Exploiting and Securing WiFi for Pervasive Human Sensing

Rui Xiao
Zhejiang University
ruixiao24@zju.edu.cn

Abstract

In recent years, the proliferation of WiFi-connected devices and related research has led to novel techniques of utilizing WiFi as sensors, i.e., inferring human activities through channel state information (CSI) perturbations. While this enables passive human sensing, it also introduces privacy risks from *leaked WiFi signals* that attackers can intercept, leading to threats like *adversarial motion sensing*. My research focuses on enhancing both the utility and security of WiFi sensing by addressing four key challenges: (1) lack of a secure sensing platform that also minimizes interference with normal WiFi communication, (2) environmental ambiguity caused by multipath effects, (3) confined sensing distance due to signal attenuation, and (4) limited scalability across different activities and users. I demonstrate solutions to these challenges through OneFi, a scalable WiFi sensing framework, and LeakyBeam, an adversarial WiFi sensing attack capable of long-range motion sensing. Finally, I discuss open problems and future challenges in achieving robust, scalable, and privacy-preserving WiFi sensing.

CCS Concepts

• **Security and privacy** → **Mobile and wireless security**; • **Human-centered computing** → **Ubiquitous and mobile computing**; • **Networks** → *Network protocols*.

Keywords

Wireless Security; WiFi Sensing; Wireless Sensing; Beamforming Feedback Information; BFI Sensing

ACM Reference Format:
Rui Xiao. 2025. Exploiting and Securing WiFi for Pervasive Human Sensing. In *The 23rd Annual International Conference on Mobile Systems, Applications and Services (MobiSys' 25), June 23–27, 2025, Anaheim, CA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3711875.3736658

1 Introduction

In recent years, the prevalence of WiFi-connected devices, such as laptops, mobile phones, and smart speakers, has significantly increased. Consequently, we are surrounded by the WiFi signals emitted by these devices. As individuals move within their homes or offices, these WiFi signals, specifically their channel state information (CSI), are perturbed, thereby implicitly capturing information about nearby human activities. This phenomenon presents new opportunities for **pervasive human sensing**, enabling applications in activity recognition, smart environments, and beyond. However, at the same time, this WiFi sensing capability also introduces significant **security and privacy risks** from *leaked WiFi signals* that travel beyond their intended boundaries. Attackers within the wireless communication range can intercept these leaked signals, leading to immediate threats, such as adversarial human motion sensing. My research aims to investigate and advance **both the utility and security aspects** of human-induced perturbation on WiFi signals. In this extended abstract, I examine WiFi's dual nature — as both a powerful enabler of sensing applications and a potential vector for privacy leakage — by addressing key technical challenges in WiFi sensing.

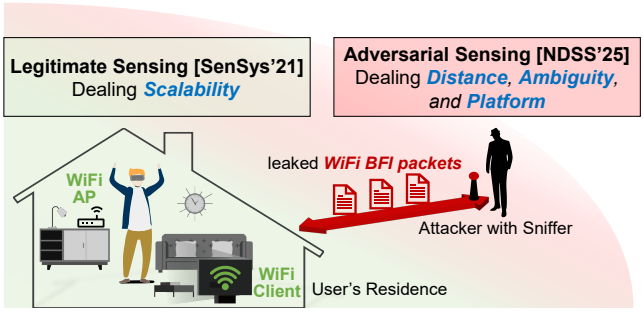

Figure 1: My research focuses on advancing both the utility and security of WiFi sensing by improving its scalability and sensing distance, dealing environmental ambiguity, and proposing new sensing platforms.

Challenges. Enhancing the utility and security of WiFi sensing requires overcoming four major challenges. (1) Lack of an Adequate Platform: Existing WiFi sensing solutions often *interfere with normal WiFi communication*. Additionally, when designing a platform that enhances sensing utility, *security concerns* must be carefully addressed to prevent unintended signal leakage. (2) Environmental Ambiguity: WiFi signals are highly susceptible to ambiguities caused by multipath effects that vary with each environment and device layout. (3) Confined Sensing Distance: WiFi signals degrade rapidly due to distance and physical obstructions, reducing the signal-to-noise ratio (SNR) and limiting their operation distance. (4) Limited Scalability: WiFi sensing systems require extensive retraining with large datasets to adapt to unseen domains, such as activities and users, incurring significant data collection and computational overhead.

Contributions. In this extended abstract, I demonstrate how my work addresses the four key challenges in WiFi sensing, as shown in Figure 1. First, I introduce *OneFi* [2], a framework designed to enhance the scalability of WiFi sensing applications, enabling robust

MobiSys' 25, Anaheim, CA, USA

ACM ISBN 979-8-4007-1453-5/25/06
https://doi.org/10.1145/3711875.3736658

performance across unseen domains with minimal data collection and retraining. Second, I introduce *LeakyBeam* [1], a long-distance adversarial WiFi sensing attack capable of extracting sensitive information from 20 m away, even under environmental ambiguity (without prior knowledge of victim's environment layout). In *LeakyBeam*, we also introduce a novel sensing platform by designing security-enhanced beamforming feedback information (BFI) packets. The platform holds the potential for secure and ubiquitous sensing while preserving normal WiFi communication, aligning with the principles of integrated sensing and communication (ISAC).

2 Promise: WiFi as Pervasive Sensor

WiFi sensing research repurposes WiFi devices as pervasive sensors, enabling human activity recognition through CSI perturbations. However, existing systems face scalability limitations, restricting them to predefined activities. When encountering unseen activities, prior approaches require large-scale data collection and model retraining. This raises a fundamental question – *"can we design a scalable WiFi sensing system that recognizes unseen activities with minimal labeled data, without requiring full model retraining?" OneFi* addresses this by exemplifying in the task of gesture recognition. *OneFi* is a one-shot gesture recognition system capable of recognizing unseen gestures using only one labeled sample. It fundamentally addresses the scalability issue with a two-fold approach. On the one hand, *OneFi* utilizes a *virtual gesture generation mechanism* such that the massive efforts in prior works can be significantly alleviated in the data collection process. On the other hand, *OneFi* employs a *lightweight one-shot learning framework* based on transductive fine-tuning to eliminate model re-training. We additionally design a self-attention based backbone, termed as WiFi Transformer, to minimize the training cost of the proposed framework. The system was evaluated over a real-world testbed using commodity WiFi devices. Our analysis revealed that *OneFi* can recognize unseen gestures with an accuracy of 84.2% when only one labeled sample is available, while the overall training process takes less than two minutes. The impact of *OneFi* has been notable, as its integration of virtual data generation and few-shot learning has emerged as a prominent direction in wireless sensing research. Recently, NVIDIA Cosmos has also aimed to accelerate the development of physical AI systems by introducing virtual training data through World Foundation Models, further validating *OneFi*'s design principles.

3 Pitfall: WiFi as Adversarial Motion Sensor

While WiFi sensing enables pervasive human sensing, it also introduces privacy risks due to leaked WiFi signals that attackers can intercept, leading to adversarial sensing threats. However, these threats have not been widely recognized due to two key factors, i.e., confined distance and environmental ambiguity. Traditional WiFi sensing is limited in range, restricting attackers outside a residence from gathering meaningful privacy-sensitive information. Additionally, attackers typically have little to no prior knowledge of the environment, further complicating precise sensing. Hence, we posed the following question – *"can an attacker with limited environmental knowledge accurately infer occupancy information from a victim's house, even from a greater distance outside?* We answer this question in the affirmative by proposing a novel and long-range attack. *LeakyBeam* leverages a new side channel from WiFi CSI, namely the beamforming feedback information (BFI). Unlike direct measurements of analog CSI, which suffer from signal attenuation, the channel information encoded in *digital BFI packets* retains the victim's movement information even when transmitted through walls over considerable distances. This is attributed to the digital encoding of the BFI content into bits and its subsequent formatting in accordance with established WiFi protocols, ensuring that the content remains clear and undistorted. Attackers can easily sniff the WiFi network to capture this side channel information, as BFI packets are transmitted in *plaintext* and are not encrypted, making *LeakyBeam* a truly practical attack. This work also sheds light on potential vulnerabilities in emerging high-frequency WiFi technologies, such as the 60 GHz mmWave 802.11ad/ay standards, which rely heavily on directional beams due to high attenuation at mmWave frequencies, exposing them to similar risks.

To mitigate this risk, we introduce a defense mechanism that obfuscates BFI packets with minimal hardware modifications. Notably, this **security-enhanced BFI sensing mechanism** has the potential to serve as a **legitimate WiFi sensing platform**. Unlike CSI, which can only be extracted from a limited number of commodity WiFi devices through driver modifications, BFI is widely accessible. With *LeakyBeam*'s security enhancements, BFI sensing could become a pervasive and ISAC-compatible platform.

4 Conclusions and Future Work

We explore approaches to enhance the utility and security of WiFi sensing by addressing its four key challenges. Moving forward, we aim to further develop secure and practical WiFi sensing technologies and platforms. A key focus will be on advancing the BFI sensing platform, optimizing BFI packet design and transmission strategies, while also implementing and open-sourcing the platform to encourage broader research adoption and real-world impact.

Acknowledgment

I sincerely thank my PhD advisor, Jinsong Han, and my collaborators for their invaluable guidance and support. This work is supported by the National Natural Science Foundation of China under grants U21A20462 and 62372400.

References

[1] Rui Xiao, Xiankai Chen, Yinghui He, Jun Han, and Jinsong Han. 2025. Lend Me Your Beam: Privacy Implications of Beamforming Feedback in WiFi. In *the 32nd Annual Network and Distributed System Security Symposium, NDSS'25*. The Internet Society.

[2] Rui Xiao, Jianwei Liu, Jinsong Han, and Kui Ren. 2021. OneFi: One-Shot Recognition for Unseen Gesture via COTS WiFi. In *19th ACM Conference on Embedded Networked Sensor Systems, SenSys'21*. ACM, 206–219.

Short Bio

Rui Xiao is a final-year Ph.D. candidate at Zhejiang University. His research interests lie at the intersection of security and mobile/wireless/sensing systems, with a particular focus on innovative analysis of physical signals to drive advancements in these areas.