Revisiting Wireless Breath and Crowd Inference Attacks With Defensive Deception

Qiuye He, Edwin Yang, Song Fang, and Shangqing Zhao, *Member, IEEE*

***Abstract*— Breathing rates and crowd counting can be used to verify the human presence, especially the former one can disclose a person's physiological status. Many studies have demonstrated success in applying channel state information (CSI) to estimate the breathing rates of stationary individuals and count the number of people in motion. Due to the invisibility of radio signals, the ubiquitous deployment of wireless infrastructures, and the elimination of the line-of-sight (LOS) requirement, such wireless inference techniques can surreptitiously work and violate user privacy. However, little research has been conducted specifically in mitigating misuse of those techniques. This paper proposes new proactive countermeasures against all existing CSI-based vital signs and crowd counting inference methods. Specifically, we set up ambush locations with carefully designed wireless signals, allowing eavesdroppers to infer a false breathing rate or person count specified by the transmitter. The true breathing rate or person count is thus protected. Experimental results on software-defined radio platforms with 5 participants demonstrate the effectiveness of the proposed defenses. An eavesdropper can be misled into believing any desired breathing rate with an error of less than 1.2 bpm when the user lies on a bed in a bedroom, and 0.9 bpm when the user sits in a chair in an office room. Additionally, our proposed defense mechanisms can deceive an attacker into believing there are moving individuals in an empty room with a 100% success rate, using both Support Vector Machine (SVM) and Decision Tree (DT) classifiers.**

***Index Terms*— Breathing rate inference, crowd counting, deceptive communication, channel state information.**

I. Introduction

VITAL signs and crowd counting inference via wireless signals has drawn increasing attention due to the widespread availability of wireless infrastructures and the lack of need for direct contact with devices [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17]. With such a technique, an eavesdropper can stealthily set up a wireless receiver on one side of the user to passively collect the signals emitted by a wireless Access Point (AP) which is on the other side of the user. The fluctuations in the received signals caused by respiration-induced chest and stomach movements can reveal sensitive vital signs, which can be analyzed by the eavesdropper for vital signs inference. Similarly, the presence of multiple moving people leads to a larger variation in the received signals over time, which can be used to estimate the number of people in a room for crowd counting.

The popularity of such techniques also brings privacy concerns. In detail, attackers can extract personal information such as vital signs, the number of individuals present, and even their locations, which can be exploited for malicious purposes like stalking or theft. For example, vital signs often contain sensitive information related to the state of personal essential body function [12], [13], [18], [19], [20]. Generally, the normal breathing rate for an adult at rest is 12 to 20 breaths per minute (bpm). Abnormal breathing may be a symptom of diseases, such as pulmonary diseases [21], heart problems or drug overdose [22], and cardiovascular diseases like stroke [19]. The disclosure of such health information can cause serious consequences such as employment discrimination based on health status [23], and a company's stock plummeting due to its CEO's health concerns [24], [25]. Furthermore, an eavesdropper can track occupancy in a home by detecting breathing [26], [27], [28], [29] or estimating person count [2], [5], [6], [7], and then break in once the target homes are vacant to reduce the chance of getting caught [30].

Though research is booming in vital signs and crowd counting inference through wireless signals, there are few research efforts discussing corresponding countermeasures. Traditional anti-eavesdropping methods usually take the following two defenses: (1) *Cryptographic key based:* by encrypting transmitted messages between legitimate parties [31], an eavesdropper without the secret key cannot successfully decode the received message; and (2) *Friendly jamming based:* an ally jammer actively sends jamming signals (e.g., [32], [33]) which interrupt the eavesdropping while the receiver can decode messages by canceling the impact of the inference signals. With either mechanism, the eavesdropper would capture encrypted or disrupted signals, which are often random and meaningless. Though the eavesdropper may not get the correct wireless signals, the unintelligibility of those signals indicates to her that her eavesdropping fails. She may thus make further efforts to break the wireless communication. For example, an eavesdropper may attempt to

Manuscript received 20 November 2023; revised 1 June 2024; accepted 5 August 2024; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor C. Peng. This work was supported in part by the National Science Foundation under Grant 2155181. An earlier version of the work was published in EAI MobiQuitous 2022 [DOI: 10.1007/978-3-031-34776-4_12]. *(Corresponding author: Song Fang.)*

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by the OU Norman Campus Institutional Review Board (IRB) Office.

Qiuye He is with the School of Science and Engineering, University of Missouri-Kansas City, Kansas City, MO 64110 USA (e-mail: qiuye.he@umkc.edu).

Edwin Yang, Song Fang, and Shangqing Zhao are with the School of Computer Science, University of Oklahoma, Norman, OK 73019 USA (e-mail: edwiny@ou.edu; songf@ou.edu; shangqing@ou.edu).

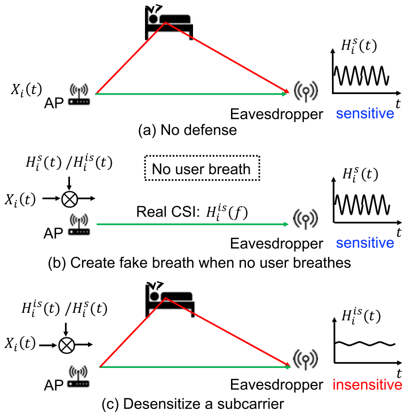
Digital Object Identifier 10.1109/TNET.2024.3453903

steal the secret key via social engineering methods (e.g., [34]) or side-channel attacks (e.g., [35]). Also, it has been shown that an attacker equipped with multiple antennas is able to separate the message from the jamming signals [36]. Other existing WiFi-based defense techniques successfully defend against corresponding attacks in practical applications, including smart home IoT [37], user location [38], and gesture recognition [39]. For example, the study [37] can detect whether the received signal is an emulated signal from a WiFi attacker or a legitimate one from a ZigBee transmitter. Another work [38] creates a mirage that obscures the direct path's Time of Flight (ToF) information to spoof the Angle of Arrival (AoA), thereby further protecting user location. Additionally, a study [39] discusses two defense methodologies, including blocking (e.g., geofencing, reducing transmitting power) and detecting, to defend against adversarial attacks in a DNN-powered WiFi-based gesture recognition system. However, blocking [39] can effectively bound the WiFi signal, preventing an attacker from receiving it, but it also affects legitimate receivers and alerts the attacker that her attack was unsuccessful. Detecting [37], [39] can identify the attackers but may also result in privacy leakage. The approach [38] provides a new direction by making an attacker obtain fake but meaningful information, but it only applies to systems utilizing AoA information. Due to the importance of personal privacy, more effective defenses are thus much-needed to prevent wireless vital signs and person count eavesdropping.

Orthogonal frequency-division multiplexing (OFDM) is widely used in modern wireless communication systems (e.g., 802.11a/g/n/ac/ad) with multiple subcarrier frequencies to encode a packet. The minute wireless signal disturbance caused by human motion can be captured by *received signal strength* (RSS) or *channel state information* (CSI). RSS only provides the average power in a received radio signal over the whole channel bandwidth, while CSI represents how the wireless channel impacts the radio signal that propagates through it (e.g., amplitude attenuation and phase shift). CSI offers fine-grained channel information, consisting of subcarrier-level information. As a result, CSI is more sensitive to human activity and has shown the best performance in inferring human activity compared with other wireless techniques [10].

What if we actively feed the eavesdropper with a meaningful but bogus breathing rate or person count? When the eavesdropper is misled by the fake ones, she would not take further methods to compromise the true one. In this paper, we thus develop novel schemes against CSI-based vital signs and crowd counting inference techniques. Specifically, we set up an *ambush location*, choose a fake breathing rate or person count, and convert it into a fake CSI. The transmitter then delivers the specified CSI to the ambush location by manipulating the transmitted wireless signals. As a result, the eavesdropper at the ambush location would infer the fake breathing rate or person count with the estimated CSI.

We first take the breathing rate inference system as an example, where the user remains static. We observe that various subcarriers exhibit varying degrees of variance in CSI amplitudes. This variance is attributed to the effects of the Fresnel Zone [16], [40], [41], a region of space between the transmitter and receiver where the radio waves propagate. Generally, as the reflected and LOS signals interfere constructively or destructively, a receiver may observe enhanced or weakened signals. Such effects may vary for different subcarriers, which can be categorized into two groups: sensitive and insensitive. With respiration-induced body movements, sensitive subcarriers enable the receiver to observe large amplitudes (or variances) of CSI measurements, while insensitive subcarriers rarely show correlated fluctuations. Thus, the breathing rate can be determined via observations of sensitive subcarriers.



(a) No defense

(b) Create fake breath when no user breathes

(c) Desensitize a subcarrier

Fig. 1. Creating a fake (sensitive or insensitive) CSI.

We give an example to illustrate our idea. Without loss of generality, we utilize a single subcarrier for discussion. For OFDM systems, a transmitter sends a publicly known pseudo-noise sequence $X_i(t)$, and the receiver estimates the channel frequency response $H_i(t)$ (i.e., CSI) from the received signal $Y_i(t)$, i.e., $H_i(t) = \frac{Y_i(t)}{X_i(t)}$ [42], [43]. If no defense strategy is enforced, as shown in Figure 1a, the eavesdropper (malicious receiver) can obtain the real CSI for the sensitive i^{th} subcarrier between itself and the AP, denoted with $H_i^s(t)$, which enables her to derive the breathing rate of the target user.

If there is no breathing activity, as shown in Figure 1b, the i^{th} subcarrier should be insensitive and the true CSI is denoted with $H_i^{is}(t)$. However, the AP multiples the signal $X_i(t)$ with a coefficient $H_i^s(t)/H_i^{is}(t)$, and sends the resultant signal, which also goes through the real wireless channel. Consequently, the received signal becomes $X_i(t) \cdot H_i^s(t)/H_i^{is}(t) \cdot H_i^{is}(t) = X_i(t)H_i^s(t)$, and thus the eavesdropper obtains an estimated subcarrier CSI $H_i^s(t)$ (sensitive), with which the breathing rate specified by the transmitter can be extracted.

Now consider the scenario in Figure 1c: the transmitter aims to hide the user's true breathing rate. Therefore, it multiples the signal $X_i(t)$ with a coefficient $H_i^{is}(t)/H_i^s(t)$. As a result, the eavesdropper obtains $X_i(t) \cdot H_i^{is}(t)/H_i^s(t) \cdot H_i^s(t) = X_i(t)H_i^{is}(t)$. The calculated subcarrier CSI then becomes $H_i^{is}(t)$, which means that such subcarrier is insensitive, causing failure of inferring the true breathing rate.

Unlike the breathing rate inference system where the user is static, people move randomly in the crowd counting system. Based on the observation that all subcarriers exhibit the similar fluctuations due to the continuous movement and changing positions of people, all subcarriers can be considered sensitive.

Therefore, by manipulating the CSIs across all subcarriers, the proposed defense scheme can enable an eavesdropper to estimate incorrect crowd count in an empty room. The specified CSI is extracted from a pre-built profile, consisting of collected CSI data for different numbers of moving individuals.

Our real-world experimental results show the proposed defenses can fool an eavesdropper into believing any desired breathing rate with an error of less than 1.2 bpm when the user lies on a bed in a bedroom and 0.9 bpm when the user sits in a chair in an office room. Furthermore, our proposed defense mechanisms can deceive an attacker into believing that there are moving individuals in an empty room with a probability of 100% and 100% for Support Vector Machine (SVM) and Decision Tree (DT) classifiers, respectively. We summarize our main contributions as follows:

- To the best of our knowledge, we are the first to propose deceptive approaches to defend against wireless vital signs and crowd counting inference attacks.
- By reverse engineering existing CSI-based breathing rate and crowd counting inference techniques, we design a customized scheme to convert a chosen breathing rate or crowd count into a fake CSI. We also develop methods to enable the eavesdropper to estimate the fake CSI and thus obtain the specified breathing rate or person count.
- We implement real-world prototypes of both existing CSI-based breathing rate and crowd counting inference and the proposed defense schemes. We experiment on top of them to examine the impact of the defenses.

The rest of the paper is organized as follows: Section II summarizes related work on wireless breathing rate inference techniques and wireless crowd counting techniques. Section III introduces the preliminaries of CSI-based breathing rate inference and CSI-based crowd counting inference, and also presents the attack model and assumptions. Defenses against breathing inference and crowd inference attacks are discussed in Sections IV and V, respectively. Section VI provides the corresponding experimental evaluation and analysis. Finally, the conclusions are presented in Section VII.

II. Related Work

A. Wireless Breathing Rate Inference Techniques

Generally, existing wireless breathing rate inference techniques fall into the following categories:

Ultra-wideband (UWB) radar based: The expansion and contraction of the chest cavity may create changes in the multipath profile of the transmitting signal, which can be captured with UWB impulse responses for breathing rate estimation [10], [44], [45]. UWB transmissions, however, spread over a large frequency bandwidth [46]. Also, the receiver structure for UWB is highly complex [47].

Doppler radar based: Doppler radar systems have been proposed to achieve breathing detection [48], [49], [50], [51]. According to the Doppler theory, a target with time-varying movement but zero net velocity will reflect the signal, whose phase is modulated in proportion to the displacement of the target [52]. A stationary person's chest and stomach can be thus regarded as a target. However, such Doppler radar based techniques suffer from the null point problem, which significantly degrades the measurement accuracy [50], [53].

Frequency Modulated Continuous Wave (FMCW) radar based: An FMCW radar has also been utilized for breathing rate inference [8], [54]. The breathing-induced body movement changes the signal reflection time. By analyzing such changes, the breathing rate can be extracted. However, high resolution (i.e., the minimum measurable change) requires a large swept bandwidth B as the resolution equals $\frac{C}{2B}$ [55], where C is the speed of light.

RSS-based: The changes in received signal strength (RSS) on wireless links have been successful in estimating breathing rate [14], [18], [56], [57]. For example, [18] puts a mobile device on the chest to collect RSS for inferring breathing rates. However, those methods are workable only when the target user stays close to the receiver. As an eavesdropper usually has a preference to be located far away to avoid being discovered, such RSS-based methods are not optimal.

CSI-based: RSS represents coarse channel information while CSI represents fine-grained one, consisting of subcarrier-level information. As a result, CSI is more sensitive to detecting breathing activity and the CSI-based approaches are able to capture breathing from a distance. Accordingly, CSI-based breathing rate inference has drawn increasing attention [12], [13], [16], [58], [59], [60], [61], [62], [63], [64]. In particular, a recent empirical study [10] reveals CSI provides the most robust estimates of respiration compared with UWB radar or RSS.

B. Wireless Crowd Counting Techniques

Existing studies on crowd counting can be broadly categorized into the following groups:

RSS-based: It observed that the RSS value will be stable if there is no person present between a pair of transmitter and receiver. However, the RSS value exhibits a larger variance when a person crosses the wireless link, with this variance increasing as the number of people increases [1], [2], [3], [65]. However, these approaches require extensive deployment of sensor nodes and the construction of a fingerprint database, resulting in significantly high costs and substantial training efforts.

CSI-based: CSI-based approaches are motivated by the observation that CSI is highly sensitive to environmental variations. Therefore, a larger number of moving people will result in a greater CSI variance in the target area [4], [5], [6], [7], [66], [67]. For example, FCC [4] theoretically found a stable monotonic function to characterize the relationship between the number of moving people and the variation in the wireless channel.

III. Preliminaries and Attack Model

A. Preliminaries

1) CSI-Based Breathing Rate Inference: Existing CSI-based breathing rate inference schemes [10], [13], [16] usually utilize three steps to infer breathing rates, namely, CSI pre-processing, subcarrier selection, and breathing cycle extraction. The first phase removes outliers and noise from the CSI to improve its reliability. As discussed earlier, each subcarrier may be sensitive or insensitive to respiration due to the constructive or destructive interference effect of LOS and reflected signals. The second phase picks up sensitive subcarriers for breathing rate inference. A sensitive subcarrier often exhibits a sinusoidal-like periodic change pattern over time in the CSI amplitudes, which corresponds to periodic breathing. In the third phase, the peak-to-peak time interval of sinusoidal CSI amplitudes can be extracted as the breathing cycle, with which, the breathing rate can be calculated.

2) CSI-Based Crowd Counting Inference: Existing studies on CSI-based crowd counting approaches [4], [5], [68], [69], [70] utilize existing WiFi infrastructure for crowd classification in indoor scenarios. The key idea is that an increase in the number of moving people introduces larger multipath variations, resulting in greater CSI variation over time. In this way, based on the measurement of how CSI varies over time, the number of moving people can be estimated. In general, there are three key phases: CSI pre-processing, feature extraction, and crowd classification. To obtain the CSI measurements caused by moving people, CSI pre-processing phase removes redundant components, such as noise, from the CSI data. Based on such processed data, distinct features (e.g., mean, standard deviation, maximum, and minimum of CSI amplitude) are extracted and then fed into a classifier (e.g., SVM, DT) to output the estimated number of moving people.

B. Attack Model and Assumptions

We consider a general scenario, where an attacker only uses a wireless receiver to launch a breathing rate or crowd counting inference attack, as she has a preference to use an existing wireless transmitter to make the attack stealthier [4], [13]. The transmitter (i.e., defender) is benign and aims to hide true breathing rates or person count and inject fake ones.

We assume that the receiver (i.e., attacker) attempts to find a position that enables her to eavesdrop on the breathing rate or person count, which is a common strategy [71]. We borrow the idea from a long-established military tactic – ambush: set up one or multiple ambush locations where an attacker may appear and be trapped. We further assume that the transmitter is able to obtain actual CSI measurements between itself and an ambush location. This can be achieved by estimating the CSI measurements from wireless signals emitted by a helper node, which is placed at the ambush location in advance and does not collaborate with the eavesdropper.

IV. Breath Inference Attacks and Defenses

In this section, to defend against CSI-based breathing rate inference attack, we propose the corresponding defenses called *HoneyBreath* in the following.

A. Overview

To lay an ambush, the transmitter first selects an ambush location. The locations where an eavesdropper may appear with the highest probabilities can be determined via eavesdropper tracking techniques (e.g., [72]) and ambush locations can be then deployed along the eavesdropper's possible route.

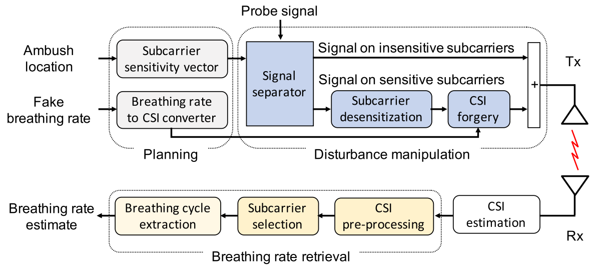


Fig. 2. Flow chart of the proposed *HoneyBreath* defense.

The transmitter then enters the *planning* phase, which consists of two parallel tasks: (1) determining sensitive subcarriers; and (2) converting a specified breathing rate into an artificial CSI. We utilize a binary decision variable α_i to indicate the sensitivity of the i^{th} subcarrier, with 1 denoting sensitive while 0 showing insensitive. The sensitivities of all N subcarriers can be represented by a vector $\boldsymbol{\alpha} = [\alpha_1, \alpha_2, \cdots, \alpha_N]^T$. Since insensitive subcarriers do not contribute to the breathing rate inference, there is no need to manipulate their CSIs.

The next phase is *disturbance manipulation*. For signals on sensitive subcarriers, the transmitter aims to make the attacker estimate the converted CSI. As any transmitting signal has to go through the real wireless channel, the transmitter then desensitizes subcarriers to remove the real impact of corresponding wireless sub-channels, and also crafts the artificial disturbance on these originally sensitive subcarriers. Finally, the transmitter combines the crafted signals on sensitive subcarriers with unchanged signals on insensitive subcarriers and transmits the aggregated signal out.

Consequently, the attacker is able to infer breathing rate based on estimated CSI by performing the general *breathing rate retrieval* process. Figure 2 shows the flow chart of the proposed ambush tactic *HoneyBreath*.

B. Planning Phase

1) Obtaining Subcarrier Sensitivity: Let $\mathrm{T_x}$, U, and $\mathrm{A_x}$ denote the transmitter, the user, and an ambush location, respectively. A wireless signal sent by $\mathrm{T_x}$ travels on two paths, the LOS path and the reflection one. The distance difference Δd between the two paths is $\Delta d = d_{TU} + d_{UA} - d_{TA}$.

Let λ_i denote the wavelength of the i^{th} subcarrier with frequency f_i, i.e., $\lambda_i = c/f_i$, where c is the speed of light. Correspondingly, the phase difference $\Delta\theta_i$ (between signals arrived at $\mathrm{A_x}$ through the two paths) equals the sum of the respective phase shifts caused by Δd and the reflection phenomenon, i.e., $\Delta\theta_i = \frac{2\pi\Delta d}{\lambda_i} + \pi$. We perform a modulus 2π operation on $\Delta\theta_i$ and obtain a phase difference $\Delta\theta'_i$ within the range of [0, 2π), i.e., $\Delta\theta'_i = \Delta\theta_i \pmod{2\pi}$.

Based on the Fresnel Zone theory [16], [40], [41], if $\Delta\theta'_i$ is close to 0 or 2π, the i^{th} subcarrier is sensitive, i.e., when $\Delta\theta'_i \in [0, \pi/2) \cup (3\pi/2, 2\pi)$, we obtain the binary decision variable $\alpha_i = 1$. On the other hand, if $\Delta\theta'_i$ approaches to π, this subcarrier becomes insensitive, i.e., $\alpha_i = 0$ for $\Delta\theta'_i \in [\pi/2, 3\pi/2]$. The relationship between α_i and $\Delta\theta'_i$ can be then denoted as $\alpha_i = \lfloor \frac{|\Delta\theta'_i - \pi|}{\pi/2} \rfloor$, where $\lfloor x \rfloor$ denotes

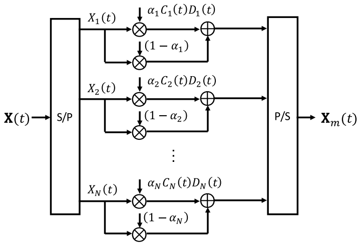


Fig. 3. An MAC process.

the floor function, representing the largest integer less than or equal to x.

2) Converting Breathing Rate to CSI: Breathing rate to CSI conversion is the process of translating a selected breathing rate into a subcarrier CSI. It has been observed that periodic chest and stomach movement caused by respiration would make the amplitude of CSI on a sensitive subcarrier present a sinusoidal-like pattern over time [12], [13], [16]. We thus model the respiration-induced CSI amplitude stream on a sensitive subcarrier as a sinusoidal wave.

Let f_b denote the specified respiration frequency (Hz), so the corresponding breathing rate equals $60 \cdot f_b$ (bpm). We then convert it into a subcarrier CSI $W_b(t)$, which can be then denoted with $|W_b(t)|e^{j\varphi(t)}$, where $|W_b(t)|$ and $\varphi(t)$ represent amplitude and phase, respectively. Since the phase could be distorted due to an unknown time lag caused by the non-synchronized transmitter and receiver [73], most studies only use the amplitude to characterize the wireless channel [74] and extract breathing rate [12], [13], [16]. We also explore CSI amplitude and refer to it as just “CSI” in the following. In terms of $\varphi(t)$, it has no impact on breathing rate inference and we omit it for the sake of simplicity. With the sinusoidal model, the CSI envelope at time t can be denoted by

$$|W_b(t)| = a \cdot sin(2\pi f_b t + \beta) + m + \mathcal{N}_0, \tag{1}$$

where a, β, m and $\mathcal{N}_0$ are the amplitude, initial phase, constant shift of the sinusoidal wave, and the additive noise.

Formation of the Specified OFDM CSI: The specified CSI for an OFDM system with N subcarriers can be denoted with $\mathbf{W}(t) = [W_1(t), W_2(t), \cdots, W_N(t)]$. Let $\mathcal{S} = \{s_1, s_2, \ldots, s_K\}$ and $\bar{\mathcal{S}} = \{p_1, p_2, \ldots, p_{K'}\}$ denote the sets formed by the indexes of the sensitive and insensitive subcarriers, where $K+K'=N$. For $i \in \mathcal{S}$, we enable $W_i(t) = W_b(t)$; for $i \in \bar{\mathcal{S}}$, we have $W_i(t) = H_i(t)$ (i.e., no manipulation is required), where $H_i(t)$ is the original CSI of the i^{th} subcarrier.

C. Disturbance Manipulation

The transmitter can utilize a multiply-accumulate (MAC) process to generate desired artificial disturbance, as shown in Figure 3. Specifically, the public training sequence $\mathbf{X}(t)$ is encoded into N subcarrier signals by a serial-to-parallel (S/P) converter module, represented with $[X_1(t), X_2(t), \cdots, X_N(t)]^T$. We use $\mathbf{J}$ to represent an $N \times 1$ vector of all 1's. Thus, after the signal separator, the original N subcarrier signals will be divided into two groups: $\mathbf{S}(t) = \text{diag}(\boldsymbol{\alpha}) \cdot \mathbf{X}(t)$ and $\mathbf{IS}(t) = \text{diag}(\mathbf{J} - \boldsymbol{\alpha}) \cdot \mathbf{X}(t)$, denoting signals on sensitive and insensitive subcarriers, respectively, where $\text{diag}(\mathbf{V})$ denotes a square diagonal matrix with the elements of vector $\mathbf{V}$ on the main diagonal.

Signals on sensitive subcarriers would then go through two modules: *subcarrier desensitization* and *CSI forgery*. The former module with the coefficient vector $\mathbf{C}(t) = [C_1(t), C_2(t), \cdots, C_N(t)]$ aims to cancel the original channel impact. Accordingly, we have $C_i(t) = H_i^{-1}(t)$ if the i^{th} subcarrier is sensitive, i.e., $i \in \mathcal{S}$, and set $C_i(t) = 0$ for $i \in \bar{\mathcal{S}}$. The latter module with a coefficient vector $\mathbf{D}(t) = [D_1(t), D_2(t), \cdots, D_N(t)]$ would add the effect of the artificial CSI where the forged subcarrier CSI $D_i(t) = W_i(t)$ if $i \in \mathcal{S}$ and we set $D_i(t) = 0$ for $i \in \bar{\mathcal{S}}$.

Finally, signals on originally sensitive and insensitive subcarriers are concatenated through a parallel-to-serial (P/S) converter module to form OFDM symbols to send via the realistic wireless channel. The resulting transmitting signal $\mathbf{X}_m(t)$ can be represented by

$$\mathbf{X}_m(t) = \text{diag}(\mathbf{D}(t)) \cdot \text{diag}(\mathbf{C}(t)) \cdot \mathbf{S}(t) + \mathbf{IS}(t). \tag{2}$$

Let $\mathbf{H}(t) = [H_1(t), \cdots, H_N(t)]^T$ denote the true OFDM CSI. The received signal at the attacker thus becomes $\mathbf{R}_m(t) = \text{diag}(\mathbf{X}_m(t)) \cdot \mathbf{H}(t)$, where we omit the noise term for the sake of simplicity. The attacker estimates CSI with the received signal and the public training sequence, i.e., $\mathbf{R}_m(t) = \text{diag}(\mathbf{X}(t)) \cdot \hat{\mathbf{H}}(t)$, where $\hat{\mathbf{H}}(t) = [\hat{H}_1(t), \cdots, \hat{H}_N(t)]^T$ represents the estimated CSI. Consequently, we have

$$\begin{aligned} \hat{H}_i(t) &= \alpha_i \cdot \frac{X_i(t) C_i(t) D_i(t)}{X_i(t)} \cdot H_i(t) + (1-\alpha_i) \cdot H_i(t) \\ &= \alpha_i \cdot D_i(t) + (1-\alpha_i) \cdot H_i(t) = W_i(t). \end{aligned} \tag{3}$$

This demonstrates that with the disturbance manipulation, when the i^{th} subcarrier is sensitive, the transmitter is able to make the attacker obtain a fake subcarrier CSI $W_i(t)$ specified by itself. Meanwhile, if the i^{th} subcarrier is insensitive, it is still observed as insensitive, i.e., the corresponding estimated subcarrier CSI equals the real value $H_i(t)$.

D. Breathing Rate Retrieval

1) CSI Pre-Processing: CSI pre-processing, consisting of outlier removal and noise reduction, aims to make the collected CSI reliable. As the collected CSI may have abrupt changes that are not caused by respiration, a Hampel filter is enforced to remove those outliers [12], [75]. We further adopt the moving average filter, which is optimal for reducing high-frequency noise while retaining a sharp step response [76].

2) Subcarrier Selection: Empirically, the CSI variance of a sensitive subcarrier is usually more than one order of magnitude larger than that of an insensitive subcarrier. This observation implies a threshold-based approach to distinguish the two types of subcarriers. Specifically, when there is no breathing activity, the average CSI variance σ^2 across all subcarriers can be measured, called *reference variance*, which will be then utilized as the threshold. Let v_i^2 denote the CSI variance for the i^{th} subcarrier. If $\log_{10}(v_i^2/\sigma^2) < 1$ holds, we regard that the subcarrier is insensitive; otherwise, this subcarrier is sensitive. If the CSI variances on all subcarriers are of the same order as the reference variance, then all subcarriers can be considered insensitive.

3) Breathing Cycle Identification: The CSI on a sensitive subcarrier often shows a sinusoidal pattern correlated with breathing activities. To obtain a breathing cycle, we can thus compute the inter-peak interval of the sinusoidal CSI.

Intuitively, the first derivative of a peak switches from positive to negative at the peak maximum, which can be used to localize the occurrence time of each peak. However, there may exist fake peaks caused by noise and consequently false zero-crossings. Motivated by the fact that a person usually cannot breathe beyond a certain frequency, a fake peak removal algorithm can be developed. Specifically, if the calculated interval is less than $60/R_{max}$ (seconds), where R_{max} (bpm) denotes the maximum possible breathing rate, this peak will be labeled as a fake one and then removed.

E. From Point Ambush to Area Ambush

With more deployed ambush locations, the probability that an eavesdropper happens to be at any of them would be higher. Meanwhile, it helps to defend against multiple collaborative attackers, each searches for opportune eavesdropping locations.

The transmitter is able to deploy κ ambush locations with κ antennas. We consider colluding eavesdroppers and need to guarantee the breathing rate inferred by each eavesdropper at any ambush location stays the same. Meanwhile, let α_r^i denote the overall sensitivity of the i^{th} subcarrier between the transmitter and the r^{th} ambush location, i.e., $\alpha_r^i = \alpha_{1r}^i \vee \alpha_{2r}^i \cdots \vee \alpha_{\kappa r}^i$. Thus, in terms of the subcarrier sensitivity vector $\boldsymbol{\alpha}$ of the transmitter for all κ ambush locations, we have $\alpha^i = \alpha_1^i \vee \alpha_2^i \cdots \vee \alpha_\kappa^i$. Let $\mathbf{W}(t)$ denote the fake CSI converted with a specified breathing rate. The transmitter aims to make the estimated CSI at each ambush location be equal to the specified fake CSI, i.e., $\hat{\mathbf{W}}_r(t) = \mathbf{W}(t)$.

As discussed in Section IV-C, the transmitting signals on sensitive subcarriers will be first desensitized and then multiply with the forged CSI before being sent out. In this scenario, the coefficient vector for subcarrier desensitization at the s^{th} transmitting antenna is $\mathbf{C}_s(t) = [C_s^1(t), \cdots, C_s^N(t)]$. Also, the coefficient vector for the CSI forgery module at each transmitting antenna is $\mathbf{D}(t) = [D_1(t), \cdots, D_N(t)]$, where we set $D_i(t) = 0$ if $\alpha^i = 0$ and have $D_i(t) = W_i(t)$ if $\alpha^i = 1$. Similarly, each transmitting antenna utilizes the same coefficient vector $\mathbf{D}(t)$ for the CSI forgery module. Accordingly, we can then solve the manipulated signal $\mathbf{X}_m(t)$, and rewrite Equation 2 as

$$\mathbf{X}_m(t) = \begin{bmatrix} \mathrm{diag}(\mathbf{D}(t)) \cdot \mathrm{diag}(\mathbf{C}_1(t)) \cdot \mathbf{S}(t) + \mathbf{IS}(t) \\ \vdots \\ \mathrm{diag}(\mathbf{D}(t)) \cdot \mathrm{diag}(\mathbf{C}_\kappa(t)) \cdot \mathbf{S}(t) + \mathbf{IS}(t) \end{bmatrix} \tag{4}$$

where $\mathbf{C}_s(t)$ is the coefficient vector for the subcarrier desensitization module at the s^{th} transmitting antenna.

Equation 4 has κ unknowns ($\mathbf{C}_1(t)$ to $\mathbf{C}_\kappa(t)$). As the number of transmitting antennas equals the number of unknowns, the linear system formed by Equation 4 has a unique solution. It demonstrates when the transmitter is able to set the coefficient vector for the subcarrier desensitization module at the s^{th} transmitting antenna with the computed $\mathbf{C}_s(t)$, the goal of deploying κ simultaneous ambush locations can be achieved.

F. Security Analysis

The proposed scheme is known by the eavesdropper. One concern is whether the eavesdropper can distinguish ambush locations or even indirectly compute the real CSI of sensitive subcarriers (to infer the true breathing rate).

1) Ambush Indistinguishability: With the Fresnel Zone principle, CSI-based breathing rate inference works at certain locations, while its performance may deteriorate greatly at other locations [9]. Thus, when the eavesdropper moves out of the ambush location, though she cannot detect the breathing rate as when she is at the ambush location, she is still unable to distinguish this case from the normal one when the ambush scheme is not enforced. Such ambush indistinguishability leaves the eavesdropper in a dilemma: if she believes the inferred breathing rate, she will be deceived; instead, if she does not trust any inferred breathing rate, her ability to eavesdropping breathing rate is lost.

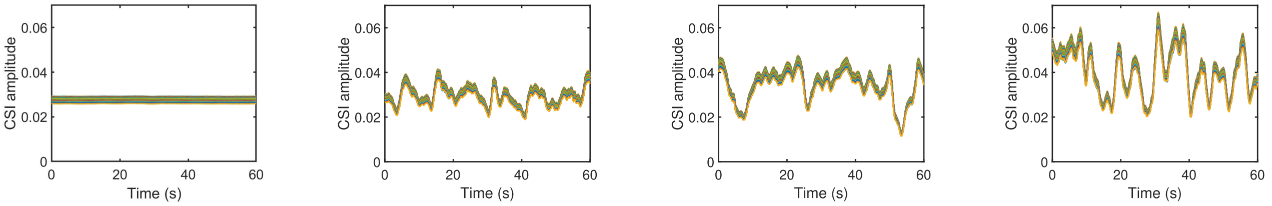
2) Indirect Calculation: To calculate the real CSI, an eavesdropper must compromise the phase of distribution manipulation. As shown in Section IV-C, suppose that the i^{th} subcarrier is sensitive, the transmitting signal on this subcarrier can be represented as $X_i^m(t) = \alpha_i C_i(t) D_i(t) X_i(t) + (1 - \alpha_i) X_i(t)$. We utilize $M_i(t) = C_i(t) D_i(t)$ to denote the total impact of disturbance manipulation. Let R_i^e denote the signal received by the eavesdropper on the i^{th} subcarrier, and $H_i^e(t)$ denote the corresponding real subcarrier CSI between the transmitter and eavesdropper. Thus, we have $R_i^e = X_i^m(t) H_i^e(t) = a_i M_i(t) X_i(t) H_i^e(t) + (1 - a_i) X_i(t) H_i^e(t)$.

To learn $M_i(t)$, the eavesdropper must learn both a_i and $H_i^e(t)$. However, this imposes a strong requirement for the eavesdropper. On one hand, without the knowledge of the accurate positions of the target user and the transmitter, the eavesdropper can hardly determine the subcarrier sensitivity except by guessing. On the other hand, the transmitter can always hide its real CSI between itself and the eavesdropper. Thus, $H_i^e(t)$ is not available. Consequently, the eavesdropper would fail to obtain $M_i(t)$ and cannot calculate the real CSIs of sensitive subcarriers for inferring the true breathing rate.

V. Crowd Inference Attacks and Defenses

A crowd inference attack using CSI is a technique that leverages wireless signals to estimate the number of people in an area of interest. The key idea of a crowd inference attack is that as more people enter the given area, the wireless signals will reflect off their bodies and change the channel characteristics. After extracting the CSI features, machine learning algorithms can be used to analyze the CSI data and estimate the number of people in the area accurately. To counteract such a CSI-based crowd inference attack, we propose the corresponding defenses called *Ghost* in the following.

We first explore the relationship between the CSI amplitude and the number of moving people in the given area. Thus, we investigate the amplitude of CSI measurements at each subcarrier within a certain time interval in several different



(a) Empty room. **(b)** One person in a room. **(c)** Two persons in a room. **(d)** Three persons in a room.

Fig. 4. CSI amplitudes at all subcarriers in different situations.

situations (i.e., empty, one person in a room, two persons in a room, three persons in a room). As shown in Figure 4, we have the following observations: (1) different subcarriers show similar fluctuations, which demonstrates they have similar responses towards movement, and all subcarriers are sensitive due to the random changes of position; (2) the CSI amplitude is not periodic or predictable due to the random walking; (3) when the room is empty (i.e., no person is present), the CSI amplitude is almost flat and stable; (4) the variation of CSI amplitude becomes larger when the number of moving people increases. Based on these observations, we can subsequently design our *Ghost* defense against the crowd inference attack.

A. Overview

To defend against the crowd inference attack, the transmitter first arbitrarily specifies a fake person number to fool the attacker into entering the ambush. Due to the fact that all subcarriers are sensitive to the random movements of people in the given area, the ambush locations can be selected in hidden or concealed areas. Additionally, the ambush locations can be determined based on the locations where the eavesdropper is most likely to appear, and then deployed along the eavesdropper's possible route.

Different from *HoneyBreath* in Section IV-A, *Ghost* targets an empty room and fools the receiver into estimating the wrong person count in the room. The transmitter first proceeds to the *planning* phase, which consists of two tasks: CSI profile construction and CSI retrieval. Based on observation (2), the CSI amplitude is not periodic or predictable. Therefore, to map the specified person count to the CSI measurements, the transmitter can construct the CSI profile by collecting the CSI measurements corresponding to the different numbers of individuals. Later, according to the fake person count selected by the transmitter, the corresponding CSI stream can be retrieved from the built library and then fed into the next phase, *disturbance manipulation*. Due to observation (1), as all subcarriers are sensitive to movements, the transmitter performs the same operation on each subcarrier. Then, all crafted signals are aggregated and sent out. Consequently, the attacker estimates the person number by performing the general *person number estimation* process. Figure 5 illustrates the flow chart of the proposed *Ghost* defense.

B. Planning Phase

1) CSI Profile Construction: Different from the breathing inference attack where the victim is static, the victims in the crowd counting system move randomly. In this way, it is not possible to predict how the CSI varies with time. To address this challenge, the CSI profile can be constructed by collecting several CSI measurements when there are different numbers of moving people. Let $\mathbf{S}^p(t) = \{\mathbf{S}_1^p(t), \mathbf{S}_2^p(t), \cdots, \mathbf{S}_k^p(t)\}$ denote the CSI profile, where $p = 0, 1, \cdots, P$ represents the person number and $k = 0, 1, \cdots, K$ means the trial number. For each scenario with a different number of individuals, CSI measurements are collected in multiple trials at different times.

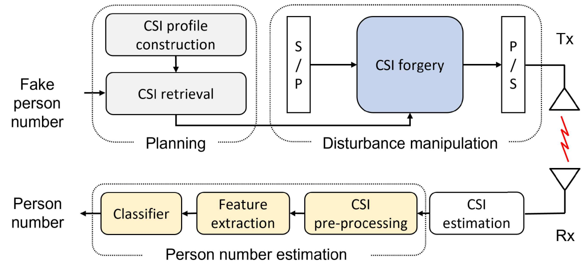


Fig. 5. Flow chart of the proposed *Ghost* defense.

2) CSI Retrieval: The transmitter plans to send specified CSI to the receiver, from which the person number can be estimated. Thus, for the given person number p that is used to fool the attacker, the corresponding CSI $\mathbf{S}_k^p(t)$ can be extracted from the library as the specified CSI.

C. Disturbance Manipulation

Different from Section IV-C, it is not required to perform different operations on sensitive subcarriers and insensitive subcarriers, respectively. Since all subcarriers are sensitive to human movements during the walking period, CSI forgery needs to be performed on each subcarrier. To achieve it, the multiply-accumulate (MAC) process is exploited by the transmitter to generate desired artificial disturbance. In detail, the S/P converter takes this input sequence and splits it into N parallel subcarrier signals. After that, a coefficient vector $\mathbf{D}(t) = \frac{\mathbf{S}_k^p(t)}{H_r(t)}$ would add the effect of the artificial CSI to signals on each subcarrier, where $H_r(t)$ is the real CSI of the empty room. Thus, the artificial CSI is $\mathbf{D}(t)\mathbf{X}(t)$. Finally, signals on all subcarriers are concatenated through a P/S converter module to form OFDM symbols.

D. Person Number Estimation

1) CSI Pre-Processing: After gathering the CSI measurements from the transmitter, the receiver first performs the CSI estimation based on the original training sequence and the received data. Since the CSI data is considerably noisy due to various factors such as interference, multipath fading, and hardware imperfections, it is necessary to remove the redundant components from the calculated amplitude values. For this smoothing process, we apply two kinds of filters, one is the Hampel filter for eliminating impulse noises, and the other is the moving average filter for removing high-frequency noise while preserving the low-frequency components.

2) Feature Extraction: By leveraging the CSI amplitude from each subcarrier, various statistical features [68], [77] can be extracted for crowd counting as follows:

- *Mean:* the average value of amplitude.
- *Standard deviation:* shows how individual amplitude values deviate from the mean amplitude value.
- *Median Absolute Difference:* a robust measure of dispersion that is not affected by outliers.
- *Maximum:* the highest amplitude value.
- *Minimum:* the lowest amplitude value.
- *Skewness:* encompasses the asymmetric shape of the CSI subcarrier profile and indicates a stronger or weaker signal on the left or right.
- *Kurtosis:* represents how tail-heavy the shape is compared to a normal distribution (meaning more extreme values).
- *Entropy:* measures the amount of signal information.

After that, the CSI at each subcarrier corresponds to a 1×8 feature vector, which can be combined into a $N \times 8$ feature matrix, where N represents the number of subcarriers. Since these CSI amplitudes present similar variations and describe the same human movement, the average value of each feature across all subcarriers is calculated and regenerates the final 1×8 feature vector, which is fed into the classifier later.

3) Classifier: Accordingly, based on these common statistical features, a feature set can be created for each training sample to form a labeled dataset. Two widely used classifiers are trained to divide inputs into different predefined classes and then make decisions as follows:

- *Support Vector Machine (SVM):* used with one-versus-one (OvO) strategies, finds the hyperplane that maximally separates the data points of different classes.
- *Decision Tree (DT):* used with OvO strategies, recursively partitions the data and selects the optimal boundaries that best separate the data points of different classes.

Based on the trained classifier, the number of moving people can be estimated from the collected CSI measurements.

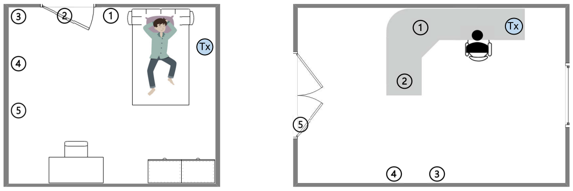
VI. Experimental Evaluation

A. Experimental Setup

We implement CSI-based breathing rate inference and our proposed ambush schemes on top of Universal Software Radio Peripheral (USRP) X310s [78]. The prototype system includes a transmitter Tx and an eavesdropper Eve (i.e., malicious receiver). Each node is a USRP X310. We recruited 5 participants and asked each to act as the target user of the inference attacks over three months. Also, each wore a Masimo MightySat Fingertip Pulse Oximeter [79] with hospital-grade technology to obtain ground-truth breathing rate. The parameters of experimental settings are summarized in Table I.

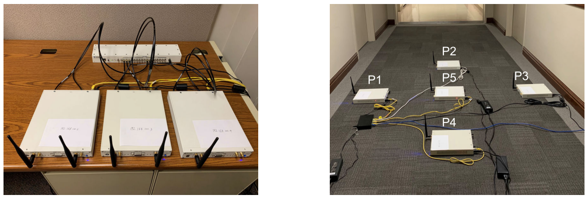
TABLE I
Experimental Setting

Experimental parameter	Value
Scenarios	bedroom (br), office room (or)
Location per scenario	L1-L5
Users	U1-U5
Estimated breathing rate	$\hat{r}$
Specified breathing rate	r_a
Ground truth	r_{gt}
Absolute estimation error (AEE)	ϵ
Absolute ambush error (AAE)	η
Defenses	**D1-D3**
Ambush points per trap area	P1-P5



(a) Bedroom (User lies down). **(b)** Office (User sits).

Fig. 6. Layout of the experimental environment.



(a) Five-antenna transmitter with USRPs. **(b)** Ambush area.

Fig. 7. Setup for deploying an ambush area.

1) Scenarios: We test two typical scenarios: (1) a bedroom, where the user lies on a bed; (2) an office room with the user sitting in a chair. Figure 6 shows the ambush locations and the position of the transmitter. For each scenario, we place Eve at 5 different ambush locations to infer the user's breathing rate, and the transmitter launches the proposed ambush scheme.

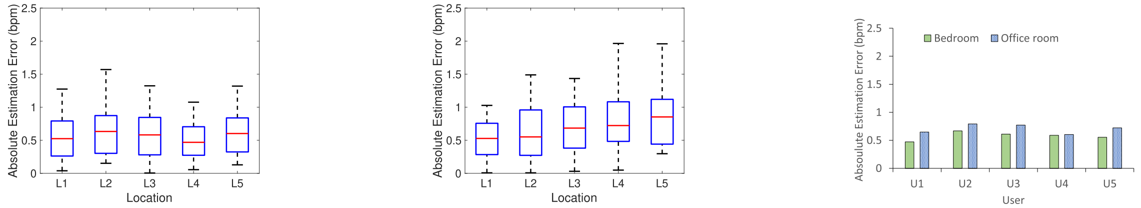
To deploy a trap area, as shown in Figure 7a, we use a 5-antenna transmitter, consisting of three USRP X310s, which are connected with a host computer through an Ethernet switch and synchronized with OctoClock-G [80]. As shown in Figure 7b, five collaborative eavesdroppers are placed at 5 specified ambush points on the corridor outside of the office room: one in the center and the other four in the circle with a radius (i.e., antenna-antenna distance) of 0.75 m.

2) Metrics: Let $\hat{r}$ denote the estimated rate. We apply the following two metrics.

- *Absolute estimation error ϵ:* the difference between true and estimated breathing rates, i.e., $|r_{gt} - \hat{r}|$, where r_{gt} is the ground truth.
- *Absolute ambush error η:* the difference between estimated and specified breathing rates, i.e., $|r_a - \hat{r}|$, where r_a is the one specified by the transmitter.

B. Breathing Rate Inference Attacks

We first verify the effectiveness of using CSI to infer breathing rates. Eve estimates each participant's breathing rate



(a) In the bedroom. **(b)** In the office room. **(c)** Mean value of ϵ.

Fig. 8. Values of ϵ and ϵ at Eve when no defense is enforced.

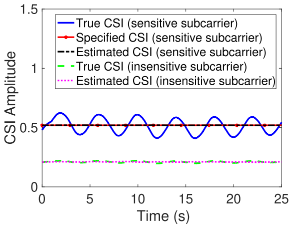


Fig. 9. Enabling Eve to obtain no breathing activity.

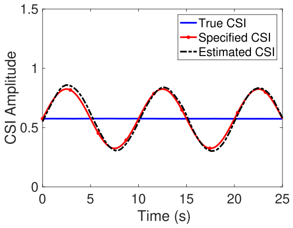


Fig. 10. Fabricating normal breath.

100 times at each ambush location. This results in a total of 5,000 trials, with each trial lasting at least one minute.

Figure 8 shows the obtained absolute estimation error when the proposed ambush scheme is not launched. Figure 8a shows that the inference technique always achieves high accuracy with less than 1.6 bpm of error at all locations in the bedroom. The median absolute estimation error ranges from 0.4 to 0.6 bpm across all locations. Meanwhile, we see the value of ϵ on average is slightly larger at Location 2 than at other locations. This is because Location 2 is not in the LOS of the user and the resultant signal fading degrades the inference performance. We have similar observations from Figure 8b. Figure 8c depicts the mean absolute estimation errors for different users (referred to as U1$\sim$U5). We can observe that the mean absolute estimation error is consistently low (i.e., below 0.8 bpm) across all users in both environments. Also, the average absolute estimation error for each user in the office room is larger than that in the bedroom. It can be explained by the fact that the user has less body movement irrelevant to breathing activity when lying on the bed than when sitting in the chair. These results demonstrate that an eavesdropper could utilize passively collected CSI to accurately infer a person's breathing rate in different scenarios.

C. Example Defenses

We examine three example defenses, in which we deploy the ambush location at Location 1 shown in Figure 6a.

1) Example 1 - Making Breath Unobservable: We first show a defense method by hiding breathing rates, i.e., when Eve appears at the ambush location, she would obtain a breathing rate of 0 (i.e., no breathing activity is detected).

Figure 9 plots the real CSI between the transmitter and the ambush location, the estimated CSI at the ambush location, as well as the subcarrier CSI specified by the transmitter. We can observe that the transmitter can make Eve observe the CSI on a sensitive subcarrier significantly near to the specified one while both greatly deviate from the true one; with the estimated CSI, Eve obtains a breathing rate of 0 though the true one is 15.1 bpm. The absolute estimation error is thus 15.1 bpm, while the absolute ambush error is 0. Besides, the CSI of the insensitive subcarrier keeps insensitive with the defense (we thus only focus on sensitive subcarriers in the later evaluation).

2) Example 2 - Fabricating Nonexistent Breath: We aim to make Eve obtain a fake breathing rate while there is no breathing activity. We specify a fake breathing rate of 6 bpm.

As shown in Figure 10, we see the true CSI is almost flat, as there is in fact no breathing activity, and the estimated CSI is quite consistent with the CSI specified by the transmitter. With the estimated CSI, Eve obtains a breathing rate of 6.4 bpm. The absolute estimation error becomes 6.4 bpm, thus the absolute ambush error is as small as 0.4 bpm.

3) Example 3 - Falsifying Breath: We aim to hide a normal breathing rate by making Eve observe an abnormal one. We randomly specify an abnormal breathing rate of 40 bpm.

Similar to the above examples, we observe from Figure 11 that the estimated CSI is quite close to the specified CSI while it greatly differs from the true CSI in both environments. The estimated breathing rate becomes 40.2 bpm, instead of the true one (i.e., 19.9 bpm) derived from the Masimo Oximeter. Therefore, the absolute estimation error is 20.3 bpm, while the absolute ambush error is just 0.2 bpm.

D. Overall Defense Impact

We examine the overall impact of the three defenses (numbered according to their respective cases): (1) a user is breathing while we aim to make Eve obtain no breathing activity; (2) no breathing activity occurs while we aim to make Eve obtain a fake breathing rate; (3) a user is breathing while we aim to make Eve obtain a different non-zero breathing rate. Eve estimates the breathing rate at every ambush location. For each estimate, we perform 100 trials. This results in a total of 11,000 trials, with each trial lasting at least one minute.

D1: We test when the user has different breathing rates in the range of 6-27 bpm. For all trials, we find that Eve always obtains an estimated breathing rate of 0, indicating the consistent success of the defense. Let $P(\epsilon_{br} \leq x)$ and $P(\epsilon_{or} \leq x)$ denote the empirical cumulative distribution

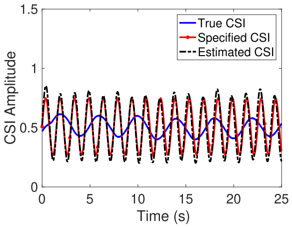


Fig. 11. Making Eve obtain abnormal breath.

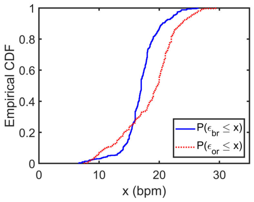


Fig. 12. CDFs of $P(\epsilon \leq x)$ for **D1**.

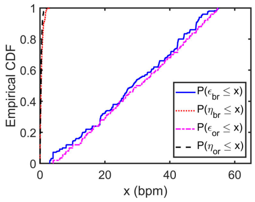


Fig. 13. CDFs of $P(\epsilon \leq x)$ and $P(\eta \leq x)$ for **D2**.

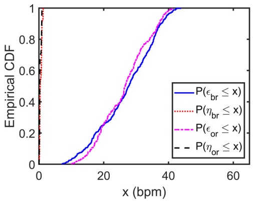


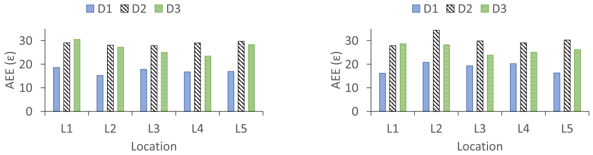
Fig. 14. CDFs of $P(\epsilon \leq x)$ and $P(\eta \leq x)$ for **D3**.

functions (CDFs) of the absolute estimation error ϵ_{br} for the bedroom and ϵ_{or} for the office room. Figure 12 shows that ϵ_{br} and ϵ_{or} lie in the ranges of [6.6, 26.5] and [7.5, 29.6] with probability 100%. Both demonstrate that Eve always has a significant error in the breathing rate estimation with the proposed defense.

D2: We randomly specify a fake breathing rate within the range of 3-55 bpm in each trial. Let $P(\eta_{br} \leq x)$ and $P(\eta_{or} \leq x)$ denote the CDFs of the absolute ambush errors η_{br} for the bedroom and η_{or} for the office room. As shown in Figure 13, we observe a small η and a high ϵ for both environments. For example, η_{br} is less than 1.5 bpm with a probability of 95.0%, while ϵ_{br} ranges from 3.0 to 54.8 bpm and is larger than 3.1 with a probability of 98.2%.

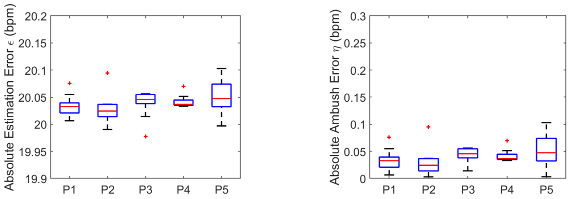
D3: Each participant has a normal breathing rate, and the transmitter chooses a bogus breathing rate randomly in an abnormal range (31-56 bpm). Figure 14 shows the CDFs of the corresponding ϵ and η. We can see that ϵ_{br} and ϵ_{or} are larger than 11 bpm with probabilities of 96.2% and 99.0%, respectively. Meanwhile, η_{br} is always less than 1.2 bpm, and η_{or} is always less than 0.9 bpm.

Figures 15a and 15b show the mean value of ϵ across all locations in both environments when the proposed defenses are employed. We observe that ϵ stays consistently high at all ambush locations for both environments. Compared with no defense, all defenses can significantly increase ϵ at Eve.



(a) In the bedroom.
(b) In the office room.

Fig. 15. Mean absolute estimation errors (AEE).



(a) Absolute estimation error.
(b) Absolute ambush error.

Fig. 16. Fabricating normal breath for a trap area.

E. Trap Area

We aim to generate fake breath rates in the trap area consisting of five ambush points (referred to as P1∼P5), as shown in Figure 7b. We choose a breathing rate of 20 bpm when the target room has no breathing activity. We perform 10 trials of deploying a trap area, with each trial lasting at least one minute.

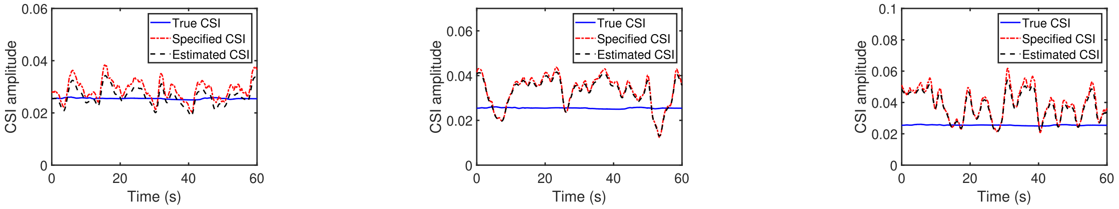
Figure 16a shows that the absolute estimation errors at all ambush points are consistently large (close to 20 bpm). Figure 16b demonstrates that the absolute ambush errors at all ambush points are quite small, with the mean value ranging from 0.03 to 0.05 bpm across all ambush points. These results demonstrate that the proposed scheme can simultaneously deploy multiple ambush points to mislead collaborative eavesdroppers (or simply increase the probability of trapping a single eavesdropper) with fake breathing rates.

F. Ghost Defense

1) Experimental Setup: Similarly, we implemented CSI-based crowd inference and our proposed defense schemes using USRP X310s [78], which were used as a transmitter (Tx) and an eavesdropper (Eve, i.e., malicious receiver).

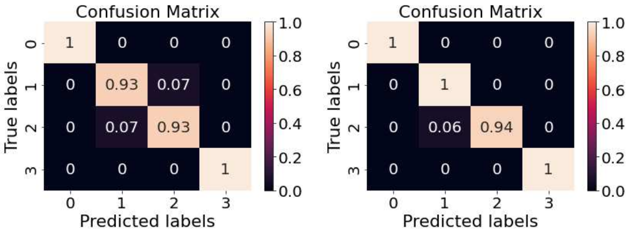
We asked 3 participants to randomly walk in a room. To build the CSI profile, we collected CSI data in four scenarios: empty room, one person in a room, two persons in a room, and three persons in a room. We performed 50 estimations for each scenario, resulting in a total of $50 \times 4 = 200$ estimations. Each estimation lasted for one minute. We then split the dataset into training (70%) and testing sets (30%). The training set was used to train the classifier, while the testing set was used to evaluate its performance.

For the defense scheme, we first performed 20 trials in the empty room. After that, we randomly selected one pre-collected CSI for each of the three defense strategies (i.e., fabricating the presence of one person, two persons, or three persons in an empty room). We conducted 20 trials for each defense strategy, resulting in $20 \times (1 + 3) = 80$ trials in



(a) One person. **(b)** Two persons. **(c)** Three persons.

Fig. 17. Estimated CSI at Eve in an empty room when our defense is enforced.



(a) SVM classifier. **(b)** DT classifier.

Fig. 18. Confusion matrix for crowd inference attack.

total, with each trial lasting at least one minute. We used the estimated CSI data to test the trained classifiers and evaluate our defense scheme.

To evaluate the crowd inference attack and the proposed defense, we used a confusion matrix to visualize the results. The accuracy was then calculated to indicate the proportion of correct predictions out of the total number of predictions.

2) Crowd Inference Attacks: We first verified the effectiveness of using CSI to estimate the number of people present. Figure 18 shows the confusion matrix for two classifiers when the proposed defense scheme is not employed. As observed, the SVM classifier achieves an accuracy of 96.5%, while the DT classifier achieves an accuracy of 98.5%.

3) Example Defenses: We examine three example defenses, in which we deploy the proposed defense in the empty room to fool the attacker to consider it as an occupied room.

We demonstrate a defense method that involves fabricating one, two, or three moving individuals in an empty room when Eve attempts to launch a crowd inference attack. Figure 17 plots the real CSIs between the transmitter and the ambush location, the estimated CSIs at the ambush location, and the subcarrier CSI specified by the transmitter. In an empty room, the transmitter can cause Eve to observe a CSI on each subcarrier that is significantly close to the specified one, while both are greatly different from the true one (since the CSI is almost flat and stable in an empty room). It is noted that the specified CSI is extracted from the built CSI profile, which consists of various collected true CSIs. Thus, by obtaining these CSIs in Figures 17a, 17b, and 17c, respectively, the attacker will estimate the corresponding person number as 1, 2, and 3, after inputting such estimated CSI into the classifier.

4) Overall Defense Impact: We examined the overall impact of our defense strategies. Specifically, we consider a scenario where the actual number of people in a room is zero (i.e., the true label is 0). If Eve launches a crowd inference attack in this empty room, both the trained SVM and DT classifiers can initially identify the empty room with 100% accuracy. However, after each defense strategy is implemented, both classifiers misclassify the empty room as containing one, two, or three people, also with a 100% probability. Consequently, the accuracy of both classifiers dropped to 0%. These results demonstrate that Eve consistently makes significant errors in estimating the crowd count when our defense strategies are applied, further confirming the effectiveness of our defenses.

VII. Conclusion

Wireless signals have demonstrated exceptional capability to detect breathing activity and estimate person count, which introduces a new threat to the security of personal information. To address this issue, we design an ambush-based strategy by actively deploying ambush locations and feeding eavesdroppers who move to those ambush locations with fake breathing rates or person count. This scheme enables the transmitter to encode the specified fake breathing rate or person count into CSI, and then utilize disturbance manipulation to deliver it to the eavesdropper. We conduct an extensive real-world evaluation on the USRP X310 platform. Experimental results in different scenarios consistently demonstrate the effectiveness of the proposed defenses.

References

[1] M. Nakatsuka, H. Iwatani, and J. Katto, “A study on passive crowd density estimation using wireless sensors,” in *Proc. 4th Intl. Conf. Mobile Comput. Ubiquitous Netw. (ICMU)*, 2008, pp. 1–6.

[2] Y. Yuan, J. Zhao, C. Qiu, and W. Xi, “Estimating crowd density in an RF-based dynamic environment,” *IEEE Sensors J.*, vol. 13, no. 10, pp. 3837–3845, Oct. 2013.

[3] C. Xu et al., “SCPL: Indoor device-free multi-subject counting and localization using radio signal strength,” in *Proc. ACM/IEEE Int. Conf. Inf. Process. Sensor Netw. (IPSN)*. New York, NY, USA. Association for Computing Machinery, Apr. 2013, pp. 79–90.

[4] W. Xi et al., “Electronic frog eye: Counting crowd using WiFi,” in *Proc. IEEE Conf. Comput. Commun.*, Oct. 2014, pp. 361–369.

[5] A. Hanif, M. Iqbal, and F. Munir, “WiSpy: Through-wall movement sensing and person counting using commodity WiFi signals,” in *Proc. IEEE SENSORS*, Oct. 2018, pp. 1–4.

[6] X. Guo, B. Liu, C. Shi, H. Liu, Y. Chen, and M. C. Chuah, “WiFi-enabled smart human dynamics monitoring,” in *Proc. 15th ACM Conf. Embedded Netw. Sensor Syst.*, New York, NY, USA, Nov. 2017, pp. 1–13.

[7] S. Liu, Y. Zhao, and B. Chen, “WiCount: A deep learning approach for crowd counting using WiFi signals,” in *Proc. IEEE Int. Symp. Parallel Distrib. Process. Appl., IEEE Int. Conf. Ubiquitous Comput. Commun. (ISPA/IUCC)*, Dec. 2017, pp. 967–974.

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

[9] L. Chen et al., “LungTrack: Towards contactless and zero dead-zone respiration monitoring with commodity RFIDs,” *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 3, pp. 1–22, Sep. 2019.

[10] P. Hillyard et al., "Experience: Cross-technology radio respiratory monitoring performance study," in *Proc. 24th Annu. Int. Conf. Mobile Comput. Netw.*, New York, NY, USA, Oct. 2018, pp. 487–496.

[11] W. Jia, H. Peng, N. Ruan, Z. Tang, and W. Zhao, "WiFind: Driver fatigue detection with fine-grained Wi-Fi signal features," *IEEE Trans. Big Data*, vol. 6, no. 2, pp. 269–282, Jun. 2020.

[12] X. Liu, J. Cao, S. Tang, J. Wen, and P. Guo, "Contactless respiration monitoring via off-the-shelf WiFi devices," *IEEE Trans. Mobile Comput.*, vol. 15, no. 10, pp. 2466–2479, Oct. 2016.

[13] J. Liu, Y. Wang, Y. Chen, J. Yang, X. Chen, and J. Cheng, "Tracking vital signs during sleep leveraging off-the-shelf WiFi," in *Proc. 16th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2015, pp. 267–276.

[14] N. Patwari, L. Brewer, Q. Tate, O. Kaltiokallio, and M. Bocca, "Breathfinding: A wireless network that monitors and locates breathing in a home," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 1, pp. 30–42, Feb. 2014.

[15] Y. Zeng, D. Wu, R. Gao, T. Gu, and D. Zhang, "FullBreathe: Full human respiration detection exploiting complementarity of CSI phase and amplitude of WiFi signals," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 2, no. 3, pp. 1–19, Sep. 2018.

[16] H. Wang et al., "Human respiration detection with commodity WiFi devices: Do user location and body orientation matter?" in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, Sep. 2016, pp. 25–36.

[17] X. Wang et al., "Placement matters: Understanding the effects of device placement for WiFi sensing," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 6, no. 1, pp. 1–25, Mar. 2022.

[18] H. Abdelnasser, K. A. Harras, and M. Youssef, "UbiBreathe: A ubiquitous non-invasive WiFi-based breathing estimator," in *Proc. 16th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2015, pp. 277–286.

[19] A. R. Fekr, M. Janidarmian, K. Radecka, and Z. Zilic, "Respiration disorders classification with informative features for m-Health applications," *IEEE J. Biomed. Health Informat.*, vol. 20, no. 3, pp. 733–747, May 2016.

[20] S. Mosleh, J. B. Coder, C. G. Scully, K. Forsyth, and M. O. A. Kalaa, "Monitoring respiratory motion with Wi-Fi CSI: Characterizing performance and the BreatheSmart algorithm," *IEEE Access*, vol. 10, pp. 131932–131951, 2022.

[21] R. A. Cox and C. Z. Torres, "Acute heart failure in adults," *Puerto Rico Health Sci. J.*, vol. 23, no. 4, pp. 265–271, 2004.

[22] D. Fan et al., "Breathing rhythm analysis in body centric networks," *IEEE Access*, vol. 6, pp. 32507–32513, 2018.

[23] D. B. Lafky and T. A. Horan, "Personal health records: Consumer attitudes toward privacy and security of their personal health information," *Health Informat. J.*, vol. 17, no. 1, pp. 63–71, Mar. 2011.

[24] H. Ellyatt. (Sep. 2012). *How CEO Health Can Affect Your Wealth*. CNBC. [Online]. Available: https://www.cnbc.com/id/49115208

[25] W. Duggan. (Dec. 2017). *CSX Stock Plummets On CEO's Health Concerns*. US News. [Online]. Available: https://money.usnews.com/investing/stock-market-news/articles/2017-12-15/csx-corporation-stock-plummets-on-ceos-health-concerns

[26] 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.

[27] S. Pradhan, W. Sun, G. Baig, and L. Qiu, "Combating replay attacks against voice assistants," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 3, no. 3, pp. 1–26, Sep. 2019.

[28] Y. Ma, G. Zhou, and S. Wang, "WiFi sensing with channel state information: A survey," *ACM Comput. Surv.*, vol. 52, pp. 1–36, Jun. 2019.

[29] F. Wang, F. Zhang, C. Wu, B. Wang, and K. J. R. Liu, "Respiration tracking for people counting and recognition," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5233–5245, Jun. 2020.

[30] C. Willis. (2017). *Vacant Homes Becoming Latest Targets for Burglars*. [Online]. Available: https://www.wsbtv.com/news/local/vacant-homes-becoming-latest-targets-for-burglars/579935438/

[31] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[32] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1125–1133.

[33] W. Shen, P. Ning, X. He, and H. Dai, "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 174–188.

[34] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *J. Inf. Secur. Appl.*, vol. 22, pp. 113–122, Jun. 2015.

[35] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing keys from PCs using a radio: Cheap electromagnetic attacks on windowed exponentiation," in *Cryptographic Hardware and Embedded Systems—CHES*, T. Güneysu and H. Handschuh, Eds., Berlin, Germany: Springer, 2015, pp. 207–228.

[36] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 160–173.

[37] X. Zhang, S. Yu, H. Zhou, P. Huang, L. Guo, and M. Li, "Signal emulation attack and defense for smart home IoT," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 3, pp. 2040–2057, May/Jun. 2023.

[38] R. Ayyalasomayajula, A. Arun, W. Sun, and D. Bharadia, "Users are closer than they appear: Protecting user location from WiFi APs," in *Proc. 24th Int. Workshop Mobile Comput. Syst. Appl.*, New York, NY, USA, Feb. 2023, pp. 124–130.

[39] Y. Zhou, H. Chen, C. Huang, and Q. Zhang, "WiAdv: Practical and robust adversarial attack against WiFi-based gesture recognition system," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 6, no. 2, pp. 1–25, Jul. 2022.

[40] Y. Zeng, D. Wu, J. Xiong, E. Yi, R. Gao, and D. Zhang, "FarSense: Pushing the range limit of WiFi-based respiration sensing with CSI ratio of two antennas," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 3, no. 3, pp. 1–26, Sep. 2019.

[41] H. Zhuo, X. Wu, Q. Zhong, and H. Zhang, "Position-free breath detection during sleep via commodity WiFi," *IEEE Sensors J.*, vol. 23, no. 20, pp. 24874–24884, Oct. 2023.

[42] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[43] R. Crepaldi, J. Lee, R. Etkin, S.-J. Lee, and R. Kravets, "CSI-SF: Estimating wireless channel state using CSI sampling & fusion," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 154–162.

[44] S. Venkatesh, C. R. Anderson, N. V. Rivera, and R. M. Buehrer, "Implementation and analysis of respiration-rate estimation using impulse-based UWB," in *Proc. IEEE Mil. Commun. Conf.*, Oct. 2005, pp. 3314–3320.

[45] J. Salmi and A. F. Molisch, "Propagation parameter estimation, modeling and measurements for ultrawideband MIMO radar," *IEEE Trans. Antennas Propag.*, vol. 59, no. 11, pp. 4257–4267, Nov. 2011.

[46] Federal Communications Commission (FCC), *Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Transmission Systems*, 1st Rep. Order, FCC 02-48, Washington, DC, USA, 2002.

[47] L. Lampe and K. Witrisal, "Challenges and recent advances in IR-UWB system design," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2010, pp. 3288–3291.

[48] A. D. Droitcour, O. Boric-Lubecke, and G. T. A. Kovacs, "Signal-to-noise ratio in Doppler radar system for heart and respiratory rate measurements," *IEEE Trans. Microw. Theory Techn.*, vol. 57, no. 10, pp. 2498–2507, Oct. 2009.

[49] M. Ascione, A. Buonanno, M. D'Urso, L. Angrisani, and R. S. L. Moriello, "A new measurement method based on music algorithm for through-the-wall detection of life signs," *IEEE Trans. Instrum. Meas.*, vol. 62, no. 1, pp. 13–26, Jan. 2013.

[50] C. Li, V. M. Lubecke, O. Boric-Lubecke, and J. Lin, "A review on recent advances in Doppler radar sensors for noncontact healthcare monitoring," *IEEE Trans. Microw. Theory Techn.*, vol. 61, no. 5, pp. 2046–2060, May 2013.

[51] T. Rahman et al., "DoppleSleep: A contactless unobtrusive sleep sensing system using short-range Doppler radar," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, New York, NY, USA, 2015, pp. 39–50.

[52] O. Boric-Lubecke, V. M. Lubecke, A. D. Droitcour, B.-K. Park, and A. Singh, *Doppler Radar Physiological Sensing*. Hoboken, NJ, USA: Wiley, 2016.

[53] Y. Xiao, J. Lin, O. Boric-Lubecke, and M. Lubecke, "Frequency-tuning technique for remote detection of heartbeat and respiration using low-power double-sideband transmission in the Ka-band," *IEEE Trans. Microw. Theory Techn.*, vol. 54, no. 5, pp. 2023–2032, May 2006.

[54] K. van Loon et al., "Wireless non-invasive continuous respiratory monitoring with FMCW radar: A clinical validation study," *J. Clin. Monitor. Comput.*, vol. 30, no. 6, pp. 797–805, Dec. 2016.

[55] F. Adib, Z. Kabelac, D. Katabi, and R. C. Miller, "3D tracking via body radio reflections," in *Proc. 11th USENIX Conf. Netw. Syst. Design Implement.*, Seattle, WA, USA, Apr. 2014, pp. 317–329.

[56] O. Kaltiokallio, H. Yigitler, R. Jäntti, and N. Patwari, “Non-invasive respiration rate monitoring using a single COTS TX-RX pair,” in *IPSN-14 Proc. 13th Int. Symp. Inf. Process. Sensor Netw.*, Apr. 2014, pp. 59–69.

[57] N. Patwari, J. Wilson, S. Ananthanarayanan, S. K. Kasera, and D. R. Westenskow, “Monitoring breathing via signal strength in wireless networks,” *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1774–1786, Aug. 2014.

[58] X. Liu, J. Cao, S. Tang, and J. Wen, “Wi-sleep: Contactless sleep monitoring via WiFi signals,” in *Proc. IEEE Real-Time Syst. Symp.*, Dec. 2014, pp. 346–355.

[59] X. Wang, C. Yang, and S. Mao, “PhaseBeat: Exploiting CSI phase data for vital sign monitoring with commodity WiFi devices,” in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst.*, Jun. 2017, pp. 1230–1239.

[60] X. Wang, C. Yang, and S. Mao, “TensorBeat: Tensor decomposition for monitoring multiperson breathing beats with commodity WiFi,” *ACM Trans. Intell. Syst. Technol.*, vol. 9, no. 1, pp. 1–27, Sep. 2017.

[61] F. Zhang et al., “From Fresnel diffraction model to fine-grained human respiration sensing with commodity Wi-Fi devices,” *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 2, no. 1, pp. 1–23, Mar. 2018.

[62] L. Gui, C. Ma, B. Sheng, Z. Guo, J. Cai, and F. Xiao, “In-home monitoring sleep turnover activities and breath rate via WiFi signals,” *IEEE Syst. J.*, vol. 17, no. 2, pp. 2355–2365, Jun. 2023.

[63] J. Liu, Y. Zeng, T. Gu, L. Wang, and D. Zhang, “WiPhone: Smartphone-based respiration monitoring using ambient reflected WiFi signals,” *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 5, no. 1, pp. 1–19, Mar. 2021.

[64] Y. Yin, X. Yang, J. Xiong, S. I. Lee, P. Chen, and Q. Niu, “Ubiquitous smartphone-based respiration sensing with Wi-Fi signal,” *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1479–1490, Jan. 2022.

[65] G. Solmaz, P. Baranwal, and F. Cirillo, “CountMeIn: Adaptive crowd estimation with Wi-Fi in smart cities,” in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, Mar. 2022, pp. 187–196.

[66] X. Ma, W. Xi, X. Zhao, Z. Chen, H. Zhang, and J. Zhao, “Wisual: Indoor crowd density estimation and distribution visualization using Wi-Fi,” *IEEE Internet Things J.*, vol. 9, no. 12, pp. 10077–10092, Jun. 2022.

[67] H. Jiang, S. Chen, Z. Xiao, J. Hu, J. Liu, and S. Dustdar, “Pa-count: Passenger counting in vehicles using Wi-Fi signals,” *IEEE Trans. Mobile Comput.*, vol. 23, no. 4, pp. 2684–2697, Apr. 2024.

[68] H. Choi, M. Fujimoto, T. Matsui, S. Misaki, and K. Yasumoto, “Wi-CaL: WiFi sensing and machine learning based device-free crowd counting and localization,” *IEEE Access*, vol. 10, pp. 24395–24410, 2022.

[69] D. Khan and I. W. Ho, “CrossCount: Efficient device-free crowd counting by leveraging transfer learning,” *IEEE Internet Things J.*, vol. 10, no. 5, pp. 4049–4058, Mar. 2023.

[70] Z. Guo, F. Xiao, B. Sheng, L. Sun, and S. Yu, “TWCC: A robust through-the-wall crowd counting system using ambient WiFi signals,” *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 4198–4211, Apr. 2022.

[71] N. Anand, S.-J. Lee, and E. W. Knightly, “STROBE: Actively securing wireless communications using zero-forcing beamforming,” in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 720–728.

[72] A. Chaman, J. Wang, J. Sun, H. Hassanieh, and R. Roy Choudhury, “Ghostbuster: Detecting the presence of hidden eavesdroppers,” in *Proc. 24th Annu. Int. Conf. Mobile Comput. Netw.*, New York, NY, USA, Oct. 2018, pp. 337–351.

[73] S. Sen, B. Radunovic, R. R. Choudhury, and T. Minka, “You are facing the Mona Lisa: Spot localization using PHY layer information,” in *Proc. 10th Int. Conf. Mobile Syst., Appl., Services*, New York, NY, USA, Jun. 2012, pp. 183–196.

[74] C. Wang, J. Liu, Y. Chen, H. Liu, and Y. Wang, “Towards in-baggage suspicious object detection using commodity WiFi,” in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, May 2018, pp. 1–9.

[75] L. Davies and U. Gather, “The identification of multiple outliers,” *J. Amer. Stat. Assoc.*, vol. 88, no. 423, pp. 782–792, Sep. 1993.

[76] S. W. Smith, *The Scientist and Engineer’s Guide To Digital Signal Processing*. San Diego, CA, USA: California Technical, 1997.

[77] J. Zhang, W. Xu, W. Hu, and S. Kanhere, “WiCare: Towards in-situ breath monitoring,” in *Proc. 14th EAI Int. Conf. Mobile Ubiquitous Systems: Comput., Netw. Services*, New York, NY, USA, 2018, pp. 126–135.

[78] Ettus Research. (2023). *USRP X310*. [Online]. Available: https://www.ettus.com/all-products/x310-kit/

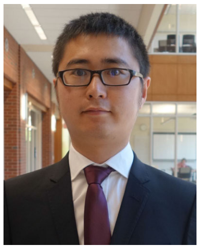
[79] Masimo. (2021). *MightySat Fingertip Pulse Oximeter With Bluetooth LE, RRp, & PVi*. [Online]. Available: https://www.masimopersonalhealth.com/products/mightysat-fingertip-pulse-oximeter-with-bluetooth-le-rrp-pvi

[80] M. Ettus. (2005). *USRP Users and Developers Guide*. [Online]. Available: www.olifantasia.com/gnuradio/usrp/files/usrp_guide. pdf

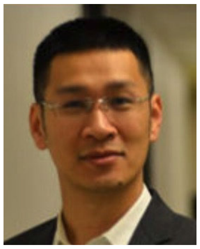
[81] Q. He, E. Yang, S. Fang, and S. Zhao, “HoneyBreath: An ambush tactic against wireless breath inference,” in *Mobile and Ubiquitous Systems: Computing, Networking and Services*. Cham, Switzerland: Springer, 2023, pp. 203–226.

Qiuye He received the Ph.D. degree in computer science from the University of Oklahoma in 2024. She is currently an Assistant Professor with the School of Science and Engineering, University of Missouri-Kansas City. Her research interests include wireless security, the Internet of Things (IoT) security, and mobile sensing and computing.

Edwin Yang received the M.S. degree from Yonsei University, Seoul, South Korea, in 2017, and the Ph.D. degree in computer science from the University of Oklahoma in 2024. His research interests are mobile system security and the IoT security.



Song Fang received the Ph.D. degree in computer science from the University of South Florida in 2018. He is currently an Associate Professor with the School of Computer Science, University of Oklahoma. His research interests include wireless and mobile system security, cyber-physical systems and IoT security, mobile computing, applying machine learning in wireless, and mobile systems.



Shangqing Zhao (Member, IEEE) received the Ph.D. degree in computer science from the University of South Florida in 2021. He is currently an Assistant Professor with the School of Computer Science, University of Oklahoma. His research interests include network and mobile system design and security.