2025 International Conference on Computing, Networking and Communications (ICNC) | 979-8-3315-2096-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICNC64010.2025.10993984

Secure-IRS: Defending Against Adversarial Physical-Layer Sensing in ISAC System

Ziyu Chen, Denny V Landika, Alvin Yang, Yizhu Wen, Haofan Cai, Yao Zheng, Hanqing Guo
University of Hawai'i at Mānoa, USA
Email: {ziyu89, dennyvp, ayang27, yizhuw, haofanc, yaozheng, guohanqi}@hawaii.edu

***Abstract*—Integrated Sensing and Communication (ISAC) systems have emerged as a key technology in 5G and 6G networks, enabling the simultaneous use of sensing and communication within the same frequency band. A major advancement in this field is the incorporation of Intelligent Reflecting Surfaces (IRS), which enhances signal coverage and strength by adjusting the reflection angle and strength of beamforming signals. While IRS technology improves wireless propagation environments and sensing accuracy, it also introduces new security challenges, particularly in adversarial wireless sensing scenarios. In this paper, we propose a novel countermeasure against adversarial sensing on the physical layer by introducing a randomized phase increment in the IRS placement, disrupting sensing accuracy. We systematically design this countermeasure, provide theoretical validation, and conduct real-world experiments with 8 groups of settings and 80 trials to demonstrate its effectiveness. Our results show that our countermeasure can greatly reduce privacy leakage by reducing 100% attack success rate, making the adversary to obtain the real indicator of the user in the ISAC scenario.**

***Index Terms*—Integrated Sensing and Communication (ISAC), Intelligent Reflecting Surfaces (IRS), Wireless Physiological Sensing, Adversarial Sensing**

I. Introduction

Integrated Sensing and Communication (ISAC) systems have gained significant attention as they combine sensing and communication into an integrated wireless setup. With the advancements in 5G and 6G technologies, particularly the availability of larger bandwidths, ISAC systems can simultaneously support both sensing and communication functions within the same frequency band, providing improved efficiency and resource utilization [1]. One key innovation driving the enhancement of ISAC systems is the incorporation of Intelligent Reflecting Surfaces (IRS). The IRS primarily changes the reflection strength and angle of the beamforming signal to improve signal coverage and strength. It involves a planar surface composed of numerous passive reflecting elements, each independently controls the amplitude and phase of incoming signals. By manipulating these signals, IRS can optimize wireless propagation environments, significantly improving sensing accuracy and communication performance [2]. This innovation enhances the detection of the Channel State Information (CSI) by improving the quality of signal reflection and ultimately enabling better sensing in scenarios where direct Line-of-Sight (LoS) communication is not feasible. Additionally, IRS technology presents an opportunity to improve spatial efficiency, especially in overcoming challenges related to signal attenuation over long distances or in environments with obstacles. IRS can create virtual LoS links by reflecting impinging radio signals, thus compensating for power loss and enhancing signal coverage [3]. Sensibility and communication can be enabled in the None Line-of-Sight (NLoS) scenario when adapting IRS in ISAC systems.

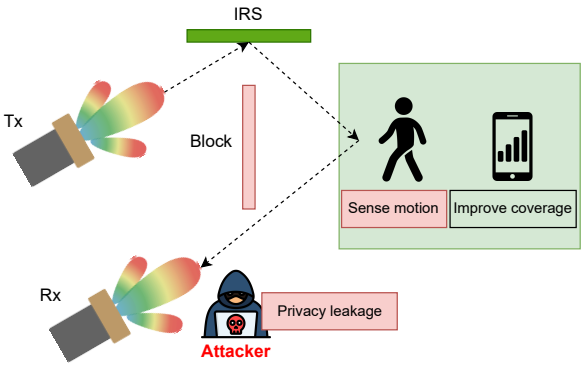


Fig. 1. An ISAC system can use an IRS to sense the user motion and provide communication signal coverage, however, the attacker can also exploit the IRS to sense the user's private sensing data and cause privacy leakage problem.

Despite these technical advantages, using the IRS in ISAC systems introduces new challenges, particularly regarding privacy and security. Radio Frequency (RF) sensing systems, even without the IRS, are capable of detecting and tracking individuals' movements without the need of a specific device. This capability is further amplified by the introduction of IRS, which improves the accuracy and range of such sensing systems. For example, as shown in Figure 1, an adversary could potentially use IRS-enhanced sensing to track the occupancy of a home by detecting signals reflected from human bodies, such as breathing patterns, even through walls. Such unauthorized surveillance could be exploited by malicious actors, such as burglars identifying when homes are empty or corporations gathering behavioral data for commercial purposes [4].

Moreover, traditional countermeasures on RF sensing, such as signal jamming or attenuation, are often ineffective or impractical in the context of ISAC systems. Jamming requires a significant amount of power and is subject to regulatory restrictions, while attenuation methods, such as increasing the distance between transmitters and receivers or applying RF shielding, can limit the functionality of legitimate communication systems. Additionally, because the human body naturally reflects radio signals, it is almost impossible to fully prevent such signals from being used for unauthorized sensing [4]. These limitations highlight the need for new, more effective methods to counter adversarial sensing in IRS-enabled ISAC systems.

In this paper, we aim to evaluate the effect of the IRS on ISAC. We propose an effective countermeasure against adver-

sarial wireless sensing on the physical layer, which not only is simpler but also overcomes the shortcomings of previous approaches. The key idea of our countermeasure is introducing a randomness phase change in the IRS placement, therefore affecting the sensing accuracy. More specifically, we propose a systematic design to theoretically validate the effectiveness of our countermeasure. Then, we conduct real-world experiments with 8 groups of settings and 80 experiments to demonstrate the practical effectiveness of our design.

II. Background

A. Wireless Sensing and ISAC

Wireless sensing technologies have evolved significantly in recent years, enabling a wide range of applications, including human activity recognition and health monitoring. The key idea of wireless sensing is to extract the CSI between the transmitter and the receiver, which can be used to induce human behaviors or biological information. For instance, [5], [6] demonstrated the use of radar to monitor vital signs without physical contact, highlighting the potential of wireless sensing for healthcare applications. Similarly, [7]–[10] explore the use of deep learning combined with wireless signals to accurately recognize various human activities in real-time. While traditional wireless sensing focuses on specific sensing tasks, ISAC has emerged as a concept that combines sensing and communication functionalities within a single framework. ISAC systems leverage the same frequency bands for both communication and sensing tasks, which improves spectral efficiency and reduces hardware costs [2]. This dual functionality is particularly appealing in the context of 5G and 6G networks, where bandwidth efficiency and real-time responsiveness are crucial.

B. Implementation of IRS in ISAC

The IRS have emerged as a critical technology to enhance both communication coverage and sensing granularity, particularly in wireless systems utilizing millimeter-wave (mmWave) frequencies. IRS can dynamically reflect and steer wireless signals, creating virtual LoS links even in NLoS environments, which is especially valuable for next-generation technologies, which, despite offering high-resolution sensing, suffer from limited range and signal degradation in the presence of obstacles. Recently, the interplay between IRS and ISAC systems has been comprehensively explored. [11] introduced beamforming techniques at ISAC base stations, using IRS to forge new channels that boost sensing metrics without compromising communication. Similarly, [12] investigated the use of passive IRS in sub-6GHz wireless sensing, and [11] also introduced a hybrid IRS model that blends active and passive elements to enhance both radar and communication, focusing on maximizing target illumination in adverse conditions.

C. Attacks and Countermeasures on Wireless Sensing

While combining communication with sensing is promising, people started to worry about the privacy risks. For example, adversaries such as neighbors or eavesdroppers can utilize Radio Frequency (RF) devices to track occupancy in a home and even sense the victim's physiological movements and health condition [4]. This creates serious privacy concerns, as unauthorized individuals could infer sensitive information like daily routines, sleep patterns, or even medical conditions, potentially leading to surveillance, identity theft, or physical threats. To defend against such attack, previous work suggested jamming the sensing signal [13], however, this approach may also affect the communication channel and therefore not suitable for the ISAC system. Another idea of countermeasure is generating fake/ghost human data points by deploying a neural network and a reflector [4]. However, although their design can successfully mislead the attacker, the approach is somewhat bulky as it requires additional hardware, making it infeasible. Similarly, [14], [15] proposed using IRS systems to defend against eavesdropping by creating virtual sensing links, however, those approaches either require expensive devices (programmable IRS [15]) or via computation-heavy algorithm, for example, re-design the sensing signal [14].

III. Threat Model

In this work, we consider a room equipped with an IRS and an ISAC system operating at mmWave frequencies, providing both communication and health monitoring services. The primary function of this system is to sense physiological data, such as human respiration and heart rate, while also facilitating communication.

The adversary's goal, in this scenario, is to infer sensitive human physiological data, such as respiration patterns. We assume that the adversary possesses the technical capabilities to intercept and analyze mmWave signals. The adversary could either hack into a legitimate receiver, gain access to the ISAC system's channel estimations, or deploy a receiver to eavesdrop on the mmWave signals reflected by the IRS. Importantly, the adversary is not physically present inside the monitored environment but can position her receiver outside the perimeter in public or concealed locations. Additionally, we assume the adversary cannot decrypt secured communication payloads but can exploit the physical layer information derived from the mmWave signal's reflections, particularly the CSI, to infer physiological data. The legitimate owner (the defender) of the space has control over the placement of IRS and the ISAC devices, but the system is vulnerable to adversarial sensing through the adversary's interception of the wireless signals.

IV. System Design

In this section, we introduce the design of our countermeasure. First, we explain the motion detection principle using CSI. Next, we integrate IRS into the system to examine how it affects the CSI data and improves sensing accuracy. Finally, we present our countermeasure designed to prevent adversaries from exploiting IRS to eavesdrop on users' physiological data.

A. Motion Detection by CSI

In our design, the Transmitter (Tx) and Receiver (Rx) use OFDM sub-carrier to detect human motion from CSI. Specifically, CSI is determined by a process where the Tx first shares a predefined reference signal, known to both the Tx and Rx, as part of the communication protocol. The Tx then transmits this reference signal over the wireless channel, where it is affected by environmental factors such as reflection, scattering, and multipath propagation. The receiver captures

this altered version of the signal. Since the Rx knows the original reference signal, it compares the received signal to the reference to determine how the channel has modified the signal in terms of amplitude and phase. In our OFDM setting, the Rx computes the CSI for each sub-carrier, and CSI can be formulated as follows:

$$h_i(t) = |h_i(t)|e^{j\theta_i(t)} \tag{1}$$

where $|h_i(t)|$ represents the amplitude, and $\theta_i(t)$ is the phase of the channel response at sub-carrier i over time t. When a person breathes, the periodic movement alters the distance between the Tx and Rx, causing cyclical variations in both $|h_i(t)|$ and $\theta_i(t)$. These variations are captured as changes in the CSI values over time. The respiration rate can then be determined by analyzing these periodic changes. For example, applying a frequency analysis, such as a Fast Fourier Transform (FFT), to the time series of $|h_i(t)|$ or $\theta_i(t)$ will reveal a dominant frequency f_r, which corresponds to the respiration rate. Specially, we apply FFT to $|h_i(t)|$ to obtain $H_i(f) = \text{FFT}(|h_i(t)|)$, where $H_i(f)$ represents the frequency domain CSI amplitude. The dominant frequency, f_a, is then determined by the amplitude of CSI as

$$f_a = \arg\max_f (|H_i(f)|) \tag{2}$$

Alternatively, we can also infer the respiration rate through the phase information as follows:

$$f_p = \arg\max_f (\theta_i(t)) \tag{3}$$

where f_p indicates the sensed respiration rate via phase.

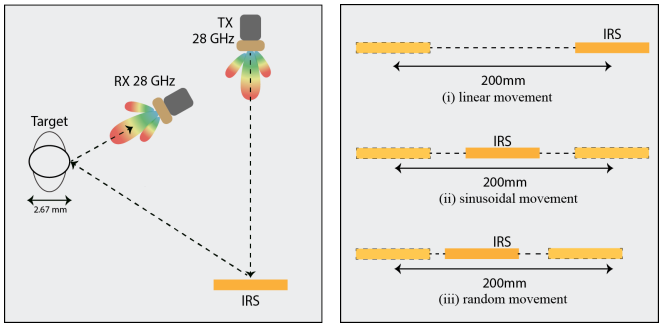
The choice between using amplitude or phase for determining respiration rate depends on the environment. Amplitude is more stable in environments with minimal reflections, making it ideal for detecting distinct chest movements. Phase, being more sensitive to small displacements, is better suited for environments with strong multipath effects. In our setting, we use both amplitude and phase to determine the respiration rate.

B. Motion Detection by CSI with IRS

IRS operates by using a surface of passive reflecting elements that can adjust the phase and amplitude of the incident electromagnetic waves. Each element of the IRS is capable of controlling the reflection of the signal by modifying the phase shift applied to the incoming wave. The IRS modifies the beam direction by adjusting the phase shift of each element, allowing the reflected signal to be steered toward a desired direction. The phase shift for the k-th element of the IRS is:

$$\theta_k = \theta_{\text{IRS}} + k\Delta\theta \tag{4}$$

where θ_{IRS} is the base phase shift applied to the first element, k is the index of the element, and $\Delta\theta$ is the incremental phase shift between adjacent elements. By tuning the phase shift of each element, the IRS can control the direction of the reflected wave, effectively steering the beam toward a desired target or area. This allows the system to create a virtual LoS path even in NLOS scenarios.



(a) Experimental Setup with an IRS (b) Setup of different IRS movements

Fig. 2. System setup and proposed defense

When combining IRS with motion detection using CSI, the system benefits from both direct path CSI and IRS-enhanced path CSI. The total CSI in this scenario is the sum of the contributions from the direct path, $h_{i,d}(t)$, and the IRS-reflected path, $h_{i,\text{IRS}}(t)$. The CSI at the i-th sub-carrier can be expressed as:

$$h_i(t) = h_{i,d}(t) + h_{i,\text{IRS}}(t) \tag{5}$$

The dynamic path contribution $h_{i,IRS}(t)$ is influenced by the IRS phase shifts, which can be expressed as:

$$h_{i,\text{IRS}}(t) = \sum_{k=1}^{N} \frac{\lambda_i}{d_k(t)} e^{-j\frac{2\pi d_k(t)}{\lambda_i} + j\theta_k} \tag{6}$$

where $d_k(t)$ is the length of the reflected path via the k-th IRS element, λ_i is the wavelength at the i-th sub-carrier, and θ_k is the phase shift introduced by the k-th IRS element. This formulation captures the total impact of the IRS on the signal received at sub-carrier i, accounting for both the physical path length and the phase control applied by each IRS element. In this scenario, since $|h_{i,\text{IRS}}| \gg |h_{i,d}|$, the respiration rate would be calculated by $h_{i,\text{IRS}}(t)$, as shown in Eq. 2 and Eq. 3.

C. Countermeasure of the Evadropping Attack

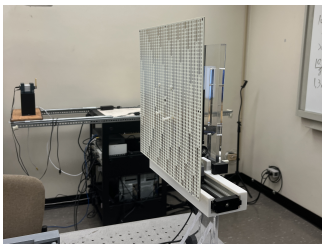
In response to the threat of eavesdropping attacks where an attacker may exploit the IRS to monitor sensitive information, the user is driven to design countermeasures. Existing studies, such as IRShield [15], address this by introducing randomness into CSI through dynamic phase adjustments for each IRS element. While effective, this approach requires a programmable IRS, which can be expensive and complex to implement in practice. Motivated by this approach, we wonder if there is a simpler way to disrupt sensing accuracy by slightly modifying the IRS channel. The answer is yes. Instead of dynamically programming each element, we propose *moving the IRS itself*, which causes changes in $d_k(t)$, the distance of the reflected path from each IRS element. As a result, both the amplitude and phase of CSI $h_{i,\text{IRS}}(t)$ are modified, based on the Eq. 6. If the IRS movement is continuous and unpredictable, the resulting changes in CSI will cause inaccuracies in the attacker's sensing results, as the calculated frequency will not solely reflect the user's respiration movements but will also be influenced by the IRS's movement. This simple yet effective approach introduces unpredictability into the channel, thereby degrading the accuracy of eavesdropping attempts. Fig. 2(a)

shows the system design with IRS, the dotted line indicates the IRS-enhanced path. To find whether a moving IRS can hamper the sensing capabilities or not compared to a static IRS, we apply three kinds of movements to the IRS. Fig. 2(b) shows the three variations of our setup: The IRS does a linear movement, sinusoidal movement, and random movement. In the next section, we will present the real-world experiment and evaluate how our defense performs under different setups.

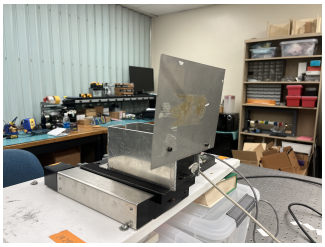
V. Experiment

A. Experiment Setup

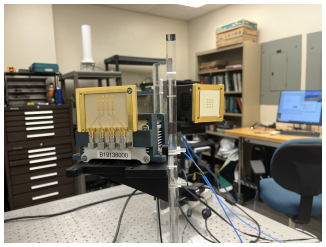
(a) Experimental Setup with an IRS



(b) XRifle IRS and the mover



(c) Target and the linear mover



(d) Transmitter and receiver

Fig. 3. Experimental setup and its key components

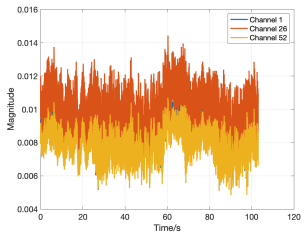
Hardwares: We set up our experiment with two Ettus N210 USRPs. One USRP is connected to a TMYTEK UDBox converter to upconvert the signal to 28 GHz, which is transmitted using a phased array antenna (TMYTEK BBox One) as the transmitter (Tx). The other USRP is connected to another phased array antenna (TMYTEK BBox Lite) to serve as the receiver (Rx). The Tx sends an OFDM signal with 52 pilot subcarriers and 128 data subcarriers at a sample rate of 625 Hz. The signal is directed toward a passive IRS (TMYTEK XRifle ES0060), which has a 51 × 51 element array operating at 26-30 GHz, an incidence angle of 0°, and a reflection angle of 60°. The IRS is mounted on a Zaber X-LHM200A motorized linear stage to enable precise movements.

We use a metal plate mounted on a Grifin Motion LNS-100 Series Linear Stage with a Galil DMC30010 mover to simulate the user's respiration movement and serve as a target. The target oscillates at 0.3 Hz to mimic typical breathing rates. The distances between devices are Tx-IRS (80.2 cm, 0°), IRS-Target (75.4 cm, 60°), and Target-Rx (34.4 cm, 60°). The detailed setup can be found in Fig. 3.

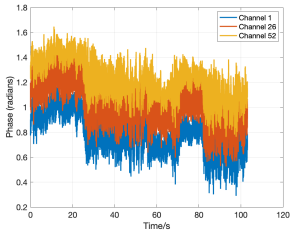
Metric Design: We measure our countermeasure performance with two metrics, **Detection Error Rate** (DER) and **Attack Success Rate** (ASR):

$$\text{DER} = \frac{|\hat{x} - \text{GT}|}{\text{GT}}, \quad \hat{x} \in \{f_a, f_p\} \tag{7}$$

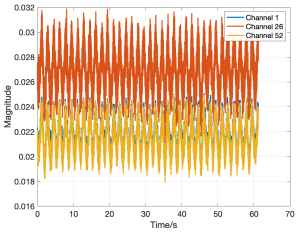
The DER measures the error rate between the attacker sensed respiration rate and the ground truth respiration rate, where $\hat{x}$ is the attacker's sensed respiration frequency, it can be derived from either amplitude(f_a) or phase(f_p) of CSI. The GT is the ground truth frequency of the target, which was set as 0.3Hz.



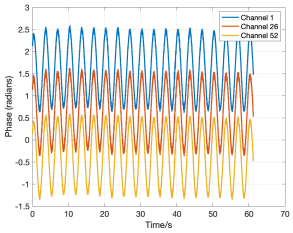
(a) Magnitude, no IRS



(b) Phase, no IRS



(c) Magnitude, static IRS



(d) Phase, static IRS

Fig. 4. The magnitude and phase of CSI

We also design another metric:

$$\text{ASR} = \left(\frac{\sum_{i=1}^{N} \mathbb{I}(\text{DER}_i \leq 0.1)}{N} \right) \tag{8}$$

where N is the total number of experiments, DER_i is the DER for the i-th test case. The $\mathbb{I}$ is an indicator function. We treat it as a successful attack if the DER equals to or less than 0.1. The summation counts the number of successful attacks, and then dividing this sum by N gives the proportion of ASR.

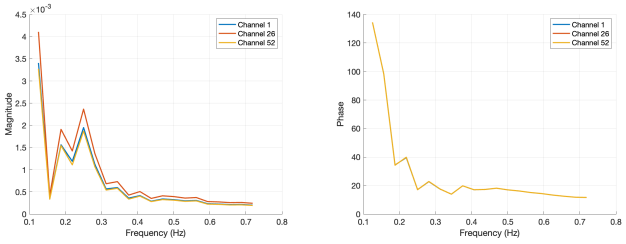
B. IRS Improves the Sensing Accuracy

We first experiment on the static IRS scenario, to observe whether the sensing capability is enhanced in the NLoS setting. Specifically, we select channel 1, 26, and 52 to capture the comprehensive sensing result across the entire frequency band. From Fig. 4, we observe that the setup with an IRS has a significantly higher amplitude (0.032) than the one without theIRS (0.012), and the waveform is much clearer than the one without the IRS both in magnitude plots and phase plots, showing that the IRS can significantly improve coverage and enhance the performance of sensing.

We then apply the fast Fourier transform (FFT) to the data. We found that for the static IRS case, the sensed frequency is close to 0.3 and has DER as low as 0, whereas the no-IRS case has a higher DER.

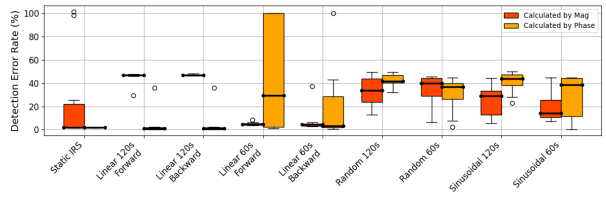
C. Effect of Our Countermeasure

Next, we apply movement to the IRS as illustrated in Fig. 2(b). We consider three distinct motion types: linear, sinusoidal, and random. For the linear motion, we further divide the experiments into forward and backward movements. Each motion type is tested over two time durations: 60 seconds and 120 seconds. To ensure the robustness of the results, we repeat each setup 10 times. Fig. 6 shows the FFT result of CSI when the IRS is moved randomly. It can be observed

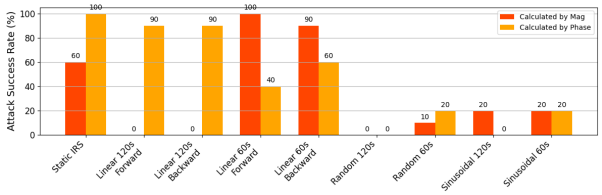


(a) Random move IRS (Mag) (b) Random move IRS (Phase)

Fig. 5. The magnitude and phase FFT plots



(a) DER of different countermeasures



(b) ASR of different countermeasures

Fig. 6. The performance of our countermeasure

that, whether decoded by magnitude or phase, the sensed respiration rate (dominant frequency) significantly deviates from the ground truth of 0.3 Hz.

We also present our result in 8 different countermeasure settings with 80 repeat experiments and plot the overall DER in a boxplot. As can be found in Fig. 6(a), in the static IRS scenario, both Mag and Phase can derive the correct target frequency, with a median DER as 0%, while the calculation by magnitude has some variance. In comparison, with the IRS movement, the DER increases significantly. In most settings, our defense can cause around 40% DER. Specifically, for the random movement, our defense makes it impossible for the eavesdropper to detect physiological data using both the magnitude and phase approaches.

To further understand the effectiveness of our countermeasure, we also calculate the ASR based on Eq. 8. We consider if the adversary can sense the respiration frequency with $> 90\%$ accuracy, then it is a successful attack. Otherwise, the defender wins as it disrupts the sensed result. We present our findings in Fig. 6(b). In the static IRS condition, the ASR is high, with 60% for magnitude and 100% for phase, note that harmonics are detected sometimes. For comparison, when the IRS is set in motion, the ASR drops significantly. For example, in the Linear 60s Forward movement, the ASR calculated by magnitude falls to 0%, while for phase, it drops to 40%. Remarkably, in the Random 120s and Sinusoidal movements, the ASR is dramatically reduced, reaching as low as 0%. These results demonstrate that our defense mechanism, which leverages IRS movement, effectively disrupts the attacker's ability to successfully eavesdrop, significantly reducing the ASR across various dynamic movement patterns.

VI. Conclusion

In this paper, we introduce a countermeasure against adversarial sensing at the physical layer by incorporating randomized distance and phase changes in the IRS. Our approach disrupts the adversary's ability to accurately sense the user's data by introducing interference in both the amplitude and phase of the CSI. Our experiments demonstrate that randomized IRS phase movement is highly effective in reducing the success rate of adversarial sensing.

VII. Acknowledgment

We would like to extend our appreciation to the anonymous reviewers for their invaluable input on our study. This work was supported in part by OAC-2417891, and Naval Information Warfare Center Pacific.

References

[1] J. Wan, H. Ren, Z. Yu, Z. Zhang, Y. Zhang, C. Pan, and J. Wang, "A framework of ris-assisted icsc user-centric based systems: Latency optimization and design," 2024. [Online]. Available: https://arxiv.org/abs/2402.13692

[2] J. Wan, H. Ren, C. Pan, Z. Yu, Z. Zhang, and Y. Zhang, "Reconfigurable intelligent surface assisted integrated sensing, communication and computation systems," *arXiv preprint arXiv:2402.13692*, 2024.

[3] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, M. Di Renzo, and N. Al-Dhahir, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE communications surveys & tutorials*, vol. 23, no. 3, pp. 1546–1577, 2021.

[4] J. Shenoy, Z. Liu, B. Tao, Z. Kabelac, and D. Vasisht, "Rf-protect: privacy against device-free human tracking," in *Proceedings of the ACM SIGCOMM 2022 Conference*, 2022, pp. 588–600.

[5] Q. Liu, H. Guo, J. Xu, H. Wang, A. Kageza, S. AlQarni, and S. Wu, "Non-contact non-invasive heart and respiration rates monitoring with mimo radar sensing," in *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2018, pp. 1–6.

[6] Z. Liang, M. Xiong, Y. Jin, J. Chen, D. Zhao, D. Yang, B. Liang, and J. Mo, "Non-contact human vital signs extraction algorithms using ir-uwb radar: A review," *Electronics*, vol. 12, no. 6, p. 1301, 2023.

[7] H. Guo, N. Zhang, S. Wu, and Q. Yang, "Deep learning driven wireless real-time human activity recognition," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–6.

[8] C. Li, M. Liu, and Z. Cao, "Wihf: Enable user identified gesture recognition with wifi," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 2020, pp. 586–595.

[9] J. Yang, X. Chen, H. Zou, C. X. Lu, D. Wang, S. Sun, and L. Xie, "Sensefi: A library and benchmark on deep-learning-empowered wifi human sensing," *Patterns*, vol. 4, no. 3, 2023.

[10] C. Li, Z. Cao, and Y. Liu, "Deep ai enabled ubiquitous wireless sensing: A survey," *ACM Computing Surveys (CSUR)*, vol. 54, no. 2, pp. 1–35, 2021.

[11] Z. Yu, X. Hu, C. Liu, M. Peng, and C. Zhong, "Location sensing and beamforming design for irs-enabled multi-user isac systems," *IEEE Transactions on Signal Processing*, vol. 70, pp. 5178–5193, 2022.

[12] D. V. P. Landika, S. Dacuycuy, and Y. Zheng, "Obstruction-free physiological motion sensing in nextg networks with intelligent reflective surfaces," in *Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation*, 2023, pp. 466–468.

[13] J. Yang, X. Guo, and Y. Li, "Design of a novel drfm jamming system based on afb-sfb," *IET International Radar Conference 2013*, 2013.

[14] M. Hua, Q. Wu, W. Chen, O. A. Dobre, and A. L. Swindlehurst, "Secure intelligent reflecting surface-aided integrated sensing and communication," *IEEE Transactions on Wireless Communications*, vol. 23, no. 1, pp. 575–591, 2023.

[15] P. Staat, S. Mulzer, S. Roth, V. Moonsamy, M. Heinrichs, R. Kronberger, A. Sezgin, and C. Paar, "Irshield: A countermeasure against adversarial physical-layer wireless sensing," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 1705–1721.