WiFi as a Sensor: Capabilities, Challenges, and Defenses

Survey on Security and Privacy Defenses in WiFi Sensing

Supervisor: Fabian Portner

Author: Sofia Dimieva

Responsible Professor: Arash Asadi

Introduction

- **RSSI (Received Signal Strength Indicator)** – Reveals coarse presence, motion detection, and proximity changes.
- **CSI (Channel State Information)** – Enables fine-grained sensing of breathing, gestures, keystrokes, and environmental mapping.
- **AoA (Angle of Arrival)** – Allows tracking of movement direction and user localization.
- **ToF (Time of Flight)** – Provides distance estimation and trajectory inference with high precision.
- **MAC Frame Headers** – Leak device identifiers, communication patterns, and session metadata.
- **Timing Metadata** – Reveals user activity patterns and device usage routines.
- **Radiometric Fingerprints** – Enable device tracking even with MAC randomization, based on unique hardware-level imperfections.

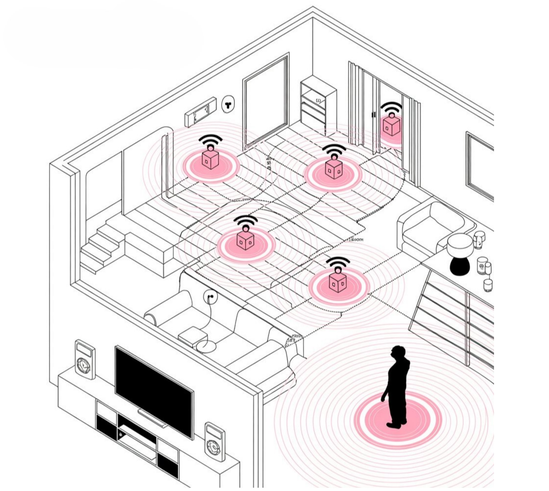


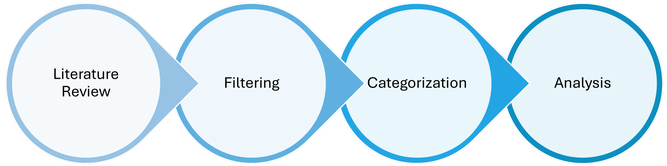
Figure 1. WiFi sensing can occur passively through walls.

Research Questions

How can WiFi sensing systems be defended against passive adversarial sensing?

- What privacy-preserving defenses exist in the literature?
- What are the assumptions, strengths, and limitations of these techniques?
- How effectively do existing defenses protect against the different signal features exploited in Wi-Fi sensing?

Methodology



Defense Taxonomy

To organize and compare existing defense strategies against unauthorized WiFi sensing, we classify them based on their core technical approach.

- This taxonomy first separates defenses that directly manipulate RF signals from those that operate at higher levels.
- **RF defenses** are further divided based on whether they alter the signal at the transmitter or through the physical environment.
- **Higher-level defenses** are split into the ones that protect protocol-level metadata—such as MAC addresses, timing, or CSI feedback—and the ones that interfere with or strengthen machine learning models used for sensing.

This structure reflects both where and how defenses operate.

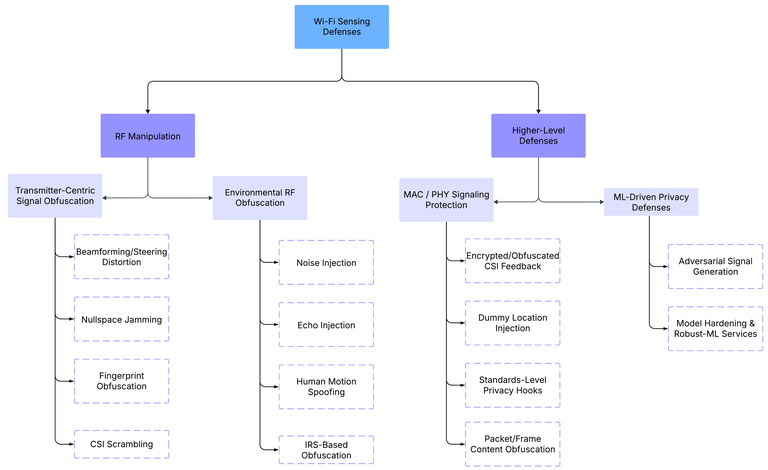


Figure 2. Defense Taxonomy

Comparative Analysis of Defense Techniques

This table summarizes each defense technique by listing its core limitations and the specific Wi-Fi signal features it helps protect. It shows how different approaches address different aspects of the sensing threat.

Defense Category	Main Limitations	Signal Features Distorted
Beamforming/Steering Distortion	Requires multi-antenna hardware; does not protect RSSI	CSI, AoA
Nullspace Jamming	Needs accurate nullspace estimation; may reduce spatial reuse	CSI
Fingerprint Obfuscation	Requires key management; may violate Wi-Fi standards	RadioID
CSI Scrambling	Custom firmware required; complex key distribution	CSI
Noise Injection	Needs external emitters; sensitive to environment and room geometry	CSI, AoA, Time
Echo Injection	Requires precise reflector placement; potential self-interference	CSI, AoA
Human Motion Spoofing	Complex to deploy; may confuse occupants	CSI, AoA
IRS-Based Obfuscation	Expensive; geometry-sensitive; attacker may adapt	CSI, AoA
Encrypted/Obfuscated CSI Feedback	Requires protocol extensions; possible compatibility issues	CSI, MAC, AoA, Timing
Dummy Location Injection	Managing believable decoys is challenging	CSI, RSSI
Standards-Level Privacy Hooks	Backward compatibility challenges; coarse-grained control	CSI
Adversarial Signal Generation	Requires model knowledge and full-duplex radios	CSI
Model Hardening	High computational cost; attacker can retrain models	CSI

Future Work

- Explore combinations of defenses across different layers to increase overall robustness.
- Developing simulations or proof-of-concept implementations to validate key techniques
- Extend taxonomy to include active adversarial sensing and cross-technology privacy threats.

s.dimieva@student.tudelft.nl