SoK: Secure Human-centered Wireless Sensing

Wei Sun
Duke University
redsunwit@gmail.com

Tingjun Chen
Duke University
tingjun.chen@duke.edu

Neil Gong
Duke University
zhenqiang.gong@duke.edu

ABSTRACT

Human-centered wireless sensing (HCWS) aims to understand the fine-grained environment and activities of a human using the diverse wireless signals around him/her. While the sensed information about a human can be used for many good purposes such as enhancing life quality, an adversary can also abuse it to steal private information about the human (e.g., location and person's identity). However, the literature lacks a systematic understanding of the privacy vulnerabilities of wireless sensing and the defenses against them, resulting in the privacy-compromising HCWS design.

In this work, we aim to bridge this gap to achieve the vision of secure human-centered wireless sensing. First, we propose a signal processing pipeline to identify private information leakage and further understand the benefits and tradeoffs of wireless sensing-based inference attacks and defenses. Based on this framework, we present the taxonomy of existing inference attacks and defenses. As a result, we can identify the open challenges and gaps in achieving privacy-preserving human-centered wireless sensing in the era of machine learning and further propose directions for future research in this field.

KEYWORDS

Human-centered wireless sensing, Inference attacks and defenses, Privacy enhancement

1 INTRODUCTION

Wireless sensing is an emerging enabling technology for many applications such as smart homes/cities, autonomous systems, and human-computer interactions. Given the advanced wireless communication techniques (*e.g.*, WiFi, and 5G) and the proliferation of wireless devices (*e.g.*, Internet-of-Things), wireless sensing is becoming more and more popular. Wireless signals in different forms, including *radio frequency (RF)* and *light*, interact with human bodies and other physical objects in the environment during transmission. As a result, the variation of the wireless signals around a human can be leveraged to understand the physical environment and human activities in it [9, 134, 142, 178]. For instance, Vasisht et al. [134] shows that wireless signals can be used to localize and identify occupants at home based on their walking patterns, thereby enabling a smart home that is aware of the occupants' locations and identities to personalize appliance settings.

Like nearly any advanced technology, wireless sensing is a double-edged sword. On the one hand, wireless sensing enables many life-quality-improving applications such as health status monitoring [3, 37, 40], energy-efficient smart home [27, 102, 134], and friendly human-computer interaction [80, 142] via understanding the physical environment and activities of human subjects. On the other hand, the same technology can be abused by an attacker to infer a human's private information such as location, living habits, and behavioral biometric characteristics (*e.g.*, walking pattern, heart rate, and hand gesture) that can identify a person, therefore leading to privacy and security risks. For instance, inferring location leads to location privacy leakage [134, 141]; inferring living habits may lead to well-planned burglary [121, 178]; and inferring hand gesture used to unlock a smartphone leads to password compromise [11, 66].

However, the literature lacks a systematic understanding of inference attacks via wireless sensing and defenses against them. In particular, existing literature surveys about wireless sensing [74, 85, 115, 144] focus on wireless sensing techniques and their *benign* applications, leaving systematization of the privacy aspect of wireless sensing largely untouched. Such a gap makes it hard to comprehensively understand the privacy vulnerabilities of wireless sensing and design effective defenses against potential inference attacks in the future. Without comprehensive systematization of wireless sensing systems, it is difficult for engineers to design privacy-preserving wireless sensing systems.

In this paper, we aim to bridge this gap. To do so, we propose a signal processing pipeline to systematize the inference attacks and defenses in human-centered wireless sensing systems. More specifically, we make the following contributions:

- **Taxonomy of wireless signals processing in the inference attacks and defenses.** Since wireless signal processing has been extensively used in human-centered wireless sensing systems for inference attacks and defenses, we propose a generalized signal processing pipeline-based framework for reasoning the existing and future inference attacks and defenses.
- **Open challenges.** We use our proposed framework to identify significant challenges facing the existing human-centered wireless sensing systems, predict the potential inference attacks, and provide directions for potential defenses against these attacks.
- **Identifying the design space towards privacy-preserving wireless sensing.** We identify the core design aspects that future wireless sensing systems should consider in their design to achieve privacy-preserving properties, and provide a design roadmap by discussing where and how human private information has been leaked based on our proposed framework.

Proceedings on Privacy Enhancing Technologies 2024(2), 313–329

https://doi.org/10.56553/popets-2024-0052

	Mobile computing community	Security and privacy community	others
Conferences/Journals	*Sigcomm, Mobicom, NSDI, Mobisys Sensys, IMWUT/Ubicomp, ToN, TOSNHotnet, IPSN, CoNext, Buildsys*	Security and Privacy, NDSS, CCS WiSec, USENIX Security, AsiaCCS	INFOCOM, TOG, VTC,CHI, ICOIN, ICC, TOBD, ECCV, CVPR, FTTC, IJDSN ToGRS, WiSPNET, Sensors, COMPSAC, TMTT, ICUW, ICASSP, Percom, RadarCon ICCA, communication letters,IEEE surveys and tutorials, Geriatric Psychiatry, RFID-TA JSAC, information systems, TOCS,JSTSP, JFI, GRSL, DySPAN, TOMC, MCM, IoTJ, AJGP, ToIM, WF-IoT, NaNA

Table 1: Summary of surveyed venues.

2 METHOD

To systematize the knowledge of inference attacks and defenses to human-centered wireless sensing, we adopt the five-step iterative process proposed by Wolfswinkel et al. [152] for literature review, which includes: (1) *Define*, (2) *Search*, (3) *Select*, (4) *Analyze*, and (5) *Present*.

Define. We define the scope of our literature review as follows:

- *Selected Source.* We use Google Scholar, ACM digital library, and IEEE Xplore as sources to collect papers. Moreover, we present the papers based on our research activities and common knowledge from the ACM, IEEE, USENIX, and ISOC communities. We report the papers published in the wireless sensing venues (e.g., SIGCOMM, MobiCom, IMWUT, Mobisys, HotNets, and Sensys) and network security and privacy venues (e.g., USENIX Security Symposium, IEEE S and P, and NDSS). Table 1 shows the summary of all the surveyed venues.
- *Search Terms.* We search the papers using the following terms: wireless sensing/localization, human activity recognition, inference/privacy attacks and defenses, eavesdropping, and human-centered wireless sensing.
- *Inclusion Criteria.* We mainly include papers from peer-reviewed journal articles as we presented in the Selected Source, which focus on how to *infer human private information in human-centered wireless sensing*. Specifically, we read the paper to understand if the paper's theme matches the human-centered wireless sensing topic. We find that some workshop or arXiv papers have the corresponding full papers published in the official conferences. So, we will simply select the full papers published in the official conferences. Moreover, we will eliminate the papers that do not discuss the *physical-layer wireless sensing techniques for inference attacks or defenses*, as human-centered wireless sensing mainly exploits the interaction between the wireless signals and the human body.

Search. Except for the well-known papers in this area based on our experience, we use the sources (*e.g.*, ACM digital library) mentioned above to search for papers. Moreover, we investigate the references in the related work presented in these papers to further build on the collected knowledge. As a result, we have 184 papers as candidates for the analysis.

Select. We aim to select the papers in the search stage, which can satisfy the inclusion criteria. Specifically, we first read the abstract and introduction sections of each paper to obtain a high-level view of its main discussion and focal points. Then, we read the core design of the paper to ensure the inclusion criteria. At last, there are 169 papers left for our systematization. The other 15 papers cannot meet our inclusion criteria. For example, some papers discuss the differential data privacy of wireless communication traffic.

Analyze. After selecting the papers, we divide them into two categories based on their topics. The first category mainly focuses on designing wireless sensing-based inference attacks that can accurately infer a victim's various private information. The second category mainly focuses on defenses against such attacks.

Present. We present our findings of formalizing the inference attacks and defenses to human-centered wireless sensing as follows.

3 THREAT MODEL

3.1 Attacker's Goal

We consider an attacker's goal to infer various private information about a victim human through sensing and analyzing the wireless signals around him/her. In particular, we summarize the private information considered in existing inference attacks as the following three categories:

- **Location.** The location represents sensitive information about a victim. Knowing the location of a victim leaks sensitive places that the victim has been to, such as those in a hospital, and enables tracking of the victim [13, 23, 60].
- **Living habits.** The living habits of a victim can leak other sensitive information about a victim. For instance, eating meals and going to the restroom frequently could be an indicator of diabetes disease. Moreover, knowing the living habits of a victim enables an attacker to commit well-informed severe crimes. For instance, an attacker may plan a burglary at a time when a victim is not at home [3, 5, 6].
- **Behavioral biometric characteristics.** Behavioral biometric characteristics refer to a person's pattern of behavior, including walking patterns, heart rate, and hand gestures. The leak of such behavioral biometric characteristics of a victim leads to severe privacy and security risks to the victim. For instance, heart rate may reveal that a victim has asthma or heart disease; hand gesture (e.g., touched locations and swiping patterns on the screen) of a victim to unlock a smartphone leads to compromise of the victim's password; and walking patterns enable an attacker to identify the victim's identity [11, 33, 54, 75].

3.2 Attacker's Capability

Sensing the type of wireless signal. We consider the attacker can sense the types of wireless signals around a victim. For instance, the attacker can first perform coarse-grained spectrum scanning to check if electromagnetic waves exist in the physical environment and then use fine-grained spectrum scanning to figure out the operating frequency of the wireless signals if they exist.

Receiving wireless signals via deploying a radio receiver. After the attacker senses the type of wireless signals, we consider the attacker is able to deploy a radio receiver to receive the wireless

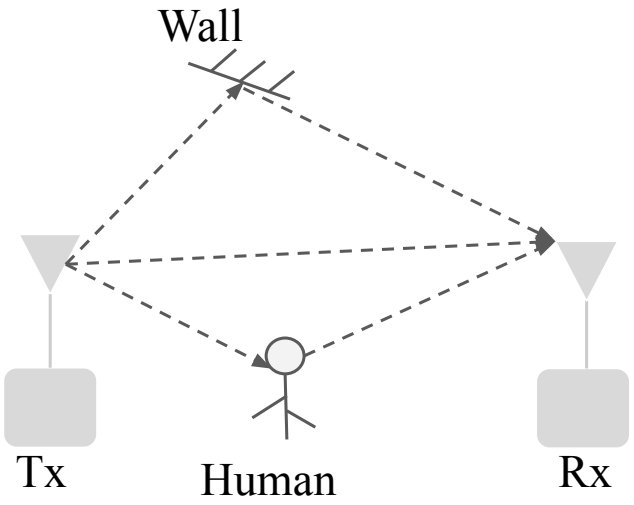

Figure 1: A typical wireless sensing system consists of a transmitter (Tx) and a receiver (Rx), where the Tx transmits wireless signals undergoing the physical environment and the Rx receives wireless signals. The wireless signals may reach the Rx through multiple paths due to reflections of the different objects (e.g., walls) and subjects (e.g., humans) in the physical environment.

Wireless technology	*Cost*	Effectiveness	Deployability
WiFi	*Medium*	High	High
BLE/Zigbee	Low	Medium	High
RFID	Low	Low	High
mmWave/UWB radar	High	High	High
VLC	Low	Low	Low
Cellular	Medium	High	Low

Table 2: Comparison of wireless technologies.

signals. The radio receiver should not be too far away from the transmitter around the victim, in order to receive wireless signals. For instance, when an attacker targets a victim in a house, the attacker can deploy its radio receiver outside/around the house.

4 HCWS AND ITS PRIVACY IMPLICATIONS

4.1 Wireless Sensing Principle

A typical wireless sensing system consists of two devices: a *transmitter (Tx)* and a *receiver (Rx)*, as shown in Fig. 1. A Tx or Rx may have one or multiple *antennas*. A Tx antenna emits wireless signals, which propagate and may be reflected by different objects (*e.g.*, walls) and subjects (*e.g.*, human) in the physical environment. An Rx antenna receives wireless signals.

To model the wireless communication between a Tx and an Rx, we start with a pair of Tx and Rx, each equipped with a single antenna. Specifically, the Tx transmits the wireless signals, denoted by $x(t)$, which is reflected by different types of objects (*e.g.*, walls, desks, and couches) and subjects (*e.g.*, human) in the physical environment, and then received by the Rx. Let $h(t)$ denote the multi-path propagation characteristics of the physical environment, or the *wireless channel*.

4.2 Wireless Technologies

There are many different kinds of wireless technologies that can be used for interference attacks. Table 2 summarizes the cost, effectiveness, and deployability of different wireless technologies. More details about these wireless technologies can be found as follows:

- **WiFi.** WiFi has been extensively explored for human-centered wireless sensing by harnessing the existing WiFi communication infrastructure [39, 56, 65]. To conduct the inference attacks using WiFi signals, the attacker needs to extract the channel state information (CSI) from the network interface card of the commercial WiFi device (e.g., laptop) or software-defined radios (e.g., USRP). Therefore, WiFi-based inference attacks do not introduce extra deployment costs and are easy to conduct with open-sourced CSI extractors [41, 154].
- **BLE/Zigbee.** Bluetooth low energy or Zigbee is designed for short-range and low-power communication, which can be also leveraged for inference attacks [14, 35, 115]. As the BLE/Zigbee-enabled devices (e.g., mobile devices) are widely deployed and the BLE/Zigbee sensor is usually low-cost, it is easy to conduct the inference attack. However, BLE/Zigbee suffers from the short communication and sensing range. It requires the attacker to be close to the target of interest. So, the attacker can be easily exposed and defended.
- **RFID.** Passive UHF RFID tags are widely used and deployed in warehouses and grocery stores for internet-of-things applications with a short communication range [80, 89, 101, 130, 141, 168]. The UHF RFID tags are low-cost, low-power, and small form factors without instrumenting complicated cryptographic algorithms, which can be used for inference attacks with the RFID reader. We can either use a commercial off-the-shelf RFID reader or software-defined radios to investigate the RFID tags, while the RFID readers are expensive. Since the passive RFID tags can be blindly investigated by any RFID reader, the RFID systems are supposed to be vulnerable to tag ID exposure.
- **mmWave/UWB Radar.** mmWave radar's physical principle is to emit the frequency-modulated continuous waves to the target of interest and analyze the signals reflected back from the target of interest for wireless sensing. Since mmWave is a high-frequency wireless signal, it usually gets attenuated easily [26, 71, 73, 164]. So, the mmWave radar is usually instrumented with a phased array antenna to concentrate the signals within a narrow beam for long-range sensing. The commercial off-the-shelf mmWave radar is usually low-cost and its sensing ability is limited by its phased array antenna. Since mmWave radar usually has a large bandwidth, it can provide very fine-grained sensing accuracy. Ultra-wideband radar (UWB) usually emits an impulse with a large bandwidth and measures the time-of-flight of the signals reflected off the target of interest, which can provide very accurate time-of-flight measurements with a larger bandwidth. In comparison to WiFi, BLE, and RFID, UWB and mmWave sensors are not widely deployed. All these sensors are usually cheap and easy to have from the market.

- **VLC.** Visible light communication usually works at high frequency which is supposed to be significantly attenuated over the air [28, 67]. Therefore, VLC-based wireless sensing has a short sensing range in comparison to WiFi. However, VLC employs a large bandwidth to measure the time of flight for accurate sensing with [67]. To do VLC-based inference attacks, we need to deploy the low-cost LED sensors close to the subject of interest in a line-of-sight scenario and VLC suffers from the interference introduced by the ambient light signals, which makes this VLC-based inference attack impractical in real-world settings.
- **Cellular.** Since the cellular communication infrastructure has been widely deployed in outdoor environments, we can use it for inference attacks such as outdoor localization [15, 61, 136]. The cellular-based inference attacks in human-centered wireless sensing suffer from the multipath effect in the outdoor area resulting in coarse-grained sensing accuracy. For example, LTrack [61] can achieve 6m localization error in 90% cases.

4.3 Workflow of Inference Attack

① **Deploying an sensing device.** When the existing wireless sensing system has already been deployed in the environment for good purposes such as enhancing life quality, the attacker can abuse it by deploying a receiver to sniff the wireless signals for human private information inference. Since the wireless signal is transparent to the attacker, the attacker needs to ensure the type of wireless signals used in the environment and choose the corresponding sniffing device to receive the wireless signals. In particular, the attacker can perform spectrum scanning to obtain the type of wireless signals in the environment and their corresponding operating frequency. Spectrum scanning can be divided into two categories: (*i*) using dedicated spectrum analyzers, which have poor time resolution due to large sweeping time [90, 108], and (*ii*) using low-cost radio receivers, which have small signal bandwidths due to the limited sampling rate [42, 107, 114]. Recently, SweepSense [38] proposes to modify the software-defined radio receiver (*i.e.*, USRP N210) to sweep the spectrum with high bandwidth and time resolution.

When there are no existing wireless sensing systems deployed in the environment, passive attacks cannot sniff any wireless signals interacting with the human body for inference attacks. However, the active attacker can deploy the transmitter to emit the wireless signals toward the physical environment and receive the backscattered signals to infer human private information, as the emitted wireless signals interact with the human body. To eliminate the multipath effect, we can either leverage the beamforming technique or multipath resolving algorithms. For example, Spotfi [60] proposes a super-resolution algorithm to estimate the angle-of-arrival (AoA) by incorporating a filtering and estimation approach to accurately identify the AoA of the direct path.

② **Sniffing and processing wireless signals.** The attacker can either actively emit the wireless signals and then receive the backscattered signals or passively receive the ambient wireless signals from the environment to infer human private information. As the received wireless signals are affected by the subject of interest in the physical environment, it is feasible to predict the human private information from these sniffed wireless signals. Then, the attacker needs to extract the wireless signals that are only affected by the subject of interest by resolving the multipath reflections, as the received signals at the attacker are the results of the multipath effect.

③ **Inferring human private information.** After obtaining the wireless signals that are only affected by the subject of interest, the attacker can design a model to predict the human private information from the wireless channel measurements through mathematical analysis or learning-based approaches.

4.4 Privacy Implications

From wireless sensing to privacy inference. Wireless sensing aims to perceive the physical environment using the received wireless signals around a human. The intuition is that the received signals are affected by the wireless channel, which is affected by the variation of the wireless environment (*e.g.*, human's movements) as the wireless signals interact with the human body. Therefore, a wireless sensing system usually analyzes the variation and extracts different properties (e.g., wireless channel) of the received signals to achieve the sensing purpose, which can reveal human private information such as human location and identity.

Bridging the gap. However, the existing wireless communication standards and specifications fail to prevent the leakage of this information due to the nature of widespread wireless signals. Wireless sensing systems have been extensively studied in academia, which mainly focuses on improving sensing accuracy without considering privacy leakage. The fundamental reason for privacy leakage is the interaction between the human body and wireless signals. Especially, with the proliferation of deep learning-based wireless sensing systems, even though deep learning has significantly improved the sensing accuracy of wireless sensing, it is vulnerable to adversarial attacks [19, 52, 53, 177]. Therefore, we provide an angle of understanding the vulnerability and privacy threat of machine learning-enabled wireless sensing systems from the whole system design point of view. Human private information is not communication data privacy but rather private information related to human movement that is sensed by the variation of the wireless signals. For example, keystrokes and gestures can reveal passwords. Human activity recognition can reveal the daily living style and human identities. The attacker can abuse the private information introduced by the human movement. For example, the attacker can detect if the house owner is at home or not for trespassing and theft. We bridge the gap between the privacy implications and wireless signal sensing parameters by connecting the physical parameters in the signal processing to the privacy inference that is targeted by the attackers.

5 A SIGNAL PROCESSING PIPELINE-BASED HCWS FRAMEWORK

We present a signal processing pipeline-based framework to categorize and systematize HCWS strategies as shown in Fig. 2. As discussed in Section 4.3, the attacker sniffs the wireless signals propagated in the physical environment using the deployed sensing device to extract different information from the wireless signals

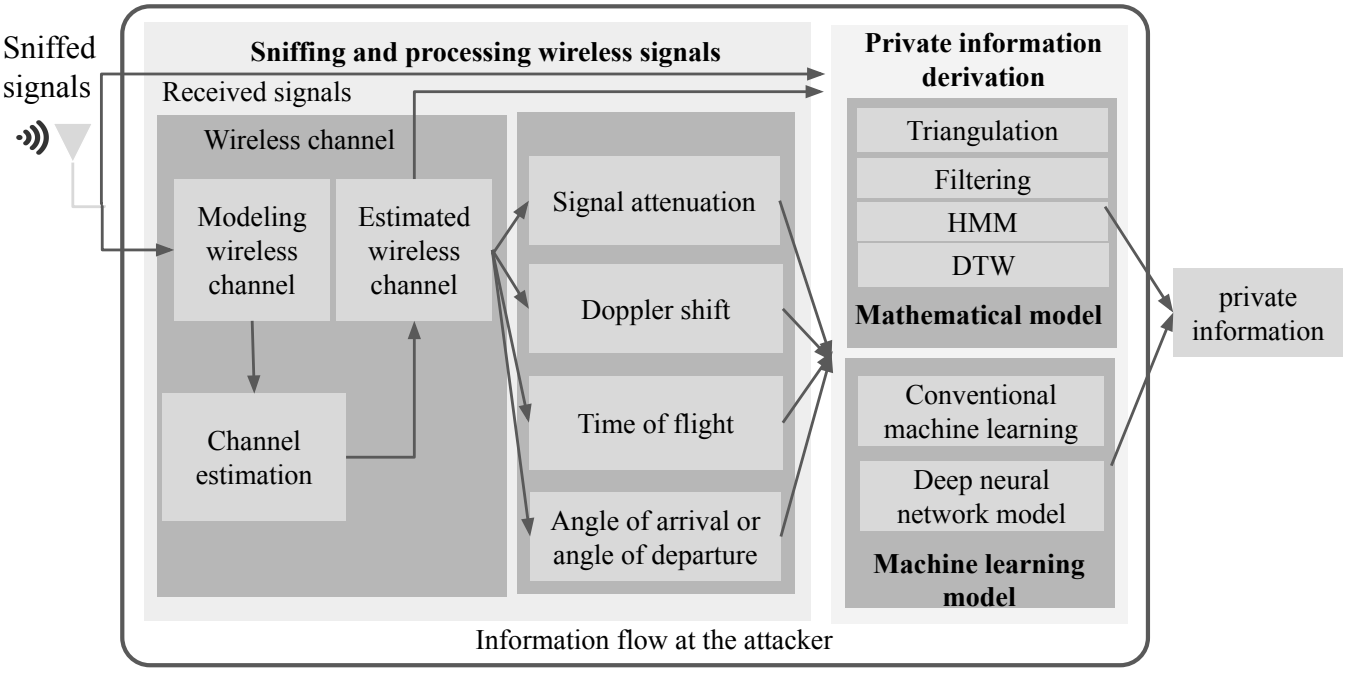

Figure 2: Overview of our proposed signal processing pipeline-based HCWS framework for analyzing and systematizing the existing human-centered wireless sensing.

for human private information derivation. The wireless signal processing pipeline is modeled and framed to systematize the HCWS.

5.1 Wireless Channel Estimation

An attacker can reconstruct a wireless channel from the received wireless signals, which will be used to derive human private information. Let's first model the wireless channel. When a device transmits a signal, this signal is distorted by the wireless environment due to human movements. Specifically, the signal undergoes the attenuation $\alpha(t)$ due to path loss and absorption. Since the signal travels over a distance of $d(t)$, its phase and strength can be changed. In a multiple-antenna wireless sensing system, we can consider the extra distance that the signal travels to/from each antenna in comparison to the reference antenna. This is characterized by the angle of arrival (AoA) $\theta_l(t)$ for l-th signal path at the antenna array-enabled Rx and the angle of departure (AoD) $\varphi_l(t)$ for l-th signal path at the antenna array-enabled Tx.

The wireless channel $h(t)$ can be obtained using signal preambles known to both the Tx and Rx and indicates the variation of the wireless environment. Let $p(t)$ denote the preamble signal, the received preamble at the Rx is given by:

$$y_p(t) = h(t) * p(t) + w(t). \quad (1)$$

With the known $p(t)$ and white Gaussian noise $w(t)$, $h(t)$ can be obtained using the maximum likelihood estimator. Based on the assumption that the signals at the adjacent frequency will undergo the same multipath, ML-based channel estimation methods have also been proposed in [17, 55, 77, 136].

5.2 Human Private Information Inference

To infer private information related to the victim, we need to find the relationship between the desired human private information and the extracted features from the received wireless signals. Prior works on human private information derivation mainly focus on the following methods.

Triangulation. The location of the victim can be obtained through triangulation, which can leverage the features from multiple receiving devices deployed by the attacker. Then, the wireless signals' features from these receiving devices deployed by the attacker can be used to reduce the ambiguity due to the noise. For example, the overlap of two features (*e.g.*, AoAs) can pinpoint the location of the victim [142]. The feature (*e.g.*, ToF) from one receiving device deployed by the attacker can formulate an ellipse. The overlap of multiple ellipses can pinpoint the location of the victim [7, 8, 81].

Filtering. To obtain the location of the victim, the attacker can use filters to filter out the extracted features that are not related to the victim. The widely used filtering methods for localization, tracking, and gesture/activity recognition include Kalman filtering and particle filtering. For example, TurboTrack [81] leverages particle filtering to achieve robot localization. Pantomime [111] uses extended Kalman filtering to achieve gesture recognition.

Markov chain modeling. Since tracking, hand gestures and human activity recognition are time-series movements, it is intuitive to leverage Markov chain models to delineate these time-series events. Prior works mainly use the Markov chain model or hidden Markov model (HMM) for tracking, localization, and gesture

recognition. For example, TurboTrack [81] uses HMM to track RFID-tagged drones. Lei et al. [159] use HMM to track moving objects through the wall.

Dynamic time warping (DTW). The main idea of DTW is to measure the similarity between the extracted and ground-truth features for human private information inference. For example, Mudra [170] uses DTW to recognize hand gestures, and Holt et al. [131] leverage the multi-dimensional DTW for hand gesture recognition.

Machine learning models. The machine learning model, especially the deep neural network, has been widely used to infer human private information due to its powerful data representation, resulting in highly accurate human private information derivation. Therefore, recent works on human-centered wireless sensing mainly design deep neural networks for highly accurate human private information derivation [13, 40, 62]. However, these machine-learning models are suffering from cyber attacks, the large training dataset collection, and scalability. Especially, in the wireless sensing domain, as the wireless environment is dynamic and full of multi-path, it is very challenging to have well-trained and trustworthy machine learning models for human-centered wireless sensing [78].

6 TAXONOMY OF EXISTING INFERENCE ATTACKS

Table 3 shows the taxonomy of existing inference attacks based on our proposed signal processing pipeline-based framework, where the sniffed wireless signals at the attacker will be processed and distilled to infer human private information. The prior works are categorized across multiple dimensions such as the attack goal, privacy leakage, wireless environment, attacking device, wireless signals, inferring private information, and property. Note that the property includes three metrics: cost, stealthiness, and wireless technology. The cost metric is measured by whether the attack requires a customized hardware device that can work with high bandwidth or a large antenna array. Usually, the customized attacking device working at the high bandwidth with a large antenna array is high-cost. The ubiquitous wireless radios such as WiFi access points and COTS software-defined radios are considered to be low-cost and are widely available. The wireless technology column indicates all the wireless technologies such as WiFi, RFID, cellular, etc. The listed papers in the last column of the table can leverage different wireless technologies as shown in Section 4.2 for the attack. For example, one paper uses WiFi technology for attack and another paper uses cellular technology for attack. The stealthiness indicates if the attack is easy to detect. For example, in comparison to the active attacker who actively transmits wireless signals for attack, the passive attacker who passively receives the wireless signals is more stealthy. Even though passive attackers are considered to be stealthier, there are always detection approaches that can disable the stealthiness property of these passive attacks as shown in Section 7. Since these academic papers from the wireless sensing domain try to push the limit of sensing accuracy, they evaluate the attack performance from the perspective of sensing accuracy or localization error. The sensing accuracy reported in the state-of-the-art techniques for human activity or gesture recognition is usually more than 0.95 [145, 169] and the localization error is at the decimeter level [84, 135]. The attack time in the wireless sensing attack can be defined as the time spent from deploying the attacking devices to successfully steal private information, which is not reported in these academic papers. We see some papers reporting the computational complexity of the sensing algorithms [42], which are not the attack time measured in real-world settings.

6.1 Received Signals-based Inference Attacks

The received wireless signals at the attacker can be used for inference attacks. Specifically, the attacker can collect the received wireless signals and then use them as features for an inference attack. For example, Zhu et al. [178] measure the variation of signal strength with a passive radio outside of the house to predict if there are occupants at home. IRshield [121] proposes to use the smart surface to distort the signal strength such that the attacker cannot predict the variation of the signal strength for occupant detection. However, the signal strength measurements are suffering from background noise. Vital-Radio [10] and Wistress [40] (i.e., stress sensing) use the variation of the signal phase caused by the chest movement to achieve the inference attack, as the phase information is resilient to the noise but sensitive to the signal's traveling path.

6.2 Wireless Channel-based Inference Attacks

After obtaining the reconstructed wireless channel, the attacker can use it as the feature for an inference attack. Furthermore, the attacker can extract the features based on the reconstructed wireless channel for an inference attack. Specifically, the attacker can extract the following features based on the reconstructed wireless channel:

- **Wireless channel.** The straightforward idea is to use the reconstructed features directly. Using the wireless channel as the features have been extensively studied to achieve gesture/activity recognition [66, 96, 137, 139, 146, 148] and indoor localization or tracking [11, 22, 33, 153].
- **Signal attenuation.** The signal attenuation can be directly derived from the signal's amplitude, which can characterize the wireless signal's power loss due to the over-the-air propagation. The signal attenuation feature has been widely used to infer human gestures/activities [2, 27, 59, 67, 116–119, 151], respiration/heart rate [1, 57, 99], and localization/tracking [16, 18, 63, 79, 92, 100, 110, 140, 157, 162, 163, 178].
- **Doppler shift.** Doppler shift is caused by the victim's movements in the physical environment, which can be used as a feature to infer private information. A victim moving at a speed of v at an angle of β from the attacker in the physical environment experiences a Doppler frequency shift given by:

$$\Delta f \propto \frac{2v \cdot \cos\beta}{c} \cdot f_c. \tag{2}$$

  The attacker can obtain the Doppler shift feature from the frequency-domain signals by applying the Fourier transform on the received signals. Prior works mainly leverage the Doppler shift for activity/gesture recognition and respiration/heart rate estimation using RF signals [25, 36, 64, 69, 82, 105, 106, 129, 138, 171].
- **Time of Flight (ToF).** ToF, denoted by τ, denotes the time duration during which the wireless signal travels through the physical

y: received signals; h: wireless channel; φ and θ: angle of departure and angle of arrival; γ:doppler shift; τ:time of flight; α:signal attenuation; cl: Conventional machine learning models; dl: Deep learning models;st:stealthiness;wt:wireless technology;asr:attack success rate;at:attack time;RF (>1): Multiple antennas; RF(=1): Single antenna; ✔: Used; ✖: Not used;↑:high;↓:low;→:not reported-:all wireless technologies;vlc:visible light communication

Attack goal	Privacy leakage	Wireless environment	Attacking device	Wireless signals						Inferring private information						Property		Papers	
					Wireless channel					Rule based				ML based					
				y	h	φ,θ	γ	τ	α	Triangulation	Filtering	Markov	DTW	cl	dl	Cost	Wireless technology	Low stealthiness (active attack)	High stealthiness (passive attack)
Location	Location	Home, one person	RF (>1)	✖	✖	✔	✖	✖	✖	✖	✖	✔	✖	✖	✖	↑/↓	-	[106,153,157, 158,16]	[130,139, 140,155]
		Home, multiple people	RF (=1)	✖	✖	✖	✖	✖	✔	✖	✔	✖	✖	✖	✖	↑/↓	-	[7,141,18, 62,148,92,120]	[18,21,23,95,135]
		Indoor,outdoor, one person	RF (>1)	✖	✔	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	↑/↓	-	[63,81,83, 110,159,25,35]	[100,110,162]
		Indoor, one person	RF (>1)	✖	✔	✔	✔	✔	✔	✔	✖	✖	✖	✖	✔	↑/↓	-	[13,14,9,51, 64,84,105, 12,79,80]	[12,34,151, 125,126,156]
Living habits	Living habits	Indoor, one person	RF (=1)	✖	✖	✖	✔	✖	✖	✖	✔	✖	✖	✖	✖	↑/↓	-	[145,127,96]	[66,145,26,121]
		Indoor, one person	RF (>1)	✖	✔	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	↑/↓	-	[118,174,87,119]	[11,117,118, 59,178]
		Indoor, one person	RF (>1)	✔	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔	↑/↓	-	[45,133,134, 6,8,54,113]	[70,15,47,52,163]
Behavioral biometric characteristic	Walking pattern	Indoor, one person	RF (>1)	✖	✔	✖	✖	✖	✔	✖	✖	✖	✔	✔	✔	↑/↓	-	[56, 60,169,46, 170,168,39,31,58, 147,173,175]	[129,61,161, 5,146]
		Indoor, one person	Light & RF (>1)	✖	✖	✖	✖	✔	✔	✖	✔	✖	✖	✖	✔	↓	vlc	[28]	[67]
	Heart /respiration rate	Indoor, one person	RF (>1)	✔	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔	↑/↓	-	[57,40,138]	[69,57]
		Indoor, one person	RF (>1)	✔	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	↑/↓	-	[10,36,171,165,99]	[1]
	Sleep stage	Indoor, one person	RF (>1)	✖	✖	✔	✖	✔	✖	✖	✖	✖	✖	✖	✔	↑/↓	-	[44,172,166,176]	[48,37]
	Hand gesture	Indoor, one person	RF (>1)	✖	✔	✖	✖	✖	✖	✖	✖	✖	✔	✖	✔	↑/↓	-	[32,75,82,137,2]	[65,160,22]
		Indoor, one person	RF (>1)	✖	✔	✖	✖	✖	✖	✖	✖	✖	✖	✔	✖	↑/↓	-	[68,89,91,144,142]	[116,167]
		Indoor, one person	RF (>1)	✖	✔	✖	✖	✖	✖	✖	✖	✖	✔	✔	✖	↑/↓	-	[88,111,131, 164,11,72,73,177]	[27,102,29,55]

Table 3: Taxonomy of existing inference attacks in the human-centered wireless sensing.

environment for distance d, and is given by:

$$\tau = d/c. \tag{3}$$

The estimation accuracy of the ToF information highly depends on the signal bandwidth B:

$$ToF \propto 1/B. \tag{4}$$

In radar-based wireless sensing systems, ToF can be derived from the multipath profile describing the signal over time in a round trip. To conduct the inference attack, the attacker can snoop the pulse or frequency-modulated continuous-wave (FMCW) signals transmitted from the radar and reflected by the victim to create a multipath profile, which can be leveraged to infer the private information of hand gestures and location [6–8, 72, 91]. ML models have been employed in radar-based wireless sensing systems to analyze the collected 3D point clouds, which can achieve fined-grained sensing on emotion/gestures/activity/behavior recognition [32, 68, 133, 172], gait velocity and strait length estimation [46], sleep sensing [44, 166, 176], human pose/mesh estimation [173, 174], 3D body skeleton [175], human identification/authentication [31, 45, 58, 134], and respiration/heart rate detection [165].

- **Angle of Arrival (AoA) and Angle of Departure (AoD).** AoA needs to be derived from the antenna array-enabled attacker. AoA of l-th signal path, denoted by $\theta_l(t)$, can be derived from the following equation:

$$d_e = D \cdot \cos\theta_l(t), \tag{5}$$

where d_e denotes the extra distance the signal travels, and D denotes the antenna separation in the antenna array. Similarly, AoD can be derived at the Tx's antenna array. AoA and/or AoD information has been widely employed to achieve activity recognition and localization/tracking [9, 88, 95, 102, 130, 141, 142, 155, 164, 168].

6.3 Discussion of Existing Inference Attacks

Discussion of received signal-based inference attacks. To use received signals for the attack, the attacker can simply infer human private information based on the machine learning-based network traffic pattern analysis. However, this received signal-based network traffic analysis suffers from the artifacts of communication data incorporated in the received signals. Usually, received signal-based wireless sensing attacks mainly leverage the signal strength of the received signals to infer the human private information, which suffers from the multipath effect in the indoor environment resulting in low sensing accuracy. Therefore, the received signal-based sensing attack usually focuses on the line-of-sight scenario, where the line-of-sight signals are dominant over the received signals in the with-device setting (e.g., a human holds a smartphone communicating with the WiFi access point). The multipath signal reflected off the human body should be resolved and used for inference attacks in device-free settings, where the victim does not co-locate with the transmitter.

Discussion of wireless channel-based inference attacks. Since the received signals-based sensing attacks are usually distorted by the communication data information, we would like to use the wireless channel to infer the human private information introduced by human movements. To use the estimated wireless channel for the attack, the attacker needs to accurately estimate the wireless channel. The attacker can simply infer the human private information based on the estimated wireless channel with machine learning models. This usually requires well-trained machine learning models on large-scale datasets, as the estimated wireless channel may not only be affected by human movements [13]. To this end, the signal path that is affected by the subject of interest should be extracted for attacking purposes, which requires the attacker to resolve the multipath over frequency, time, or space dimension. To do so, ToF can be leveraged to achieve high sensing accuracy by resolving the multipath in the frequency domain with a large bandwidth, and AoA/AoD can be leveraged to achieve sensing accuracy by resolving the multipath in the space domain with an antenna array. However, the attacker needs to be instrumented with a large antenna array or occupy a large frequency band, which will further burden the existing wireless spectrum usage. An attacker can use signal attenuation derived from the estimated wireless channel for the attack, which is straightforward. However, it suffers from the multipath effect resulting in inaccurate attenuation estimation. Doppler shift is another factor that can be leveraged for sensing attack, while it is related to the moving speed of the subject of the target. As a result, Doppler shift cannot achieve fine-grained sensing attacks, even though the speed of the human movement is slow in practice.

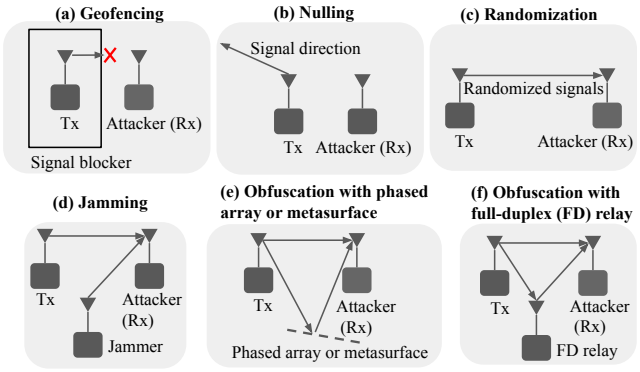

Figure 3: Illustration of the prevention strategy. (a) geofencing that can block the wireless signals at the transmitter. (b) Nulling can nullify the signals received by the attacker. (c) Randomization introduces artifacts to the transmitted wireless signals. (d) Jamming can distort the received signals at the attacker. Obfuscation with a phased array or meta surface (e) and full-duplex relay (f) can distort the received wireless signals at the attacker.

7 TAXONOMY OF EXISTING DEFENSES

7.1 Prevention Strategy

Fig. 3 summarizes and illustrates the prevention strategies against the inference attacks in HCWS. Table 4 (a) presents the taxonomy of prevention strategies against inference attacks.

7.1.1 Shielding Wireless Signals. The root cause of the inference attack is due to the widespread propagation nature of wireless signals and the multipath effect in the physical environment, thereby any attacker residing in the coverage area of the Tx can sniff the

wireless signals. To prevent the inference attack, we can shield the transmitted signals such that the attacker's Rx cannot receive them using the following two methods:

- **Geofencing.** Geofencing is a way that can block the wireless signal so that it becomes inaccessible to the attacker. To do so, we can cover the walls with electromagnetic shielding paints, customize the wireless signal coverage with 3D fabricated reflectors [23, 26, 156] or backscatter arrays [70, 167], as shown in Fig. 3(a).
- **Nulling.** To eliminate or mitigate the wireless signal propagation that is accessible to the attacker, the TX can also beamform the signal towards the desired Rx [29] to minimize the signals leaking in the direction that could be received by the attacker, as shown in Fig. 3(b). Furthermore, if the location of the attacker is known, the Tx can apply beamforming to generate a deep null towards the attacker. Abedi et al. [4] leverage the nulling capability of WiFi access points, and PushID [143] uses the blind beamforming to extend the coverage of the backscatter communication, which can be used to eliminate the eavesdropping in WiFi backscatter sensing systems.

7.1.2 Obfuscating Wireless Signals. To prevent inference attacks, we can also obfuscate the transmitted signals, such that the attacker cannot extract useful features from the sniffed wireless signals. To do so, the Tx can either randomize the transmitted signals or jam the received signals at the attacker's Rx as follows.

- **Randomizing the transmitted signals.** To obfuscate the transmitted signals, one way is to randomize the transmitted signals such that the attacker cannot predict anything from the traffic analysis based on the received signals as shown in Fig. 3(c). For example, RF-Cloak [43] randomizes the illuminated signals transmitted from the RFID reader to disable the attacker. Wijewardena et al. [149] consider randomization of the signal strengths to disable the attacker.
- **Jamming the signals received by the attacker.** Another way to obfuscate the transmitted signals is to deploy a signal generator to jam the received signals at the attacker, such that the signal-to-interference plus noise ratio (SINR) at the attacker is under the noise floor to disable the attacker, as shown in Fig. 3(d). For example, Jiao et al. [56] consider injecting artificial channels at the Tx to prevent inference attacks. Huang et al. [48] use programmable metasurface to jam the pilot of the signals, and Lyu et al.[83] use the programmable metasurface to jam the over-the-air signals.

7.1.3 Obfuscating the Wireless Channel. Prevention methods mentioned above mainly focus on Tx-side shielding and obfuscation. The wireless channel plays an important role in human-centered wireless sensing and can also be obfuscated using techniques such as programmable phased arrays, metasurfaces, or full-duplex relays. Obfuscating the wireless channel eventually leads to noisier wireless signals received by the attacker.

- **Reconfigurable phased array or metasurface-based wireless channel obfuscation.** To obfuscate the wireless channel, we can use a reconfigurable phased array consisting of multiple discrete phase shifters that can change the phase of the wireless signals, as shown in Fig. 3(e). For example, LAIA [70] uses a phased array to control the wireless channel in the desired way by changing the wireless signal's phase. We can also use the programmable metasurface to change the impinged signal's phase in the desired way. As such, the signals received by the attacker cannot help to extract the clean wireless channel that is only affected by the victim for private information inference. For example, IRShield [121] designs a metasurface that can change the wireless channel to disable eavesdropping. Hu et al. [47] use the reconfigurable metasurface to change the wireless channel coefficients. Staat et al. [120] use the metasurface to achieve the jamming purpose that could disable eavesdroppers.
- **Full-duplex relay-based wireless channel obfuscation.** Another way to obfuscate the wireless channel is to use full-duplex relays, as shown in Fig. 3(g). An amplify-and-forward (AF) relay amplifies and delays the impinging signal from the Tx and then forwards it to the attacker, during which the AF relay can change the amplitude and/or phase of the Tx signal. As such, the AF relay can change the wireless channel in the desired way such that the attacker cannot extract the desired and clean wireless signals affected by the victim for private information inference. For example, PhyCloak [104] uses the AF relay node to change the wireless channel that can prevent the attacker. Channel Spoofer [103] further demonstrates the AF relay node can change the wireless channel as designed. Sun et al. [125, 126] use the AF relay to achieve destructive signal addition at the attacker in RFID-based sensing systems.

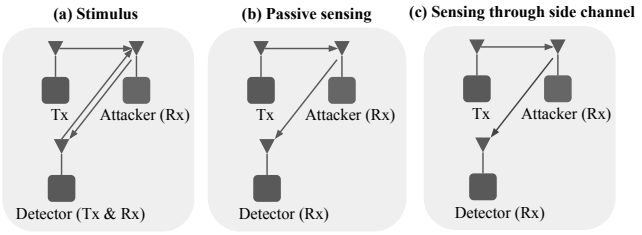

Figure 4: Illustration of the detection strategy. (a) Stimulus uses the generated wireless signals to excite the attacker for detection purposes. (b) Passive sensing can detect the existence of the attacker by overhearing the emanations from him/her. (c) Sensing through the side channel can detect the attacker by sensing the leakage of the undesired side-channel information from the attacker's Rx.

When the attacker is performing the active inference attack, the feasible defenses are jamming and obfuscation techniques. This is because the active attacker does not rely on the legitimate transmitter's transmissions to infer the human private information.

7.2 Detection Strategy

Detection of inference attacks aims to detect an attacker's Rx, which is challenging because the passive inference attack only passively sniffs the wireless signals in the environment without transmitting any signals. Detecting an attacker's Rx can be viewed as a sensing problem, where the detector aims to sense the Rx used and deployed by the attacker. To this end, there are three methods for detecting an

(a) Prevention

Shielding		Obfuscating wireless signals		Obfuscating wireless channel			Property			Papers
Geofencing	Nulling	Randomization	Jamming	Phased array	Metasurface	FD relay	Cost	Stealthiness	Wireless tech.	
✓	✗	✗	✗	✗	✗	✗	↑	↓	-	[23, 26, 70, 156, 167]
✗	✗	✗	✗	✓	✗	✗	-	↓	-	[70, 120, 167]
✗	✓	✗	✗	✗	✗	✗	-	↓	-	[4, 29, 143, 160]
✗	✗	✓	✗	✗	✗	✗	-	↓	-	[43, 149]
✗	✗	✗	✓	✗	✗	✗	-	↓	-	[48, 56, 83, 113, 120, 149]
✗	✗	✗	✗	✗	✓	✗	↑	↑	-	[26, 47, 48, 120, 121]
✗	✗	✗	✗	✗	✗	✓	↑	↑	-	[103, 104, 125, 126]

(b) Detection

Stimulus	Passive sensing	Side-channel	Cost	Stealthiness	Wireless tech.	Papers
✗	✓	✗	-	↓	-	[21, 24, 34, 86, 93, 97, 98, 112, 119, 150, 160]
✓	✗	✗	-	↑	-	[24, 49, 50, 71, 76, 109, 122–124, 132, 147]
✗	✗	✓	-	↑	-	[28, 171]

Table 4: Taxonomy of existing prevention (a) and detection (b) strategies for the defenses against the inference attacks. ✓: used, ✗: not used, -:all possible cases, ↑: high, and ↓: low.

Rx (*i.e.*, attacker), as illustrated in Fig. 4. We present the taxonomy of detection strategies against the inference attacks in Table 4(b).

- **Stimulus.** Although the attacker's passive Rx does not actively emit any signal, we can actively transmit a known stimulation signal that can trigger the attacker's Rx circuit to leak unintended signals, which can then be captured for detection purposes, as shown in Fig. 4(a). For example, many research papers [71, 109, 122–124, 132] show that by actively transmitting a known stimulation signal, the attacker's circuit can be triggered to reflect the unintended wireless signals, which could be further analyzed to detect the attacker. Recent works [49, 50, 76] also show that by emitting light signals, hidden cameras can be detected.
- **Passive sensing.** The passive devices deployed by the attacker can still leak the wireless signals, although it is inactive and just listening. So, we can sense these weak signal leakage from the attacker to detect the presence of the inference attack as shown in Fig. 4(b). For example, many research papers [21, 24, 86, 93, 97, 98, 112, 150] demonstrate and analyze the signal leakage from the local oscillator of the radio that can be sensed to detect the attacker. Recent works [34, 160] show the security issue of the leaky wave antennas in Terahertz communication and sensing, which can be detected to eliminate the attack.
- **Sensing through side-channel.** A passive device that does not actively transmit any signal can also leak the signals through side channels. Therefore, we can detect the presence of the attacker over these side channels, as shown in Fig. 4(c). For example, Cui et al. [28] use a wireless signal sniffer to detect the signal leakage of the visible light communication and sensing systems.

Since the active attacker needs to transmit the wireless signals and analyze the backscattered signals for inference attack, it is easy to detect them through passive sensing and sensing through side channels.

8 CHALLENGES FOR PRIVACY-PRESERVING HCWS

C1: Sniffing device deployment. The active attackers can always transmit known wireless signals to infer human private information, while the passive attackers need to rely on the existing wireless signals transmitted by the deployed wireless sensing systems for inference attacks. However, passive attacks are more covert than active attacks. As a result, passive attacks are difficult to detect. Active attacks are easy to detect and localized by analyzing the transmitted wireless signals from the active attackers.

Note that the existing passive attacks usually assume the attacker knows the exact signal type and frequency band the wireless sensing systems have used, which is not realistic for deploying real-world inference attacks. From the defense perspective, the signal type and frequency band used by the wireless sensing systems are also private information. If we can protect this information from being leaked, we can fundamentally defend against passive attacks.

C2: Compensating hardware imperfection and artifacts. The hardware imperfection of the transceiver introduces an extra phase shift $\phi(t)$, and the moving transceiver or reflectors will introduce phase shift $\gamma(t)$ due to the Doppler shift effect. All these changes are collectively referred to as the wireless channel. Therefore, for the signal transmitted at a carrier frequency of f_c (or with wavelength $\lambda = \frac{c}{f_c}$ where c is the speed of light), the single-path wireless channel $h(t)$ can be defined as:

$$h(t) = \alpha(t) \cdot \exp\left(-j2\pi\frac{d(t)}{\lambda} + j\phi(t) + j\gamma(t)\right). \quad (6)$$

In a real-world wireless environment, the signal received at the Rx is a composition of multiple copies of the original signal due to the multipath effect, where each copy can experience different attenuation, delay, and/or phase change. We can represent the channel seen by the Rx as the combination of all the possible L single-path channels:

$$h(t) = \sum_{l=1}^{L} \alpha_l(t) \cdot \exp\left(-j2\pi\frac{d_l(t)}{\lambda} + j\phi(t) + j\gamma_l(t)\right). \quad (7)$$

We are only interested in $d_l(t)$ or $\gamma_l(t)$, which is related to the subject of interest. As a result, it is highly challenging to resolve the composited signals received at the receiver due to the multipath effect. The hardware imperfection introduced by the transmitter is hard to compensate for, as the attacker cannot obtain the transmitter's hardware artifacts. As this hardware imperfection is unique to the hardware itself, it's usually leveraged for hardware fingerprinting.

The attacker needs to eliminate the human-introduced artifacts that are hidden in the wireless signals. For example, different people could perform the same activity or gesture with different scales and/or orientations with respect to the attacker. To remove the human-introduced artifacts in the extracted features, the attacker can rescale the time-series features [87, 94, 170]. To remove the orientation artifacts in the extracted features, the prior works mainly leverage the space diversity by using two antennas to receive the wireless signals based on the fact that the orientation artifact can be canceled out across different antennas [127, 169]. After the preprocessing, the attacker can use them as the input of private information inference components for indoor localization [51, 161] and tracking [12].

C3: Vulnerable machine learning-based private information inference. Recently, we find that deep learning has been extensively studied in human-centered wireless sensing for high sensing accuracy without considering privacy leakage. Therefore, it is important to build trustworthy deep-learning models and apply them to the existing signal-processing pipeline of human-centered wireless sensing. We identify the following gaps or challenges to achieve privacy-preserving ML-enabled human-centered wireless sensing systems. Under our signal processing pipeline-based framework, we find that the wireless sensing systems often leverage machine learning models for human private information inference, which are vulnerable to adversarial attacks [20, 128]. Specifically, the attacker can add small carefully crafted noises to wireless signals to turn them into adversarial examples, which can obfuscate the machine learning models employed by the legitimate transceiver, such that the legitimate wireless sensing systems would make random inferences about human's private information. Even though we can directly apply the existing defensive mechanisms from the trustworthy machine learning community to secure the machine learning models used in HCWS, it is challenging to integrate these defensive mechanisms from the end-to-end HCWS system design point of view. This is because the existing defensive mechanisms for machine learning models are only designed for machine learning models without considering the integration and role of these models in an end-to-end system.

C5: Resolving multipath in a dynamic and multiple person environment. The prior works on human-centered wireless sensing mainly focus on one subject of interest in a quasi-static wireless environment. This is because wireless sensing mainly leverages the variation of the wireless environment affected by human movements to infer human private information. When there are multiple different reflectors (e.g., walls, chairs, furniture, etc.) or moving artifacts in the environment, the received wireless signals at the attacker will be distorted. So, it is important for the attacker to resolve the multipath and extract the signal path that is only affected by the subject of interest. We illustrate the pros and cons of the following multipath resolving approaches from the time, frequency, and space domains.

- **Resolving multipath in the time domain.** To eliminate the artifacts introduced by the wireless environment, the straightforward idea is to assume the wireless environment is only affected by the victim and all other objects are relatively static. Specifically, the signal cancellation approach can be employed to cancel out the effects from all the other non-victims (*e.g.*, walls, desks), while this approach barely works in the dynamic environment. This is because we cannot assume the environment-introduced artifacts are not changing over time for our cancellation purpose.
- **Resolving multipath in the frequency domain.** The main idea of resolving multipath in the frequency domain is to leverage the characteristic of the frequency-selective wireless channel in which the wireless signals operating at different frequencies will be affected by the physical environment differently. To do so, we leverage wireless signals that occupy a wide frequency band to measure the time-of-flight for resolving the multipath, while the wide-band signals are barely available due to the limited wireless spectrum.
- **Resolving multipath in the space domain.** Resolving the multipath in the space domain is intuitive, as the different objects in the physical environment will be located in different places. Therefore, the signals reflected by these different objects will undergo different physical paths, resulting in different AoA values that can be measured to resolve the multipath signal propagation. However, using multiple arrays will introduce deployment costs. Given the receiving antenna array, the AoA resolution is limited by this array's aperture size. When two objects are close to each other, they will introduce similar signal propagation paths that cannot be resolved over the space domain.

C6: Obfuscating the attacker without affecting the legitimate receiver's sensing purposes. Wireless sensing can be leveraged for human-computer interaction, smart homes, and asset tracking. So, it is important to obfuscate the attacker without affecting the legitimate receiver's sensing purposes. However, this is very difficult and challenging, as the attacker and legitimate receiver share the same wireless environment. As a result, the legitimate receiver will also receive these distorted wireless signals. The distorted signal cancellation at the legitimate receiver will also introduce extra artifacts that are hard to eliminate. Since we do not know where the attacker is, it is not possible to shine the very narrow beam toward the attacker without affecting the legitimate receiver's sensing purposes.

Shielding wireless signals and wireless channels will affect and even suspend normal wireless communication due to the weak received signal strength at the legitimate receiver, which will not be desirable for joint communication and sensing systems as wireless sensing is usually a byproduct of wireless communication. In comparison to the prevention methods, the detection methods (e.g., passive sensing and sensing through side channels) will not affect the existing wireless communication, while it is very difficult to detect the leaked side-channel information from the attacker that is weak and usually under noise floor.

9 DISCUSSIONS AND FUTURE DIRECTIONS

Applying trustworthy machine learning. The existing trustworthy machine learning models do not take into account privacy issues when they are integrated into human-centered wireless sensing systems [13, 158]. For example, we know that adversarial examples can be leveraged to obfuscate the machine-learning models, while we still do not know how to apply the adversarial examples to achieve privacy-preserving ML-enabled human-centered wireless sensing systems from the end-to-end system design point of view. One possible solution is to generate the adversarial examples at the input features of the attacker's machine learning models without considering the end-to-end HCWS design, which requires us to access the attacker's sensing system. Since the input features of the machine learning models are coming from the signal processing pipeline, we can introduce over-the-air adversarial examples with smart surface or full-duplex relay nodes.

- **Adversarial examples added to the wireless channel.** To defend against an inference attack conducted based on the wireless channel, we can turn it into adversarial examples via deploying the programmable smart surface or full-duplex radio in the physical environment, such that the adversarially perturbed wireless channel makes the attacker's machine learning models randomly and incorrectly predict a victim's private information as shown in Fig. 5. The recent paper presents WiADv [177], a system that uses the full-duplex radio to obfuscate the estimated wireless channel at the receiver of the wireless sensing-based gesture recognition systems.
- **Adversarial examples added to the received signals.** To defend against an inference attack conducted based on the received signals, the adversarial examples could be generated by a generator (i.e., full-duplex node) to introduce misclassification to the attacker's machine learning models. In this case, the wireless signals received by the attacker's Rx consist of the signals transmitted from the legitimate Tx and the signals generated by the generator. In other words, the composition of the signals transmitted from the legitimate Tx and the signals generated by the generator should be adversarial examples to the attacker's machine learning models. Such defenses are illustrated in Fig. 5. For example, a recent paper proposes RF-Protect [113], a system that uses the smart surface to obfuscate the radar-based human activity recognition systems by generating ghost reflections.

To protect a legitimate Rx from being affected by these adversarial examples, it could use different mechanisms from the attacker to analyze the received wireless signals. In particular, a legitimate Rx may know the added adversarial perturbations and filter them before analyzing the wireless signals if the Rx and the Tx have established a secure communication channel in advance and can exchange the added adversarial perturbations. Moreover, the generated adversarial examples can be directed to the attacker's Rx without interfering with the legitimate Rx's sensing purpose using either directional antennas or beamforming techniques. In particular, we know the locations of the legitimate Rx and thus we can direct the adversarial examples towards directions not covering the legitimate Rx. Furthermore, it is an interesting future research direction to carefully design the adversarial examples, such that the legitimate Rx's analysis is unaffected by the adversarially perturbed wireless signals while the attacker's machine learning models make random and even incorrect inferences based on the adversarially perturbed wireless signals.

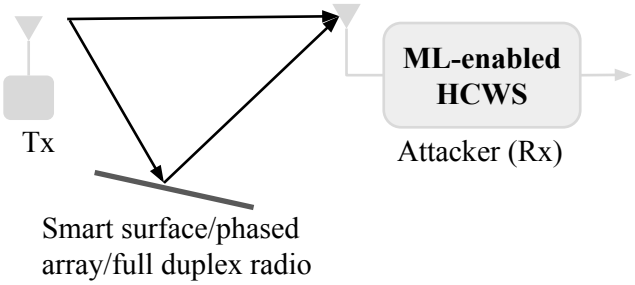

Figure 5: Adversarial example introduced by the smart surface, phased array, or full-duplex radio can disable the private information inference at the attacker.

Defenses with formal privacy guarantees. Existing defenses do not have formal privacy guarantees. For instance, the prevention strategies with wireless signal obfuscation simply add noise to the signals received by the attacker without considering the privacy guarantee. When the attacker employs machine learning models for human private information inference, this added noise can be mitigated through adversarial training or incoherent averaging over multiple received signals. The detection strategies mainly focus on detecting the signal leakage at the attacker's Rx. Therefore, the defenses may be broken by advanced and adaptive inference attacks that know these defenses. Therefore, it is important to generate the noise derived from the differential privacy mechanisms [30], which can provide a privacy guarantee. Moreover, we could also leverage differential privacy and analyze the tradeoff between the privacy guarantee and the utility of wireless sensing or communication to achieve joint sensing and communication or defenses without affecting the legitimate transceiver's sensing purpose.

Multimodal sensor fusion-based inference attacks. Existing inference attacks only leverage wireless signals from a single Rx. To be resilient and robust to the dynamic and multipath wireless environment, the attacker can leverage multimodal sensor fusion, in which multiple Rxs can be used to sense the variation of the physical environment. As such, this multimodal sensor fusion provides improved diversity for the attacker to infer private information about the victim. To mitigate the privacy leakage in human-centered wireless sensing, we can still leverage the above defensive mechanisms. This is because multimodal sensor fusion highly depends on trustworthy signal sources from different devices. The above defensive mechanisms can also defend against the inference attack on each individual device in multimodal sensor fusion-based inference attacks. However, how effective using the above defensive mechanisms against the multimodal sensor fusion-based inference attacks needs further exploration. Moreover, One great challenge of multimodal sensor fusion-based inference attacks is data stream synchronization, as these multimodal features are extracted from multiple devices.

Detecting inference attack based on the estimated wireless

channel. We identify that existing detection methods haven't leveraged wireless channels. It is an interesting future research direction to explore wireless channel-based detection methods. For instance, we can detect an attacker's Rx by measuring the wireless channel wireless channel. One idea is that the existence of the attacker's Rx changes the multipath reflection profile of the wireless channel. This is because wireless signal propagation highly depends on the reflection of different objects in the physical environment. Therefore, by comparing the difference of the multipath profile of the physical environment, we can detect the attacker's Rx. However, this highly depends on the granularity of the multipath profile. We believe that advanced sensors (e.g., LiDAR or mmWave Radar) can be used to create the 3D point cloud of the environment and then leverage computer vision techniques to identify the attackers.

10 CONCLUSIONS

In this work, we systematized the literature on human-centered wireless sensing-based inference attacks and defenses through frameworks and insights. To do so, we propose a signal processing pipeline-based framework to bridge the gap between wireless sensing and privacy implications. Then, we instantiate the wireless sensing-based inference attacks and defenses. Based on this, we address the open challenges and identify the design space for privacy-preserving wireless sensing.

ACKNOWLEDGMENTS

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. We are grateful to the anonymous reviewers and our shepherd for their insightful feedback.

REFERENCES

[1] Heba Abdelnasser, Khaled A Harras, and Moustafa Youssef. 2015. UbiBreathe: A ubiquitous non-invasive WiFi-based breathing estimator. In *Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. ACM, New York, 277–286.

[2] Heba Abdelnasser, Moustafa Youssef, and Khaled A Harras. 2015. Wigest: A ubiquitous wifi-based gesture recognition system. In *2015 IEEE conference on computer communications (INFOCOM)*. IEEE, IEEE, New York, 1472–1480.

[3] Ali Abedi and Omid Abari. 2020. WiFi Says" Hi!" Back to Strangers!. In *Proceedings of the 19th ACM Workshop on Hot Topics in Networks*. ACM, New York, 132–138.

[4] Ali Abedi and Omid Abari. 2021. Can WiFi Backscatter Achieve the Range of RFID? Nulling to the Rescue. In *Proceedings of the Twentieth ACM Workshop on Hot Topics in Networks*. ACM, New York, 171–177.

[5] Abbas Acar, Hossein Fereidooni, Tigist Abera, Amit Kumar Sikder, Markus Miettinen, Hidayet Aksu, Mauro Conti, Ahmad-Reza Sadeghi, and Selcuk Uluagac. 2020. Peek-a-boo: I see your smart home activities, even encrypted!. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, New York, 207–218.

[6] Fadel Adib, Chen-Yu Hsu, Hongzi Mao, Dina Katabi, and Frédo Durand. 2015. Capturing the human figure through a wall. *ACM Transactions on Graphics (TOG)* 34, 6 (2015), 1–13.

[7] Fadel Adib, Zachary Kabelac, and Dina Katabi. 2015. {Multi-Person} Localization via {RF} Body Reflections. In *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)*. USENIX, New York, 279–292.

[8] Fadel Adib, Zach Kabelac, Dina Katabi, and Robert C Miller. 2014. 3D tracking via body radio reflections. In *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*. USENIX, New York, 317–329.

[9] Fadel Adib and Dina Katabi. 2013. See through walls with WiFi!. In *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*. ACM, New York, 75–86.

[10] Fadel Adib, Hongzi Mao, Zachary Kabelac, Dina Katabi, and Robert C Miller. 2015. Smart homes that monitor breathing and heart rate. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. ACM, New York, 837–846.

[11] Kamran Ali, Alex X Liu, Wei Wang, and Muhammad Shahzad. 2015. Keystroke recognition using wifi signals. In *Proceedings of the 21st annual international conference on mobile computing and networking*. ACM, New York, 90–102.

[12] Pubudu Aravinda, Sulochana Sooriyaarachchi, Chandana Gamage, and Navinda Kottege. 2021. Optimization of RSSI based indoor localization and tracking to monitor workers in a hazardous working zone using Machine Learning techniques. In *2021 International Conference on Information Networking (ICOIN)*. IEEE, IEEE, New York, 305–310.

[13] Roshan Ayyalasomayajula, Aditya Arun, Chenfeng Wu, Sanatan Sharma, Abhishek Rajkumar Sethi, Deepak Vasisht, and Dinesh Bharadia. 2020. Deep learning based wireless localization for indoor navigation. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*. ACM, New York, 1–14.

[14] Roshan Ayyalasomayajula, Deepak Vasisht, and Dinesh Bharadia. 2018. BLoc: CSI-based accurate localization for BLE tags. In *Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies*. ACM, New York, 126–138.

[15] Sangwook Bae, Mincheol Son, Dongkwan Kim, CheolJun Park, Jiho Lee, Sooel Son, and Yongdae Kim. 2022. Watching the Watchers: Practical Video Identification Attack in {LTE} Networks. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX, New York, 1307–1324.

[16] Paramvir Bahl and Venkata N Padmanabhan. 2000. RADAR: An in-building RF-based user location and tracking system. In *Proceedings IEEE INFOCOM 2000. Conference on computer communications. Nineteenth annual joint conference of the IEEE computer and communications societies (Cat. No. 00CH37064)*, Vol. 2. Ieee, IEEE, New York, 775–784.

[17] Arjun Bakshi, Yifan Mao, Kannan Srinivasan, and Srinivasan Parthasarathy. 2019. Fast and efficient cross band channel prediction using machine learning. In *The 25th Annual International Conference on Mobile Computing and Networking*. ACM, New York, 1–16.

[18] Paolo Barsocchi, Stefano Lenzi, Stefano Chessa, and Gaetano Giunta. 2009. A novel approach to indoor RSSI localization by automatic calibration of the wireless propagation model. In *VTC Spring 2009-IEEE 69th Vehicular Technology Conference*. IEEE, IEEE, New York, 1–5.

[19] Nicholas Carlini and David Wagner. 2017. Adversarial examples are not easily detected: Bypassing ten detection methods. In *Proceedings of the 10th ACM workshop on artificial intelligence and security*. ACM, New York, 3–14.

[20] Nicholas Carlini and David Wagner. 2017. Towards evaluating the robustness of neural networks. In *2017 ieee symposium on security and privacy (sp)*. Ieee, IEEE, New York, 39–57.

[21] Anadi Chaman, Jiaming Wang, Jiachen Sun, Haitham Hassanieh, and Romit Roy Choudhury. 2018. Ghostbuster: Detecting the presence of hidden eavesdroppers. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. ACM, New York, 337–351.

[22] Bo Chen, Vivek Yenamandra, and Kannan Srinivasan. 2015. Tracking keystrokes using wireless signals. In *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, New York, 31–44.

[23] Lili Chen, Wenjun Hu, Kyle Jamieson, Xiaojiang Chen, Dingyi Fang, and Jeremy Gummeson. 2021. Pushing the Physical Limits of {IoT} Devices with Programmable Metasurfaces. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*. USENIX, Vitual, 425–438.

[24] Yushi Cheng, Xiaoyu Ji, Tianyang Lu, and Wenyuan Xu. 2018. Dewicam: Detecting hidden wireless cameras via smartphones. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. ACM, New York, 1–13.

[25] Kevin Chetty, Graeme E Smith, and Karl Woodbridge. 2011. Through-the-wall sensing of personnel using passive bistatic wifi radar at standoff distances. *IEEE Transactions on Geoscience and Remote Sensing* 50, 4 (2011), 1218–1226.

[26] Kun Woo Cho, Mohammad H Mazaheri, Jeremy Gummeson, Omid Abari, and Kyle Jamieson. 2023. {mmWall}: A Steerable, Transflective Metamaterial Surface for {NextG}{mmWave} Networks. In *20th USENIX Symposium on Networked Systems Design and Implementation (NSDI 23)*. USENIX, Boston, 1647–1665.

[27] Gabe Cohn, Daniel Morris, Shwetak Patel, and Desney Tan. 2012. Humantenna: using the body as an antenna for real-time whole-body interaction. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, New York, 1901–1910.

[28] Minhao Cui, Yuda Feng, Qing Wang, and Jie Xiong. 2020. Sniffing visible light communication through walls. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*. ACM, New York, 1–14.

[29] Hong-Ning Dai, Qiu Wang, Dong Li, and Raymond Chi-Wing Wong. 2013. On eavesdropping attacks in wireless sensor networks with directional antennas. *International Journal of Distributed Sensor Networks* 9, 8 (2013), 760834.

[30] Cynthia Dwork, Aaron Roth, et al. 2014. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science* 9, 3–4 (2014), 211–407.

[31] Lijie Fan, Tianhong Li, Rongyao Fang, Rumen Hristov, Yuan Yuan, and Dina Katabi. 2020. Learning longterm representations for person re-identification

using radio signals. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*. IEEE/CVF, New York, 10699–10709.

[32] Lijie Fan, Tianhong Li, Yuan Yuan, and Dina Katabi. 2020. In-home daily-life captioning using radio signals. In *European Conference on Computer Vision*. Springer, Springer, New York, 105–123.

[33] Chao Feng, Jie Xiong, Liqiong Chang, Fuwei Wang, Ju Wang, and Dingyi Fang. 2021. RF-Identity: Non-Intrusive Person Identification Based on Commodity RFID Devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 1 (2021), 1–23.

[34] Yasaman Ghasempour, Chia-Yi Yeh, Rabi Shrestha, Yasith Amarasinghe, Daniel Mittleman, and Edward W Knightly. 2020. LeakyTrack: Non-coherent single-antenna nodal and environmental mobility tracking with a leaky-wave antenna. In *SenSys' 20: Proceedings of the 18th Conference on Embedded Networked Sensor Systems*. ACM, New York, 417–426.

[35] Hadi Givehchian, Nishant Bhaskar, Eliana Rodriguez Herrera, Héctor Rodrigo López Soto, Christian Dameff, Dinesh Bharadia, and Aaron Schulman. 2022. Evaluating physical-layer ble location tracking attacks on mobile devices. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, IEEE, San Francisco, 1690–1704.

[36] Changzhan Gu, Changzhi Li, Jenshan Lin, Jiang Long, Jiangtao Huangfu, and Lixin Ran. 2009. Instrument-based noncontact Doppler radar vital sign detection system using heterodyne digital quadrature demodulation architecture. *IEEE Transactions on Instrumentation and Measurement* 59, 6 (2009), 1580–1588.

[37] Yu Gu, Yifan Zhang, Jie Li, Yusheng Ji, Xin An, and Fuji Ren. 2018. Sleepy: Wireless channel data driven sleep monitoring via commodity WiFi devices. *IEEE Transactions on Big Data* 6, 2 (2018), 258–268.

[38] Yeswanth Guddeti, Raghav Subbaraman, Moein Khazraee, Aaron Schulman, and Dinesh Bharadia. 2019. {SweepSense}: Sensing 5 {GHz} in 5 Milliseconds with Low-cost Radios. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*. USENIX, BOSTON, 317–330.

[39] Xiaonan Guo, Bo Liu, Cong Shi, Hongbo Liu, Yingying Chen, and Mooi Choo Chuah. 2017. WiFi-enabled smart human dynamics monitoring. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*. ACM, New York, 1–13.

[40] Unsoo Ha, Sohrab Madani, and Fadel Adib. 2021. WiStress: Contactless stress monitoring using wireless signals. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 3 (2021), 1–37.

[41] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. 2023. Linux 802.11n CSI Tool. https://dhalperi.github.io/linux-80211n-csitool/.

[42] Haitham Hassanieh, Lixin Shi, Omid Abari, Ezzeldin Hamed, and Dina Katabi. 2014. GHz-wide sensing and decoding using the sparse Fourier transform. In *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*. IEEE, IEEE, Toronto, 2256–2264.

[43] Haitham Hassanieh, Jue Wang, Dina Katabi, and Tadayoshi Kohno. 2015. Securing {RFIDs} by Randomizing the Modulation and Channel. In *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)*. USENIX, Santa Clara, 235–249.

[44] Chen-Yu Hsu, Aayush Ahuja, Shichao Yue, Rumen Hristov, Zachary Kabelac, and Dina Katabi. 2017. Zero-effort in-home sleep and insomnia monitoring using radio signals. *Proceedings of the ACM on Interactive, mobile, wearable and ubiquitous technologies* 1, 3 (2017), 1–18.

[45] Chen-Yu Hsu, Rumen Hristov, Guang-He Lee, Mingmin Zhao, and Dina Katabi. 2019. Enabling identification and behavioral sensing in homes using radio reflections. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, Glasgow, 1–13.

[46] Chen-Yu Hsu, Yuchen Liu, Zachary Kabelac, Rumen Hristov, Dina Katabi, and Christine Liu. 2017. Extracting gait velocity and stride length from surrounding radio signals. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, Denver, 2116–2126.

[47] Lei Hu, Guyue Li, Hongyi Luo, and Aiqun Hu. 2021. On the RIS manipulating attack and its countermeasures in physical-layer key generation. In *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. IEEE, IEEE, Honolulu, 1–5.

[48] Ke-Wen Huang and Hui-Ming Wang. 2020. Intelligent reflecting surface aided pilot contamination attack and its countermeasure. *IEEE Transactions on Wireless Communications* 20, 1 (2020), 345–359.

[49] Internet. 2022. Glint finder - camera detector. https://play.google.com/store/apps/detailsid=com.workshop512.glintfinder.

[50] Internet. 2022. Hidden camera detector. https://apps.apple.com/us/app/hidden-camera-detector/id532882360.

[51] Charu Jain, Gundepudi V Surya Sashank, S Markkandan, et al. 2021. Low-cost BLE based indoor localization using RSSI fingerprinting and machine learning. In *2021 sixth international conference on wireless communications, signal processing and networking (WiSPNET)*. IEEE, IEEE, Chennai, 363–367.

[52] Jinyuan Jia and Neil Zhenqiang Gong. 2018. {AttriGuard}: A practical defense against attribute inference attacks via adversarial machine learning. In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX, Baltimore, 513–529.

[53] Jinyuan Jia, Ahmed Salem, Michael Backes, Yang Zhang, and Neil Zhenqiang Gong. 2019. Memguard: Defending against black-box membership inference attacks via adversarial examples. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*. ACM, London, 259–274.

[54] Shang Jiang, Jianguo Jiang, Siye Wang, Yanfang Zhang, Yue Feng, Ziwen Cao, and Yi Liu. 2022. RF-Gait: Gait-Based Person Identification with COTS RFID. *Wireless Communications and Mobile Computing* 2022, 4 (2022), 417–426.

[55] Wenjun Jiang, Chenglin Miao, Fenglong Ma, Shuochao Yao, Yaqing Wang, Ye Yuan, Hongfei Xue, Chen Song, Xin Ma, Dimitrios Koutsonikolas, et al. 2018. Towards environment independent device free human activity recognition. In *Proceedings of the 24th annual international conference on mobile computing and networking*. ACM, New Delhi, 289–304.

[56] Xianjun Jiao, Michael Mehari, Wei Liu, Muhammad Aslam, and Ingrid Moerman. 2021. openwifi CSI fuzzer for authorized sensing and covert channels. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, Abu Dhabi, 377–379.

[57] Ossi Kaltiokallio, Hüseyin Yiğitler, Riku Jäntti, and Neal Patwari. 2014. Non-invasive respiration rate monitoring using a single COTS TX-RX pair. In *IPSN-14 Proceedings of the 13th International Symposium on Information Processing in Sensor Networks*. IEEE, IEEE, New York, 59–69.

[58] Belal Korany, Chitra R Karanam, Hong Cai, and Yasamin Mostofi. 2019. XModal-ID: Using WiFi for through-wall person identification from candidate video footage. In *The 25th Annual International Conference on Mobile Computing and Networking*. ACM, New York, 1–15.

[59] Ahmed E Kosba, Ahmed Saeed, and Moustafa Youssef. 2012. RASID: A robust WLAN device-free passive motion detection system. In *2012 IEEE International Conference on Pervasive Computing and Communications*. IEEE, IEEE, New York, 180–189.

[60] Manikanta Kotaru, Kiran Joshi, Dinesh Bharadia, and Sachin Katti. 2015. Spotfi: Decimeter level localization using wifi. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*. ACM, New York, 269–282.

[61] Martin Kotuliak, Simon Erni, Patrick Leu, Marc Röschlin, and Srdjan Čapkun. 2022. {LTrack}: Stealthy tracking of mobile phones in {LTE}. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX, New York, 1291–1306.

[62] Aristotelis Koutris, Theodoros Siozos, Yannis Kopsinis, Aggelos Pikrakis, Timon Merk, Matthias Mahlig, Stylianos Papaharalabos, and Peter Karlsson. 2022. Deep Learning-Based Indoor Localization Using Multi-View BLE Signal. *Sensors* 22, 7 (2022), 2759.

[63] Ka-Ho Lam, Chi-Chung Cheung, and Wah-Ching Lee. 2018. New RSSI-based LoRa localization algorithms for very noisy outdoor environment. In *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 2. IEEE, IEEE, New York, 794–799.

[64] Changzhi Li and Jenshan Lin. 2008. Random body movement cancellation in Doppler radar vital sign detection. *IEEE Transactions on Microwave Theory and Techniques* 56, 12 (2008), 3143–3152.

[65] Hong Li, Wei Yang, Jianxin Wang, Yang Xu, and Liusheng Huang. 2016. WiFinger: Talk to your smart devices with finger-grained gesture. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, New York, 250–261.

[66] Mengyuan Li, Yan Meng, Junyi Liu, Haojin Zhu, Xiaohui Liang, Yao Liu, and Na Ruan. 2016. When CSI meets public WiFi: inferring your mobile phone password via WiFi signals. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. ACM, New York, 1068–1079.

[67] Tianxing Li, Chuankai An, Zhao Tian, Andrew T Campbell, and Xia Zhou. 2015. Human sensing using visible light communication. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, New York, 331–344.

[68] Tianhong Li, Lijie Fan, Mingmin Zhao, Yingcheng Liu, and Dina Katabi. 2019. Making the invisible visible: Action recognition through walls and occlusions. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*. IEEE/CVF, New York, 872–881.

[69] Wenda Li, Bo Tan, and Robert J Piechocki. 2016. Non-contact breathing detection using passive radar. In *2016 IEEE International Conference on Communications (ICC)*. IEEE, IEEE, New York, 1–6.

[70] Zhuqi Li, Yaxiong Xie, Longfei Shangguan, Rotman Ivan Zelaya, Jeremy Gummeson, Wenjun Hu, and Kyle Jamieson. 2019. Towards programming the radio environment with large arrays of inexpensive antennas. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*. USENIX, Boston, 285–300.

[71] Zhengxiong Li, Zhuolin Yang, Chen Song, Changzhi Li, Zhengyu Peng, and Wenyao Xu. 2018. E-eye: Hidden electronics recognition through mmwave nonlinear effects. In *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*. ACM, New York, 68–81.

[72] Jaime Lien, Nicholas Gillian, M Emre Karagozler, Patrick Amihood, Carsten Schwesig, Erik Olson, Hakim Raja, and Ivan Poupyrev. 2016. Soli: Ubiquitous gesture sensing with millimeter wave radar. *ACM Transactions on Graphics (TOG)* 35, 4 (2016), 1–19.

[73] Haipeng Liu, Kening Cui, Kaiyuan Hu, Yuheng Wang, Anfu Zhou, Liang Liu, and Huadong Ma. 2022. mTransSee: Enabling Environment-Independent mmWave Sensing Based Gesture Recognition via Transfer Learning. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 1 (2022), 1–28.

[74] Jian Liu, Hongbo Liu, Yingying Chen, Yan Wang, and Chen Wang. 2019. Wireless sensing for human activity: A survey. *IEEE Communications Surveys & Tutorials* 22, 3 (2019), 1629–1645.

[75] Jianwei Liu, Xiang Zou, Feng Lin, Jinsong Han, Xian Xu, and Kui Ren. 2021. Hand-Key: Leveraging Multiple Hand Biometrics for Attack-Resilient User Authentication Using COTS RFID. In *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)*. IEEE, IEEE, New York, 1042–1052.

[76] Tian Liu, Ziyu Liu, Jun Huang, Rui Tan, and Zhen Tan. 2018. Detecting wireless spy cameras via stimulating and probing. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, Munich, 243–255.

[77] Zikun Liu, Gagandeep Singh, Chenren Xu, and Deepak Vasisht. 2021. FIRE: enabling reciprocity for FDD MIMO systems. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. ACM, New York, 628–641.

[78] Zikun Liu, Changming Xu, Emerson Sie, Gagandeep Singh, and Deepak Vasisht. 2023. Exploring Practical Vulnerabilities of Machine Learning-based Wireless Systems. In *20th USENIX Symposium on Networked Systems Design and Implementation (NSDI 23)*. USENIX, New York, 1801–1817.

[79] Chris Xiaoxuan Lu, Yang Li, Peijun Zhao, Changhao Chen, Linhai Xie, Hongkai Wen, Rui Tan, and Niki Trigoni. 2018. Simultaneous localization and mapping with power network electromagnetic field. In *Proceedings of the 24th annual international conference on mobile computing and networking*. ACM, New York, 607–622.

[80] Chengwen Luo, Zhongru Yang, Xingyu Feng, Jin Zhang, Hong Jia, Jianqiang Li, Jiawei Wu, and Wen Hu. 2021. RFaceID: Towards RFID-Based Facial Recognition. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 4 (2021), 1–21.

[81] Zhihong Luo, Qiping Zhang, Yunfei Ma, Manish Singh, and Fadel Adib. 2019. 3D Backscatter Localization for {Fine-Grained} Robotics. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*. ACM, New York, 765–782.

[82] Bastien Lyonnet, Cornel Ioana, and Moeness G Amin. 2010. Human gait classification using microdoppler time-frequency signal representations. In *2010 IEEE Radar Conference*. IEEE, IEEE, New York, 915–919.

[83] Bin Lyu, Dinh Thai Hoang, Shimin Gong, Dusit Niyato, and Dong In Kim. 2020. IRS-based wireless jamming attacks: When jammers can attack without power. *IEEE Wireless Communications Letters* 9, 10 (2020), 1663–1667.

[84] Yunfei Ma, Nicholas Selby, and Fadel Adib. 2017. Minding the billions: Ultra-wideband localization for deployed rfid tags. In *Proceedings of the 23rd annual international conference on mobile computing and networking*. ACM, New York, 248–260.

[85] Marwa Mamdouh, Mohamed AI Elrukhsi, and Ahmed Khattab. 2018. Securing the internet of things and wireless sensor networks via machine learning: A survey. In *2018 International Conference on Computer and Applications (ICCA)*. IEEE, IEEE, New York, 215–218.

[86] Julio César Manco Vásquez, Jesús María Ibáñez Díaz, Javier Vía Rodríguez, Luis Ignacio Santamaría Caballero, et al. 2015. Detection of radio receivers: an experimental evaluation approach. *Thesis* 5, 4 (2015), 417–426.

[87] David McGlynn and Michael G Madden. 2010. An ensemble dynamic time warping classifier with application to activity recognition. In *International Conference on Innovative Techniques and Applications of Artificial Intelligence*. Springer, Springer, New York, 339–352.

[88] Pedro Melgarejo, Xinyu Zhang, Parameswaran Ramanathan, and David Chu. 2014. Leveraging directional antenna capabilities for fine-grained gesture recognition. In *Proceedings of the 2014 ACM International Joint Conference on pervasive and ubiquitous computing*. ACM, New York, 541–551.

[89] Massimo Merenda, Giuseppe Cimino, Riccardo Carotenuto, Francesco Giuseppe Della Corte, and Demetrio Iero. 2021. Device-free hand gesture recognition exploiting Machine Learning applied to RFID. In *2021 6th International Conference on Smart and Sustainable Technologies (SpliTech)*. IEEE, IEEE, New York, 1–5.

[90] microsoft. 2022. Microsoft. Spectrum Observatory. http://observatory.microsoftspectrum.com/.

[91] Pavlo Molchanov, Shalini Gupta, Kihwan Kim, and Kari Pulli. 2015. Short-range FMCW monopulse radar for hand-gesture sensing. In *2015 IEEE Radar Conference (RadarCon)*. IEEE, IEEE, New York, 1491–1496.

[92] M Moussa and M Youssef. 2009. Smart Devices for Smart Environments: Device-free Passive Detection in Real Environments. Pervasive Computing and Communications. In *2009. PerCom 2009. IEEE International Conference on. IEEE*. IEEE, New York, 417–426.

[93] Amitav Mukherjee and A Lee Swindlehurst. 2012. Detecting passive eavesdroppers in the MIMO wiretap channel. In *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, IEEE, New York, 2809–2812.

[94] Meinard Müller. 2007. Dynamic time warping. *Information retrieval for music and motion* 5, 4 (2007), 69–84.

[95] Santosh Nannuru, Yunpeng Li, Yan Zeng, Mark Coates, and Bo Yang. 2012. Radio-frequency tomography for passive indoor multitarget tracking. *IEEE Transactions on Mobile Computing* 12, 12 (2012), 2322–2333.

[96] Sameera Palipana, David Rojas, Piyush Agrawal, and Dirk Pesch. 2018. FallDeFi: Ubiquitous fall detection using commodity Wi-Fi devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 4 (2018), 1–25.

[97] Sanghoon Park, Lawrence E Larson, and Laurence B Milstein. 2006. Hidden mobile terminal device discovery in a UWB environment. In *2006 IEEE International Conference on Ultra-Wideband*. IEEE, IEEE, New York, 417–421.

[98] Sanghoon Park, Lawrence E Larson, and Laurence B Milstein. 2010. An RF receiver detection technique for cognitive radio coexistence. *IEEE Transactions on Circuits and Systems II: Express Briefs* 57, 8 (2010), 652–656.

[99] Neal Patwari, Lara Brewer, Quinn Tate, Ossi Kaltiokallio, and Maurizio Bocca. 2013. Breathfinding: A wireless network that monitors and locates breathing in a home. *IEEE Journal of Selected Topics in Signal Processing* 8, 1 (2013), 30–42.

[100] Anindya S Paul and Eric A Wan. 2009. RSSI-based indoor localization and tracking using sigma-point Kalman smoothers. *IEEE Journal of selected topics in signal processing* 3, 5 (2009), 860–873.

[101] Mauro Piva, Gaia Maselli, and Francesco Restuccia. 2021. The tags are alright: Robust large-scale rfid clone detection through federated data-augmented radio fingerprinting. In *Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*. ACM, New York, 41–50.

[102] Qifan Pu, Sidhant Gupta, Shyamnath Gollakota, and Shwetak Patel. 2013. Whole-home gesture recognition using wireless signals. In *Proceedings of the 19th annual international conference on Mobile computing & networking*. ACM, New York, 27–38.

[103] Yue Qiao, Kannan Srinivasan, and Anish Arora. 2017. Channel spoofer: Defeating channel variability and unpredictability. In *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*. ACM, Incheon, 402–413.

[104] Yue Qiao, Ouyang Zhang, Wenjie Zhou, Kannan Srinivasan, and Anish Arora. 2016. {PhyCloak}: Obfuscating Sensing from Communication Signals. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. USENIX, Santa Clara, 685–699.

[105] Shobha Sundar Ram, Yang Li, Adrian Lin, and Hao Ling. 2008. Doppler-based detection and tracking of humans in indoor environments. *Journal of the Franklin Institute* 345, 6 (2008), 679–699.

[106] Shobha Sundar Ram and Hao Ling. 2008. Through-wall tracking of human movers using joint Doppler and array processing. *IEEE Geoscience and Remote Sensing Letters* 5, 3 (2008), 537–541.

[107] Moslem Rashidi, Kasra Haghighi, Ashkan Panahi, and Mats Viberg. 2011. A NLLS based sub-nyquist rate spectrum sensing for wideband cognitive radio. In *2011 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. IEEE, IEEE, New York, 545–551.

[108] S Salous, N Nikandrou, and NF Bajj. 1998. Digital techniques for mobile radio chirp sounders. *IEE Proceedings-Communications* 145, 3 (1998), 191–196.

[109] Sarah Ann Seguin. 2009. *Detection of low cost radio frequency receivers based on their unintended electromagnetic emissions and an active stimulation*. Missouri University of Science and Technology, Missouri.

[110] Moustafa Seifeldin, Ahmed Saeed, Ahmed E Kosba, Amr El-Keyi, and Moustafa Youssef. 2012. Nuzzer: A large-scale device-free passive localization system for wireless environments. *IEEE Transactions on Mobile Computing* 12, 7 (2012), 1321–1334.

[111] Longfei Shangguan, Zimu Zhou, and Kyle Jamieson. 2017. Enabling gesture-based interactions with objects. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, New York, 239–251.

[112] Rahul Anand Sharma, Elahe Soltanaghaei, Anthony Rowe, and Vyas Sekar. 2022. Lumos: Identifying and Localizing Diverse Hidden {IoT} Devices in an Unfamiliar Environment. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX, Boston, 1095–1112.

[113] Jayanth Shenoy, Zikun Liu, Bill Tao, Zachary Kabelac, and Deepak Vasisht. 2022. Rf-protect: privacy against device-free human tracking. In *Proceedings of the ACM SIGCOMM 2022 Conference*. ACM, New York, 588–600.

[114] Lixin Shi, Paramvir Bahl, and Dina Katabi. 2015. Beyond Sensing:{Multi-GHz} Realtime Spectrum Analytics. In *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)*. USENIX, New York, 159–172.

[115] Sunny Shrestha, Esa Irby, Raghav Thapa, and Sanchari Das. 2022. SoK: a systematic literature review of Bluetooth security threats and mitigation measures. In *International Symposium on Emerging Information Security and Applications*. Springer, Springer, New York, 108–127.

[116] Stephan Sigg, Ulf Blanke, and Gerhard Tröster. 2014. The telepathic phone: Frictionless activity recognition from wifi-rssi. In *2014 IEEE international conference*

on pervasive computing and communications (PerCom). IEEE, IEEE, New York, 148–155.

[117] Stephan Sigg, Markus Scholz, Shuyu Shi, Yusheng Ji, and Michael Beigl. 2013. RF-sensing of activities from non-cooperative subjects in device-free recognition systems using ambient and local signals. *IEEE Transactions on Mobile Computing* 13, 4 (2013), 907–920.

[118] Stephan Sigg, Shuyu Shi, Felix Buesching, Yusheng Ji, and Lars Wolf. 2013. Leveraging RF-channel fluctuation for activity recognition: Active and passive systems, continuous and RSSI-based signal features. In *Proceedings of International Conference on Advances in Mobile Computing & Multimedia*. ACM, New York, 43–52.

[119] Vijay Srinivasan, John Stankovic, and Kamin Whitehouse. 2008. Protecting your daily in-home activity information from a wireless snooping attack. In *Proceedings of the 10th international conference on Ubiquitous computing*. ACM, New York, 202–211.

[120] Paul Staat, Harald Elders-Boll, Christian Zenger, and Christof Paar. 2021. Mirror Mirror on the Wall: Next-Generation Wireless Jamming Attacks Based on Software-Controlled Surfaces. *arXiv preprint arXiv:2107.01709* 5, 4 (2021), 417–426.

[121] Paul Staat, Simon Mulzer, Stefan Roth, Veelasha Moonsamy, Markus Heinrichs, Rainer Kronberger, Aydin Sezgin, and Christof Paar. 2022. IRShield: A countermeasure against adversarial physical-layer wireless sensing. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, IEEE, San Francisco, 1705–1721.

[122] Colin Stagner, Andrew Conrad, Christopher Osterwise, Daryl G Beetner, and Steven Grant. 2011. A practical superheterodyne-receiver detector using stimulated emissions. *IEEE Transactions on Instrumentation and Measurement* 60, 4 (2011), 1461–1468.

[123] Colin Stagner, Matthew Halligan, Christopher Osterwise, Daryl G Beetner, and Steven L Grant. 2012. Locating noncooperative radio receivers using wideband stimulated emissions. *IEEE Transactions on Instrumentation and Measurement* 62, 3 (2012), 667–674.

[124] Colin Blake Stagner. 2013. *Detecting and locating electronic devices using their unintended electromagnetic emissions*. Missouri University of Science and Technology, Missouri.

[125] Wei Sun. 2020. Destructive full duplex relay for commodity rfid system. In *2020 IEEE International Conference on RFID (RFID)*. IEEE, IEEE, New York, 1–8.

[126] Wei Sun. 2021. Destructive and constructive full duplex relaying for commodity rfid system. *IEEE Journal of Radio Frequency Identification* 5, 4 (2021), 417–426.

[127] Wei Sun. 2021. Orientation-Aware RFID-Based Sensing. In *2021 IEEE International Conference on RFID Technology and Applications (RFID-TA)*. IEEE, IEEE, New York, 52–54.

[128] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, and Rob Fergus. 2013. Intriguing properties of neural networks. *arXiv preprint arXiv:1312.6199* 1–2, 3–4 (2013), 211–407.

[129] Bo Tan, Karl Woodbridge, and Kevin Chetty. 2016. Awireless passive radar system for real-time through-wall movement detection. *IEEE Trans. Aerospace Electron. Systems* 52, 5 (2016), 2596–2603.

[130] Masaya Tanbo, Ryoma Nojiri, Yuusuke Kawakita, and Haruhisa Ichikawa. 2015. Active RFID attached object clustering method based on RSSI series for finding lost objects. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. IEEE, IEEE, New York, 363–368.

[131] Gineke A Ten Holt, Marcel JT Reinders, and Emile A Hendriks. 2007. Multi-dimensional dynamic time warping for gesture recognition. In *Thirteenth annual conference of the Advanced School for Computing and Imaging*, Vol. 300. ACM, New York, 1.

[132] Vivek Thotla, Mohammad Tayeb Ahmad Ghasr, Maciej J Zawodniok, Sarangapani Jagannathan, and Sanjeev Agarwal. 2013. Detection of super-regenerative receivers using hurst parameter. *IEEE Transactions on Instrumentation and Measurement* 62, 11 (2013), 3006–3014.

[133] Ipsit V Vahia, Zachary Kabelac, Chen-Yu Hsu, Brent P Forester, Patrick Monette, Rose May, Katherine Hobbs, Usman Munir, Kreshnik Hoti, and Dina Katabi. 2020. Radio signal sensing and signal processing to monitor behavioral symptoms in dementia: a case study. *The American Journal of Geriatric Psychiatry* 28, 8 (2020), 820–825.

[134] Deepak Vasisht, Anubhav Jain, Chen-Yu Hsu, Zachary Kabelac, and Dina Katabi. 2018. Duet: Estimating user position and identity in smart homes using intermittent and incomplete RF-data. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (2018), 1–21.

[135] Deepak Vasisht, Swarun Kumar, and Dina Katabi. 2016. {Decimeter-Level} Localization with a Single {WiFi} Access Point. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. USENIX, New York, 165–178.

[136] Deepak Vasisht, Swarun Kumar, Hariharan Rahul, and Dina Katabi. 2016. Eliminating channel feedback in next-generation cellular networks. In *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM, New York, 398–411.

[137] Aditya Virmani and Muhammad Shahzad. 2017. Position and orientation agnostic gesture recognition using wifi. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, New York, 252–264.

[138] Fu-Kang Wang, Tzyy-Sheng Horng, Kang-Chun Peng, Je-Kuan Jau, Jian-Yu Li, and Cheng-Chung Chen. 2011. Single-antenna Doppler radars using self and mutual injection locking for vital sign detection with random body movement cancellation. *IEEE Transactions on Microwave Theory and Techniques* 59, 12 (2011), 3577–3587.

[139] Hao Wang, Daqing Zhang, Yasha Wang, Junyi Ma, Yuxiang Wang, and Shengjie Li. 2016. RT-Fall: A real-time and contactless fall detection system with commodity WiFi devices. *IEEE Transactions on Mobile Computing* 16, 2 (2016), 511–526.

[140] Jie Wang, Qinghua Gao, Yan Yu, Peng Cheng, Lifei Wu, and Hongyu Wang. 2012. Robust device-free wireless localization based on differential RSS measurements. *IEEE transactions on industrial electronics* 60, 12 (2012), 5943–5952.

[141] Jue Wang and Dina Katabi. 2013. Dude, where's my card? RFID positioning that works with multipath and non-line of sight. In *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*. ACM, New York, 51–62.

[142] Jue Wang, Deepak Vasisht, and Dina Katabi. 2014. RF-IDraw: Virtual touch screen in the air using RF signals. *ACM SIGCOMM Computer Communication Review* 44, 4 (2014), 235–246.

[143] Jingxian Wang, Junbo Zhang, Rajarshi Saha, Haojian Jin, and Swarun Kumar. 2019. Pushing the Range Limits of Commercial Passive {RFIDs}. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*. USENIX, New York, 301–316.

[144] Ning Wang, Pu Wang, Amir Alipour-Fanid, Long Jiao, and Kai Zeng. 2019. Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. *IEEE Internet of Things Journal* 6, 5 (2019), 8169–8181.

[145] Wei Wang, Alex X Liu, Muhammad Shahzad, Kang Ling, and Sanglu Lu. 2015. Understanding and modeling of wifi signal based human activity recognition. In *Proceedings of the 21st annual international conference on mobile computing and networking*. ACM, New York, 65–76.

[146] Wei Wang, Alex X Liu, Muhammad Shahzad, Kang Ling, and Sanglu Lu. 2017. Device-free human activity recognition using commercial WiFi devices. *IEEE Journal on Selected Areas in Communications* 35, 5 (2017), 1118–1131.

[147] Yan Wang, Jian Liu, Yingying Chen, Marco Gruteser, Jie Yang, and Hongbo Liu. 2014. E-eyes: device-free location-oriented activity identification using fine-grained wifi signatures. In *Proceedings of the 20th annual international conference on Mobile computing and networking*. ACM, New York, 617–628.

[148] Yuxi Wang, Kaishun Wu, and Lionel M Ni. 2016. Wifall: Device-free fall detection by wireless networks. *IEEE Transactions on Mobile Computing* 16, 2 (2016), 581–594.

[149] Pruthuvi Maheshakya Wijewardena, Aditya Bhaskara, Sneha Kumar Kasera, Syed Ayaz Mahmud, and Neal Patwari. 2020. A plug-n-play game theoretic framework for defending against radio window attacks. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, New York, 284–294.

[150] Ben Wild and Kannan Ramchandran. 2005. Detecting primary receivers for cognitive radio applications. In *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.* IEEE, IEEE, New York, 124–130.

[151] Joey Wilson and Neal Patwari. 2010. See-through walls: Motion tracking using variance-based radio tomography networks. *IEEE Transactions on Mobile Computing* 10, 5 (2010), 612–621.

[152] Joost F Wolfswinkel, Elfi Furtmueller, and Celeste PM Wilderom. 2013. Using grounded theory as a method for rigorously reviewing literature. *European journal of information systems* 22, 1 (2013), 45–55.

[153] Wei Xi, Jizhong Zhao, Xiang-Yang Li, Kun Zhao, Shaojie Tang, Xue Liu, and Zhiping Jiang. 2014. Electronic frog eye: Counting crowd using WiFi. In *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*. IEEE, IEEE, New York, 361–369.

[154] Yaxiong Xie, Mo Li, and Yaxiong Xie. 2023. Atheros CSI Tool. https://wands.sg/research/wifi/AtherosCSI/.

[155] Yaxiong Xie, Jie Xiong, Mo Li, and Kyle Jamieson. 2019. mD-Track: Leveraging multi-dimensionality for passive indoor Wi-Fi tracking. In *The 25th Annual International Conference on Mobile Computing and Networking*. ACM, New York, 1–16.

[156] Xi Xiong, Justin Chan, Ethan Yu, Nisha Kumari, Ardalan Amiri Sani, Changxi Zheng, and Xia Zhou. 2017. Customizing indoor wireless coverage via 3D-fabricated reflectors. In *Proceedings of the 4th ACM International Conference on Systems for Energy-Efficient Built Environments*. ACM, Delft, 1–10.

[157] Chenren Xu, Bernhard Firner, Robert S Moore, Yanyong Zhang, Wade Trappe, Richard Howard, Feixiong Zhang, and Ning An. 2013. SCPL: Indoor device-free multi-subject counting and localization using radio signal strength. In *Proceedings of the 12th international conference on Information Processing in Sensor Networks*. ACM, New York, 79–90.

[158] Huatao Xu, Dong Wang, Run Zhao, and Qian Zhang. 2019. FaHo: deep learning enhanced holographic localization for RFID tags. In *Proceedings of the 17th Conference on Embedded Networked Sensor Systems*. ACM, New York, 351–363.

[159] Lei Yang, Qiongzheng Lin, Xiangyang Li, Tianci Liu, and Yunhao Liu. 2015. See through walls with COTS RFID system!. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, New York, 487–499.

[160] Chia-Yi Yeh, Yasaman Ghasempour, Yasith Amarasinghe, Daniel M Mittleman, and Edward W Knightly. 2020. Security in terahertz WLANs with Leaky wave antennas. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, New York, 317–327.

[161] Simon Yiu, Marzieh Dashti, Holger Claussen, and Fernando Perez-Cruz. 2017. Wireless RSSI fingerprinting localization. *SignBbbkal Processing* 131 (2017), 235–244.

[162] Moustafa Youssef, Matthew Mah, and Ashok Agrawala. 2007. Challenges: device-free passive localization for wireless environments. In *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*. ACM, New York, 222–229.

[163] Hongli Yu, Bin Yang, Jinjun Liu, and Gwo-Jong Yu. 2018. Passive human trajectory tracking study in indoor environment with CSI. In *2018 International Conference on Networking and Network Applications (NaNA)*. IEEE, IEEE, New York, 372–377.

[164] Jih-Tsun Yu, Li Yen, and Po-Hsuan Tseng. 2020. mmWave radar-based hand gesture recognition using range-angle image. In *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*. IEEE, IEEE, New York, 1–5.

[165] Shichao Yue, Hao He, Hao Wang, Hariharan Rahul, and Dina Katabi. 2018. Extracting multi-person respiration from entangled RF signals. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (2018), 1–22.

[166] Shichao Yue, Yuzhe Yang, Hao Wang, Hariharan Rahul, and Dina Katabi. 2020. BodyCompass: Monitoring sleep posture with wireless signals. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 2 (2020), 1–25.

[167] R Ivan Zelaya, William Sussman, Jeremy Gummeson, Kyle Jamieson, and Wenjun Hu. 2021. LAVA: fine-grained 3D indoor wireless coverage for small IoT devices. In *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*. ACM, Virtual, 123–136.

[168] Daqiang Zhang, Jingyu Zhou, Minyi Guo, Jiannong Cao, and Tianbao Li. 2010. TASA: Tag-free activity sensing using RFID tag arrays. *IEEE Transactions on Parallel and Distributed Systems* 22, 4 (2010), 558–570.

[169] Fusang Zhang, Kai Niu, Jie Xiong, Beihong Jin, Tao Gu, Yuhang Jiang, and Daqing Zhang. 2019. Towards a diffraction-based sensing approach on human activity recognition. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 1 (2019), 1–25.

[170] Ouyang Zhang and Kannan Srinivasan. 2016. Mudra: User-friendly fine-grained gesture recognition using WiFi signals. In *Proceedings of the 12th International on Conference on emerging Networking EXperiments and Technologies*. ACM, New York, 83–96.

[171] Heng Zhao, Hong Hong, Li Sun, Yusheng Li, Changzhi Li, and Xiaohua Zhu. 2017. Noncontact physiological dynamics detection using low-power digital-IF Doppler radar. *IEEE Transactions on Instrumentation and Measurement* 66, 7 (2017), 1780–1788.

[172] Mingmin Zhao, Fadel Adib, and Dina Katabi. 2016. Emotion recognition using wireless signals. In *Proceedings of the 22nd annual international conference on mobile computing and networking*. ACM, New York, 95–108.

[173] Mingmin Zhao, Tianhong Li, Mohammad Abu Alsheikh, Yonglong Tian, Hang Zhao, Antonio Torralba, and Dina Katabi. 2018. Through-wall human pose estimation using radio signals. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. IEEE, New York, 7356–7365.

[174] Mingmin Zhao, Yingcheng Liu, Aniruddh Raghu, Tianhong Li, Hang Zhao, Antonio Torralba, and Dina Katabi. 2019. Through-wall human mesh recovery using radio signals. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*. IEEE/CVF, New York, 10113–10122.

[175] Mingmin Zhao, Yonglong Tian, Hang Zhao, Mohammad Abu Alsheikh, Tianhong Li, Rumen Hristov, Zachary Kabelac, Dina Katabi, and Antonio Torralba. 2018. RF-based 3D skeletons. In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*. ACM, New York, 267–281.

[176] Mingmin Zhao, Shichao Yue, Dina Katabi, Tommi S Jaakkola, and Matt T Bianchi. 2017. Learning sleep stages from radio signals: A conditional adversarial architecture. In *International Conference on Machine Learning*. PMLR, PMLR, New York, 4100–4109.

[177] Yuxuan Zhou, Huangxun Chen, Chenyu Huang, and Qian Zhang. 2022. WiADv: Practical and robust adversarial attack against WiFi-based gesture recognition system. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 2 (2022), 1–25.

[178] Yanzi Zhu, Zhujun Xiao, Yuxin Chen, Zhijing Li, Max Liu, Ben Y Zhao, and Haitao Zheng. 2020. Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors. In *Network and Distributed Systems Security (NDSS) Symposium 2020*. ISOC, New York, 1–12.