Radar-Inspired Defenses for Wi-Fi Sensing Privacy

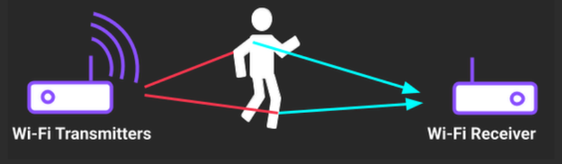
A Survey of Radar Defenses and Their Applicability to Wi-Fi Sensing

RQ: What are the state-of-the-art radar defenses, and to what extent are they applicable to Wi-Fi sensing?

What is Wi-Fi Sensing?

- It allows **passive eavesdropping** on environmental changes
- Using **ordinary** Wi-Fi devices, attackers may **see** through walls, **hear** speech, recover **passwords** from keystrokes, and make **3D pose** estimations.
- These estimates are contained in the **Channel State Information** used for signal demodulation, modelled as in [1]

$$\underbrace{\sum_{l=0}^{L-1}}_{\text{Multipath signals}} \underbrace{a_l(t)}_{\text{Amplitude}} \underbrace{e^{-j2\pi f \frac{d_l(t)}{c}}}_{\text{Phase shift}}$$



How does Wi-Fi work?

- Radio Frequency waves, typically at 2.4GHz and 5GHz
- Usually narrow bandwidths (up to 80MHz with exceptions)
- Governed by family of standards and protocols (802.11)
- Omnidirectional wave transmission
- Prioritizes performance and spectral efficiency

RAdio Detection And Ranging

- Actively transmit and receive signals for precise environment modelling
- Full control over waveform optimized for localization
- Often uses Frequency Modulated Continuous Wave rather than Orthogonal Frequency Division Multiplexing
- Typically mmWave (30GHz-300GHz), multi-GHz bandwidth

Deceptive Jamming	Doppler Spoofing	Spoof path lengths over subsequent chirps to inject **fake** velocity $e^{j2\pi f \frac{v_{sp}}{c} t}$	Supressed by CSI Ratio Algorithms, true signal revealed under the spoofed noise
	False Target Generation	Fool SAR Satellites with **plausible** terrain data. Augmented with **generative AI** (GANs)	Adapted to OFDM; plausible and effective, but computationally expensive
Metasurfaces	Static Cloak	**Redirective** (transformation-optics) **Absorptive** (wearable embroidery) **Scattering** (Mantle/ Plasmonic)	Fully limited by radial motion assumption and multipath signals in Wi-Fi networks
	Time-Modulated Cloak	Sensing and reactive cancelling, achieves monochromatic **invisibility**	
Waveform Design	Reconfigurable Intelligent Surfaces	**Cognitive** systems, estimate Angle of Arrival, suppress true echo and return false targets	Promising for deceptive jamming and improved communication
	Non-Orthogonality	Increases inter-carrier **interference**, Spectrally Efficient FDM, key needed to **decrypt** subcarriers	Promising for encryption-based strategies, especially with new-gen Wi-Fi 7 and 5G
Anti-Intercept	Chaotic Modulation	Pseudo-Random Binary Phase Sequences **superimposed** onto waveform, key needed to **decrypt**	
	Frequency Hopping	**Random**, **adaptive** hopping across frequency bins to avoid eavesdropping and jamming	Narrow bandwidth, spectrally inefficient performance.
	Region-based	Beamforming such as **Rapid Sidelobe Time Modulation**, directional security	Potential as hybrid with deceptive jamming to enact spatial control

Obfuscation
Concealment
Hybrid
Applicable
Inapplicable

[1] F. Miao, Y. Huang, Z. Lu, T. Ohtsuki, G. Gui, and H. Sari, "Wi-Fi sensing techniques for human activity recognition: Brief survey, potential challenges, and research directions," ACM Comput. Surv., vol. 57, no. 5, Jan. 2025.

By Stanislaw Ostyk-Narbutt (sostyknarbutt@tudelft.nl). Supervised by Fabian Portner and Arash Asadi