WiFiLeaks: Exposing Stationary Human Presence Through a Wall With Commodity Mobile Devices

Yangyang Gu, Jing Chen, *Senior Member, IEEE*, Kun He, Cong Wu, Ziming Zhao, *Member, IEEE*, and Ruiying Du

***Abstract*—WiFi devices are ubiquitous and may leak user and household privacy. In this paper, we report an attack, namely WiFiLeaks, which uses a commodity mobile device to passively detect stationary human presence through a wall by analyzing the channel state information of wireless signals transmitted by indoor WiFi devices. In our adversarial scenario, attackers cannot control the WiFi transmitter or use advanced radio devices. The main challenge of this attack is how to extract robust features from non-customized signals for stationary human presence. To address this challenge, we first combine methods based on outliers and wavelet denoising to enhance the low-frequency information related to human presence. Then we propose a novel feature extraction method based on the correlation among subcarriers since stationary human presence can enhance their correlations. We evaluate WiFiLeaks using nine different WiFi transmitter and one commodity smartphone in four different settings. The evaluations show WiFiLeaks can still achieve accuracy rates of 83.33% and 100% for human presence and absence at 20 meters between the monitor device and the transmitter in through-the-wall scenarios.**

***Index Terms*—Stationary human detection, channel state information, through the wall, commodity mobile devices.**

I. Introduction

WIFI devices, e.g., routers, smart thermostats, and smart home hubs, play an essential role in our daily lives [1], [2] as their shipments are likely to cross the six-billion mark in 2025 [3]. These devices send WiFi signals all day long, which penetrate walls to ensure coverage. Studies indicate that the presence of human bodies can influence the propagation of WiFi signals [4], [5], and the WiFi Channel State Information (CSI) can capture these variations [6]. As a result, in our adversary scenario, an attacker with a commodity device located outside a room, can use the information to infer human presence inside the room, even if the WiFi devices and network are secure at the data link layer and above. This attack, namely Through-The-Wall (TTW) human detection attack, violates WiFi users' privacy and also poses potential risks such as burglary or kidnapping when the attacker identifies the absence or presence of individuals within a room [7]. With the rise of single-person households [8], this attack will become a huge potential threat.

While existing WiFi-based human detection methods primarily focus on detecting moving human presence based on temporal variations in multipath signals [9], [10], [11], [12], our work addresses the challenge of detecting stationary human presence in TTW scenarios. To characterize the minor impact of stationary human presence, previous methods either require the WiFi transmitter to actively transmit specific signals with a high rate (e.g., 1,000 packets per second) or passively rely on specialized radio devices, such as Universal Software Radio Peripheral (USRP) to obtain high time-resolution and signal-to-noise data [13], [14], [15], [16], [17]. These constraints limit the application of these approaches to our adversarial scenario.

To passively infer stationary human presence in TTW scenarios using a commodity WiFi device, such as a smartphone, we must tackle two key challenges. The *first challenge* lies in characterizing stationary human presence from the collected raw data with low time-resolution, since the transmitter operates at a low and unstable packet transmission rate in passive adversary scenarios. For example, a well-functioning WiFi camera typically has a mean packet rate of only 108 [9], resulting in the loss of some temporal details compared to the previously mentioned packet rate of 1,000. To address this, we explore continuous CSI measurements, which contain multiple subcarrier, from a spatial perspective rather than focusing solely on temporal variations. In other words, we vertically explore the relationship among CSI subcarriers rather than the horizontal time variation of certain subcarriers, as motivated by [18]. Specifically, we characterize stationary human presence by calculating the correlation among subcarriers, since the correlation is more distinguishable than the temporal variation of subcarriers as discussed in Section II-B. Furthermore, we extract a new robust feature to characterize stationary human presence from this correlation analysis.

The *second challenge* pertains to the low signal-to-noise ratio of the raw CSI signal caused by signal attenuation through walls. Although the influence of human presence on the CSI signal is concentrated at low frequencies [13], the influence of walls on CSI makes it difficult to obtain a CSI signal with a high signal-to-noise ratio using conventional band-pass filtering. Therefore, we opt for the wavelet transform

Manuscript received 3 July 2023; revised 12 October 2023; accepted 25 October 2023. Date of publication 30 October 2023; date of current version 7 May 2024. This research was supported in part by the National Key R&D Program of China under Grant 2021YFB2700200, and in part by the National Natural Science Foundation of China under Grants U1836202, 61772383, 62076187, 61802214, and 62172303. Recommended for acceptance by D. Koutsonikolas. *(Corresponding author: Jing Chen.)*

Yangyang Gu, Jing Chen, Kun He, Cong Wu, and Ruiying Du are with the School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China (e-mail: guyangyang.whu.edu.cn; chenjing@whu.edu.cn; hekun@whu.edu.cn; cnacwu@whu.edu.cn; duraying@whu.edu.cn).

Ziming Zhao is with Computer Science and Engineering, University at Buffalo, Buffalo, NY 14068 USA (e-mail: zimingzh@buffalo.edu).

Digital Object Identifier 10.1109/TMC.2023.3328349

to decompose and reconstruct the CSI signal. In doing so, we meticulously select appropriate wavelet bases and other parameters for the wavelet transform to achieve high-quality signals. Before applying the wavelet transform, we employ a Hampel filter [19] with a window size equal to the length of the sample, as opposed to the default value, to eliminate outliers while preserving sufficient detail for stationary human detection.

In this paper, we propose WiFiLeaks, the first TTW human detection attack that passively achieves accurate inference of stationary human presence using commodity mobile devices. Here, *stationary* refers to subjects standing or sitting with minimal activities, such as reading. Additionally, WiFiLeaks outperforms previous methods in detecting moving human presence. In the feature extraction module, we use eigenvectors and 2-norm normalization to highlight the correlation among CSI subcarriers as well as to improve the generalization of the final feature, respectively. In the model training module, we utilize Support Vector Machine (SVM) [20] for classifying human presence and absence, which is lightweight for a commodity device. *Ablation Studies* in Section IV-D and *Comparison with State-of-Art* in Section IV-H demonstrate the effectiveness and superiority of our methods. The attacker can collect training data from a similar room to the target room to pre-train the attack model. Our experimental results demonstrate that WiFiLeaks is effective for unseen subjects and devices in the training data, and a short period of stationary human presence data (e.g., 5 minutes) is sufficient for training the model.

The contributions of this paper are summarized as follows:

- We design WiFiLeaks, the first TTW human detection attack that passively detects stationary human presence through the wall based on CSI just using commodity devices. WiFiLeaks also achieves higher accuracy in detecting moving human presence than prior works.
- We present an analysis of why human presence increases the correlation among CSI subcarriers, and demonstrate that the correlation among CSI subcarriers is more distinguishable than the temporal variation of subcarriers.
- We employ a data processing method rooted in the specially parameterized Hampel filter and wavelet transform to emphasize the influence of human body on the CSI weakened by the wall. This method enables WiFiLeaks to introduce a robust feature extraction method based on the subcarrier correlation to characterize the stationary human presence from CSI.
- We evaluate WiFiLeaks with nine WiFi devices, including routers, cameras, and home voice assistants, and one commodity smartphone in four rooms with different sizes and wall types. The experiment results show that WiFiLeaks achieves an accuracy of 83.33% and 100% for human presence and absence at a distance of 20 meters between the monitor device and the transmitting device in TTW scenarios.

II. Background

A. CSI Signal

CSI is the physical channel state information of wireless signals on different subcarriers with different frequencies [21]. It describes how these signals propagate from the transmitter to the receiver at certain carrier frequencies. The wireless signal propagates through multiple paths and arrives at the receiver with different time delays and signal attenuation incurred by signal reflection, diffraction, and scattering of surrounding objects. A CSI measurement on multiple frequencies can be formulated as

$$\boldsymbol{h} = (H(t; f_1), \ldots, H(t; f_k), \ldots, H(t; f_N))^T, \tag{1}$$

where f_k is the frequency of the kth subcarrier and N is the number of subcarriers. $H(t; f_k)$ is the CSI value over the kth subcarrier, which is a complex value with amplitude and phase [22], [23], [24]. Specifically, $H(t; f_k)$ can be formulated as

$$H(t; f_k) = \sum_{j=1}^{M} a_j(t) e^{i(\phi_j + 2\pi f_k \tau_j(t))}, \tag{2}$$

where M is the number of multipath components, $a_j(t)$ is the amplitude of the jth path, $\tau_j(t)$ is the time delay, and ϕ_j is the phase delay caused by reflections or diffraction. $a_j(t)$, $\tau_j(t)$, and ϕ_j represent the characteristics of the propagation path j.

The CSI measurement can be computed by analyzing the received packets [6], [21], [25]. In our work, we utilize nexmon_csi [6], which is available for 64 subcarriers at 2.4 G bandwidth 20 MHz channel bandwidth. Our work focuses on sensing humans using commodity mobile devices, which are commonly equipped with a single antenna. We exploit the amplitude of CSI, i.e., $|H(t; f_k)|$ for sensing, as it is more reliable than phase measurements when using a single antenna to receive wireless signals [9], [26], [27].

B. CSI Model Affected by Human Presence and Wall Blocking

The multipath propagation of the wireless signal consists of M_{sta} static paths independent on the human body and M_{dyn} dynamic paths dependent on the human body [22], [28]. Therefore, $H(t; f_k)$ can be donated as a sum of two components

$$H(t; f_k) = H_{sta}(f_k) + H_{dyn}(t; f_k), \tag{3}$$

where the static component $H_{sta}(f_k)$ is time-invariant due to the cluster of multipath components with fixed lengths. $H_{sta}(f_k)$ can be denoted as

$$H_{sta}(f_k) = a_{sta}(f_k) e^{i\phi_{sta}(f_k)}, \tag{4}$$

where $a_{sta}(f_k)$ and $\phi_{sta}(f_k)$ are the amplitude and phase at the frequency f_k. The diffraction paths caused by the human body have lower amplitude and random phase changes. Therefore, we only consider the reflection paths which have obviously changing amplitudes, and assume that different subcarriers share the same reflection path. The jth propagation is with amplitude

$a_j(t)$ and time delay $\tau_j(t)$. $H_{dyn}(t; f_k)$ can be denoted as

$$H_{dyn}(t; f_k) = \sum_{j=1}^{M_{dyn}} a_j(t) e^{-i2\pi f_k \tau_j(t) + i\phi_j}, \tag{5}$$

where $a_j(t)$ is time-varying and depends on the sum of the distance between the person and the transceiver [29], [30]. By applying the Friis path loss equation, $a_j(t)$ can be denoted as

$$a_j(t) = \frac{\alpha d_0 \sqrt{P_r}}{d_j(t)}, \tag{6}$$

where α is the reflection loss, d_0 is the distance between the transmitter and the receiver, P_r is the received power, and $d_j(t)$ is the sum of the distance between the person and the transceiver.

To simplify the calculation, we first assume that there is only one specular reflection path, so the amplitude response of the kth subcarrier can be denoted as

$$\begin{aligned} |H(t; f_k)| = {} & [2a_{sta}(f_k)a_j(t)\cos(2\pi f_k \tau_j(t) + \phi_{sta}(f_k) \\ & + \phi_j(f_k)) + a_{sta}^2(f_k) + a_j^2(t)]^{\frac{1}{2}} + N(o, \sigma_{amp}), \end{aligned} \tag{7}$$

where $N(o, \sigma_{amp})$ is the white noise and phase shift of the jth reflection path $f_k \tau_j(t) = \frac{f_k d_j(t)}{c}$ (c is the speed of light).

From (7), we can derive that human presence can increase the correlation among subcarriers. We discuss the reasons from two aspects of stationary human presence and moving human presence. When the person is in a stationary state, the difference between two subcarriers with frequencies f_1 and f_2 mainly depends on $2a_s(f_k)a_j(t)\cos(2\pi f_k \tau_j(t) + \phi_{sta}(f_k) + \phi_j(f_k))$ in (7) since $a_j(t)$ keeps constant. Therefore, the smaller the difference between f_1 and f_2, the more similar trend the change of the two subcarriers. However, the correlation between subcarriers in the stationary state is slightly higher than that of an empty room since the limitation of the range of the cosine term $\cos(2\pi f_k \tau_j(t) + \phi_{sta}(f_k) + \phi_j(f_k))$. When the person is in a moving state, the change of the subcarrier amplitude is mainly affected by the change of the term $a_j^2(t)$ in (7). Therefore, the correlation among subcarriers is significantly larger than that of an empty room. In the condition of multiple reflection paths, the same conclusion can be drawn using a similar analysis.

The energy of the received signal will be significantly reduced if the wall blocks direct and reflection propagation paths. For instance, the power of the received signal is attenuated by 10∽18 dB when the 2.4 G WiFi signal passes through the plain concrete wall [31]. This is equivalent to adding a noise N_w to (7)

$$\begin{aligned} |H(t; f_k)| = {} & [2a_{sta}(f_k)a_j(t)\cos(2\pi f_k \tau_j(t) + \phi_{sta}(f_k) \\ & + \phi_j(f_k)) + a_{sta}^2(f_k) + a_j^2(t)]^{\frac{1}{2}} \\ & + N_w + N(o, \sigma_{amp}). \end{aligned} \tag{8}$$

Therefore, the CSI measurements may lose the characteristics of amplitude's variability due to the influence of obstacles [4].

C. Feasibility Validation

To validate the effect of human presence and wall blocking on CSI, we collect data from a WiFi camera (XiaoYi Smart Camera Y3), which has a relatively stable upload data stream at a mean rate of 78 packets per second. The camera is connected to a wireless router working at 2.4 G in a room, which has a wooden door and one double-glazed wall, and three concrete walls. During the data collection, two monitoring devices of the same type, i.e., two Nexus 5 phones, collect the CSI data. One device is 2 meters from the door outside the room, while the other is beside the door inside the room. The camera in the diagonal corner of the door is 8 meters from the phone inside the room. To compare the effects of the moving person and the stationary person, we collect both types of data. Specifically, there is one human subject inside the room walking around during the moving data collection and sitting on a chair during the stationary data collection. Some raw CSI data collected is shown in Fig. 1.

We focus on CSI measurements influenced by the moving/stationary person to detect human presence in TTW scenarios. Comparing Fig. 1(a) and (d), we find that the amplitude changes still have a certain similarity, but the amplitude range is decreasing when one person is moving in the room. However, comparing Fig. 1(b) and (e), (c) and (f), there is no obvious similarity in the amplitude changes, and the outdoor amplitude does not seem to describe the same influence as the indoor amplitude due to the impact of the wall. Fig. 1(d), (e), and (f) show outdoor amplitude changes of the same subcarrier under three states (moving, stationary, and empty). We can observe that the influence of a moving person on CSI is greater and more discriminative than that of an empty room. However, the impact of a sitting person on CSI is almost the same as that of an empty room.

As Fig. 1 shows, using only the amplitude changes in the time domain to distinguish a stationary person and an empty room is difficult. We choose to instead extract features from the correlation of subcarriers. Fig. 2 shows three subcarriers for stationary human presence and absence after removing some outliers with the Hampel filter [19]. The data sources of Fig. 2(a) and (b) are the same as Fig. 1(e) and (f), respectively. Correlation coefficients of three subcarriers in Fig. 2(a) are 0.74, 0.63, and 0.75 respectively, while that in Fig. 2(b) are 0.61, 0.48, and 0.37 respectively. The correlation of amplitude changes influenced by stationary human presence is higher than that influenced by human absence.

III. System Design

In this section, we present the threat model first and then illustrate the design of WiFiLeaks.

A. Threat Model

We assume the attacker has the following capabilities and limitations: i) the attacker can approach the target room to palace a monitor device and has access to rough floor plans of the target room, which correspond to the threat model of

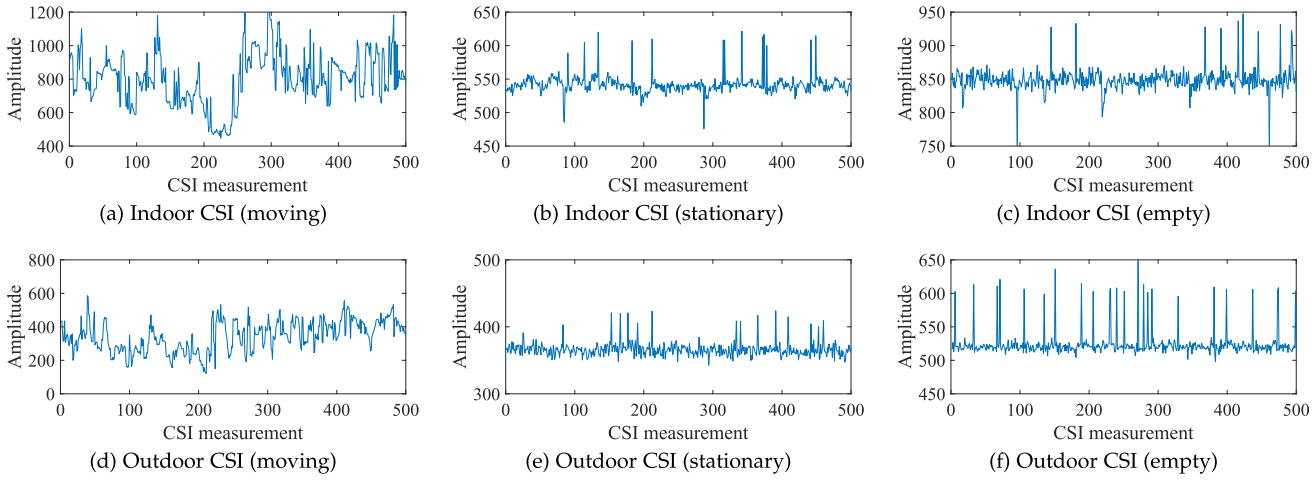


Fig. 1. Raw amplitude of the subcarrier with the same sequence number when two identical monitoring devices collect data at the same time inside the room and outside the room. (a) Collected indoors with a subject moving. (b) Collected indoors with a subject stationary. (c) Collected indoors with the room empty. (d) Collected outdoors with a subject moving. (e) Collected outdoors with a subject stationary. (f) Collected outdoors with the room empty.

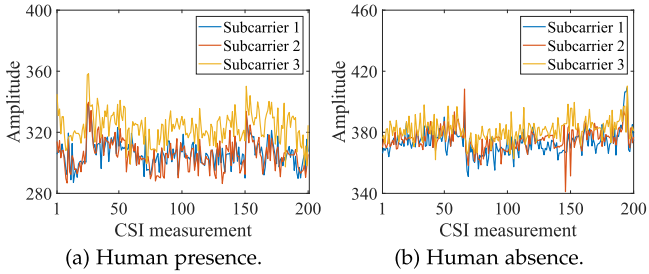


Fig. 2. Amplitude changes of three subcarriers influenced by (a) stationary human presence and (b) human absence.

previous attack [9]; ii) the attacker cannot enter the target room to deploy any customized devices, and has no knowledge of the location of wireless devices; iii) the attacker cannot utilize specialized high-level devices, e.g., antenna arrays and USRP radios. We note that the attack is passive, and it is not easy to be perceived by people around. In our attack scenario, the attacker uses only a commodity mobile device for sensing.

B. Problem Formulation

Our attack is to passively infer human presence using a commodity mobile device in TTW scenarios, which can be formulated as a binary classification model $g_\theta : \boldsymbol{H} \rightarrow [0, 1]$, where g_θ represents the model with the parameters θ and $\boldsymbol{H}$ is a CSI sample. Specifically, our work can simultaneously satisfy three requirements for a practical attack scenario that existing work cannot simultaneously meet: i) the definition of human presence includes stationary people and not just moving ones; ii) perform long-distance (e.g., greater than 10 meters) human detection in TTW scenarios; iii) it cannot control the transmitter to emit a specific signal source or use some expensive specialized equipment as detectors.

C. Overview of WiFiLeaks

WiFiLeaks consists of four modules: *data collector*, *data preprocessor*, *feature extractor*, and *human detector*, as shown in Fig. 3.

The data collector module passively eavesdrops on the WiFi data packets nearby by a common mobile device, which makes our attack more concealed. The data preprocessor module removes experimental noise to highlight the impact of stationary human presence. On the basis of the correlation among subcarriers, the feature extractor module conducts a feature extraction method that can capture the subtle difference between stationary human presence and human absence. Finally, the human detector module builds a detection model in the training phase and detects whether someone is in the target room by the detection model in the attack phase.

D. Data Collector

WiFiLeaks sniffs the WiFi signals nearby and separates the data streams based on source MAC addresses. It selects the wireless device with the faster data transmission rate from the available ones as the target device in the attack phase. In the training phase, the attacker collects the CSI measurements of human presence and absence from a similar room to the target room, respectively. In the attack phase, WiFiLeaks collects the CSI measurements from the target room to detect human presence. Note that, the CSI measurement monitoring is concealed, as the monitoring device works passively, i.e., not interfering with the normal work of the WiFi device or sending any packets. We can obtain a sequence $\boldsymbol{S}$ of CSI measurements, which can be given as $\boldsymbol{S} = (\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_w)^T$, where w is the number of CSI measurements collected.

E. Data Preprocessor

In the data processor, WiFiLeaks removes experimental noise and highlights the impact of stationary human presence. During

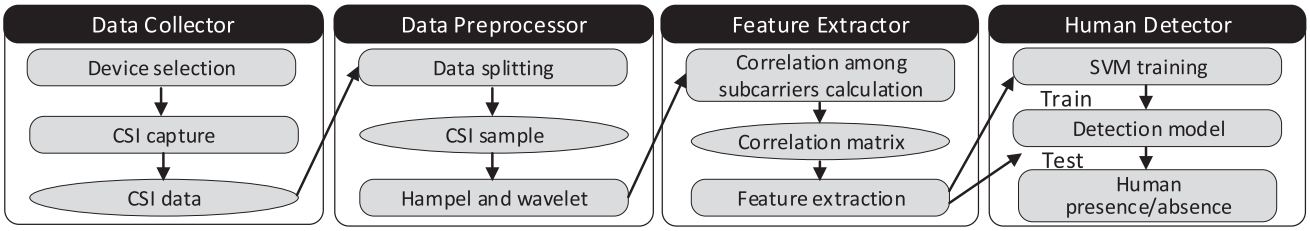
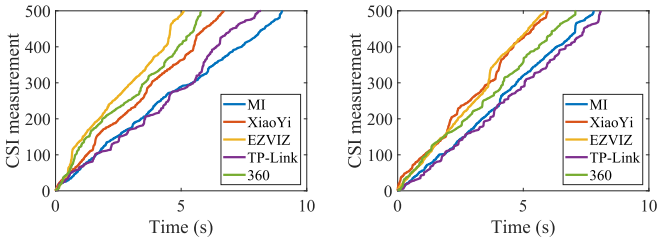
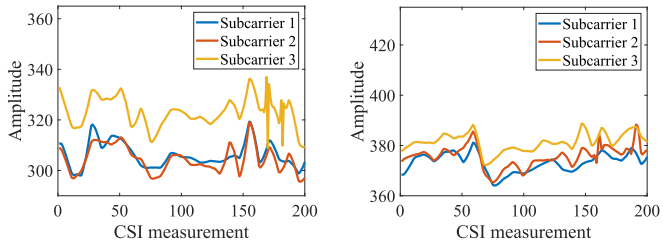


Fig. 3. Workflow of WiFiLeaks.



(a) Human presence. (b) Human absence.

Fig. 4. Relationship between the number and timestamp of CSI measurements collected from different bands of WiFi cameras under (a) human presence and (b) human absence conditions.



(a) Human presence. (b) Human absence.

Fig. 5. Amplitude changes of three subcarriers influenced by (a) stationary human presence and (b) human absence after denoising.

the training phase, it first splits the sequence $\boldsymbol{S}$ into samples at an interval of K.

Data Splitting: The traffic shows different patterns for different WiFi devices, even for the same type of device. As an example, Fig. 4 shows the relationship between the number and timestamp of CSI measurements from different devices. To weaken the instability of data in the time domain, WiFiLeaks packs r continuous CSI measurements of $\boldsymbol{S}$ into a sample. The lasting time of collecting r CSI measurements is t_r. If not a sufficient amount of CSI measurements are collected, these data will be discarded in the training and attack phase.

Specifically, the two attributes must satisfy the following valid condition: $\begin{cases} r = K \\ t_r \leq T_K \end{cases}$, where K and T_K are the thresholds for the two attributes, respectively. A sample $\boldsymbol{H}$ can be expressed as

$$\boldsymbol{H} = (|\boldsymbol{h}_1|, |\boldsymbol{h}_2|, \ldots, |\boldsymbol{h}_K|)^T, \tag{9}$$

where $|\boldsymbol{h}_K|$ represents the amplitude of the Kth CSI measurement. We define H_j as the amplitude of the jth subcarrier, which is a K-dimensional column vector.

Hampel and Wavelet: WiFiLeaks performs denoising to remove the noise of CSI data while retaining the characteristics regarding stationary human detection. It first empirically removes n subcarriers with many burst noises near the guard bands from available subcarriers [32], [33]. WiFiLeaks applies the commonly used Hampel filter [19] to each subcarrier. The window size of the filter is equal to the number of CSI measurements in a sample. The value will be replaced with the median of the subcarrier when the value differs from the median by more than three standard deviations. Specifically, the normal value must satisfy the following valid condition: $||H(t; f_k)| - \mu| \leq 3\sigma$, where μ and σ are the median and the MAD of the kth subcarrier. Then we empirically use a 3-level "Sym4" wavelet transform [34] with a posterior median threshold rule on the amplitude of each subcarrier to enhance the low-frequency information related to human presence. Fig. 5 shows three subcarriers influenced by stationary human presence and absence after removing the noise. The correlation among subcarriers of stationary human presence is higher than that of human absence.

At the end of the data preprocessor module, WiFiLeaks obtains the sample $\boldsymbol{H'}$, which can be expressed as

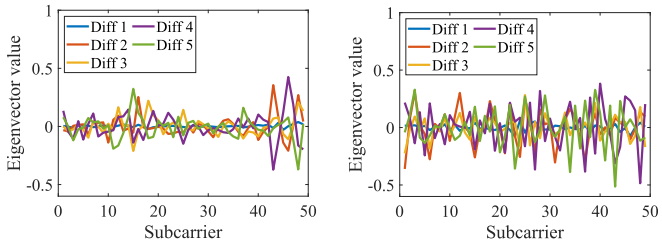
$$\boldsymbol{H'} = (H'_1, H'_2, \ldots, H'_M), \tag{10}$$

where H'_M represents the Mth denoised subcarrier.

F. Feature Extractor

Although some existing works [9], [14], [27] are very effective in distinguishing between moving human presence and absence by using some features in the time domain, e.g., variance, these features are ineffective to detect stationary human presence. Inspired by R-TTWD [18], WiFiLeaks focuses on the frequency domain characteristics of CSI, that is, the correlation among subcarriers, which is more distinguishing than variations in the time domain as shown in Fig. 5. Different from R-TTWD, WiFiLeaks only uses the outlier-based data cleaning methods and the more robust wavelet denoising method for the CSI data, which retains more detailed information and provides the possibility of detecting stationary human presence. Moreover, WiFiLeaks performs 2-norm normalization to improve the generalization ability of the feature.

Correlation Among Subcarriers Calculation: WiFiLeaks calculates the correlation among subcarriers for feature extraction. Based on the observation of the correlation among subcarriers,



(a) Human presence. (b) Human absence.

Fig. 6. First-order difference values of some eigenvectors from two samples of (a) human presence and (b) human absence. The data source is the same as Fig. 2.

WiFiLeaks uses the Pearson correlation coefficient to measure the correlation. The correlation coefficient $C(j,l)$ of the jth subcarrier H'_j and the lth subcarrier H'_l can be given as

$$C(j,l) = \frac{\sum_{q=1}^{K}\left(H'_j(q)-\bar{H'_j}\right)\left(H'_l(q)-\bar{H'_l}\right)}{\sqrt{\sum_{q=1}^{K}\left(H'_j(q)-\bar{H'_j}^2\right)\sum_{q=1}^{K}\left(H'_l(q)-\bar{H'_l}^2\right)}}, \tag{11}$$

where $\bar{H'_j} = \sum_{q=1}^{K} H'_j(q)/K$ and $\bar{H'_l} = \sum_{q=1}^{K} H'_l(q)/K$.

The correlation matrix $\boldsymbol{C}$ can be expressed as

$$\boldsymbol{C} = \begin{bmatrix} C(1,1) & \cdots & C(1,M) \\ C(2,1) & \cdots & C(2,M) \\ \vdots & \ddots & \vdots \\ C(M,1) & \cdots & C(M,M) \end{bmatrix}. \tag{12}$$

Feature Extraction: This step is to extract the feature of the stationary human presence from the correlation matrix. To highlight the correlation characteristics among subcarriers, WiFiLeaks performs eigendecomposition [35] on this matrix. The eigenvector matrix can be expressed as $\boldsymbol{P} = (\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_m, \ldots, \boldsymbol{p}_M)$. Compared with Fig. 6(a) and (b), the first-order difference values of some eigenvectors for stationary human presence are less than that for human absence. As a result, WiFiLeaks calculates the mean of the second-order difference of the eigenvectors to obtain further fluctuation characteristics and gets the array $\boldsymbol{u} = (u_1, u_2, \ldots, u_m, \ldots, u_M)$, where u_m can be given as

$$u_m = \frac{\sum_{j=2}^{M-1} |\boldsymbol{p}_m(j+1) - 2\boldsymbol{p}_m(j) + \boldsymbol{p}_m(j-1)|}{M-2}. \tag{13}$$

Furthermore, to improve the generalization ability of the model, WiFiLeaks performs 2-norm normalization on the array $\boldsymbol{u}$. Finally, we obtain the final feature $\boldsymbol{F} = (f_1, f_2, \ldots, f_m, \ldots, f_M)$, where f_m can be given as

$$f_m = \frac{u_m}{\sqrt{\sum_{j=1}^{M} d_j^2}}. \tag{14}$$

G. Human Detector

WiFiLeaks trains the detection model in the training phase and uses the model to detect stationary human presence in the attack phase. We conduct the SVM [20] on the training data to train a detection model in the training phase. SVM transforms low-dimensional nonlinear data into linear data in high-dimensional space through the kernel function. It then finds the optimal classification hyperplane by maximizing the distance from the support vectors on both sides, where the support vector consists of the sample points closest to the hyperplane. Therefore, SVM is suitable for classifying stationary samples and empty samples with small differences. Additionally, the decision function of SVM depends on a few support vectors, which can simplify the computational complexity. In the training phase, to find a parameter combination with good generalization performance, we perform a grid search with the 5-fold cross-validation using the training data. The final combination is shown in Table I. WiFiLeaks directly uses feature $\boldsymbol{F}$ as the input of the classifier to detect stationary human presence in the attack phase.

TABLE I
KEY PARAMETERS USED IN OUR EXPERIMENTS

Parameters	Value
The dimension M of $\boldsymbol{H}$, the number n of removed subcarriers	50, 2
$kernel$ and $gamma$ of SVM	rbf, 6
Sample size K	1000
Time threshold of collecting a sample T_K	30s

TABLE II
SPECIFIC ROOMS USED IN OUR EXPERIMENTS

Room	Length	Width	Height	Wall type
Room 1	8.9m	5.9m	3m	Concrete (20cm), double-glazed (8cm)
Room 2	14.5m	9m	3m	Concrete (25cm)
Room 3	8.8m	4.5m	3m	Concrete (20cm), double-glazed (8cm)
Room 4	8.9m	5.9m	3m	Concrete (20cm), double-glazed (8cm)

IV. EXPERIMENT AND EVALUATION

In this section, we present the evaluation setup of WiFiLeaks, and report the evaluation results in different settings, including different splitting parameters, devices, subjects, room layouts, proportions, locations, distances, etc.

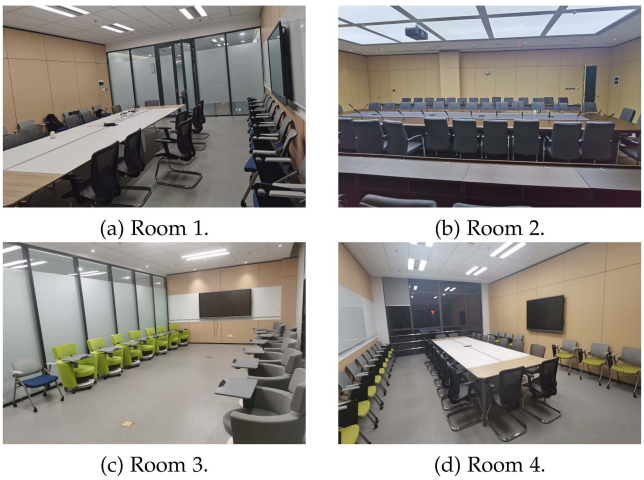
A. Experimental Setup

Evaluation Scenario: We used the CSI extraction tool nexmon_csi [6] to collect CSI measurements, which can be easily deployed on mobile devices. The LG Nexus 5 smartphone was used as the monitoring device. We used the *monitor* mode of the WiFi chip to collect all nearby WiFi packets. We also used a CISCO router as the wireless device in the target room, which worked at a 2.4 G band with 20 MHz channel bandwidth. Therefore, only 52 subcarriers are available for the Data Preprocessor module [33]. We evaluated the performance of WiFiLeaks using nine different WiFi devices as shown in Table III in four rooms as shown in Fig. 7. Under these settings, the smartphone passively collected CSI measurements and other meta information, such

TABLE III
SPECIFIC DEVICES USED IN OUR EXPERIMENTS

Device Type	Device Model	Mean Packet Per Second
WiFi Camera	XiaoMi Cloud Camera (MI)	61
	XiaoYi Smart Camera Y3 (Y3)	78
	EZVIZ C6CN (C6CN)	96
	TP-Link TL-IPC43AN-4 (C43)	56
	360 D806 Cloud Camera (D806)	80
WiFi Router	TP-LINK_C7A4 (C7A4)	108
	CISCO RV100W (Cisco)	100
Home Voice Assistant	XiaoMi AI Speaker (MiAi)	2
	Amazon Echo (Echo)	0.36

We use the abbreviations in parentheses to indicate specific devices in the rest of the paper. For example, Y3 stands for xiaoyi smart camera Y3.



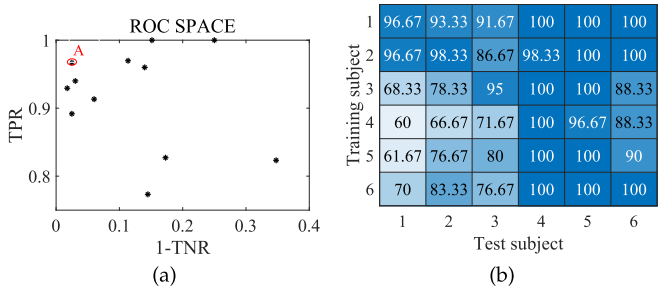
(a) Room 1. (b) Room 2. (c) Room 3. (d) Room 4.

Fig. 7. Four rooms used in our experiments. (a), (b), and (c) Three conference rooms (Room1, Room 2, and Room 3) of different sizes and layouts. (d) A conference room (Room 4) with the same layout as Room 1 but in a different location. Specific information is shown in Table II.

as timestamps and MAC addresses of wireless devices. The key parameters are listed in Table I.

Evaluation Metrics: We use the following metrics to evaluate the performance of WiFiLeaks: i) True Positive Rate (TPR) is defined as the correct detection ratio of samples collected when the human is present, i.e., TPR $= \frac{\text{TP}}{\text{TP+FN}}$, where TP is the number of positive samples that are correctly detected. FN is the number of positive samples that are falsely detected as negative; ii) True Negative Rate (TNR) is defined as the correct detection ratio of samples collected when no human is present, i.e., TNR $= \frac{\text{TN}}{\text{TN+FP}}$, where TN is the number of negative samples that are correctly detected. FP is the number of negative samples that are falsely detected as positive. In addition, we use the Receiver Operating Characteristic (ROC) space [36] to find the optimal K value in Section IV-B. ROC space can be used to compare the performance of different K values by plotting the TPR along the y-axis and 1-TNR along the x-axis. In ROC space, the better values are in the upper, left corner (high TPR, high TNR).

Data Collection: To verify that WiFiLeaks is still effective for moving human presence, we also collected a small amount of moving data when collecting stationary data, and regarded



(a) (b)

Fig. 8. (a) ROC SPACE of different sample sizes. (b) The confusion matrix of testing the model trained by the data from a single subject. The value omits the percent sign.

these two types of data as human presence data. Specifically, we collected CSI measurements in two different settings: i) human absence data: there was no subject in the target room; ii) human presence data: one or more subjects were moving or stationary in the room. The subject in the room was required to randomly move for about five minutes and then sit on a chair for more fifteen minutes. In addition, the subject sitting on a chair was allowed to do simple activities, e.g., reading. To avoid additional interference from other moving objects, there were no moving objects around the receiver when it was collecting data. Unless otherwise specified, Room 1 (Fig. 7(a)) with Y3 was the main experimental scenario and the receiver was 2 meters from the room.

B. Impact of Splitting Parameters

We evaluate the impact of the proposed data-splitting method. Initially, we determine the threshold for K based on the valid condition mentioned in Section III-E. Subsequently, we determine the threshold for T_K using Table III.

For our evaluation, we consider a sample size ranging from 100 to 1,200 in steps of 100. To determine the optimal K value, we present the ROC space based on the evaluation results. Fig. 8(a) illustrates that point **A** is closest to the point (0, 1), with a corresponding sample size of 1,000. Considering the ROC space of other devices, we ultimately choose 1,000 as the value of K for our experiments. Additionally, we set the value of T_K at 30 seconds based on the transmission rates of various devices in Table III and our specific practice. Notably, MiAi and Echo have slower data transmission rates, so their sample size values for K and T_K are 100 and 50 (for MiAi) and 60 seconds and 180 seconds (for Echo), respectively.

C. Generalization Performance of WiFiLeaks

To evaluate the generalization performance of WiFiLeaks under different conditions such as different devices, subjects, and room layouts, we collected datasets under each condition. We randomly selected some data for model training, while the remaining data was for model evaluation. The details of data collection and the performance evaluation of WiFiLeaks under different conditions are presented in the subsequent sections.

TABLE IV
GENERALIZATION PERFORMANCE OF WIFILEAKS UNDER DIFFERENT DEVICES

Training device	MI	Y3	C6CN	C43	D806	C7A4	Cisco	MiAi	Echo
Y3, Cisco, D806	81.67% 97.5%	100% 100%	68.33% 100%	100% 92.5%	83.33% 100%	98.33% 100%	100% 95%	85.71% 80%	40% 100%
MI, Cisco, D806	85% 100%	100% 100%	65% 100%	96.67% 100%	95% 100%	98.33% 100%	95% 95%	85.71% 93.33%	26.67% 100%
MI, Cisco, C6CN	96.67% 97.5%	100% 100%	93.33% 92.5%	100% 37.5%	100% 100%	100% 97.5%	100% 100%	100% 10%	73.33% 100%
MI, C43, C6CN	95% 100%	100% 100%	90% 100%	96.67% 77.5%	88.33% 100%	100% 97.5%	100% 100%	94.29% 33.33%	60% 100%

Training datasets of training devices are used to train the model. Datasets of all devices are used to test the model. Two numbers in each grid represent TPR and TNR, respectively.

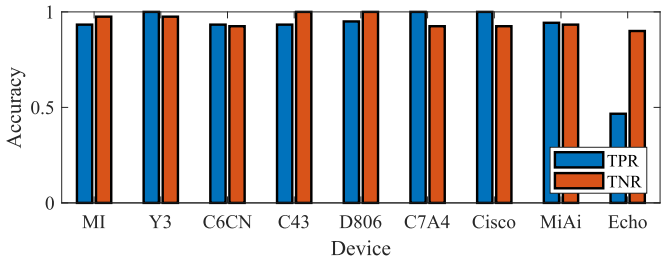


Fig. 9. Accuracy of WiFiLeaks for different devices.

TABLE V
TPR VALUES OF WIFILEAKS WITH THE MODEL TRAINED ON DATASETS FROM TWO SUBJECTS

Training subject	Subject 1	Subject 2	Subject 3	Subject 4	Subject 5	Subject 6
Subject 1, 5	88.33%	88.33%	86.67%	100%	100%	98.33%
Subject 2, 4	91.67%	95%	86.67%	100%	100%	98.33%
Subject 3, 6	85%	90%	95%	100%	100%	98.33%
Subject 1, 6	88.33%	90%	83.33%	100%	100%	100%

1) Applicability and Generalization Performance of WiFiLeaks Under Different Devices: To assess the impact of different devices, we selected three common and typical device types: WiFi cameras, WiFi routers, and home voice assistants (as shown in Table III). In Room 1, we invited two subjects to participate in this evaluation. For each device, we collected one dataset containing 60 k CSI measurements as human presence data from each subject, along with two datasets containing 80 k CSI measurements as human absence data. For applicability evaluation, we used one dataset of human presence data and one dataset of human absence data as the training dataset for each device. The remaining datasets were used as the test dataset. To evaluate generalization, we randomly selected three training datasets from the three devices to train a multi-device model, and other datasets from all devices were used to evaluate the model.

The applicability performance is illustrated in Fig. 9, where the TPR values of the devices are 93.33%, 100%, 93.33%, 93.33%, 95%, 100%, 100%, 94.29%, and 46.67%, respectively, while the TNR values are 97.5%, 97.5%, 92.5%, 100%, 100%, 92.5%, 92.5%, 93.33%, and 90%, respectively. The accuracy rates of WiFi cameras and WiFi routers all exceed 90%, while the accuracy rates of Echo are relatively low due to its low data transmission rate. Notably, MiAi achieves satisfactory accuracy despite its low mean packet per second. Although the amplitude of low-rate CSI signals may be less effective in expressing the characteristics of human presence in noisy environments, the overall performance demonstrates the wide applicability of WiFiLeaks to different devices.

The generalization performance is summarized in Table IV, where four cases are presented due to space limitations. The table reveals that most devices achieve TPR and TNR values exceeding 85%, while the performance of voice assistants is relatively poorer due to their low data transmission rates. These results indicate that the attacker can achieve good attack performance even without prior knowledge of the target device's information. Overall, the results verify the generalization capability of WiFiLeaks to different devices.

2) Generalization Performance of WiFiLeaks Under Different Subjects: To evaluate the impact of different subjects on accuracy, we collected 6 $\times$ 60 k CSI measurements as human presence data from six subjects (four males and two females) with variations in height, weight, and body shape. The 80 k CSI measurements collected in the previous section served as human absence data. Half of the human absence data was used for model training, while the other half was used for testing. We evaluated the generalization performance of WiFiLeaks by training models with data from one subject and two subjects, respectively, and testing the models with the remaining data.

Fig. 8(b) presents the TPR confusion matrix for the model trained using the human presence data from a single subject, with TNR values consistently reaching 100%. The performance of the last three subjects is relatively poor, with the lowest TPR value at only 60%. However, when training the model using human presence data from two subjects, the overall performance is satisfactory, as shown in Table V (partial results displayed due to space limitations). The lowest TPR value still reaches 85%. These results indicate that the attacker can achieve good attack performance even without collecting training data from the target subject, thereby confirming the generalization capability of WiFiLeaks to different subjects.

3) Applicability and Generalization Performance of WiFiLeaks Under Different Room Layouts: Considering the possible impact of different room layouts, we selected four

TABLE VI
EVALUATION RESULTS OF THE CROSS TEST FOR Y3 IN ROOM 1

Training room	Room 1	Room 2	Room 3	Room 4
Room 1	93.33% 100%	79% 0	98.33% 57.5%	100% 90%
Room 2	98.33% 0	95% 97.5%	100% 0	100% 35%
Room 3	56.67% 100%	26.67% 80%	93.33% 97.5%	100% 100%
Room 4	93.33% 100%	79% 0	98.33% 57.5%	100% 90%
Room 1, Room 2	86.67% 100%	46.67% 25%	100% 60%	100% 100%

Two numbers in each grid represent TPR and TNR, respectively.

different rooms as shown in Fig. 7. Room 1 features coated glass walls on the front and back and concrete walls on the sides. Room 2 is entirely surrounded by concrete walls. Room 3 has concrete walls on three sides and glass on the remaining side. Room 4 has the same wall type and size as Room 1 but differs in location and certain furniture arrangements. Table II provides specific information about these rooms. Two subjects participated in this evaluation. For each room, we collected 60 k CSI measurements as human presence data from each subject, along with 80 k CSI measurements as human absence data. One subject's human presence data and half of the human absence data were used to train a model for each room, while the remaining data was used for testing.

Table VI presents the TPR and TNR values for each room, where the TPR values range from 93.33% to 100% and the TNR values range from 97.5% to 100%. However, the test results for room layouts with significant differences (e.g., Room 1 and Room 2) exhibit relatively poor performance, with a TPR value of only 46.67% for the test data from Room 2, even when training the model with data from Room 1 and Room 2. Notably, the cross-test results for Room 1 and Room 4 yield satisfactory performance. These results indicate that the attacker can achieve good attack performance by collecting training data from a room similar to the target room, thereby confirming the wide applicability and generalization capability of WiFiLeaks to similar rooms.

The above evaluation results demonstrate that the attacker can collect training data from specific devices and subjects in a room similar to the target room to achieve successful attacks. This significantly enhances the attack's feasibility, stealth, and the risk of exposing human presence privacy.

D. Ablation Studies

To demonstrate the effectiveness of WiFiLeaks, we conducted ablation studies on our proposed methods for human presence information enhancement and feature extraction. These studies were performed using the dataset collected in Section IV-C1 from Y3. We investigated the impact of removing the wavelet denoising module or the Hampel filter and wavelet denoising module from the data preprocessor. Furthermore, we explored the impact of using first-order difference in [18] instead of second-order difference with 2-norm normalization in our scheme. As shown in Table VII, the best performance is achieved using our complete scheme, indicating that removing any of the mentioned modules would be detrimental to the task of human presence detection. These results confirm the effectiveness of our proposed methods for our attack.

TABLE VII
PERFORMANCE OF COMPARING WIFILEAKS WITH REMOVING THE MODULE OF WAVELET DENOISING AND HAMPEL FILTER & WAVELET DENOISING, AND REPLACING THE FEATURE EXTRACTION METHOD WITH THAT IN [18]

Metrics	Wavelet	Wavelet & Hampel	Feature	WiFiLeaks
TPR	71%	75%	73.33%	95%
TNR	95%	2.5%	100%	97.5%

TABLE VIII
EVALUATION RESULTS OF THE CROSS TEST FOR Y3 IN ROOM 1

Proportion	Mo → Mo	St → Mo	Mo → St	St → St
0	100%	27.5%	100%	100%
20%	100%	72.5%	100%	92.5%
40%	100%	77.5%	100%	92.5%
60%	100%	87.5%	100%	92.5%
80%	100%	87.5%	100%	92.5%
100%	100%	92.5%	100%	92.5%

MO and *ST* represent moving data and stationary data. For example, the intersection of *ST* → MO and 20% represents that the testing data is the stationary data, and the human presence training data consists of one set of moving data and 20% of one set of stationary data.

E. Impact of the Proportion of Training Data

To assess the impact of different proportions of the moving data and stationary data in the training data on attack performance, we conducted an evaluation involving two subjects. For each subject, we collected 40 k CSI measurements for both moving data and stationary data. The evaluation utilized the human absence data obtained from Y3 (described in Section IV-C1). We employed various ratios of moving data and stationary data from one subject as positive data for training the detection model. The remaining data collected from the other subject was used to evaluate the attack model.

When the detection model is trained with no moving data, the accuracy of the human absence data is 17.5%. However, under all other conditions, the accuracy consistently reaches 100%. Table VIII demonstrates that the accuracy of the moving data is consistently 100%, surpassing the performance of prior works [9], [13], [18], [27]. Without the inclusion of stationary data in the training data, the accuracy of the stationary data is only 27.5%. Nevertheless, when the proportion of stationary data reaches 60%, the accuracy of stationary human presence is 87.5%. Models trained primarily with stationary data consistently achieve high accuracy rates. This can be attributed to the fact that our model is capable of distinguishing between stationary human presence and absence. As a result, the characteristics of moving human presence closely resemble those of stationary samples, making it easier to differentiate moving testing samples as human presence. Therefore, attackers need to gather sufficient stationary training data. For instance, Table III indicates that approximately 5 minutes of data collection time

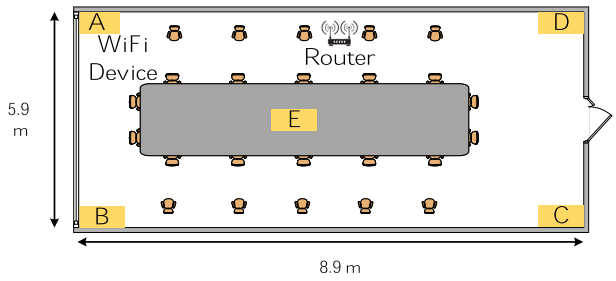


Fig. 10. Five locations (A, B, C, D, and E) of WiFi devices in Room 1.

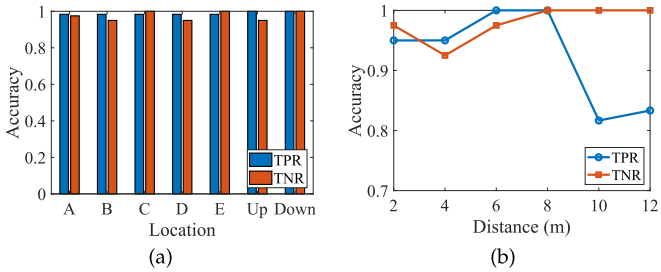


Fig. 11. Accuracy of WiFiLeaks for different locations and distances. (a) Values of TPR and TNR for different locations. "Up" and "Down" represent that the location of the monitoring device is upstairs and downstairs, respectively. (b) Values of TNR and TPR for different distances.

is required when the proportion of stationary data is 60%. This approach proves to be time-saving and practical for attackers.

F. Impact of Locations of the Target Device

To assess the impact of the transmitter's location within the room, we positioned the target device (Y3) in five different locations within Room 1, as depicted in Fig. 10. Two subjects participated in the data collection process, with only one subject present in the room at a time. Additionally, the monitoring device was placed upstairs and downstairs to collect data when the transmitter was located at position E. We collected 60 k CSI measurements as human presence data from each subject and 80 k CSI measurements as human absence data at each location. For each location, we employed the human presence data from one subject and the human absence data (40 k CSI measurements) to train an attack model. The remaining data served as test data.

Fig. 11(a) illustrates the performance of WiFiLeaks at different locations. The TPR values for the seven locations are 98.33%, 98.33%, 98.33%, 98.33%, 98.33%, 100%, and 100%, while the TNR values are 97.5%, 95%, 100%, 95%, 100%, 95%, and 100%. Varying the locations of the transmitter and receiver can induce changes in the multipath transmission of the signal. However, such changes do not significantly affect the accuracy of WiFiLeaks. Consequently, WiFiLeaks exhibits consistent performance across different locations of the target device.

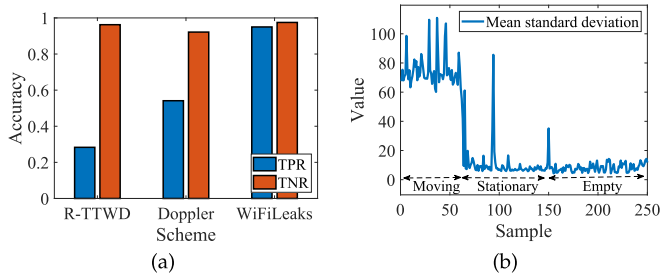


Fig. 12. (a) Values of TPR and TNR for different schemes. (b) Standard deviation of different types of data (i.e., moving, stationary, and empty data).

G. Impact of Distances of the Monitoring Device

Considering the attenuation of the WiFi signal at different propagation distances, we positioned the monitoring device at distances of two, four, six, eight, ten, and twelve meters from the room to collect CSI data. Two subjects participated in the data collection process, with 60 k CSI measurements collected as human presence data from each subject and 80 k CSI measurements collected as human absence data at each distance. Similar to previous experiments, we employed the human presence data from one subject and the human absence data (40 k CSI measurements) to train an attack model for each distance. The remaining data served as test data.

Fig. 11(b) presents the performance of WiFiLeaks at different distances. From a distance of 2 meters to 12 meters, TPR values are 95%, 95%, 100%, 100%, 81.67%, and 83.33%, respectively, and TNR values are 97.5%, 92.5%, 97.5%, 100%, 100%, and 100%. Notably, TPR exhibits a slight downward trend when the distance exceeds 8 meters. However, even at a distance of 12 meters, the TPR remains at 83.33%, with the TNR value at 100%. Furthermore, considering that the distance between the WiFi device and the wall is approximately 8 meters within the room, the distance between the monitoring device and the WiFi device is approximately 20 meters at a distance of 12 meters. Therefore, WiFiLeaks still performs well at relatively long distances of up to 20 meters in TTW scenarios.

H. Comparison With State-of-the-Art

To demonstrate the advantages of WiFiLeaks, we compared it with state-of-the-art TTW human detection schemes. Since there was no prior work that specifically addresses the passive detection of stationary human presence in TTW scenarios using a single monitor with a single antenna, we compared WiFiLeaks with schemes that shared similar features, applications, or devices. Specifically, we compare WiFiLeaks with R-TTWD [18], which also relies on correlation across subcarriers for its features. However, R-TTWD's data processing and feature extraction may overlook certain detailed information, rendering it ineffective for stationary human detection. As depicted in Fig. 12(a), R-TTWD achieves a TPR of 54.14% and a TNR of 92.16%. We also compare WiFiLeaks with DOPPLER [15], which can detect stationary human presence using six pairs of antennas. Since our data was derived from a single pair of antennas, it may not provide sufficient resolution for DOPPLER,

TABLE IX
EVALUATION RESULTS OF DIFFERENT FEATURE SOURCES

Feature source	Amplitude	Phase	Amplitude & Phase
TPR	95%	86.67%	88.33%
TNR	97.5%	0	20%

resulting in suboptimal performance in our scenarios. As shown in Fig. 12(a), DOPPLER attains a TPR of 28.33% and a TNR of 96.25%, while WiFiLeaks achieves a TPR of 95% and a TNR of 97.5%. Finally, we compare WiFiLeaks with Etu [9], which is designed for moving human detection using a threshold based on standard deviation with the same type of device as WiFiLeaks. Since the threshold depends on the specific scenario, we directly display the mean standard deviation in Fig. 12(b) calculated by Etu's method with our data. As depicted in Fig. 12(b), the values calculated from samples of moving subjects are significantly higher than those from empty room samples, indicating the effectiveness of Etu for moving human detection. However, the values calculated from samples of stationary subjects are nearly identical to those from empty room samples, suggesting that Etu's method may not be suitable for stationary human detection in our scenarios. Additional comparisons can be found in Table X.

V. MITIGATION TECHNIQUES

WiFiLeaks relies on two key factors: i) the ability of indoor wireless devices to transmit WiFi signals that can penetrate most walls, including concrete and glass walls [31], enabling the monitoring device to capture indoor WiFi signals; ii) the stronger correlation among subcarriers influenced by human presence compared to human absence. In this section, we discuss potential mitigation techniques against WiFiLeaks based on these factors.

Regarding the first factor, there are two possible defensive approaches: focusing on WiFi devices and obstacles. To prevent the sniffing of signals by the monitoring device outside the room, one option is to reduce the transmission power of WiFi devices. However, this also impacts the signal quality and functionality of the WiFi devices. Alternatively, a directional antenna can be used to narrow the signal-receiving area, although this integration may incur additional costs [37]. Increasing the difficulty of signal transmission through obstacles can be achieved using electromagnetic shielding techniques [38]. However, this also introduces additional costs and may affect the normal operation of other WiFi devices in the room, such as smartphones. Therefore, defending against WiFiLeaks based on the first factor can be costly.

For the second factor, one defense is to introduce co-channel interference to reduce the correlation among subcarriers [39]. However, deploying additional co-channel Access Points (APs) may negatively affect the signal quality of regular WiFi communication. Additionally, most existing routers have built-in mechanisms for automatically switching wireless channels. Another defensive approach is signal obfuscation [9], [37]. For instance, PhyCloak [37] disrupts the CSI by utilizing a full-duplex radio, but this solution comes at a high cost. Another defense proposed in [9] involves an AP sending customized fake data packets at random power levels, similar to the power of the actual transmitter. It relies on the AP sending customized fake data packets, which can increase power consumption but may be a potential effective defensive approach.

VI. DISCUSSIONS

We discuss the limitations of WiFiLeaks and our future work in this section.

A. Limitations

WiFiLeaks still has certain limitations that require further improvement.

Training Data Collection: WiFiLeaks relies on diverse training data to enhance its effectiveness in detecting human presence as shown in Table VIII. However, when the data from stationary subjects comprises 60% of the overall dataset, the detection accuracy rate can reach 87.5%. Additionally, the environment and devices inside the room generally remain unchanged over a short period, ensuring that the trained model can be used for an extended period.

Interference From Moving Objects: While WiFiLeaks can achieve long-distance detection, it requires an unobstructed path between the monitoring device and the room during the detection process. Any other moving objects present could result in false decisions. In our experiment, we asked a human subject to walk between the monitoring device and the room when the room was empty. With a distance of ten meters between the room and the monitoring device, we collected twenty samples, but only one was classified correctly.

Attack Platform: Although WiFiLeaks relies on a rooted smartphone for collecting WiFi data packets, it can also be deployed on other platforms with the assistance of nexmon_csi [32]. Besides the Android platform, an embedded platform like Raspberry Pi is an ideal choice for deploying WiFiLeaks to create a device for human presence detection. Therefore, root access is not essential for WiFiLeaks to perform the attack.

Room Layout: As shown in Table VI, the performance of WiFiLeaks is not always good for rooms with large differences and good for similar rooms. Considering scenarios such as commercial rooms and hotel rooms with uniform layouts that are common nowadays, the threat to user privacy from WiFiLeaks remains high. Therefore, the limitation of different room layouts to our work is limited.

B. Detection Performance on Multiple Subjects

To evaluate the performance of WiFiLeaks in scenarios involving multiple subjects in the target room, we collected 20 k CSI measurements for two, three, and four subjects respectively, which served as the test data to evaluate the model trained in Section IV-C1 for Y3. When collecting data, there were no restrictions on their positions, movements, etc. The results indicate that all TPR values are 100%, which is reasonable since the presence of multiple subjects improves the correlation across subcarriers as described in Section II-B. Although WiFiLeaks performs well in multi-subject scenarios, it may fail to detect the

TABLE X
TYPICAL HUMAN PRESENCE DETECTION SCHEMES

Reference	Application	Sensing Type	Scenario	Distance	Feature and Classifier
Etu [9]	Moving-only	Passive sensing	TTW	12m	Mean standard deviation, threshold-based
R-TTWD [18]	Moving-only	Active sensing	TTW	6m	The first-order difference, one-class SVM
DOPPLER [15]	Stationary-included	Active sensing	TTW	9m	Mean Doppler spectrum, naïve bayes classifier
TWPad [16]	Stationary-included	Active sensing	TTW	N/A	AoA, joint hypothesis statistical test
DeMan [13]	Stationary-included	Active sensing	Indoor	6m	Eigenvalue, sinusoidal model
Non-Linear [30]	Stationary-included	Active sensing	Indoor	5m	kPCA, threshold-based
WiFiLeaks	**Stationary-included**	**Passive sensing**	**TTW**	**20m**	**The second-order difference, SVM**

Distance denotes the distance between the receiver and the transmitter.

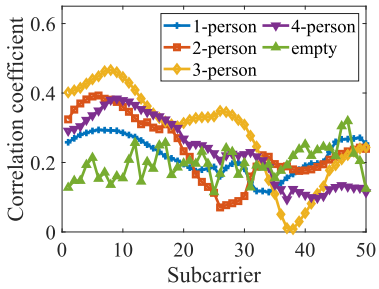


Fig. 13. Correlation coefficients for samples of different subject numbers in the room.

exact number of indoor subjects in certain situations. We utilized the multi-subject data to assess whether the features extracted by WiFiLeaks could be used for human number detection. We employed the K Nearest Neighbor (KNN) algorithm for multi-classification, but the accuracy rate achieved was only 32.5%. Existing solutions [40], [41], [42] focus on estimating the number of subjects in indoor scenarios, where more detailed features can be captured. However, Fig. 13 demonstrates that the correlation relationship in multi-subject scenarios exhibits strong similarity, making it challenging to distinguish the number of subjects. Moreover, existing solutions require active transmitter control to transmit specific signals, which is not suitable for our passive scenarios. It should be noted that counting the number of subjects in the room falls outside the scope of our work.

C. Detection Performance Using Phase of CSI

The phase of CSI can capture more subtle motions in indoor scenarios, such as human breathing sensing [43]. To assess the performance of applying the phase of CSI in our TTW scenario, we also extracted features from the phase in addition to the amplitude. We trained a model using the phase features alone and another model using both amplitude and phase features. Table IX presents the results, showing that the TPR and TNR values for the models using phase features are 86.67% and 0, and 88.33% and 20%, respectively. In contrast, the model utilizing amplitude features achieves TPR and TNR values of 95% and 97.5%. The reason behind this discrepancy is that the phase captured by our passive monitor with a single antenna suffers from synchronization errors with the transmitter and is influenced by the presence of walls [9], [44]. Hence, we exclusively utilize the amplitude of CSI in our scheme.

D. Distinction Between Humans and Other Moving Objects

In smart homes, there are many moving objects, such as pets and sweeping robots. A natural question is whether the solution for detecting human presence can distinguish between moving humans and other moving objects. Zhu et al. [9] made a similar attack to ours, where we have similar experiment environments and devices. The evaluation results in [9] show that their attack cannot distinguish pet moving and human moving because pets cause similar impacts as humans on CSI collected from common WiFi devices, e.g., wireless cameras and routers. Therefore, it can be inferred that our attack cannot distinguish between humans and pets either. It may be helpful to distinguish humans from other moving objects using some dedicated signal transmitter, e.g., USRP, to build models for each type of moving object. However, the strong requirement limits the practicability of WiFiLeaks in our scenarios. We may study this issue as another work.

VII. RELATED WORK

Due to the fact that CSI measurements reflect the physical channel status of wireless signals, and are susceptible to moving subjects, CSI can achieve finer-grained sensing of physical environments. Therefore, CSI is widely used for human activity detection [22], [45], [46], [47], [48], [49], [50], [51], human identification [52], [53], [53], [54], [55], [56]. However, there exist some strict requirements for human activity detection and human identification, such as a high transmission rate of 1,000 packets per second, dedicated hardware, line-of-sight environments, etc. In this section, we focus on CSI-based human presence detection methods and brief recent studies, which can be categorized into moving-only and stationary-included.

For moving-only methods, they focus on detecting moving subjects to enrich services, e.g., intrusion detection, emergency response, and track trajectory. Some researchers [45], [57], [58], [59] focused on detecting whether there are moving subjects in the target area by monitoring the variety of subcarriers incurred by motions. Wilson et al. [10] proposed to track the subject's motion trajectory by monitoring the variety of CSI from different WiFi devices. Zhou et al. [60] used pre-established CSI fingerprints in the target environment to detect human presence and estimate the subject's location. Some researchers [11], [12] proposed new quantitative metrics to detect moving human presence. However, these methods are based on the impact of moving subjects on the subcarrier's variation and are only effective

for moving human presence. WiFiLeaks adopts a novel feature extraction method based on the correlation among subcarriers to reserve the impact of both moving and stationary subjects on CSI. Zhu et al. [18] also extracted a feature based on the correlation. However, this feature cannot capture the information related to stationary human presence and is only effective for moving human presence in their experiments.

For stationary-included methods, their requirements are impractical under our adversarial scenario. Wu et al. [13] required the transmitter and receiver to be indoors to capture the subtle variations, e.g., breathing, caused by the stationary human body in the room, while these subtle variations are difficult to capture in TTW scenarios [4]. Domenico et al. [15] utilized the analysis of the mean Doppler spectrum which requires a fixed frequency data transmission rate. However, in our adversary scenario, the attacker has no permission or access to the WiFi network and the WiFi device inside the room. Some researchers [16], [17] achieved stationary human detection based on the Angle of Arrival (AoA) or the Time-Reversal (TR) technique. They both require devices equipped with antenna arrays and the receiver to be actively connected to the transmitter, which is demanding in our adversarial scenario.

Importantly, existing methods heavily depend on the stable packet rate of the wireless transmitter, or even on installing the conspicuous antenna arrays at a short distance [14], [61], [62], [63]. These constrained conditions bring significant challenges to adversarial TTW scenarios. Zhu et al. [9] made a meaningful attempt under these challenges. They tracked the moving subject in the adversarial TTW scenario based on the knowledge of the floor plan of the target room or building. They first estimated the coarse locations of the anchors (selected WiFi signal transmitters), then detected the movement trajectory of the subject based on the impact of the moving subject near an anchor on the variety of CSI measurements. However, the stationary subject has little impact on the variety of CSI measurements as shown in Fig. 2, which is hard to detect in their adversary TTW scenarios.

Different from previous work, WiFiLeaks utilizes CSI to detect moving and stationary subjects in TTW scenarios. Comparing with typical human presence detection methods, our work can detect human presence at a longer distance in adversarial TTW scenarios.

VIII. Conclusion

We present WiFiLeaks as a practical CSI-based stationary human presence detection attack and implement it on the LG Nexus 5. Unlike existing moving-only and stationary-included methods that only detect moving subjects or actively send costumed signals to detect stationary subjects, WiFiLeaks passively detects stationary human presence in TTW scenarios with high accuracy and generalizes to moving human presence with better performance than prior works. The attack is implemented by monitoring indoor CSI measurements and developing human presence detection models. We evaluate our attack using 4,877 k CSI measurements of the training and test data collected in different conditions. WiFiLeaks is effective for unseen subjects and devices in the training data, and a short period of stationary human presence data (e.g., 5 minutes) is sufficient for training the model. Experiment results also demonstrate that WiFiLeaks can still achieve the accuracy rates of 83.33% and 100% for human presence and absence at a distance of 20 meters between our monitor device and the indoor WiFi device in TTW scenarios.

References

[1] HornerNetworks, "Smart home layout," 2021. [Online]. Available: https://www.hornernetworks.com/smart-home-layout

[2] onefirefly, "Smart layouts," 2021. [Online]. Available: https://onefirefly.com/creative-services/smart-layouts

[3] A. Jain, "Smart home market witnessing rapid growth," 2021. [Online]. Available: https://www.counterpointresearch.com/smart-home-market-witnessing-rapid-growth/

[4] X. Wu, Z. Chu, P. Yang, C. Xiang, X. Zheng, and W. Huang, "TW-See: Human activity recognition through the wall with commodity Wi-Fi devices," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 306–319, Jan. 2019.

[5] K. Joshi, D. Bharadia, M. Kotaru, and S. Katti, "WiDeo: Fine-grained device-free motion tracing using RF backscatter," in *Proc. 12th USENIX Symp. Netw. Syst. Des. Implementation*, 2015, pp. 189–204.

[6] F. Gringoli, M. Schulz, J. Link, and M. Hollick, "Free your CSI: A channel state information extraction platform for modern Wi-Fi chipsets," in *Proc. 13th Int. Workshop Wireless Netw. Testbeds Exp. Eval. Characterization*, 2019, pp. 21–28.

[7] K. Iboshi, "We asked 86 burglars how they broke into homes," 2019. [Online]. Available: https://www.ktvb.com/article/news/crime/we-asked-86-burglars-how-they-broke-into-homes/277--344333696

[8] P. N. Cohen, "The rise of one-person households," *Socius*, vol. 7, 2021, Art. no. 23780231211062315.

[9] Y. Zhu et al., "Et Tu Alexa? When commodity WiFi devices turn into adversarial motion sensors," in *Proc. 27th Annu. Netw. Distrib. Syst. Secur. Symp.*, 2020.

[10] J. Wilson and N. Patwari, "See-through walls: Motion tracking using variance-based radio tomography networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 5, pp. 612–621, May 2011.

[11] L. Gong et al., "An adaptive wireless passive human detection via fine-grained physical layer information," *Ad Hoc Netw.*, vol. 38, pp. 38–50, 2016.

[12] Z. Zhou, Z. Yang, C. Wu, Y. Liu, and L. M. Ni, "On multipath link characterization and adaptation for device-free human detection," in *Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst.*, 2015, pp. 389–398.

[13] C. Wu, Z. Yang, Z. Zhou, X. Liu, Y. Liu, and J. Cao, "Non-invasive detection of moving and stationary human with WiFi," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 11, pp. 2329–2342, Nov. 2015.

[14] F. Adib and D. Katabi, "See through walls with WiFi!," in *Proc. ACM SIGCOMM Conf. SIGCOMM*, 2013, pp. 75–86.

[15] S. D. Domenico, M. D. Sanctis, E. Cianca, and M. Ruggieri, "WiFi-based through-the-wall presence detection of stationary and moving humans analyzing the doppler spectrum," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 33, no. 5/6, pp. 14–19, May/Jun. 2018.

[16] J. Wang, Z. Tian, X. Yang, M. Zhou, and Y. She, "TWPad: Through the wall passive human detection based on joint hypothesis statistical test," in *Proc. IEEE Int. Conf. Commun.*, 2021, pp. 1–6.

[17] Q. Xu, Y. Chen, B. Wang, and K. Liu, "Radio biometrics: Human recognition through a wall," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 5, pp. 1141–1155, May 2017.

[18] H. Zhu, F. Xiao, L. Sun, R. Wang, and P. Yang, "R-TTWD: Robust device-free through-the-wall detection of moving human with WiFi," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 5, pp. 1090–1103, May 2017.

[19] L. Davies and U. Gather, "The identification of multiple outliers," *J. Amer. Stat. Assoc.*, vol. 88, pp. 782–792, 1993.

[20] C. Chang and C. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intell. Syst. Technol.*, vol. 2, 2011, Art. no. 27.

[21] Y. Xie, Z. Li, and M. Li, "Precise power delay profiling with commodity WiFi," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, 2015, pp. 53–64.

[22] W. Wang, A. Liu, M. Shahzad, K. Ling, and S. Lu, "Understanding and modeling of WiFi signal based human activity recognition," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, 2015, pp. 65–76.

[23] K. Qian, C. Wu, Z. Yang, Y. Liu, and K. Jamieson, "Widar: Decimeter-level passive tracking via velocity monitoring with commodity Wi-Fi," in *Proc. 18th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2017, Art. no. 6.

[24] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[25] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: Gathering 802.11n traces with channel state information," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 41, 2011, Art. no. 53.
[26] J. Gjengset, J. Xiong, G. McPhillips, and K. Jamieson, "Phaser: Enabling phased array signal processing on commodity WiFi access points," in *Proc. 20th Annu. Int. Conf. Mobile Comput. Netw.*, 2014, pp. 153–164.
[27] K. Qian, C. Wu, Z. Yang, Y. Liu, and Z. Zhou, "PADS: Passive detection of moving targets with dynamic speed using PHY layer information," in *Proc. IEEE 20th Int. Conf. Parallel Distrib. Syst.*, 2014, pp. 1–8.
[28] D. Wu, Y. Zeng, F. Zhang, and D. Zhang, "WiFi CSI-based device-free sensing: From fresnel zone model to CSI-ratio model," *CCF Trans. Pervasive Comput. Interaction*, vol. 4, pp. 88–102, 2022.
[29] N. Patwari and J. Wilson, "RF sensor networks for device-free localization: Measurements, models, and algorithms," *Proc. IEEE*, vol. 98, no. 11, pp. 1961–1973, Nov. 2010.
[30] S. Palipana, P. Agrawal, and D. Pesch, "Channel state information based human presence detection using non-linear techniques," in *Proc. 3rd ACM Int. Conf. Syst. Energy-Efficient Built Environ.*, 2016, pp. 177–186.
[31] HUAWEI, "Wi-Fi signal," 2021. [Online]. Available: https://info.support.huawei.com/network/ptmngsys/Web/ONT_Basics/zh/htmlfiles/wifi_signal.html
[32] J. link and M. schulz, "Nexmon_csi," 2020. [Online]. Available: https://github.com/seemoo-lab/nexmon_csi
[33] D. Coleman, *Wi-Fi 6 & 6E for Dummies*. Hoboken, NJ, USA: Wiley, 2022.
[34] M. J. Shensa, "The discrete wavelet transform: Wedding the a trous and mallat algorithms," *IEEE Trans. Signal Process.*, vol. 40, no. 10, pp. 2464–2482, Oct. 1992.
[35] H. Abdi, "The eigen-decomposition: Eigenvalues and eigenvectors," in *Encyclopedia of Measurement and Statistics*, Thousand Oaks, CA, USA: SAGE, 2007.
[36] S. Roy, "ROC space," 2018. [Online]. Available: https://scottroy.github.io/ROC-space-and-AUC.html
[37] Y. Qiao, O. Zhang, W. Zhou, K. Srinivasan, and A. Arora, "PhyCloak: Obfuscating sensing from communication signals," in *Proc. 13th USENIX Symp. Netw. Syst. Des. Implementation*, 2016, pp. 685–699.
[38] H. Chen, K. Lee, J. Lin, and M. Koch, "Comparison of electromagnetic shielding effectiveness properties of diverse conductive textiles via various measurement techniques," *J. Mater. Process. Technol.*, vol. 192/193, pp. 549–554, 2007.
[39] J. Huang et al., "Towards anti-interference human activity recognition based on WiFi subcarrier correlation selection," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6739–6754, Jun. 2020.
[40] S. D. Domenico, M. D. Sanctis, E. Cianca, and G. Bianchi, "A trained-once crowd counting method using differential WiFi channel state information," in *Proc. 3rd Int. Workshop Phys. Analytics*, 2016, pp. 37–42.
[41] W. Xi et al., "Electronic frog eye: Counting crowd using WiFi," in *Proc. IEEE Conf. Comput. Commun.*, 2014, pp. 361–369.
[42] C. Wu, F. Zhang, B. Wang, and K. Liu, "mmTrack: Passive multi-person localization using commodity millimeter wave radio," in *Proc. IEEE 39th Conf. Comput. Commun.*, 2020, pp. 2400–2409.
[43] D. Zhang, Y. Hu, Y. Chen, and B. Zeng, "BreathTrack: Tracking indoor human breath status via commodity WiFi," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3899–3911, Apr. 2019.
[44] H. Zhu, Y. Zhuo, Q. Liu, and S. Chang, "-splicer: Perceiving accurate CSI phases with commodity WiFi devices," *IEEE Trans. Mobile Comput.*, vol. 17, no. 9, pp. 2155–2165, Sep. 2018.
[45] N. Damodaran, E. Haruni, M. Kokhkharova, and J. Schäfer, "Device free human activity and fall recognition using WiFi channel state information (CSI)," *CCF Trans. Pervasive Comput. Interaction*, vol. 2, pp. 1–17, 2020.
[46] W. Jiang et al., "Towards environment independent device free human activity recognition," in *Proc. 24th Annu. Int. Conf. Mobile Comput. Netw.*, 2018, pp. 289–304.
[47] Z. Hao, Y. Duan, X. Dang, and T. Zhang, "CSI-HC: A WiFi-based indoor complex human motion recognition method," *Mobile Inf. Syst.*, vol. 2020, pp. 1–20, 2020.
[48] 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," *IEEE Trans. Mobile Comput.*, vol. 16, no. 2, pp. 511–526, Feb. 2017.
[49] Y. Wang, J. Liu, Y. Chen, M. Gruteser, J. Yang, and H. Liu, "E-eyes: Device-free location-oriented activity identification using fine-grained WiFi signatures," in *Proc. 20th Annu. Int. Conf. Mobile Comput. Netw.*, 2014, pp. 617–628.
[50] Y. Gu, J. Zhan, Y. Ji, J. Li, F. Ren, and S. Gao, "MoSense: An RF-based motion detection system via off-the-shelf WiFi devices," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2326–2341, Dec. 2017.
[51] Y. Wang, X. Jiang, R. Cao, and X. Wang, "Robust indoor human activity recognition using wireless signals," *Sensors*, vol. 15, pp. 17195–17208, 2015.
[52] F. Hong, X. Wang, Y. Yang, Y. Zong, Y. Zhang, and Z. Guo, "WFID: Passive device-free human identification using WiFi signal," in *Proc. 13th Int. Conf. Mobile Ubiquitous Syst.: Comput. Netw. Serv.*, 2016, pp. 47–56.
[53] T. Xin, B. Guo, Z. Wang, M. Li, Z. Yu, and X. Zhou, "FreeSense: Indoor human identification with Wi-Fi signals," in *Proc. IEEE Glob. Commun. Conf.*, 2016, pp. 1–7.
[54] J. Zhang et al., "Gate-ID: WiFi-based human identification irrespective of walking directions in smart home," *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7610–7624, May 2021.
[55] J. Zhang, B. Wei, W. Hu, and S. S. Kanhere, "WiFi-ID: Human identification using WiFi signal," in *Proc. Int. Conf. Distrib. Comput. Sensor Syst.*, 2016, pp. 75–82.
[56] Y. Gu et al., "Secure user authentication leveraging keystroke dynamics via Wi-Fi sensing," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2784–2795, Apr. 2022.
[57] Z. Zhou, Z. Yang, C. Wu, L. Shangguan, and Y. Liu, "Omnidirectional coverage for device-free passive human detection," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1819–1829, Jul. 2014.
[58] J. Xiao, K. Wu, Y. Yi, L. Wang, and L. M. Ni, "FIMD: Fine-grained device-free motion detection," in *Proc. IEEE 18th Int. Conf. Parallel Distrib. Syst.*, 2012, pp. 229–235.
[59] A. Banerjee, D. Maas, M. Bocca, N. Patwari, and S. Kasera, "Violating privacy through walls by passive monitoring of radio windows," in *Proc. 7th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2014, pp. 69–80.
[60] R. Zhou, X. Lu, P. Zhao, and J. Chen, "Device-free presence detection and localization with SVM and CSI fingerprinting," *IEEE Sensors J.*, vol. 17, no. 23, pp. 7990–7999, Dec. 2017.
[61] F. Adib, C. Hsu, H. Mao, D. Katabi, and F. Durand, "Capturing the human figure through a wall," *ACM Trans. Graph.*, vol. 34, 2015, Art. no. 219.
[62] M. Zhao et al., "Through-wall human pose estimation using radio signals," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2018, pp. 7356–7365.
[63] C. Uysal and T. Filik, "A new RF sensing framework for human detection through the wall," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 3600–3610, Mar. 2023.

Yangyang Gu received the BE degree in Internet of Things engineering from Wuhan University, Hebei, China, in 2019. He is currently working toward the PhD degree with the School of Cyber Science and Engineering, Wuhan University, Hubei, China. His research interests include human privacy and wireless sensing.

Jing Chen (Senior Member, IEEE) received the PhD degree in computer science from the Huazhong University of Science and Technology, Wuhan. He is currently a full professor with the School of Cyber Science and Engineering, Wuhan University. He is served as the vice chair of the ACM Turing Award Celebration Conference (TURC) 2023. He has published more than 150 research papers in many international journals and conferences, including USENIX Security, ACM CCS, INFOCOM, *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Information Forensics and Security*, *IEEE Transactions on Mobile Computing*, *IEEE Transactions on Computers*, *IEEE Transactions on Parallel and Distributed Systems*, *IEEE Transactions on Services Computing*, etc. He was twice runner-up for the best paper with INFOCOM 2018 and INFOCOM 2021. His research interests include the areas of network security, cloud security, and mobile security.

Kun He received the PhD degree in computer science from Wuhan University. He is currently an associate professor with Wuhan University. He has published research papers in USENIX Security, CCS, INFOCOM, *IEEE Transactions on Information Forensics and Security*, *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Mobile Computing*, etc. His research interests include cryptography, network security, mobile computing, and cloud computing.

Cong Wu received the PhD degree from the School of Cyber Science and Engineering, Wuhan University, in 2022. He is currently a research fellow with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests include AI system security and Web3 security. His research outcomes have appeared in USENIX Security, ACM CCS, *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Information Forensics and Security*.

Ziming Zhao (Member, IEEE) received the PhD degree in computer science from Arizona State University, Tempe, Arizona, in 2014. He is an assistant professor with the Department of Computer Science and Engineering (CSE) and the director of the CyberspACe securiTy and forensIcs lab (CactiLab), University at Buffalo. His current research interests include systems and software security, trusted execution environment, formal methods for security, and usable security. His research has been supported by the U.S. National Science Foundation (NSF), the U.S. Department of Defense, the U.S. Air Force Office of Scientific Research, and the U.S. National Centers of Academic Excellence in Cybersecurity. He is a recipient of an NSF CAREER award and an NSF CRII award. His research outcomes have appeared in IEEE S&P, USENIX Security, ACM CCS, NDSS, ACM MobiSys, ACM/IEEE DAC, ACM TISSEC/TOPS, *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Information Forensics and Security*, etc. He is also a recipient of best paper awards from USENIX Security 2019, ACM AsiaCCS 2022, ACM CODASPY 2014, and ITU Kaleidoscope 2016.

Ruiying Du received the BS, MS, and PhD degrees in computer science from Wuhan University, Wuhan, China, in 1987, 1994, and 2008, respectively. She is currently a professor with the School of Cyber Science and Engineering, Wuhan University. Her research interests include network security, wireless network, and mobile computing. She has published more than 80 research papers in many international journals and conferences, such as the *IEEE Transactions on Parallel and Distributed Systems*, INFOCOM, SECON, TrustCom, and NSS.