Privacy And Security Risks of Passive Through-Wall Wi-Fi Sensing: A Survey Of CSI-Based Attacks and Defense Mechanisms

Sakshi Laxman Jadhav[1], Vaishnavi Surykant Kalokhe[2], Mrs. Guna Dhondwad[3]
[1,2,3]*MIT Arts Commerce and Science College, Alandi*
doi.org/10.64643/ijirt.208601-459

***Abstract*—Wi-Fi sensing has emerged as an important technology that uses wireless signals to detect and analyze changes in the surrounding environment. Unlike conventional Wi-Fi communication, sensing techniques can extract information about human presence, movement, location, and other activities from changes in wireless signals. Recent research has raised significant privacy and security concerns because attackers may exploit these capabilities to monitor individuals without their knowledge.**

This paper presents a survey of current techniques that demonstrate the possibility of spying through walls using Wi-Fi signals, with particular focus on passive Wi-Fi sensing attacks. The survey examines techniques based on Channel State Information (CSI) and other Wi-Fi signal characteristics that allow an observer to infer presence, motion, activity, and in some settings movement direction behind physical barriers. Existing research demonstrates that wireless observations can reveal sensitive behavioral information without requiring a conventional camera or direct visual access. The paper reviews passive attack models, CSI-based sensing pipelines, through-wall sensing research, and defense approaches including channel obfuscation, privacy-preserving signal processing, active defenses, and passive system-level protections. It also identifies limitations such as environmental dependence, hardware availability, multipath effects, multiperson interference, and the gap between controlled experiments and real-world deployment. Finally, the paper discusses future directions for secure Wi-Fi sensing, including privacy-aware wireless standards, controlled CSI access, attack detection, adaptive defenses, and privacy-preserving machine learning.

***Index Terms*—Wi-Fi Sensing; Through-Wall Sensing; Channel State Information (CSI); Passive Attack; Wireless Security; Privacy; Human Activity Recognition; Wi-Fi Security**

I. INTRODUCTION

Wireless communication signals are increasingly being reused as a sensing medium. Traditional Wi-Fi systems are designed to transport information between devices, but the same radio signals also interact with people and objects in the physical environment. Changes in reflection, scattering, absorption, and multipath propagation can alter measurable characteristics of the wireless channel. By analyzing these changes, sensing systems can infer physical events such as human presence, movement, activity, and location [1], [2].

The growth of Wi-Fi sensing is driven by attractive properties such as low deployment cost, non-contact operation, and the availability of wireless infrastructure. Applications include indoor localization, human activity recognition, healthcare monitoring, fall detection, smart-home automation, and security monitoring [1], [2]. Research has also demonstrated sensing in non-line-of-sight and through-wall conditions, showing that wireless sensing is not limited to open line-of-sight environments [3], [4].

These benefits create a corresponding privacy problem. A person may reasonably expect a wall to provide visual privacy, yet wireless signals can interact with the environment on both sides of a wall. A malicious observer who can obtain suitable wireless measurements may therefore infer information about activity inside a protected space. Unlike conventional network attacks, this threat can be difficult to notice because the attacker may only observe existing radio transmissions rather than interrupting communication [1], [5].

This paper focuses on passive Wi-Fi sensing attacks and their privacy implications, particularly in through

wall scenarios. The objective is not to provide operational instructions for surveillance, but to organize existing research, explain the technical basis of the threat, compare attack and defense approaches, and identify open research problems.

II. RESEARCH OBJECTIVES

The main objectives of this survey are:

1. To explain the technical foundations of Wi-Fi sensing and Channel State Information (CSI).
2. To examine how passive observation of wireless signals can support human presence, motion, activity, and location inference.
3. To review research demonstrating Wi-Fi sensing in non-line-of-sight and through-wall environments.
4. To analyze the privacy and security risks created by passive sensing.
5. To classify and compare existing defense mechanisms.
6. To identify limitations in current research and propose future research directions for privacy-preserving Wi-Fi sensing.

III. BACKGROUND AND TECHNICAL FOUNDATIONS

3.1. Wi-Fi Sensing

Wi-Fi sensing uses changes in radio-frequency propagation to infer properties of the physical environment. A transmitter emits a wireless signal, the signal interacts with the environment, and a receiver measures the resulting channel. Human movement changes some propagation paths and therefore changes the observed wireless measurements.

A simplified sensing chain is:
Wi-Fi transmission → environmental interaction → channel variation → measurement collection → preprocessing → feature extraction → inference.
The inference stage may use statistical signal processing or machine-learning models. The sensing output can be a binary event such as presence/absence or a richer classification such as an activity or estimated location

3.2. Channel State Information

CSI describes how a wireless channel affects transmitted signals. In OFDM-based Wi-Fi, the channel can be characterized across multiple subcarriers. CSI commonly includes amplitude and phase information for these subcarriers. A simplified channel representation is: $H(f) = |H(f)| \exp(j\theta(f))$ where $|H(f)|$ is the channel amplitude response and $\theta(f)$ is the phase response at a particular frequency or subcarrier.
When a person moves, reflections and scattering paths can change, causing time-varying CSI. These changes can be filtered, transformed, and classified to infer physical events [1].

3.3. Multipath Propagation

Indoor radio propagation is dominated by multipath effects. Signals may reach a receiver through direct, reflected, and scattered paths. Walls, furniture, doors, and human bodies can contribute to these paths. Multipath is normally treated as a communication challenge, but for sensing it becomes a source of environmental information.

3.4. Through-Wall and Non-Line-of-Sight Sensing

Research has demonstrated that Wi-Fi CSI can be used for human activity recognition beyond direct line of sight. A 2024 study evaluated low-cost ESP32-S3-based directional antenna systems for long-range through-wall human activity recognition and reported strong performance in its experimental office environment [3]. Another study investigated through-wall imaging from Wi-Fi CSI and showed that learned models can translate CSI measurements into image-like representations for downstream tasks [4].
These studies demonstrate feasibility under particular experimental conditions; they should not be interpreted as proof that reliable surveillance is possible in every building or through every wall. Material composition, wall thickness, antenna placement, distance, interference, device capabilities, and environmental changes can strongly affect performance [3], [4].

IV. PASSIVE WI-FI SENSING ATTACK MODEL

A passive Wi-Fi sensing attack is an observation-based threat in which the adversary attempts to infer private information from wireless signals without intentionally modifying the communication or sensing environment. The distinction is important because traditional intrusion detection mechanisms often focus

on network events such as authentication failures, packet injection, scanning, or denial of service.

The passive sensing threat can be represented conceptually as:
Existing wireless activity → observation → signal/channel features → processing → inference of private information.
The inferred information may include occupancy, movement, activity, approximate location, or behavioral patterns. A recent survey of secure Wi-Fi sensing classifies attacks as active or passive and describes passive attacks as monitoring/eavesdropping approaches that aim to obtain sensitive information without altering the sensing system [1].
The feasibility of a passive attack depends on the observer's access to useful measurements. Not all Wi-Fi hardware exposes raw CSI, and signal quality can degrade with distance, walls, interference, and environmental variability. Therefore, a responsible security assessment should distinguish between theoretical information leakage and a repeatable real-world attack capability.

V. LITERATURE REVIEW

5.1. Secure Wi-Fi Sensing Survey

Liu et al. [1] published a 2025 survey that provides a broad taxonomy of attacks and defenses in Wi-Fi sensing. The authors divide attacks into active and passive categories and defenses into active and passive categories. The survey identifies privacy leakage through sensing as a major concern and discusses approaches including signal obfuscation and privacy-preserving mechanisms.

5.2. Wi-Fi CSI Sensing

Armenta-Garcia et al. [2] reviewed Wi-Fi sensing applications, preprocessing methods, and detection algorithms based on CSI. Their work shows the breadth of sensing tasks that can be derived from channel measurements, while also emphasizing the importance of preprocessing and model design.

5.3. Through-Wall Human Activity Recognition

A 2024 Engineering Applications of Artificial Intelligence study investigated Wi-Fi-based human activity recognition through walls using deep learning [3]. The study addresses the challenge that non-line-of-sight paths can be weaker and more unpredictable than direct paths, yet demonstrates the potential of CSI-based models to recognize activities beyond walls.

5.4. Through-Wall Imaging

Strohmayer et al. explored through-wall imaging using Wi-Fi CSI and multimodal learning [4]. The work illustrates how CSI can be transformed into representations that support image-based downstream analysis. From a privacy perspective, this direction is significant because it shows that wireless measurements can potentially reveal increasingly rich descriptions of an indoor environment.

5.5. Passive Wireless Human Sensing

Passive Wi-Fi radar research has shown that ordinary Wi-Fi transmissions, including beacon-like signals in some scenarios, can be used as illumination for human sensing [5]. Earlier passive Wi-Fi sensing research also explored health-related measurements such as breathing, tremor, and falls [6]. These works demonstrate that wireless sensing does not necessarily require a dedicated radar transmitter.

5.6. Privacy-Preserving Defenses

IRShield is a representative defense approach that uses an intelligent reflecting surface to intentionally obfuscate wireless channels. The published evaluation reported substantial reduction in a state-of-the-art human motion detection attack under the tested conditions [7]. More recent work has also investigated time-varying CSI obfuscation for protecting Wi-Fi sensing and communication against covert eavesdropping [8].

VI. TAXONOMY OF PRIVACY THREATS

The reviewed literature suggests several privacy threat categories:

A. Presence inference: determining whether a space is occupied.
B. Motion inference: detecting movement or changes in movement.
C. Activity inference: classifying activities such as walking, sitting, or falling.
D. Location inference: estimating the position or movement path of a person.
E. Behavioral inference: combining repeated

observations to identify routines or patterns.

F. Identity-related inference: exploiting unique movement or gait characteristics to distinguish individuals.

The risk generally increases as the sensing output becomes more detailed. A binary occupancy result reveals less information than a continuous behavioral profile. However, repeated low-level observations can accumulate into sensitive information even when each individual observation appears harmless.

VII. COMPARISON OF ATTACK AND DEFENSE APPROACHES

The following comparison summarizes the major approaches identified in the literature. Attack/Threat | Primary information | Typical requirement | Main privacy concern Passive channel observation | Presence/motion | Access to suitable wireless measurements | Difficult to notice CSI-based activity inference | Activities | CSI or comparable channel features | Behavioral leakage Through-wall HAR | Activity beyond wall | Suitable RF geometry and trained model | Loss of physical privacy Through-wall imaging | Environment/person representation | High-quality data and trained model | Rich visual/semantic leakage Gait/behavioral inference | Identity-related patterns | Stable sensing configuration | Long-term tracking Defense | Basic principle | Advantage | Limitation CSI access control | Restrict detailed channel data | Reduces unauthorized collection | Does not stop all physicallayer leakage Signal/channel obfuscation | Make observations less informative | Directly targets sensing | May affect communication/sensing quality Metasurface-based defense | Randomize propagation environment | Strong physical-layer protection potential | Additional hardware/infrastructure Privacy-preserving ML | Minimize sensitive outputs | Supports legitimate applications | Requires careful model design Detection and policy controls | Identify or limit unauthorized sensing | Useful for governance | Difficult when observation is passive

VIII. PRIVACY AND SECURITY ANALYSIS

8.1. Loss of Physical Privacy

The most important concern is that wireless sensing can weaken the traditional assumption that physical separation guarantees privacy. Walls can block direct vision while still allowing radio-frequency interactions.

8.2. Stealth

Passive observation may not generate obvious network symptoms. If no packets are modified and no service is interrupted, a conventional network monitoring system may have limited visibility into the sensing activity [1].

8.3. Data Aggregation Risk

A single sensing event may be low sensitivity, but repeated measurements can reveal routines. For example, repeated occupancy observations could reveal approximate schedules. This is a classic privacy amplification problem: small pieces of information can become sensitive when aggregated.

8.4. Security of Legitimate Sensing Systems

The problem is not limited to external attackers. Legitimate Wi-Fi sensing systems also need strong access control, data minimization, secure storage, and transparent consent mechanisms. A sensing system that collects detailed CSI should treat the data as potentially sensitive rather than as ordinary network telemetry.

8.5. Limitations of Encryption

Wi-Fi encryption protects communication contents, but sensing may depend on physical-layer channel characteristics rather than application-layer payloads. Therefore, encryption alone should not be considered a complete defense against every Wi-Fi sensing privacy threat.

IX. DEFENSE MECHANISMS

9.1. CSI and Hardware Access Control

Restricting access to raw or high-resolution CSI can reduce the number of applications capable of performing detailed sensing. Operating-system permissions, driver controls, hardware-level restrictions, and authenticated sensing interfaces are potential approaches.

9.2. Channel Obfuscation

Channel obfuscation deliberately changes the wireless propagation environment or the observed signal so that

unauthorized sensing becomes unreliable. IRShield demonstrates the use of intelligent reflecting surfaces for this purpose [7]. Time-varying CSI obfuscation is another direction that attempts to preserve legitimate communication while reducing information available to unauthorized observers [8].

9.3. Privacy-Preserving Machine Learning

A sensing system can be designed to output only the information needed for a legitimate task. Local processing, feature minimization, privacy-preserving representations, and controlled model access can reduce unnecessary exposure.

9.4. Active Defense

Active defenses intentionally modify wireless conditions to mislead or degrade unauthorized inference. Examples include controlled channel perturbation and adversarial signal transformation. Their main challenge is avoiding unacceptable impact on legitimate users.

9.5. Passive Defense

Passive defenses include access control, data minimization, secure storage, auditing, user consent, and organizational policies. These measures do not necessarily alter the radio environment but can reduce the consequences of sensing data leakage.

9.6. Combined Defense

No single mechanism is likely to solve the entire problem. A practical architecture should combine physical layer protection, access control, privacy-aware processing, monitoring, and governance.

X. RESEARCH GAPS

The literature reveals several research gaps.

1. Real-world generalization: Many sensing systems are evaluated in controlled environments. More diverse buildings, materials, device configurations, and interference conditions are required.
2. Standardized evaluation: Research would benefit from common metrics for privacy leakage, sensing accuracy, attacker capability, wall conditions, and communication overhead.
3. Multi-person environments: Separating multiple individuals remains difficult because their signal effects overlap.
4. Hardware accessibility: CSI availability differs substantially across Wi-Fi chipsets and firmware. A realistic threat model must explicitly state the measurement capability assumed.
5. Detection of passive observers: Because passive sensing can be difficult to observe, new methods are needed to detect suspicious physical-layer observation without degrading normal communication.
6. Utility-privacy trade-off: Defenses must protect users without destroying legitimate applications such as fall detection or emergency monitoring.
7. Ethical and legal governance: Technical feasibility does not define acceptable use. Consent, transparency, data minimization, and accountability should be integrated into system design.

XI. PROPOSED PRIVACY-PRESERVING ARCHITECTURE

Based on the reviewed literature, this paper proposes a conceptual layered architecture for secure Wi-Fi sensing.

Layer 1 Wireless Environment: Wi-Fi access points and client devices generate normal communication signals.

Layer 2 Measurement Protection: Raw CSI and related measurements are restricted using hardware/driver permissions and authenticated interfaces.

Layer 3 Privacy Filter: The sensing pipeline removes unnecessary information and applies controlled obfuscation when required.

Layer 4 Local Inference: Machine-learning inference is performed locally whenever possible so that raw measurements do not leave the trusted environment.

Layer 5 Policy and Consent: Users and administrators define when sensing is permitted, what information may be inferred, and how long data can be retained.

Layer 6 Monitoring and Audit: Access to sensing data is logged, abnormal collection patterns are investigated, and privacy policies are periodically reviewed. The architecture follows a defense-in-depth principle. If one layer fails, the remaining layers can reduce the likelihood or impact of privacy leakage.

XII. FUTURE SCOPE

Future work should investigate privacy-aware Wi-Fi standards and interfaces that explicitly consider sensing as a security property. Research should also explore adaptive defenses that recognize when a high privacy risk exists and change the sensing or propagation environment accordingly.

Another important direction is privacy-preserving machine learning. Instead of transmitting raw CSI to a central server, models could perform inference locally and return only the minimum information required by the application.

Benchmark datasets should also include realistic through-wall conditions, multiple occupants, changing furniture, different wall materials, and cross-device evaluation. Such datasets would help determine whether reported sensing capabilities generalize beyond laboratory environments.

Finally, future research should connect technical defenses with ethical and legal requirements. A system capable of sensing through walls should provide clear consent mechanisms, data-retention limits, access controls, and accountability.

XIII. CONCLUSION

Wi-Fi sensing transforms ordinary wireless communication infrastructure into a source of information about the physical environment. CSI and related signal characteristics can support useful applications including activity recognition, localization, and health monitoring. At the same time, the ability to infer human activity without cameras creates a significant privacy challenge.

This survey reviewed passive Wi-Fi sensing as a security and privacy threat, with particular emphasis on through-wall and non-line-of-sight sensing. Existing research demonstrates the feasibility of human activity recognition and richer environmental inference under specific experimental conditions [1]–[5]. Passive observation is especially concerning because it may not require modification of communication and may therefore be difficult for users to detect.The review also examined defenses including CSI access control, channel obfuscation, intelligent reflecting surfaces, privacy-preserving machine learning, active defenses, and passive governance measures. Current defenses face trade-offs involving cost, communication quality, sensing utility, deployment complexity, and generalization.

The central conclusion is that Wi-Fi sensing should be treated as both a sensing technology and a cybersecurity/privacy surface. Future wireless systems should incorporate sensing privacy from the design stage. Stronger measurement controls, privacy-preserving inference, adaptive channel protection, standardized evaluation, and clear consent and governance mechanisms are necessary for secure and responsible deployment.

REFERENCES

[1] 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, Art. no. 1913, 2025, doi: 10.3390/s25061913.

[2] J. A. Armenta-Garcia, F. F. Gonzalez-Navarro, and J. Caro-Gutierrez, “Wireless sensing applications with WiFi Channel State Information, preprocessing techniques, and detection algorithms: A survey,” Computer Communications, vol. 224, pp. 254–274, 2024, doi: 10.1016/j.comcom.2024.06.011.

[3] “WiFi-based human activity recognition through wall using deep learning,” Engineering Applications of Artificial Intelligence, vol. 127, Art. no. 107171, 2024, doi: 10.1016/j.engappai.2023.107171.

[4] J. Strohmayer, R. Sterzinger, C. Stippel, and M. Kampel, “Through-wall imaging based on WiFi Channel State Information,” arXiv:2401.17417, 2024.

[5] “Passive WiFi Radar for Human Sensing Using A Stand-Alone Access Point,” University College London Repository, 2020.

[6] U. M. Khan, Z. Kabir, and S. A. Hassan, “Wireless health monitoring using passive WiFi sensing,” arXiv:1704.00620, 2017.

[7] “IRShield: A countermeasure against adversarial physical-layer wireless sensing,” research paper on privacy-preserving wireless sensing using intelligent reflecting surfaces, 2021.

[8] Z. Chu, G. Li, Q. Meng, H. Li, and Y. Zeng, “Privacy-preserving WiFi sensing in WSNs via CSI obfuscation,” *Computers & Security*, 2025.