HeartPrint: Exploring a Heartbeat-Based Multiuser Authentication With Single mmWave Radar

Yao Wang, Tao Gu, *Senior Member, IEEE*, Tom H. Luan, *Senior Member, IEEE*, Minjie Lyu, and Yue Li

***Abstract*—Continuous authentication is crucial for protecting user's privacy throughout their login session. Existing studies employ wireless sensing technologies to provide device-free and unobtrusive authentication; the user's behavior is continually assessed without their direct involvement until it deviates from their normal pattern. However, these works primarily concentrate on single-user authentication, which poses challenges in multiuser scenarios, such as smart homes and offices, where more than one user usually exists. In this article, we propose *HeartPrint*, a continuous multiuser authentication system, that employs a single commodity mmWave radar to capture the unique self-driving heartbeat motions from multiple users. Specifically, *HeartPrint* leverages the effect of skin surface vibrations caused by heartbeat on radio frequency (RF) transmissions. To profile individual heartbeat signals from the entangled components that are induced by multiple users, we first use a clustering method to position each user in the environment, then focus on the signal reflected from each position separately. The irrelevant body movements are eliminated from the RF signal by using a proposed signal energy comparison method for preserving fine-grained heartbeat traits. We then develop a pipeline to extract the most informative features for characterizing each user and feed them to an elaborated classifier for user authentication. We evaluate *HeartPrint* with 54 participants and demonstrate that it achieves an average authentication accuracy of over 95%. Additionally, we show that it is resilient against spoofing attacks, with an average attack success rate of less than 3%.**

***Index Terms*—Heartbeat-based biometrics, mmWave sensing, multiuser authentication.**

I. Introduction

With the forthcoming boom in Internet of Things (IoT) rich settings, everyday ordinary applications, such as access control, autonomous surveillance, and customized services, are implanted with sensing and control capabilities. It becomes even more critical to ensure that authentication procedures to such services remain secure and user-friendly. User authentication systems have evolved from "things you know" (e.g., passwords and graphical patterns) or "things you have" (e.g., software tokens and smart cards) to "things you are" (e.g., fingerprints and voice). Considering the cases that password is vulnerable to leakage and security possession is often forgotten to take or lost by people, biometric-based authentication brings a trouble-free and reliable way for users to access application services. Most biometric identifiers, such as fingerprint, facial appearance, and voice, nevertheless, are susceptible to be subverted by spoofing attacks [1], [2], [3]. The crucial weakness in these mechanisms is that they just provide a one-time confirmation for service login. As a result, new modalities that enable continuous user authentication are urgently needed.

To this end, solutions that leverage dynamic behavioral biometrics, such as eye movements [4], [5], [6], hand gestures [7], and keystroke dynamics [8], [9], are proposed for continuous authentication. However, they all require user's active interaction with the authentication system, which is labor-intensive and cumbersome. For example, eye movement-based methods require the user to incessantly look at the display and follow the visual stimuli on it. Recent studies have used intrinsic physiological biometrics, such as heartbeat and breathing, to eliminate the requirement for users to actively engage in the authentication process and allow systems to authenticate users at all times during the login session. For instance, Liu *et al.* [10] and Lin *et al.* [11] used channel state information (CSI) of WiFi signals and Doppler radar to discern user's breathing and heartbeat motions for continuous authentication, respectively. While they offer the benefit of removing users from active authentication and requiring no user interaction, the primary constraint is that they can only verify single users, which precludes their wider usage in multiuser environments (e.g., smart homes and offices).

Efforts are being made to expand the current applications to multiuser settings. For example, *MultiAuth* [12] and *WiWho* [13] reuse WiFi signals to sense the user's daily activities and walking gaits for multiuser identification, respectively. However, before deploying these solutions in the real world, several limitations need to be reconsidered.

1) The performance of these systems is less than satisfactory compared to the state-of-the-art works (see Table III), e.g., the authentication accuracy for three users is around 85%–90%. This is because the operating frequency of the WiFi signal is fixed and the reflected

Manuscript received 30 December 2021; revised 7 April 2022 and 23 June 2022; accepted 25 July 2022. Date of publication 3 August 2022; date of current version 7 December 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 62002278, and in part by the Natural Science Basic Research Program of Shaanxi under Grant 2022JQ-658. *(Corresponding author: Tao Gu.)*

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by Institutional Review Board (IRB) of Xidian University under Grant 2021-0776.

Yao Wang, Tom H. Luan, Minjie Lyu, and Yue Li are with the State Key Laboratory of Integrated Services Networks and the School of Cyber Engineering, Xidian University, Xi'an 710126, China (e-mail: wangyao@xidian.edu.cn; tom.luan@xidian.edu.cn; mjlv@xidian.edu.cn; liyue@xidian.edu.cn).

Tao Gu is with the Department of Computing, Macquarie University, Sydney, NSW 2109, Australia (e-mail: tao.gu@mq.edu.au).

Digital Object Identifier 10.1109/JIOT.2022.3196143

signals from multiple users are inextricably mingled in both time and frequency domains, it is difficult to separate the multiple components precisely.
2) They require at least a separation of 0.8–1 m between users during authentication, which obviates the situations when people are next to each other such as couples sharing the same bed or passengers sitting shoulder to shoulder in the rear seat.
3) They are still confronted with requiring users to perform proactive interactions with the system, i.e., complete the predefined actions or keep walking during authentication.

Research Focuses: Based on the above investigations, we intend to design a feasible mechanism to mitigate the present shortcomings. In this article, we introduce *HeartPrint*, a noncontact and passive continuous user authentication system that can verify multiple users simultaneously by sensing their heartbeat motions via a single mmWave radar. Specifically, we have the following considerations.

1) *Comparable Authentication Accuracy:* Existing radio frequency (RF)-based multiuser authentication solutions leave an unimpressive accuracy, which is mostly due to the fixed signal frequency used. To improve it, we adopt frequency-modulated mmWave to precisely distinguish different users, thereby providing accurate authentication for multiple users which is comparable to the state-of-the-art works.
2) *No Separation Distance Requirement:* Previous studies typically require about 1-m distance between users as to separate signals from one to another. By leveraging mmWave's high range resolution property, our system can still work effectively even when individuals are in close proximity to one another. This capacity may reduce deployment costs since more people can be detected per unit of area.
3) *Effortless and Secure:* It is expected that no proactive user engagement is needed during the authentication process. The anticipation is in keeping with the design goal of a smart environment, where more functionalities are performed by the infrastructure itself, rather than depending on people. Since heartbeat activity is naturally occurring and involuntary, *HeartPrint* does not need any physical efforts from users. Besides, compared with the traditional biometrics (e.g., voice and gait), heartbeats are more difficult to be counterfeited for spoofing attacks.

Technical Challenges: Achieving the proposed system requires us to overcome several challenges.

1) RF reflections from different users pile up and interfere over the wireless channel, the interference becomes intense as users come close by. To isolate signals reflected off different users who are close to each other, we employ a clustering method to find the users and concentrate on each of them separately. Note that the mmWave radar we deploy is able to detect multiple targets which are at least 3.75 cm apart, this means that even if users are shoulder to shoulder, we can still distinguish the chest vibrations due to different heartbeats.
2) Heartbeats are subject to body motions, such as hand and limb movements that would overpower the minor skin vibrations produced by heartbeats. To eliminate such interference on heartbeat signals, we calculate the signal energy for a given time interval and use the signal's historical average as the threshold to determine those large-amplitude movements.
3) To effectively verify different users, inherent features that are capable of representing user-specific heartbeats are urgently needed. We do this by combining wavelet packet transform (WPT) and recursive feature elimination (RFE) techniques to select the most informative features from the signals. Following that, we train a machine-learning-based model by using the selected features to make decisions for users in the environment.

In this work, we show the feasibility of employing heartbeat biometrics to contentiously and simultaneously verify multiple users in a noncontact and passive way. The system can be used in entrance control, access control, and tailgate detection applications. Smart homes can deploy the system for allowing users to perform identity-based operations, such as parental control and online payment. Traditional one-time authentications can be further extended to enable liveness detection capability with our system.

In sum, we have the following contributions in this article.

1) We present a continuous authentication system that can verify multiple users simultaneously with a single mmWave radar. Our system verifies users in a contactless and inconspicuous way by sensing their distinctive heartbeat motions. This method will be promising in shifting the current authentication paradigm toward more leak-proof and convenient.
2) We develop a feature selection pipeline for heartbeat signals that first uses WPT to decompose the signal and extracts elaborated statistical features from the decomposed coefficients, then adopts RFE to select the most representative features. We show how choosing the appropriate amount of features to achieve both high accuracy and low false positive rate.
3) We conduct extensive evaluations with 37 participants in our experiment. The results demonstrate that our system is robust to contextual changes and resilient against spoofing attacks.

II. Background and Rationale

In this section, we provide the background on the physiology of cardiac activity and the rationale behind authenticating users by sensing skin vibrations induced by the heartbeat. We also present the attack scenarios that might potentially jeopardize our system.

A. Heartbeat-Based Biometrics

Heartbeat motion refers to the pattern of contraction (i.e., systole) and relaxation (i.e., diastole) of the heart during one cardiac cycle [11]. When the heart beats, it circulates blood through systemic circuits of the body. As shown in Fig. 1(a)–(c), the heartbeat cycle consists of three main

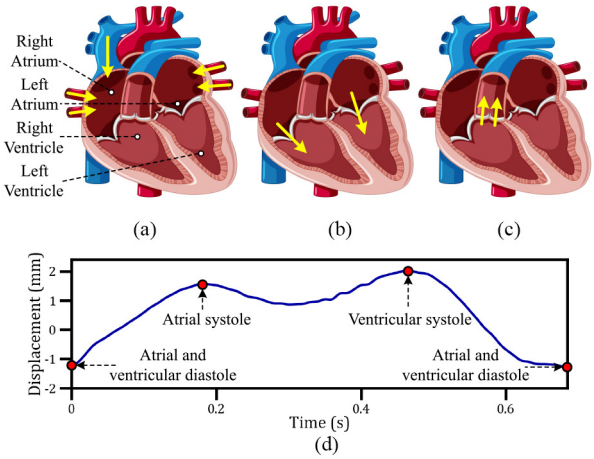

Fig. 1. Heartbeat motion cycle. (a)–(c) Heartbeat mechanism and (d) corresponding variations captured by mmWave.

phases [14]: 1) atrial and ventricular diastole phase; 2) atrial systole phase; and 3) ventricular systole phase. In particular, heart chambers first relax and fill with blood, atria then contract and blood is pumped into ventricles, ventricles finally contract and push blood out of the heart. Due to the intricate and diverse physiology of the human body, such as cardiac volume and muscle strength, the heartbeat cycle phases vary from person to person. Existing studies have also verified the uniqueness of heartbeat motions [15], [16]. Besides, since cardiac movement is inherently associated with the structure and regulation of the heart, it is difficult to forge the biometrics for conducting spoofing attacks. Therefore, we exploit the heartbeat motion as a unique biometric factor for user authentication.

B. Sensing the Heartbeat Motion

In this article, we present a noncontact approach for sensing heartbeat motion by a mmWave radar. The basic principle behind it is to detect fluctuations in skin surface vibration caused by heartbeat activities. Specifically, the mmWave sensor emits frequency-modulated continuous wave (FMCW) toward the user, the reflected signals are then regulated by skin vibrations due to heartbeat and received by the sensor.

In our context, we utilize the intrinsic ranging capability of FMCW and massive MIMO of the radar to isolate multiple users in the environment. For each user, we calculate the phase changes of the reflected signals to measure the small-scale body surface movements produced by the heartbeat. When it vibrates a distance δd, the phase change $\delta\phi$ between sequential measurements is calculated as [17]

$$\delta\phi = \frac{4\pi}{\lambda}\delta d \tag{1}$$

where λ is the wavelength of transmitted FMCW. It is observed from (1) that a shorter wavelength of the emitted wave gives rise to a higher displacement resolution for the same phase change. As a result, we implement 77-GHz high-frequency mmWave with the wavelength of around 4 mm to achieve a displacement resolution of about 1 mm, which is capable of sensing the minute skin vibrations. As shown in Fig. 1(d), the heartbeat variations are captured and identified using the configured mmWave radar.

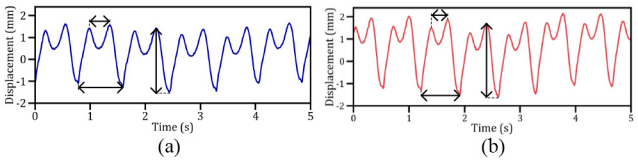

Fig. 2. Comparison of heartbeat signals captured by the mmWave radar. (a) User A's heartbeat signal. (b) User B's heartbeat signal.

C. Individual Difference in Heartbeat Motion

Due to the differences in the human physiological structure, heartbeat signals might perform distinct patterns among individuals. Although several existing studies have revealed the feasibility of using mmWave radar to estimate heart rate [18], [19], [20], they do not focus on distinguishing the minor differences in users' heartbeat motions. To validate whether it is possible to detect the subtle differences between individuals with mmWave radar, we recruit two participants to conduct an investigation. They are asked to sit facing the radar at a distance of 2 m and stay motionless. Fig. 2 shows their heartbeat motion samples. By analyzing the signals, we have the following two observations that bring the feasibility of using mmWave to capture heartbeat motions for user authentication: 1) different users have distinct signals in terms of cycle patterns, such as amplitude and width between peaks/troughs and 2) the heartbeat patterns from the same user are relatively stable for consecutive cycles. These motivate us to use high-resolution mmWave to identify the user-specific heartbeat motions for authenticating different users.

D. Threat Model

We consider an adversary explores the existing literature for social engineering attacks [21], [22] to breach the security of *HeartPrint*. In spite of the fact that heartbeat motion is more complicated and intrinsically difficult to be counterfeited than traditional biometric modalities (e.g., fingerprint and face), we take into account of the following spoofing attack scenarios to confirm its resilience. We do not consider the typical imitation attack in this study since heartbeat is a spontaneous activity that cannot be controlled or imitated [23]. Besides, we assume that the user's biometric template is secure; the security risks associated with the disclosure of biometric templates are beyond the scope of this article.

1) Arbitrary Attack: We assume that an adversary might know that heartbeat cycle trends captured by mmWave are similar between users (i.e., they have two peaks and two troughs in one cycle, as shown in Fig. 2). To subvert the system, the adversary remains in the same place as the authorized users do, attempting to use the random heartbeat events to generate the same impacts and pass through the system.

2) Signal Replay Attack: We assume that an adversary 1) knows the basic rationale of *HeartPrint* that uses mmWave to sense the skin vibration and 2) is able to tamper the internal

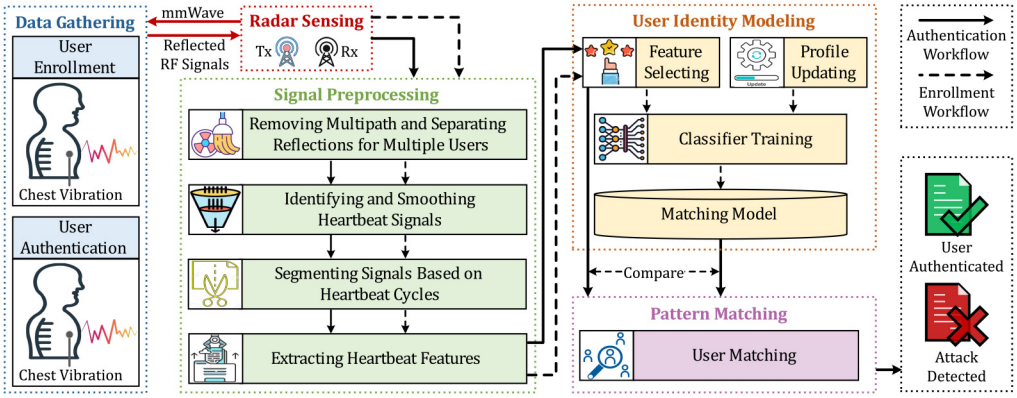

Fig. 3. System overview of *HeartPrint*. In enrollment workflow, users register their identities and the system generates a trained classifier accordingly; in authentication workflow, the trained classifier compares the input profiles derived by the user's heartbeat signal with the stored ones to determine legitimate users against spoofs.

communication of the system. To conduct the attack, the adversary places a mmWave radar in an inconspicuous place to surreptitiously record the authorized user's skin-reflected signals. Then, the adversary injects the prerecorded signals to the system in the hope of spoofing *HeartPrint*.

III. System Overview

The basic concept behind *HeartPrint* is to analyze the unique features of the captured heartbeat signals to enable continuous authentication for multiple users in complex environments. Fig. 3 depicts the workflow of *HeartPrint*, it gathers reflected signals from mmWave radar as input and generates authentication results as output. Specifically, the system consists of the following three modules.

A. Signal Preprocessing

Since the reflected RF signals captured by the radar include both signals that bounce off the users and background clutters such as reflections from walls and furniture, our system first suppresses multipath interference and separates the reflected signals from users in the environment. After isolating reflections for each user, it continues by analyzing the isolated reflections to identify heartbeat signals. Next, to apprehend the essential biometric details in a complete heartbeat cycle, we divide the time-series heartbeat signal into segments according to the cycle pattern (i.e., up-down-up-down trend). Finally, to procure representative features for heartbeat motion that can determine different users, we employ the WPT method to facilitate feature analysis by breaking the segment into a number of elementary waveforms and extracting corresponding features from them.

B. User Identity Modeling

Afterward, *HeartPrint* marks and stores the extracted features for use in building the authentication model. Considering that task-aware features might improve both model interpretability and classification accuracy, we further perform feature selection based on RFE by concluding a subset of features that offer more identifiable information rooted in heartbeat motions. The selected features are subsequently used to train a machine-learning-based matching model for user authentication. Because heartbeat rhythms may alter significantly in response to moods and exercises, *HeartPrint* also allows model updating to account for these variations.

C. Pattern Matching

During authentication, the matching model compares the new incoming heartbeat signal with the stored user biometric templates in order to determine if the user has been authenticated or whether an attack has been detected.

IV. Signal Preprocessing

As the user's heart beats, the distance from the radar to the skin surface of the human body changes slightly and regularly. *HeartPrint* estimates the heartbeat patterns by exploiting this phenomenon and extracts corresponding features to identify different users. To capture fine-grained heartbeat signals, we implement the following procedures.

A. Clutter Suppression and Signal Separation

As depicted in Fig. 4(a), we take a typical household scenario as an example to explain *HeartPrint's* operation. The device is placed in the corner of the room, where it has several users, appliances, and furniture. When the system is working, the RF signals bounce off the users, the wall, and the furniture before returning to the system. The major challenge in this step is to identify the user's reflections from the captured signals. Rather than calculating the energy loss of reflected signals [20], we present a computation-efficient method that exploits the inherent characteristic of mmWave, i.e., it is able to distinguish RX chirps reflected from different objects. For better understanding of the measurement, readers are suggested to refer to [24], [25], and [26]. Here, we just summarize the fundamental principles for object detection as follows.

When the radar detects an object at a distance of d_1, it combines the TX and the corresponding RX chirps [i.e., the green dashed line in Fig. 4(b)] to produce an intermediate

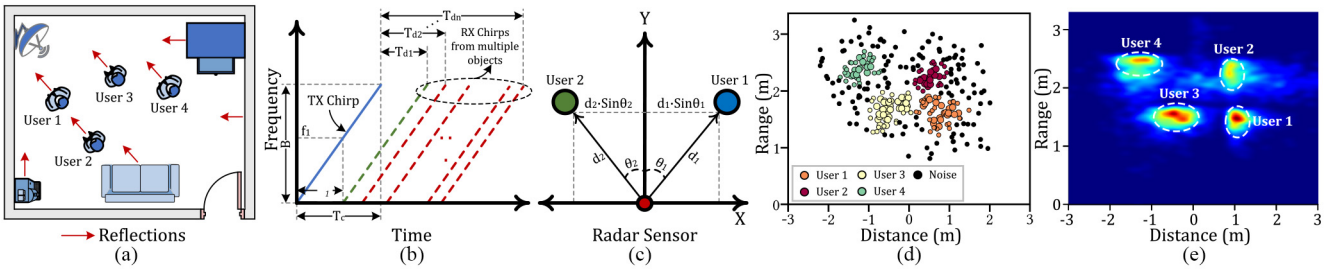

Fig. 4. Illustration of signal separation for multiple users. (a) Scenario illustration. (b) Received chirps. (c) Location measurement. (d) User clustering. (e) Signal separation.

frequency (IF) signal, which is expressed as

$$S_{\mathrm{IF}}(t) = A\sin(2\pi f_1 t + \phi_1) \tag{2}$$

where A, f_1, and ϕ_1 are the amplitude, frequency, and phase of the IF signal, respectively. Given the slope of the chirp S, f_1 can be calculated as

$$f_1 = S\tau_1 = S\frac{2d_1}{c} \tag{3}$$

where τ_1 is the time delay of the RX chirp and c is the speed of light. According to (1), ϕ_1 is $([4\pi d_1]/\lambda)$, such that we can further derive (2) into

$$S_{\mathrm{IF}}(t) = A\sin\left(S\frac{4\pi d_1}{c}t + \frac{4\pi d_1}{\lambda}\right). \tag{4}$$

As the distance of static objects is fixed, their reflected signals are constant over time. Consequently, we can have reflections only left with those from humans by eliminating such unchanging time measurements.

From (4), we also observe that the radar generates different signals for multiple objects at different distances. As illustrated in Fig. 4(b), the RX chirps are separated by a different amount of time delay (i.e., T_{dn}) which is proportional to the distance from the radar to the object. In this case, a Fourier transform is used to process the signal consisting of multiple tones, resulting in a frequency spectrum with discrete peaks for each tone, each peak indicating the presence of an object at a certain distance. Further, on the basis of the Fourier transform theory, frequency components can be separated as long as their frequency difference δf is more than $(1/[T_c])$ Hz, where T_c is the chirp duration [25]. By using (3), the relationship is represented as

$$\delta f = S\frac{2\delta d}{c} > \frac{1}{T_c}. \tag{5}$$

Since the chirp bandwidth $B = ST_c$, the range resolution δd for separating different objects can be expressed as

$$\delta d > \frac{c}{2ST_c} = \frac{c}{2B}. \tag{6}$$

In our implementation, the configuration of our radar sensor provides a 4-GHz bandwidth, the range resolution is calculated by $(c/[2B]) = ([3\times10^8][2\times4\times10^9]) = 3.75$ cm. This indicates that chirps reflected from different objects can be distinguished if they are at least 3.75 cm apart. In our scenario, we are particularly concerned with the skin vibrations in the chest due to heartbeat. Even when users are standing abreast without spacing, our system is still able to identify the signals from different users since their chest positions are separated by arms.

Next, we split the reflections for each of the users in the environment. To separate users, only using range information is insufficient, since they might have identical ranges to the radar (i.e., $d_1 = d_2$) yet be in different directions, as shown in Fig. 4(c). We therefore introduce another horizontal distance parameter to determine the position of the user relative to the radar. For example, the horizontal distance from User 1 to the radar is calculated as $d_1\sin\theta_1$, where d_1 denotes the user's range and can be estimated by (1), and θ_1 represents the Angle of Arrival (AoA) that is measured as follows [25]:

$$\theta_1 = \sin^{-1}\left(\frac{\lambda\delta\phi_1}{2\pi l}\right) \tag{7}$$

where λ, $\delta\phi_1$, and l are the wavelength, phase change, and spacing between RX antennas, respectively. In this way, data samples from users in the environment can be presented by using both range and horizontal distance information.

Although reflections from static objects are eliminated by clutter suppression, the remaining signals may include rebound interference between users if users are close to each other. To effectively separate different users, our idea is that data points directly from users may be clustered, while those interference data between users are typically dispersed in low density. Our practice to this end is using DBSCAN [27], a density-aware clustering method that defines clusters as continuous regions of high density and identifies scattered outliers to cope with noise. In comparison to K-means, DBSCAN does not require prior knowledge of the number of clusters, which is more appropriate in our scenario where the number of users is variable. To determine its parameters, we adopt k-distance graph and grid search [28] to tune the algorithm for optimal performance. Experimentally, the parameters ε and n with the best performance are 0.3 and 10, respectively. Fig. 4(d) shows the clustering results for the users, which are represented by different colors. As shown in Fig. 4(e), we are enabled to confirm the Areas of Interest (AoI) for different users by using the determined locations after user clustering, allowing us to further analyze their signals separately.

B. Heartbeat Signal Identification and Smoothing

In this step, *HeartPrint* focuses on each user and processes the corresponding AoI to identify heartbeat-related signals.

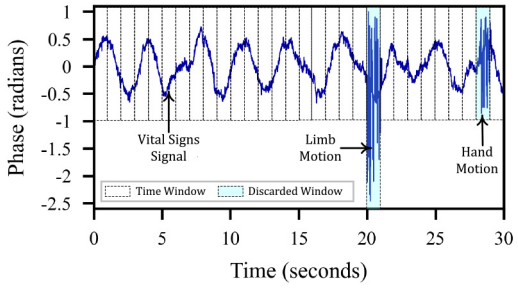

Fig. 5. Illustration of large-amplitude movements elimination.

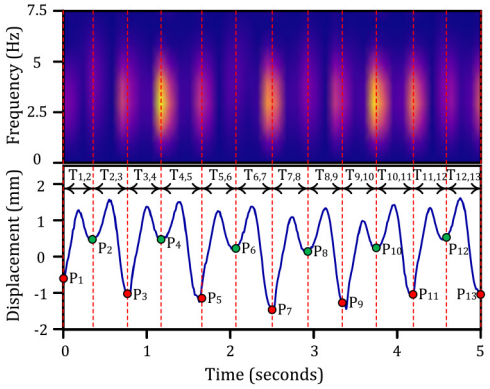

Fig. 6. Illustration of waveform trough determination.

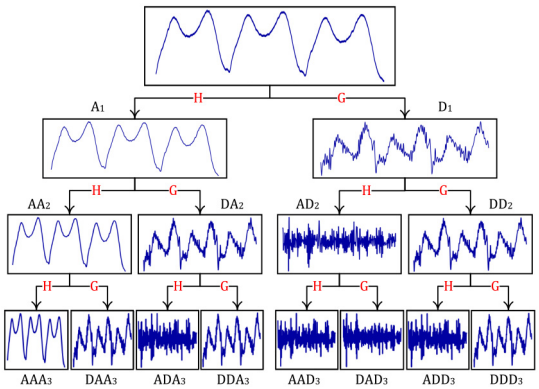

Fig. 7. WPT of heartbeat signal segment.

Since heartbeat motions are typically in the range of 0.67–3.33 Hz [29], it is intuitive to adapt a band-pass filter to sort out heartbeat components. In practice, however, people are less likely to keep still all the time, they may have hand or limb movements, such as typing on keyboard, reading books, and taking a drink. In Fig. 5, we exhibit an example when the participant moves limb and hand at different times. Compared to minute vibrations of heartbeat, such aperiodic and large-amplitude movements introduce impulse-like disturbances which are not be readily eliminated by band-pass filtering. To remove the negative impact on heartbeat signal extraction, our basic idea is to compare signal energy within a certain time window. Specifically, as shown in Fig. 5, we implement the following operations to delete those interferences.

1) We first slide a specific time window over the signal; since such movements are generally transitory, we perform the window of 1 s in the implementation.
2) For each window, we then calculate the signal's energy, i.e., $\int_t^{t+1} s^2(t)dt$.
3) Finally, we compare the energy of the current window with the signal's historical average. If its energy is sufficiently higher than the average, it is considered that the window is not dominated by the user's vital signs and discards the window. Empirically, we choose the discarded window to be at least three times than the average window energy.

After clearing irrelevant movements, we further use a Butterworth band-pass filter [30] to elicit a heartbeat signal from its frequency domain. This enables us to filter out respiration from vital signs signals as well as power-line noises.

C. Heartbeat Signal Segmentation

To simplify heartbeat signal analysis, we split the signal into smaller segments according to heartbeat cycles. As illustrated in Fig. 1(d), a typical heartbeat cycle contains two peaks and two troughs. Intuitively, we can determine a cycle by finding two consecutive troughs. Through spectral analysis [31], local troughs can be estimated, as shown in Fig. 6. However, it is observed that the points within cycles (i.e., denoted as green dots) are also identified as local troughs. To divide the heartbeat cycle correctly, we develop an interval restriction approach which is described as follows.

1) After spectral analysis, we first calculate the time intervals between the estimated points, i.e., $(T_{1,2}, T_{2,3}, \ldots, T_{n,n+1})$. We sort the interval group and find its maximum and minimum, which is represented as $(T_{\min}, T_{\text{Max}})$.
2) Then, we manually choose the first local trough point in the interval group as a valid trough, and the next valid trough P_m is determined only if the interval between the current local trough point and the previous valid trough locates in the range of $[2T_{\min}, 2T_{\max}]$.

Based on the interval restriction, we can obtain the consecutive valid troughs that divide the heartbeat signal into cycles, as denoted by the red dots in Fig. 6. Since minor differences might appear between cycles to the same user, to extract robust and comprehensive features from the segment, we use three heartbeat cycles as a segment in this work (the selection of cycle numbers is studied in Section VII-A). For instance, we use the waveform starting from P_1 to P_7 as one heartbeat segment.

D. Heartbeat Feature Extraction

Due to the dynamic nature of the heartbeat signal, it includes immediate information that are not easily apparent intuitively. To meticulously analyze heartbeat motions, we use WPT [32] as illustrated in Fig. 7. It decomposes the segment into detail (i.e., D) and approximation (i.e., A) ingredients by a high-pass (i.e., G) and a low-pass (i.e., H) filter, respectively. With

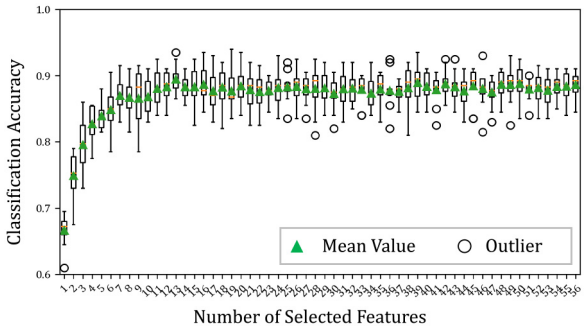

Fig. 8. Impact of different feature sets on classification accuracy.

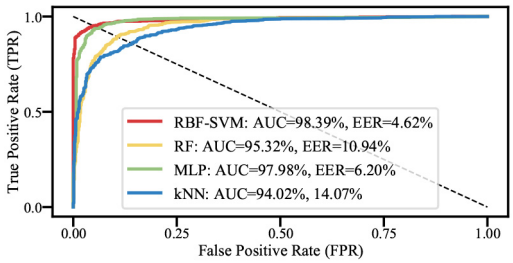

Fig. 9. Classification performance of different classifiers.

WPT, we can undertake multiresolution analysis in multiple frequency domains to acquire representative biometrics, allowing us to detect minor changes in heartbeat movements across people. In addition, existing studies [10], [33], [34] have also demonstrated the effectiveness of using WPT to analyze biometric signals.

In our implementation, we use the *db1 Daubechies* wavelet to decompose heartbeat segments into three levels, as shown in Fig. 7. By repetitiously applying the wavelet decomposition on both detail and approximation components, the 3-level WPT separates the original segment into $\sum_{i=1}^{3} 2^i = 14$ subspaces. These subspaces are distributed in different frequency bands and thus are beneficial to discovering specific features. To represent the signal in each subspace, we empirically employ four statistical metrics which are described as follows.

1) *Skewness:* It describes the symmetry of the signal, denoted as $(1/n)\sum_{i=1}^{n}([(x_i-\bar{x})^3]/\sigma^3)$.
2) *Kurtosis:* It describes the tail heaviness of the signal, denoted as $(1/n)\sum_{i=1}^{n}([(x_i-\bar{x})^4]/\sigma^4)$.
3) *Shape Factor:* It describes the smoothness of the signal, denoted as $([\sqrt{(1/n)\sum_{i=1}^{n} x_i^2}]/[(1/n)\sum_{i=1}^{n}|x_i|])$.
4) *Impulse Factor:* It describes the impulse reaction of the signal, denoted as $([\max|x_i|)/[(1/n)\sum_{i=1}^{n}|x_i|])$.

In summary, we get a total of $14 \times 4 = 56$ metrics for each heartbeat segment. They are used as the potential features for constructing the user matching model.

V. User Identity Modeling

A. Heartbeat Feature Selection

As w observe from Fig. 7, the WPT process is likely to generate the same components (e.g., ADA_3 and ADD_3), which would hence provide duplicate features. When putting the constructed matching model into production in practice, it is critical to keep the most important features, discarding the redundant and less informative ones from the potential extracted features. This is because less features means that the model becomes easier to be interpreted and faster to be trained. For this purpose, we further study the 56 retrieved features and choose the most distinctive ones that are rooted in heartbeat motions.

In particular, we use the RFE method [35] that adopts a linear kernel support vector machine (SVM) to achieve such process. To search for an optimal subset of features, RFE starts with all the 56 features in the data set and removes the low-correlated features until the desired number remains. We use fivefold cross-validation and randomly choose data from ten participants to train the classifier (details of data collection are discussed in Section VI-B). After model fitting, RFE considers the training coefficients of the classifier as importance scores for the input features. Then, it ranks the features according to their importance and drops the low-value features. This process repeats recursively until a specific set of features are determined that makes the classification reach a desired accuracy. We show the process in Fig. 8, it is observed that the accuracy is close to 90% when we choose the first 14 features; in addition, we also find that the accuracy basically remains stable even if we choose more features. The results reveal that the first 14 features are capable to represent heartbeat motions and the remaining features are not sensitive to the classification task. Based on this investigation, we decrease the number of original features to 14 and use them to construct the matching model in the following section.

B. Model Selection and Pattern Matching

In order to facilitate the deployment of the system, we expect to port our software to embedded processors (e.g., Arduino board) in future applications. In this view, we tend to employ the shallow machine-learning-based classifier to train the user matching model instead of deep learning methods since it requires less computational costs.

To construct the matching model, we compare four classifiers and choose the most appropriate one for our scenario. The four classifiers are random forest (RF), k nearest neighbors (kNN), multilayer perceptron (MLP), and radial basis function-based SVM (RBF-SVM), respectively. We implement fivefold cross-validation and grid search method [28] to tune their parameters for optimal performance. To make the comparison, we also randomly choose ten participants' data to train these classifiers (refer to Section VI-B for the details of data collection). Besides, since our data consists of multiple users (i.e., multiclass classification), we perform the one-versus-rest strategy [36] to train the classifiers.

Taking RBF-SVM as an example, we prebuild a set of potential parameters, it contains seven values which are logarithmically spaced from 10^{-3} to 10^{3}. After iterating through the parameter set, we adopt the parameters $\mathcal{C}$ and γ that perform best are 10^{-1} and 10^{-2}, respectively. In Fig. 9, we show the performance of the four classifiers in form of the average ROC curve of the ten classes (refer to Section VI-C for the

TABLE I
CONFIGURATIONS OF FMCW SIGNAL

Param.	Val.	Param.	Val.
Bandwidth	4GHz	ADC Sampling Rate	2.5M/s
Chirp Slope	53MHz/μs	Chirp Repetition	184μs
Chirps per Frame	128	Samples per Chirp	128

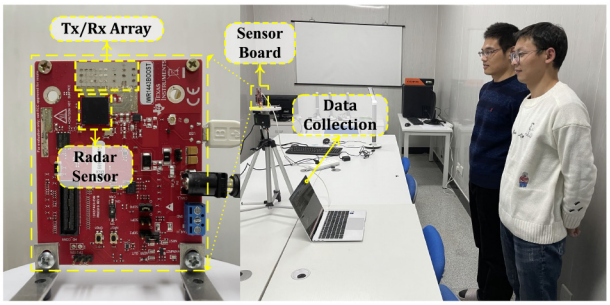

Fig. 10. Evaluation setup for heartbeat motion sensing.

details of the ROC curve), it is observed that RBF-SVM's two performance metrics [i.e., AUC and equal error rate (EER)] are the best among the four classifiers. As a consequence, we adopt SVM-RBF as the user pattern matching model in our implementation.

VI. Evaluation Preparation

A. System Setting

We conduct experiments with a commercial off-the-shelf IWR1443BOOST mmWave radar [37], it has three TXs and four RXs. The use of multiple antennas is beneficial to identify different users in a complex environment. In our high-resolution application, we need to make sure that the chirps emitted by the radar can capture the skin vibration produced by heartbeat. For this purpose, we delicately configure the FMCW signal as listed in Table I. It enables a range resolution of 3.75 cm (i.e., it is able to distinguish nearby adjacent objects which are at least 3.75 cm apart), and a displacement resolution of 1 mm (i.e., it has the ability to detect vibrations that are as small as a millimeter). Fig. 10 shows the evaluation setups, the sensor board emits signals toward the users and collects their reflected data. Then, the board performs a fast Fourier transform (FFT) on the collected data to obtain the corresponding range profiles which are subsequently transmitted to the laptop for further analysis. The laptop is equipped with an Intel Core i7-10700 CPU @ 2.90 GHz. We open-source the core code of our system as well as the processed data sets at https://github.com/Duby0112/HeartPrint.

B. Data Acquisition

To validate the feasibility and effectiveness of *HeartPrint*, we collect data from legitimate users and the attack scenarios that are described in Section II-D. The details are as follows.

1) Legitimate Data Collection: We enlist the help of 54 healthy participants (i.e., no heart-related diseases) ranging in age from 19 to 35 years old to evaluate the performance of *HeartPrint*. Participants are informed that their data is only used for biometric authentication experiments. We collect data in a typical office setting as shown in Fig. 10, which includes appliances, furniture, and walls. Each participant is asked to stand facing the device at a distance of 2 m and keep relaxed without any constraints, they are free to move hands and limbs. This default setting is used unless stated otherwise. For each participant, we record the data for around 30 min in total and collect 200 heartbeat segments from the recordings. To reduce the impact of fatigue on our data, the data collection is done through multiple rounds over the course of two months. Overall, we get $54 \times 200 = 10\,800$ samples to evaluate legitimate user access authentication.

2) Spoofing Data Collection: We further collect spoofing data to evaluate our system under attack scenarios. 1) *Arbitrary Attack:* We randomly ask 10 of the 54 participants to serve as victims and other 44 participants act as attackers. For each victim, every attacker randomly performs 20 heartbeat segments. A total of $44 \times 20 \times 10 = 8800$ samples are generated. *2) Signal Replay Attack:* Ten random participants are invited as victims, and we use an extra mmWave radar (i.e., the malicious device used by attackers) to collect the victim's signal. We assume that the end device of *HeartPrint* is safe, this means that the attacker does not know the specifics of our system, such as how many heartbeat cycles are there in one segment and the settings of the FMCW signal. To collect data, we use the factory configuration of the FMCW signal to record heartbeat motion for 10 min on each victim, then divide the signal into 5-s segments. In total, we obtain $10 \times ([10 \times 60]/5) = 1200$ samples.

C. Performance Criterion

We use the following criterions to evaluate *HeartPrint*.

1) *Authentication Accuracy:* The proportion of legitimate samples that have been correctly classified. A greater authentication accuracy means that the system is more likely to accept legitimate users.
2) *Attack Success Rate:* It represents the percentage of attack instances that the system falsely accepts. A lower attack success rate means that the system can more effectively detect spoofing attacks.
3) *ROC Curve:* The receiver operating characteristic (ROC) curve is used to illustrate the performance of a classifier at all discrimination thresholds. It plots out the attack detection rate (i.e., true positive rate) and false alarm rate (i.e., false positive rate) for every possible decision cutoff between 0 and 1 for a classifier. A larger area under the ROC curve (AUC) indicates that the system is performing better.
4) *Equal Error Rate:* The EER is an indicator of biometric performance used to determine the thresholds for false positive rate and false negative rate. The indicator implies that the ratio of false positives is equal to the ratio of false negatives. A system with lower EER is considered to be more accurate.

VII. Performance Evaluation

A. Performance of Legitimate User Authentication

In this section, we first investigate the number of heartbeat cycles in the data segment that gives the best performance.

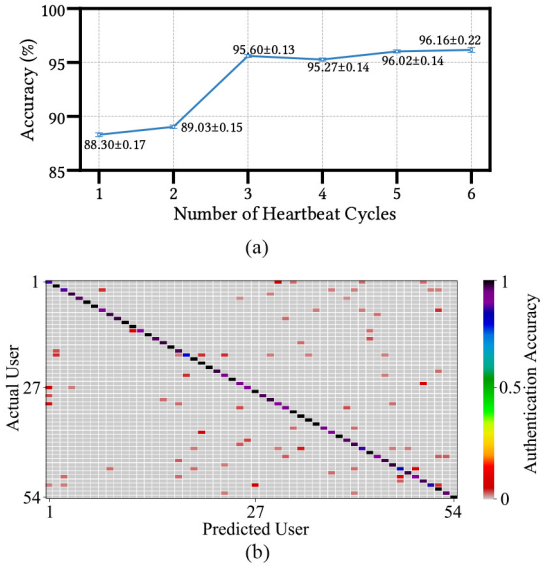

Fig. 11. Performance of legitimate user authentication. (a) Authentication accuracy with different heartbeat cycles. (b) Confusion matrix for single-user identification.

Specifically, we continuously increase the heartbeat cycles from 1 cycle to 6 cycles at a step size of 1 cycle and construct the corresponding matching models. Fig. 11(a) shows the average authentication accuracy with different heartbeat cycles, where the error bars are the standard deviation (STD) of accuracy among 54 participants. It is observed that the average accuracy is improved from 88.30% to 95.60% with an increase of more than 7% when the heartbeat cycles are raised from 1 to 3. In addition, the STD decreases slightly with more heartbeat cycles. However, when the heartbeat cycles are greater than 3, the performance is not improved significantly. The average accuracy of 95.27%, 96.02%, and 96.16%, and the STD of 0.14%, 0.14%, and 0.22% are for 4 cycles, 5 cycles, and 6 cycles, respectively. Accordingly, 3 cycles per data segment is the optimal choice in our implementation, and the average accuracy of more than 95% confirms the effectiveness of *HeartPrint* in authenticating legitimate users.

We further validate the performance of identifying a single user when using three heartbeat cycles for the data segment. Fig. 11(b) shows the confusion matrix for identifying each individual participant. The identification accuracies of the 54 participants are presented in sequence along its diagonal. The darker the color along the diagonal axis, the higher the identification accuracy. The results validate that our system is effective to identify individuals.

B. Performance of Attack Defense

In this section, we evaluate the ability of our system to resist the spoofing attacks described in Section II-D. Results are shown in Fig. 12.

Arbitrary Attack: From Fig. 12(a), we observe that the success rates of arbitrary attack for the ten victims are all less than 2%, with mean value of 1.36% and STD of 0.32%. Low STD indicates that the attack success rate for each individual tends to be clustered around the mean value. In terms of the ROC

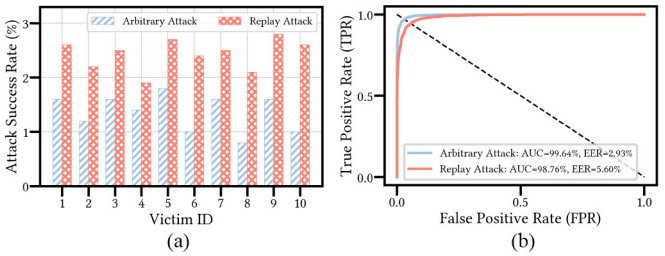

Fig. 12. Performance under spoofing attacks. (a) Attack success rate. (b) ROC curves.

curve, as shown in Fig. 12(b), the AUC and EER are 99.64% and 2.93%, respectively. The results indicate that *HeartPrint* is effective in distinguishing legitimate users from arbitrary attacks. This is expected since heartbeat motions between individuals are nearly impossible to be identical as we stated in Section II-A. The slight attack success rate in this experiment is due to our massive trial-and-error approach, i.e., we have close to 10 thousand attack samples for this experiment, it means attackers have nearly 10 thousand attempts to spoof our system. If given limited trials in practice, our system possesses the adequate capability to deny arbitrary attacks.

Replay Attack: As shown in Fig. 12(a), the success rates of signal replay attack for the ten victims are all less than 3%, with 2.43% mean value and 0.27% STD. The results show that the system still remains strong resilience against more advanced signal replay attacks. Additionally, the AUC of 98.76% and EER of 5.60% further evidence that, even if attackers spend considerable effort capturing signals from the legitimate users and snooping on their communications with the system, our system is still effective to discriminate the counterfeit samples. This is because attackers lack particular knowledge of *HeartPrint*, such as the FMCW chirp configuration that is adopted in our implementation and how many heartbeat cycles are there in one data segment, our system retains its resilience as validated by the results. Moreover, it is not trivial to launch such replay attack on *HeartPrint* in practice, since it requires solid background techniques, including communication eavesdropping, information injection, signal modulation, etc.

It is worth noting that our system is innately immune to imitation attacks, since heartbeat is an involuntary activity that can hardly be controlled or imitated [23]. In contrast, some prior biometric-based schemes which rely on gait [38], respiration [10], and human behavior [12] are susceptible to such attacks, where attackers may spoof the authentication system by impersonating the actual individual with their observations and understanding.

C. Performance With Diverse Factors

To ensure user experience, our system should be resistant to various changes in real life. In this section, we evaluate the authentication accuracy of *HeartPrint* under multiple impact factors. The experiments below follow the settings in Table II. The default settings are used unless stated otherwise.

TABLE II
EXPERIMENT SETTINGS

Factor	Range	Default
Distance	1 - 4 meters	2 meters
Number of Users	1 - 4 users	1 user
User Orientation	Front, Back, Left, Right	Front
Device Angle	-60°- 60°	0°
Body Motion	Static, Typing, Driving, Speaking	Static
Body Posture	Standing, Sitting, Lying	Standing

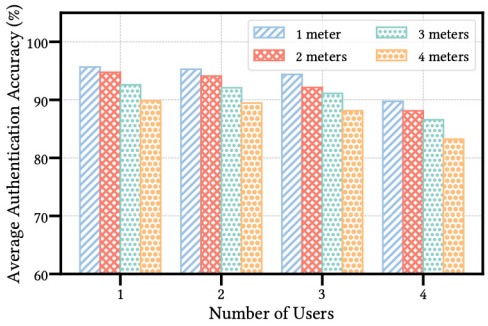

Fig. 13. Impact of multiple users with different distances.

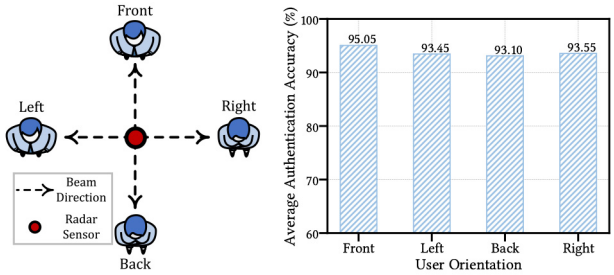

Fig. 14. Authentication performance with different user orientations. (a) Illustration of user orientation to the device. (b) Result of different user orientations.

Impact of Multiple Users With Different Distances: We first test *HeartPrint* with up to four users at distances ranging from 1 to 4 m. We randomly recruit 1 (as a control group), 2, 3, and 4 users from the participants to stand side by side at a distance of 1, 2, 3, and 4 m from the radar, respectively. We conduct ten studies with different groups of people and collect 200 segments from each user. The average authentication accuracy is shown in Fig. 13. We observe that the accuracy reaches up to 90% when the number of users is less than 3 and the sensing distance is within 3 m. Within 4 m, the accuracy is approaching to 90% as the number of users extends to 4. The results show that *HeartPrint* is capable of authenticating different users concurrently within a certain distance. In addition, we also notice that the authentication performance is affected when the number of users or the distance increases. This is owing to the mmWave's quick attenuation, and it might be further enhanced by configuring beamforming settings and expanding heartbeat cycles.

Impact of User Orientation: To verify that *HeartPrint* works well even when users are not directly facing it, we undertake

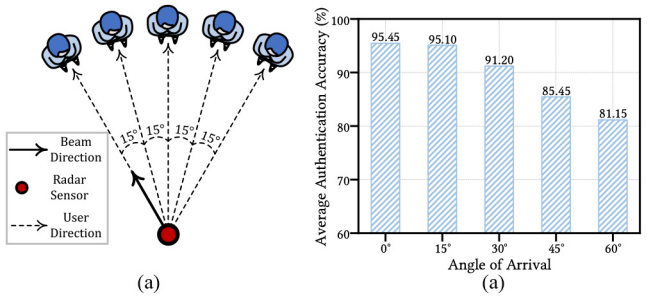

Fig. 15. Authentication performance with different AoAs. (a) Illustration of different AoAs. (b) Result of different AoAs.

studies in which we urge the participants to position themselves in different directions with regard to the device. As illustrated in Fig. 14(a), we randomly ask ten participants to perform four distinct orientations to the device: facing the device (Front), having the back to the device (Back), and facing the device from left or right (Left/Right). Each participant provides 200 segments, and the results are shown in Fig. 14(b). We can see that the average accuracies under the four orientations are over 93% and they fluctuate slightly across all orientations. The results prove that user orientation has relatively little impact on heartbeat detection, since heartbeat motions cause skin vibrations of the body and our device can detect such vibrations from different orientations.

Impact of AoA: In the experiment, our MIMO radar has a maximum AoA of 60°. A wider angle is likely to result in weaker signals and noisier phase measurements. To study its impact on sensing performance, ten participants are invited separately to stand at angles ranging from 0° to 60° at a step size of 15° with respect to the radar's pointing direction, as illustrated in Fig. 15(a). We collect 200 segments from each participant and present the results in Fig. 15(b). It is observed that the average accuracy gradually decreases from 0° to 60°, and it achieves over 91% within 30°. Specifically, it is noted that the sensing performance is greatly affected when the AoA is approaching to the far edge (i.e., 85.45% at 45° and 81.15% at 60°). This is due to the inherent limitation of mmWave radar, i.e., phase shift is susceptible to changes in AoA, thus the estimation accuracy of phase change decays with the increasing of AoA. Based on this study, we suggest to limit the AoA to less than 30° in practical applications.

Impact of Body Motion and Posture: In this experiment, we would like to evaluate the performance throughout everyday activities, without demanding people to quit their current work at hand. Specifically, ten participants are involved, and each of them is instructed to do four kinds of motions (i.e., being static, typing on smartphone, imitating driving, and talking) and three types of postures (i.e., standing, sitting, and lying). We collect 200 segments from each participant and the results are shown in Fig. 16. From Fig. 16(a), we can see that the average authentication accuracy corresponding to the user being static and imitating driving reaches above 94%, while the accuracy for typing and talking slightly decreases to 90.15% and 91.20%, respectively. The reason behind the results is expected, for the case of driving, since limb and hand motions

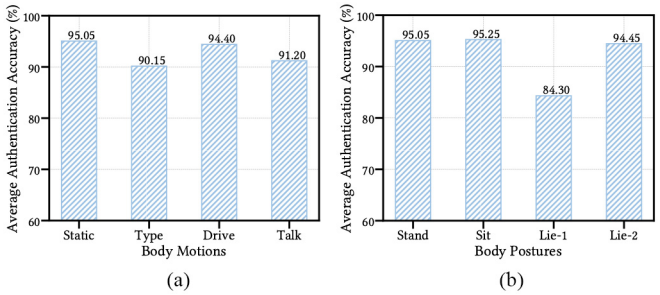

Fig. 16. Authentication performance with different body motions and postures. (a) Result of different body motions. (b) Result of different body postures.

are relatively gentle, they are likely to be identified as irregular interferences and removed by *HeartPrint* as described in the method in Section IV-B. Typing on smartphones might block signal transmission to some extent, leading to non-line-of-sight phenomenon, so it affects the performance slightly. As for talking, the vibration of vocal cords also contributes to vibrations in the skin surface, which potentially disturbs the sensing performance for heartbeat motions. Despite that, *HeartPrint* provides an acceptable performance in user authentication (all the accuracies are over 90%).

Fig. 16(b) shows the result when the user has different postures. In the figure, *Lie-1* denotes that the participant lies before the device without adjusting the pointing direction of the antennas, while in the case of *Lie-2*, we move the antennas to point to the participant lying down. We can observe that the average accuracy achieves over 94% when the user is in the pointing direction of the radar (i.e., stand, sit, and lie-2). However, the authentication accuracy drops to 84.30% in the case of *Lie-1*. This is because the user forms an angle with the device in this situation, and as we analyzed in the paragraph *Impact of AoA*, larger AoA might weaken the sensing performance. This could be alleviated by deploying devices with different pointing directions according to different environments. For example in a bedroom environment, it is appropriate to install the device that is pointing to the bed surface.

VIII. Related Work

In this section, we summarize previous related works in the following areas.

Continuous User Authentication: Most conventional biometric user authentications, such as fingerprint [42], iris recognition [43], and facial identification [44], give just a one-time verification at the start of a login session, which is susceptible to counterfeits. In order to repair this security flaw, behavior-based continuous authentications are investigated. For example, user's unique walking pattern is served as a behavioral biometric modality for continuous authentication (e.g., Zeng *et al.* [13] and Yang *et al.* [38]). Ali *et al.* [9] exploited keystroke dynamics, especially the distinctive formation and direction pattern that the hands and fingers move when typing, to recognize user's keystrokes, which can be readily applied to biometric authentications. When speaking, the vibration of vocal cords causes skin disturbance around the near-throat region, such unique vocal vibrations have also been explored for continuous authentication by Li *et al.* [41]. Besides, some studies utilize the interaction of a finger touching on a physical surface for user authentication, e.g., dynamic finger vibrations [21] and fingerprint-induced sonic effect [45]. Although these literature provide brilliant solutions for continuous authentication, they necessitate user's ongoing and active interaction with the system, which is conspicuous and inconvenient in practical applications.

Vital Sign-Based User Authentication: Vital signs are used to find unobtrusive and idiosyncratic passive authentication procedures in order to overcome the above limits. Lin *et al.* [46] designed a cancelable biometric authentication system by using the phenomenon of brain reactions to visual stimuli. The multilead electrocardiogram (ECG) biosignals are the most investigated biometric indicators in continuous user authentication scenarios (e.g., Arteaga-Falconi *et al.* [47] and Zhao *et al.* [48]). Since ECG signal acquisition is complicated, another cardiac-related physiological identifier photoplethysmogram (PPG) is proposed to improve usability [39]. However, these studies have the limitations of requiring users to wear a skin-contact accessory, which is cumbersome and limits their real-world applications. To implement a noncontact solution, RF signals have been focused to sense human vital signs for continuous authentication. For instance, *Cardiac Scan* employs a continuous wave radar to monitor heartbeat motion and verify users according to their unique heart activity patterns [11]. *BreathID* derives user-specific breathing signals from the WiFi signals to passively authenticate valid users in a noncontact way [10]. Nonetheless, these solutions either require a specific device or the effective sensing distance is limited, greatly minimizing their application possibilities.

Comparison of Related Work: Table III presents the comparison between our work and some of the existing works. From the table, we find that RF signal-based works have at least two benefits for usability compared to sensor-based approaches, 1) they free users from active involvement during the authentication procedure and 2) they enable continuous authentication in a contactless and unobtrusive manner, i.e., no longer requiring special apparatus (e.g., camera and microphone) to be attached to the body. Furthermore, among the RF-based works, the most related study to ours is *Cardiac Scan* [11], in which the authors deploy a continuous-wave radar to capture the unique heart motion for user authentication. The following are the prominent features that set this work apart from ours.

1) Due to different sensing mechanisms, *Cardiac Scan* can detect only one user at a time within the range of 2 m, whereas our system is able to authenticate several users simultaneously with a wider sensing range.
2) To suppress clutters caused by body movements, *Cardiac Scan* applies two radars to detect the user from the front and the back of the body. We use a single radar in our setting and propose an interference elimination approach for removing motion-corrupted segments from the signal, making the deployment of our system more cost efficient.

TABLE III
COMPARISON BETWEEN DIFFERENT SYSTEMS

Work	Modality	Sensing Mechanism	Effective Distance	Number of Subjects	User Involvement	Multi-user	Authentication Accuracy
BreathID [10]	Respiration	WiFi	2m	20	No	No	95%
MultiAuth [12]	Behavior	WiFi	N/A	15	No	Yes	87.60%
WiWho [13]	Gait	WiFi	N/A	20	No	Yes	92%
Wang et al. [33]	Heartbeat	Accelerometer	Contact	20	Yes	No	96.49%
FaceHeart [39]	PPG	Camera	Contact	18	Yes	No	97.51%
BreathPrint [40]	Respiration	Microphone	2cm	10	Yes	No	94%
Cardiac Scan [11]	Heartbeat	Continuous wave radar	2m	78	No	No	98.61%
VocalPrint [41]	Vocal vibration	mmWave radar	2m	41	No	No	96%
MU-ID [38]	Gait	mmWave radar	N/A	10	No	Yes	97%
Ours	**Heartbeat**	**mmWave radar**	**4m**	**54**	**No**	**Yes**	**95.60%**

3) To define heartbeat signals, *Cardiac Scan* adopts intricate fiducial-based descriptors to represent heartbeat features, while our system employs generic WPT technique and regular statistical metrics to describe heartbeat signals. The simplicity of our work signifies that it can be effortlessly conducted by people who have little or even no signal processing background knowledge. With these exclusive traits, we contribute a completely different kind of continuous user authentication solution.

IX. DISCUSSION

In this section, we discuss the potential limitations and propose possible ways to further improve *HeartPrint*.

Exercising and Health Condition: In this work, we train the matching model with the heartbeat data that are collected from healthy participants under normal physical conditions. Users who just finish exercising, have strong mood swings, or suffer from heart-related troubles (e.g., arrhythmia) might have considerable variations in heartbeat motion, thereby the authentication is likely to lose effectiveness. Such context-related shortcomings are also present in other biometric-based solutions. For example, face authentication fails when a mask is worn, and iris recognition is incompatible with persons who have eye disorders. To increase the practicability of *HeartPrint*, one feasible approach is to conduct a longitudinal study, which involves collecting data from possible contexts and studying how sensitive our system is to such changes. For instance, we may analyze how quickly the user's heart rate returns to normal after exercise and utilize the heartbeat recovery rate as one of the features in pattern matching.

Quasistatic State: Our system needs users to maintain a quasistatic state during authentication, e.g., typing and drinking without making significant body movements. This limitation is a common problem for wireless sensing, it is because phase changes induced by full-body movements would typically submerge those created by heartbeats, leading to the failure of tracking small skin vibrations. Honestly, it is not a trivial task to mine the submersed signal due to its low signal-to-noise ratio (SNR). To apply our system into full-body movement scenarios, one possible way is to perform intermittent authentication, i.e., users are required to stop their ongoing activities for authentication once in a while.

Movements From Other Objects: In this article, we use the intrinsic property of FMCW to distinguish different moving objects. It then examines the reflect signal from each moving object to identify heartbeats. Due to the difference in movement frequency, e.g., the periodicity of heartbeats is generally smaller than fans, our system separates such moving objects from a human. Even if *HeartPrint* misidentifies an object as a human, e.g., a wall-mounted clock whose frequency (1 Hz) is probably close to the heartbeat, it has no effect on the heartbeat sensing since the clock's position is fixed and its signals are isolated by FMCW. However, our system is likely to presume a pet as a user in the region, as it might have similar vital signs frequency to human's and its position is dynamic. To mitigate this problem, we can make a more detailed investigation of heartbeat frequencies for system users and their pets and calibrate the system's band-pass filter to be more fine-grained.

X. CONCLUSION

In this article, we propose *HeartPrint*, a system that tracks heartbeat motions for continuous user authentication. To authenticate multiple users concurrently, we employ a 77-GHz mmWave radar to separate different users and analyze their respective reflected signals due to heartbeat. We show the feasibility that heartbeat signals can be used as a robust identifier for user authentication and propose an interference elimination method to remove the effects of hand and limb movements on heartbeat signals. To accurately verify legitimate users, we conduct in-depth studies to determine the appropriate data segment and its corresponding features, as well as the matching model. We implement extensive experiments to evaluate the performance under spoofing attacks and application scenarios. The results show that our system is resilient to spoofing attacks and effective to verify multiple users. We make efforts to authenticate regular users in this article. In future work, we hope to improve our system to adapt to people who are taking exercise and people with heart-related problems.

ACKNOWLEDGMENT

The authors would like to thank all the reviewers and editors for their very careful review of our manuscript. They would also like to thank Xiaoluan Zhang and Qianfeng Wang for their support of this article.

REFERENCES

[1] G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, "Radio frequency fingerprint identification for LoRa using spectrogram and CNN," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2021, pp. 1–10.

[2] N. Erdogmus and S. Marcel, "Spoofing face recognition with 3D masks," *IEEE Trans. Inf. Forensics Security*, vol. 9, pp. 1084–1097, 2014.

[3] Y. Wang, W. Cai, T. Gu, W. Shao, Y. Li, and Y. Yu, "Secure your voice: An oral airflow-based continuous liveness detection for voice assistants," *Proc. ACM Interact. Mobile Wearable Ubiquitous Technol.*, vol. 3, no. 4, pp. 1–28, 2019.

[4] Y. Zhang, W. Hu, W. Xu, C. T. Chou, and J. Hu, "Continuous authentication using eye movement response of implicit visual stimuli," *Proc. ACM Interact. Mobile Wearable Ubiquitous Technol.*, vol. 1, no. 4, pp. 1–22, 2018.

[5] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Looks like eve: Exposing insider threats using eye movement biometrics," *ACM Trans. Privacy Security*, vol. 19, no. 1, pp. 1–31, 2016.

[6] Y. Wang, W. Cai, T. Gu, and W. Shao, "Your eyes reveal your secrets: An eye movement based password inference on smartphone," *IEEE Trans. Mobile Comput.*, vol. 19, no. 11, pp. 2714–2730, Nov. 2020.

[7] Y. Song, Z. Cai, and Z.-L. Zhang, "Multi-touch authentication using hand geometry and behavioral information," in *Proc. IEEE Symp. Security Privacy (SP)*, 2017, pp. 357–372.

[8] J. Kim and P. Kang, "Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features," *Pattern Recognit.*, vol. 108, Dec. 2020, Art. no. 107556.

[9] K. Ali, A. X. Liu, W. Wang, and M. Shahzad, "Keystroke recognition using WiFi signals," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw. (MOBICOM)*, 2015, pp. 90–102.

[10] J. Liu, Y. Chen, Y. Dong, Y. Wang, T. Zhao, and Y.-D. Yao, "Continuous user verification via respiratory biometrics," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2020, pp. 1–10.

[11] F. Lin, C. Song, Y. Zhuang, W. Xu, C. Li, and K. Ren, "Cardiac scan: A non-contact and continuous heart-based user authentication system," in *Proc. 23rd Annu. Int. Conf. Mobile Comput. Netw. (MOBICOM)*, 2017, pp. 315–328.

[12] H. Kong *et al.*, "MultiAuth: Enable multi-user authentication with single commodity WiFi device," in *Proc. Int. Symp. Theory Algorithmic Found. Protocol Des. Mobile Netw. Mobile Comput. (MOBIHOC)*, 2021, pp. 31–40.

[13] Y. Z. Zeng, P. H. Pathak, and P. Mohapatra, "WiWho: WiFi-based person identification in smart spaces," in *Proc. ACM/IEEE Int. Conf. Inf. Process. Sens. Netw. (IPSN)*, 2016, pp. 1–12.

[14] J. Kranjec, S. Beguš, G. Geršak, and J. Drnovšek, "Non-contact heart rate and heart rate variability measurements: A review," *Biomed. Signal Process. Control*, vol. 13, pp. 102–112, Sep. 2014.

[15] A. Fratini, M. Sansone, P. Bifulco, and M. Cesarelli, "Individual identification via electrocardiogram analysis," *Biomed. Eng. Online*, vol. 14, no. 1, pp. 1–23, 2015.

[16] B. H. Kim and J. Y. Pyun, "ECG identification for personal authentication using LSTM-based deep recurrent neural networks," *Sensors*, vol. 20, no. 11, p. 3069, 2020.

[17] C. Xu *et al.*, "Waveear: Exploring a mmWave-based noise-resistant speech sensing for voice-user interface," in *Proc. 17th Annu. Int. Conf. Mobile Syst. Appl. Serv. (MOBISYS)*, 2019, pp. 14–26.

[18] A. Ahmad, J. C. Roh, D. Wang, and A. Dubey, "Vital signs monitoring of multiple people using a FMCW millimeter-wave sensor," in *Proc. IEEE Radar Conf.*, 2018, pp. 1450–1455.

[19] H. Lee, B.-H. Kim, J.-K. Park, and J.-G. Yook, "A novel vital-sign sensing algorithm for multiple subjects based on 24-GHz FMCW doppler radar," *Remote Sens.*, vol. 11, no. 10, p. 1237, 2019.

[20] Z. Yang, P. H. Pathak, Y. Zeng, X. Liran, and P. Mohapatra, "Vital sign and sleep monitoring using millimeter wave," *ACM Trans. Sens. Netw.*, vol. 13, no. 2, pp. 1–32, 2017.

[21] J. Liu, C. Wang, Y. Y. Chen, and N. Saxena, "VibWrite: Towards finger-input authentication on ubiquitous surfaces via physical vibration," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, 2017, pp. 73–87.

[22] J. Li, K. Fawaz, and Y. Kim, "Velody: Nonlinear vibration challenge-response for resilient user authentication," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2019, pp. 1201–1213.

[23] F. Dela, K. J. Mikines, M. Von Linstow, and H. Galbo, "Heart rate and plasma catecholamines during 24 h of everyday life in trained and untrained men," *J. Appl. Physiol.*, vol. 73, no. 6, pp. 2389–2395, 1992.

[24] S. Rao, *Introduction to mmWave Radar Sensing: FMCW Radars*, Texas Instrum., Dallas, TX, USA, 2020, pp. 1–70.

[25] C. Iovescu and S. Rao, *The Fundamentals of Millimeter Wave Sensors*, Texas Instrum., Dallas, TX, USA, 2017, pp. 1–8.

[26] S. Yue, H. He, H. Wang, H. Rahul, and D. Katabi, "Extracting multi-person respiration from entangled RF signals," *Proc. ACM Interact. Mobile Wearable Ubiquitous Technol.*, vol. 2, no. 2, pp. 1–22, 2018.

[27] X. Shuai, Y. Shen, Y. Tang, S. Shi, L. Ji, and G. Xing, "milliEye: A lightweight mmWave radar and camera fusion system for robust object detection," in *Proc. Int. Conf. Internet Things Des. Implement.*, 2021, pp. 145–157.

[28] I. Syarif, A. Prugel-Bennett, and G. Wills, "SVM parameter optimization using grid search and genetic algorithm to improve classification performance," *Telkomnika*, vol. 14, no. 4, p. 1502, 2016.

[29] F. Adib, H. Z. Mao, Z. Kabelac, D. Katabi, and R. C. Miller, "Smart homes that monitor breathing and heart rate," in *Proc. 33rd Annu. ACM Conf. Human Factors Comput. Syst.*, 2015, pp. 837–846.

[30] S. Daud and R. Sudirman, "Butterworth bandpass and stationary wavelet transform filter comparison for Electroencephalography signal," in *Proc. 6th Int. Conf. Intell. Syst. Model. Simul.*, 2015, pp. 123–126.

[31] F. Scholkmann, J. Boss, and M. Wolf, "An efficient algorithm for automatic peak detection in noisy periodic and quasi-periodic signals," *Algorithms*, vol. 5, no. 4, pp. 588–603, 2012.

[32] R. X. Gao and R. Q. Yan, *Wavelet Packet Transform*. Boston, MA, USA: Springer, 2011, pp. 69–81.

[33] L. Wang *et al.*, "Unlock with your heart: Heartbeat-based authentication on commercial mobile phones," *Proc. ACM Interact. Mobile Wearable Ubiquitous Technol.*, vol. 2, no. 3, p. 140, 2018.

[34] U. R. Acharya, S. V. Sree, A. P. C. Alvin, and J. S. Suri, "Use of principal component analysis for automatic classification of epileptic EEG activities in wavelet framework," *Expert Syst. Appl.*, vol. 39, no. 10, pp. 9072–9078, 2012.

[35] X.-W. Chen and J. C. Jeong, "Enhanced recursive feature elimination," in *Proc. 6th Int. Conf. Mach. Learn. Appl. (ICMLA)*, 2007, pp. 429–435.

[36] Y. Xue and M. Hauskrecht, "Active learning of multi-class classification models from ordered class sets," in *Proc. AAAI Conf. Artif. Intell.*, vol. 33, 2019, pp. 5589–5596.

[37] "IWR1443 Evaluation Module (IWR1443BOOST) mmWave Sensing Solution User's Guide." Texas Instruments. 2020. [Online]. Available: https://www.ti.com/tool/IWR1443BOOST (Accessed: May 19, 2020).

[38] X. Yang, J. Liu, Y. Chen, X. Guo, and Y. Xie, "MU-ID: Multi-user identification through gaits using millimeter wave radios," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2020, pp. 2589–2598.

[39] Y. Chen, J. Sun, X. Jin, T. Li, R. Zhang, and Y. Zhang, "Your face your heart: Secure mobile face authentication with photoplethysmograms," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2017, pp. 1–9.

[40] J. Chauhan, Y. Hu, S. Seneviratne, A. Misra, A. Seneviratne, and Y. Lee, "BreathPrint: Breathing acoustics-based user authentication," in *Proc. 15th Annu. Int. Conf. Mobile Syst. Appl. Serv. (MOBISYS)*, 2017, pp. 278–291.

[41] H. Li *et al.*, "VocalPrint: Exploring a resilient and secure voice authentication via mmWave biometric interrogation," in *Proc. 18th Conf. Embedded Netw. Sens. Syst. (SENSYS)*, 2020, pp. 312–325.

[42] O. Ogbanufe and D. J. Kim, "Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment," *Decis. Support Syst.*, vol. 106, pp. 1–14, Feb. 2018.

[43] H. Shahriar, H. Haddad, and M. Islam, "An iris-based authentication framework to prevent presentation attacks," in *Proc. IEEE 41st Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, 2017, pp. 504–509.

[44] R. Raghavendra, K. B. Raja, and C. Busch, "Presentation attack detection for face recognition using light field camera," *IEEE Trans. Image Process.*, vol. 24, pp. 1060–1075, 2015.

[45] A. S. Rathore *et al.*, "SonicPrint: A generally adoptable and secure fingerprint biometrics in smart devices," in *Proc. Int. Conf. Mobile Syst. Appl. Serv. (MOBISYS)*, 2020, pp. 121–134.

[46] F. Lin, K. W. Cho, C. Song, W. Y. Xu, and Z. P. Jin, "Brain password: A secure and truly cancelable brain biometrics for smart headwear," in *Proc. 16th Annu. Int. Conf. Mobile Syst. Appl. Serv. (MOBISYS)*, 2018, pp. 296–309.

[47] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, "ECG authentication for mobile devices," *IEEE Trans. Instrum. Meas.*, vol. 65, no. 3, pp. 591–600, Mar. 2016.

[48] Z. Zhao, L. Yang, D. Chen, and Y. Luo, "A human ECG identification system based on ensemble empirical mode decomposition," *Sensors*, vol. 13, no. 5, pp. 6832–6864, 2013.