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.

I. INTRODUCTION

Most computer systems require the user authentication only at the login step. The systems then can be accessed once the authentication is successful, even the user may temporarily leave afterwards [1]. However, such an one-time authentication scheme could expose systems to adversaries, especially during the user’s absent period, and cause severe security issues, such as the illegal copy of private documents, the peep of sensitive information, malicious modifications of system configurations, etc. The victim systems can be common computers, as shown in Fig. 1 and could also be the emerging mobile devices [2], e.g., smart phones or wearables, as well as various Internet of Things (IoTs) devices in a smart cyber-space.

To defend this crucial security issue, the concept of continuous authentication was proposed [3], aiming to keep track of the current user’s legal identity throughout the system’s operation. In case the authentication interrupts, e.g., the legal user leaves and/or the adversary appears, the system is locked automatically. One naive way for achieving this is to ask the user to frequently authenticate herself, e.g., by her password or fingerprint, but this will interrupt the user’s normal operations on the system, i.e., highly inconvenient and not user-friendly.

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 [4]. Then we can match them with the pre-recorded feature profiles for the authentication. As the entire process is fully passive to the user and does not require any user’s touch on the device, e.g., no password input, the authentication thus can continuous, without interrupting the user’s operations on the system.

Following this principle, there are two main types of designs proposed in the literature, the camera-based and wireless-based solutions. For the former category, the features, like the colors of the user’s cloth and skin [4] and the gaze moving pattern [5], can be utilized. However, the camera-based designs suffer two obvious issues. First, due to the limited camera view angle, the user should be directly captured by the camera (without blocking) in good lighting conditions, which may limit the usable scenarios [1]. Second, cameras can also cause the privacy leakage issue [6], [7] if the recorded video is not properly protected or gets hacked by the adversaries. Due to these concerns, the wireless sensing based designs promising appear recently [1], [8]–[11], which can effectively bypass these two issues. However, the existing designs either require the user to perform certain activities [9]–[11], e.g., walking, or a dedicated hardware design [1], which could inevitably interrupt the user’s operations as well, or increase the system deploying and maintaining costs, e.g., not pervasive enough.

Motivated by these existing works, in this paper, we explore the opportunity to achieve the continuous user authentication using commodity wireless techniques, like Wi-Fi [12], without imposing any activities performed by the user. If this is viable, the solution should be able to preserve the merits from prior wireless-based designs, and meanwhile also largely reduces the system cost. However, the key questions is without the dedicated wireless design, whether suitable features from Wi-Fi signals exist to strongly identify a user’s identity along for the continuous authentication design. Such an identification implies that the explored features should be related to the
user’s biometric features directly, rather than the performed activities as previously studied [9]–[11], which, to our best knowledge, has not been explored yet.

Our investigation in this paper is inspired by the existing studies from the bio-electromagnetics domain [13]–[16], which have the proper model to abstract the human body for understanding the interactions between the electromagnetic waves and human body. Based on such a design preliminary, 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. Then, our next effort is to extract suitable Wi-Fi signal features to fully represent the user’s identity component. To this end, we conduct an in-depth analysis and figure out a set of Wi-Fi biometrics traits or features from the channel state information (CSI) [17]. Based on this, we finally design a continuous authentication system, BodyPIN, which can achieve both a high true-positive (TP) rate, for the least interruption to the legal users, and a low false-positive (FP) rate, for the least misses of the adversaries.

Fig. 1 depicts 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 turn 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 implement a BodyPIN prototype using Intel 5300 wireless NICs. Extensive evaluations show that it can achieve very good authentication performance, nearly 90% authenticating accuracy and defending precision with a group of 30 subjects. 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. IMPACT OF HUMAN BODY ON WI-FI SIGNALS

Existing studies have empirically demonstrate that our human body could have impacts on the electromagnetic waves, like absorption, within a certain frequency band, which covers Wi-Fi’s frequencies [13]–[16]. 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 tissues [16], such as the skin, fat under the skin, muscle, fat on the viscera, viscera, bone, etc., and the radius of layer i is ri, where i ∈ [1, n] and n is the total number of layers. Although this model is simple, similar as prior studies [14], we find that it is effective enough for our analysis.

As shown in Fig. 2 we denote the distances from the user to the transmitter and receiver as l1 and l2, respectively. Other useful notations are tabulated in Table I. According to the table, the initial Wi-Fi signals generated at the transmitter side, i.e., X, can be mathematically written as:

$$X = A \cdot e^{-j2\pi f t + \phi_0},$$  \hspace{1cm} (1)

where $\phi_0$ is the initial phase, and A and f are the amplitude and frequency, respectively. After the signal X’s transmission from the transmitter to the receiver, its amplitude and phase both will change, and the receiver can receive multiple copies of this signal due to the multipath. For the cope that bypasses the user’s body (stated below), we find that its signal changes convey the user’s biometric features.

**Amplitude.** During signal X’s transmission, its amplitude A decays, in terms of the signal power, along the time. Such a decay effect occurs for every propagation medium. In particular for the power decay of wireless signals, the decayed power amount can be computed through the Friis transmission equation [18]. 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:

$$A' = A \cdot c_1^0 \cdot c_2^0 \cdot \prod_{i=1}^{n} c_i,$$  \hspace{1cm} (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.** Next, we compute the phase changes, which are caused by the time (propagation) delay, $t$. In particular, we consider $t$ as a sum of every time delay taking place at every propagation medium, e.g., in the air or various body layers, as $t = \sum_{i=1}^{m} t_i$, 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 $\mu_i$ and $\varepsilon_i$ 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.

$$t = \sum_{i=1}^{n} d_i \cdot \sqrt{\mu_i \varepsilon_i}.$$ 

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

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

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:

$$Y = \prod_{i=1}^{n} c_i e^{-j \frac{2\pi f}{c} \left( d_{i1} + d_{i2} \right) \sqrt{\mu_i \varepsilon_i} + \left( l_1 + l_2 \right) \sqrt{\mu_0 \varepsilon_0} X,}$$

where the component marked with the wave line is uniquely determined by each individual user.

**Summary.** Based on the mathematical expressions of this component, we conclude that the properties of human body, such as the absorption ability, permittivity, permeability and the length of each tissue layer, could have joint impacts on the Wi-Fi signals, which are user-dependent. In [16], permittivity and permeability of the tissues, such as 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 influence on the Wi-Fi signals, which motivates our continuous authentication design in the next section.

On the other hand, as the received $Y$ is just one multipath copy from all received signals by the receiver. It implies that when the user is closer to the line of sight path from the sender to the receiver, it is more likely that the user’s unique features can be reliably detected. As unveiled in §IV, the authentication is robust in multiple real-world scenarios, which is sufficient for the practical usage.

## III. System Design

In this section, we elaborate the BodyPIN design. We first describe the system working flow (§III-A), followed by the Wi-Fi based biometrics feature extraction (§III-B) and the authentication design (§III-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 (after one- or two-minute recording) 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, at 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.

### B. Wi-Fi based biometric feature extraction

As suggested by the insights from the analysis in Section II, 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 Wi-Fi protocols, 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) [19] 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:

$$Y = H \cdot X + n,$$

where $n$ is for channel noise. Recently, many advanced Wi-Fi NICs can report the detailed channel state information (CSI)
Fig. 3: System working flow. Once a legal user logs in, the Wi-Fi signals are recorded for the biometric feature extraction. The extracted features are registered for the continuous authentication. To this end, new samples of the Wi-Fi based features are collected and further matched with the registered ones. If matched, the current user is viewed to be legal; Otherwise, BodyPIN locks the system until the primary authentication is passed 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 1st, 15th and 30th subcarrier are depicted).

to describe channel $H$ in each subcarrier level, which can be obtained through many existing CSI extraction tools [12], [20].

**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 Section 2.4, we observe that such a component (related to a series of properties of the user) is also included in the obtained CSI information, which can be reflected from both the amplitude and phase two aspects of the CSI.

With many prior investigations [21], [22] to extract various types of features from CSI time series, 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 $8 \times 30 \times 2 = 480$.

Although rich features could be identified, we find that they cannot be directly adopted, due to the surrounding noises and imperfection of WiFi adapter. As a result, the raw CSI, both amplitude and phase, collected by the CSI tool [12], will suffer non-negligible fluctuation as illustrated in Fig. 4(a, c). Inspired by the related works [21], [23], we need to carefully process the collected CSIs (for removing such noises) 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 (5th order, 1Hz of the cut-off frequency) to filter these noises and smooth the time series of CSI amplitude [21], [23]. The filtering results are shown in the Fig. 4(b), where the 1st and the 2nd 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 [20], [22], [24], [25] and conclude that it is introduced by joint impacts from a series of offsets shown as follows:

$$\phi = \phi_t + \phi_s + \phi_b + \phi_m + 2\pi f \Delta t,$$

where $\phi$ and $\phi_t$ stand for the measured phase and true phase, respectively. The $\phi_s, \phi_b$ and $\phi_m$ 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:

$$\phi_t' = \phi_{t+1} - \phi_t,$$

where $\phi_t'$ 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) [26]. 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 $n$ biometrics 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 $i^{th}$ dimension of the $j^{th}$ sample is represented by $s_{ij}$. With these samples, we first compute the mean $\mu_i$ and variance $\sigma_{i}^2$ of each dimension, which are represented by $\mu^j$ and $\sigma_j^2$. Afterwards, for any sample $s$, we have its authentic probability equation as follows by the Bayes inference:

$$p(1|s) = \frac{p(1) \cdot p(s|1)}{p(s)}$$

(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

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

(8)

Supposing $p(s^j|1)$ follows a Gaussian distribution. Combining the computed mean, $\mu^j$, and variance, $\sigma_j^2$, we have:

$$p(1|s) \propto \prod_{j=1}^{m} \frac{1}{\sqrt{2\pi\sigma_j^2}} e^{-\frac{(s_j^j - \mu_j^j)^2}{2\sigma_j^2}}$$

(9)

After the value is computed, we normalize it by an operator of $\sqrt{\cdot}$, 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, $p^t$, at the 90%. When facing a new sample, if the probability, $p(1|s_{\text{new}})$, is greater than $p^t$, BodyPIN will consider it is from the legal user. The final decision is jointly made by the probability thresholds at all recording periods:

$$p(1|s_{\text{new}}) \geq p^t_1 \parallel p(1|s_{\text{new}}) \geq p^t_2 \parallel \cdots \parallel p(1|s_{\text{new}}) \geq p^t_t$$

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. 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.

IV. 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. 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. The detailed information of these 30 subjects, i.e., their weights, heights and apparels, is recorded in Fig. 7.

![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.](image)

![Fig. 7: Subjects’ detailed information. (left): Their weights and heights; (right): Subjects’ apparels.](image)

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

B. Overall performance

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

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 for 60 minutes and record corresponding CSI based biometrics. 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 interrupts in these 60 minutes, we record the first interruption time as the 60 minutes, that is, BodyPIN does not interrupts 8 subjects in these 60 minutes. We compute the mean interruption interval \((mI^2)\) by using following equation.

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

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 made a questionnaire about the acceptable interruption interval among these subjects, 27 out of 30 think this interruption interval is acceptable considering of the security issue.

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 interrupts a subject, the accuracy on this subject is 100\%. By this definition, we have the mean authentication accuracy as:

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

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\%.

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 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.

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

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).

Authentication time delay. The main authentication time delay consists of applying filters, computing CSI based biometrics and bimeetrics matching. We use a desktop with Intel i5-3470S CPU and 32GB RAM to evaluate the authentication delay. We repeatedly do these computation and record the cost of time for 1K times, which results in a boxplot shown in Fig. 8 (right). From the figure, we know...
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.

The 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.

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.

| Reserved information | mI | mA | mDP |
|----------------------|----|----|-----|
| 85%                  | 44.83 | 89.43% | 84.11% |
| 90%                  | 43.50 | 88.16% | 90.18% |
| 95%                  | 41.30 | 84.49% | 92.23% |
| 100%                 | 37.80 | 81.46% | 83.50% |

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 §IV-B.

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 phenomena, 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 phenomena (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.

CSI recording duration and clustering groups for preparing registering features. Having depicted in §III, 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 into 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 §III and illustrated in Fig 5.

Relative location among transmitter, receiver and user.

We change router position at 4 typical places in a 5m × 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 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.

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 0.6 m 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 0.6 m, 1.2 m, 1.8 m, 2.4 m, 3.0 m and 3.6 m 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 accuracy are 73%, 81%, 87%, 90%, 93%, 91%, respectively. This indicates BodyPIN still works well when facing the interference from a subject 1.8 m 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 distance. 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 in the room, then one user was asked to sit before the monitor. 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.

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 3rd 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 WiFi signals depicted in §II. We highly recommend to set relative position of transmitter and receiver there where would cause the least LOS interference from other subjects.

D. Comparison evaluation

We make an extended evaluation to test the possibility of applying BodyPIN as an alternative log-in authentication keys like fingerprint, face, etc. To do this, we use the dataset collected at the §IV-B to train multi-class classifiers with LibSVM [27] (radius basis function kernel, L1 regularization, L1 loss and one-against-all strategy). For each subject, data collected in the first 48 minutes is for training, the remaining 12-minute data is for testing.

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

Fig. 11: BodyPIN is extended as multi-class classifiers on CSI based biometrics of 30 subjects. (left): classification accuracy; (right): comparison with existing works.

We evaluate the user capacity of BodyPIN from 2 to 30. When evaluating the user capacity of $i$ ($i \in [2, 30]$), we randomly select training dataset of $i$ subjects and test with their testing sets. As shown in Fig. 11 (left), BodyPIN can achieve good performance, e.g., nearly 100% accuracy with few subjects and more than 92% accuracy with the user capacity of 30. We compare the accuracy with FreeSense [9], WiFiID [11] and WiWho [10], and find BodyPIN outperforms them, shown in Fig. 11 (right).

The additional evaluation demonstrates a possibility that applying BodyPIN as an alternative log-in authentication keys. However, it is still an open problem to make CSI based biometrics stable and accurate as high as fingerprint, face, etc.
Bio-eletromagnetics. The BodyPIN design relates to the bio-eletromagnetics literatures [13]–[16]. Some human tissues, such as body muscle, kidney and liver, with different dielectric properties are measured by signals from 10Hz to 2GHz [16]. The body’s absorption is studied by [13] in range of 30MHz to 6GHz, and [15] in range of 1GHz to 15GHz. In [14], 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.

Biometrics based continuous authentication. The camera can achieve continuous authentication, e.g., sensing the user’s cloth and skin [2], and the gaze moving patterns [3]. 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 [10], WiFi-ID [11]. FreeSense [9] and Radio-Bio [28]. However, they require the user to perform certain activities, e.g., walking, as they essentially recognize the user’s activities, instead of the users themselves. Therefore, these designs are not suitable for the continuous authentication, since frequently performing the required activities could easily interrupt the user’s normal usage of the computer system and dramatically sacrifices the user experience.

Wi-Fi time series matching. Techniques of Wi-Fi time series matching are also related to this paper. Existing techniques mainly fall into two categories. First, the dynamic time wrapping [29] is widely used in Wi-Fi time series comparison for action recognition [30], [31]. Another category is to convert the Wi-Fi time series to statistics features such as minimum, maximum and mean in [9]–[11], [28]. Guided by the second category, we also extract useful features in BodyPIN, while our feature extraction is inspired by the bio-eletromagnetic model derived, so that they can uniquely and reliably represent different users for the continuous authentication.

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, we believe BodyPIN could be a useful and practical system.

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 MobICOM, 2017.
[2] H. Feng, K. Fawaz, and K. G. Shin, “Continuous authentication for voice assistants,” in MobICOM, 2017.
[3] I. Traore, Continuous authentication using biometrics: data, models, and metrics. IGI Global, 2011.
[4] K. Niinuma and A. K. Jain, “Continuous user authentication using temporal information,” in Biometric Technology for Human Identification VII, vol. 7667, 2010, p. 76670L.
[5] S. Eberz, K. Rasmussen, V. Lenders, and I. Martinovic, “Preventing lunchtime attacks: fighting insider threats with eye movement biometrics,” 2015.
[6] Y. Cheng, X. Ji, X. Zhou, and W. Xu, “Homespy: inferring user presence via encrypted traffic of home surveillance camera,” in ICPADS.
[7] R. Hoyle, R. Templeman, D. Anthony, D. Crandall, and A. Kapadia, “Sensitive lifelogs: a privacy analysis of photos from wearable cameras,” in CHI.
[8] J. Lv, W. Yang, D. Man, X. Du, M. Yu, and M. Guizani, “Wi-device-free passive identity identification via wi signals,” in GLOBECOM, 2017.
[9] T. Xin, B. Guo, Z. Wang, M. Li, and Z. Yu, “Freesense: indoor human identification with wifi signals,” arXiv preprint arXiv:1608.03430, 2016.
[10] Y. Zeng, P. H. Pathak, and M. Mohapatra, “Wiwho: wifi-based person identification in smart spaces,” in IPSN, 2016.
[11] J. Zhang, B. Wei, W. Hu, and S. S. Kanhere, “Wi-id: human identification using with signal,” in DCOSS, 2016.
[12] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, “Tool release: Gathering 802.11 n traces with channel state information,” SIGCOMM Computer Communication Review, vol. 41, no. 1, pp. 53–55, 2011.
[13] 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.
[14] I. Dove, “Analysis of radio propagation inside the human body for indoor localization purposes,” Master’s thesis, University of Twente, 2014.
[15] G. Melia, “Electromagnetic absorption by the human body from 1-15 ghz,” Ph.D. dissertation, University of York, 2013.
[16] S. Gabriel, R. Lau, and C. Gabriel, “The dielectric properties of biological tissues: I. measurements in the frequency range 10 hz to 20 ghz,” Physics in Medicine and Biology, vol. 41, no. 11, p. 2251, 1996.
[17] Y. Shen and E. Martinez, “Channel estimation in ofdm systems,” Freescale semiconductor application note, pp. 1–15, 2006.
[18] J. A. Shaw, “Radiometry and the friis transmission equation,” American Journal of Physics, vol. 81, no. 1, pp. 33–37, 2013.
[19] R. v. Nee and R. Prasad, OFDM for wireless multimedia communications. Artech House, Inc., 2000.
[20] Y. Xie, Z. Li, and M. Li, “Precise power delay profiling with commodity wifi,” in MobICOM, 2015.
[21] Y. Wang, K. Wu, and L. M. Ni, “Wifall: Device-free fall detection by wireless networks,” Transactions on Mobile Computing, vol. 16, no. 2, pp. 581–594, 2017.
[22] 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.
[23] R. Hoyle, C. Wu, Z. Zhou, Y. Zheng, Z. Yang, and Y. Liu, “Inferring motion direction using commodity wi-fi for interactive exergames,” in CHI, 2017.
[24] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti, “Spotfi: Decimeter level localization using wifi,” in SIGCOMM Computer Communication Review, vol. 45, no. 4. ACM, 2015, pp. 269–282.
[25] 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.
[26] J. Jolliffe, “Principal component analysis,” in International encyclopedia of statistical science. Springer, 2011, pp. 1094–1096.
[27] C.-C. Chang and C.-J. Lin, “LIBSVM: A library for support vector machines,” ACM Transactions on Intelligent Systems and Technology (TIST), vol. 2, pp. 27:1–27:27, 2011.
[28] 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.

[29] D. J. Berndt and J. Clifford, “Using dynamic time warping to find patterns in time series,” in KDD workshop, 1994.

[30] K. Ali, A. X. Liu, W. Wang, and M. Shahzad, “Keystroke recognition using wifi signals,” in MobiCom, 2015.

[31] S. Palipana, D. Rojas, P. Agrawal, and D. Pesch, “Falldefi: Ubiquitous fall detection using commodity wi-fi devices,” IMWUT, 2018.