Demo: Disrupting In-Car mmWave Sensing Through IRS Manipulation

Hanqing Guo*, Dong Li†, Ruofeng Liu‡, Yao Zheng*
* *University of Hawai'i at Mānoa*
†*University of Maryland, Baltimore County*
‡*Michigan State University*

***Abstract*—Intelligent Reflecting Surfaces (IRS) have emerged as a key enabler for enhancing in-car sensing, enabling high-resolution, non-intrusive monitoring of passenger vital signs through mmWave technology. By intelligently steering wireless signals, IRS significantly improves non-line-of-sight (NLoS) detection, overcoming occlusion challenges in vehicle interiors. However, despite these advantages, IRS-based sensing introduces new security vulnerabilities that have been largely overlooked. In this study, we demonstrate that an adversary can manipulate the IRS to mislead in-car sensing results, posing a significant threat to passenger safety and system reliability. By simply modifying the IRS's movement, an attacker can cause incorrect vital sign measurements, and potential failures in safety-critical applications such as child presence detection and driver monitoring systems. To validate this threat, we design and implement four different attack scenarios, simulating various adversarial control strategies on IRS reflection parameters. Our experimental results reveal that, under optimal conditions, an attacker can achieve up to a 90% attack success rate, effectively disrupting the integrity of IRS-assisted in-car sensing systems. Our study provides the first exploration of IRS-based attacks on in-car sensing, shedding light on a novel security vulnerability in next-generation automotive technology. The demo video can be found in https://youtu.be/1VL5LiFgqTg.**

***Index Terms*—Intelligent Reflecting Surfaces (IRS), Wireless Physiological Sensing, Adversarial Attack**

1. Introduction

Intelligent Reflecting Surfaces (IRS) have become a key technology in wireless communications, enhancing signal propagation and in-car mmWave sensing for passenger vital sign monitoring. By steering wireless signals, IRS improves Non-Line-of-Sight (NLoS) detection, making it valuable for driver monitoring, child presence detection, and safety applications. However, the integration of IRS into automotive systems introduces new security vulnerabilities. IRS relies on controllable phase shifting to direct mmWave signals, making it susceptible to adversarial manipulation. Recent studies have demonstrated that adversaries can exploit these characteristics to disrupt sensing systems. For instance, Xie et al. [1] explored targeted adversarial attacks on mmWave-based human activity recognition systems, achieving high success rates in misleading the sensing outcomes. Similarly, Hunt et al. [2] introduced a black-box attack framework capable of manipulating automotive mmWave radar perceptions, effectively adding or removing objects from the vehicle's sensing data. Furthermore, security challenges in mmWave-based vehicular sensing have been extensively studied. Sun et al. [3] analyzed physical-layer security threats against mmWave-based sensing in autonomous vehicles, showing that attackers could introduce adversarial noise to disrupt sensor reliability. Meanwhile, Mensi et al. [4] compared the vulnerabilities of IRS-assisted vehicle-to-infrastructure (V2I) communication versus traditional relaying schemes, highlighting potential security weaknesses in IRS-based automotive environments. Although prior work has demonstrated successful attacks on mmWave-based sensing, none of them consider the presence of IRS in automotive environments or investigate adversarial threats in in-car sensing scenarios. To bridge this gap, we present the first study on adversarial IRS manipulation in vehicular mmWave sensing.

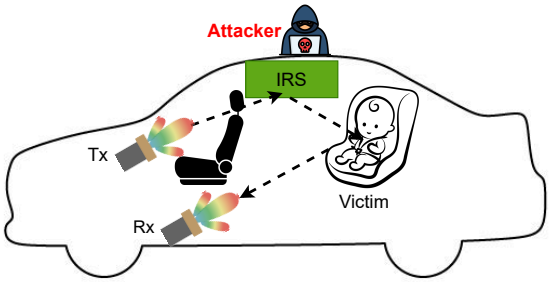


Figure 1. The attacker manipulates the IRS placed inside the vehicle to alter signal reflections, misleading the sensing system. The victim (a passenger or child in the backseat) may be falsely detected or remain undetected due to adversarial IRS control. The mmWave transmitter (Tx) and receiver (Rx) communicate under normal conditions, but adversarial IRS manipulation disrupts accurate sensing.

In this work, we demonstrate that an attacker with prior access to the IRS control system (whether through firmware modification, remote hijacking, or external IRS spoofing), can intentionally disrupt the sensing process. By strategically altering IRS reflection parameters, the attacker can induce distorted passenger monitoring data, leading to safety-critical failures.

2025 IEEE Security and Privacy Workshops (SPW) | 979-8-3315-6643-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/SPW67851.2025.00031

DOI 10.1109/SPW67851.2025.00031

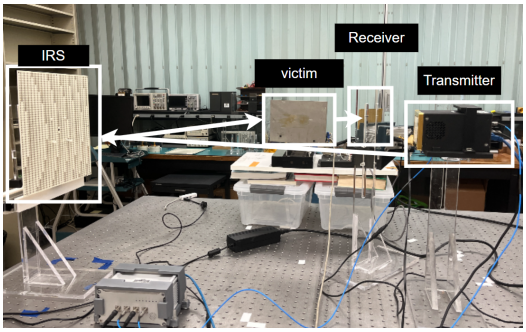


Figure 2. Experimental setup and its key components

2. Attack Design

In this section, we introduce our attack, where an adversary continuously modifies the position of the IRS to disrupt in-car mmWave sensing. Motion detection via CSI relies on extracting changes in amplitude and phase, allowing the system to track human movement and vital signs. When an IRS is introduced, it enhances sensing by steering reflections to create virtual LoS paths, improving detection accuracy in NLoS environments. However, our study reveals that continuous IRS movement alters the reflected CSI, misleading the sensing system. Specifically, shifting the IRS position modifies the reflected path length, causing unintended variations in both amplitude and phase. These distortions corrupt the extracted respiration rate and can result in false detections or misclassifications of occupant presence. We evaluate this attack under three movement patterns: linear, sinusoidal, and random IRS motion, demonstrating that even minor adjustments can significantly degrade sensing accuracy. Our results suggest that an adversary can exploit IRS mobility as a practical, low-cost method to mislead in-car sensing without requiring direct access to the mmWave transceivers.

3. Experiment

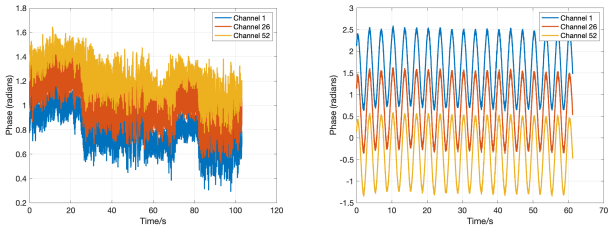
3.1. Experiment Setup

Hardwares: In Fig. 2, our setup consists of a mmWave transmitter and receiver, an IRS, and a victim, simulated by a metal plate oscillating at 0.3 Hz to mimic respiration. Detailed in Appendix C.

Metric Design: We evaluate our attack using the Attack Success Rate (ASR), defined as the fraction of cases where the attacker alters the sensed respiration rate by at least 10%. Formally,

$$\text{ASR} = \left(\sum_{i=1}^{N} \mathbb{I}(\text{Error}_i \geq 10\%) \right) / N \qquad (1)$$

where Error measures the deviation between the ground truth (GT) respiration rate and the attacked rate. Each attack setting runs for $N = 10$ trials, and ASR is computed over all attempts.



(a) Without IRS (b) With static IRS

Figure 3. The effect of IRS for Enhance Sensing

3.2. IRS Improves the Sensing Accuracy

We first evaluate the static IRS scenario to assess its impact on NLoS sensing enhancement. We select channels 1, 26, and 52 to capture results across the frequency band. As shown in Fig. 3, the IRS setup significantly improves waveform clarity, demonstrating enhanced sensing performance.

3.3. Attack Performance

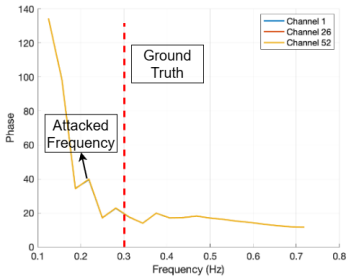


Figure 4. The attacker can manipulate the sensing result from 0.3Hz to 0.22Hz

Fig. 4 illustrates how the attacker can manipulate the sensed respiration frequency, shifting it from the ground truth of 0.3 Hz (red dashed line) to an incorrect frequency of 0.22 Hz. This suggests that IRS manipulation significantly impacts the accuracy of respiration rate detection, potentially leading to false physiological monitoring outcomes (e.g., underestimating breathing rate in medical applications).

TABLE 1. ATTACK SUCCESS RATE FOR DIFFERENT SETTINGS

Settings	Linear Fwd	Linear Bwd	Sinusoidal	Random
ASR	60%	40%	80%	90%

Table 1 shows the Attack Success Rate (ASR) for different IRS movements, revealing that random motion (90%) is the most disruptive, followed by sinusoidal motion (80%), both causing significant CSI distortions. Linear forward (60%) and backward (40%) movements are less effective, suggesting that predictable shifts are easier to compensate for. These results confirm that IRS mobility can severely degrade sensing accuracy, with dynamic, unpredictable move-

ments posing the greatest threat, emphasizing the need for countermeasures against adversarial IRS manipulation.

4. Conclusion

We demonstrate an adversarial IRS manipulation attack that disrupts mmWave-based in-car sensing by altering reflected CSI. Our results show that random IRS movement (90% ASR) is the most effective, significantly misleading respiration rate detection. Future work will explore targeted IRS attacks that manipulate specific frequency bands and adaptive countermeasures like IRS anomaly detection, phase randomization, and AI-driven filtering to enhance sensing security.

5. 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] Y. Xie, R. Jiang, X. Guo, Y. Wang, J. Cheng, and Y. Chen, "Universal targeted adversarial attacks against mmwave-based human activity recognition," *arXiv preprint arXiv:2103.05090*, 2021.

[2] D. Hunt, K. Angell, Z. Qi, T. Chen, and M. Pajic, "Madradar: A black-box physical layer attack framework on mmwave automotive fmcw radars," *arXiv preprint arXiv:2311.16024*, 2023.

[3] Z. Sun, S. Balakrishnan, L. Su, A. Bhuyan, P. Wang, and C. Qiao, "Who is in control? practical physical layer attack and defense for mmwave based sensing in autonomous vehicles," *arXiv preprint arXiv:2011.10947*, 2020.

[4] N. Mensi, D. B. Rawat, and E. Balti, "Physical layer security for v2i communications: Reflecting surfaces vs. relaying," *arXiv preprint arXiv:2010.07216*, 2020.

[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.

Appendix

Appendix A: Background

Wireless sensing has advanced significantly, enabling contactless human activity recognition and health monitoring. By extracting Channel State Information (CSI), wireless systems can infer vital signs and movements. Prior studies have leveraged radar-based sensing for non-intrusive vital sign monitoring [5], [6], while deep learning has further enhanced real-time human activity recognition using wireless signals [7]–[10]. In in-car environments, traditional wireless sensing faces severe challenges due to signal blockage and Non-Line-of-Sight (NLoS) conditions. To overcome this, Intelligent Reflecting Surfaces (IRS) have emerged as a key technology, dynamically reflecting and steering wireless signals to establish virtual Line-of-Sight (LoS) links. This capability makes IRS particularly effective for mmWave-based in-car sensing, ensuring accurate passenger detection and vital sign monitoring even in obstructed scenarios.

Appendix B: Threat Model

We consider an adversary manipulating IRS-assisted in-car sensing to mislead passenger detection and vital sign monitoring by altering IRS reflection patterns. The attacker can compromise the IRS controller via firmware tampering, remote hijacking, or malicious OTA updates. The attack assumes IRS is actively used for mmWave sensing, and the attacker has access to IRS control but not direct control over mmWave transceivers, highlighting the need for secure IRS management and anomaly detection mechanisms.

Appendix C: Hardware

Our experiment uses two Ettus N210 USRPs as the transmitter (Tx) and receiver (Rx). The Tx, connected to a TMYTEK UDBox converter, upconverts the signal to 28 GHz and transmits it via a TMYTEK BBox One phased array antenna. The Rx, equipped with a TMYTEK BBox Lite antenna, captures the signal. The OFDM transmission consists of 52 pilot subcarriers and 128 data subcarriers at 625 Hz. A passive IRS (TMYTEK XRifle ES0060, 51×51 elements, 26-30 GHz) reflects the signal at a 60° angle and is mounted on a Zaber X-LHM200A motorized linear stage for controlled movement. To simulate respiration, a metal plate on a Grifin Motion LNS-100 stage with a Galil DMC30010 mover oscillates at 0.3 Hz. Device distances are Tx-IRS (80.2 cm, 0°), IRS-Target (75.4 cm, 60°), and Target-Rx (34.4 cm, 60°).