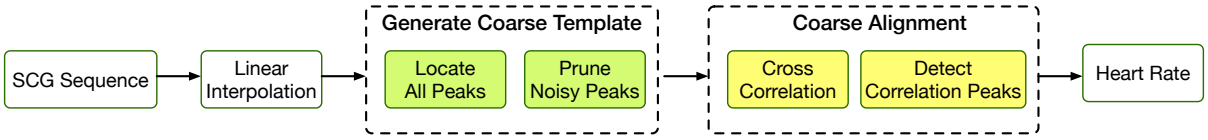


Fig. 6. Heart Rate Estimation Scheme

could be changing by as much as 1/20 of the cycle length since a normal heartbeat lasts for about one second at a heart rate of 60 BPM.

Second, the peak amplitude in the SCG signal varies significantly. Figure 5(b) shows the PDF for the ratio of the amplitude of the AO peak to the RF peak in the same heartbeat cycle. These two peaks are the most prominent features in the SCG signal. Different persons have different AO to RF ratios, as shown in Figure 4. The standard deviations of AO to RF ratio is larger than 0.25 for all volunteers. This implies that the AO to RF ratio for the same person also varies significantly, *e.g.*, in consecutive heartbeat cycles, either the AO or the RF peak could be the highest peak in the cycle, see Figure 4(b). Therefore, it is challenging to identify the AO and RF peaks using a small number of heartbeat cycles. Existing systems use hints from other measurements, such as the photoplethysmogram (PPG) [59], to help identify the AO peak. However, our system only has the SCG signals as the reference to perform the segmentation.

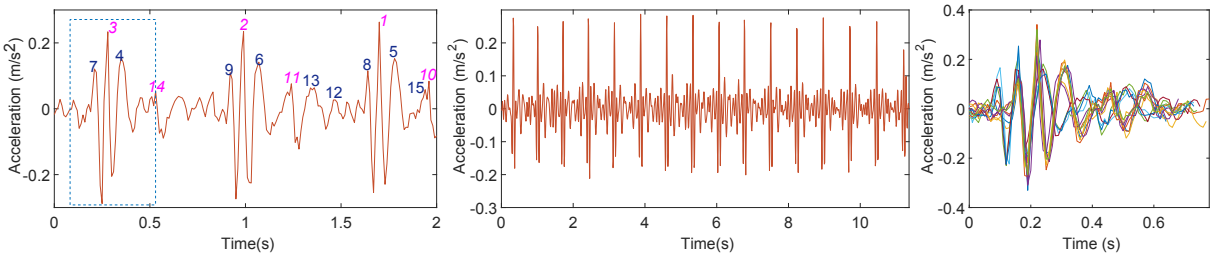
Fortunately, we observe that the time interval between the AO stage and RF stage is relatively stable. Figure 5(c) shows the PDF of the deviation in the time interval between the AO and the RF peak. The standard deviation of the AO-RF interval is 9.48 *ms*, which is much smaller than that of the heartbeat interval. This implies that the ratio of the AO-RF interval to the heartbeat interval also changes significantly, as the AO-RF interval is stable and the heartbeat interval is unstable. We further verified that the AO-RF intervals are stable under different states. We collect SCG signals when users finish exercising, recline on the sofa and lie on the bed. While the heart rates are significantly higher in the exercising state, the standard deviation of the AO-RF interval is still small (*i.e.*, 11.2 *ms*). The standard deviations of AO-RF interval for the reclining and lying states are 8.25 *ms* and 5.86 *ms*, respectively.

Based on the above observations, we choose to use the interval between the ATC stage and the RF stage as the reference for heartbeat segmentation and alignment. We choose the ATC-RF interval due to two reasons. First, the ATC-RF interval contains the two highest peaks in the SCG signal, *i.e.*, AO and RF, that can be easily identified. Second, the time interval between AO and RF has smaller variations than other parts of the heartbeat cycle. We design a two-step process to divide and align the heartbeat using the signals in the reference interval as follows.

4.2 Heart Rate Estimation

Given a new SCG sequence, the first step is to use a heart rate estimation algorithm, as shown in Figure 6, to measure the heart rates. To estimate the heart rates, we first use a linear interpolation algorithm to normalize the accelerometer readings to a standard sampling rate (*e.g.*, 100 Hz). This step ensures that our system can work on mobile phones that have different sampling rates for the accelerometer.

The second step of heart rate estimation is to derive a coarse-template of the reference ATC-RF interval from the SCG signals. To identify the ATC-RF interval, we first locate all the peaks (local maximum points) in an SCG sequence with a two-second duration. We assume that the heart rates of the user are between 50 BPM and 120 BPM. Therefore, there is at least one full heartbeat cycle in the two-second SCG signal. We sort the local maximum points by their amplitudes as the labels shown in Figure 7(a). We then perform a pruning algorithm to remove noisy peaks. Starting from the highest peaks, we add the peaks into a candidate set one-by-one in the descending order of their amplitudes. If the current peak is within a time interval of τ to one of the candidate peaks in the set,



(a) Coarse-template selection (b) Correlation results of the coarse-template (c) Coarse alignment results

Fig. 7. Coarse Estimation on Heart Rate

the current peak is removed. We set the threshold τ to be 200 *ms*, as the AO-RF intervals are larger than 200 *ms* when the heart rate is slower than 120 BPM. After the pruning process, only the peaks corresponding to AO and RF are in the candidate set, *e.g.*, peaks 3, 14, 2, 11, 1 and 10 in Figure 7(a). As there are multiple heartbeat cycles in the two-second SCG sequence, there are multiple candidates of AO and RF peaks. We choose the two peaks that are the closest to each other as the AO and RF for the coarse-template since the AO-RF interval is usually smaller than the RF-AO interval. We then measure the interval μ between the selected AO and RF peaks. We use a segment with a duration of 1.5μ as the coarse-template, starting from 0.5μ before the AO peak to include the ATC stage. The resulting coarse-template is shown the blue dashed rectangle in Figure 7(a).

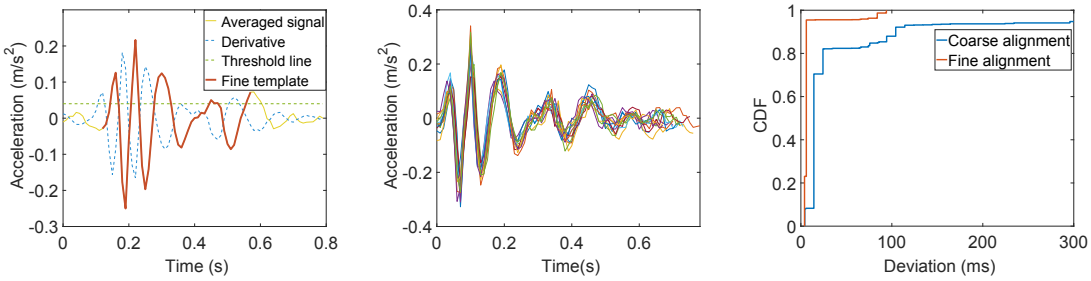
In the third step, we perform a cross-correlation between the coarse-template with the continuous SCG signals. Figure 7(b) shows the result of the correlation, where each heartbeat corresponds to a peak that is easier to be identified than the AO or RF peaks in the raw SCG. We use a threshold based scheme to detect peaks in the correlation result. By measuring the number of correlation peaks, we can derive the heartbeat interval and the heart rates of the given SCG signal. The coarse-template based scheme gives more stable heart rate estimation than auto-correlation or FFT based schemes. This is because the similarity of AO and RF peaks for some user may introduce multiple peaks in the auto-correlation and FFT of the SCG signal, which leads to large errors in heart rate estimation.

Due to the variations in the timing and amplitude of the AO and RF peaks, our coarse-template could be imprecise. For example, our heuristic algorithm could select a wrong peak to be the AO or RF. Moreover, the coarse-template derived from a single heartbeat cycle could be noisy due to the interference from breathing or other micro movements when collecting the SCG samples. Consequently, the segmentation result based on correlation of the coarse-template is not well aligned. As shown in Figure 7(c), the segmentation results of fifteen heartbeat samples collected at different times from the same person are not perfectly aligned with each other due to the errors in the coarse-template.

4.3 Fine-grained Alignment

We use a fine-alignment-template to help align the SCG signals that are collected under different conditions. The fine-alignment-template is produced in the training process and we generate one fine-template for each scenario. For a new SCG sequence, we first use the heart rate estimation scheme to get the heart rates that are used for selecting the fine-template. Note that the fine-template generated in the training process can be applied to all SCG samples with a similar heart rate. Therefore, we only need to generate the fine-template once.

We use an SCG sequence that contains at least ten consecutive heartbeats to generate the fine-template. First, we use the coarse segmentation scheme to divide the heartbeat signal into individual cycles. Second, we average over all the heartbeat cycles to reduce the impact of occasionally misaligned cycles and the noises caused by micro-movements. The smoothed signal is shown in Figure 8(a). Third, we use the smoothed signal to estimate the



(a) Fine-alignment-template selection (b) Fine alignment results (c) CDF of the time deviations in different alignment schemes

Fig. 8. Fine alignment results

start of the ATC stage, instead of using a heuristic interval in the coarse-template. We observe that the smoothed SCG signal remains almost static before the ATC stage and starts to change drastically at the ATC stage. Thus, to estimate the start of the ATC stage, we first normalize the amplitude of the smoothed signal by dividing the samples by the maximum amplitude of the signal. We then estimate the first derivative of the smoothed signal $S'(t) = dS(t)/dt$ using the expression $S(t) \approx S(t+m) - S(t)$, where we take the time difference m as four sample points (*i.e.*, 40 *ms* at a sampling rate of 100 Hz). As shown in Figure 8(a), the first derivative of the SCG signal, $S'(t)$, has a high amplitude at the start of ATC. Therefore, we use a threshold based scheme to detect the ATC start on the normalized SCG signal. We use the smoothed SCG signal between the ATC starting point and the RF as the fine-alignment-template, see Figure 8(a).

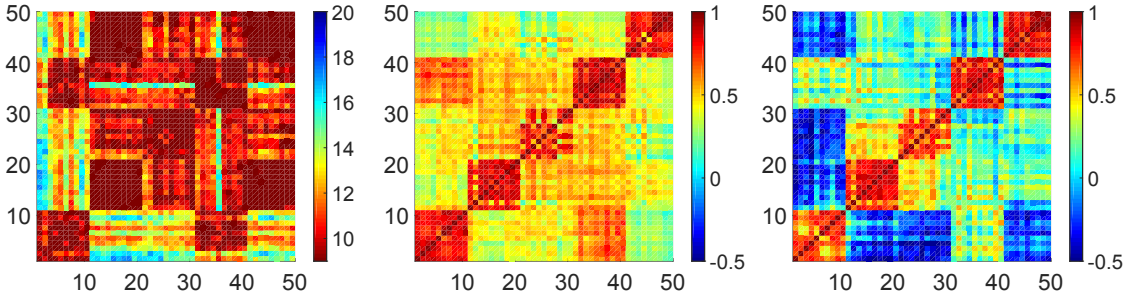
The fine-template is used for aligning the heartbeat cycles in a testing continuous heartbeat sequence. We perform a cross-correlation between the fine-template and the testing sequence. Note that the fine-template should have a similar heart rate as the testing sequence, as it is selected based on the heart rate estimation. Therefore, by locating the peaks in the cross-correlation result, we can accurately align the starting point of the ATC stage of different heartbeat cycles. Figure 8(b) shows the aligned of fifteen heartbeat cycles collected over a period of three days for a user. We observe that our fine alignment scheme can precisely match the key features of the AO-RF interval. To evaluate the performance of the alignment scheme, we collected SCG signals from five users, each containing 100 heartbeat cycles. Figure 8(c) shows the CDF of alignment deviations for the heart rate estimation algorithm and the fine alignment algorithm. For the alignment achieved by the coarse-template, the average deviation is 45.23 *ms*, which is much larger than the average deviation of 9.02 *ms* from the fine alignment algorithm.

5 FEATURE EXTRACTION

In this section, we focus on extracting features for user authentication from the SCG signals. Firstly, we preprocess the SCG signals to normalize both the amplitude and the length of the heartbeat signals. Secondly, we use the wavelet-based method to extract one set of feature vectors from each heartbeat cycle.

5.1 Normalization

The normalization algorithm takes the aligned heartbeat signals and uses two steps to reduce the variations of the SCG signals. The first step is to reduce the variation of the SCG amplitude so that heartbeats collected under different conditions have comparable amplitudes. The amplitude of SCG signals depends on the angle between the mobile phone's y-axis and the chest of the user, the position of the mobile phone, and the pressure that the user applied to the phone when collecting the heartbeat signal. Our system allows the user to collect the SCG signals in slightly different ways. Therefore, the amplitudes of the SCG signals collected under different conditions are



(a) Distance calculated through DTW (b) Correlation of the raw SCG sequence (c) Correlation of the DWT features

Fig. 9. Distance for features extracted from five users' heartbeat signals with 10 heartbeats for each user

different from each other. To verify this, we ask five users to repeat the data collection process, *i.e.*, press the phone on the chest and then release, for more than 100 times. The angle between the mobile phone's y-axis and the chest is inconsistent, as the users cannot precisely repeat the action. We observe that standard deviation of the maximum acceleration for each heartbeat cycle is larger than 0.0217 m/s^2, which is about one-tenth of the average amplitude of the AO peak. To remove this effect, we normalize the SCG signals of each heartbeat cycle by dividing with the maximum amplitude of the cycle.

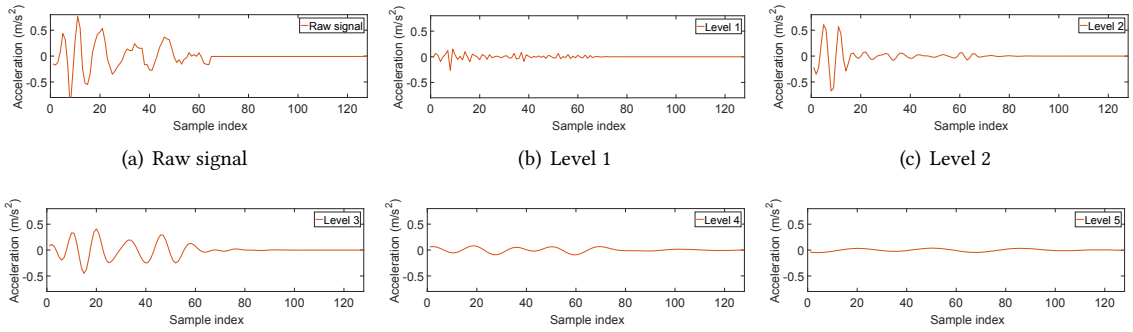
The second step is to normalize the heartbeat duration so that all heartbeat signals have the same length. Remember that consecutive heartbeats may have different intervals. However, we observe that the AO-RF stage has small time-variations as shown in Figure 5(c). Therefore, most time variations come from the stages after the RF stage. As we have precisely aligned the starting point of the heartbeat cycle, the ATC stage, in Section 4.3, we pad zeros at the end of each heartbeat cycle to guarantee the same duration. This will introduce little interference, as the amplitudes of the SCG signals are quite small after the RF stage, see Figure 4. In this way, we pad all heartbeat cycles into the same length (*e.g.*, 128 points) that can accommodate the longest heartbeat cycle.

5.2 Wavelet-based Feature Extraction

The feature extraction process needs to retain the characteristics of the user's heartbeats and remove irrelevant noises. Existing systems have proposed different feature extraction schemes. First, there are ECG-based [6, 28, 34, 50] and radio-based systems [39] that extract features based on the interval between different heartbeat stages. However, this scheme is not applicable to SCG signals because the variations in the amplitude of SCG lead to unreliable heartbeat stage identifications.

Second, one of the common approaches for waveform matching is to use the Dynamic Time Warping (DTW) algorithm that calculates the distance between two waveforms [48, 61]. However, the DTW algorithm may move the peaks in one waveform by a short time offset to match with peaks in the other waveform. Therefore, DTW ignores the timing difference in heartbeat motion stages and only compares the amplitude of the SCG peaks. This leads to a high false positive rate because the timing differences between heartbeat stages are ignored. Figure 9(a) shows the Euclidean distance between SCG signals of five different users (with 10 heartbeat samples for each user) calculated through DTW. A smaller distance means two heartbeat signals are more similar to each other. While the samples from the same person always have the smallest distances to each other (red squares), we observe that samples from different users also have very small DTW distances. Therefore, the DTW distance may falsely recognize samples from an attacker as those from the authorized user.

Third, it is also possible to use the raw time sequence of the SCG as a feature vector. However, the raw SCG sequences are noisy. The noises in SCG may come from the respiration, body and hand movements during the



(a) Raw signal (b) Level 1 (c) Level 2

(d) Level 3 (e) Level 4 (f) Level 5

Fig. 10. Five levels of DWT decompositions

capturing process. These noises reduce the reliability of the raw SCG sequence. Figure 9(b) shows the correlation coefficients of the raw SCG sequences between the same five users as in Figure 9(a). A higher correlation coefficient means that the two samples are more similar to each other. We observe that some users, *e.g.*, user 3, the correlation coefficients between his/her own samples are low due to the noises in SCG. Therefore, directly using the raw SCG sequences as features leads to high false negative rate, where the user's own heartbeat may be wrongly rejected due to noises in the SCG signals.

In this paper, we use Discrete Wavelet Transform (DWT) to extract features from the SCG signal. The DWT decomposes the signal into two parts of coefficients: the approximation coefficients that represent the low-frequency components and the detailed coefficients that represent the high-frequency components. By iteratively applying the wavelet decomposition on the approximation coefficients, the DWT can separate the original signals into multiple levels that contain components in different frequency ranges.

In our system, we use the discrete Meyer wavelet to decompose SCG signals into five levels. With a sampling rate of 100Hz, level 1 to 5 represent signal components in the frequency range of 25 $\sim$ 50 Hz, 12.5 $\sim$ 25 Hz, 6.25 $\sim$ 12.5 Hz, 3.13 $\sim$ 6.25 Hz and 1.56 $\sim$ 3.13 Hz, respectively. Figure 10 shows the reconstructed SCG signals from the detailed coefficients at the five levels.

To reduce noises from imperfections of the built-in accelerometers, we remove the high-frequency components in level 1. For heart rates in the range of 50~120 BPM, the heartbeat frequency is in the range of 1 $\sim$ 2 Hz. Therefore, we can remove level 5 where the signal component has a frequency lower than 3.13 Hz, which may not contain useful detailed features within a heartbeat cycle. In this way, we also remove the low-frequency movement interferences in the SCG signals. For example, the respiration movements have low frequencies in the range of 0.2 $\sim$ 0.4 Hz [60].

In summary, we use the detailed coefficients from the second level to the fourth level as the feature vector for heartbeat authentication. For a normalized heartbeat signal with 128 samples, the resulting DWT-based feature is a 56 dimensional vector. Our DWT-based feature extraction scheme has the following two advantages. First, by removing the coefficients in level 1 and below level 5, we reduce the noises in the SCG signal. Second, DWT has high time-resolution at levels representing the high-frequency components. Therefore, the high-frequency components retain the time intervals of sharp peaks in the SCG. For low-frequency components in the SCG, DWT is more tolerable in variations in the time domain. In this way, we achieve a balance between keeping the timing information and tolerating the variations in the heartbeat stages. Figure 9(c) shows the correlation coefficients of the DWT features for the five users. We observe that our DWT-based features outperform both the raw SCG features and the DTW based distance.

6 USER AUTHENTICATION

In this section, we use the features extracted from SCG signals in the previous section to build the authentication system.

6.1 Heartbeat Pattern Selection

Before the training or authentication process, our system first classifies the collected SCG signals into different scenarios. The scenarios are defined using both the heart rates and the postures of the user. For heart rates, we consider three cases for normal heart rates: $50 \sim 80$ BPM, $80 \sim 100$ BPM, and $100 \sim 120$ BPM. We select these three classes because they represent the normal heart rates, high heart rates caused by emotional changes and higher heart rates in the exercising state. For user postures, we consider three cases: sitting/standing, reclining, and lying down. Therefore, we have $3 \times 3 = 9$ different heartbeat patterns for the given user. Our system uses different heartbeat patterns to handle heart motion changes under different scenarios. For example, the acceleration of heart motions depends on the orientation of the heart so that heartbeat patterns collected in the sitting posture are different to that in the lying posture.

Our system uses the heart rates and the accelerometer readings to obtain the scenario information. Normally, we only need five heartbeats to perform the coarse heartbeat rate estimation for scenario selection. We use the accelerometer reading on the z-axis, which is perpendicular to the front surface of the phone, to determine the posture. As we require the user to press the mobile phone perpendicularly to his/her chest, the posture of the user can be derived from the angle between the gravity direction and the z-axis of the phone. For example, when the user is standing upright with the mobile phone pressed vertically on his/her chest, the acceleration readings along the z-axis should be close to the gravitational acceleration ($g = 9.8\ m/s^2$). Similarly, the acceleration readings along the z-axis for the reclining and lying down posture should be around $0.7g$ and 0, respectively, since the angle between the z-axis and the gravity direction are around $\pi/4$ and $\pi/2$ for these two cases. Therefore, we classify the three postures, sitting/standing, reclining, and lying down, by the z-axis acceleration range of $0.86g \sim g$ (angle in $-\pi/6 \sim \pi/6$), $0.5g \sim 0.86g$ (angle in $\pi/6 \sim \pi/3$) and $0g \sim 0.5g$ (angle in $\pi/3 \sim \pi/2$), respectively.

6.2 Training Process

Our training process includes two steps. The first step is to extract the fine-alignment-template as described in Section 4. This step requires at least ten heartbeat cycles. After that, we segment and align the heartbeats in the training samples and extract DWT features as described in Section 5.

The second step is to generate SVM patterns from the training samples. To train the authentication model, we build an SVM classifier which classifies heartbeat signals into two classes, *i.e.*, the positive class (the authorized user) and the negative class (attackers). During the training process, we use heartbeat instances from 9 benchmark persons randomly drawn from a standard global database as the negative class. Using the benchmark persons is helpful to determine the decision boundary for the positive class and enhance the authentication accuracy [62]. Once the heartbeat model is trained, the classifier can compute the likelihood that an unknown heartbeat instance belongs to the positive class. For those unseen instances from the attacker, the classifier can identify them as in the negative class since their heartbeat features have a low fitness probability to the features from the authorized user. We use the LIBSVM tool [10] with Radial Basis Function (RBF) kernel to build our SVM model. The optimal values for parameters v and γ of the RBF kernel are chosen via the standard grid search procedure.

6.3 Multiple Heartbeats Authentication

To authenticate the user, we first get the per-heartbeat score that denotes the likelihood of whether the given heartbeat is from the authorized user. Then, we dynamically determine the number of the required heartbeats to improve the confidence of the decision as the following steps.

Once the average score of multiple continuous heartbeats is larger than T_h, which implies a high likelihood that the heartbeats are from the authorized user, the mobile phone will be directly unlocked. Otherwise, our system requires the user to press the phone on the chest until collecting ten heartbeats to compute the final average score. The mobile phone would be finally unlocked when the final average score is larger than the threshold T_a. The value of T_h and T_a determines a tradeoff between False Positive Rate (FPR) and False Negative Rate (FNR). The process to select T_h and T_a is further described in Section 7.3. If the heartbeat-based authentication fails, the authorized user can unlock the phone using other approaches (*e.g.*, PIN or fingerprint) and log in the system to augment the buffered heartbeat signals into the heartbeat pattern database which will be used to retrain the SVM model.

7 IMPLEMENTATION AND EVALUATION

7.1 Implementation

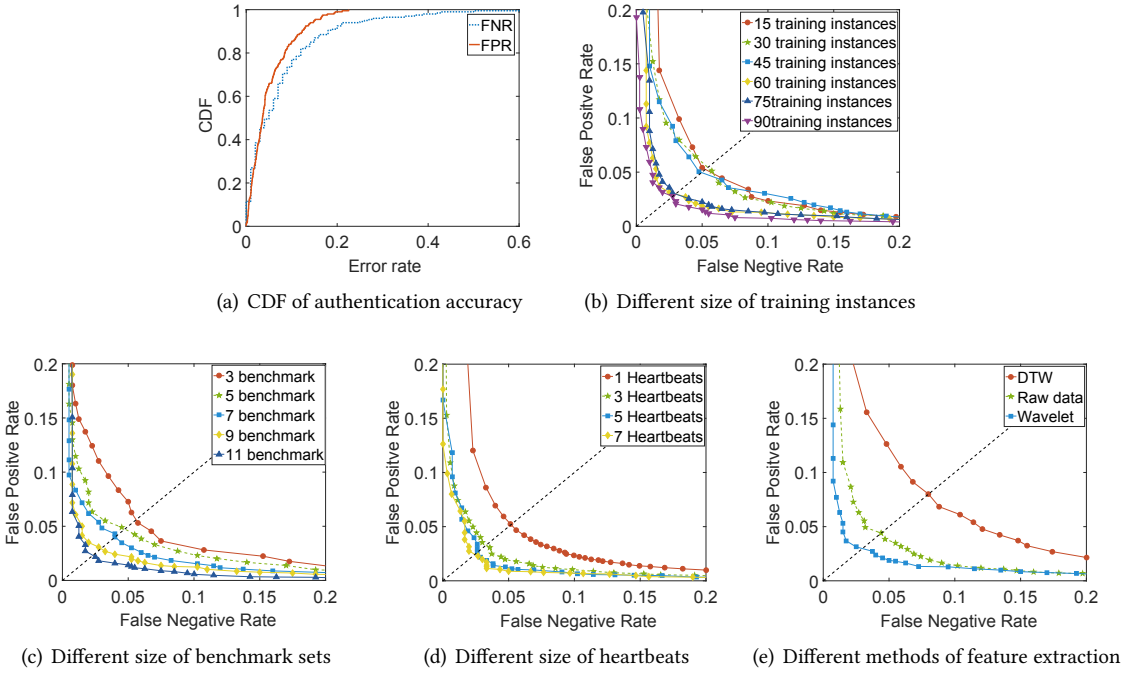
We implemented our system on the Android platform. Our prototype works as an APP that uses the built-in accelerometer to capture the heartbeat vibration and performs user authentication on recent Android devices, *e.g.*, Samsung Galaxy S5 with Android 5.0 OS and Nexus 6P with Android 8.0 OS, *etc.*. If not specified, the sampling rate of the built-in accelerometer is fixed at 100 samples per second. When performing user authentication, the users are asked to press the smartphone on his/her chest, as shown in Figure 1(a). Our APP segments the heart beats into individual cycles and estimates the heart rates in realtime, as shown in Figure 1(b). We use the LIBSVM tool [10] in Java to predict the authorized user and display the result on the smartphone screen.

7.2 Evaluation Setup

For most of the evaluation, we recruited 20 participants (5 females) from 21 to 29 years. All the participants are healthy graduate students and have no experience of heartbeat based user authentication. The average heart rates of the participants were in the range of 61 to 105 BPM, with an average of 83 BPM. Before the experiments, there was a brief five-minutes introduction session to the participants, which introduced the usage of the APP and the correct way for data collection. We marked the same position for collecting the SCG signals on the clothes of participants. In each session, participants were asked to press the smartphone on the mark for 10 seconds and release the smartphone from the chest for 10 seconds. Each data collection process lasted 20 minutes with 60 sessions of 20 seconds. All participants conducted authentication accuracy experiments. We randomly assigned participants from each gender to conduct the authentication scenario experiments (five participants with one female) and robustness experiments (five participants with one female). We also enrolled 15 other participants in different age groups to evaluate the robustness of our system. We collected more than 110, 000 heartbeats in our experiments. If not specified, the results reported in the following sections are obtained through an offline training and prediction process running on a workstation.

7.3 Authentication Accuracy

To evaluate authentication accuracy, we use one user as the authorized user and randomly select 9 users among the 20 participants as the benchmark users. In SVM training process, samples from authorized user serve as positive samples and samples from benchmark users serves as negative samples. If not specified, we use a training sample size of 60 heartbeat cycles for each user in the training process. In the testing process, the participants not appeared in training (*i.e.*, $20 - 1 - 9 = 10$ subjects) are acting as attackers. Note that none of the heartbeat signals from the attackers are seen during the training process. We use the cross-validation to evaluate the False Negative Rate (FNR) and False Positive Rate (FPR) for each authorized user. The FNR is the rate that the authorized user is miss-recognized as an attacker, and the FPR is the rate that an attacker is miss-recognized as the authorized user. For cross-validation, we randomly divide the SCG samples of the trained user into five groups with the



(a) CDF of authentication accuracy (b) Different size of training instances

(c) Different size of benchmark sets (d) Different size of heartbeats (e) Different methods of feature extraction

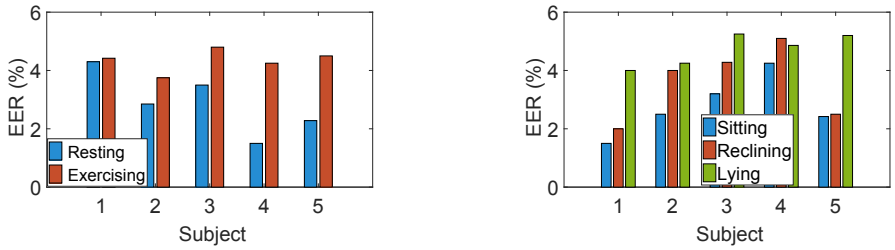
Fig. 11. Tradeoff between FNR and FPR

same sample size of 60 heartbeats as we collected more than 300 heartbeats from each user. Each time we use one group of samples as the training samples, and use the other four groups as the testing samples for the authorized user. We rotate the groups so that all samples are used for training once and report the average FNR and FPR for the given authorized user. We also rotate the authorized user so that every participant acts as the authorized user once. If not specified, the reported FNR and FPR are the average of 20 experiments where all the 20 participants act as the authorized user once.

Using one heartbeat cycle, our system achieves an average FNR and FPR of 7.57% *and* 5.08%*, respectively.* Figure 11(a) shows the distribution of FNR and FPR when different participants act as the authorized user under an SVM decision boundary of 0.15. For more than 80% of the participants, the average FNR and FPR are smaller than 12% and 8.6%, respectively. Note that we can tradeoff between FNR and FPR by adjusting the SVM decision boundary. With a higher decision boundary, a heartbeat sample is more likely to be rejected so that FNR will increase and the FPR will decrease. By carefully adjusting the decision boundary, we can make the FNR and FPR equal to each other and the equal value is called the Equal Error Rate (EER). Figure 11(d) shows the tradeoff between FNR and FPR and the EER for a single heartbeat cycle is 5.2%.

By combining the likelihood of five heartbeat cycles, our system achieves an EER of 2.62%. Figure 11(d) shows the EERs for combined decision made on 1, 3, 5, 7 heartbeats are 5.17%, 3.33%, 2.62%, 2.48%, respectively. Using a larger number of heartbeats for decision improves the performance. Therefore, we choose to make a quick decision using the first five heartbeats, when the average likelihood given by the SVM model is larger than 0.3. This gives a chance to unlock the mobile phone within five seconds. If the user does not pass the quick decision, our system may take as long as ten seconds to accumulate ten heartbeats for the final decision.

Our results show that 60 *heartbeat instances are practically enough for training the SVM classifier model.* Figure 11(b) shows the FNR and FPR under different training sample sizes, from 15 to 90 heartbeat instances. We observe



(a) EER in the resting and the exercising state

(b) EER for different body postures

Fig. 12. Authentication performance under different scenarios

that the EER reduces with a larger number of training heartbeat instances. Nevertheless, an SVM model trained by 60 instances has nearly the same performance as those trained with a larger number of instances. Therefore, we choose to collect 60 heartbeat instances in the initial data collection process. This reduces the duration of the initial data collection process to less than two minutes.

A larger benchmark set size leads to lower authentication EER. Figure 11(c) shows we can achieve EERs of 5.53%, 4.71%, 4.15%, 2.82%, 2.64% with the benchmark size of 3, 5, 7, 9, 11 users, respectively. The performance gain diminishes after the benchmark size is larger than 9 users. Therefore, we choose to use 9 benchmark users as the default setting of our system.

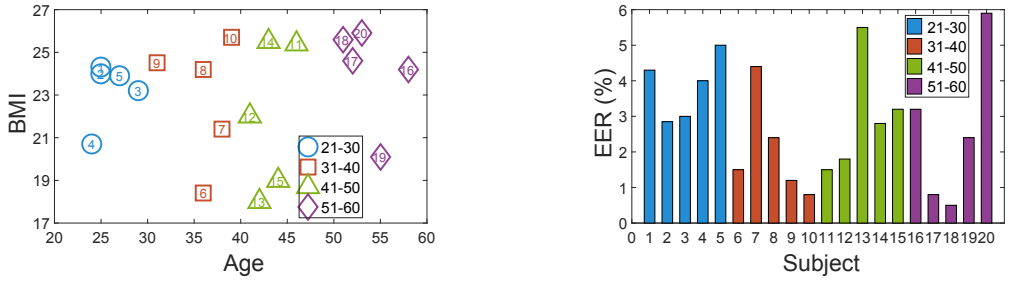
Wavelet-based features outperform both DTW-based and raw SCG sequence based features in heartbeat-based authentication. Figure 11(e) gives the FNR and FPR of the three different feature extraction methods. While the EER of wavelet-based method is 2.7%, the EERs for DTW-based method and raw SCG sequence based method are 4.42% and 8.01%, respectively. This shows wavelet-based features truly remove the noises in the SCG signals and improve the performance of our system.

7.4 Authentication Scenarios

To evaluate the performance of authentication under different scenarios, we randomly select five participants (including one female) for the experiments. As we have a smaller user set, we choose to use three participants as the benchmark user and the rest participant as the attacker. Similar to the evaluations in Section 7.3, we use the cross-validation approach and rotate the roles of the participants and each participant acts as the authorized user once. For each participant, we collect 250 instances over a period of 1 months. Note that the EERs in this section is not directly comparable to the values reported in Section 7.3 due to the smaller user set and different policies in choosing the benchmark set.

Our system achieves comparable performance under different scenarios, including in the resting state, in the exercising state and under different body postures. For the scenarios where the heart rates of the user change, we collect the SCG signals of each participant in both the resting state and the exercising state (*i.e.*, after running for 2 minutes). The average heart rates of the participants in the resting state and exercising state are 73 BPM and 109 BPM, respectively. Figure 12(a) shows that the average EER of the exercising state (4.34%) is slightly higher than the resting state (2.89%). This is mainly due to the less stable heartbeat patterns in the exercising states. Nevertheless, the EER in the exercising state is still lower than 5% so that our system can work in this scenario.

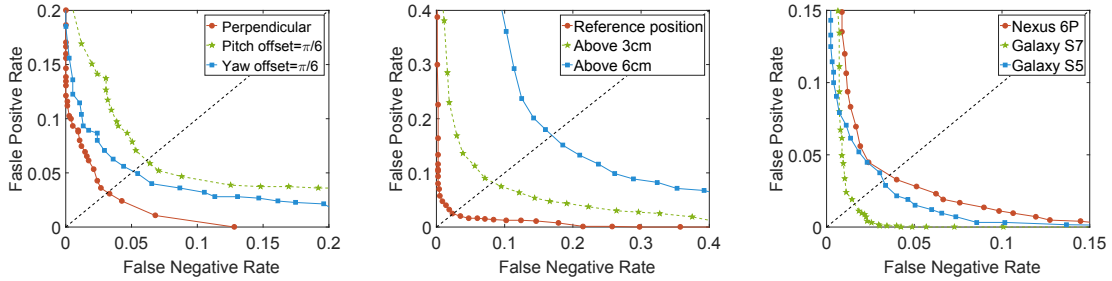
For different body postures, Figure 12(b) shows that our system achieves an average EERs of 2.77%, 3.57%, and 4.71% under the sitting, reclining and lying postures, respectively. The performance for the sitting posture is better than the other two postures. This is because the readings of the y-axis of the accelerometer in the other two postures capture both the SCG signals and the gravitational acceleration that may interfere with the weak SCG signals.



(a) BMI of subjects

(b) EER for subjects with various ages

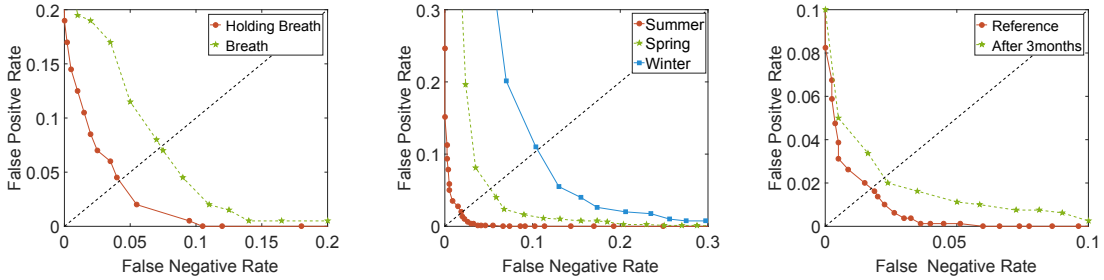
Fig. 13. Authentication performance under different age groups



(a) Robustness over different angles for data collection

(b) Robustness over different positions for data collection

(c) Robustness over different phone modules



(d) Robustness over breathing interference

(e) Robustness over different clothes

(f) Robustness over time

Fig. 14. Evaluation of the robustness of heartbeat-based authentication

7.5 Robustness

We use the same five users as in the evaluations for authentication scenarios (Section 7.4) to evaluate the robustness of our system under different conditions. In the robustness evaluations, our system is trained with the standard set of training data, but the testing data set is collected under different conditions. For example, we treat the data collected at the position marked on the users' chest as the standard training data and use data collected at slightly moved positions as the testing data to evaluate the robustness of our system over differences in data collection positions. Note that in the following experiments, the testing data with the changed conditions are never seen by the training model. For each condition, we collect 250 heartbeat samples for each user.

Our system is robust over various ages and somatotypes. We recruit 20 participants of different ages and somatotypes characterized by Body Mass Index (BMI) as shown in Figure 13(a). Figure 13(b) shows the average EERs for age groups of 21 ∼ 30, 31 ∼ 40, 41 ∼ 50, and 51 ∼ 60 are 3.83%, 2.06%, 2.96%, and 2.56%, respectively. Additionally, we observe that the BMI values have a wide distribution across different age groups as shown in Figure 13(a). This implies that the age and BMI distributions have no significant impact on our authentication scheme.

The EER degrades by only 2.95% when the angle of the mobile phone is changed by less than 30 degrees. In the standard case, the user presses the mobile phone perpendicularly on his/her chest. However, users may slightly change the angle that the phone contacts with the body. In this experiment, we instruct the user to deviate from the perpendicular angle with either a *Pitch* offset (the up-down angle) or a *Yaw* offset (the left-right angle) of 30 degrees. Figure 14(a) shows that our system achieves average EERs of 3.19%, 5.20%, and 6.14% for the *Perpendicular*, *Pitch offset of 30 degrees*, and *Yaw offset of 30 degrees* cases, respectively. Therefore, heartbeat samples collected in the perpendicular direction can be used for authentication when the user slightly changes the angle of the phone.

Our system can tolerate position deviations as large as 3 cm from the standard testing point. In the previous evaluations, we mark the testing point on the clothes of the participants and ask the participants to press the phone on the mark. To evaluate the case that the user put the phone at a slightly different position, we ask participants to collect data by pressing the phone at 3 *cm* or 6 *cm* above the mark. As Figure 14(b) shown, the EERs of "Reference position", "Above 3 *cm*" and "Above 6 *cm*" are 2.84%, 7.46%, and 17.2%, respectively. Compared to the "Reference position", the EER of the "Above 3 *cm*" case is slightly larger while that of the "Above 6 *cm*" case deteriorates significantly. This is because the SCG signal has a small amplitude at a position that is far from the reference position.

Our system is effective for different types of mobile phones. We perform authentication on Samsung Galaxy S5, Galaxy S7, and Nexus 6P, respectively. The EERs of S5, S7, and Nexus 6P are 1.68%, 3.26%, and 3.64%, respectively. Despite that we find that the noise of Nexus 6P is considerably larger than S5 and S7, the authentication performance of our system for Nexus 6P is only slightly worse than S5 and S7. This is mainly because that our wavelet-based feature extraction can effectively reduce noise in accelerometer readings.

Our system is robust against the interferences from human respiration. To evaluate the impact of human respiration, we instruct the participants to breathe normally and hold his/her breath when collecting data. The samples collected with normal breath are served as the standard training samples to train the system. From Figure 14(d), we observe that the EER for the case of holding breath is slightly smaller than the case of the normal breath. Human respiration does not interfere with our heartbeat based authentication because: i) Our system uses DWT to reduce the low-frequency noise introduced by breathing; ii) Heartbeats introduce larger accelerations than breathing [66].

Our system achieves an EER lower than 10.69% for different types of clothes. We collect data when the participants are wearing different types of clothes, *i.e.*, summer, spring, and winter clothes. The standard training data set is collected when the participants wear summer clothes, *i.e.*, T-shirts with an average thickness of 3 *mm*. For spring and winter clothes, we ask the participants to wear jackets (with an average thickness of 5 *mm*) and coats (with an average thickness of 11 *mm*). Figure 14(e) shows that the average EERs for three types of clothes are 2.13%, 4.58%, and 10.69%, respectively. While the EER increases with the thickness of clothes, our system still can reliably detect the heartbeats over thick winter clothes.

Our results show that the heartbeat patterns are stable over a long period. To evaluate the stability of heartbeat patterns, we first train the system using the heartbeat samples collected at a reference time point, *e.g.*, the initialization time of the system. We then use the heartbeat patterns to predict heartbeats of the same user collected after three months. As shown in Figure 14(f), the EER for samples collected after three months is 2.35%, which is slightly worse than the EER for samples collected at the reference time. This shows the heartbeat patterns

Table 1. Time consumption

	Heart rate estimation	Fine-grained alignment	SVM-based Heartbeat Authentication	Total
Time	2.01 *ms*	1.69 *ms*	44.65 *ms*	48.35 *ms*

are quite stable over a period of three months. In reality, we can always augment fresh heartbeat samples into the training dataset to keep track of the slowly changing patterns for the authorized user.

7.6 Latency and Power Consumption

Our system achieves a latency of 48.35 ms for authentication with one heartbeat cycle. We measured the processing time for our system on a Samsung Galaxy S5 with Qualcomm Snapdragon 2.5 GHz quad-core CPU. Our implementation has two parallel threads: the display thread and the authentication thread. Our real-time application processes the SCG signals with a segment size of 100 data samples (with time duration of 1 second under a sampling rate of 100 Hz). The processing time of one segment is 2.01 *ms* and 1.69 *ms* for heart rate estimation and fine-grained alignment on average. The processing time of the SVM-based authentication for one heartbeat signal is 44.65 *ms* (we skip the wavelet feature extraction on the Android APP). Therefore, the overall latency for our system is only $2.01 + 1.69 + 44.65 = 48.35$ *ms*, which is acceptable for users.

Our system incurs a moderate power consumption of 153.2 ± 9.5 *mW on commercial smartphones.* We use PowerTutor [65] to measure the power consumption of our system on Samsung Galaxy S5. We measured the average power consumption for five minutes with five sessions of one minute. In each session, the user performed heartbeat authentication for six rounds within one minute. Without considering the LCD power consumption, the average power consumptions of CPU is 153.2 ± 9.5 mW.

8 LIMITATIONS AND DISCUSSION

Our current implementation for heartbeat-based authentication has the following limitations.

Effects of Motion: In our current design, the users should remain static when collecting the heartbeats. Accelerometers are sensitive to both body movements and hand movements. Therefore, we cannot reliably measure the SCG signals when the user is walking or running. Additionally, our system cannot measure the SCG signals when the phone is vibrating for an incoming call.

Effects of Health Condition: The volunteers in our experiments are healthy people whose heart rates are relatively stable. However, the heart rate of people with heart conditions, such as arrhythmias, may have considerable variability. Such heart conditions may interfere with the heartbeat pattern selection severely. Furthermore, pacemakers may also interfere with the heartbeat patterns. We leave the performance study for people with pacemakers and heart conditions as future works.

Training Efforts: We need about 60 heartbeats for training the heartbeat patterns for a given scenario. It takes about two minutes to collect the initial training samples, and more samples may be required for training in other scenarios. In the future, we will consider using transfer learning technologies to reduce the number of heartbeats needed for new authentication scenarios.

9 CONCLUSIONS

In this paper, we develop a new authentication system that uses the heartbeat signals collected by built-in accelerometers on commercial mobile phones. We show that the heartbeat signals can serve as the unique identifier for the user and the heartbeat features extracted can remain valid over a long period of time. Our authentication scheme and its implementation provide a new way to unlock personal mobile devices and can be combined with other biometrics based systems, *e.g.*, fingerprints, to enhance the security of the mobile system.

ACKNOWLEDGMENTS

We would like to thank our anonymous reviewers for their valuable comments. This work is partially supported by National Natural Science Foundation of China under Numbers 61472185, 61373129, 61772265, 61602194, and 61321491, JiangSu Natural Science Foundation No. BK20151390, National Key R&D Program of China 2018YFB1003800, and Collaborative Innovation Center of Novel Software Technology.

REFERENCES

[1] Fadel Adib, Hongzi Mao, Zachary Kabelac, Dina Katabi, and Robert C Miller. 2015. Smart homes that monitor breathing and heart rate. In *Proceedings of ACM CHI*.
[2] Foteini Agrafioti, Jiexin Gao, and Dimitrios Hatzinakos. 2011. Heart biometrics: Theory, methods and applications. In *Biometrics*. InTech.
[3] Foteini Agrafioti and Dimitrios Hatzinakos. 2010. Signal validation for cardiac biometrics. In *Proceedings of IEEE ICASSP*.
[4] Federico Alegre, Asmaa Amehraye, and Nicholas Evans. 2013. Spoofing countermeasures to protect automatic speaker verification from voice conversion. In *Proceedings of IEEE ICASSP*.
[5] Kamran Ali, Alex X. Liu, Wei Wang, and Muhammad Shahzad. 2015. Keystroke Recognition Using WiFi Signals. In *Proceedings of ACM MobiCom*.
[6] Juan Sebastian Arteaga-Falconi, Hussein Al Osman, and Abdulmotaleb El Saddik. 2016. ECG authentication for mobile devices. *IEEE Transactions on Instrumentation and Measurement* 65, 3 (2016), 591–600.
[7] Mossab Baloul, Estelle Cherrier, and Christophe Rosenberger. 2012. Challenge-based speaker recognition for mobile authentication. In *Proceedings of IEEE BIOSIG*.
[8] Christoph Bruser, Kurt Stadlthanner, Stijn de Waele, and Steffen Leonhardt. 2011. Adaptive beat-to-beat heart rate estimation in ballistocardiograms. *IEEE Transactions on Information Technology in Biomedicine* 15, 5 (2011), 778–786.
[9] Paolo Castiglioni, Andrea Faini, Gianfranco Parati, and Marco Di Rienzo. 2007. Wearable seismocardiography. In *Proceedings of IEEE EMBS*.
[10] Chih-Chung Chang and Chih-Jen Lin. 2011. LIBSVM: a library for support vector machines. *ACM transactions on intelligent systems and technology (TIST)* 2, 3 (2011), 27.
[11] Jagmohan Chauhan, Yining Hu, Suranga Seneviratne, Archan Misra, Aruna Seneviratne, and Youngki Lee. 2017. BreathPrint: Breathing acoustics-based user authentication. In *Proceedings of ACM MobiSys*.
[12] Tilendra Choudhary and M Sabarimalai Manikandan. 2015. A novel unified framework for noise-robust ECG-based biometric authentication. In *Proceedings of IEEE SPIN*.
[13] Phillip L De Leon, Michael Pucher, Junichi Yamagishi, Inma Hernaez, and Ibon Saratxaga. 2012. Evaluation of speaker verification security and detection of HMM-based synthetic speech. *IEEE Transactions on Audio, Speech, and Language Processing* 20, 8 (2012), 2280–2290.
[14] Marco Di Rienzo, Paolo Meriggi, Francesco Rizzo, Emanuele Vaini, Andrea Faini, Giampiero Merati, Gianfranco Parati, and Paolo Castiglioni. 2011. A wearable system for the seismocardiogram assessment in daily life conditions. In *Proceedings of IEEE EMBC*.
[15] Marco Di Rienzo, Emanuele Vaini, Paolo Castiglioni, Prospero Lombardi, Gianfranco Parati, Carolina Lombardi, Paolo Meriggi, and Francesco Rizzo. 2014. Wearable seismocardiography for the beat-to-beat assessment of cardiac intervals during sleep. In *Proceedings of IEEE EMBC*.
[16] M Di Rienzo, E Vaini, P Castiglioni, G Merati, P Meriggi, G Parati, A Faini, and F Rizzo. 2013. Wearable seismocardiography: Towards a beat-by-beat assessment of cardiac mechanics in ambulant subjects. *Autonomic Neuroscience: Basic and Clinical* 178, 1 (2013), 50–59.
[17] Nesli Erdogmus and Sebastien Marcel. 2014. Spoofing face recognition with 3D masks. *IEEE transactions on information forensics and security* 9, 7 (2014), 1084–1097.
[18] Mohammed E Fathy, Vishal M Patel, and Rama Chellappa. 2015. Face-based active authentication on mobile devices. In *Proceedings of IEEE ICASSP*. 1687–1691.
[19] Huan Feng, Kassem Fawaz, and Kang G Shin. 2017. Continuous authentication for voice assistants. In *Proceedings of ACM MobiCom*.
[20] David Friedrich, Xavier L Aubert, Hartmut Führ, and Andreas Brauers. 2011. Heart rate estimation on a beat-to-beat basis via ballistocardiography-a hybrid approach. In *Proceedings of IEEE EMBC*.
[21] Guodong Guo, Lingyun Wen, and Shuicheng Yan. 2014. Face authentication with makeup changes. *IEEE Transactions on Circuits and Systems for Video Technology* 24, 5 (2014), 814–825.
[22] John E Hall. 2011. Guyton and Hall textbook of medical physiology. *Philadelphia, PA: Saunders Elsevier* (2011), 107.
[23] Takahiro Hashizume, Takuya Arizono, and Koji Yatani. 2018. Auth'n'Scan: Opportunistic Photoplethysmography in Mobile Fingerprint Authentication. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 4 (2018), 137.
[24] Chenyu Huang, Huangxun Chen, Lin Yang, and Qian Zhang. 2018. BreathLive: Liveness Detection for Heart Sound Authentication with Deep Breathing. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 1 (2018), 12.

[25] Mohammad Shamim Imtiaz, Rajeena Shrestha, Talwinder Dhillon, Kazi Ata Yousuf, Bilal Saeed, Anh Dinh, and Khan Wahid. 2013. Correlation between seismocardiogram and systolic blood pressure. In *Proceedings of IEEE CCECE*.
[26] Omer T Inan, Pierre-Francois Migeotte, Kwang-Suk Park, Mozziyar Etemadi, Kouhyar Tavakolian, Ramon Casanella, John Zanetti, Jens Tank, Irina Funtova, G Kim Prisk, et al. 2015. Ballistocardiography and seismocardiography: A review of recent advances. *IEEE journal of biomedical and health informatics* 19, 4 (2015), 1414–1427.
[27] John M Irvine, Steven A Israel, W Todd Scruggs, and William J Worek. 2008. eigenPulse: Robust human identification from cardiovascular function. *Pattern Recognition* 41, 11 (2008), 3427–3435.
[28] Steven A Israel, John M Irvine, Andrew Cheng, Mark D Wiederhold, and Brenda K Wiederhold. 2005. ECG to identify individuals. *Pattern recognition* 38, 1 (2005), 133–142.
[29] Zhenhua Jia, Musaab Alaziz, Xiang Chi, Richard E Howard, Yanyong Zhang, Pei Zhang, Wade Trappe, Anand Sivasubramaniam, and Ning An. 2016. HB-phone: a bed-mounted geophone-based heartbeat monitoring system. In *Proceedings of ACM/IEEE IPSN*.
[30] Zhenhua Jia, Amelie Bonde, Sugang Li, Chenren Xu, Jingxian Wang, Yanyong Zhang, Richard E Howard, and Pei Zhang. 2017. Monitoring a Person's Heart Rate and Respiratory Rate on a Shared Bed Using Geophones. In *Proceedings of ACM SenSys*.
[31] Chaouki Kasmi and Jose Lopes Esteves. 2015. IEMI threats for information security: Remote command injection on modern smartphones. *IEEE Transactions on Electromagnetic Compatibility* 57, 6 (2015), 1752–1755.
[32] Arnold M Katz. 2010. *Physiology of the Heart*. Lippincott Williams & Wilkins.
[33] Risto Korpinen, Laila Saarnivaara, and K Siren. 1995. QT interval of the ECG, heart rate and arterial pressure during anaesthetic induction: comparative effects of alfentanil and esmolol. *Acta anaesthesiologica scandinavica* 39, 6 (1995), 809–813.
[34] Masaki Kyoso and Akihiko Uchiyama. 2001. Development of an ECG identification system. In *Proceedings of IEEE Engineering in medicine and biology society*.
[35] Federica Landreani, Mattia Morri, Alba Martin-Yebra, Claudia Casellato, Esteban Pavan, Carlo Frigo, and Enrico G Caiani. 2017. Ultra-short-term heart rate variability analysis on accelerometric signals from mobile phone. In *Proceedings of IEEE EHB*.
[36] Alexandre Laurin, Andrew Blaber, and Kouhyar Tavakolian. 2013. Seismocardiograms return valid heart rate variability indices. In *Proceedings of IEEE CinC*.
[37] Jeongwhan Lee, Keesam Jeong, Jiyoung Yoon, and Myoungho Lee. 1996. A simple real-time QRS detection algorithm. In *Proceedings of IEEE Engineering in Medicine and Biology Society*.
[38] Ming Li and Xin Li. 2014. Verification based ECG biometrics with cardiac irregular conditions using heartbeat level and segment level information fusion. In *Proceedings of IEEE ICASSP*.
[39] Feng Lin, Chen Song, Yan Zhuang, Wenyao Xu, Changzhi Li, and Kui Ren. 2017. Cardiac Scan: A Non-contact and Continuous Heart-based User Authentication System. In *Proceedings of ACM MobiCom*.
[40] Jian Liu, Yan Wang, Yingying Chen, Jie Yang, Xu Chen, and Jerry Cheng. 2015. Tracking vital signs during sleep leveraging off-the-shelf WiFi. In *Proceedings of ACM MobiHoc*.
[41] David C Mack, James T Patrie, Paul M Suratt, Robin A Felder, and Majd Alwan. 2009. Development and preliminary validation of heart rate and breathing rate detection using a passive, ballistocardiography-based sleep monitoring system. *IEEE Transactions on Information Technology in Biomedicine* 13, 1 (2009), 111–120.
[42] Marek Malik. 1996. Heart rate variability. *Annals of Noninvasive Electrocardiology* 1, 2 (1996), 151–181.
[43] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. 2002. Impact of artificial "gummy" fingers on fingerprint systems. In *Optical Security and Counterfeit Deterrence Techniques IV*, Vol. 4677. 275–290.
[44] Reham Mohamed and Moustafa Youssef. 2017. HeartSense: Ubiquitous Accurate Multi-Modal Fusion-based Heart Rate Estimation Using Smartphones. In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*.
[45] Dietmar Mücke. 1996. *Elektrokardiographie systematisch*. UNI-MED-Verlag.
[46] B Neubauer and HJ Gundersen. 1978. Analysis of heart rate variations in patients with multiple sclerosis. A simple measure of autonomic nervous disturbances using an ordinary ECG. *Journal of Neurology, Neurosurgery & Psychiatry* 41, 5 (1978), 417–419.
[47] Lawrence O'Gorman. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proc. IEEE* 91, 12 (2003), 2021–2040.
[48] Medha Pandit and Josef Kittler. 1998. Feature selection for a DTW-based speaker verification system. In *Proceedings of IEEE ICASSP*.
[49] Giuseppe Petracca, Yuqiong Sun, Trent Jaeger, and Ahmad Atamli. 2015. Audroid: Preventing attacks on audio channels in mobile devices. In *Proceedings of ACM ACSAC*.
[50] Konstantinos N Plataniotis, Dimitrios Hatzinakos, and Jimmy KM Lee. 2006. ECG biometric recognition without fiducial detection. In *Proceedings of IEEE Biometric Consortium Conference*.
[51] Kun Qian, Chenshu Wu, Fu Xiao, Yue Zheng, Yi Zhang, Zheng Yang, and Yunhao Liu. 2018. Acousticcardiogram: Monitoring Heartbeats using Acoustic Signals on Smart Devices. In *Proceedings of IEEE INFOCOM*.
[52] J Ramos-Castro, J Moreno, H Miranda-Vidal, MA Garcia-Gonzalez, Mireya Fernández-Chimeno, G Rodas, and Ll Capdevila. 2012. Heart rate variability analysis using a seismocardiogram signal. In *Proceedings of IEEE EMBS*.
[53] Nalini K Ratha, Ruud M Bolle, Vinayaka D Pandit, and Vaibhav Vaish. 2000. Robust fingerprint authentication using local structural similarity. In *Proceedings of IEEE Workshop on Applications of Computer Vision*.

[54] Florian Schaub, Ruben Deyhle, and Michael Weber. 2012. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *Proceedings of ACM MUM*.
[55] Nabilah Shabrina, Tsuyoshi Isshiki, and Hiroaki Kunieda. 2016. Fingerprint authentication on touch sensor using Phase-Only Correlation method. In *Proceedings of IEEE IC-ICTES*.
[56] Mojtaba Jafari Tadi, Eero Lehtonen, Tero Koivisto, Mikko Pänkäälä, Ari Paasio, and Mika Teräs. 2015. Seismocardiography: Toward heart rate variability (HRV) estimation. In *Proceedings of IEEE MeMeA*.
[57] Shejin Thavalengal, Petronel Bigioi, and Peter Corcoran. 2015. Iris authentication in handheld devices-considerations for constraint-free acquisition. *IEEE Transactions on Consumer Electronics* 61, 2 (2015), 245–253.
[58] LCM Vanderlei, RA Silva, CM Pastre, Fábio Mícolis de Azevedo, and MF Godoy. 2008. Comparison of the Polar S810i monitor and the ECG for the analysis of heart rate variability in the time and frequency domains. *Brazilian Journal of Medical and Biological Research* 41, 10 (2008), 854–859.
[59] Edward Jay Wang, Junyi Zhu, Mohit Jain, Tien-Jui Lee, Elliot Saba, Lama Nachman, and Shwetak N Patel. 2018. Seismo: Blood Pressure Monitoring using Built-in Smartphone Accelerometer and Camera. In *Proceedings of ACM CHI*.
[60] Hao Wang, Daqing Zhang, Junyi Ma, Yasha Wang, Yuxiang Wang, Dan Wu, Tao Gu, and Bing Xie. 2016. Human respiration detection with commodity WiFi devices: do user location and body orientation matter?. In *Proceedings of ACM UbiComp*.
[61] Jin Wang, Mary She, Saeid Nahavandi, and Abbas Kouzani. 2010. A review of vision-based gait recognition methods for human identification. In *Proceedings of IEEE DICTA*.
[62] Wei Wang, Alex X Liu, and Muhammad Shahzad. 2016. Gait recognition using WiFi signals. In *Proceedings of ACM UbiComp*.
[63] Xuyu Wang, Chao Yang, and Shiwen Mao. 2017. PhaseBeat: Exploiting CSI phase data for vital sign monitoring with commodity WiFi devices. In *Proceedings of IEEE ICDCS*.
[64] Zhicheng Yang, Parth H Pathak, Yunze Zeng, Xixi Liran, and Prasant Mohapatra. 2016. Monitoring vital signs using millimeter wave. In *Proceedings of ACM MobiHoc*.
[65] Lide Zhang, Birjodh Tiwana, Zhiyun Qian, Zhaoguang Wang, Robert P. Dick, Zhuoqing Morley Mao, and Lei Yang. 2010. Accurate online power estimation and automatic battery behavior based power model generation for smartphones. In *Proceedings of IEEE CODES+ISSS*.
[66] Mingmin Zhao, Fadel Adib, and Dina Katabi. 2016. Emotion recognition using wireless signals. In *Proceedings of ACM MobiCom*.

Received May 2018; revised July 2018; accepted September 2018