WiPIN: Operation-free Person Identification using WiFi Signals

Fei Wang  
Xi’an Jiaotong University &  
Carnegie Mellon University  
feiwang@cmu.com

Jinsong Han  
Xi’an Jiaotong University  
hanjinsong@gmail.com

Ziyi Dai  
Xi’an Jiaotong University  
dzy219@gmail.com

Han Ding  
Xi’an Jiaotong University  
handing.xjtuxjtu@foxmail.com

Dong Huang  
Carnegie Mellon University  
donghaung@cmu.edu

ABSTRACT
Person identification is critical for sensitive applications such as system login/unlock, access control and payment. In this paper, we present an operation-free person identification system, namely WiPIN, that identifies biometric features of users using Wi-Fi signals. Our approach is based on an entirely new insight that different persons have distinct effects, including the absorption and reflection, on the Wi-Fi signals. We show that through effective signal processing and feature extraction/matching designs, the Channel State Information (CSI) used in recent Wi-Fi protocols can be utilized for person identification without requiring any collaborative operations, such as wiping, walking, or speaking. We theoretically analyzed the interaction between the human body and Wi-Fi Signals via an interactive model. We proposed a mapping rule between variation patterns of Wi-Fi signals and human biologic features, and demonstrated the feasibility of establishing CSI based person identifiers. We conducted extensive experiments over commodity off-the-shelf Wi-Fi devices. The results show WiPIN achieves 92% accuracy in person identification over a group of 30 users, with sufficient robustness to environment noises.

CCS CONCEPTS
• Human-centered computing → Ubiquitous and mobile computing

KEYWORDS
Human Identification, WiFi Sensing, Operation-free

1 INTRODUCTION
Person identification is crucial for sensitive applications, such as system login/unlock, access control, and payment. Personal identifiers used for recognizing the person are mainly based on distinguishing biologic features, or biometrics. Existing person identification solutions can be divided into two categories, operation-based and operation-free identification. Both above patterns, however, have limitations in person identification. Operation based solutions usually rely on certain pre-defined activities or behaviors to generate or validate biometrics, leading inconvenience to users. Gait and voice are the most typical biometrics used by operation based solutions. On the other hand, operation-free solutions dominate the market since the involved biometrics show excellent uniqueness, such as fingerprint, iris, or facial. Nevertheless, collecting those biometrics requires physically touching or cooperating with the scanner, indicating the dependence on specific devices for acquiring the biologic data, as well as inconvenience caused by the restriction on users in the data-acquiring process.

With above observations, we are motivated to design an operation-free biometric based person identification system without restrictions on users or needs of costly devices. The inspiration is deriving from our preliminary experiments on Wi-Fi systems. That is, people are diverse in their biometrics, such as height, weight, or fat rates. Those characteristics incur distinct affections on Wi-Fi signals reflected from a person. Intuitively, the human body can be analogized as an object with geometrically irregular reflections and varying materials, yielding distinct absorption and reflection effects on the Wi-Fi signals. Thus, it is attractive to utilize Wi-Fi signals to directly identify persons since Wi-Fi signals are ubiquitous and low-cost.
However, we must address following two challenges to utilize the above phenomenon for person identification.

(1) Noise cancellation. In current Wi-Fi systems, the signal received at the Rx antenna is mixed by multiple reflections from multiple paths[20]. The signal from the line-of-sight path is the most dominant one but the signals reflected from the human body are weak. Besides, commodity Wi-Fi device encounters certain system error and measure error[33], which may also introduce uncertain noise to the person identification. To address above issues, we develop a Wi-Fi signal preprocessing pipeline, including the Butterworth filter based noise cancellation and IFFT-FFT frequency-domain processing based multipath effect mitigation. With this preprocessing pipeline, noisy raw Wi-Fi signals are effectively cleaned.

(2) Robust feature extracting. Extracting stable and distinct biologic features is essential for biometric based person identification. However, Wi-Fi signals inevitably fluctuate due to the environmental noise and device diversity. Even worse, the signals reflected by the person are too weak to represent a person’s biometrics distinguishably. Our solution is twofold. First, we carefully select and design features from Wi-Fi signals and develop a regression model to predict some biometrics like body fat rate accurately, which indicates these features have relationship with human and is with potential for human identification. Then, we combine Support Vector Machine based classifier with a deep learning trick (a activation layer of deep network called SoftMax) to achieve human identification.

Leveraging above observation and preliminary works, we propose a Wi-Fi based operation-free person identification system, namely WiPIN, which can identify a person merely via Wi-Fi signals reflected from him/her. Our main contributions are summarized as follows:

• We demonstrate an observation that the variance of Wi-Fi signals has correlation with human body components. We build up an interacting model to analyze the observation.

• We build a mapping rule between the Wi-Fi signal variation and four human biologic features, including the water rate, fat rate, muscle rate, and bone rate. With this highly-correlated rule, we confidently extract distinct features from the Wi-Fi signals to do human identification.

• We prototype our system using two mini PCs embedded Intel 5300 NICs. Extensive experimental results show that WiPIN can achieve high accuracy in real time, i.e., 100% accuracy with 2 persons, and 92% accuracy with 30 persons.

The rest of this paper is organized as follows. We first show our observation on Wi-Fi signals variation related to a specific person in Section 2, followed by the analysis of this observation in Section 3. Then the design of WiPIN, including the preprocessing pipeline, feature extraction and mapping rule will be described in Section 4. We present extensive experiment to show the performance of our system in Section 5. Before the conclusion section, limitations of WiPIN and related works are summarized in Section 6 and Section 7 respectively.

2 OBSERVATIONS

We invite 10 volunteers subject with IRB approval to participate in our preliminary experiments. We observe that the Wi-Fi signals collected at the receiver are different when changing the person standing nearby a Tx-Rx antenna pair, as shown in Fig. 1. We perform the experiment in a 5m × 6m room. The distance between the Rx and Tx antennas is 2.4m. We ask 10 volunteers standing nearby the antennas respectively and sample the Wi-Fi signals up to 20 times for each of them. The result is plotted in Fig. 2 in terms of mean amplitude of WiFi signals. Since no other surroundings factors changes obviously, we safely conclude that the main reason cause this phenomenon is the variety of humans. Before leveraging the variety of person to perform the person identification, we notice two issues.

(1) Is the signal based feature distinct for users? As shown in Fig. 2, there are some uncertainties among the collected signals. Correspondingly, the volunteers #4 and #9, #5 and #8 are indistinguishable if merely using the mean amplitude of WiFi signals. It is necessary to extract distinct features from the WiFi signals. (2) Is the signal based feature stable? Once we establish the distinct signal based features, their stability should be guaranteed considering the varying appearance of users. For example, a user may change his/her clothes each day. The extracted features should be effectively resilient to those personal changes.

To combat above issues, we adopt the Channel State Information (CSI)[35] of WiFi signals as the source of feature generation. Before extracting features, we perform a well-designed pipeline to pre-processing the sampled signals. These processes are indeed key modules of WiPIN, which will be elaborated in Section 4. Here we just visualize the extracted features with Generalized Discriminant Analysis (GDA) [18] for these 10 volunteers. The objective function of GDA for multi-class dimensionality reduction can be simplified as Eq. 1

\[
J = \max \frac{D_p}{D_w}
\]

where \(D_p\) is the samples’ distance between different classes, \(D_w\) is the samples’ distance within one class. GDA aims to map the original data into a new feature space where the distance within class is small while the distance between classes is large.
We use a toolbox released by Maaten et. al. [27] and plot the first 2 dominant features in Fig. 3. where every hollow circle represents a dimension-reduced sample. The samples for different volunteers are differentiated via different colors. We can find that the circles with a same color (of one volunteer) are clustered closely, while the clusters of samples (for different volunteers) are separated sparsely. The clear gaps among different clusters indicate that users can be effectively identified if using the Wi-Fi signals. Moreover, the tensely clustered samples also imply high reliability of Wi-Fi signal based person identification.

We are motivated to dig the insight behind the excellent ability of Wi-Fi signals in distinguishing people. It is known that biometric information is related to the human characteristics and hence can be used for personal authentication. Intuitively, the body shape first comes into our mind. Obviously, people in different body shapes yield different signals reflection patterns, which may lead to distinct Wi-Fi signals variation.

Furthermore, We investigate a set of biometrics for the 10 volunteers, including their fat rate, water rate, muscle rate, and bone rate. Then we collect 30 CSI sequences samples for each person, in which 20 are used for training and the left 10 for test. With the training dataset, we setup a mapping rule between the samples and those biometrics using Support Vector Regression (SVR)[24], which is a regression algorithm derived from Support Vector Machine (SVM)[5] and has been implemented at LIBSVM toolbox[2]. We compute the averages value of the prediction results for each person and plot them in Fig. 4. We find that using Wi-Fi signals can accurately predict the four biometrics for people.

\[ S = A e^{-2\pi f t + \phi_0}, \]

(2)

where A is the absorption of propagation media along this path, t is the propagation delay in this path, \(\phi_0\) is the initial phase of the signal, and f is the frequency of the signal. As shown in Fig. 5(a), a larger number of copies of the signal combine together at the Rx antenna due to the multipath effect. In our model we only consider the line-of-sight path of Tx-Rx and the paths that signals are reflected by three layers in the human body. We will describe how WiPIN tackles the issue of multipath effect in Section 4.

For each propagation path, there are several sub-paths in which signal travels in different media. The propagation delay t of a propagation path is the sum of propagation delays over all sub-paths:

\[ t = \sum_{i=1}^{n} t_i, \]

(3)

where n is the number of sub-paths.
For the $i$-th sub-path, the signal propagation delay $t_i$ is calculated via Eq. 4.

$$t_i = \frac{d_i}{v_i}, \quad (4)$$

where $d_i$ is the length of the $i$-th sub-path and $v_i$ is the propagation speed of signals along the $i$-th sub-path.

The propagation speed of signals is computed via Eq. 5[12].

$$v_i = \frac{1}{\sqrt{\mu_i \varepsilon_i}}, \quad (5)$$

where $\mu_i$ and $\varepsilon_i$ are the medium’s permeability and permittivity of the $i$-th sub-path.

Combining Eqs. 2 - 4, we have

$$t = \sum_{i=1}^{n} \frac{d_i}{\sqrt{\mu_i \varepsilon_i}} = \sum_{i=1}^{n} d_i \sqrt{\mu_i \varepsilon_i}. \quad (6)$$

Thus, the signal received from the path $S$ is

$$S = A e^{-j2\pi f \sum_{i=1}^{n} (d_i \sqrt{\mu_i \varepsilon_i})} \phi. \quad (7)$$

From Eq. 7, the received signal is determined by the lengths of sub-paths, the permeability, permittivity, and absorption $A$ of the media. Previous studies reveal that $A$ is correlated with the media characteristics and propagation distance[12]. Suppose that the permeability and permittivity of every medium are known, we have a deduction.

**Theorem 3.1.** Received Wi-Fi signals is deterministic if a standing nearby Tx-RX antenna pair and is determined by the propagation distance within every medium.

which indicates that when a certain person stands nearby the Tx-Rx antenna pairs, the characteristics of his/her body layers including permeability, permittivity and propagation distance result in unique received signals. We utilize to this theorem to identify human.

### 3.2 Theorem Proof

Next, we mathematically prove the Theorem 3.1. by exploring the signal propagation along the 3rd path in Fig. 5(a).

As illustrated in Fig. 5(b), the 3rd path is comprised of a set of sub-paths, including $\overline{AN}$, $\overline{NP}$, $\overline{PC}$ and $\overline{CB}$. According to the refraction/reflection principles, $\overline{AN}$ and $\overline{NP}$ are axial symmetrical with $\overline{PC}$ and $\overline{CB}$. We donate the distance between point A and point B as $\overline{AB}$. We assume that its value is $D$. We also set $\overline{OP} = R_2$ and $\overline{OQ} = l$. We build a plane rectangular coordinate system whose origin point is $A$ and horizontal axis is line $\overline{AB}$. In this plane, the coordinate of point $O$ is $(2/D, -l + R_2)$.

We assume that the coordinate of point $N$ is $(x_0, y_0)$. We aim to calculate $(x_0, y_0)$ to determine all the propagation distance, including $\overline{AN}$, $\overline{NP}$, $\overline{PC}$ and $\overline{CB}$. 

![Figure 5: Interacting Model.](image-url)
WiPIN: Operation-free Person Identification using WiFi Signals

We denote the slope of line $AN$, $NP$, and $NO$ as $k_1$, $k_2$, and $k_3$, respectively. $k_1$, $k_2$, and $k_3$ are computed as

$$k_1 = \frac{y_0}{x_0}$$  \hspace{1cm} (8)

$$k_2 = \frac{y_0 + l - R_2}{x_0 - 2/D}$$  \hspace{1cm} (9)

$$k_3 = \frac{y_0 + l}{x_0 - 2/D}$$  \hspace{1cm} (10)

The included angle between line $AN$ and line $NO$ is denoted as $\theta_1$. We can calculate $\tan \theta_1$ as

$$\tan \theta_1 = \frac{k_1 - k_3}{1 + k_1 k_3}$$  \hspace{1cm} (11)

Similarly, for the included angle between line $NP$ and line $NO$, denoted as $\theta_2$, we have

$$\tan \theta_2 = \frac{k_2 - k_3}{1 + k_2 k_3}$$  \hspace{1cm} (12)

Meanwhile, according to the law of refraction, $\theta_1$ and $\theta_2$ have to meet the following requirement.

$$\sin \theta_1 = \frac{v_1}{v_2}$$  \hspace{1cm} (13)

where $v_1$ is the signal propagation speed within the 1st medium and $v_2$ is the one within the 2nd medium. As in Fig. 5(b), the 1st propagation medium is the air, the 2nd one are the components of human body at the first layer.

We further formulate $NP$ as

$$NP = \sqrt{(x_0 - D/2)^2 + (y_0 + l - R_2)^2}.$$  \hspace{1cm} (14)

We calculate the cosine of $\theta_2$ on triangle $\Delta NOP$:

$$\cos \theta_2 = \frac{NP^2 + R_2 - R_3^2}{2NP \times R_3}.$$  \hspace{1cm} (15)

In addition, $\theta_1$ and $\theta_2$ also satisfy a constraint:

$$0 < \theta_1, \theta_2 < \frac{\pi}{2}.$$  \hspace{1cm} (16)

There are 8 unknown variables, $x_0$, $y_0$, $k_1$, $k_2$, $k_3$, $\theta_1$, $\theta_2$ and $NP$ in Eqs. 7 - 14. Fortunately, we have 8 independent equations. Thus, we can solve the 8 unknown variables, including $x_0$ and $y_0$. As aforementioned, once the coordinate of point $N$ is deterministic, we can obtain the propagation distance within each medium, which is deterministic towards the person. Furthermore, we expect to use the propagation distance of those paths as a unique property towards the person, i.e., his/her fingerprint.

We then simplify the result expression of $x_0$ and $y_0$ as follows,

$$x_0 = f(v_1, v_2, D, l, R_1, R_2, R_3) = f(y_0, e_0, M, E, R, D, l),$$  \hspace{1cm} (17)

$$y_0 = g(v_1, v_2, D, l, R_1, R_2, R_3) = g(y_0, e_0, M, E, R, D, l),$$  \hspace{1cm} (18)

where $\mu_0$ and $\varepsilon_0$ are the permeability and the permittivity of the air, $M$, $E$ and $R$ are the set of permeabilities, permittivities and radiuses of layers of human body.

Ultimately, our interacting model in Eq. 7 is extended to:

$$S = Ae^{-j2\pi f \sum_{i=1}^{M} \phi_i(h_i(x_0, e_0, M, E, R, L))} e^{j\tau_i} + \phi_h,$$  \hspace{1cm} (19)

where $h_i$ is a function to compute the $i$-th sub-path of a given propagation path, and $L$ is the set of location parameters of Tx, Rx and human body.

For different human standing nearby the Tx-Rx antenna pairs, their biometrics vary in $M$, $E$ and $R$. These properties will result in distinct received signals with high probability.

4 SYSTEM DESIGN

WiPIN comprises of three modules: signal pre-processing, feature extraction, and identities matching.

4.1 Signal Pre-processing

WiPIN utilizes the Channel State Information (CSI) to extract required features. Necessary pre-processing procedures are performed in WiPIN, including the noise cancellation and multipath effect mitigation.

4.1.1 Channel State Information. CSI, denoted as $H$ in the following, is a complex number. Its modulus and phase represent the amplitude and phase of Wi-Fi signals, respectively. In indoor environments, besides propagating through the line-of-sight path, Wi-Fi signals are also reflected on the environmental objects, forming variant transmitting paths. The received signal at the receiver is a mixture combined by all signals along these paths[20]. This phenomenon is called multipath effect and can be expressed by the following formula

$$H = \sum_{k=1}^{n} a_k e^{-j2\pi f t_k} + N,$$  \hspace{1cm} (20)

where $k$ is the index of the paths, $a_k$ is the decay of the $k$-th path, and $t_k$ is the delay of the $k$-th path. $N$ is the noise of the channel.

Current Wi-Fi protocols, e.g., IEEE 802.11n/ac, apply orthogonal frequency division modulation (OFDM) in the physical layer. OFDM is an effective method to fully utilize system bandwidth. It splits the available band into several sub-bands, namely subcarriers, where the information is transmitted in parallel. Using the Linux 802.11n CSI tool[13], we can obtain the CSI of 30 subcarriers at 5GHz for each packet. If recording $f$ packets, we can get $H$ that belongs to $C^{f \times 30}$.

4.1.2 Noise Cancellation. The raw CSI $H$ is a matrix of $C^{f \times 30}$, in which each row contains the CSI value of signals at a given time point in 30 subcarriers. As an example, we plot the CSI collected within 1 second in Fig. 6. In this figure, each line stands for the amplitude time series of every subcarrier.
We apply a Butterworth filter to remove the noise[22]. The reason that we choose this filter is because it has smoother pass band responses compared to other filters, such as Chebyshev filter and Elliptic filter. This characteristic helps WiPIN to reserve as much biologic information as possible in the collected signals. In particular, we empirically set the parameter of low-pass Butterworth filter as 5th-order with cut-off frequency of 10Hz to filter noises those with high frequency. The filtered CSI time series are plotted in Fig. 6(b). Then we compute the average value within a short time period, denoted as $l$, for every line to conceal the noise and reduce the $H$’s dimensions to $C_{10}$ for lower computing overhead. We empirically determine the value of $l$ in Section 5.

4.1.3 Multipath Effect Mitigation. As expressed in Eq. 20, CSI is a mixture of signals from all propagation paths, including the line-of-sight path, the paths reflected from human body, and other reflection paths. Our objective is to remove the signals along other reflection paths as much as possible. We apply IFFT on $H$. In our experiment, the bandwidth of the system is 40MHz. Correspondingly, the time resolution is $\Delta t = \frac{1}{B} = 25ns$, which yields a distance resolution of $\Delta t = \frac{1}{B} \times c = 7.5m$. Because the length of $tx$-$human$-$rx$ path is less than 7.5m in our experimental setup, signals along the line-of-sight path and the ones reflected from human body are the dominate part in the first 25ns, as marked within a red bar in Fig. 7. This observation allows us to depress the impact of multipath effect by removing the signals after this period. Note within this period, the signals reflected from the human body are much weaker than the ones from the line-of-sight path. Still, the signals from the line-of-sight can be analogized as a constant, the fluctuation of mixed signals at the receiver are mainly caused by the signals reflected from the human body. Thus, the collected signal is applicable for identifying individual users.

4.2 Feature Extraction

We retain the CSI in all subcarriers since the absorption and reflection at different frequencies are necessarily to be involved in the ultimate features. Specifically, the CSI of all subcarriers implies the signals present selective decline at different frequencies [10], which thoroughly contains the unique feature of each user. After mitigating the impact of multipath effect, the 30 average values of CSI time domain signals are used as 30 features. Besides them, we also leverage another 9 features, once presented in prior works [21, 26], to depict the CSI frequency domain profile.

They are (1) the mean, (2) the standard deviation, (3) the median absolute deviation, (4) the mean absolute deviation, (5) interquartile range, (6) the root mean square, (7) the entropy, (8) the skewness, and (9) the kurtosis of the CSI amplitude profile. The first 6 statistics values are common, so we here explain the meaning of the skewness, the kurtosis and the entropy.

The entropy is used to describe the discrete degree of the CSI amplitude profile. Assume that the maximum and minimum values of CSI are $M$ and $m$, respectively. To calculate the entropy, we equally divide $[m,M]$ into 10 bins, and count the CSI amplitudes $n_i$ that fall in the $i$-th bin. Then, we record $\frac{n_i}{N}$ as the probability that the CSI amplitude profile fall in this bin, donated as $p_i$. The entropy of CSI amplitudes is computed via Eq. 21:

$$E = -\sum_{i=1}^{10} p_i \log p_i.$$  \hspace{1cm} (21)

In particular, the skewness is originally a measure on the asymmetry of the probability distribution in statistics. We adopt this feature to measure the asymmetry of the CSI amplitude profile. We compute the sample skewness using Eq. 22 as follow.

$$s = \frac{1}{n} \sum_{i=1}^{n} (x_i - \bar{x})^3 / \left(\sqrt{\frac{1}{n-1} \sum_{i=1}^{n} (x_i - \bar{x})^2}\right)^{3/2},$$  \hspace{1cm} (22)

where $n$ is the subcarrier number, $\bar{x}$ is the sample mean of CSI amplitudes among all subcarriers, $x_i$ is the amplitude of the $i$-th subcarrier, and $s$ is the skewness.

The kurtosis also describes the shape of a probability distribution. We use it to measure the smoothness of the CSI amplitude profile. We compute the sample kurtosis via Eq. 23.

Figure 6: Noise Cancellation via Butterworth Filter.

Figure 7: Partial Multipath Effect Mitigation.
The task of the matching module is to identify the legitimate user from the others. For each classifier, the classification score is written as:

\[ y_i = \sum_{i=1}^{C} e^{y_i} \]

where \( y_i \) is the predicted identity of the test data, \( i = \min_{i \in [1,2,\ldots,C]} \| y_i - \max \{ y \} \| \).

However, in one-against-all SVM, the number of training data is imbalanced for each of the \( C \) classifiers. This makes it unreliable to directly compare scores among the \( C \) classifiers as in Eq. 26. In this paper, we used a simple and efficient method to compute the confidence scores. Using the softmax function, we first normalize those scores with correct identification results. Such treatment has been widely adopted in the deep-learning[15] community. The normalized \( y_i \) is then used as the confidence that \( x \) is mapped to the \( i \)-th person:

\[ y_i = \frac{e^{y_i}}{\sum_{i=1}^{C} e^{y_i}}. \]

Finally, we determine the confidence threshold of valid identity matching by exploring the distribution of maximum normalized scores of training data. The confidence threshold is set as the 5th percentile of these scores. As an example, we plot 100 maximum scores that correspond to the persons that are correctly identified in Fig. 9. The 5th percentile is 0.5278, which can be considered as the threshold for invalid user detection. In other words, WiPIN will decide a person as invalid if his/her maximum normalized prediction score is lower than 0.5278.

5 EVALUATION

We perform extensive experiments over commodity off-the-shelf Wi-Fi devices and to evaluate performance of WiPIN.

5.1 Experimental Setups

In our experiments, we used two Intel 5300 wireless NICs as the transmitter and receiver, respectively. The communication frequency is 5 GHz and the packet transmission rate is 500 Hz.

As illustrated in Fig. 10, the transmitter and receiver are placed on two cartons of 1.2 m high and 2.4 m apart. We recruited 30 subjects with IRB approval. During the experiment, each volunteer does no any actions, but naturally stands
We evaluate the robustness of WiPIN by investigating the impact of clothing changes and environment noise. We then extended the experiment to detect invalid users. In each experiment trail, we randomly select \( i \) subject (\( i \in \{2, ..., 30\} \)) as valid users. WiPIN was trained on valid users, and tested on these valid users. We repeated the experiment trials for 100 times and report the average accuracies in Fig. 11. We can see that the accuracy gradually decreases with increasing \( i \). WiPIN achieves 100% identification accuracy when \( i = 2 \) (two valid users), remains high identification accuracy, i.e., 92%, for \( i = 30 \) (all users are valid).

We then extended the experiment to detect invalid users. In each experiment trail, \( i \) (\( i \in \{3, ..., 29\} \)) persons are randomly selected as valid user, while others are treated as invalid users. WiPIN was trained on valid users, and tested on all users. In this situation, we define the accurate predictions as those instances that in/valid users are correctly recognized. The accuracy of WiPIN then becomes the ratio of accurate predictions in all test instances. We note that when the number of valid users in the system is small, e.g., \( i = 3 \), WiPIN merely achieves 74% accuracy. With the system has more valid users, the accuracy of WiPIN increases. In particular, WiPIN achieve 92% when \( i = 29 \), implying that WiPIN performs well if the dataset is sufficient large. We will discuss this issue at Section 6.

5.3 Robustness

We evaluate the robustness of WiPIN by investigating the influence from clothing changes and environment noise. **Impact of Clothing Changes:** It is common that users change their clothes. We roughly divide the clothes into three categories (Fig. 15): summer clothes (e.g., T-shirt), autumn clothes (e.g., windbreaker) and winter clothes (e.g., down jacket). We recruit 10 volunteer and ask every volunteer to wear 9 clothes, showed in Fig. 15, to participate in this series of experiments. For each clothes that a volunteer wears, we collect the CSI data for 15 times, 10/15 for further training, 5/15 for further test. We perform 10 cases of training/test processes:

- Case 1 - 3. We select the data of one category of clothes as the training set, build the model, and predict by using the data of all three categories of clothes as the test set.
- Case 4 - 6. We select the data of two categories of clothes as the training set, build the model, and predict by using the data of all three clothes as the test set.
- Case 7. We select the data of all categories of clothes as the training set, build the model, and predict by using the data of all three clothes as the test set.
- Case 8 - 10. We select the data of one category of clothes as the training set, build the model, and predict by using this category of clothes as the test set.

We plot the average classification accuracy for each case in Fig. 12. The first 7 bars indicate that changing clothes has certain impacts on the classification accuracy of WiPIN. However, WiPIN can achieve at least 77% accuracy when utilizing only one category of clothes as the training sets. That is, if the clothes a user wears changes drastically, e.g., from a summer clothes to a winter clothes, the accuracy would decrease. On the other hand, the bars of cases 8 - 10 in Fig. 12 demonstrate that WiPIN achieves an average accuracy of 94%. These results mean that within a certain period, e.g. a session, in which a person wears clothes in a same category, high identification accuracy can be guaranteed.

**Feature Stability vs. Time:** To evaluate the feature stability of WiPIN, we observe the feature changes of 10 volunteers over 15 consecutive days. We apply 2 strategies to train the identification model.

**Strategy 1:** using the CSI data of the first day as the training set, and the data of other days as the test set. This strategy simulates the scenario of non-updating on the user’s biologic features in the database.

**Strategy 2:** using all CSI data in the first \( j \)th days as the training set, and the data after the \( j \)th day as the test set. This strategy correlates the feature-updating enabled scenario. We plot the results in Fig. 13. We find that when using Strategy 1, the accuracy of WiPIN decreases gradually. This is because the Wi-Fi signal is unstable in the environment and a person’s biologic features vary over time. This result shows that time-varying does leave an impact on the feature stability, implying the necessity of updating the features for users. On the other hand, if we allow WiPIN to update the user’s biometric-oriented signal features (as performed in Strategy 2), WiPIN can keep high accuracy in certain period(say, decreasing to 90% after 10 days). In practice, we suggest that a proper updating period is about 10 days.

**Impact of Environment Noises:** We test the impact of environment on WiPIN. We choose 5 different places in our
WiPIN: Operation-free Person Identification using WiFi Signals

Figure 11: Overall Accuracy. Figure 12: Accuracy vs. Clothing. Figure 13: Accuracy vs. Time. Figure 14: Accuracy vs. Rooms.

Figure 15: Three Clothes Categories.

office building, including the places at an empty laboratory #1, a crowded laboratory #2, a crowded seminar room, an empty meeting room, and a narrow corridor, respectively. All these places are diverse in terms of surroundings, i.e., environment noise. We involve 10 volunteers in this experiment. At each place, we collect 15 samples for every volunteer, in which 10 are used as training data and the left as test data. The results are showed in Fig. 14. We can see that the average accuracy is about 94%. Specifically, in the seminar room and corridor, WiPIN does not work as well as in laboratory #1 and the meeting room. This is because the multipath effect is stronger in the former places, making the signals reflected from the human body relatively weaker.

Impact of Antenna Height: We evaluate WiPIN under the height settings of Tx-Rx antenna pair as 0m, 0.4m, 0.8m, 1.2m, 1.6m and 2m, respectively. We also involve 10 volunteers in this experiment. As shown in Fig. 16, WiPIN achieves the best performance with the setting as 1.2m and 1.6m, which corresponds to the average heights of one’s abdomen and chest. Above results imply that a person’s body contributes main affections on the Wi-Fi signals, which coincides with our analysis and model presented in Section 3.

5.4 Computation Overhead

The computation overhead of WiPIN comprises of CSI-signal preprocessing, feature extracting, and user matching. We first examine the accuracy of WiPIN over the 30 volunteers. We adjust the sampling time from 0 to 5 seconds. Fig. 17 shows that WiPIN achieves 92% accuracy while the time that user stands is longer than 200ms in average. Then we collect signals within 200ms and calculate the time required for processing the data collected in this period. We use a desktop PC (with a CPU mode 2.7 GHz Intel Core i5, memory of 8GB DDR3) and run Matlab R2015b to do this computation. As the cumulative computation time shown in Fig. 18, WiPIN requires about 230ms to identify a person. The result proves that WiPIN is time-efficient and applicable to real-time person identification applications.

5.5 Comparison with Prior Works

In this section, we compare WiPIN with three state-of-the-art works, Wi-Who[36], WiFi-ID[37], and FreeSense[34], in Fig. 19. Wi-Who and WiFi-ID can identify up to 6 persons, while FreeSense supports the identification among 9 individuals. As Fig. 19 shows, WiPIN greatly outperforms those three approaches in terms of accuracy. In addition, these works are all operation-based approaches, requiring the user to walk 2m-6m, which is inconvenient and raises barriers for real-world applications.

6 DISCUSSION

Variation of biometrics: The principle of WiPIN is mapping the Wi-Fi signals to the properties of human body. WiPIN works well when the biologic features of users remain stable. However, certain events e.g., losing weight or building muscle, will change the body properties accordingly. Furthermore, if a user suffers from some diseases, e.g., a fever or a diarrhoea, his/her body properties may change sharply.
Under such circumstance, WiPIN will pay a penalty of more frequent updating features for a high identification accuracy.

**Stability of environments:** Although WiPIN mitigates the multipath effect and is tolerant to the variance incurred on the reflection paths with high propagation delay, WiPIN prefers a relatively stable environment. This is because the signals reflecting the person’s biologic information will be significantly influenced if the environment changes too much. Future work can explore more advanced method to extract signals only from human body.

**Sample space of users:** Our experiments in Section 5 show that WiPIN may suffer from a relatively low accuracy in detecting invalid users, like 74% when the system maintains 3 users and merely involves them in training phase. The issue can be addressed if inviting more persons to act as invalid users in the training phase, even if the number of valid users is very small. For example, the accuracy increases to 92% when the number of invalid users becomes 27 in the training phase. In this way, the high accuracy can be guaranteed.

**Applications Scenario:** WiPIN requires users to be at pre-defined positions for identification. This requirement really narrows the application scope of WiPIN. However, we argue that there are still many scenarios where human identity recognition occurs at fixed positions, e.g., the build entrance, and WiPIN is applicable.

### 7 RELATED WORK

Operation based identification usually involves specific motions, actions, and behaviors correlated to human biometrics, including the breathing[3], speaking[9] and walking [11], etc. Several works[6, 23] identify users from the patterns of screen-touching personal device. Monrose et.al. [19] and Tari et.al. [25] utilize the typing styles of users to improve the security of password-inputing. This kind of works are easy to be forged. For example, an attacker might use recorded voices or silicone membranes to cheat the voice or fingerprint based authentication system. However, above attacks do not work for WiPIN, because WiPIN utilizes the reflection and absorption effect of human body on Wi-Fi signals. Attackers may create a human model with 3D print, however the electromagnetic characteristics of human body can not be create.

Recently, a number of researches utilize Wi-Fi signals to grasp the biometric-oriented operations. For example, WiFiU[31], WiWho[36], and WiFi-ID[37] extract human gait patterns via Wi-Fi signals to perform person identification. WiWho identified a person with average accuracy of 92% to 80% from a group of 2 to 6 people. WiFi-ID achieved accuracies of 93 to 77% for 2 to 6 people. WiFiU achieved 79.28% accuracy in a 50 people dataset. The way of users breathing[3], speaking[9] and walking [11] has also been proposed for identification system. These works suppose that people would keep their walking style static, meanwhile, the users are required walk along the same paths when test, which is not practical for use. In addition, this kind of works are also easy to be forged. For example, an attacker can record a video when users walking, then practice to walk with a similar gait as the users to be a fake. Compared to these works, our WiPIN system does not require users to walk along a specific paths when training or test, which is operation-free. What’s more important, forging our WiPIN is full of challenges with the same reasons as the above paragraph said.

Xi et.al develop a Wi-Fi sensing system to count the crowd in the area of interests[32]. Wang et.al propose WiHear to understand the affection pattern of Wi-Fi signal when people are speaking[30]. Ali et.al and Li et.al propose to use Wi-Fi signals to infer keyboard strikes[1]. Wi-Fi signals can also be utilized to track the location of users[14, 16, 29]. WiPIN works in a similar principle above, but extracting distinct features for identification from the extremely ffeble signals against powerful noises and interferences. Besides, identifying human is a much more fine-grained sensing task compared to activity recognition and localization, and WiPIN achieves it.

### 8 CONCLUSION

In this paper, we propose WiPIN, a low-cost, operation-free yet accurate authentication system using COTS Wi-Fi devices. We demonstrated the strong correlation between the variance of Wi-Fi signals and human body components. We
developed an interactive model to analyze the correlation in-depth and a pre-processing pipeline for noise cancellation. Based on the interactive model, we built a high-dimensional mapping from features of Wi-Fi signals to the identity of users. Experimental results show that WiPIN can achieve high identification accuracy in real time.

ACKNOWLEDGE

We thank Wei Xi, Zhiping Jiang, Kun Zhao and Ge Wang for helpful discussion. We thank Li Du, Shiyang Zhuang and Xu He for deploying Linux CSI tool.

REFERENCES

[1] Kamran Ali, Alex X Liu, Wei Wang, and Muhammad Shahzad. 2015. Keystroke Recognition Using WiFi Signals. In Proceedings of ACM MobiCom.
[2] Chih-Chung Chang and Chih-Jen Lin. 2011. LIBSVM: A Library for Support Vector Machines. ACM Transactions on Intelligent Systems and Technology 2 (2011), 27:1–27:27. Issue 3. Software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm.
[3] Jigmohan Chauhan, Tining Hu, Suranga Seneviratne, Archan Misra, Aruna Seneviratne, and Youngki Lee. 2017. BreathPrint: Breathing Acoustics-based User Authentication. In Proceedings of ACM MobiSys.
[4] Andreas Christ, Theodoros Samaras, Anja Klingenböck, and Niels Kuster. 2006. Characterization of the Electromagnetic Near-Field Absorption in Layered Biological Tissue in the Frequency Range From 30 MHz to 6000 MHz. Physics in Medicine and Biology 51, 19 (2006), 4951.
[5] Corinna Cortes and Vladimir Vapnik. 1995. Support-vector networks. Machine learning 20, 3 (1995), 273–297.
[6] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. Touch Me Once and I Know It’s You!: Implicit Authentication based on Touch Screen Patterns. In Proceedings of ACM SIGCHI.
[7] Ilka Dove. 2014. Analysis of Radio Propagation Inside the Human Body for In-Body Localization Purposes. Master thesis, University of Twente.
[8] Rong-En Fan, Kai-Wei Chang, Cho-Jui Hsieh, Xiang-Rui Wang, and Chih-Jen Lin. 2008. LIBLINEAR: A Library for Large Linear Classification. Journal of Machine Learning Research 9, Aug (2008), 1871–1874.
[9] Kevin R Farrell, Richard J Mammone, and Khaled T Assaleh. 1994. Speaker Recognition using Neural Networks and Conventional Classifiers. IEEE Transactions on Speech and Audio Processing 2, 1 (1994), 194–205.
[10] Giorgio Franceschetti and Sabatino Stornelli. 2006. Wireless Networks: From the Physical Layer to Communication, Computing, Sensing and Control. Academic Press.
[11] Davoodzadeh Gafurov, Einar Snekknes, and Patrick Bour. 2007. Spoof Attacks on Gait Authentication System. IEEE Transactions on Information Forensics and Security 2, 3 (2007), 491–502.
[12] Bhag Singh Gaur and Huseyin R Hiziroglu. 2004. Electromagnetic Field Theory Fundamentals. Cambridge University Press.
[13] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. 2011. Tool Release: Gathering 802.11 n Traces with Channel State Information. ACM SIGCOMM Computer Communication Review 41, 1 (2011), 53–53.
[14] Manikanta Kotaru, Kiran Joshi, Dinesh Bhuradia, and Sachin Katti. 2015. Spotfi: Decimeter Level Localization Using WiFi. In Proceedings of ACM SIGCOMM.
[15] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. 2012. ImageNet Classification with Deep Convolutional Neural Networks. In Proceedings of NIPS. MIT Press.
[16] Xiang Li, Shengjie Li, Daqing Zhang, Jie Xiong, Yasha Wang, and Hong Mei. 2016. Dynamic-Music: Accurate Device-free Indoor Localization. In Proceedings of ACM 2016 Ubicomp.
[17] Gregory Melia. 2013. Electromagnetic Absorption by the Human Body from 1-15 GHz. Ph.D. Dissertation. University of York.
[18] Sebastian Milka, Gunnar Ratsch, Jason Weston, Bernhard Scholkopf, and Klaus-Robert Mullers. 1999. Fisher Discriminant Analysis with Kernels. In Processing of IEEE Neural Networks for Signal Processing, Signal Society Workshop.
[19] Fabian Monrose, Michael K Reiter, and Susanne Wetzler. 2002. Password Hardening based on Keystroke Dynamics. International Journal of Information Security 1, 2 (2002), 69–83.
[20] Theodore S Rappaport et al. 1996. Wireless Communications: Principles and Practice. New Jersey: Prentice Hall PTR.
[21] Jorge-L Reyes-Ortiz, Luca Oneto, Albert Sama, Xavier Parra, and Davide Anguita. 2016. Transition-Aware Human Activity Recognition Using Smartphones. Neurocomputing 171 (2016), 734–767.
[22] Ivan W Selesnick and C Sidney Burrus. 1998. Generalized Digital Butterworth Filter Design. IEEE Transactions on Signal Processing 46, 6 (1998), 1688–1694.
[23] Muhammad Shahzad, Alex X Liu, and Arjmand Samuel. 2013. Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures: You Can See It but You Can not Do It. In Proceedings of ACM MobiCom.
[24] Alex J Smola and Bernhard Schölkopf. 2004. A Tutorial on Support Vector Regression. Statistics and Computing 14, 3 (2004), 199–222.
[25] Furkan Tari, Ant Ozok, and Stephen H Holden. 2006. A Comparison of Perceived and Real Shoulder-Surfing Risks between Alphanumeric and Graphical Passwords. In Proceedings of ACM SOUPS.
[26] Edison Thomaz, Irfan Essa, and Gregory D Abowd. 2015. A Practical Approach for Recognizing Eating Moments with Wrist-Mounted Inertial Sensing. In Proceedings of ACM UBICOMP.
[27] Laurens Van Der Maaten, Michael K Reiter, and Susanne Wetzel. 2002. Password Hardening Based on Keystroke Dynamics. J Mach Learn Res 10 (2009), 66–71.
[28] Vladimir Naumovich Vapnik and Vlamin Vapnik. 1998. Statistical Learning Theory. Vol. 1. Wiley New York.
[29] Deepak Vasisht, Swaran Kumar, and Dina Katabi. 2016. Decimeter-Level Localization with a Single WiFi Access Point.. In Proceedings of NSDI.
[30] Guanghua Wang, Yongpan Zou, Zimu Zhou, Kaishun Wu, and Lionel M Ni. 2016. We Can Hear You with Wi-Fi! IEEE Transactions on Mobile Computing 15, 11 (2016), 2907–2920.
[31] Wei Wang, Alex X Liu, and Muhammad Shahzad. 2016. Gait Recognition Using WiFi Signals. In Proceedings of ACM UBICOMP.
[32] Wei Xi, Jizhong Zhao, Xiang-Yang Li, Kun Zhao, Shaojie Tang, Xue Liu, and Zhiping Jiang. 2014. Electronic Frog Eye: Counting Crowd Using WiFi. In Proceedings of IEEE INFOCOM.
[33] Yaxiong Xie, Zhenjiang Li, and Mo Li. 2015. Precise Power Delay Profiling with Commodity WiFi. In Proceedings of ACM MobiCom.
[34] Tong Xin, Bin Guo, Zhi Wang, Mingyang Li, Zhiwen Yu, and Xingshe Zhou. 2016. FreeSense: Indoor Human Identification with Wi-Fi Signals. In Proceedings of IEEE GLOBECOM.
[35] Zheng Yang, Zimu Zhou, and Yunhao Liu. 2013. From RSSI to CSI: Indoor Localization via Channel Response. ACM/IEEE IPSN.
[36] Yunze Zeng, Parth H Pathak, and Prasant Mohapatra. 2016. WiWho: WiFi-Based Person Identification in Smart Spaces. In Proceedings of ACM/IEEE IPSN.
[37] Jin Zhang, Bo Wei, Wen Hu, and Salil S Kanhere. 2016. WiFi-ID: Human Identification Using WiFi Signal. In Proceedings of IEEE DCOSS.