Seeing With WiFi: Exploring the State and Prospects of WiFi Sensing

Oscar Dahlqivst, Anakha Krishnavilasom Gopalakrishnan, Yuxuan Cui

***Abstract*—WiFi sensing is an emerging technology that uses WiFi transmitters and receivers to see their environment by analyzing the characteristics of the received waves. This paper is an introductory literature study discussing the state of research and WiFi sensing's commercial potential and challenges. This paper lays out the variety of techniques and hardware required for WiFi sensing and finds that despite WiFi sensing's generally high accuracy challenges remain, such as poor adaption to new environments, costs, privacy, and inconsistency in accessing valuable signal metrics. WiFi sensing's future has both positive and negative prospects in front of it.**

***Index Terms*—Radar, WiFi, WiFi Sensing**

I. Introduction

WiFi sensing refers to the use of WiFi signals as a passive radar to monitor and map its surroundings. Essentially using waves meant for data communication as a camera to see.

WiFi sensing has been an attractive area of research due to its ubiquity, versatility, and performance. It is the most easily accessible radar technology we have access to. WiFi sensing can be used in many different areas, including motion detection, home security, sleep monitoring, fall detection, gait recognition, gesture control, activities of daily living monitoring, lighting control, and energy management [1].

This report collects existing publications to give an overview of the current state of WiFi sensing. Specifically for commercial WiFi devices. We introduce some background of WiFi sensing, basic hardware, protocols, bandwidth, and how the WiFi sees the surrounding. Then we will discuss how accurate WiFi sensing can be now, some practical uses, and hardware that can achieve. WiFi sensing is currently an immature technology and it still has many problems so we will illustrate the challenges of it from different aspects.

II. Background

A. WiFi as Radar

WiFi, like any wireless network protocol transmits radio waves that reflect and interact with its environment. The specifics of WiFi waves and protocols are defined in the IEEE 802.11 standard. It would be possible to use the same frequencies as WiFi in a normal active radar system WiFi sensing is instead a passive radar. A WiFi receiver with sensing functionality could be placed somewhere near any WiFi transmitter and observing the multipath and degradation of the signal infer the environment indirectly.

B. WiFi Frequencies and Devices

WiFi devices only use a specific set of frequency ranges. Most commonly around 2.4 and 5 GHz. There are other proposed and seldom used bands but these are rarely studied for the purposes of WiFi sensing. WiFi sensing effectiveness depends on there already being preexisting WiFi signals to observe so the more specialized the transmitter frequencies that are required the less useful WiFi sensing is.

The frequencies used for WiFi sensing greatly impact how the environment is perceived. Compared to 5 GHz the 2.4 GHz band has higher penetration of solids and is less predictable when it comes to reflection. While 5 GHz has more predictable reflections it is also more prone to attenuation from obstacles. The 2.4 GHz band is also used by many other wireless devices and protocols creating more interference.

An important property of WiFi signals for the purposes of WiFi sensing is its usage of Orthogonal Frequency Division Multiplexing or OFDM. It is a modulation technique that divides a data stream into multiple non-interfering parallel streams for almost the same bandwidth usage. OFDM is useful for WiFi sensing because each subcarrier differs slightly in behavior and this difference can be modeled and learned to increase sensing capabilities. OFDM is used in many of the active WiFi standards such as IEEE802.11 a/g/n/ac.

C. Sensing Metrics

The signal data available for WiFi sensing calculation depends on the receiver hardware. The simplest metric that can be obtained from a receiver is the Received Signal Strength Indicator (RSSI). RSSI is defined as the power of the received signal for a given point in time.

The preferred metric for WiFi sensing is the Channel state information (CSI). The word CSI can be a wide variety of channel information but for WiFi, CSI is the measurable amplitude and phase shift for each of the OFDM multi-path channels between a receiver and a transmitter. [2]. For a transmitter with M antennas and a receiver with N antennas and S subcarriers between each antenna pair the CSI at a given instance will be a matrix of size [S, N, M] with each item in the matrix being an amplitude and phase shift.

Mathematically CSI is commonly represented by a function $H(f, m, n, t)$. Its arguments in order are the OFDM subcarrier frequency, the index of the transmitter antenna, the index of the receiver antenna, and time [2].

Sometimes WiFi sensing uses measurements other than RSSI and CSI due to different hardware having different accessible metrics [3].

D. Sensing Techniques

Trying to deduce useful sensing information from a given WiFi receiver's metrics requires complex processing of the data. The two main WiFi sensing techniques are modeling based and learning based. Most WiFi sensing implementations use a combination of the two techniques.

Modeling Based algorithms are derived from physical theories or statistical models based on empirical measurements, inferring some function Y = f (CSI) where Y is some more useful data.

Learning Based WiFi sensing refers to the use of machine learning techniques to extract meaningful information from WiFi signals for sensing purposes[4], [5]. the major steps are, Data collection, Feature extraction, Training a model, Model evaluation, Deployment, and Inference.

E. 80211bf

WiFi sensing has been deemed a high enough priority for IEEE to establish a task group with the goal of developing amendments to IEEE 802.11 with the goal of adding standardized protocols allowing future WiFi sensing devices to negotiate capabilities and intent [6]. Members of 802.11bf are prolific in the WiFi sensing field and the group is commonly mentioned in reports. The 802.11bf is still an ongoing project that actively calls for participation and contribution from different perspectives [7]. A draft of the proposal was published in 2022 and the task is planned to finish in 2024 [8].

III. Overview

A. Sensing Tasks

Table I below shows some uses of WiFi sensing, such as environment sensing, activity recognition, and so on. We provide some specific examples of different aspects of these uses.

Sensing application	Example	Description
Environment sensing	Temperature [9]	Detect ambient properties of the environment.
Activity Recognition	Pose [10], [11], [12], Gesture [12], [5]	Recognize human activity, for example: "sitting", "standing with left arm lifted" or "typing on keyboard".
Position & Movement	Localization [5], [13], [14], Speed Estimation [15], Human Counting [4]	Tracking existence, location, or amounts of targets in an environment.
Human health	Respiration [16], [17], [5], [13], [18]	Using CSI to track Respiration/Heart rates.
Food and Agricultural	Fruit Ripeness [5], [13]	Tracking the moisture levels of produce.

TABLE I
EXAMPLES OF WIFI SENSING EXPERIMENTS

WiFi sensing has achieved very high accuracy in all of these tasks. It is hard to find a general accuracy for the field because of the vastly different types of accuracy measurements. Studied papers generally find their accuracies satisfactory and surveys of the field find most papers archive at least 90% accuracy in their desired tasks, even in though-the-wall situations [2].

B. Commercial Potential

WiFi sensing has a wide range of commercial applications [15] including Smart home and Building Security [14], Smart Transportation and Healthcare Monitoring [16], [17], [5], [13] etc.

Smart Homes Traditional home security systems often rely on visual detection (cameras). An intruder alarm can then be sounded, both within the property and remotely via smartphones, etc. WiFi sensing can be used to detect when individuals have arrived home, and when they have left, and power down appliances and devices, motion detection accordingly.

Smart Transportation systems WiFi sensing to track the movement of vehicles and pedestrians and optimize traffic flow. It can also be used to monitor parking spots and detect when they become available.

Healthcare WiFi sensing can be used to monitor the movements of patients and staff and ensure that they are following all safety protocols.

C. Product Realisation

To our research there is yet no commercial product that uses WiFi sensing, there are multiple articles regarding research acquisitions in the field but none is yet to materialize.

S. M. Hernandez and E. Bulut state the following in their 2023 WiFi sensing paper focused on low-cost IoT devices:

> WiFi sensing can be used to recognize an outstanding number of unique physical actions or properties of a given environment. However, while we have seen a great number of laboratory experiments demonstrating novel methods for sensing, to the best of our knowledge, none of these works integrate WiFi sensing predictions into real physical systems. To push WiFi sensing forward as a technology, we need to not only think about interesting use cases and interesting sensing modalities, but we need to deploy these systems and allow them to be leveraged in the real-world such as through intelligent HVAC systems (...) [5]

D. Hardware

Table II shows some hardware used in WiFi sensing. We can use ready-made commercial WiFi routers like TP-link Talon AD7200 router. They can also be made by combining specific network cards, antennas, and a PC.

Hardware Category	**Example**
Network Card[1]	Intel 5300 NIC [16], [12], [4].
Mobile Phone	Google Nexus [19]
IoT Device	ESP32 [5]
Specialized	Horn Antenna [14], Special Mobile Device [20], [21]

TABLE II
TYPES OF WIFI SENSING HARDWARE

[1] Network cards also require antennas and a PC/AP

IV. Challenges

A. Cross Domain

For WiFi sensing to be cross-domain adaptable means the implementation works in a new environment that it has not been previously trained on. It should adapt to new devices, noise, room layout, size of users, movement, positions of transmitters, and interference from other devices among many other factors.

For a commercial WiFi sensing product to be useful it needs to be deployable anywhere without requiring an arduous re-training process. Current solutions struggle even when moving the same program to a room next over in the same building. [2]

As of February 2023, an exhaustive survey of the field concludes that no satisfactory solution yet exists and more data and research will be required [2]. The survey outlines different proposed methods to improve cross-domain support all och which are variations of different ML approaches to learn higher-order patterns. The survey concludes much more training data is required.

B. CSI Unavailability

CSI is the preferred metric for CSI but it is not always available, even if the hardware has the matrix internally there is no guarantee if or how you access that data for further processing. Each device needs a different solution and not all have been [5].

A growing concern is that newer WiFi standards do not include CSI. Mainstream standards from IEEE 802.11ac and beyond do not have CSI as it instead uses beamforming. For these devices, the only type of feedback that can be obtained is the beamforming weights [3]. Research is ongoing regarding how well models based on beamforming weights can perform. The most recent of the investigated papers regarding this topic outperformed RSSI but were only able to estimate a fraction of what can be deduced from CSI in real-world scenarios [3].

C. Privacy

WiFi sensing requires the collection and storage of data about the wireless signals transmitted and received by the sensing devices. The collected data can include sensitive information about the location, movement, and behavior of individuals, Identities, activities, and relationships of individuals. This collected data can be used to build detailed profiles or models of individuals or groups, that can raise privacy concerns if used without proper consent or oversight. The collected data may be shared without any consent of people. WiFi sensing can raise ethical considerations related to the collection and use of sensitive information, particularly if the sensing system is used in environments where individuals may have limited control or awareness of the data collection process. This can raise questions about the legitimacy, transparency, and accountability of WiFi sensing systems.

D. Costs

WiFi sensing can be expensive due to several factors, including hardware costs, infrastructure costs, deployment costs, and integration costs.

Hardware costs: WiFi sensing requires specialized hardware, such as WiFi adapters or antennas, that may be more expensive than off-the-shelf WiFi devices. For example, a high-gain directional antenna, which can improve the accuracy and range of WiFi sensing, can cost several hundred dollars.

Infrastructure costs: WiFi sensing may require additional infrastructure, such as network cabling, power supplies, or computing resources, to support the sensing devices and process the collected data. For example, a WiFi sensing system that needs advanced real-time data processing and analysis may require a high-performance computing cluster.

Deployment costs: WiFi sensing systems need specialized deployment techniques, for example, site surveys, signal mapping, or calibration, to ensure accurate and reliable sensing. For example, a WiFi sensing system that is deployed in a large outdoor area may require multiple access points and antennas, which raise the deployment and installation costs.

Integration costs: WiFi sensing needs integrated with other systems or applications, such as data analysis, automation, or security systems, to realize its full potential. For example, a WiFi sensing system that is integrated with a security system may require custom software development and testing, which may increase the integration costs.

V. Conclusion

WiFi sensing has made significant progress in achieving high accuracy for various tasks through training and processing. However, challenges keep on, and commercial implementation of WiFi sensing is still pending despite its popularity. Improvement in cross-domain adaptability is necessary, requiring more diverse data for training deployable models without manual involvement. Additionally, consideration of computational capabilities and cost effective hardware alternatives is needed. The phasing out of CSI poses a problem, and further research is required to explore the efficacy of alternative techniques such as beamforming. Although the future of WiFi sensing remains uncertain, its potential applications in industries like healthcare, smart homes, and security warrant attention as it continues to evolve.

References

[1] O. C. A. K. R. L. Chenshu Wu, Beibei Wang, "Wi-fi can do more: Toward ubiquitous wireless sensing." *IEEE Communications Standards Magazine*, vol. 6, no. 2, pp. 1 – 7, 2022. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9855454

[2] C. CHEN, Z. GANG, and L. YOUFANG, "Cross-domain wifi sensing with channel state information: A survey." *ACM Computing Surveys*, vol. 55, no. 11, pp. 1 – 37, 2023.

[3] Y. Jiang, X. Zhu, R. Du, Y. Lv, T. X. Han, D. X. Yang, Y. Zhang, Y. Li, and Y. Gong, "On the design of beamforming feedback for wi-fi sensing," *IEEE Wireless Communications Letters*, vol. 11, no. 10, pp. 2036–2040, 2022.

[4] Z. Guo, F. Xiao, B. Sheng, L. Sun, and S. Yu, "Twcc: A robust through-the-wall crowd counting system using ambient wifi signals," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 4, pp. 4198–4211, 2022.

[5] S. M. Hernandez and E. Bulut, “Wifi sensing on the edge: Signal processing techniques and challenges for real-world systems,” *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 46–76, 2023.

[6] “Meeting update.” [Online]. Available: https://www.ieee802.org/11/Reports/tgbfupdate.htm

[7] C. Chen, H. Song, Q. Li, F. Meneghello, F. Restuccia, and C. Cordeiro, “Wi-fi sensing based on ieee 802.11bf,” *IEEE Communications Magazine*, vol. 61, no. 1, pp. 121–127, 2023.

[8] R. Du, H. Xie, M. Hu, Narengerile, Y. Xin, S. McCann, M. Montemurro, T. X. Han, and J. Xu, “An overview on ieee 802.11bf: Wlan sensing,” 2022.

[9] J. Li, A. Sharma, D. Mishra, and A. Seneviratne, “Thermal profiling by wifi sensing in iot networks,” in *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, pp. 1–6.

[10] L. Xu, X. Zheng, X. Li, Y. Zhang, L. Liu, and H. Ma, “Wicam: Imperceptible adversarial attack on deep learning based wifi sensing,” in *2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2022, pp. 10–18.

[11] J. Yu, P. Wang, T. Koike-Akino, Y. Wang, P. V. Orlik, and R. M. Buehrer, “Multi-band wi-fi sensing with matched feature granularity,” *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 23 810–23 825, 2022.

[12] H. Fei, F. Xiao, J. Han, H. Huang, and L. Sun, “Multi-variations activity based gaits recognition using commodity wifi,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2263–2273, 2020.

[13] S. Tan, “Towards ubiquitous sensing using commodity wifi.” *Association for Computing Machinery*, vol. 2, no. 4, pp. 1 – 100.

[14] 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.

[15] S. Depatla and Y. Mostofi, “Passive crowd speed estimation in adjacent regions with minimal wifi sensing,” *IEEE Transactions on Mobile Computing*, vol. 19, no. 10, pp. 2429–2444, 2020.

[16] W. Li, R. J. Piechocki, K. Woodbridge, C. Tang, and K. Chetty, “Passive wifi radar for human sensing using a stand-alone access point,” *IEEE Transactions on Geoscience and Remote Sensing*, vol. 59, no. 3, pp. 1986–1998, 2021.

[17] D. Wu, D. Zhang, C. Xu, H. Wang, and X. Li, “Device-free wifi human sensing: From pattern-based to model-based approaches,” *IEEE Communications Magazine*, vol. 55, no. 10, pp. 91–97, 2017.

[18] K. Ali, M. Alloulah, F. Kawsar, and A. X. Liu, “On goodness of wifi based monitoring of sleep vital signs in the wild,” *IEEE Transactions on Mobile Computing*, vol. 22, no. 1, pp. 341–355, 2023.

[19] M. Schulz, J. Link, F. Gringoli, and M. Hollick, “Shadow wi-fi: Teaching smartphones to transmit raw signals and to extract channel state information to implement practical covert channels over wi-fi,” p. 256–268, 2018. [Online]. Available: https://doi.org/10.1145/3210240.3210333

[20] U. Mahmood Khan, Z. Kabir, and S. A. Hassan, “Wireless health monitoring using passive wifi sensing,” in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2017, pp. 1771–1776.

[21] Z. K. C. Y. B. K. K. N. Yuren Zhou, Billy Pik Lik Lau, “A novel microwave architecture for passive sensing applications.” *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 1 – 3, 2020. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8985258