Radar-Inspired Defenses for Wi-Fi Sensing Privacy

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

Stanisław Ostyk-Narbutt

Supervisors: Arash Asadi, Fabian Portner

EEMCS, Delft University of Technology, The Netherlands

A Thesis Submitted to EEMCS Faculty Delft University of Technology,
In Partial Fulfilment of the Requirements
For the Bachelor of Computer Science and Engineering
June 18, 2025

Name of the student: Stanisław Ostyk-Narbutt
Final project course: CSE3000 Research Project
Thesis committee: Arash Asadi, Fabian Portner, Ranga Rao Venkatesha Prasad

Abstract

Wi-Fi sensing poses a serious threat to privacy due to its passive and covert nature. Nonetheless, the field of defenses is largely underdeveloped. This survey draws from the vast field of radar systems and their state-of-the-art countermeasures to discover potentially new Wi-Fi sensing defenses. The study identifies four particularly promising approaches: false target generation for deceptive jamming, reconfigurable intelligent surfaces (RIS) for dynamic signal manipulation using metasurfaces, encrypted waveform design for secure transmission, and hybrid region-based techniques for spatial access control. By transferring insights from radar systems to the context of Wi-Fi sensing, this work lays the groundwork for the future development of practical and resilient privacy-preserving defenses.

1 Introduction

Wi-Fi sensing is a technique that leverages ambient wireless signals to detect and interpret human activities, movements, and environmental changes [1]. Although it has been proven beneficial across domains such as healthcare monitoring [2], smart homes [3], and security systems [4], it poses a fundamental threat to privacy. Wi-Fi devices can be exploited to acquire information passively and covertly, rendering the intrusion virtually undetectable to the victim [5]. By analyzing channel state information present in Wi-Fi signals, adversaries can effectively repurpose wireless infrastructure as radar systems. This enables privacy-invasive sensing even through obstacles such as walls [6]. The severity of this threat is emphasized by emerging capabilities, including 3D human pose estimation using off-the-shelf hardware [7], keystroke inference through finger motion analysis [8], and speech reconstruction by tracking subtle lip movements [9]. As Wi-Fi sensing techniques evolve, the need for effective, privacy-preserving defenses is becoming increasingly urgent.

To address the growing privacy risks, this work introduces a novel perspective: conceptualizing Wi-Fi sensing as a form of radar. Drawing on this analogy, this paper explores whether established radar-domain defenses, specifically Electronic Countermeasures (ECMs) and Electronic Counter-Countermeasures (ECCMs), can inform the development of effective privacy-preserving defenses in Wi-Fi networks. In radar systems, ECMs encompass techniques designed to degrade or disrupt radar performance, whereas ECCMs aim to mitigate these disruptions by making the radar more resilient or less susceptible to interference. By framing Wi-Fi sensing through this lens, this paper seeks to translate decades of largely military-inspired [10] radar defense knowledge into actionable insights for safeguarding user privacy in wireless environments.

Radar and Wi-Fi sensing work on a shared technical principle of analyzing reflected wireless signals to detect motion and presence. This similarity, visually highlighted in Figure 1, suggests that the strategies developed within radar applications could also be useful for countering unwanted Wi-Fi-based surveillance. Strategies from radar ECMs and ECCMs offer a broad set of concealment and obfuscation methods which will be explored in this paper. These include utilizing engineered materials for stealth [11] and spoofing signal properties used for sensing [12].

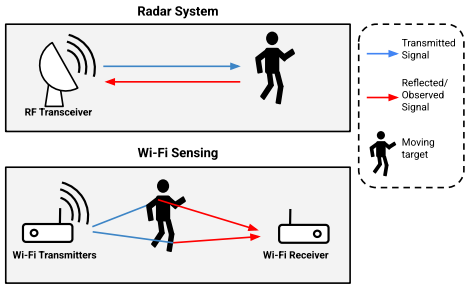

Figure 1: Diagram of How Radar and Wi-Fi Transmit and Observe Reflected Signals to Sense a Moving Target to Highlight Similarities

By examining the landscape of radar defense strategies and evaluating their technical and practical relevance to Wi-Fi environments, this work seeks to inform the design of new privacy-preserving mechanisms that do not compromise the communication functionality of Wi-Fi networks. The objective is to bridge concepts from radar ECMs and ECCMs with the theoretical constraints of wireless communication, encouraging innovative approaches to protect against illicit sensing. This leads to the central research question:

> *What are the state-of-the-art radar defenses, and to what extent can they be applied to counter unauthorized Wi-Fi sensing?*

The structure of this paper begins with a review of related work in Section 2, which frames the broader research landscape and highlights the key contributions of this study. To support the technical concepts that follow, Section 3 provides essential background on both radar systems and Wi-Fi sensing. This groundwork leads into Section 4, which presents a novel taxonomy and survey of the discovered radar defense techniques. Their relevance to Wi-Fi-based surveillance scenarios is critically examined in Section 5. Section 6 then synthesizes the findings, highlighting promising directions for future exploration. Broader ethical implications and principles of responsible research are considered in Section 7. The paper concludes in Section 8 with a summary of key insights.

2 Related Work

Although defenses are well-established in radar systems, their applicability to Wi-Fi sensing remains underexplored. Existing surveys often treat radar defenses and wireless communication security as distinct research domains, resulting in a lack of cross-disciplinary understanding. This separation hinders efforts to adapt radar-based defense strategies to address emerging privacy risks in Wi-Fi sensing.

Reeshen et al. [13] provide a comprehensive survey of radar defenses within the context of electronic warfare. Their taxonomy spans a wide range of military ECM strategies, particularly those tailored to modern battlefield environments. However, many of these techniques rely on ag-

gressive interference methods, such as jamming and deceptive emissions, that are fundamentally incompatible with the operational constraints of civilian Wi-Fi networks. Building on their work, this paper shifts focus towards broader, communication-preserving ECMs and ECCMs that can be applied in typical Wi-Fi network settings.

Conversely, the Wi-Fi sensing literature primarily focuses on enabling new applications rather than addressing adversarial threats. Surveys by Ahmad et al. [14], Wei et al. [15], and Miao et al. [16] highlight significant advances in activity recognition, gesture detection, and environmental interaction. However, these works largely overlook the privacy implications associated with passive sensing.

Liu et al. [17] present one of the most detailed reviews of privacy countermeasures in Wi-Fi sensing, covering both passive and active techniques. Nonetheless, their scope remains confined to the sparse approaches already developed specifically for Wi-Fi. In contrast, this paper adopts a cross-domain perspective, drawing from the broader ECM and ECCM literature to examine whether strategies originating from the field of radar can inspire a new class of defenses that preserve wireless communication while mitigating the potency of unauthorized sensing.

Thus, the key contributions of this work are:

1. A wide-reaching survey and novel taxonomy of radar defenses, emphasizing their underlying mechanisms and operational assumptions.
2. A theoretical analysis on the feasibility of adapting these radar defenses to Wi-Fi sensing scenarios, with a focus on preserving communication functionality while hindering illicit sensing.

3 Background Information

This section lays the technical groundwork for comparing radar systems and Wi-Fi sensing at the signal level, which is essential for evaluating the potential of adapting radar defenses to counter privacy threats in Wi-Fi environments. Section 3.1 describes how radar systems actively probe the environment by transmitting signals and analyzing their reflections. Section 3.2 explains how Wi-Fi devices, although designed for communication, can be adapted to infer similar information from passive signal observations under more limited conditions. The comparison between the two systems is then presented in Section 3.3.

3.1 Overview of Radar Systems

Radar (Radio Detection and Ranging) is a sensing technology that transmits radio frequency (RF) signals and processes their reflections to infer object distance, motion, and shape [18]. Widely used in military, automotive, and biomedical contexts [19, 20], radar enables precise environmental modeling through full control over the transmitted waveform.

Leveraging the flexibility in waveform design, many systems employ Frequency Modulated Continuous Wave (FMCW) signals, where the frequency varies over time according to a known chirp function. This enables continuous transmission while distinguishing signal reflections by their time delay [21].

Motion is inferred through frequency shifts in the reflected signal, known as Doppler signatures. More detailed motion, such as limb movements or respiration, introduces subtle frequency modulations named micro-Doppler signatures, which provide intricate information about fine-grained motion patterns [22]. To improve resolution, some systems operate in the millimeter-wave (mmWave) band (30–300 GHz), where wider bandwidths enable more precise spatial and motion estimation [23].

3.2 Overview of Wi-Fi Sensing

Wi-Fi networks are designed primarily for reliable and high-throughput data communication. However, as RF signals in Wi-Fi propagate, they interact with the environment through reflection, scattering, and absorption. These interactions introduce measurable perturbations that can be analyzed to infer the presence, motion, and behavior of objects or individuals. Wi-Fi sensing leverages this effect by repurposing standard devices to extract environmental information from regular data transmissions.

Most modern Wi-Fi sensing techniques rely on Channel State Information (CSI), which describes how the wireless channel affects a transmitted signal. CSI captures amplitude and phase values across multiple frequency subcarriers in Orthogonal Frequency Division Multiplexing (OFDM) systems [1]. In typical communication settings, CSI is used to correct for signal distortions caused by multipath propagation, such as reflections from walls or objects. However, because these distortions change over time as the environment changes, CSI can also serve as a fine-grained indicator of motion.

For each received packet, the CSI over L signal paths can be modeled as a function of time $H(t)$ by the relationship:

$$H(t) = \sum_{l=0}^{L-1} a_l(t) e^{-j2\pi f \frac{d_l(t)}{c}} \tag{1}$$

where $a_l(t)$ and $d_l(t)$ represent the amplitude and path length of the lth multipath component, f is the carrier frequency, c is the speed of light, and j is the imaginary number [16]. Since Wi-Fi preambles are standardized and publicly known, adversaries can estimate CSI values passively by eavesdropping on packet transmissions, without cooperation from the devices emitting the signals [24].

3.3 Comparison of Radar and Wi-Fi Sensing

While both radar and Wi-Fi sensing analyze reflected RF signals, they differ in purpose, constraints, and signal design. Importantly, Wi-Fi is governed by IEEE 802.11 standards, typically operating in 20–80 MHz bands at 2.4 and 5 GHz [23]. Radar systems, by contrast, use wider bandwidths for higher spatial and temporal resolution. Even high-bandwidth Wi-Fi protocols like 802.11ad/ay, which reach up to 2 GHz at mmWave frequencies, remain optimized for throughput rather than sensing. These differences complicate the direct application of radar defenses to Wi-Fi environments. These primary differences are summarized in Table 1.

Table 1: Technical Comparison Between Radar and Wi-Fi Sensing

Aspect	Radar	Wi-Fi Sensing
Waveform Control	Full control over waveform design	Constrained by IEEE 802.11 standards
Bandwidth	Typically 100s of MHz to multi-GHz	Narrow (20–80 MHz), except in 802.11ad/ay (up to 2 GHz)
Signal Access	Active measurement (transmit and receive)	Passive estimation from ongoing communication
Design Priorities	Optimized for accuracy in range and velocity	Optimized for throughput and efficiency

4 Survey of Novel Radar Defenses

This study takes an exploratory approach to assess the feasibility of adapting radar-based defenses to Wi-Fi sensing. Given the lack of defined, fixed terminology for radar defenses, a broad, open-ended survey was conducted using thematic queries on radar deception, signal spoofing, Doppler manipulation, and defensive techniques. Emphasis was placed on recent, reputable work with novel contributions. Strategies that disrupt legitimate communication, such as spot jamming and barrage jamming, were excluded due to their incompatibility with Wi-Fi environments [10].

This paper develops a defense taxonomy through open coding, grouping radar techniques iteratively based on recurring functional traits rather than fixed classifications. While traditional schemes such as active versus passive [17] are common, they often fail to capture hybrid or unconventional methods relevant to Wi-Fi adaptation. To support the subsequent transferability analysis, nine state-of-the-art radar techniques were identified. A limited selection of representative papers was chosen to exemplify each technique. These techniques were grouped into four functionally descriptive categories, as illustrated in the taxonomy of Figure 2. These categories are further classified as either ECM or ECCM and color-coded by their underlying objective: either obfuscation (distorting signals), concealment-oriented (focus on stealth), or hybrid (both). This taxonomy serves as the structure of the literature survey, presented in Sections 4.1 through 4.4.

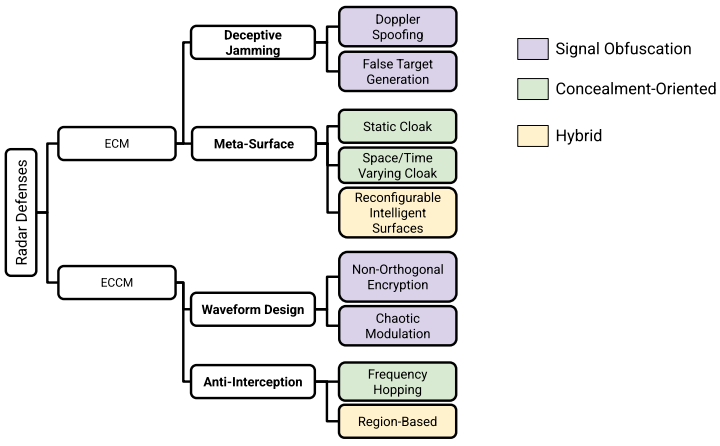

Figure 2: Proposed Taxonomy of Discovered Radar Defenses

4.1 Deceptive Jamming

Deceptive jamming encompasses a family of electronic countermeasures that intentionally transmits distortions to mislead a radar. These techniques introduce false or manipulated returns into the signal environment, creating deceiving observations that reduce the reliability of adversarial sensing.

Doppler Spoofing

Doppler spoofing is a signal-level deception method that falsifies motion cues in radar systems. By manipulating phase or frequency characteristics of the radar signal, an adversary can alter the perceived velocity of a target, thereby degrading motion-based classification, tracking, or filtering. Unlike noise-based jamming, which indiscriminately overwhelms the receiver, Doppler spoofing produces targeted and structured interference that mimics plausible physical behavior.

An effective approach to Doppler spoofing is path-length modulation, where the adversary applies a controlled time-varying phase shift to the reflected signal. This induces a synthetic Doppler shift, causing the radar to interpret the target as moving at a false velocity. The spoofed signal model proposed by Argyriou [12] to induce a spoofed velocity v_{sp} for the k-th subcarrier of an OFDM signal as a function of time t is:

$$x^{(k)}\text{sp}(t) = e^{j2\pi k\delta f \frac{v_{sp}}{c} t} \tag{2}$$

for a signal frequency δf, and c is the speed of light. This modulation induces a Doppler shift corresponding to a fictitious target motion, causing the radar to perceive a different speed or trajectory. Simulations of this model verify degraded sensing performance for slow-moving pedestrians.

In mmWave systems, Doppler spoofing has advanced significantly due to the high resolution and short wavelengths inherent to these frequencies. A common approach involves introducing controlled phase shifts between consecutive chirps in FMCW radars, effectively altering the perceived motion of a target. By manipulating inter-chirp phase coherence, an attacker can generate spoofed Doppler signatures that cause the radar to misinterpret velocity, such as perceiving a stationary object as moving or vice versa. This technique is particularly effective in autonomous vehicle radars, where motion estimation depends heavily on the stability of phase relationships across chirps, making them especially susceptible to structured, signal-level deception [25, 26, 27].

False Target Generation

False target generation represents the most advanced form of deceptive jamming. Rather than merely distorting existing signal features, these techniques synthesize entirely fictitious objects that appear consistent with genuine radar echoes.

These methods have been prevalent in mmWave sensing with systems such as mmSpoof used to mislead automotive radars about the presence and motion of artificially generated obstacles [28], and further applied to mimic vitals in health monitoring using false micro-Doppler traces [25].

In Synthetic Aperture Radar (SAR) satellites, which generate high-resolution terrain imagery by combining successive radar echoes, false target generation has been extended to deceive geospatial interpretation [29]. A widely

used approach introduces fictitious objects through delay and phase modulation, embedding them at specific coordinates via time-modulated waveforms. SAR-domain algorithms such as inverse range Doppler and adaptive delay modulation have shown effectiveness in practical deception scenarios [30]. Even in more advanced terrain-mapping systems such as TOPSAR which incorporates progressive scans, studies demonstrate that these methods can produce fabricated scenes with minimal statistical deviation from genuine terrain data [31].

Machine learning models, particularly Generative Adversarial Networks (GANs), have significantly advanced the realism of false target generation. Systems like RF-Protect [32] use GANs to generate signals representing realistic human activity that deceive sensing systems. Similar techniques have emerged in the SAR domain, where GANs are used to generate terrain imagery with minimal statistical deviation from real-world scans [33]. These methods represent the current frontier of deceptive jamming, combining signal-level manipulation with synthetic data to mislead sensing systems.

4.2 Metasurfaces

An increasingly explored class of electronic countermeasures uses metasurfaces, which are composite materials engineered to suppress radar backscatter and conceal targets. These engineered surfaces control electromagnetic wave behavior to reduce detectability, supporting both passive and active cloaking strategies. This section surveys three key categories: static cloaks with fixed electromagnetic properties, time-modulated metasurfaces with dynamic control over wave interactions, and cognitive self-reconfigurable cloaks that adapt to sensing conditions in real-time.

Static Cloaking

Static cloaking suppresses radar backscatter by modifying how incident waves interact with a target. Techniques fall into three primary categories:

1. **Redirective Cloaks**: Based on electromagnetic transformation optics, these guide waves around an object using spatial coordinate mappings, creating apparent invisibility from select angles [34]. While conceptually powerful, they often require superluminal phase velocities and are highly dispersive, making them narrowband and sensitive to idealized conditions. Transmission-line implementations partially relax these constraints but remain narrowband and sensitive to radar parameters.
2. **Absorptive Cloaks**: Instead of steering waves, these dissipate energy through lossy, frequency-selective materials. Notable advancements include textile-integrated metasurfaces, such as embroidery-based absorbers that achieve up to 99% attenuation at designated frequencies while preserving flexibility and sub-millimeter profiles [35]. These are well-suited for conformal and wearable applications.
3. **Scattering Cancellation Cloaks**: Also known as mantle or plasmonic cloaks, these induce destructive interference between genuine object reflections and engineered surface reflections. They enable ultrathin designs but typically trade off bandwidth and angle flexibility [34].

Together, these static cloaking strategies offer compact, passive stealth capabilities, representing state-of-the-art passive radar countermeasures.

Time-Modulated Cloaking

Static cloaks are effective for stationary targets but struggle under motion, as Doppler shifts reintroduce detectable signatures. Time-modulated cloaking overcomes this limitation by altering the temporal characteristics of scattered radar waves to suppress Doppler-based detection. These methods exploit radar signal-processing assumptions, particularly those in Moving Target Indicator filters, which depend on Doppler cues to distinguish moving targets from static clutter.

One foundational approach, proposed by Kozlov et al. [36], uses temporal phase modulation to cancel Doppler shifts caused by radial motion. However, this method is limited to narrow angles of incidence and assumes motion aligned with the radar's line of sight, making it unidirectional and less adaptable to real-world scenarios.

Zhang et al. [11] extend this concept with a smart Doppler cloak featuring real-time sensing and feedback control. Their system dynamically adjusts modulation parameters based on the direction and polarization of incoming waves, enabling Doppler suppression across a broader angular and motion range. Operating at carrier frequencies up to 6 GHz with modulation allowing induced frequencies of 400 kHz, it can mask high-speed targets under controlled, single-frequency radar conditions. This architecture represents a significant step toward adaptive cloaking and conceptually bridges toward Reconfigurable Intelligent Surfaces, where sensing, control, and multidirectional response are unified into multifunctional ECM platforms. However, the work critically is only developed against monochromatic radars which operate on single-frequencies. Adding support for varied-frequency radars would likely significantly degrade the performance of the experimental smart cloak.

Reconfigurable Intelligent Surfaces

An emerging extension of time-modulated cloaking involves the use of Reconfigurable Intelligent Surfaces (RIS), also referred to in the literature as Intelligent Scattering Reflectors (ISR) or cognitive metasurfaces. RIS architectures augment traditional metasurface cloaks by integrating real-time sensing and control capabilities. These systems employ arrays of tunable reflective elements, guided by sensing algorithms, to dynamically shape the wavefront of scattered signals in response to changing environmental conditions.

As demonstrated by Xiong et al. [37], RIS can be synergistically combined with absorptive or imperfect cloaks to overcome a key limitation of conventional time-modulated designs: their restriction to radial motion relative to the radar line of sight. By estimating the Angle of Arrival of incident radar waves and adjusting the reflection phase across the array, the RIS enables destructive interference along arbitrary directions, supporting effective cloaking for targets with complex trajectories or operating in heterogeneous environments.

Beyond concealment, RIS systems offer the unique potential to unify stealth and deception within a single platform. While traditional cloaks seek only to suppress detectability, cognitive RIS can simultaneously generate spoofed echoes,

misleading radar systems about a target's location or motion. Wang et al. [38] propose such a hybrid ECM architecture, in which the RIS is programmed to deflect authentic phase-shifted signals mimicking the target's true echo while concurrently producing false angle-dependent reflections that simulate decoys. This dual functionality effectively combines signature suppression with angle-domain spoofing, offering a versatile mechanism for electromagnetic obfuscation. As such, RIS-based systems represent a paradigm shift in ECM design, transitioning from passive cloaking surfaces to adaptive, multifunctional platforms capable of both evasion and deception under real-world constraints.

4.3 Waveform Design

Waveform design stems from the field of dual radar and secure communication systems. It modifies signal structure to degrade an adversary's ability to interpret intercepted or reflected transmissions. Although associated with Low Probability of Intercept (LPI) radar systems, this section focuses on anti-recognition; unlike concealment-based LPI techniques covered in Section 4.4, these strategies aim to obfuscate a signal's content. By leveraging encryption at the signal level, the wave becomes unintelligible, thus simultaneously harder to detect.

Non-Orthogonal Encryption

A core method in this space is frequency-based waveform encryption, which introduces controlled distortion, often through non-orthogonal subcarrier allocation. Salem et al. [39] showed that violating OFDM orthogonality generates deliberate inter-carrier interference (ICI), decryptable only with a shared symmetric key. Without the key, attackers face exponential complexity in decoding via vector-based maximum likelihood estimation, which is computationally infeasible with large key spaces.

Building on this, Xu [40] proposed Spectrally Efficient Frequency Division Multiplexing (SEFDM), which increases ICI by packing subcarriers more densely. This hides the structure of the subcarrier signals from adversaries while enhancing throughput. This approach compounds distortion in a way that resists brute-force analysis of the wave properties.

Chaotic Modulation

Chaotic modulation employs time-domain encryption. Zhu et al. [41] introduce chaotic waveform design using Pseudo-Random Binary Phase Sequences (PRBPS), which inject non-linear phase shifts into radar pulses. These waveforms outperform traditional chirp functions in LPI characteristics, broadening their utility where signal masking is insufficient.

Generative Adversarial Networks (GANs) have further augmented waveform security with amplitude-controllable perturbations that are superimposed onto the original waveform [42]. Whereas legitimate receivers can apply a demodulation framework akin to decryption to bypass the perturbations, the GAN learns to trick eavesdroppers, thus marking a shift from static encryption toward adaptive, learned obfuscation strategies.

Together, these techniques demonstrate how waveform design can embed complexity directly into the transmission itself, obfuscating radar signatures without resorting to jamming or spectrum denial. As a radar ECCM strategy, waveform design offers a communication-preserving, scalable path to degrading adversarial sensing in environments where the waveform contains sensitive information.

4.4 Anti-Interception

Anti-interception techniques, another subset of Low Probability of Intercept (LPI) strategies, aim to reduce detectability by adversaries. Two main approaches stand out: frequency hopping and region-based beamforming.

Frequency Hopping

Frequency hopping is a foundational strategy for LPI, with novel techniques prioritizing randomization and adaptivity:

- **Randomized Hopping:** By introducing non-deterministic frequency changes, randomized hopping schemes make it more difficult for adversaries to track or spoof the radar signal. *BlueFMCW* [43] exemplifies this approach by using randomized sub-chirp permutations and a phase alignment algorithm that preserves coherent signal reconstruction despite that rapid frequency hopping. This disperses spectral energy across frequency bins, hindering eavesdropping while maintaining full range resolution.
- **Adaptive, Learning-Based Hopping:** Reinforcement learning enables dynamic hopping strategies that respond to real-time interference. Modeling frequency selection as a Markov decision process, Q-learning-based methods [44] allow systems to learn optimal hopping patterns based on observed jamming or eavesdropping behavior. This adaptivity strengthens resilience against evolving threats and marks a shift from static frequency planning to resilient agility.

Together, these approaches highlight how frequency hopping is transitioning from basic avoidance to intelligent, eavesdropper-aware signal security.

Region-Based

Region-based techniques in radar use advanced beamforming to spatially confine radiated energy, reducing signal leakage into areas where adversaries could intercept or exploit emissions. Inspired by secure wireless communication strategies, these methods enhance Low Probability of Intercept (LPI) and Detection (LPD) by precisely shaping the radiation pattern to minimize electromagnetic signatures outside the intended receiver's zone.

Rapid Sidelobe Time Modulation (Rapid LSTM) is a technique drawn from the domain of secure communications. It dynamically modulates antenna sidelobes over time to introduce controlled signal distortion in non-target directions [45]. This time-varying interference prevents adversaries in adjacent spatial regions from reliably interpreting waveform content, even if signal strength remains detectable. Unlike traditional spatial filtering, which primarily reduces power leakage, Rapid LSTM actively conceals waveform structure, making intercepted signals difficult to reconstruct or classify. By combining real-time beamforming with temporal modulation, it substantially enhances LPI and LPD, increasing the resilience of radar systems against adversarial detection.

5 Transferring Radar to Wi-Fi Sensing

This section assesses the potential for adapting the surveyed radar-based defenses to Wi-Fi sensing under the differences outlined in Section 3.3. Each defense category from the taxonomy is theoretically evaluated based on existing literature in the Wi-Fi domain in Sections 5.1 through 5.4. To assist the analysis for each category, one or more of the five aspects that follow are considered whenever relevant, applied as analytical lenses rather than rigid scoring criteria:

1. **Standard compliance** with IEEE 802.11 protocols
2. **Communication impact** on legitimate data
3. **Hardware feasibility** on commodity Wi-Fi devices
4. **Resilience** to adversarial suppression
5. **Practical feasibility** in real-world settings

5.1 Applicability of Deceptive Jamming

Among deceptive jamming techniques, **false target generation** emerges as the most promising approach for Wi-Fi sensing environments. Compared to spoofing, it offers greater resilience to countermeasures, produces more realistic signals, and maintains communication integrity.

Limitations of Spoofing Spoofing has already been investigated in the domain of Wi-Fi sensing in various experiments. Representative papers are CSI "fuzzer" by Jiao et al. [46] which distorts CSI measurements with negligible throughput degradation and the standard-compliant spoofing method compatible with unmodified 802.11 devices by Cominelli et al. [47]. These works illustrate the implementation feasibility and communication-preserving potential of spoofing, although both approaches rely on detectable patterns, making them vulnerable to suppression.

Chu et al.'s SnoopFi [48] exposes this vulnerability by demonstrating how keyspace limitations and CSI Ratio Algorithms can defeat several spoofing defenses, including advanced anti-sensing Wi-Fi frameworks such as WiCloak [49]. Their findings suggest that unless spoofing becomes more sophisticated, it remains exploitable by adversarial suppression. This echoes a broader problem in Wi-Fi ECMs: defenses often evolve without anticipating an intelligent adversary's response. Blakely and Pethel [50] further reinforce this weakness, showing that quantum noise-based methods can differentiate real from spoofed signals, raising the bar for deception. Ultimately, spoofing largely lacks resilience, rendering it predominantly inapplicable to Wi-Fi sensing.

Promise of False Target Generation In contrast, false target generation, especially techniques inspired by Synthetic Aperture Radar (SAR), shows higher promise across all evaluation dimensions. Gusti et al. [51] successfully adapt SAR deception techniques to OFDM-based radars, producing synthetic reflections that obscure real activity. Their work extends Falcone et al. [52] who demonstrate SAR-like imaging using ISAR in passive Wi-Fi radar, establishing a clear technical bridge between the domains. Unlike spoofing, which perturbs isolated parameters, false targets recreate coherent spatiotemporal signatures of realistic fake targets, better aligning with the complexity of modern CSI-based sensing.

RF-Protect's GAN-based signals which mimic human behavior [32] best demonstrated the applicability of deceptive jamming against Wi-Fi. These learned patterns vary over time and space, resisting adversarial suppression that exploits deterministic artifacts. When viewed alongside SAR-based deception, RF-Protect exemplifies a shift in ECM design, from spoofed path injection to complex fake environments. This transition toward learning-based, realistic deception reflects a growing recognition that ECM effectiveness hinges on mimicking, not masking, the underlying signal statistics of real targets.

These techniques offer high-fidelity deception, standard compatibility, and stronger resistance to adversarial inference. Although future work should address real-time deployment on constrained devices and communication performance, current evidence clearly favors this class of ECMs for privacy protection in Wi-Fi sensing.

5.2 Applicability of Metasurfaces

Metasurfaces play a key role in radar countermeasures, yet are often overlooked in Wi-Fi sensing. Existing defenses rely mostly on signal obfuscation via Reconfigurable Intelligent Surfaces (RIS), with minimal focus on cloaking. This section examines the limitations of static metasurfaces, the potential of dynamic cloaks, and how future RIS defenses could draw from deceptive jamming to enhance wireless privacy.

Limitations of Cloaks Static cloaking techniques, including transformation optics and transmission-line structures, are fundamentally incompatible with indoor Wi-Fi sensing. Their inherently unidirectional behavior, a consequence of their reliance on radial motion relative to the radar, fails to cloak the multipath, omnidirectional signals of Wi-Fi, limiting their effectiveness in concealing presence or motion.

Absorptive metasurfaces, including textile-based designs such as those by Yang et al. [35], may offer more practical potential. These low-profile materials absorb signals from multiple angles, which suits the spatial characteristics of Wi-Fi environments. In principle, they could be used as wearable privacy shields in settings that require controlled access, such as high-security zones.

While this may inspire a novel set of defenses, realistic applications deem it ultimately impractical. Entire physical environments, including people and objects, would need to be covered in such materials. The same pitfall limits the implementation of time-modulated cloaks such as the smart cloak [11]. This largely prohibits the realistic transferability of cloaking metasurfaces in settings such as homes and offices despite theoretical privacy enhancement.

Promise of Dynamic Surfaces RIS offer programmable control over wireless reflections and have gained attention as a platform for countermeasures in Wi-Fi sensing. Cigno et al. [53] proposed a RIS-based system that introduces chaotic backscatter to disrupt CSI. This is a trend further illustrated by IRShield [54], a similar proposal for an RIS against Wi-Fi sensing that suppresses CSI to reduce sensing detection rates below 5 percent. While effective at degrading sensing accuracy, both methods are limited to obfuscation and show spatial bias that may make its interference patterns predictable.

Together, these works reflect a broader trend in RIS-based defenses: current systems emphasize disruption over concealment, with minimal exploration of deceptive techniques. This highlights an emerging opportunity to shift RIS research toward hybrid strategies that combine suppression with actively misleading sensing algorithms.

As RIS technology matures, future directions could move beyond basic suppression and toward hybrid deceptive strategies, limiting spatial bias discussed by Cigno et al. RIS could be used to generate misleading CSI by redirecting or modifying reflections. Drawing from the field of deceptive jamming, GANs may be adapted to RIS contexts to fabricate realistic yet false CSI traces that mislead sensing algorithms. The shift from concealment in radar RIS to deception opens new possibilities for hybrid metasurfaces in Wi-Fi sensing.

5.3 Applicability of Waveform Design

In radar systems, Section 4.3 on waveform design revealed the significant effectiveness of signal-layer encryption. Methods such as non-orthogonal carrier interference and chaotic sequence modulation obscure channel information, while authorized receivers recover it using encryption keys. Applying these techniques to Wi-Fi is challenging due to IEEE 802.11 standards, which restrict low-level waveform customization. However, this constraint also encourages standard-compliant reinterpretations and future protocol extensions, particularly as the field of integrated sensing and communications continues to advance.

Feasibility of Waveform Encryption Despite IEEE 802.11 protocols imposing strict physical-layer constraints, recent research demonstrates that waveform-based encryption is feasible in Wi-Fi with targeted modifications. Xu et al. [40] implement a waveform-defined security framework using SEFDM within an 802.11a-based network. Although 802.11a is outdated, its OFDM structure remains relevant to modern standards, making their results broadly applicable. In follow-up work, Xu [55] introduces phase obfuscation via adjacent-subcarrier modulation, which degrades CSI-based motion sensing while preserving communication.

Mohammed et al. [56] further extend this direction by proposing a time-domain waveform encryption method, also based on 802.11a. Although they acknowledge potential brute-force vulnerabilities, they highlight how newer standards such as 5G and Wi-Fi 7 offer expanded key spaces that improve resilience against adversarial suppression. Collectively, these studies suggest that with modest protocol or hardware updates, waveform-level defenses can be integrated into network architectures.

Promise of Encryption in Wi-Fi Sensing WiShield [57] presents a promising approach to encryption-based sensing defense. It allows authorized devices to share cryptographic keys to encrypt the waveform structure, enabling legitimate sensing technologies such as smart-homes [3] while preventing unauthorized access to CSI. Although key exchange remains a challenge, this trade-off is practically viable in typical Wi-Fi environments including smart homes or healthcare, where seamless operation across trusted devices is essential.

Waveform design techniques, especially those using CSI phase obfuscation and encrypted modulation, represent a promising direction for Wi-Fi sensing defenses. The transfer of the broader radar field of waveform design may offer novel solutions unexplored in W-Fi sensing, from PRBPS chaotic sequences to GAN-based waveform synthesis, embedding advanced encryption forms directly into the physical layer. These approaches support secure, communication-preserving defenses that leverage newer Wi-Fi standards for wider key space thus even more security and resilience.

5.4 Applicability of Anti-Interception

Novel anti-interception techniques such as frequency hopping and region-based defenses face significant challenges when applied to Wi-Fi sensing. However, beamforming could serve as a conceptual bridge to inspire hybrid defenses with other surveyed defense categories.

Limitations of Frequency Hopping Frequency hopping, used in early Wi-Fi through Frequency-Hopping Spread Spectrum (FHSS), was eventually replaced by Orthogonal Frequency-Division Multiplexing (OFDM) due to its negative impact on communication performance. FHSS introduced coordination overhead, reduced spectral efficiency, and struggled to scale in multi-user environments. This transition highlights how Wi-Fi prioritizes stable, high-throughput communication over spectral agility.

These design constraints highlight the ineffectiveness of frequency hopping as a privacy defense. Unlike radar systems such as BlueFMCW, which benefit from wide and flexible spectrum access, Wi-Fi operates in narrow, regulated bands with strict protocol rules. As a result, frequency hopping does little to obscure physical-layer features as CSI when monitored by an adversary with a wideband receiver. Pirayesh et al. [58] have already concluded that FHSS performs poorly under modern interference and provides minimal resilience. Therefore, in the broader context of Wi-Fi sensing defense, frequency hopping represents a legacy approach that is unlikely to meet the performance, compatibility, or privacy needs of contemporary networks.

Potential of Region-Based Techniques Region-based defenses draw from radar strategies that manipulate signal direction to control where information is leaked. In Wi-Fi, however, their effectiveness is limited as most wireless networks use omnidirectional antennas to support broad coverage and user mobility. Even when beamforming is available, adversaries can still extract useful data from multipath reflections, which are central to Wi-Fi sensing. This makes it difficult to fully restrict sensing based on direction alone.

Nonetheless, region-based techniques offer conceptual value that could be transferred to Wi-Fi. Aegis [59], for example, uses directional antennas to transmit spoofed Doppler signals into areas where eavesdroppers may be present while preserving signal integrity in a central "private zone." This selective interference provides spatial access control without disrupting communication. This represents the possibility for region-based methods to incorporate deceptive jamming strategies; such hybrid defenses may offer resilient solutions against Wi-Fi sensing if further researched.

Table 2: Promising Radar-Inspired Defenses for Wi-Fi Sensing: Origins, Benefits, Limitations, Existing Work, and Future Directions

Defense	Radar Domain	Benefits	Limitations	Existing Wi-Fi Efforts	Future Possibilities
False Target Generation	SAR Satellites, mmWave autonomous vehicles	Controllable deception, indistinguishable from real targets	Computational cost, limited on constrained hardware	GAN-based *RF-Protect* by Shenoy et al.	Integration into Wi-Fi devices for Real-time deployment
Reconfigurable Intelligent Surfaces	Cognitive metasurfaces	Dynamic CSI manipulation, spatial control	Deployment cost and spatial bias; complexity in real-time coordination	Region-based *IRShield* by Staat et al.	Hybrid with deceptive jamming and improved communication
Encrypted Waveform	LPI radar	Physical-layer privacy, preserves communication	IEEE 802.11 limits flexibility; secure key exchange required	SEFDM encryption by Xu et al., Mohammed et al. in 802.11a	Extend encryption to new generation Wi-Fi (i.e. Wi-Fi 7)
Hybrid Region-Based Beamforming	Rapid LSTM in Antenna Arrays	Spatially confined, preserves communication zones	Requires specialized hardware with spatial awareness	Directional spoofing with *Aegis* by Yao et al.	Hybrid with deceptive jamming

6 Discussion

Although many radar defenses are not directly applicable to Wi-Fi due to technical or practical constraints, the significant analysis and discussion in Section 5 identifies a subset of techniques with potential for enhancing Wi-Fi sensing privacy. Section 6.1 highlights the most promising of these approaches. This is followed by a discussion of the study's limitations in Section 6.2, and future research directions in Section 6.3, guided by insights from emerging trends.

6.1 Cross-Domain Insights

The taxonomy in Section 4 answered the first part of the research question on the state-of-the-art radar defenses, whereas their applicability to Wi-Fi is addressed in Section 5.

Table 2 summarizes the most promising radar-inspired defenses for Wi-Fi sensing, emphasizing both the technical adaptability of specific techniques and the strategic value of the broader categories they represent. Radar domains such as SAR and mmWave systems proved especially relevant, offering advanced deception strategies well-aligned with Wi-Fi privacy needs. For instance, the growing field of SAR-based false target generation shows especially strong potential for misleading passive sensing in complex environments.

Among the surveyed techniques, four stand out as particularly transferable: false target generation, reconfigurable intelligent surfaces (RIS), encrypted waveform design, and hybrid region-based spatial control. Together, these approaches provide a foundation for future Wi-Fi sensing defense research that is adaptive, non-disruptive to communication, and resilient to adversarial techniques.

6.2 Limitations

This survey set out an ambitious objective to bridge two expansive and technically complex domains, both of which are fast-evolving and shaped by continuous research advancements. As a result, several limitations must be acknowledged regarding the scope and methodology of this work, which constrain the extent to which the proposed defenses can be directly adapted to Wi-Fi sensing.

- **Physical Deployment and Experimentation**: Many surveyed papers are employ simulations, whereas real-world constraints (e.g., latency, hardware limitations, IEEE 802.11 compliance) may hinder implementation.
- **Vulnerability to adaptive adversaries**: Attackers capable of counter-adapting may reduce the long-term effectiveness of the defenses.
- **Non-exhaustive survey scope**: A systematic review was not feasible due to the lack of established terminology previous to the discovered taxonomy.

6.3 Future Work

Future research should focus on advancing radar-inspired defenses beyond conceptual proposals toward practical deployment in real-world Wi-Fi environments. The most promising radar-inspired defenses in Table 2 further outline several promising directions that merit further research. Further building on these insights, future research should prioritize the following factors and emerging trends:

- **Empirical validation**: Develop physical implementations and test defenses in real-world Wi-Fi sensing scenarios to evaluate performance under practical constraints and monitored communication impact.
- **Generative AI Integration**: Advance false target generation using emerging, state-of-the-art generative AI models and methods for more sophisticated and plausible fake object signal synthesis.
- **Upcoming Wi-Fi Standard Integration**: Align defense techniques with the upcoming sensing-oriented IEEE 802.11bf, particularly addressing privacy risks of the proposed mmWave bands (up to 60 GHz) [60].

7 Responsible Research

The covert and increasingly powerful nature of Wi-Fi sensing raises important ethical and methodological considerations. This section reflects on the broader implications of researching defenses in this domain, particularly the potential consequences of enabling malicious technologies. Section 7.1 outlines key ethical concerns, including the risks of misuse and unintended societal impact. Section 7.2 then discusses the reproducibility of this work, detailing the steps taken to ensure transparency despite the open-ended and interdisciplinary nature of the literature.

7.1 Ethical Considerations

This paper deals with several ethical considerations that are crucial to consider when surveying radar systems and proposing new directions for research in Wi-Fi sensing defenses.

In accordance with the **TU Delft Code of Conduct** [61], this work explicitly reflects on the value of integrity by critically assessing the consequences brought by researching and proposing defenses in Wi-Fi sensing.

Privacy Preservation The fundamental problem of adversarial Wi-Fi sensing poses exceedingly large ethical concerns for unsuspecting people who may fall victim to passive human scanning. With the abundance of Wi-Fi networks, the growing capabilities of Wi-Fi sensing previously discussed threaten privacy. From through-wall pose estimation to password inference, the ever-increasing adversarial possibilities exhibit serious risks. In surveying defenses for preventing wireless sensing, this paper is firmly rooted in the ethical imperative to safeguard privacy.

Potential Misuse While this survey is driven by the goal of protecting privacy, the potential adversarial misuse of the proposed defenses must be acknowledged. Techniques intended to block unauthorized sensing may also interfere with legitimate applications, such as healthcare monitoring [2]. In particular, deceptive jamming methods like spoofing and false target generation could be misused to distort medical data or disrupt smart home systems by nefarious adversaries. Although this risk of misuse cannot be ignored, the continued development of defenses is imperative for privacy. Therefore, developers of legitimate Wi-Fi sensing technologies must implement safeguards to prevent malicious use and ensure system integrity. These could potentially include the LPI techniques discussed in this paper.

Electronic Warfare This paper draws upon radar research, a field historically shaped by its military applications in electronic warfare [10]. While the intent is strictly to facilitate cross-domain knowledge transfer, the structural and functional similarities between radar and Wi-Fi sensing make it plausible that advancements in the latter could inform future developments in electronic warfare. This potential feedback loop raises ethical concerns, particularly regarding the morally ambiguous use of military technologies. Nonetheless, given that electronic warfare research is significantly more advanced and mature than that of Wi-Fi sensing, the influence is predominantly unidirectional. It is therefore unlikely that Wi-Fi sensing defenses facilitate electronic warfare advancements, though worth considering.

7.2 Reproducibility

The open-ended nature of this survey makes it difficult to enforce reproducibility, however, steps were taken wherever possible to ensure it and mitigate biases.

Usage of Generative AI Due to the unresolved terminology and open-ended nature of radar defense literature, traditional keyword-based searches in academic databases were supplemented with thematic exploration using the *Deep Research* feature in ChatGPT, an AI research tool used to uncover related concepts within radar defenses under varying terminology, for example the largely equivalent use of RIS and ISR across literature on cognitive metasurfaces.

To ensure reproducibility despite the non-deterministic output if AI tools, Deep Research was used solely to broaden the initial search scope. Any new research themes identified through this process were critically reviewed then manually surveyed in academic databases with the inclusion and exclusion criteria from Section 4, thus mitigating any bias.

Grammatical and stylistic suggestions during the final revision of the paper were additionally supported by AI tools.

Methodology Reflection As this work did not follow a formal systematic review protocol, full reproducibility of the survey process is not guaranteed. This limitation stems from both the constrained timeline of the project and the absence of an established taxonomy or well-defined set of defensive techniques before the survey was conducted. Despite this, the review was extensive, covering a broad range of relevant literature. Transparency was prioritized by documenting both included and excluded techniques. For instance, the exclusion of jamming methods not aligned with the objective of the survey was transparently documented in Section 4.

Although the selection process is not fully replicable, future surveys would likely arrive at a similar high-level taxonomy given the breadth of the literature reviewed. While the specific techniques selected for each category may reflect some selection bias, this is mitigated by their role in illustrating broader trends. Alternative examples would likely highlight similar patterns within each category.

Transparent Evaluation Criteria The adaptation of radar defenses to the Wi-Fi domain may have introduced bias in determining which categories were considered more applicable. To reduce this risk and enhance reproducibility, five clear evaluation aspects are explicitly stated at the beginning of Section 5. Additionally, the adaptability analysis was supported by a brief secondary survey of existing literature in the Wi-Fi sensing domain. This ensured that selected techniques were grounded in prior academic work, helping to validate their relevance and minimize subjective bias.

8 Conclusion

This paper discovered the state-of-the-art radar defenses and explored the potential of adapting radar ECMs and ECCMs to defend against privacy threats posed by Wi-Fi sensing. From the surveyed radar literature, four categories of techniques were proposed for a taxonomy of communication-preserving defenses within the field of radar: deceptive jamming, metasurfaces, waveform design, and region-based techniques.

While many radar defenses were found incompatible within the constraints of IEEE 802.11 standards, four stood out for their adaptability. In particular, false target generation (especially using GANs), reconfigurable intelligent surfaces, encrypted waveform design, and hybrid region-based spatial control emerged as promising directions for future research. These techniques balance theoretical feasibility with sensing degradation and offer a foundation for novel Wi-Fi-compatible defenses for safeguarding privacy.

As Wi-Fi sensing grows more sophisticated and pervasive, the prospect of ordinary wireless devices silently observing us becomes increasingly unsettling. Yet, if an aircraft traveling at supersonic speeds can evade the most advanced radar systems, *may we not also devise the means to remain unseen?*

References

[1] Y. Ma, G. Zhou, and S. Wang, "Wifi sensing with channel state information: A survey," *ACM Comput. Surv.*, vol. 52, no. 3, Jun. 2019. [Online]. Available: https://doi.org/10.1145/3310194

[2] Y. Ge, A. Taha, S. A. Shah, K. Dashtipour, S. Zhu, J. Cooper, Q. H. Abbasi, and M. A. Imran, "Contactless wifi sensing and monitoring for future healthcare - emerging trends, challenges, and opportunities," *IEEE Reviews in Biomedical Engineering*, vol. 16, pp. 171–191, 2023.

[3] H. Jiang, C. Cai, X. Ma, Y. Yang, and J. Liu, "Smart home based on wifi sensing: A survey," *IEEE Access*, vol. 6, pp. 13 317–13 325, 2018.

[4] S. Zhang, R. H. Venkatnarayan, and M. Shahzad, "A wifi-based home security system," in *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2020, pp. 129–137.

[5] Y. Zhu, Z. Xiao, Y. Chen, Z. Li, M. Liu, B. Zhao, and H. Zheng, "Et tu alexa? when commodity wifi devices turn into adversarial motion sensors," in *Proceedings 2020 Network and Distributed System Security Symposium*, 01 2020.

[6] H. Sun, L. G. Chia, and S. G. Razul, "Through-wall human sensing with wifi passive radar," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 57, no. 4, pp. 2135–2148, 2021.

[7] J. Geng, D. Huang, and F. D. la Torre, "Densepose from wifi," 2022. [Online]. Available: https://arxiv.org/abs/2301.00250

[8] Y. Meng, J. Li, H. Zhu, X. Liang, Y. Liu, and N. Ruan, "Revealing your mobile password via wifi signals: Attacks and countermeasures," *IEEE Transactions on Mobile Computing*, vol. 19, no. 2, pp. 432–449, 2020.

[9] G. Wang, Y. Zou, Z. Zhou, K. Wu, and L. M. Ni, "We can hear you with wi-fi!" *IEEE Transactions on Mobile Computing*, vol. 15, no. 11, pp. 2907–2920, 2016.

[10] F. A. Butt and M. Jalil, "An overview of electronic warfare in radar systems," in *2013 The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE)*, 2013, pp. 213–217.

[11] X. G. Zhang, Y. L. Sun, Q. Yu, Q. Cheng, W. X. Jiang, C.-W. Qiu, and T. J. Cui, "Smart Doppler Cloak Operating in Broad Band and Full Polarizations," *Advanced Materials*, vol. 33, no. 17, p. 2007966, 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/adma.202007966

[12] A. Argyriou, "Obfuscation of human micro-doppler signatures in passive wireless radar," *IEEE Access*, vol. 11, pp. 40 121–40 127, 2023.

[13] R. Reddy and S. Sinha, "State-of-the-art review: Electronic warfare against radar systems," *IEEE Access*, vol. 13, pp. 57 530–57 567, 2025.

[14] I. Ahmad, A. Ullah, and W. Choi, "Wifi-based human sensing with deep learning: Recent advances, challenges, and opportunities," *IEEE Open Journal of the Communications Society*, vol. 5, p. 3595–3623, Jan. 2024.

[15] Z. Wei, W. Chen, S. Ning, W. Lin, N. Li, B. Lian, X. Sun, and J. Zhao, "A survey on wifi-based human identification: Scenarios, challenges, and current solutions," *ACM Transactions on Sensor Networks*, vol. 21, no. 1, p. 1–32, Jan. 2025.

[16] 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. [Online]. Available: https://doi.org/10.1145/3705893

[17] X. Liu, X. Meng, H. Duan, Z. Hu, and M. Wang, "A survey on secure wifi sensing technology: Attacks and defenses," *Sensors*, vol. 25, no. 6, p. 1913, Mar. 2025.

[18] S. Batool, F. Frezza, F. Mangini, and P. Simeoni, "Introduction to radar scattering application in remote sensing and diagnostics: Review," *Atmosphere*, vol. 11, no. 5, 2020. [Online]. Available: https://www.mdpi.com/2073-4433/11/5/517

[19] A. Judice, J. Livin, A. James, and S. Bharathi, "Current advancements in radar communication and its future research directions," in *2023 International Conference on Circuit Power and Computing Technologies (ICCPCT)*, 2023, pp. 203–207.

[20] M. T. Buyukakkaslar, M. A. Erturk, and M. A. Aydin, "A Review on Radar-Based Human Detection Techniques," *Sensors (Basel, Switzerland)*, vol. 24, no. 17, p. 5709, Sep. 2024. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11398015/

[21] S. Jardak, T. Kiuru, M. Metso, P. Pursula, J. Häkli, M. Hirvonen, S. Ahmed, and M.-S. Alouini, "Detection and localization of multiple short range targets using fmcw radar signal," in *2016 Global Symposium on Millimeter Waves (GSMM) ESA Workshop on Millimetre-Wave Technology and Applications*, 2016, pp. 1–4.

[22] M. G. Amin, Z. Zeng, and T. Shan, "Hand gesture recognition based on radar micro-doppler signature envelopes," in *2019 IEEE Radar Conference (RadarConf)*, 2019, pp. 1–6.

[23] A. N. Uwaechia and N. M. Mahyuddin, "A Comprehensive Survey on Millimeter Wave Communications for Fifth-Generation Wireless Networks: Feasibility and Challenges," *IEEE Access*, vol. 8, pp. 62 367–62 414, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9050553/

[24] C. Li, M. Xu, Y. Du, L. Liu, C. Shi, Y. Wang, H. Liu, and Y. Chen, "Practical adversarial attack on wifi sensing through unnoticeable communication packet perturbation," in *Proceedings of the 30th Annual International Conference on Mobile Computing and*

Networking, ser. ACM MobiCom '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 373–387. [Online]. Available: https://doi.org/10.1145/3636534.3649367

[25] D. Rodriguez, J. Wang, and C. Li, "Spoofing attacks to radar motion sensors with portable rf devices," in *2021 IEEE Radio and Wireless Symposium (RWS)*, 2021, pp. 73–75.

[26] R. Komissarov and A. Wool, "Spoofing attacks against vehicular fmcw radar," in *Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security*, ser. ASHES '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 91–97. [Online]. Available: https://doi-org.tudelft.idm.oclc.org/10.1145/3474376.3487283

[27] 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," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3199–3214, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9417240/

[28] R. Reddy Vennam, I. K. Jain, K. Bansal, J. Orozco, P. Shukla, A. Ranganathan, and D. Bharadia, "mm-spoof: Resilient spoofing of automotive millimeter-wave radars using reflect array," in *2023 IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 1807–1821.

[29] D. Li, J. Liu, J. Li, L. Gao, P. Zheng, and Z. He, "Simulation and analysis of repeater deceptive jamming to sar based on shift-frequency," in *2022 International Applied Computational Electromagnetics Society Symposium (ACES-China)*, 2022, pp. 1–4.

[30] S. A. Elgamel and M. S. Abdel-Latif, "Synthetic Aperture Radar Active Decoy," *Advances in Military Technology*, vol. 17, no. 1, pp. 47–62, Apr. 2022. [Online]. Available: https://www.aimt.cz/index.php/aimt/article/view/1520

[31] T. Tian, F. Zhou, X. Bai, Z. Zhang, B. Zhao, and W. Fan, "A partitioned deceptive jamming method against topsar," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 2, pp. 1538–1552, 2020.

[32] 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*. Amsterdam Netherlands: ACM, Aug. 2022, pp. 588–600. [Online]. Available: https://dl.acm.org/doi/10.1145/3544216.3544256

[33] W. Fan, F. Zhou, and T. Tian, "A deceptive jamming template synthesis method for sar using generative adversarial nets," in *IGARSS 2020 - 2020 IEEE International Geoscience and Remote Sensing Symposium*, 2020, pp. 6926–6929.

[34] S. Vellucci, A. Monti, M. Barbuto, A. Toscano, and F. Bilotti, "Progress and perspective on advanced cloaking metasurfaces: from invisibility to intelligent antennas," *EPJ Applied Metamaterials*, vol. 8, p. 7, Jan. 2021.

[35] Y. Yang, J. Wang, C. Song, R. Pei, J. M. Purushothama, and Y. Zhang, "Electromagnetic shielding using flexible embroidery metamaterial absorbers: Design, analysis and experiments," *Materials Design*, vol. 222, p. 111079, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0264127522007018

[36] V. Kozlov, D. Vovchuk, and P. Ginzburg, "Broadband radar invisibility with time-dependent metasurfaces," *Scientific Reports*, vol. 11, no. 1, 2021.

[37] X. Xiong, B. Zheng, A. L. Swindlehurst, J. Tang, and W. Wu, "A new intelligent reflecting surface-aided electromagnetic stealth strategy," *IEEE Wireless Communications Letters*, vol. 13, no. 5, pp. 1498–1502, 2024.

[38] H. Wang, B. Zheng, X. Shao, and R. Zhang, "Intelligent reflecting surface-aided radar spoofing," *IEEE Wireless Communications Letters*, vol. 13, no. 10, pp. 2722–2726, 2024.

[39] A. Salem, C. Masouros, and K.-K. Wong, "On the secrecy performance of interference exploitation with psk: A non-gaussian signaling analysis," *IEEE Transactions on Wireless Communications*, vol. 20, no. 11, pp. 7100–7117, 2021.

[40] T. Xu, "Waveform-Defined Security: A Low-Cost Framework for Secure Communications," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10 652–10 667, Jul. 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9612581

[41] P. Zhu, H. Qiu, W. Meng, X. Yu, G. Cui, and J. Zhu, "Encrypted waveform design for low-probability of intercept radar," in *2024 9th International Conference on Signal and Image Processing (ICSIP)*, 2024, pp. 89–93.

[42] P. Qi, Y. Meng, S. Zheng, X. Zhou, N. Cheng, and Z. Li, "Adversarial defense embedded waveform design for reliable communication in the physical layer," *IEEE Internet of Things Journal*, vol. 11, no. 10, pp. 18 136–18 153, 2024.

[43] T. Moon, J. Park, and S. Kim, "Bluefmcw: random frequency hopping radar for mitigation of interference and spoofing," *EURASIP Journal on Advances in Signal Processing*, vol. 2022, no. 1, 2022.

[44] Ailiya, W. Yi, and Y. Yuan, "Reinforcement learning-based joint adaptive frequency hopping and pulse-width allocation for radar anti-jamming," in *2020 IEEE Radar Conference (RadarConf20)*, 2020, pp. 1–6.

[45] J. Zhao, S. Qiao, J. H. Booske, and N. Behdad, "Low probability of intercept/detect (lpi/lpd) secure communications using antenna arrays employing rapid sidelobe time modulation," *IEEE Transactions on Antennas and Propagation*, vol. 72, no. 8, pp. 6448–6463, 2024.

[46] X. Jiao, M. Mehari, W. Liu, M. Aslam, and I. Moerman, "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, ser. WiSec '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 377–379. [Online]. Available: https://doi.org/10.1145/3448300.3468255

[47] M. Cominelli, F. Gringoli, and R. Lo Cigno, "AntiSense: Standard-compliant CSI obfuscation against unauthorized Wi-Fi sensing," *Computer Communications*, vol. 185, pp. 92–103, Mar. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366421004916

[48] Z. Chu, G. Li, Q. Meng, H. Li, and Y. Zeng, "Defeating CSI obfuscation mechanisms: A study on unauthorized Wi-Fi Sensing in wireless sensor network," *Computer Networks*, vol. 263, p. 111208, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128625001768

[49] J. Jiang, J. Wang, Y. Liu, Y. Chen, and Y. Liu, "Wicloak: Protect location privacy of wifi devices," in *2024 23rd ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, 2024, pp. 101–112.

[50] J. Blakely and S. Pethel, "Quantum limits to classically spoofing an electromagnetic signal," *Physical Review Research*, vol. 4, Jun. 2022.

[51] E. Giusti, M. Martorella, A. Capria, M. Conti, C. Moscardini, and F. Berizzi, "Electronic countermeasure for ofdm-based imaging passive radars," in *2018 International Conference on Radar (RADAR)*, 2018, pp. 1–4.

[52] P. Falcone, F. Colone, A. Macera, D. Pastina, and P. Lombardo, "Advances in isar processing for high resolution cross-range profiling with passive radar," in *2012 13th International Radar Symposium*, 2012, pp. 421–425.

[53] R. L. Cigno, F. Gringoli, M. Cominelli, and L. Ghiro, "Integrating csi sensing in wireless networks: Challenges to privacy and countermeasures," *IEEE Network*, vol. 36, no. 4, pp. 174–180, 2022.

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

[55] T. Xu, "Waveform-defined privacy: A signal solution to protect wireless sensing," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, 2021, pp. 1–5.

[56] H. Mohammed and D. Saha, "Encrypted-OFDM: A secured wireless waveform," *Computer Networks*, vol. 255, p. 110871, Dec. 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128624007035

[57] J. Hu, H. Jiang, S. Chen, Q. Zhang, Z. Xiao, D. Liu, J. Liu, and B. Li, "Wishield: Privacy against wi-fi human tracking," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 10, pp. 2970–2984, 2024.

[58] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 24, no. 2, pp. 767–809, 2022.

[59] Y. Yao, Y. Li, X. Liu, Z. Chi, W. Wang, T. Xie, and T. Zhu, "Aegis: An Interference-Negligible RF Sensing Shield," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, Apr. 2018, pp. 1718–1726. [Online]. Available: https://ieeexplore.ieee.org/document/8485883

[60] T. Ropitault, S. Blandino, A. Sahoo, and N. T. Golmie, "Ieee 802.11bf: Enabling the widespread adoption of wi-fi sensing," 2023-05-31 2023. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=935175

[61] S. Roeser and S. Copeland, "TU Delft Code of Conduct," Delft University of Technology, 2020.