The Metamorphosis of Signal:

WiFi Sensing and the New Physics of Spatial Perception

A Multidisciplinary Analysis of Radio Wave Physics, Artificial Intelligence, IEEE 802.11bf Standardization, and Ethical-Societal Implications

Federico Prevosto

Co-Founder, GRAL
Torino, Italy

GRAL Research Paper
April 2026

Abstract

WiFi Sensing represents a paradigm shift in the very conception of wireless networks: from passive infrastructure for binary data transport to an active perceptual system capable of detecting the presence, movement, morphology, and even vital parameters of human beings through the analysis of perturbations in Channel State Information (CSI). This paper provides a multidisciplinary and systematic analysis of this emerging technology, integrating the physical foundations of multipath propagation, deep learning architectures for human pose estimation, passive biometric identification mechanisms, contactless vital sign monitoring, and ethical and security implications. The IEEE 802.11bf standard, officially published in September 2025, is examined in depth as the milestone that formally transitions WiFi from a communication medium to a native sensing platform. The most recent research frontiers are analyzed, including the integration of Large Language Models (LLMs) with CSI data, adversarial attacks on sensing systems, and privacy countermeasures. The paper concludes with a forward-looking perspective on open challenges and future research directions, outlining a vision in which every connected environment will become inherently aware of the presence and health status of its occupants.

Keywords: *WiFi Sensing, Channel State Information, IEEE 802.11bf, Deep Learning, DensePose, Passive Biometrics, Contactless Vital Sign Monitoring, Privacy, Adversarial Attacks, Large Language Models, Ambient Intelligence.*

Table of Contents

Table of Contents

1. Introduction

1.1 The Paradox of Perceptual Invisibility

Until recently, the WiFi signal was conceived exclusively as a vector for the transport of binary data — an invisible current of encoded information whose only recognized function was to connect devices to each other and to the global network. The electromagnetic waves emitted by residential and enterprise routers traversed bodies, walls, and furnishings without any informational value being attributed to these interactions. The perturbations suffered by the signal during multipath propagation were regarded as noise to be minimized, not data to be extracted.

However, scientific research over the past decade has revealed a fundamental paradox: those very distortions once deemed undesirable contain an enormous wealth of information about the physical environment traversed. Every reflection, absorption, and scattering event of the signal constitutes, in effect, a fingerprint of the space and the bodies occupying it. WiFi Sensing is the discipline that inverts the traditional perspective, transforming the router from a simple communication node into a sophisticated environmental sensor, capable of "seeing" through opaque obstacles without the aid of cameras, wearable sensors, or any additional device.

1.2 Context and Motivations

The need to monitor indoor spaces has grown exponentially in recent years, driven by multiple converging factors. Industrial automation requires spatial awareness systems to ensure operator safety on production lines. Remote healthcare, accelerated by the COVID-19 pandemic, demands continuous monitoring tools for frail and elderly patients in home settings. Next-generation smart homes require adaptive systems that understand not only whether a room is occupied, but by whom, in what posture, and with what vital parameters.

Traditional ambient sensing technologies present significant structural limitations that WiFi Sensing promises to overcome. Cameras, while offering the highest perceptual resolution, raise severe privacy concerns and are ineffective in low-light conditions or under occlusion. Passive infrared (PIR) sensors have limited range, cannot distinguish between humans and pets, and provide no information about posture or identity. Wearable devices require constant maintenance, user compliance, and fail when forgotten or removed. Dedicated LiDAR and radar systems, while effective, entail high hardware costs and significant power consumption.

WiFi Sensing overcomes these obstacles by leveraging an infrastructure that is already ubiquitous and operational in virtually every inhabited environment on the planet. According to the most recent estimates, over 20 billion active WiFi devices exist worldwide as of 2025. This

ubiquity represents an unprecedented competitive advantage: no new hardware needs to be installed; the task is simply to extract information already embedded in existing signals.

1.3 Objectives and Structure of the Paper

This paper aims to provide a comprehensive, rigorous, and up-to-date analysis of WiFi Sensing, organized along a multidisciplinary structure that reflects the intrinsic complexity of the field. Section 2 presents the physical foundations of radio propagation and Channel State Information architecture. Section 3 examines the artificial intelligence architectures employed for human pose estimation and activity recognition. Section 4 explores the frontiers of passive biometrics and individual identification. Section 5 analyzes contactless vital sign monitoring. Section 6 is dedicated to the IEEE 802.11bf standard. Section 7 addresses security concerns, adversarial attacks, and privacy. Section 8 presents the emerging convergence between WiFi Sensing and Large Language Models. Section 9 illustrates real-world application domains. Finally, Section 10 outlines open challenges and future directions.

2. Physical Foundations of Radio Propagation and Channel State Information

2.1 Multipath Propagation Mechanics

The physical principle underlying WiFi Sensing resides in the fundamental interaction between electromagnetic waves and matter. A WiFi signal, transmitted in the 2.4 GHz, 5 GHz, and more recently 6 GHz frequency bands, does not travel a single straight-line path from transmitter to receiver. Instead, radio waves undergo a complex series of physical phenomena during propagation: reflection off rigid surfaces (walls, floors, furniture), diffraction around edges, scattering from irregular surfaces, and absorption by materials with high water content.

The human body, composed of approximately 60% water, acts as a particularly significant dynamic obstacle for radio waves at WiFi frequencies. The dielectric constant of water at 2.4 GHz is approximately 80, orders of magnitude greater than that of air (approximately 1). This means the human body reflects, absorbs, and shields a significant portion of incident electromagnetic energy. When a person moves within an environment, they dynamically alter the signal propagation paths, generating measurable variations in the radio channel response.

The result is the multipath propagation phenomenon: the transmitted signal reaches the receiver through hundreds or thousands of distinct trajectories, each with a specific time delay, attenuation, and phase shift. The coherent superposition of all these paths at the receiver generates a complex interference pattern that changes as a function of the environment's geometry and the positions of the bodies within it.

2.2 From RSSI to CSI: A Revolution in Granularity

For decades, the only commonly accessible indicator of radio channel quality was the Received Signal Strength Indicator (RSSI), a scalar measure of the total power of the received signal. RSSI presents fundamental limitations for sensing: as a single aggregated value, it cannot distinguish between variations induced by different subcarriers nor capture phase information, making it sensitive to noise and environmental fluctuations.

The true revolution arrived with Channel State Information (CSI), made accessible starting with the IEEE 802.11n standard and its successors. In modern WiFi standards, transmission employs Orthogonal Frequency Division Multiplexing (OFDM) technology, which divides the radio channel into multiple orthogonal subcarriers. CSI captures the channel response for each individual subcarrier, providing a complex vector description of the radio channel:

$$H(f, t) = A(f, t) \cdot e^{j\varphi(f, t)}$$

where H is the channel frequency response, A(f, t) represents the amplitude of the subcarrier at frequency f and time t, and φ(f, t) the corresponding phase. In a WiFi system with 56 subcarriers and 3 antennas, CSI produces a 3×56 matrix of complex values for each received packet, with an acquisition rate that can reach 1,000 packets per second.

This spectral and temporal granularity is the key that unlocked modern WiFi Sensing. By analyzing the temporal variation of the CSI matrix across all subcarriers and antennas, it becomes possible to isolate Doppler frequencies induced by human movements, separating them from the static contribution of the surrounding environment.

2.3 The Fresnel Model and Micro-Movement Sensitivity

An aspect often overlooked in the popular literature, yet fundamental to understanding the sensitivity of WiFi Sensing, is the Fresnel zone model. When a body moves within the first Fresnel zone between transmitter and receiver — the ellipsoidal region where the path length difference is less than half a wavelength — CSI variations are maximized. At 5 GHz, the wavelength is approximately 6 cm, meaning that displacements on the order of a few centimeters can generate significant phase variations.

This submillimeter phase sensitivity is what makes micro-movement monitoring possible: oscillations of the chest wall during breathing (typical amplitude: 4–12 mm) and cardiac pulsations transmitted to the body surface (typical amplitude: 0.2–0.5 mm). The CSI ratio, computed between co-located antennas, eliminates common environmental noise and isolates variations induced exclusively by the target’s movement.

3. Artificial Intelligence Architectures for WiFi Sensing

3.1 From Raw Signal to Semantic Understanding

CSI produces an inherently complex and noisy data stream. Raw data contains overlapping contributions from static sources (walls, furniture), electromagnetic interference, and human movements of interest. Artificial intelligence intervenes to solve what physics terms an inverse problem: starting from the perturbations of the received signal, it reconstructs the cause that generated them — namely the position, pose, and identity of human beings in the environment.

The evolution of AI architectures applied to WiFi Sensing can be divided into three distinct generations. The first generation (2015–2018) relied on traditional machine learning methods: Support Vector Machines (SVM), Random Forest, and Gaussian Mixture Models, fed by manually extracted CSI features (variance, entropy, wavelet transform coefficients). These methods achieved accuracies of 80–90% in recognizing macro-activities (walking, sitting, standing), but proved fragile with respect to environmental changes.

The second generation (2018–2022) introduced end-to-end deep learning. Convolutional Neural Networks (CNNs) treat CSI data as two-dimensional images — time-frequency spectrograms — identifying discriminative patterns without manual feature engineering. Recurrent networks (LSTM, GRU, BiGRU) capture temporal dependencies in CSI sequences, proving particularly effective for recognizing cyclic activities such as walking. Hybrid CNN-LSTM architectures combine the advantages of both approaches.

The third generation (2022–present) is characterized by the adoption of Transformer architectures and attention mechanisms, capable of modeling global relationships in CSI data and generalizing better across diverse environments. Transformers excel at capturing long-range correlations between subcarriers and time instants, overcoming the local receptive field limitations of CNNs.

3.2 DensePose from WiFi: Dense Pose Estimation

The seminal study “DensePose from WiFi,” published in January 2023 by a team at Carnegie Mellon University, represented a milestone in the field. The researchers demonstrated that it is possible to estimate dense human body pose — that is, point-to-point correspondence between the 2D body surface and the 3D model — using exclusively standard WiFi signals, without any camera.

The proposed architecture unfolds in three principal phases. In the first phase, raw CSI samples (amplitude and phase) from three receiving antennas are sanitized through signal cleaning algorithms. In the second phase, a two-branch encoder-decoder translates sanitized CSI

samples into 2D feature maps that emulate features extracted from conventional images. In the third phase, a modified DensePose-RCNN architecture uses these 2D features to estimate UV maps of the human body, representing the dense correspondence between 2D coordinates and the 3D body surface.

A key element of the approach is transfer learning: the model is pre-trained on image-based DensePose, then adapted to accept WiFi inputs. This leverages the rich knowledge about human body structure learned by the visual model. In experiments, the system achieved a mean Average Precision (AP) of 87.2% at the 50% IoU threshold, demonstrating performance comparable to camera-based systems for detecting people's positions.

3.3 RF-Pose and Person-in-WiFi: The Precursors

Before DensePose from WiFi, two foundational studies paved the way for human pose estimation via radio signals. RF-Pose, developed at MIT CSAIL in 2018, first introduced the use of radio signals for human skeleton pose estimation through opaque obstacles. Using a custom radio device operating at sub-6 GHz frequencies, RF-Pose demonstrated that it is possible to detect 14 human body keypoints through walls, with accuracy approaching that of camera-based systems in line-of-sight conditions.

Person-in-WiFi (2019) confirmed the feasibility of identifying the shape and identity of the human body starting exclusively from CSI data extracted from commercial routers. This study showed that standard WiFi signals contain sufficient information for body segmentation and person localization, without the need for specialized hardware.

3.4 Open-Source Implementations and Democratization

A noteworthy recent evolution is the emergence of open-source implementations that make WiFi Sensing accessible to researchers and developers. The RuView project, for example, reimplemented the DensePose from WiFi architecture in Rust, achieving a processing speed of 54,000 frames per second. The system operates on ESP32 microcontrollers costing approximately $9, demonstrating that WiFi Sensing can function on ultra-low-cost hardware, without cloud connectivity, with entirely on-device processing.

4. Passive Biometrics: Identity in the Signal

4.1 The Wireless Fingerprint

Beyond macro-analysis of movement, research is advancing into one of the most fascinating and simultaneously controversial territories of WiFi Sensing: passive biometrics. The fundamental principle is that every individual has a unique body mass, height, gait, and skeletal geometry that produces characteristic and potentially identifying CSI perturbations. In essence, the way a person perturbs an electromagnetic field can serve as a "wireless fingerprint."

The recent literature documents intense research activity in this domain. A comprehensive survey published in 2024 on PMC systematized the three principal phases of WiFi-based human identification: CSI data collection, preprocessing (including feature extraction related to gait, gestures, radio biometrics, and respiratory frequency), and classification through machine learning models.

4.2 Gait Recognition

Gait recognition is considered the most promising biometric mechanism for WiFi Sensing, as it involves full-body motion, is difficult to spoof, and requires no interaction or cooperation from the subject. Systems such as WiWho, WiFi-ID, and WiGait have demonstrated the feasibility of individual identification by analyzing walking cycles reflected in CSI patterns.

GaitFi proposed an innovative multimodal approach combining WiFi signals and video for human identification, using a Lightweight Residual Convolution Network as the backbone. Results showed that fusion of the two perceptual modalities significantly improves robustness compared to unimodal systems, especially under unfavorable lighting conditions.

More recent approaches, such as NeuralWave and HumanFi, adopt deep learning to automatically extract discriminative features from raw CSI, overcoming the limitations of traditional hand-crafted feature classifiers. NeuralWiGait integrates CNN and BiGRU (Bidirectional Gated Recurrent Unit) in a hybrid framework capable of simultaneously capturing spatial and temporal gait features, achieving accuracies exceeding 95% in controlled environments.

4.3 Toward Identification via Millimeter Waves

An emerging frontier is the use of millimeter-wave (mmWave) WiFi at 60 GHz for person identification. Recent research has demonstrated that CSI at 60 GHz significantly outperforms 5 GHz CSI for person identification, owing to the high spatial sensitivity of millimeter waves. Models such as TemporalConvNet and CNN-BiLSTM with temporal attention achieve

accuracies of 93–96% on 60 GHz data, indicating that next-generation WiFi (Wi-Fi 7 and beyond) will bring substantial improvements in wireless biometrics.

4.4 Palm Authentication via WiFi

A particularly innovative application is HandPass, a system for authentication based on WiFi CSI palm scanning. Using a Raspberry Pi with antenna power reduced to 1 dBm, the researchers acquired CSI data from the hands of 20 participants, leveraging the biophysical characteristics of the hand (size, shape, finger angular spread, phalanx length) as biometric markers. The specific electromagnetic signal alterations caused by each hand's unique geometry produce an identifying CSI imprint that can be used for access control.

5. Contactless Vital Sign Monitoring

5.1 The Router as a Passive Diagnostic Device

One of the most promising applications of WiFi Sensing is the contactless monitoring of vital parameters: respiratory rate and heart rate. The physical principle exploited is the submillimeter sensitivity of CSI phase to micro-movements of the chest wall and body surface induced by cardiopulmonary activity.

Breathing generates chest wall oscillations with a typical amplitude of 4–12 mm and a frequency of 12–20 breaths per minute in healthy adults. Cardiac activity generates micro-vibrations with an amplitude of 0.2–0.5 mm and a frequency of 60–100 beats per minute. Both these signals modulate the CSI phase in a detectable manner, provided that environmental noise and static clutter are adequately removed.

5.2 Vital Signal Extraction Techniques

Research has developed two principal approaches for respiratory monitoring. The first uses CSI signal processing in the complex domain, applying band-pass filters and spectral analysis (FFT) to isolate the frequency components corresponding to respiration. The second, more recent approach leverages analysis of the CSI ratio trajectory in the complex plane, where respiratory motion generates characteristic elliptical trajectories.

For cardiac monitoring, the challenges are greater due to the reduced amplitude of vibrations. Advanced techniques include rotary projection combined with adaptive subcarrier selection (HSR subcarrier selection) and end-to-end CNN networks that learn the mapping directly from raw CSI data to heart rate. Hybrid systems combining WiFi CSI with mmWave data have achieved accuracies of 99% in vital sign monitoring under controlled conditions.

5.3 Clinical and Home Applications

Contactless vital sign monitoring has transformative potential in multiple clinical settings. In hospital environments, particularly neonatal intensive care units (NICUs), contactless monitoring eliminates the discomfort and infection risk associated with traditional adhesive sensors. In long-term care facilities, continuous and invisible monitoring of vital parameters enables early detection of health deterioration. A study of 612 residents across five care facilities demonstrated that contactless radar-based monitoring can predict 77% of hospitalizations with an average lead time of 5.6 days, and 89% of those due to respiratory or cardiac conditions.

In the home setting, WiFi Sensing can monitor sleep quality by analyzing nocturnal respiratory patterns, detect apneas, and provide alerts in case of anomalies without requiring any wearable

device. This ability to transform the household router into a passive diagnostic device represents a paradigm shift in preventive healthcare.

6. The IEEE 802.11bf Standard: WiFi Becomes a Native Sensor

6.1 Genesis and Standardization Process

Until recently, WiFi Sensing was limited by the absence of standardized APIs and the heterogeneity of proprietary implementations. The need for a unified framework led to the formation of the IEEE 802.11bf Task Group, first discussed in the Wireless LAN Next-Generation Standing Committee in July 2019. The project was officially authorized in September 2020, with the objective of creating an amendment to the IEEE 802.11 standard that natively enables sensing functionalities.

The standardization process traversed numerous revision cycles: Draft 0.1 was released in April 2022, followed by multiple letter ballots and SA ballots with increasing approval rates (up to 96% in the second SA recirculation of November 2024). The IEEE 802.11bf-2025 standard was officially published on September 26, 2025, marking the definitive transition of WiFi from a communication medium to a sensing platform.

6.2 Technical Architecture of the Standard

The IEEE 802.11bf amendment defines modifications to the Medium Access Control (MAC) layer and the Physical Layer (PHY) service interfaces for High Efficiency (HE), Extremely High Throughput (EHT), Directional Multi-Gigabit (DMG), and Enhanced DMG (EDMG) modes. The operative bands covered include license-exempt frequencies between 1 GHz and 7.125 GHz (2.4, 5, and 6 GHz) and above 45 GHz.

The WLAN sensing framework defined by the standard is structured around five principal operational phases: Sensing Session Setup, in which two or more stations (STAs) negotiate the parameters of the sensing session; Sensing Measurement Setup, where the technical specifications of the measurement are configured (subcarriers, sampling rate, duration); Sensing Measurement Instance, the actual CSI data acquisition phase; Sensing Measurement Termination, for orderly conclusion of the measurement; and finally, the results processing phase.

6.3 Bistatic and Multistatic Sensing

One of the key innovations of the standard is its support for bistatic and multistatic sensing configurations. In monostatic sensing, the transmitter and receiver are the same device; in bistatic sensing, they are separate devices; and in multistatic sensing, multiple devices from different manufacturers collaborate to construct a three-dimensional perceptual map of the environment. This multi-vendor interoperability is the feature that will transform the WiFi ecosystem from a network of independent access points into a distributed perceptual mesh.

The standard also ensures backward compatibility with existing IEEE 802.11 devices, enabling a gradual transition. Next-generation routers will be able to alternate data transmission cycles with high-frequency environmental scanning cycles, with time-sharing optimization that minimizes degradation of communication performance.

7. Security, Adversarial Attacks, and Privacy Implications

7.1 The Privacy Paradox in WiFi Sensing

WiFi Sensing presents a fundamental ethical paradox: the same technology that promises to improve safety and health without violating visual privacy can, paradoxically, become an instrument of invisible surveillance even more pervasive than cameras. An attacker with access to a WiFi device can, in theory, detect the presence, movement, activities, and even keystrokes of a victim without their awareness.

Research has demonstrated that public WiFi sensing datasets contain unintended private information. Studies have shown that gesture and activity recognition datasets can reveal private user attributes such as height, weight, and gender when subjected to targeted attacks. Beamforming feedback, transmitted in plaintext in the 802.11ac standard and subsequent iterations, further exacerbates privacy exposure, enabling more accurate inference of keystrokes and passwords.

7.2 Attack Taxonomy

A comprehensive survey published in 2025 proposed a systematic classification of attacks on WiFi Sensing systems based on three roles: the wireless system as victim, as weapon, and as shield. Analyzing over 200 publications from 2020 to 2024, the researchers identified multiple attack vectors threatening the reliability and security of sensing systems.

Attacks on the sensing target encompass static attacks (use of intelligent reflecting surfaces to alter propagation), dynamic attacks (injection of controlled movements into the environment), and adversarial attacks (perturbations optimized to deceive deep learning models). Attacks on the sensing source include jamming, spoofing, and manipulation of WiFi packet pilot symbols. The WiIntruder framework demonstrated the feasibility of universal perturbation attacks capable of simultaneously degrading the performance of multiple sensing applications, including user authentication and respiratory monitoring.

7.3 Countermeasures and Defenses

The scientific community has responded with a range of countermeasures. CSI obfuscation systems, such as AntiSense and IRShield, introduce spatial randomness into the signal to prevent unauthorized sensing while preserving communication quality. More recent approaches propose source-defined channel randomization techniques that temporally vary the filters applied to the signal, preventing an attacker from building a stable model of the environment.

On the regulatory front, the privacy question in WiFi Sensing remains largely unexplored at the legislative level. The European GDPR could be applicable insofar as processed CSI data enables identification of specific individuals, but established case law is lacking. The IEEE 802.11bf standard includes a separate amendment (802.11bh) specifically dedicated to user privacy protection, but implementation details remain under development.

8. The Convergence of WiFi Sensing and Large Language Models

8.1 A New Paradigm: Wi-Chat and IoT-LLM

One of the most recent and conceptually disruptive frontiers of WiFi Sensing is its integration with Large Language Models (LLMs). The year 2025 saw the publication of Wi-Chat, the first WiFi-based human activity recognition system powered by an LLM. Wi-Chat demonstrates that language models can process raw WiFi signals and infer human activities by incorporating WiFi sensing physical principles into prompts, without resorting to traditional signal processing techniques.

The approach is conceptually revolutionary: instead of training a specialized neural network for each sensing task, Wi-Chat leverages the zero-shot reasoning capability of LLMs, guiding them with physical knowledge about signal propagation. Experimental results show that LLMs can achieve significant performance in activity recognition, opening a paradigm in which understanding of the physical world is mediated by the model's linguistic competence.

8.2 IoT-LLM: Reasoning About Real-World Sensor Data

The IoT-LLM framework, published in Patterns (Cell Press) at the end of 2025, expands this vision by proposing a unified system in which LLMs reason about heterogeneous IoT data, including high-dimensional WiFi CSI data (typical shape: $T \times 3 \times 114$, where T is the temporal length, 3 the antennas, and 114 the subcarriers). The framework uses compression and dimensionality reduction techniques (PCA) to transform CSI data into textualized representations compatible with LLM input.

The evaluation of the framework across five real-world IoT tasks — including WiFi-based human activity recognition and WiFi-based indoor localization — demonstrated that LLMs, when properly guided, can compete with specialized models on traditional sensory tasks. This convergence between natural language processing and physical sensing paves the way for Personal Health LLMs (Ph-LLMs) capable of continuously interpreting WiFi data for proactive health monitoring.

8.3 Implications for Ambient Intelligence

The LLM-WiFi Sensing integration could radically transform the concept of ambient intelligence. In a future scenario, a home system could not only detect that an elderly person has fallen (sensing), but also reason about context ("the user fell in the bathroom at 3 AM, has not risen in 2 minutes, heart rate is irregular"), generate a natural-language alert to medical personnel, and verbally communicate with the victim via a voice assistant — all without any wearable device or camera.

9. Real-World Application Domains

9.1 Invisible Security and Intrusion Detection

WiFi Sensing enables intrusion detection without blind spots and with the ability to distinguish between humans and domestic animals through analysis of the silhouette and gait reflected in the signal. Unlike conventional PIR sensors, a WiFi Sensing system can operate through walls, cover an entire dwelling with a single transmitter-receiver pair, and provide information about the intruder's location and identity.

9.2 Smart Care and Fall Detection

Continuous monitoring of frail individuals in sensitive environments represents perhaps the most urgent and socially relevant application. In bathrooms, where the use of cameras is precluded for ethical reasons and the risk of falls is highest, WiFi Sensing offers a unique solution: continuous monitoring of presence, posture, and vital signs without any visual intrusion. Fall detection is already one of the most mature use cases, with commercial WiFi-based systems achieving sensitivities exceeding 95%.

9.3 Adaptive Energy Management

Optimization of HVAC (Heating, Ventilation, and Air Conditioning) systems and lighting based on actual spatial occupancy and user posture represents an application with significant economic impact. Unlike binary occupancy sensors, WiFi Sensing can determine the exact number of people in a room, their positions, and activity levels, enabling granular and predictive energy adjustments.

9.4 Human-Machine Interaction and Gesture Recognition

WiFi-based gesture recognition enables contactless, device-free control of smart devices. Users can control lights, appliances, and entertainment systems with simple gestures in the air. Research has demonstrated reliable recognition of sign language via WiFi (SignFi), opening possibilities for assistive communication for individuals with hearing disabilities.

9.5 Automotive and In-Vehicle Sensing

WiFi Sensing extends to the vehicular context as well. The V2iFi system demonstrated the feasibility of monitoring vital signs inside a vehicle using WiFi signals, enabling detection of driver drowsiness states, passenger monitoring, and automatic adjustment of comfort systems without dedicated sensors.

10. Open Challenges and Future Directions

10.1 Cross-Domain Generalization

The most significant challenge for WiFi Sensing remains cross-domain generalization: models trained in a specific environment (a room with a particular furniture arrangement and a specific device placement) tend to degrade significantly when transferred to a different environment. The variability in environmental geometry, propagation conditions, and device hardware characteristics renders generalization an open research problem.

Promising approaches include unsupervised domain adaptation, federated learning for distributed training across multiple environments while preserving privacy, and model-based architectures that incorporate radio propagation knowledge into the neural network structure, reducing dependence on environment-specific training data.

10.2 Multi-Person Scalability

Current systems exhibit declining performance when the number of people in the environment exceeds 3–5. Separating individual contributions in the CSI signal in crowded scenarios requires advances in beamforming techniques, MIMO spatial resolution, and multi-target attention architectures.

10.3 Robustness and Security

As documented in Section 7, vulnerability to adversarial attacks represents a significant obstacle for deployment in safety-critical applications. Future research must develop intrinsically robust architectures, formal robustness certification techniques, and mutual authentication protocols between sensing devices.

10.4 Integration with 6G and Next-Generation Networks

Sixth-generation (6G) networks, anticipated around 2030, will natively include sensing capabilities integrated into communication (Integrated Sensing and Communication, ISAC). WiFi Sensing, with the 802.11bf standard, anticipates this convergence in the local area network domain. Interoperability between WiFi Sensing and cellular sensing (5G NR and 6G) will create multi-scale perceptual ecosystems, from room level (WiFi) to urban level (cellular).

10.5 Toward Universal Ambient Intelligence

The long-term vision is one of universal ambient intelligence, in which every connected environment — from a single room to an entire building, from a vehicle to a city — is endowed with native perceptual awareness, without dedicated sensors. With the adoption of the IEEE

802.11bf standard, already published, and the evolution of Large Language Models toward sensory data interpretation, this vision is rapidly transitioning from academic speculation to engineering reality.

The future challenge will no longer be signal coverage, but its perceptual resolution: a world in which the invisible energy that connects us also serves as a silent guardian of our safety and health, balancing the promises of innovation with the non-negotiable respect for privacy and human dignity.

11. Conclusion

WiFi Sensing represents the definitive convergence of telecommunications, artificial intelligence, and spatial perception. With the publication of the IEEE 802.11bf standard in September 2025, WiFi has officially ceased to be exclusively a communication medium, becoming instead a native, standardized, and interoperable sensing platform.

This analysis has documented how this transformation is sustained by solid physical foundations (the submillimeter sensitivity of CSI phase), increasingly sophisticated AI architectures (from CNNs to Transformers, from transfer learning to LLMs), applications of immediate social relevance (elderly monitoring, fall detection, smart healthcare), and a rapidly expanding research ecosystem.

At the same time, this work has highlighted the significant challenges that remain: cross-domain generalization, multi-person scalability, robustness to adversarial attacks, and above all, the ethical paradox of a technology that promises visual privacy while potentially enabling even more pervasive surveillance. The scientific community and legislators must work in synergy to ensure that the ambient intelligence of the future is not only technically effective but ethically sustainable.

In conclusion, WiFi Sensing is not simply a new feature added to routers: it is a paradigm shift in the relationship between human beings and the electromagnetic environment that surrounds them. For the first time in the history of technology, the invisible energy that connects us can also understand us.

References

[1] J. Geng, D. Huang, F. De La Torre, "DensePose From WiFi," arXiv:2301.00250, Carnegie Mellon University, 2023.

[2] M. Zhao, T. Li, M. Abu Alsheikh, Y. Tian, H. Zhao, A. Torralba, D. Katabi, "Through-Wall Human Pose Estimation Using Radio Signals (RF-Pose)," MIT CSAIL, CVPR 2018.

[3] F. Wang, S. Zhou, S. Panev, J. Han, D. Huang, "Person-in-WiFi: Fine-grained Person Perception Using WiFi," ICCV 2019.

[4] T. Ropitault, S. Blandino, A. Sahoo, N. Golmie, "IEEE 802.11bf: Enabling the Widespread Adoption of Wi-Fi Sensing," IEEE Communications Standards Magazine, 2023.

[5] Y. Ma, G. Zhou, S. Wang, H. Zhao, W. Jung, "An Overview on IEEE 802.11bf: WLAN Sensing," IEEE Journal on Selected Areas in Communications, 2024.

[6] IEEE Std 802.11bf-2025, "Amendment 4: Enhancements for Wireless LAN Sensing," IEEE Standards Association, Published September 26, 2025.

[7] X. Liu, X. Meng, H. Duan, Z. Hu, M. Wang, "A Survey on Secure WiFi Sensing Technology: Attacks and Defenses," Sensors, 25(6), 1913, 2025.

[8] M. Alhazbi et al., "WiFi-Based Human Identification with Machine Learning: A Comprehensive Survey," PMC, 2024.

[9] H. Zhang, et al., "Wi-Chat: Large Language Model Powered Wi-Fi Sensing," arXiv:2502.12421, 2025.

[10] T. Zhu, et al., "IoT-LLM: A Framework for Enhancing Large Language Model Reasoning from Real-World Sensor Data," Patterns (Cell Press), 2025.

[11] Y. Lang, et al., "GaitFi: Robust Device-Free Human Identification via WiFi and Videos," IEEE Transactions on Computational Intelligence and AI in Games, 2022.

[12] J. Jiang, S. Jiang, Y. Liu, et al., "Wi-Gait: Pushing the Limits of Robust Passive Personnel Identification Using Wi-Fi Signals," Computer Networks, 229, 2023.

[13] Z. Wu, et al., "NeuralWiGait: An Accurate WiFi-based Gait Recognition System Using Hybrid Deep Learning Framework," The Journal of Supercomputing, 2025.

[14] N. Bhat, et al., "Beyond Sub-6 GHz: Leveraging mmWave Wi-Fi for Gait-Based Person Identification," arXiv:2510.08160, 2025.

[15] L. Silva, et al., "HandPass: A Wi-Fi CSI Palm Authentication Approach for Access Control," arXiv:2510.22133, 2025.

[16] S. Zhou, W. Zhang, et al., "Adversarial WiFi Sensing for Privacy Preservation of Human Behaviors," IEEE Communications Letters, 24(2), 2020.

[17] C. Li, M. Xu, et al., "Practical Adversarial Attack on WiFi Sensing Through Unnoticeable Communication Packet Perturbation," ACM MobiCom, 2024.

[18] Y. Zhou, C. Li, et al., "RIStealth: Practical and Covert Physical-Layer Attack Against WiFi-Based Intrusion Detection via RIS," ACM SenSys, 2023.

[19] M. Cominelli, F. Gringoli, R. Lo Cigno, "AntiSense: Standard-Compliant CSI Obfuscation Against Unauthorized Wi-Fi Sensing," Computer Communications, 185, 2022.

[20] J. Chen, et al., "Privacy-preserving WiFi Sensing in WSNs via CSI Obfuscation," Computers & Security, 2025.

[21] Y. Shi, X. Zhang, L. Fu, H. Zhang, "An Investigation of the Private-Attribute Leakage in WiFi Sensing," High-Confidence Computing, 4, 2024.

[22] M. S. Raheel, et al., "Contactless Vital Sign Monitoring Systems: A Comprehensive Survey," Sensors & Diagnostics, RSC Publishing, 2024.

[23] J. Sun, X. Bian, M. Li, "Non-Contact Heart Rate Monitoring Method Based on Wi-Fi CSI Signal," Sensors, 2024.

[24] P. Sruthi, S. K. Udgata, "Wi-Fi Sensing Based Person Identification and Activity Recognition Using Two-Phase Deep Learning Model," Engineering Applications of Artificial Intelligence, 132, 2024.

[25] L. Zhang, et al., "A Comprehensive Survey on Wi-Fi Sensing for Human Identity Recognition," Electronics, 12(23), 4858, 2023.

[26] S. Shang, et al., "WirelessLLM: Empowering Large Language Models Towards Wireless Intelligence," arXiv:2405.17053, 2024.

[27] RuView Project, "WiFi DensePose: Real-time Human Pose Estimation via WiFi Signals," GitHub, 2025.

[28] R. K. Liu, et al., "Origin Wireless AI: IEEE 802.11bf WiFi Sensing Project," Origin Wireless AI, 2022-2025.

[29] L. Lu, et al., "An Imperceptible Eavesdropping Attack on WiFi Sensing Systems," IEEE/ACM Transactions on Networking, 32, 2024.

[30] Y. Chen, et al., "A Survey of Wireless Sensing Security from a Role-Based View: Victim, Weapon, and Shield," arXiv:2412.03064, 2024.

[31] L. Xu, et al., "Integration of LLMs and the Physical World: Research and Application," ACM Digital Library, 2024.

[32] Tapestry Health / Neteera Technologies, "Contactless Remote Patient Monitoring in Long-Term Care: Collaborative Study on 612 Residents," 2025.

[33] T. Zheng, Z. Chen, C. Cai, J. Luo, X. Zhang, "V2iFi: In-Vehicle Vital Sign Monitoring via Compact RF Sensing," 2020.

[34] WhoFi: WiFi-Based Person Identification Using Deep Neural Networks with Transformer Encoding, NTU-Fi Dataset, Accuracy up to 95.5%, 2025.

[35] IEEE 802.11bh-2024, "Amendment: Enhancements for User Privacy Protection," Published June 3, 2025.