Continuous User Authentication by Contactless Wireless Sensing

Fei Wang, *Student Member, IEEE,* Zhenjiang Li, *Member, IEEE,* Jinsong Han, *Senior Member, IEEE,*

***Abstract*—This paper presents BodyPIN, which is a continuous user authentication system by contactless wireless sensing using commodity Wi-Fi. BodyPIN can track the current user's legal identity throughout a computer system's execution. In case the authentication fails, the consequent accesses will be denied to protect the system. The recent rich wireless-based user identification designs cannot be applied to BodyPIN directly, because they identify a user's various activities, rather than the user herself. The enforced to be performed activities can thus interrupt the user's operations on the system, highly inconvenient and not user-friendly. In this paper, we leverage the bio-electromagnetics domain human model for quantifying the impact of human body on the bypassing Wi-Fi signals and deriving the component that indicates a user's identity. Then we extract suitable Wi-Fi signal features to fully represent such an identity component, based on which we fulfill the continuous user authentication design. We implement a BodyPIN prototype by commodity Wi-Fi NICs without any extra or dedicated wireless hardware. We show that BodyPIN achieves promising authentication performances, which is also lightweight and robust under various practical settings.**

***Index Terms*—Continuous authentication, Security awareness, Wireless sensing**

I. Introduction

MOST computer systems mainly authenticate users at the login stage. The systems then can be accessed once the authentication is successful, even the user may temporarily leave the system afterwards [1]. However, such an one-time authentication scheme could expose systems to adversaries, especially during the user's absent period as shown in Fig. 1, and cause severe security issues, such as the illegal copy of private documents, the peep of sensitive information, and malicious modifications on the system.

To defend such a crucial security issue, the concept of *continuous authentication* is proposed recently [2], aiming to keep tracking the current user's legal identity throughout the system's operation. In case the authentication is failed, *e.g.,* the legal user leaves and/or the adversary appears, the system is locked automatically. One naive way to achieve this is asking the user to periodically authenticate herself, *e.g.,* by passwords or fingerprints, but this will distract the user from normal operations, *i.e.,* highly inconvenient and not user-friendly.

Fig. 1: **System illustration**. **(left)**: Wi-Fi related biometrics are registered by BodyPIN after a legal user logs in; **(middle)**: if the user leaves, the system turns to be unaccessible; **(right)**: adversary's access is also denied.

To overcome this limitation, the *contactless sensing* based designs are widely proposed. Specifically, various sensors can be adopted to sense the user's certain biometric features [1], [3]–[9]. Then we can match them with the pre-recorded feature profiles for the authentication. As the entire process is fully *passive* to the user without any user's touch on the device, *e.g.,* no password input, the authentication thus be can continuous, without interrupting the user's operations on the system.

Following this principle, there are two main types of designs, *i.e.,* the camera-based and wireless-based solutions. For the former category, the features, like colors of the user's cloth and skin [3], the gaze moving pattern [4], and face [5] can be utilized. However, the camera-based designs suffer three obvious issues. First, due to the limited camera view angle, the user should be directly captured by the camera (without blocking) in good illumination conditions [1]. Second, systems can be easily fooled by the images/videos generated by generative adversarial networks (GANs) [10]–[12]. Third, cameras can also cause the privacy leakage issue [13]–[15] if the recorded video is not properly protected or gets hacked by adversaries. Due to these concerns, the wireless-based designs promising appear recently [1], [6]–[9]. However, the existing designs either require the user to perform certain activities [7]–[9], or a dedicated hardware design [1], [6], which could inevitably interrupt the user's operations, or increase the system deploying and maintaining costs, *i.e.,* not pervasive enough.

Motivated by these existing works, in this paper, we explore the opportunity to achieve the continuous user authentication using commodity Wi-Fi [16], without imposing any activities performed by the user. If this is viable, the solution should

This paper is partially supported by the NSFC Grant No. 61872285 and 61572396, Fundamental Research Funds for the Central Universities, and GRF grant from Research Grants Council of Hong Kong No. CityU 11217817. *(Corresponding authors: Zhenjiang Li and Jinsong Han.)*

F. Wang is with School of Computer Science, Xi'an Jiaotong University, Xi'an China. He is also with Institute of Cyberspace Research, Zhejiang University, Hangzhou China, and Shaanxi Province Key Laboratory of Computer Network. E-mail: fai.er@stu.xjtu.edu.cn.

Z. Li is with the Department of Computer Science, City University of Hong Kong, Hong Kong. E-mail: zhenjiang.li@cityu.edu.hk.

J. Han is with Institute of Cyberspace Research, School of Cyber Science and Technology, Zhejiang University, Hangzhou China. He is also with Research Institute of Cyberspace Governance in Zhejiang University, Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies, and Shaanxi Province Key Laboratory of Computer Network, Xi'an Jiaotong University, Xi'an China. E-mail: hanjinsong@zju.edu.cn.

Copyright (c) 20xx IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

be able to preserve the merits from prior wireless-based designs, largely improve the user convenience and reduce the system cost. However, the key question is that *without highly-dedicated wireless designs, whether suitable features from Wi-Fi signals exist to strongly identify a user's identity along for the continuous authentication design*. Such a requirement implies that the solution should be related to the user's biometric features directly, rather than the performed activities [7]–[9], which so far as we know has not been explored yet.

Our investigation is inspired by the existing studies from the bio-electromagnetics domain [17]–[20], which have the proper model, the layered tissue model [17], [18], to abstract the human body for understanding its interactions with the electromagnetic waves. Based on this model, we quantify the impact of our body on bypassing Wi-Fi signals and derive the component that indicates a user's identity, which is jointly determined by the user body's appearance, *e.g.,* the radius of our body's intersecting surface, and also our body's internal factors, *e.g.,* permittivity, permeability, body-fat ratio, *etc*. The component is hence highly user-dependent, which is qualified for the user authentication. To this end, we conduct an in-depth analysis and figure out a set of Wi-Fi biometrics traits from the channel state information (CSI) [21]. Based on this, we finally design a continuous authentication system, BodyPIN.

Fig. 1 shows how BodyPIN works. In Fig. 1 (left), when a legal user logs in a computer system, her Wi-Fi related biometrics features are registered for the continuous authentication. Later, when the user leaves, the Wi-Fi feature matching becomes unsuccessful and the system turns to be unaccessible, as in Fig. 1 (middle). In such a case, the system can deny the access from those who have the mismatched Wi-Fi biometrics features, as illustrated in Fig. 1 (right). Following this working flow, we develop a prototype using Intel 5300 NICs. Extensive evaluations show that it can achieve both a high true-positive (TP) rate, for the least interruption to legal users, and a low false-positive (FP) rate, for the trustful defence to adversaries. Meanwhile, the computation is light-weighted, around $300ms$, which is sufficient for the real-time authentication.

In summary, the contributions of this paper are as follows:

- We propose a continuous user authentication system, BodyPIN, using the commodity Wi-Fi signals through a contactless wireless sensing design.
- We identify the signal component that are directly related to each individual user and extract a set of suitable Wi-Fi signal features to represent it for the authentication.
- We implement a BodyPIN prototype and conduct extensive experiments for the evaluation, which demonstrates promising and robust performance.

II. Related Work

Bio-eletromagnetics. The BodyPIN design relates to the bio-eletromagnetics literatures [17]–[20]. Some human tissues, such as body muscle, kidney and liver, with different dielectric properties are measured by signals from 10Hz to 20GHz [20]. The body's absorption is studied by [17] in range of 30MHz to 6GHz, and [19] in range of 1GHz to 15GHz. In [18], an in-body electromagnetic transmit model is proposed and tested in 2.45GHz. These works validate our body could have unique impacts on wireless signals. Based on this, we further use the effective body model from this domain in the BodyPIN design.

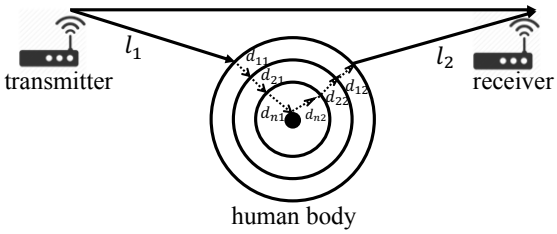


Fig. 2: The human body is modeled as a series of circles that represent different tissue layers and each layer could cause different attenuations for the bypassing Wi-Fi signals.

Biometrics based continuous authentication. Many works use behavioral biometrics for user authentication, like the manners of screen-touching [22], [23], key-typing [24] and mouse-clicking [25]. However behavioral biometrics are vulnerable to the imitation. The camera can also achieve continuous authentication, *e.g.,* sensing the user's cloth and skin [3], or the gaze moving patterns [4]. As stated in the introduction, it requires strict line of the sight and lighting conditions. More importantly, it may have severe privacy concerns about the recorded video. To overcome these issues, there are recent designs using wireless to achieve the continuous authentication, like [1], which however requires a dedicated hardware design. Compared with these existing works, BodyPIN is a wireless-based solution avoiding camera's drawbacks, while utilizes commercial Wi-Fi devices only.

Wi-Fi based human identification. There also exist many Wi-Fi-based human identification systems, *e.g.,* WiWho [8], WiFi-ID [9], FreeSense [7] and Radio-Bio [26]. However, they require the user to perform certain activities, *e.g.,* walking, as they essentially recognize users' activities, not the users themselves. Thus, these designs are not suitable for the continuous authentication, as frequently performing the required activities can easily interrupt user's normal usage of computer systems and dramatically sacrifices the user experience.

III. Impact of Human Body on Wi-Fi Signals

Existing studies have empirically demonstrated that our human body could have impacts on the electromagnetic waves, like absorption, within a certain frequency band, which covers Wi-Fi's frequencies [17]–[20]. In this section, we strive to further quantify the impact and setup the relation between the Wi-Fi signal features and each individual user's characteristics, based on which we can achieve the BodyPIN design.

To this end, we first borrow the classic human model from the bio-electromagnetics domain, as in Fig. 2, which abstracts the human body as a series of circles to represent different tissue layers [20], such as the skin, fat under the skin, muscle, fat on the viscera, viscera, bone, *etc*, and the radius of layer i is r_i, where $i \in [1, n]$ and n is the total number of layers.

As shown in Fig. 2, we denote the distances from the user to the transmitter and receiver as l_1 and l_2, respectively. Other useful notations are tabulated in Table I. According to the

Symbols	Meaning
f	Frequency of the Wi-Fi signal
A	Initial amplitude of the Wi-Fi signal
ϕ_0	Initial phase of the Wi-Fi signal
m	Total amount of propagation mediums
l_1	Distance from the transmitter to the user
l_2	Distance from the user to the receiver
d_{i1}	In-body length of Wi-Fi in the the $i^{\text{th.}}$ layer of human body
d_{i2}	Out-body length of Wi-Fi in the the $i^{\text{th.}}$ layer of human body
μ_i	Permeability of the $i^{\text{th.}}$ layer of human body
ε_i	Permittivity of the $i^{\text{th.}}$ layer of human body
μ_0	Permeability of the air
ε_0	Permittivity of the air
c_1^0	Power decay from the transmitter to the user
c_2^0	Power decay from the user to the receiver
c_i	Power decay in the $i^{\text{th.}}$ layer of human body

TABLE I: List of the mathematical symbols.

table, the initial Wi-Fi signals generated at the transmitter side, *i.e.,* X, can be mathematically written as:

$$X \quad = \quad A \cdot e^{-j \cdot 2\pi \cdot f \cdot t + \phi_0}, \tag{1}$$

where ϕ_0 is the initial phase, and A and f are the amplitude and frequency, respectively. After the signal X's transmission, both of its amplitude and phase will change.

Amplitude. During signal X's transmission, its amplitude A decays, in terms of the signal power, along the time. The amount of decayed power can be computed through the Friis transmission equation [27]. To facilitate the understanding, we omit the sophisticated intermediate steps and provide the expression of received signal amplitude A' reflected by the user as follows:

$$A' \quad = \quad A \cdot c_1^0 \cdot c_2^0 \cdot \prod_{i=1}^{n} c_i, \tag{2}$$

where c_i is the power decay due to the layer i of the user's body (Fig. 2), n is the total number of layers that reflect the signals, c_1^0 and c_2^0 represent power decays from the transmitter to the user and from the user to the receiver, respectively.

Phase. The phase changes along the time (propagation) delay, t. In particular, we consider $t = \sum_{i=1}^{m} t_i$, where m is the total amount of propagation mediums and t_i is the delayed time caused by every medium. Each t_i can be calculated by $t_i = \frac{d_i}{v_i}$, where d_i is the length of the i^{th} medium and v_i is the speed of Wi-Fi signals in this medium. The v_i can be further computed via $v_i = \frac{1}{\sqrt{\mu_i \varepsilon_i}}$, where μ_i and ε_i represent the permeability and permittivity of the transmission medium i. By combining the three equations above, we can derive the time delay from each Wi-Fi propagation medium by the summarization as follows.

$$t \quad = \quad \sum\nolimits_{i=1}^{m} d_i \cdot \sqrt{\mu_i \varepsilon_i}.$$

According to Fig. 2, the time delay t can be rephrased as:

$$t \quad = \quad \sum_{i=1}^{n} (d_{i1} + d_{i2}) \cdot \sqrt{\mu_i \varepsilon_i} + (l_1 + l_2) \cdot \sqrt{\mu_0 \varepsilon_0}, \tag{3}$$

where the former part is caused by our human body and the later part is caused by propagation over the air. Then according to the Eq. 1, Eq. 2 and Eq. 3, the reflected Wi-Fi signal copy Y, received by the receiver, can be represented by:

$$Y = \prod_{i=1}^{n} c_i e^{-j2\pi f \sum\limits_{i=1}^{n} (d_{i1}+d_{i2})\sqrt{\mu_i \varepsilon_i}} c_1^0 c_2^0 e^{-j2\pi f((l_1+l_2)\sqrt{\mu_0 \varepsilon_0})} X,$$

where $\prod_{i=1}^{n} c_i e^{-j2\pi f \sum\limits_{i=1}^{n} (d_{i1}+d_{i2})\sqrt{\mu_i \varepsilon_i}}$ is uniquely determined by each individual user.

Summary. In the equation above, the term $\prod_{i=1}^{n} c_i$ indicates that the power decays in all tissues jointly contribute to the variation in the amplitude. While the $\sum\limits_{i=1}^{n} (d_{i1} + d_{i2})\sqrt{\mu_i \varepsilon_i}$ component indicates that the permittivity, permeability and the thickness of each tissue could also have joint impacts on Wi-Fi phase, which are user-dependent. In [20], permittivity and permeability of the tissues, like the muscle, kidney, liver, *etc*, have been empirically measured. People indeed find that different tissues could cause different influences on the bypassing wireless signals. The intuition is clear — each type of the tissues has unique compositions and could thus lead to a unique change in the amplitude and phase on the Wi-Fi signals, which motivates our continuous authentication design in the next section.

IV. System Design

In this section, we elaborate the BodyPIN design. We first describe the system working flow (§IV-A), followed by the Wi-Fi based biometrics feature extraction (§IV-B) and the authentication design (§IV-C).

A. System working flow

Fig. 3 shows the working flow of the BodyPIN system. After a legal user logs into the computer system by any conventional authentication (*i.e., primary authentication*), such as passwords, fingerprints, face recognitions, *etc*., successfully, BodyPIN starts to record the Wi-Fi time series. In particular, BodyPIN processes the channel state information (CSI) from the received Wi-Fi packets, by removing identified amplitude and phase errors, to obtain desired biometric related features. These features are registered in the system and utilized to train a classifier to recognize this legal user for the continuous authentication. More precisely, the system periodically collects CSI samples to generate new Wi-Fi based features about the current user, and then matches them with the registered ones. If matched, the current user is viewed to be legal and the classifier can also be updated by the newly collected features; Otherwise, BodyPIN locks the system until the primary authentication is passed again.

Two points are worth noting: 1) BodyPIN is not positioned to replace any primary authentication methods. Hence, the user still needs to well protect their primary authentication keys, like passwords and fingerprints, in the first place. 2) The aim of the on-site feature extraction for training the classifier is to improve the authentication robustness and minimize the possibilities of the false alarm cases that could interrupt the user's normal operations.

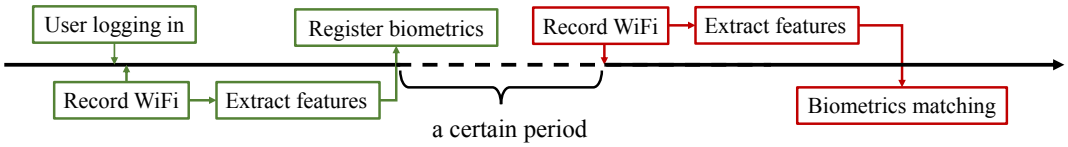


Fig. 3: System working flow. Once a legal user logs in, the Wi-Fi signals are recorded for feature extraction. The extracted biometric features are registered for continuous authentication. After a certain period, new Wi-Fi samples are recorded to match with registered ones. If matched, the current user is legal. Otherwise, BodyPIN locks the system until user logging in again.

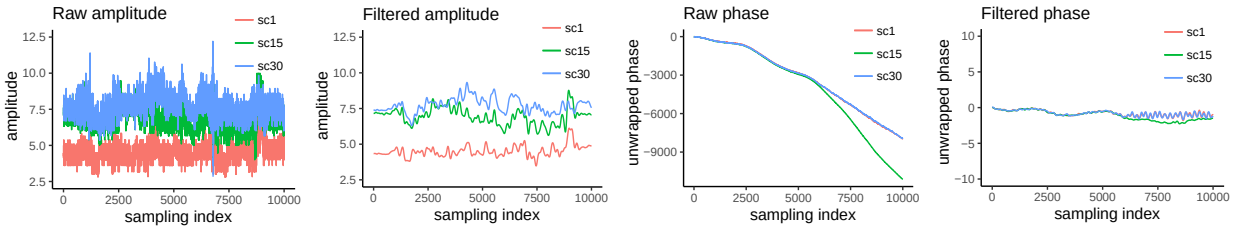


Fig. 4: Processing CSI amplitudes and angles. (a), (b): We use low-pass Butterworth filter to suppress the jitters in the CSI amplitude series. (c), (d): We compute and further filter the differences of every two continuous phases. The results are shown in (d), which are for a further feature extraction (series of the 1^{st}, 15^{th} and 30^{th} subcarrier are depicted).

B. Wi-Fi based biometric feature extraction

As suggested by the insights from the analysis in §III, we extract Wi-Fi based user's biometric features in this section. Prior to the design details, we briefly introduce the related Wi-Fi information related to BodyPIN in the following.

Channel state information. In modern computers and mobile devices [28], Wi-Fi is widely supported, *e.g.,* 802.11n/ac. The digit information delivered from the transmitter to the receiver is carried by multiple electromagnetic waves at different frequencies, where each specific-frequency band is called subcarrier, so that the orthogonal frequency division modulation (OFDM) [29] can be applied for the data transmission. Supposing the transmitter transmits X and the receiver receives it as Y after the propagation through the wireless channel H. We thus have:

$$Y \quad = \quad H \cdot X + n, \tag{4}$$

where n is for channel noise. Recently, many advanced Wi-Fi NICs can report the detailed channel state information (CSI) to describe channel H in each subcarrier level [16], [30].

Wi-Fi based features. The CSI information essentially describes the relation of Y/X. Further recalling the component marked with the wave line in the derived Y in §III, we can observe that such a component (related to properties of the user) is also obtained in the CSI information.

As the user-specific properties are highly compressed in the *amplitude* and *phase* of the CSI series, which makes it an ill-posed problem to do user continuous authentication through a two-stage schema, first parsing all user biometrics attributes including permittivity, permeability and the thickness of each tissue, then authenticating users with the parsed features. Without analytic solutions, our solution is data-driven, to record a period of CSI series, and to learn a binary classifier for authentication directly from the CSI series. Deep learning methods [31], [32] may learn this classifier from raw CSI series directly. However, due to the training and feature updating considerations, we seek to extract empirical features for CSI time series. With many prior investigations to extract features of time series from multi-modal sensory data, such as CSI [33], [34], accelerometers [35] and gyroscopes [36], in BodyPIN, we select a preliminary set of features from the CSI amplitude and phase, including *1) mean, 2) maximum, 3) minimum, 4) mean absolute deviation, (5) interquartile range, (6) root mean square, (7) skewness and (8) kurtosis*. Both amplitudes and phases of all subcarriers, *e.g.,* 30 subcarriers from Intel 5300 NICs, can be applied to these features, which lead to the feature dimensions being $8 \times 30 \times 2 = 480$.

Due to the surrounding noises and imperfection of WiFi adapter, the raw CSI, both amplitude and phase, collected by the CSI tool [16], will suffer non-negligible fluctuation as illustrated in Fig. 4 (a, c). Inspired by the related works [33], [37], we need to carefully filter the collected CSI before designing the classifier for the continuous authentication.

(1) Processing CSI amplitudes. Generally, when a user sitting before the monitor, her body movement is usually in low frequency. Owing to this, we consider the high-frequency jitters shown in Fig. 4 (a) are noises, thus, we apply a low-pass Butterworth filter (5^{th} order, 1Hz of the cut-off frequency) to filter these noises and smooth the time series of CSI amplitude [33], [37]. The filtering results are shown in the Fig. 4 (b), where the 1^{st} and the 2^{nd} subfigures are the raw amplitudes and the filtered amplitudes, respectively. We find that the filter can dramatically reduce jitters in the raw amplitude series.

(2) Processing CSI phases. The noises in the time series of the CSI phases is much different compared with amplitudes, as shown in in Fig. 4 (c), it has a decreasing slope in the sampling duration. Prior work have studied this phenomena [30], [34], [38], [39] and conclude that it is introduced by joint impacts

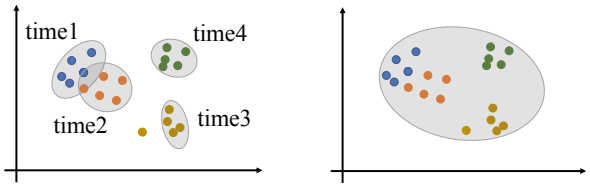


Fig. 5: Matching and authentication in a 2D view. **left**: User's biometrics are extracted at 4 continuous periods and stored. A user whose biometrics features match with one of the stored biometrics is viewed to be legal. **right**: If we do not use multiple clustering strategy, the authentic range needs to be much larger, which would lead to higher false positive rates.

from a series of offsets shown as follows:

$$\phi = \phi_T + \phi_s + \phi_b + \phi_m + 2\pi f \Delta t, \tag{5}$$

where ϕ and ϕ_T stand for the measured phase and true phase, respectively. The ϕ_s, ϕ_b and ϕ_m are sampling frequency offset, packet boundary detection uncertainty and measurement error, respectively, which are considered uncontrollable but follow certain probability distributions, *e.g.,* the Gaussian. The last component, *i.e.,* $2\pi f \Delta t$, is a constant, where f is the carrier frequency offset of the receiver.

To eliminate the carrier frequency offset in a lightweight manner, we find that the phase errors can be largely removed by the *difference of two continuous phases* as follows:

$$\phi'_t = \phi_{t+1} - \phi_t, \tag{6}$$

where ϕ'_t is the phase difference at the sampling time of t. We import such differentiated phases, instead of raw phases, to the Butterwork filter for the feature extraction.

(3) Putting them all together. In summary, after BodyPIN collects the CSI samples, it first processes their amplitudes and phases, and then extracts the selected features, based on which a classifier can be trained. To avoid the curse of dimensionality, we apply unsupervised dimensionality reduction on these features by principal component analysis (PCA) [40]. Empirically, we reserve 90% of information (variance) in the feature dataset. Prior to train the classifier, we normalize the feature values in the dataset within [-1, +1].

C. Continuous authentication via biometrics matching

So far, we have introduced the CSI based biometrics feature extraction. In this subsection, we elaborate the matching and authentication designs in BodyPIN.

Matching strategy. According to the system working flow in Fig. 3, BodyPIN records the CSI series for registering a legal user's biometrics features when she logs into the computer system for the first time, by the primary authentication. In constructing the classifier to recognize legal users, we consider a practical setting — as the user may not always stay still, the reflected Wi-Fi signals from the user may vary at the receiver side. As a consequence, the constituents of the user-dependent factors extracted from various signals can be slightly different, *e.g.,* the impacts of some factors may vary, even though they belong to the same user.

To tackle this issue, we set BodyPIN to continuously record CSI for several periods, *e.g.,* each period last for 30 seconds. For example, as shown in the Fig. 5 (left), BodyPIN records CSI and extracts biometrics features for 4 periods. In each period, biometrics samples are collected to form a clustering range, and these ranges together can be further converted to an aggregated Bayes probability range, for deciding whether a newly coming feature sample corresponds the legal user.

Technically, taking the $time1$ shown in Fig. 5 for example, in this period, we collect n biometrcis samples, *e.g.,* one-second CSI series contributing one sample, for the legal user, represented by s_1 to s_n. Supposing the dimension of these samples is m, and the value of the j^{th} dimension of the i^{th} sample is represented by s_i^j. With these samples, we first compute the $mean$, and $variance$ of each dimension, which are represented by μ^j and σ^{2^j}. Afterwards, for any sample s, we have its authentic probability equation as follows by the Bayes inference:

$$p(1|s) = \frac{p(1) * p(s|1)}{p(s)}, \tag{7}$$

where in recording biometrics, $p(1) = 1$, and $p(s)$ is unreachable and neglected in our application. Supposing the values in different dimensions are independently with each other, we have a further equation based on Eq. 7:

$$p(1|s) \propto \prod_{j=1}^{m} p(s^j|1) \tag{8}$$

Supposing $p(s^j|1)$ follows a Gaussian distribution. Combining the computed $mean$, μ^j, and $variance$, σ^{2^j}, we have:

$$p(1|s) \propto \prod_{j=1}^{m} \frac{1}{\sqrt{2\pi\sigma^{2^j}}} e^{-\frac{(s^j-\mu^j)^2}{2\sigma^{2^j}}}. \tag{9}$$

After the value is computed, we normalize it by an operator of $\sqrt[m]{\cdot}$, and take the result as $p(1|s)$. Finally, we can obtain the probabilities of the n samples, from $p(1|s_1)$ to $p(1|s_n)$.

Authentication. For the authentication, we sort these n probabilities in a descending order and set a probability threshold, p', at the 90%. When facing a new sample, if the probability, $p(1|s_{new})$, is greater than p', BodyPIN will consider it is from the legal user. The final decision is jointly made by the probability thresholds at all recording periods:

$$p(1|s_{new}) \geq p'_1 \parallel p(1|s_{new}) \geq p'_2 \parallel \cdots \parallel p(1|s_{new}) \geq p'_t,$$

where $\parallel$ is the operator of the logical OR, and t is the number of continuous CSI based biometrics sampling periods. For the example Fig. 5, the t equals to 4.

Eq. 10 indicates that if the authentic probability is greater than any one of the probability thresholds, BodyPIN considers the user to be legal. As shown in Fig. 5, if the new biometrics sample is within any one of these 4 shadow ranges, it passes the authentication. One significant advantage of this strategy is clear, that is, it makes BodyPIN resilient to user state change. In addition, dividing recorded CSI series with multiple smaller periods, comparing with the whole series, can largely decrease the *false positive* (FP) rate, *i.e.,* recognizing an illegal user as the legal one. We still use Fig. 5 (left) to explain this issue.

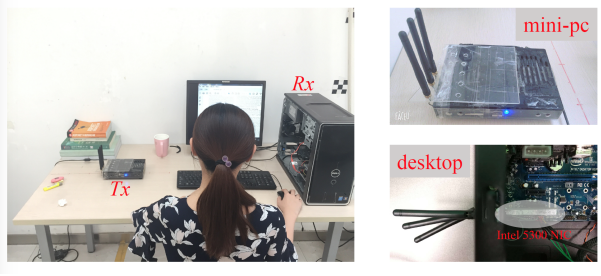
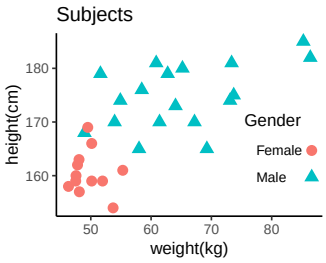


Fig. 6: System deployment. We refit a mini-pc with Intel 5300 NIC and take it as the transmitter. A desktop attached with Intel 5300 NIC works as a computer system embedded with BodyPIN. Subjects are asked to sit before the monitor and to act as their usual behaviors.



Apparel	Number
T-shirt	14
Blouse	6
Coat	5
Dress	3
Jacket	2

Fig. 7: Subjects' detailed information. **(left)**: Their weights and heights; **(right)**: Subjects' apparels.

With our strategy, the authentic ranges are 4 small shadow circles. However, if we adopt a long recording time, in order to cover these samples shown in the figure, we need one much larger circle, shown in Fig. 5 (right), which would cover much bigger range and causes higher FP rates.

Updating classifier. Considering the common variation of user's pose and position, which may lead to new user biometrics features and cause false negative (FN), we update the classifier with the latest recorded biometrics features during the continuous authentication.

V. Evaluation

A. Experimental setup

In our experiments, we utilize Intel 5300 wireless NICs to record CSI. Specifically, the frequency is 5 GHz and the packet transmission rate is 50 Hz. As shown in Fig. 6, the transmitter is a mini-pc and the receiver is a desktop, which runs Ubuntu 14.04 OS. We use a PCIe-X1 to mini-PCIe adapter to make the card attached on the motherboard of desktop. 30 subjects are recruited in the experiment, which we believe is a relatively common scenarios in practice, such as in the office and laboratory. Some of them play as the common user and operate on the computer. Other subjects act as the surrounding people to mainly investigate the robustness of our system against such an influence. During the data collection, Wi-Fi devices always record the CSI first. Then each subject takes turn to act as the computer user and the other subjects will participate to test the influence of nearby people. The detailed information of these 30 subjects, *i.e.,* their weights, heights and apparels, is recorded in Fig. 7.

B. Overall performance

We show overall performances, including *mean interruption interval, mean authentication accuracy, mean defending precision and authentication time delay* in this subsection.

Metric 1: mean interruption interval. We first consider the case that BodyPIN authorizes legal users wrongly as adversaries (true negative), which interrupts the user's operation due to the re-logging in. We ask 30 subjects to sit as in Fig. 6 and to do routine activities for 60 minutes and record corresponding CSI based biometrics. Their activities are mainly two-folds. 1. operating a computer, such as browsing websites, clicking the mouse, and typing on keyboard. 2. other daily activities before a computer, such as raising hands, shaking the head, and moving forward and backward. We do continuous authentication every 5 minutes and record the time and frequency of the first interruption in Fig. 8 (left). For instance, BodyPIN first interrupts 5 subjects at time of the 40 minutes. Meanwhile, if BodyPIN does not interrupt in these 60 minutes, we record the first interruption time as the 60 minutes, that is, BodyPIN does not interrupt 8 subjects in these 60 minutes. We compute the mean interruption interval (mI^2) by using following equation.

$$mI^2 = \sum_{t\in\{5,10,\ldots,60\}} n_t \times t/N, \tag{10}$$

where n_t is the *amount* of the first interruption taking place at time t, and N stands for the amount of subjects 30. Then, we have the average interruption interval of BodyPIN in the evaluation dataset is 43.5 minutes. We conduct a questionnaire about the acceptable interruption interval among these subjects, and 27 out of 30 think this interruption interval is acceptable.

Metric 2: mean authentication accuracy. We examine the next metric, named mean authentication accuracy (mA^2), to evaluate BodyPIN performance on true positive (TP) authentication. As shown in Fig. 8 (left), one subject is interrupted by BodyPIN at the 10 minutes, which means BodyPIN works incorrectly at the second time on this subject (first time is at 5 minutes). Thus, we compute the accuracy of this situation as $(10-5)/10 = 50\%$. For example, if the first interruption happens at time 55, the corresponding accuracy is $(55-5)/55 = 90.91\%$. Note that, if BodyPIN does not interrupt a subject, the accuracy on this subject is 100%. By this definition, we have the mean authentication accuracy as:

$$mA^2 = \frac{\sum_{t\in\{5,10,\ldots,55\}} n_t \frac{t-5}{t} + n_{60} \times 100\%}{N}, \tag{11}$$

where the n_{60} is the frequency of first interruption happening at the 60 minutes. Inputting the value shown in Fig. 8 (left), we have mean authentication accuracy as 88.16%.

Metric 3: mean defending precision. We then evaluate the third metric, mean defending precision (mDP) of BodyPIN, which is a metric for defending adversaries correctly.

In particular, for one subject, we treat him/her as the authorized user, and consider the remaining 29 subjects as adversaries. We set BodyPIN does continuous authentication

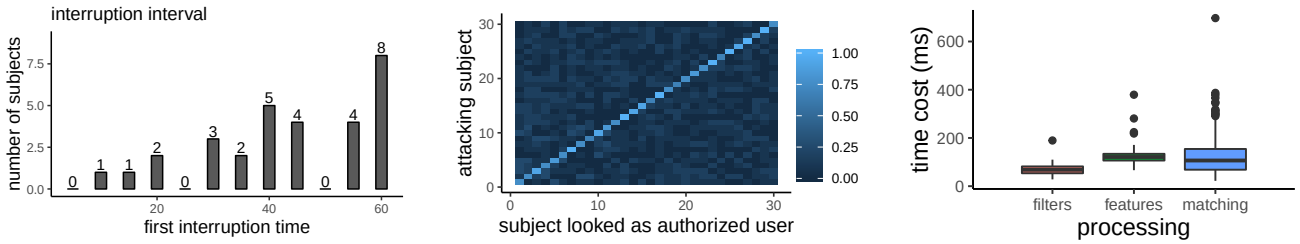


Fig. 8: Overall evaluation results of BodyPIN. **(left)**: Time and frequency of first interruption happening; **(middle)**: Confusion matrix on defending precision. **(right)**: Time cost at 3 main processing stages, applying filters, extracting features and matching.

every 5 minutes, thus, every adversary is tested by $60/5 = 12$ times. We repeat similar testings for the other 29 subjects.

As shown in Fig. 8 (middle), the value of the element in the (i, j) block represents the frequency in our dataset that BodyPIN wrongly considers the j^th adversary as authorized user when we doing above processing at the i^th subject. Then we can compute mean defending precision with Eq. 12.

$$mDP = 1 - \frac{\sum_{i \neq j,\ i,j \in [1,N]} p(i,j)}{(N-1) \times N} \tag{12}$$

where N is 30, $p(i, j)$ is the element value at the block of (i, j). Finally, the mean defending precision of BodyPIN is 90.18% based on Fig. 8 (middle). A further improvement of this defending precision and also the mean interruption interval (discussed above) could be one future work of this paper.

Metric 4: authentication time delay. The main authentication time delay consists of applying filters, computing CSI based biometrics and biomectrics matching. We use a desktop with Intel i5-3470S CPU and 32GB RAM to evaluate the authentication delay. We repeatedly do these computations and record the cost of time for 1K times, which results in a boxplot shown in Fig. 8 (right). From the figure, we know medians of time cost on these three processing stages are $70ms$, $115ms$ and $105ms$, respectively. This light-weighted computation requirement enables BodyPIN run continuous authentication in real-time system. We notice the maximal delay is $1300ms$ (200+400+700), which is acceptable for the common usage.

C. Micro-benchmark experiments

There exist some empirical selections in designing BodyPIN algorithms. To make a better understanding on the relation between these selections and performance, we conduct micro-benchmark experiments in this subsection.

1. Information reserving rate in dimensionality reduction. In the CSI based biometrics features processing, we apply PCA to reduce data dimensionality. In the overall evaluation, we selectively reserve 90% information (variance) of the data. Here we adjust the information reserving rate to evaluate the ability of dimensionality reduction.

As shown in Table II (up), we find (1) PCA is good for all three metrics; (2) if PCA is applied, reserving less information arises less interruption (more authentication accuracy); however, (3) if PCA is applied, reserving less information harms the precision of detecting adversaries. By analyzing this phenomenon, we infer that major features of subjects are embedded in high variance dimensions, reserving these features helps to identify legal users continuously (reason of 2). Besides, we think the reason behind phenomenon (3) is a few subjects related features may exist in the small variance dimensions, and if we ignore them, BodyPIN works worse in identifying adversaries.

Reserved information	mI^2	mA^2	mDP
85%	44.83	89.43%	84.11%
90%	**43.50**	**88.16%**	**90.18%**
95%	41.50	84.49%	92.23%
100%	37.80	81.46%	83.50%

Recording duration	**Clustering group**	mI^2	mA^2	mDP
1	4	36.67	80.16%	92.34%
2	**4**	**43.50**	**88.16%**	**90.18%**
3	4	45.17	89.83%	90.46%
2	1	34.67	81.43%	85.35%
2	2	41.83	86.49%	86.74%
2	6	43.33	87.86%	93.54%

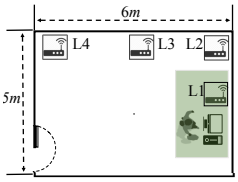
TABLE II: Ablation results on empirical selection of, **up:** reserved information rate by PCA; **bottom:** CSI recording duration and clustering group for registering features. The result marked with bold font is the initial setting in §V-B

2. CSI recording duration and clustering groups for preparing registering features. Having depicted in §IV, after authentic user logs in, BodyPIN records CSI series for a certain time to prepare registering CSI based biometrics features. In the primary evaluation, we record 2 minutes and divide them to 4 clustering groups, as illustrated in Fig. 5 (left). We examine several other settings as shown in Table II (bottom).

From the first settings in Table II (bottom), we conclude increasing CSI recording duration can make user's features stable and lead to less interruptions and better performance on authorize legal users and defend illegal users. Meanwhile, we ascribe the reason of the last three settings results to the advantages of the multiple clustering strategy, depicted in §IV and illustrated in Fig. 5.

3. Relative location among transmitter, receiver and user. We change router position at 4 typical places in a $5m \times 6m$ room to evaluate BodyPIN, which leads to users sitting in line-of-sight (LOS) and non-line-of-sight (NLOS), shown in Fig. 9 (left). The scene of the overall evaluation is marked with green shadow. The involved subjects and process of data collection keep the same with the overall evaluation.

The results shown in Fig. 9 (right) demonstrate BodyPIN



Location	L1	L2	L3	L4
Tx-Rx distance	$0.8m$	$2.8m$	$3.5m$	$5.5m$
User position	NLOS	NLOS	LOS	LOS
mI^2	43.50	40.67	41.33	39.17
mA^2	88.16%	85.74%	86.85%	84.84%
mDP	90.18%	88.18%	89.27%	87.24%

Fig. 9: Settings on relative location among transmitter, receiver and user. The setting marked with green shadow is the data collecting scene shown in Fig. 6.

is robust to the change of relative location among transmitter, receiver and user, which is practical for use. Specially, comparing results of L1/L2, L3/L4, we notice BodyPIN works better if transmitter and receiver put closer. Meanwhile, comparing results of L2 and L3, which with similar distance, we conclude that BodyPIN works better when users sitting in LOS.

4. Interference from other subjects. All above results are derived from situation that only the user is in the room shown in Fig. 9 (left), which arise our concerns on applying BodyPIN in a more normal situation. Next, we evaluate the performance of BodyPIN when facing the interference from other subjects in surroundings. The data collection process and evaluation metrics in this part are much different to those in the above, thus, we explain them in details before going to results. Note that, in this part, the relative location is the same as the L1 shown in Fig. 9 (left) if not mentioned.

(1) Distance of one other subject. Illustrating in the first row of Fig. 10, we first asked one user to sit before a monitor and collected corresponding CSI series for 2 minutes, then we asked one subject to stand behind the use with a distance about $0.6m$ and collected corresponding CSI series for 2 minutes. During CSI collection, the user was asked to do the least motions. The former 2-minute series are to train classifier, and the later 2-minute series are for testing BodyPIN when facing other subject. We tested distances around $0.6m$, $1.2m$, $1.8m$, $2.4m$, $3.0m$ and $3.6m$ and did this on up to 10 users.

To make it clear, we divide the later 2-minute series into 10 testing samples, then we obtain 100 testing samples on 10 users for every distance. The authentication accuracies are 73%, 81%, 87%, 90%, 93%, 91%, respectively. This indicates BodyPIN still works well when facing the interference from a subject $1.8m$ away from this relative location.

(2) Number of other subjects. As shown in the Fig. 10 (middle), we first asked user to sit before a monitor and collected corresponding CSI series for 2 minutes, then, we asked 2 other subjects to stand behind the user and collected CSI series for 2 minutes. Subjects were asked to change their positions randomly for 10 times, and number of tested subjects increase from 2 to 5. Thus, we have $10 \times 10 = 100$ samples when testing every specific number. The authentication results are 87%, 83%, 80%, and 75% for number of 2, 3, 4 and 5, respectively. This indicates user may have to re-log in with his/her keys such as password, fingerprint, face *etc* if many subjects appear in surrounding suddenly.

(3) Motions of other subjects. We first asked 5 subjects to move casually such as walking, standing and talking to others, in the room, then one user was asked to sit before the monitor. There is no requirement on the distance among these subjects. Concurrently, we recorded CSI series for 30 minutes for training classifiers. The amount of involved users is still 10. We use the first 2-minute CSI series to train classifiers, meanwhile, BodyPIN is set to do continuous authentication every 3 minutes. Similar to metrics in overall evaluation, finally, we have mI^2, mA^2 and mDP of 17.70, 82.07% and 84.23%, which indicates BodyPIN can still work properly in noisy environment.

Fig. 10: Testing influence from nearby subjects. **(top)**: various distances to the user; **(middle)**: increasing nearby subjects' amount; **(bottom)**: influence from subjects' casual motions.

(4) Relative location of other subjects. Please look at the Fig. 9 (left), in the above three experiments, we selected relative position setting of L1 and asked other subjects appearing behind the user, which cause the interference of other subjects is mainly from NLOS. To test the interference from LOS, we applied setting of L4 and utilized metrics as the above 3^{rd} experiment. Not surprisingly, the performance decreases to mI^2 of 12.60, mA^2 of 67.07% and mDP 69.50%, respectively. This problem matches the human body impacts on Wi-Fi signals depicted in §III. We highly recommend to set relative position of transmitter and receiver at places that would cause the least LOS interference from other subjects.

VI. Conclusion

In this paper, we demonstrate a contactless continuous authentication system, BodyPIN, by using the human body biometrics features conveyed in Wi-Fi signals. BodyPIN requires no extra or dedicated wireless hardware but achieves promising authentication performances, *i.e.,* acceptable interruption interval, high authenticating and defending accuracy, lightweight computation, resilience on surrounding people, *etc*. Due to these strengths, BodyPIN could serve as a useful and practical system for the continuous authentication.

References

[1] 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 *ACM MobiCom*, 2017.

[2] I. Traore, *Continuous authentication using biometrics: data, models, and metrics*. IGI Global, 2011.

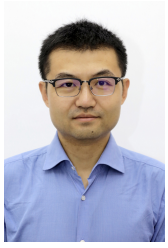
[3] K. Niinuma and A. K. Jain, "Continuous user authentication using temporal information," in *Biometric Technology for Human Identification VII*, vol. 7667. International Society for Optics and Photonics, 2010, p. 76670L.

[4] S. Eberz, K. Rasmussen, V. Lenders, and I. Martinovic, "Preventing lunchtime attacks: fighting insider threats with eye movement biometrics," 2015.
[5] R. Ranjan, V. M. Patel, and R. Chellappa, "Hyperface: A deep multi-task learning framework for face detection, landmark localization, pose estimation, and gender recognition," *IEEE TPAMI*, vol. 41, no. 1, pp. 121–135, 2019.
[6] J. Lv, W. Yang, D. Man, X. Du, M. Yu, and M. Guizani, "Wii: device-free passive identity identification via wifi signals," in *IEEE GLOBECOM*, 2017.
[7] T. Xin, B. Guo, Z. Wang, M. Li, and Z. Yu, "Freesense: indoor human identification with wifi signals," *arXiv preprint arXiv:1608.03430*, 2016.
[8] Y. Zeng, P. H. Pathak, and P. Mohapatra, "Wiwho: wifi-based person identification in smart spaces," in *IEEE IPSN*, 2016.
[9] J. Zhang, B. Wei, W. Hu, and S. S. Kanhere, "Wifi-id: human identification using wifi signal," in *IEEE DCOSS*, 2016.
[10] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *NIPS*, 2014, pp. 2672–2680.
[11] A. Kurakin, I. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," *arXiv preprint arXiv:1607.02533*, 2016.
[12] A. Brock, J. Donahue, and K. Simonyan, "Large scale gan training for high fidelity natural image synthesis," *arXiv preprint arXiv:1809.11096*, 2018.
[13] C. Slobogin, "Public privacy: camera surveillance of public places and the right to anonymity," 2002.
[14] Y. Cheng, X. Ji, X. Zhou, and W. Xu, "Homespy: inferring user presence via encrypted traffic of home surveillance camera," in *IEEE ICPADS*, 2017.
[15] R. Hoyle, R. Templeman, D. Anthony, D. Crandall, and A. Kapadia, "Sensitive lifelogs: a privacy analysis of photos from wearable cameras," in *ACM CHI*, 2015.
[16] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: Gathering 802.11 n traces with channel state information," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 1, pp. 53–53, 2011.
[17] A. Christ, T. Samaras, A. Klingenböck, and N. Kuster, "Characterization of the electromagnetic near-field absorption in layered biological tissue in the frequency range from 30 mhz to 6000 mhz," *Physics in Medicine & Biology*, vol. 51, no. 19, p. 4951, 2006.
[18] I. Dove, "Analysis of radio propagation inside the human body for in-body localization purposes," Master's thesis, University of Twente, 2014.
[19] G. Melia, "Electromagnetic absorption by the human body from 1-15 ghz," Ph.D. dissertation, University of York, 2013.
[20] S. Gabriel, R. Lau, and C. Gabriel, "The dielectric properties of biological tissues: Ii. measurements in the frequency range 10 hz to 20 ghz," *Physics in Medicine and Biology*, vol. 41, no. 11, p. 2251, 1996.
[21] Y. Shen and E. Martinez, "Channel estimation in ofdm systems," *Freescale semiconductor application note*, pp. 1–15, 2006.
[22] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 136–148, 2013.
[23] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," in *IEEE Conference on Technologies for Homeland Security*, 2012, pp. 451–456.
[24] G. Kambourakis, D. Damopoulos, D. Papamartzivanos, and E. Pavlidakis, "Introducing touchstroke: keystroke-based authentication system for smartphones," *Security and Communication Networks*, vol. 9, no. 6, pp. 542–554, 2016.
[25] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "Hmog: New behavioral biometric features for continuous authentication of smartphone users," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 877–892, 2016.
[26] Q. Xu, Y. Chen, B. Wang, and K. R. Liu, "Radio biometrics: human recognition through a wall," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1141–1155, 2017.
[27] J. A. Shaw, "Radiometry and the friis transmission equation," *American Journal of Physics*, vol. 81, no. 1, pp. 33–37, 2013.
[28] P. Zhou, Y. Zheng, and M. Li, "How long to wait?: predicting bus arrival time with mobile phone based participatory sensing," in *ACM MobiSys*, 2012.
[29] R. v. Nee and R. Prasad, *OFDM for wireless multimedia communications*. Artech House, Inc., 2000.
[30] Y. Xie, Z. Li, and M. Li, "Precise power delay profiling with commodity wifi," in *ACM MobiCom*, 2015.
[31] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *NIPS*, 2012, pp. 1097–1105.
[32] R. Salakhutdinov and G. Hinton, "Deep boltzmann machines," in *Artificial Intelligence and Statistics*, 2009, pp. 448–455.
[33] Y. Wang, K. Wu, and L. M. Ni, "Wifall: Device-free fall detection by wireless networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 2, pp. 581–594, 2017.
[34] H. Wang, D. Zhang, Y. Wang, J. Ma, Y. Wang, and S. Li, "Rt-fall: a real-time and contactless fall detection system with commodity wifi devices," *Transactions on Mobile Computing (TMC)*, vol. 16, no. 2, pp. 511–526, 2017.
[35] E. Thomaz, I. Essa, and G. D. Abowd, "A practical approach for recognizing eating moments with wrist-mounted inertial sensing," in *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 2015, pp. 1029–1040.
[36] J.-L. Reyes-Ortiz, L. Oneto, A. Samà, X. Parra, and D. Anguita, "Transition-aware human activity recognition using smartphones," *Neurocomputing*, vol. 171, pp. 754–767, 2016.
[37] K. Qian, C. Wu, Z. Zhou, Y. Zheng, Z. Yang, and Y. Liu, "Inferring motion direction using commodity wi-fi for interactive exergames," in *ACM CHI*, 2017.
[38] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti, "Spotfi: Decimeter level localization using wifi," in *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 4, 2015, pp. 269–282.
[39] X. Wang, L. Gao, and S. Mao, "Biloc: Bi-modal deep learning for indoor localization with commodity 5ghz wifi." *IEEE Access*, vol. 5, pp. 4209–4220, 2017.
[40] I. Jolliffe, "Principal component analysis," in *International encyclopedia of statistical science*. Springer, 2011, pp. 1094–1096.

Fei Wang received the B.E. degree in computer science and technology from Xi'an Jiaotong University, Xi'an, China in 2013. He is currently a Ph.D. student at school of computer science, Xi'an Jiaotong University, Xi'an, China. His research interests include deep learning, time series mining, human sensing, and sensors.

Zhenjiang Li received the B.E. degree in computer science and technology from Xi'an Jiaotong University, Xi'an, China, in 2007, the M.Phil. degree in electronic and computer engineering and the Ph.D. degree in computer science and engineering from The Hong Kong University of Science and Technology, Hong Kong, in 2009 and 2012, respectively.

He is currently an Assistant Professor of Computer Science Department at City University of Hong Kong, Hong Kong. His research interests include wearable sensing, and distributed computing.



Jinsong Han received the PhD degree in computer science from the Hong Kong University of Science and Technology, in 2007. He is now a professor in the Institute of Cyberspace Research, College of Computer Science and Technology, Zhejiang University. He is a senior member of the ACM and IEEE. His research interests focus on mobile computing, RFID, and wireless network.