HoneyBreath: An Ambush Tactic Against Wireless Breath Inference

Qiuye He[1][0000−0003−1315−1994], Edwin Yang[1][0000−0002−1794−5014], Song Fang[1][0000−0001−7879−3731], and Shangqing Zhao[1][0000−0001−8543−2977]

University of Oklahoma, Norman OK 73019, USA

Abstract. Breathing rates can be used to verify the human presence and disclose a person's physiological status. Many studies have demonstrated success in applying channel state information (CSI) to infer breathing rates. 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. In this paper, we discover a new type of proactive countermeasures against all existing CSI-based vital signs inference techniques. Specifically, we set up ambush locations with carefully designed wireless signals, where eavesdroppers infer a fake breathing rate specified by the transmitter. The true breathing rate is thus protected. Experimental results on software-defined radio platforms show with the proposed defenses, the eavesdropper is no longer able to infer breathing rates accurately using CSI, and would be fooled by a fake one crafted by the transmitter instead.

Keywords: Breathing rate inference · Deceptive communication · Anti-eavesdropping · Channel state information.

1 Introduction

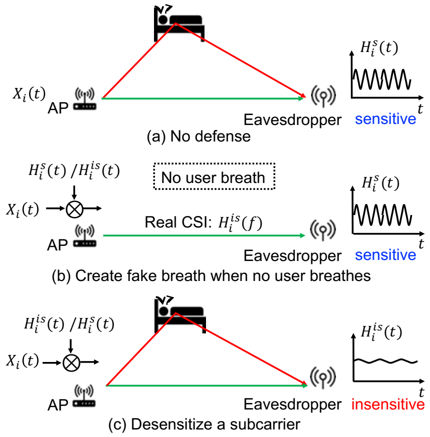
Vital signs inference via wireless signals has drawn increasing attention because of the ubiquitous deployment of wireless infrastructures and the elimination of body contact with devices [1,3,10,28,29,38,36,41,62,64,56,57]. With such a technique, an eavesdropper can stealthily set up a wireless receiver 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 respiration-induced chest and stomach fluctuation may cause subtle disturbances in the received signals, which can be analyzed by the eavesdropper to learn sensitive vital signs.

The popularity of such techniques also brings privacy concerns as vital signs often contain sensitive information related to the state of personal essential body function [1,22,36,38,60]. Generally, the normal breathing rate for an adult at rest is 12 to 20 breaths per minute (bpm). Rapid, shallow breathing is often related to pulmonary diseases [11], hypertension or hyperthyroidism [7]; slow breathing may be caused by heart problems or drug overdose [20]; shortness of breath can be a symptom of diseases such as asthma or pneumonia [53]; sleep apnea is often associated with cardiovascular diseases like stroke [22]. The disclosure of such health information can cause serious consequences such as employment discrimination based on health status [32], and a company's stock plummeting due to its CEO's health concerns [16,15]. Except for health information, there are also extensive research efforts that detect breathing for user presence identification [61,43,39,55], which can result in serious security issues. An adversary (e.g., a burglary) can infer whether users are at home or not by eavesdropping on wireless signals and then may target rooms without the user's presence to commit crimes to reduce the chance of getting caught.

Though research is booming in vital signs 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 [48], 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., [26,47]) 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 steal the secret key via social engineering methods (e.g., [31]) or side-channel attacks (e.g., [23]). Also, it has been shown that an attacker equipped with multiple antennas is able to separate the message from the jamming signals [50]. Due to the importance of health privacy, a more effective defense is thus much-needed to prevent wireless vital signs 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 chest and stomach fluctuation 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 breathing and has shown the best performance in inferring breathing rate compared with other wireless techniques [28].

What if we actively feed the eavesdropper with a meaningful but bogus breathing rate? When the eavesdropper is misled by the fake breathing rate, she would not take further methods to compromise the true one. In this paper, we thus develop a novel scheme against CSI-based vital signs inference techniques. Specifically, we set up an *ambush location*, choose a fake breathing rate, and convert it into a fake CSI. The transmitter then delivers the converted CSI



(a) No defense

(b) Create fake breath when no user breathes

(c) Desensitize a subcarrier

Fig. 1: Creating a fake (sensitive or insensitive) 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 with the estimated CSI.

Generally, as the reflected and line-of-sight (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 movement, sensitive subcarriers enable the receiver to observe large amplitudes (or variances), while insensitive subcarriers rarely show correlated fluctuations. Thus, the breathing rate can be determined via observations of sensitive subcarriers.

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., subcarrier CSI) from the received, distorted copy $Y_i(t)$, i.e., $H_i(t) = \frac{Y_i(t)}{X_i(t)}$ [25,12]. If no defense 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 breath 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. Thus, 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 $H_i^{is}(t)$ (insensitive), causing failure of inferring the true breathing rate.

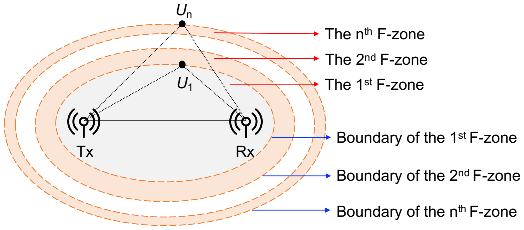

U_n
U_1
Tx
Rx
The nth F-zone
The 2nd F-zone
The 1st F-zone
Boundary of the 1st F-zone
Boundary of the 2nd F-zone
Boundary of the nth F-zone

Fig. 2: Demonstration of Fresnel Zones.

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. We summarize our main contributions as follows:

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

2 Preliminaries

In this section, we impart preliminary knowledge about the Fresnel Zone model and the general method used by existing work using CSI to infer breathing rates.

2.1 Fresnel Zone

In the context of wireless signal propagation, Fresnel Zones refer to concentric ellipses with the transmitter (Tx) and receiver (Rx) at two focal points, and denote regions of different wireless signal propagation strengths between the pair of communicators, as shown in Figure 2. For a given radio wavelength λ, each ellipse can be constructed by ensuring

$$|\mathrm{Tx}, U_n| + |\mathrm{Rx}, U_n| - |\mathrm{Tx}, \mathrm{Rx}| = n\lambda/2, \tag{1}$$

where U_n is a point in the n^{th} ellipse, and $|u, v|$ denotes the Euclidean distance between two points u and v. The innermost ellipse is the first Fresnel Zone, representing the region where the LOS signals can pass through. The n^{th} (when $n \geq 2$) Fresnel Zone is the region between the $(n-1)^{\mathrm{th}}$ and n^{th} ellipses.

The received signal at Rx is a linear combination of reflected and LOS signals. The distance difference ΔD (i.e., $n\lambda/2$) between the two paths generates a phase difference of $\frac{\Delta D}{\lambda} \cdot 2\pi = n\pi$ between the two signals. As the phase shift introduced by the reflection is π [56], the total phase difference $\Delta\phi$ between reflected and LOS signals equals $(n+1)\pi$. Thus, if n is even, we obtain $\Delta\phi \bmod 2\pi = \pi$, causing the two signals to arrive at Rx to have opposite phases and destructively interfere with each other. In contrast, we have $\Delta\phi \bmod 2\pi = 0$ if n is odd, i.e., both signals have the same phase and constructively interfere with each other to form a boosted signal. The Fresnel Zone model can thus help reveal the signal change pattern (i.e., sensitive or insensitive) in each subcarrier (with different waveforms) caused by respiration-induced body movement [56].

2.2 CSI-based Breathing Rate Inference

Existing CSI-based breathing rate inference schemes [36,56,28] 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 then extracted as the breathing cycle, with which, the breathing rate can be calculated.

3 Attack Model and Assumptions

We consider a general scenario, where an attacker only uses a wireless receiver to launch a breathing rate inference attack, as she has a preference to take advantage of an existing wireless transmitter to make the attack stealthier [36]. The transmitter (i.e., defender) is benign and aims to hide true breathing rates and inject fake ones into the eavesdropper.

We assume that the receiver (i.e., attacker) attempts to find a position that enables her to eavesdrop on the breathing rate, which is a common strategy [4]. 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 between itself and an ambush location. This can be achieved by estimating the CSI from wireless signals emitted by a helper node placed at the ambush location.

4 Ambush Design

4.1 Overview

To lay an ambush, the transmitter first selects an ambush location and arbitrarily specifies a fake breathing rate to fool the attacker entering the ambush.

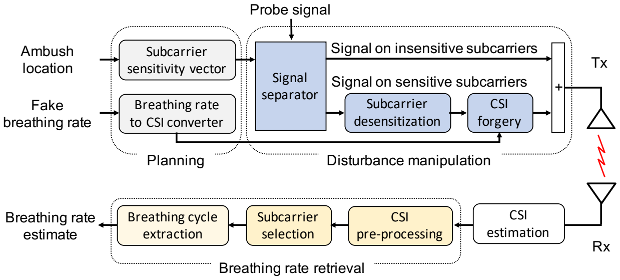


Fig. 3: Flow chart of the proposed ambush tactic.

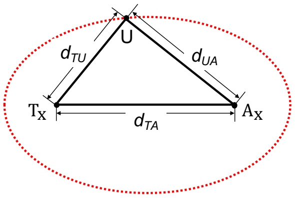


Fig. 4: Selecting an ambush location.

The locations where an eavesdropper may appear with the highest probabilities can be determined via eavesdropper tracking techniques (e.g., [9]) and ambush locations can be then deployed along the eavesdropper's possible route.

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 applies a module of desensitizing subcarriers to remove the real impact of corresponding wireless sub-channels, and also crafts the artificial disturbance on these originally sensitive subcarriers for the attacker to observe. 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 infers breathing rate with estimated CSI by performing the general *breathing rate retrieval* process. Figure 3 shows the flow chart of the proposed ambush tactic.

4.2 Planning Phase

Obtaining Subcarrier Sensitivity As shown in Figure 4, T_x, U, and 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 $[0, 2\pi)$, i.e., $\Delta\theta_i' = \Delta\theta_i \pmod{2\pi}$.

Based on the Fresnel Zone theory [56], 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 the floor function, representing the largest integer less than or equal to x.

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 [36,38,56]. 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 [46], most studies only use the amplitude to characterize the wireless channel [54] and extract breathing rate [36,38,56]. 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

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

where a, β, m and $\mathcal{N}_0$ are the amplitude, initial phase, constant shift (which defines a mean level) of the sinusoidal wave, and the additive noise. In turn, with such a CSI envelope, the attacker can infer the breathing rate as $60 \cdot f_b$.

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.

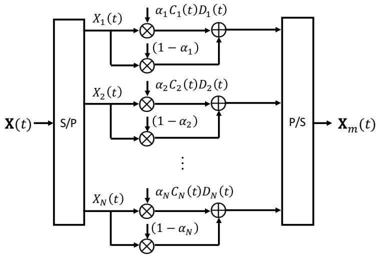


Fig. 5: An MAC process.

4.3 Disturbance Manipulation

The transmitter can utilize a multiply-accumulate (MAC) process to generate desired artificial disturbance, as shown in Figure 5. 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, so that the real respiration-induced channel disturbance (i.e., the real breathing rate) can be hidden for the attacker. 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 for the attacker to estimate, 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

$$\mathbf{X}_m(t) = \text{diag}(\mathbf{D}(t)) \cdot \text{diag}(\mathbf{C}(t)) \cdot \mathbf{S}(t) + \mathbf{IS}(t). \tag{3}$$

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

$$\begin{aligned} \hat{H}_i(t) &= \alpha_i \cdot \frac{X_i(t) C_i(t) D_i(t)}{X_i(t)} \cdot H_i(t) + (1-\alpha_i) \cdot H_i(t) \\ &= \alpha_i \cdot D_i(t) + (1-\alpha_i) \cdot H_i(t) = W_i(t). \end{aligned} \tag{4}$$

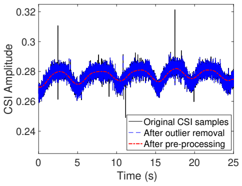


Fig. 6: CSI pre-processing.

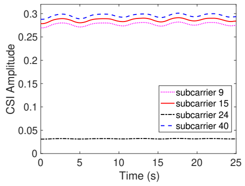


Fig. 7: Subcarrier sensitivity.

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 in the planning phase. 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 $H_i(t)$. This is because the transmitter does not manipulate signals on insensitive subcarriers.

4.4 Breathing Rate Retrieval

CSI Pre-processing CSI pre-processing, consisting of outlier removal and noise reduction, aims to make the collected CSI reliable. The imperfect CSI can be caused by non-respiratory environmental change or hardware imperfections.

Hampel filter is a classical technique to remove outliers (i.e., samples that significantly differ from neighboring ones) in a given series [13,38]. As the collected CSI may have abrupt changes that are not caused by respiration, a Hampel filter is enforced to remove those outliers. It is observed that the CSI variations caused by the chest and stomach movement usually lie at the low end of the spectrum. Thus, we further adopt the moving average filter, which is optimal for reducing high-frequency noise while retaining a sharp step response [49]. Figure 6 illustrates an example of CSI pre-processing. It can be seen that the outliers and high-frequency noise are effectively removed.

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 to determine the sensitivity of each subcarrier. 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 variance is caused by noise and the subcarrier is insensitive; otherwise, this subcarrier is sensitive. If CSI variances on all subcarriers have the same order with the reference variance, all subcarriers are insensitive (i.e., no breathing activity is detected).

Figure 7 plots the CSIs observed on 4 different subcarriers. In this example, we can see that subcarrier 24 has a quite flat CSI which rarely discloses any useful information about the breathing activity, while the CSIs of the remaining

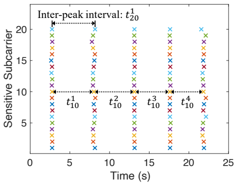


Fig. 8: Local peaks.

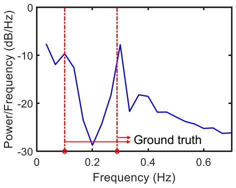


Fig. 9: Peaks in PSD.

subcarriers show evident periodical fluctuations. Accordingly, we can determine that subcarriers 9, 15, and 40 are sensitive, while subcarrier 24 is insensitive.

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 (i.e., the time between successive peaks) 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 between the current peak with the previous one 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.

Figure 8 shows all detected local peaks on 20 sensitive subcarriers during 25 seconds. The breathing rate is calculated as 12.7 bpm for this example.

Inferring Multi-user Breathing Rates For the multi-user scenario, we use the power spectral density (PSD) [36] to identify the frequencies with strong signal power in the frequency domain. Normally, each breathing signal from one person contributes to one evident peak in the obtained PSD [55]. The PSD on the i^{th} sensitive subcarrier with L samples can be obtained by $PSD_i = 10\log_{10}\frac{|FFT(H_i)|^2}{L}$, where H_i is the vector of CSI amplitude on the i^{th} subcarrier.

When there are two users, the two strongest peaks in the PSD would indicate their breathing rates, as in an example shown in Figure 9. The ground truths of two users' breathing rates are 6.0 and 17.3 bpm (corresponding to 0.10 ad 0.29 Hz); the estimated breathing rates based on the first two strongest peaks are 6.0 and 18.0 bpm (i.e., 0.10 and 0.30 Hz), showing that the estimation of two-user breathing rates is accurate.

4.5 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 of which searches for opportune eavesdropping locations.

Setting up Two Ambush Locations The transmitter with two antennas can set up two ambush locations. Let $\mathbf{H}_{sr}(t)$ $(s,\ r \in \{1,2\})$ denote the overall CSI between the s^{th} transmit antenna and the r^{th} ambush location. The corresponding subcarrier sensitivity vector is represented by $\boldsymbol{\alpha}_{sr} = [\alpha_{sr}^1, \cdots, \alpha_{sr}^N]$, which can be pre-obtained with the method proposed in Section 4.2. At each ambush location, the received signal is the superposition of two signals, each from a different transmit antenna. If at least one of the two subcarriers between the respective transmit antenna and the r^{th} ambush location is sensitive, we regard that this overall subcarrier between the transmitter and the r^{th} ambush location is sensitive. Mathematically, let $\boldsymbol{\alpha}_r = [\alpha_r^1, \cdots, \alpha_r^N]$ denote the resultant subcarrier sensitivity vector of the transmitter for the r^{th} ambush location, and $\alpha_r^i = \alpha_{1r}^i \vee \alpha_{2r}^i$. On the other hand, it may arouse suspicion of two colluding eavesdroppers if the breathing rates they infer separately are different. Thus, the transmitter should enable both ambush locations to observe the same breathing rate, i.e., the manipulated CSIs at corresponding sensitive subcarriers should be equal. If a subcarrier at either ambush location is sensitive, we then regard that the overall subcarrier between the transmitter and the two ambush locations is sensitive. Similarly, let $\boldsymbol{\alpha} = [\alpha^1, \cdots, \alpha^N]$ denote the subcarrier sensitivity vector of the transmitter for the two ambush locations, and $\alpha^i = \alpha_1^i \vee \alpha_2^i$.

Let $W(t)$ denote the fake CSI which is converted with a specified breathing rate. The transmitter aims to make the estimated CSI on sensitive subcarriers at each eavesdropper to be equal to $W(t)$.

As discussed in Section 4.3, the transmitting signals on sensitive subcarriers will be first desensitized and then multiply with the forged CSI before being sent out. In this scenario, let $H_{sr}^i(t)$ denote the CSI on i^{th} subcarrier between the s^{th} transmit antenna and the r^{th} ambush location. Thus, in terms of the coefficient vector $\mathbf{C}_s(t) = [C_s^1(t), \cdots, C_s^N(t)]$ for subcarrier desensitization at the s^{th} transmit antenna, if $\alpha^i = 0$ (i.e., the i^{th} subcarrier between the transmitter and the two ambush locations is insensitive), we set $C_s^i(t) = 0$, otherwise, we have $C_1^i(t) = \frac{H_{21}^i(t) - H_{22}^i(t)}{\zeta^i}$ and $C_2^i(t) = \frac{H_{12}^i(t) - H_{11}^i(t)}{\zeta^i}$, where $\zeta^i = H_{21}^i(t)H_{12}^i(t) - H_{22}^i(t)H_{11}^i(t)$. Also, the coefficient vector for the CSI forgery module at each transmit 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 $D_i(t) = W(t)$ if $\alpha^i = 1$.

We rewrite Equation 3 and the transmitting signal $\mathbf{X}_m(t) = [\mathbf{X}_1(t), \mathbf{X}_2(t)]^T$ after manipulation becomes

$$\mathbf{X}_m(t) = \begin{bmatrix} \text{diag}(\mathbf{D}(t)) \cdot \text{diag}(\mathbf{C}_1(t)) \cdot \mathbf{S}(t) + \mathbf{IS}(t) \\ \text{diag}(\mathbf{D}(t)) \cdot \text{diag}(\mathbf{C}_2(t)) \cdot \mathbf{S}(t) + \mathbf{IS}(t) \end{bmatrix}. \tag{5}$$

The transmitting signal $\mathbf{X}_m(t)$ would go through the realistic wireless channel. At the ambush location side, the received signal and the public training sequence will be then utilized to estimate CSI. Let $\hat{\mathbf{W}}_1(t)$ and $\hat{\mathbf{W}}_2(t)$ denote the estimated

CSIs at the two ambush locations. We thus obtain

$$\hat{W}_r^i(t) = \alpha^i \cdot W(t) + (1 - \alpha^i) \cdot (H_{1r}^i(t) + H_{2r}^i(t)). \tag{6}$$

This implies the success of setting up two ambush locations simultaneously.

General Scheme for Area Ambush The transmitter can 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.

The sensitivity of the i^{th} subcarrier between the s^{th} transmit antenna and the r^{th} ambush location can be represented by α_{sr}^i $(s,\ r \in \{1, 2, \cdots, \kappa\})$. 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 $\mathbf{X}(t) = [\mathbf{X}_1(t), \cdots, \mathbf{X}_\kappa(t)]^T$ denote the manipulated signal sent by κ transmit antennas. The transmitter aims to make the estimated CSI at each ambush location be equal to the specified fake CSI, i.e., $\hat{\mathbf{W}}_r(t) = \mathbf{W}(t)$. Similarly, each transmit 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 5 as

$$\mathbf{X}_m(t) = \begin{bmatrix} \text{diag}(\mathbf{D}(t)) \cdot \text{diag}(\mathbf{C}_1(t)) \cdot \mathbf{S}(t) + \mathbf{IS}(t) \\ \vdots \\ \text{diag}(\mathbf{D}(t)) \cdot \text{diag}(\mathbf{C}_\kappa(t)) \cdot \mathbf{S}(t) + \mathbf{IS}(t) \end{bmatrix}, \tag{7}$$

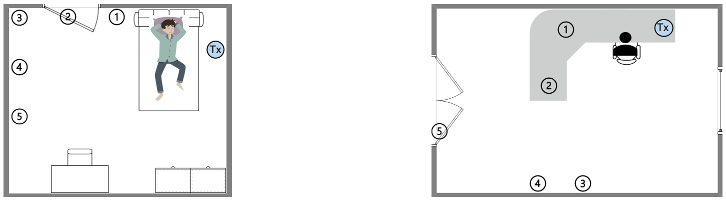
where $\mathbf{C}_s(t)$ is the coefficient vector for the subcarrier desensitization module at the s^{th} transmit antenna.

Equation 7 has κ unknowns ($\mathbf{C}_1(t)$ to $\mathbf{C}_\kappa(t)$). As the number of transmit antennas equals the number of unknowns, the linear system formed by Equation 7 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} transmit antenna with the computed $\mathbf{C}_s(t)$, the goal of deploying κ simultaneous ambush locations can be achieved.

4.6 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).

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 [10]. 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



(a) Bedroom (User lies down).

(b) Office (User sits).

Fig. 10: Layout of the experimental environment.

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.

Indirect Calculation: To calculate the real CSI, an eavesdropper must compromise the phase of distribution manipulation. As shown in Section 4.3, 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 $R_i^e = X_i^m(t) H_i^e(t) = a_i M_i(t) X_i(t) H_i^e(t) + (1 - a_i) X_i(t) H_i^e(t)$.

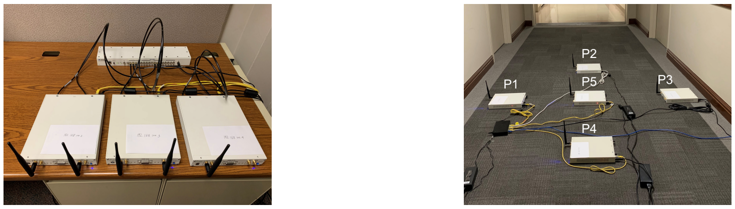
To learn $M_i(t)$, the eavesdropper must learn both a_i and $H_i^e(t)$. However, this imposes a strong requirement for the eavesdropper. On one hand, without the knowledge of the accurate positions of the target user and the transmitter, the eavesdropper can hardly determine the subcarrier sensitivity 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.

5 Experimental Evaluation

We implement CSI-based breathing rate inference and our proposed ambush schemes on top of Universal Software Radio Peripheral (USRP) X310s [19], which are equipped with SBX-120 daughterboards [18] and run GNU Radio [24] – an open-source software toolkit.

5.1 Evaluation Setup

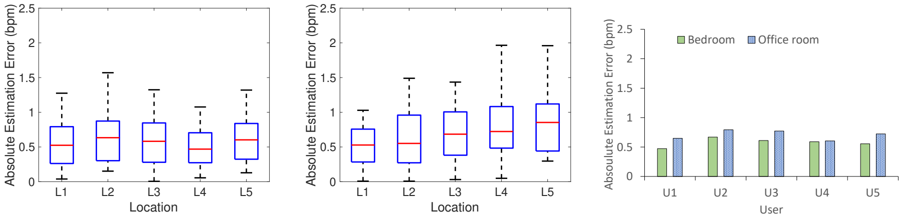
The prototype system includes a transmitter Tx and an eavesdropper Eve (i.e., malicious receiver). Each node is a USRP X310. We recruited 5 participants and asked each to act as the target user of the inference attacks over three



(a) Five-antenna transmitter with USRPs.

(b) Ambush area.

Fig. 11: Setup for deploying an ambush area.



(a) In the bedroom.

(b) In the office room.

(c) Mean value of ϵ.

Fig. 12: Values of ϵ and ϵ at Eve when no defense is enforced.

months.[1] Also, each wore a Masimo MightySat Fingertip Pulse Oximeter [40] with hospital-grade technology to obtain ground-truth breathing rate.

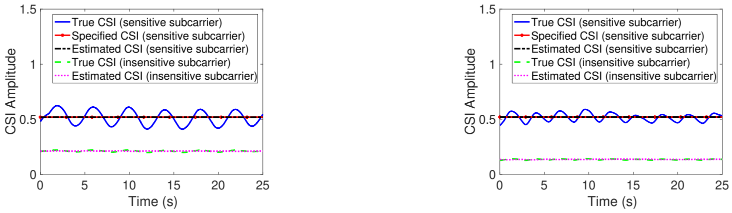
Testing Scenarios: We test two typical scenarios: (1) a bedroom, where the user lies on a bed; and (2) an office room, where the user sits in a chair. Figure 10 shows the ambush locations and the position of the transmitter. For each scenario, we place Eve at 5 different ambush locations to infer the user's breathing rate, and the transmitter launches the proposed ambush scheme.

To deploy a trap area, as shown in Figure 11a, 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 [17]. As shown in Figure 11b, 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.

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.

[1] The study has been approved by our institution's IRB.



(a) In the bedroom.

(b) In the office room.

Fig. 13: Enabling Eve to obtain no breathing activity.

5.2 Breathing Rate Inference Attacks

We first verify the effectiveness of using CSI to infer breathing rates. As shown in Figure 10, Eve is put at each ambush location in both of the two scenarios to estimate each participant's breathing rate, with 100 trials performed for every estimate. Figure 12 shows the obtained absolute estimation error when the proposed ambush scheme is not launched.

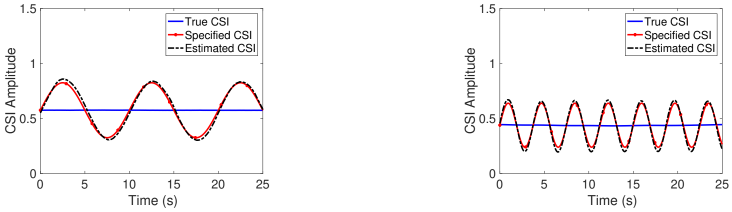
Figure 12a shows that the inference technique always achieves high accuracy with less than 1.6 bpm of error at all locations in the bedroom. The median absolute estimation error ranges from 0.4 to 0.6 bpm across all locations. Meanwhile, we see the value of ϵ on average is slightly larger at Location 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 12b. Figure 12c 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 convincingly that an eavesdropper could utilize passively collected CSI to accurately infer a person's breathing rate in different scenarios.

5.3 Example Defenses

We examine three example defenses, in which we deploy the ambush location at Location 1 shown in Figure 10a and Location 3 shown in Figure 10b.

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).

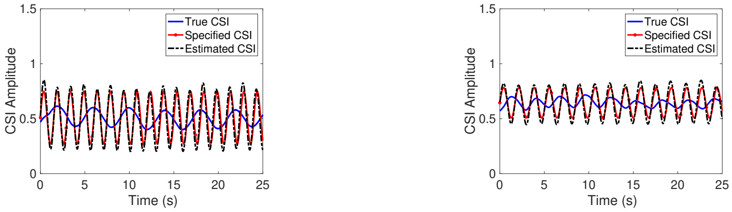
Figure 13 plots the real CSIs between the transmitter and the ambush location, the estimated CSIs at the ambush location, as well as the subcarrier CSI specified by the transmitter. In both environments, the transmitter can make Eve observe a CSI on a sensitive subcarrier significantly near to the specified one while both greatly deviate from the true one; with the estimated CSI, Eve



(a) In the bedroom.

(b) In the office room.

Fig. 14: Fabricating normal breath.



(a) In the bedroom.

(b) In the office room.

Fig. 15: Making Eve obtain abnormal breath.

obtains a breathing rate of 0 though the respective true breathing rates are 15.1 and 20.8 bpm. The absolute estimation errors in the bedroom and the office room are thus 15.1 and 20.8 bpm, while the corresponding absolute ambush errors are both 0. Besides, the CSI of the insensitive subcarrier keeps insensitive with the defense (we thus only focus on sensitive subcarriers in the later evaluation).

Example 2 - Fabricating Nonexistent Breath: We aim to make Eve obtain a fake breathing rate while there is no breathing activity in both scenarios. We specify a fake breathing rate of 6 (16) bpm for the bedroom (office) room.

As shown in Figure 14, 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 in the bedroom and 16.1 bpm in the office room. The absolute estimation errors in the two scenarios become 6.4 and 16.1 bpm, respectively; the respective absolute ambush errors are as small as 0.4 bpm and 0.1 bpm.

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 for the bedroom and 35 bpm for the office room.

Similar to the above examples, we observe from Figure 15 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 of Eve in the bedroom becomes 40.2 bpm, instead of the true one (i.e., 19.9 bpm) derived from the Masimo Oximeter. In the office room, Eve obtains a breathing rate of 35.2 bpm, instead of the ground truth (i.e., 17.0 bpm). Therefore, the absolute estimation errors

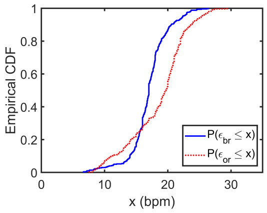


Fig. 16: CDFs of $P(\epsilon \leq x)$ for **D1**.

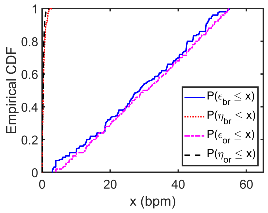


Fig. 17: CDFs of $P(\epsilon \leq x)$ and $P(\eta \leq x)$ for **D2**.

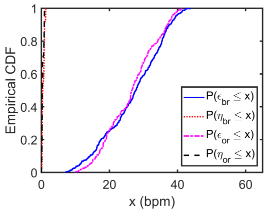
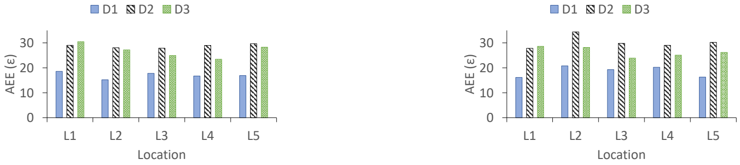


Fig. 18: CDFs of $P(\epsilon \leq x)$ and $P(\eta \leq x)$ for **D3**.



(a) In the bedroom.

(b) In the office room.

Fig. 19: Mean absolute estimation errors (AEE).

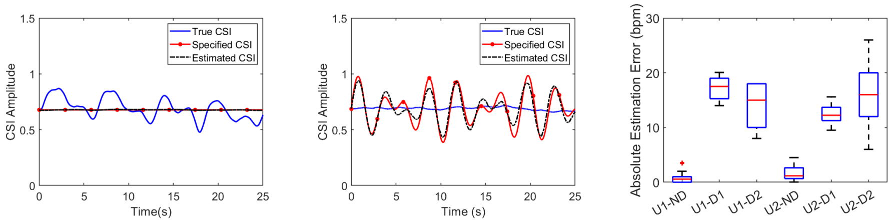
for the bedroom and the office room are 20.3 bpm and 18.2 bpm, respectively, while the absolute ambush errors in these two scenarios are both just 0.2 bpm.

5.4 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.

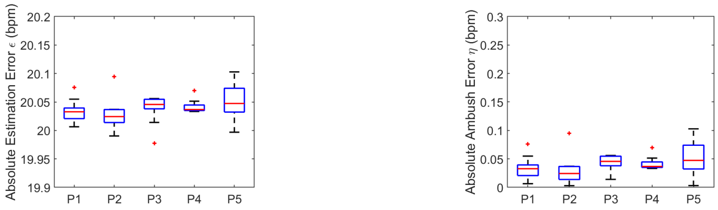
D1: We test when the user has different breathing rates in the range of 6-27 bpm. For all trials, we find that Eve always obtains an estimated breathing rate of 0, indicating the consistent success of the defense. Let $P(\epsilon_{br} \leq x)$ and $P(\epsilon_{or} \leq x)$ denote the empirical cumulative distribution functions (CDFs) of the absolute estimation error ϵ_{br} for the bedroom and ϵ_{or} for the office room. Figure 16 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 17, 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%.



(a) Canceling two-user breath. **(b)** Creating two-user breath. **(c)** Comparison of ϵ.

Fig. 20: Extending defenses in two-user scenario.



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

Fig. 21: Fabricating normal breath for a trap area.

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 18 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 19a and 19b 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.

5.5 Two-user Scenario

First, we aim to make two persons' breathing unobservable (referred to as **D1**). We consider the scenario when two participants are in the office room simultaneously. As shown in Figure 20a, the estimated CSI is quite close to the specified one while both deviate from the true CSI. Consequently, Eve obtains a breathing rate of 0 though the true breathing rates of the two users are 6.0 and 10.0 bpm, respectively. Second, we aim to make Eve observe two specified breathing rates (16 and 22 bpm) when there is no breathing activity (referred to as **D2**). As shown in Figure 20b, though the true CSI is almost flat, indicating no person in the room, the estimated CSI and the specified one are alike, leading Eve to obtain two-person breathing rates of 16.0 and 22.1 bpm.

We repeat the above two experiments 40 times. For comparison, we also perform 40 attempts of inferring two-person breathing rates when no defense is applied (this case is denoted with **ND**). Figure 20c presents the absolute estimation errors (ϵ) for the cases with two real or fake users (U1 and U2). Without the defenses, the mean value of ϵ is quite small (around 0.8 bpm); while it is significantly increased (within the range of 12.6-17.2 bpm) with the proposed defenses (D1 and D2). Also, for D1, the mean values of the absolute ambush error η for the two users both equal about 0, while for D2, they are 0.1 and 0.4 bpm. These results convincingly show the proposed scheme can successfully mislead Eve with specified breathing rates for the two-user scenario.

5.6 Trap Area Evaluation

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 11b. 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.

Figure 21a shows that the absolute estimation errors at all ambush points are consistently large (close to 20 bpm). Figure 21b 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 to trap a single eavesdropper) with fake breathing rates.

6 Related Work

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 [52,45,28]. UWB transmissions, however, spread over a large frequency bandwidth [21]. Also, the receiver structure for UWB is highly complex [33].

Doppler radar based: Doppler radar systems have been proposed to achieve breathing detection [34,14,6,35,44]. 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 [8]. 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 [63,27,35].

Frequency Modulated Continuous Wave (FMCW) radar based: An FMCW radar has also been utilized for breathing rate inference [3,51,5]. 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 $\frac{C}{2B}$ [2], 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 [30,42,41,1]. For example, [1] 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 channel information, 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 [37,38,58,36,56,59,65]. In particular, a recent empirical study [28] reveals CSI provides the most robust estimates of breathing rate compared with UWB radar or RSS.

7 Conclusion

Wireless signal has demonstrated exceptional capability to detect breathing activity, which introduces a new threat to the security of personal health 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. This scheme enables the transmitter to encode the specified fake breathing rate 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.

Acknowledgments

We would like to thank our anonymous reviewers for their insightful comments and feedback. This work was supported in part by NSF under Grants No.1948547.

References

1. Abdelnasser, H., Harras, K.A., Youssef, M.: Ubibreathe: A ubiquitous non-invasive WiFi-based breathing estimator. In: Proc. of ACM International Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc). p. 277–286 (2015)
2. Adib, F., Kabelac, Z., Katabi, D., Miller, R.C.: 3d tracking via body radio reflections. In: 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14). pp. 317–329. USENIX Association, Seattle, WA (Apr 2014)
3. Adib, F., Mao, H., Kabelac, Z., Katabi, D., Miller, R.C.: Smart homes that monitor breathing and heart rate. In: Proc. of ACM Conference on Human Factors in Computing Systems (CHI). p. 837–846 (2015)
4. Anand, N., Sung-Ju Lee, Knightly, E.W.: Strobe: Actively securing wireless communications using zero-forcing beamforming. In: 2012 Proc. IEEE INFOCOM. pp. 720–728 (March 2012)

5. Anitori, L., de Jong, A., Nennie, F.: Fmcw radar for life-sign detection. In: 2009 IEEE Radar Conference. pp. 1–6 (2009)
6. Ascione, M., Buonanno, A., D'Urso, M., Angrisani, L., Schiano Lo Moriello, R.: A new measurement method based on music algorithm for through-the-wall detection of life signs. IEEE Transactions on Instrumentation and Measurement **62**(1), 13–26 (2013)
7. BJ, C., 3rd: Treatment of heart failure in infants and children. Heart Disease **2**(5), 354–361 (2000)
8. Boric-Lubecke, O., Lubecke, V.M., Droitcour, A.D., Park, B.K., Singh, A.: Doppler radar physiological sensing. Wiley Online Library (2016)
9. Chaman, A., Wang, J., Sun, J., Hassanieh, H., Roy Choudhury, R.: Ghostbuster: Detecting the presence of hidden eavesdroppers. In: Proc. of the 24th Annual International Conference on Mobile Computing and Networking. p. 337–351. MobiCom '18, Association for Computing Machinery, New York, NY, USA (2018)
10. Chen, L., Xiong, J., Chen, X., Lee, S.I., Zhang, D., Yan, T., Fang, D.: Lungtrack: Towards contactless and zero dead-zone respiration monitoring with commodity rfids. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. **3**(3), 79:1–79:22 (Sep 2019)
11. Cox, R.A., Torres, C.Z.: Acute heart failure in adults. Puerto Rico Health Sciences Journal **23**(4), 265–271 (2004)
12. Crepaldi, R., Jeongkeun Lee, Etkin, R., Sung-Ju Lee, Kravets, R.: Csi-sf: Estimating wireless channel state using csi sampling fusion. In: 2012 Proc. IEEE INFOCOM. pp. 154–162 (2012)
13. Davies, L., Gather, U.: The identification of multiple outliers. Journal of the American Statistical Association **88**(423), 782–792 (1993)
14. Droitcour, A.D., Boric-Lubecke, O., Kovacs, G.T.A.: Signal-to-noise ratio in doppler radar system for heart and respiratory rate measurements. IEEE Transactions on Microwave Theory and Techniques **57**(10), 2498–2507 (2009)
15. Duggan, W.: CSX stock plummets on CEO's health concerns. US News (Dec 2017), https://money.usnews.com/investing/stock-market-news/articles/2017-12-15/csx-corporation-stock-plummets-on-ceos-health-concerns
16. Ellyatt, H.: How CEO health can affect your wealth. CNBC (Sep 2012), https://www.cnbc.com/id/49115208
17. Ettus, M.: Usrp users and developers guide. www. olifantasia. com/gnuradio/usrp/files/usrp_guide. pdf (2005)
18. Ettus Research: SBX 400-4400 MHz Rx/Tx (2022), https://www.ettus.com/all-products/sbx120/
19. Ettus Research: USRP X310 (2022), https://www.ettus.com/all-products/x310-kit/
20. Fan, D., Ren, A., Zhao, N., Yang, X., Zhang, Z., Shah, S.A., Hu, F., Abbasi, Q.H.: Breathing rhythm analysis in body centric networks. IEEE Access **6**, 32507–32513 (2018)
21. Federal Communications Commission and others: Revision of part 15 of the commission's rules regarding ultra-wideband transmission systems. First Report and Order, FCC 02-48 (2002)
22. Fekr, A.R., Janidarmian, M., Radecka, K., Zilic, Z.: Respiration disorders classification with informative features for m-health applications. IEEE Journal of Biomedical and Health Informatics **20**(3), 733–747 (May 2016)
23. Genkin, D., Pachmanov, L., Pipman, I., Tromer, E.: Stealing keys from pcs using a radio: Cheap electromagnetic attacks on windowed exponentiation. In: Güneysu,

T., Handschuh, H. (eds.) Cryptographic Hardware and Embedded Systems – CHES 2015. pp. 207–228. Springer Berlin Heidelberg, Berlin, Heidelberg (2015)

24. GNU Radio project: GNU Radio - the free & open source radio ecosystem (2022), https://www.gnuradio.org
25. Goldsmith, A.: Wireless Communications. Cambridge University Press, New York, NY, USA (2005)
26. Gollakota, S., Katabi, D.: Physical layer wireless security made fast and channel independent. In: 2011 Proc. IEEE INFOCOM. pp. 1125–1133 (April 2011)
27. Gu, C.: Short-range noncontact sensors for healthcare and other emerging applications: A review. Sensors **16**(8), 1169 (2016)
28. Hillyard, P., Luong, A., Abrar, A.S., Patwari, N., Sundar, K., Farney, R., Burch, J., Porucznik, C., Pollard, S.H.: Experience: Cross-technology radio respiratory monitoring performance study. In: Proc. of the 24th Annual International Conference on Mobile Computing and Networking. p. 487–496. MobiCom '18, Association for Computing Machinery, New York, NY, USA (2018)
29. Jia, W., Peng, H., Ruan, N., Tang, Z., Zhao, W.: WiFind: Driver fatigue detection with fine-grained wi-fi signal features. IEEE Transactions on Big Data **6**(2), 269–282 (2020)
30. Kaltiokallio, O., Yiğitler, H., Jäntti, R., Patwari, N.: Non-invasive respiration rate monitoring using a single cots tx-rx pair. In: Proc. of the 13th International Symp. on Information Processing in Sensor Networks (IPSN). pp. 59–69 (2014)
31. Krombholz, K., Hobel, H., Huber, M., Weippl, E.: Advanced social engineering attacks. Journal of Information Security and Applications **22**, 113 – 122 (2015), special Issue on Security of Information and Networks
32. Lafky, D.B., Horan, T.A.: Personal health records: Consumer attitudes toward privacy and security of their personal health information. Health Informatics Journal **17**(1), 63–71 (2011)
33. Lampe, L., Witrisal, K.: Challenges and recent advances in ir-uwb system design. In: Proc. of 2010 IEEE International Symposium on Circuits and Systems. pp. 3288–3291 (2010)
34. Li, C., Ling, J., Li, J., Lin, J.: Accurate doppler radar noncontact vital sign detection using the relax algorithm. IEEE Transactions on Instrumentation and Measurement **59**(3), 687–695 (2010)
35. Li, C., Lubecke, V.M., Boric-Lubecke, O., Lin, J.: A review on recent advances in doppler radar sensors for noncontact healthcare monitoring. IEEE Transactions on Microwave Theory and Techniques **61**(5), 2046–2060 (2013)
36. Liu, J., Wang, Y., Chen, Y., Yang, J., Chen, X., Cheng, J.: Tracking vital signs during sleep leveraging off-the-shelf WiFi. In: Proc. of ACM International Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc). pp. 267–276 (2015)
37. Liu, X., Cao, J., Tang, S., Wen, J.: Wi-sleep: Contactless sleep monitoring via WiFi signals. In: 2014 IEEE Real-Time Systems Symposium. pp. 346–355 (Dec 2014)
38. Liu, X., Cao, J., Tang, S., Wen, J., Guo, P.: Contactless respiration monitoring via off-the-shelf WiFi devices. IEEE Transactions on Mobile Computing **15**(10), 2466–2479 (Oct 2016)
39. Ma, Y., Zhou, G., Wang, S.: WiFi sensing with channel state information: A survey. ACM Comput. Surv. **52**(3) (jun 2019)
40. Masimo: MightySat fingertip pulse oximeter with bluetooth LE, RRp, & PVi (2021), https://www.masimopersonalhealth.com/products/mightysat-fingertip-pulse-oximeter-with-bluetooth-le-rrp-pvi

41. Patwari, N., Brewer, L., Tate, Q., Kaltiokallio, O., Bocca, M.: Breathfinding: A wireless network that monitors and locates breathing in a home. IEEE Journal of Selected Topics in Signal Processing **8**(1), 30–42 (Feb 2014)
42. Patwari, N., Wilson, J., Ananthanarayanan, S., Kasera, S.K., Westenskow, D.R.: Monitoring breathing via signal strength in wireless networks. IEEE Transactions on Mobile Computing **13**(8), 1774–1786 (Aug 2014)
43. Pradhan, S., Sun, W., Baig, G., Qiu, L.: Combating replay attacks against voice assistants. Proc. of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies **3**(3), 1–26 (2019)
44. Rahman, T., Adams, A.T., Ravichandran, R.V., Zhang, M., Patel, S.N., Kientz, J.A., Choudhury, T.: Dopplesleep: A contactless unobtrusive sleep sensing system using short-range doppler radar. In: Proc. of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing. p. 39–50. UbiComp '15, Association for Computing Machinery, New York, NY, USA (2015)
45. Salmi, J., Molisch, A.F.: Propagation parameter estimation, modeling and measurements for ultrawideband mimo radar. IEEE Transactions on Antennas and Propagation **59**(11), 4257–4267 (2011)
46. Sen, S., Radunovic, B., Choudhury, R.R., Minka, T.: You are facing the mona lisa: Spot localization using phy layer information. In: Proc. of the 10th International Conference on Mobile Systems, Applications, and Services. p. 183–196. MobiSys '12, Association for Computing Machinery, New York, NY, USA (2012)
47. Shen, W., Ning, P., He, X., Dai, H.: Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time. In: 2013 IEEE Symposium on Security and Privacy. pp. 174–188 (May 2013)
48. Shiu, Y.S., Chang, S.Y., Wu, H.C., Huang, S.C.H., Chen, H.H.: Physical layer security in wireless networks: a tutorial. IEEE Wireless Communications **18**(2), 66–74 (April 2011)
49. Smith, S.W., et al.: The scientist and engineer's guide to digital signal processing. California Technical Pub. San Diego (1997)
50. Tippenhauer, N.O., Malisa, L., Ranganathan, A., Capkun, S.: On limitations of friendly jamming for confidentiality. In: Proc. of the 2013 IEEE Symposium on Security and Privacy. p. 160–173. SP '13, IEEE Computer Society, USA (2013)
51. Van Loon, K., Breteler, M., Van Wolfwinkel, L., Leyssius, A.R., Kossen, S., Kalkman, C., van Zaane, B., Peelen, L.: Wireless non-invasive continuous respiratory monitoring with fmcw radar: a clinical validation study. Journal of clinical monitoring and computing **30**(6), 797–805 (2016)
52. Venkatesh, S., Anderson, C.R., Rivera, N.V., Buehrer, R.M.: Implementation and analysis of respiration-rate estimation using impulse-based uwb. In: 2005 IEEE Military Communications Conference (MILCOM). pp. 3314–3320 Vol. 5 (2005)
53. Wahls, S.A.: Causes and evaluation of chronic dyspnea. American family physician **86 2**, 173–82 (2012)
54. Wang, C., Liu, J., Chen, Y., Liu, H., Wang, Y.: Towards in-baggage suspicious object detection using commodity WiFi. In: 2018 IEEE Conference on Communications and Network Security (CNS). pp. 1–9 (2018)
55. Wang, F., Zhang, F., Wu, C., Wang, B., Liu, K.J.R.: Respiration tracking for people counting and recognition. IEEE Internet of Things Journal **7**(6), 5233–5245 (2020)
56. Wang, H., Zhang, D., Ma, J., Wang, Y., Wang, Y., Wu, D., Gu, T., Xie, B.: Human respiration detection with commodity WiFi devices: Do user location and body orientation matter? In: Proc. of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp). pp. 25–36 (2016)

57. Wang, X., Niu, K., Xiong, J., Qian, B., Yao, Z., Lou, T., Zhang, D.: Placement matters: Understanding the effects of device placement for WiFi sensing. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. **6**(1) (2022)
58. Wang, X., Yang, C., Mao, S.: Phasebeat: Exploiting csi phase data for vital sign monitoring with commodity WiFi devices. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). pp. 1230–1239 (June 2017)
59. Wang, X., Yang, C., Mao, S.: Tensorbeat: Tensor decomposition for monitoring multiperson breathing beats with commodity WiFi. ACM Trans. Intell. Syst. Technol. **9**(1) (Sep 2017)
60. Whited, L., Graham, D.D.: Abnormal respirations. StatPearls, Treasure Island, FL, USA (2019), https://www.ncbi.nlm.nih.gov/books/NBK470309/
61. Wu, C., Yang, Z., Zhou, Z., Liu, X., Liu, Y., Cao, J.: Non-invasive detection of moving and stationary human with WiFi. IEEE Journal on Selected Areas in Communications **33**(11), 2329–2342 (2015)
62. Yang, Y., Cao, J., Liu, X., Xing, K.: Multi-person sleeping respiration monitoring with cots WiFi devices. In: 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS). pp. 37–45 (Oct 2018)
63. Yanming Xiao, Lin, J., Boric-Lubecke, O., Lubecke, V.M.: Frequency-tuning technique for remote detection of heartbeat and respiration using low-power double-sideband transmission in the ka-band. IEEE Transactions on Microwave Theory and Techniques **54**(5), 2023–2032 (2006)
64. Zeng, Y., Wu, D., Gao, R., Gu, T., Zhang, D.: Fullbreathe: Full human respiration detection exploiting complementarity of CSI phase and amplitude of WiFi signals. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. **2**(3) (Sep 2018)
65. Zhang, F., Zhang, D., Xiong, J., Wang, H., Niu, K., Jin, B., Wang, Y.: From Fresnel diffraction model to fine-grained human respiration sensing with commodity Wi-Fi devices. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. **2**(1) (Mar 2018)