Reconstruction attack on Wi-Fi sensing obfuscation[*]

Chae-Yeon Park, So-Eun Jeon, and Il-Gu Lee[†]

Sungshin Women's University, Seoul, South Korea
{220254013, 220237020, iglee}@sungshin.ac.kr

Abstract

With the recent advancements in wireless communication technology, Wi-Fi sensing technology, which transmits information through Wi-Fi signals while simultaneously detecting and identifying objects, has attracted considerable attention. However, this technology carries the potential risk of leaking private information to third parties through channel state information (CSI). To address this issue, existing security measures have explored obfuscation techniques that alter the phase or amplitude of the CSI. However, the obfuscation techniques are vulnerable to reconstruction attacks. Therefore, this study analyzes the vulnerabilities of obfuscation techniques by designing two attack scenarios. Experimental results show that even in a signal-to-noise ratio (SNR) environment of 5 dB, the masking estimation accuracy (MEA) for both attack models was 97.05% and 98.59%. Notably, in low-quality channel environments with an SNR below 10 dB, the white-box attack model demonstrated a higher MEA than the oracle attack model, proving that it is a more realistic attack method in unstable channel conditions.

Keywords. Wi-Fi sensing obfuscation, Channel state information, Reconstruction attack

1 Introduction

In the 6G era, integrated sensing and communication (ISAC) systems, which simultaneously transmit information through wireless signals while detecting and identifying objects, are gaining significant attention. According to Business Research Insight's ISAC market report, the ISAC market is projected to reach $10.13 billion by 2025 and is expected to grow to $28 billion by 2033 [1]. Indeed, ISAC technology is applied to autonomous vehicles, smart home care, smart city security and surveillance, supporting traffic safety, and managing medically vulnerable populations [2][3]. One of the key technologies in ISAC systems is Wi-Fi sensing. Wi-Fi sensing leverages existing Wi-Fi access points (APs) and is compatible with legacy Wi-Fi standards, offering the advantages of high resource utilization and low cost.

The combination and advancement of multiple-input multiple-output (MIMO) and orthogonal frequency-division multiplexing (OFDM) technologies have enabled the sharing of more precise channel state information (CSI) between the transmitter and receiver [4]. MIMO is a wireless communication technology that uses multiple transmit and receive antennas, while OFDM is a method

[*] Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. 42, December 16-18, 2025, Sapporo, Japan. © The copyright of this paper remains with the author(s).

[†] Corresponding author

that divides a wideband channel into multiple subcarriers to transmit data. The CSI is a three-dimensional matrix value that quantifies channel characteristics, such as amplitude attenuation and phase changes, occurring during wireless signal transmission from the transmitter to the receiver, expressed as complex numbers [4]. Basically, CSI reflects the channel characteristics where Wi-Fi signals are reflected, scattered, and diffracted by walls, people, and objects. This enables the tracking of a person's location and their behavior detection. Specifically, CSI amplitude variations in the time domain can detect human presence, falls, and movement changes and can be used to recognize activity status and gestures [4][5]. CSI phase changes in the spatial and frequency domains associated with the transmission delay time and reception direction can be utilized to localize and track a person's position [4][6].

The CSI-based Wi-Fi sensing technology can be used for fall detection, smart home control, digital healthcare, and indoor location-based services. However, it simultaneously poses the risk of privacy information leakage. For instance, CSI can be used to infer private attributes such as a user's height, weight, and gender [7]. Furthermore, by exploiting the characteristic that password input on mobile devices varies depending on hand and finger movements, an outsider could detect a person's hand movements inside a room, infer their input pattern, and derive the password [8][9]. Particularly in security-sensitive communication environments, such as military settings, the potential damage from privacy data leaks caused by Wi-Fi sensing is predicted to be extremely significant.

Therefore, obfuscation techniques that interfere with third-party CSI extraction have gained attention as a response to these issues. Wi-Fi sensing obfuscation intentionally alters the receiver's channel response by rotating the phase components or partially modulating the amplitude of the preamble of the transmitted signal. Indeed, artificially inserting random peaks into the CSI amplitude at the transmitter results in degraded location-tracking performance [10]. However, using high modulation and coding schemes (MCS), such as 64-QAM and 256-QAM, imposes the limitation of significantly reducing packet transmission rates [10]. Consequently, recent studies have proposed obfuscation techniques that artificially alter the transmitted signal while maintaining normal communication quality for legitimate receivers, thereby increasing eavesdropping difficulty [11][12][13].

However, conventional Wi-Fi sensing obfuscation techniques fail to guarantee the confidentiality of CSI from third parties. This is because an eavesdropper can exploit the repetitive structure and autocorrelation of the preamble for reverse engineering obfuscation masking. The preamble consists of a short-time field (STF) and a long-time field (LTF), with the CSI value embedded within the LTF. Here, the preamble is public information defined in the IEEE 802.11 standard. Therefore, even after preamble obfuscation, an attacker can use publicly available preamble information to determine the starting position of an LTF. Subsequently, they extracted the LTF and estimated the masking values.

Therefore, this study demonstrates that the defensive effectiveness of Wi-Fi sensing obfuscation techniques that alter the signal amplitude or phase is lost in an attack environment in which the attacker knows the standard preamble structure and the method for generating transmission signal masking. The Oracle attack model represents an ideal attack scenario without noise. The white-box attack model represents a realistic white-box attack scenario that considers the presence of noise. This enables the quantitative analysis of security vulnerabilities in conventional obfuscation techniques.

The main contributions of this paper are as follows.

- It presented two reconstruction attack scenarios that can exploit vulnerabilities in conventional Wi-Fi sensing obfuscation techniques.
- It highlights the risks posed by the exposed preamble structure in Wi-Fi sensing environments and proposes considerations for designing secure communication techniques in the future.

The remainder of this paper is organized as follows. Section 2 analyzes conventional obfuscation techniques. Section 3 describes the background and target model, and Section 4 analyzes the attack performance based on attack scenarios. Section 5 analyzes the experimental results, and Section 6 concludes the paper.

2 Related work

Table 1 summarizes the proposed techniques and the limitations of recent Wi-Fi sensing obfuscation methods.

Table 1: Related work on Wi-Fi sensing obfuscation

Reference	Proposed Idea	Limitation
Marcello et al. [11]	Proposal of a CSI obfuscation method that leverages high-pass, low-pass, and band-pass filters.	Not considering the legitimate receiver's accuracy in human activity recognition (HAR) during communication.
Chu et al. [12]	Proposal of a dynamic channel obfuscation technique using a time-varying filter.	Vulnerable to statistical inference of a time-varying filter under long-term observation.
Ghiro et al. [13]	The implementation of the obfuscation technique on real OpenWi-Fi.	Does not address reverse-engineering of signal generation to estimate obfuscation masking.

Marcello et al. [11] proposed a method for obfuscating CSI using high-, low-, and band-pass filters. They demonstrated that applying this technique to a human activity recognition (HAR) system reduces the accuracy of location estimation attacks. However, the accuracy of HAR systems for legitimate users was not evaluated.

Chu et al. [12] proposed a dynamic channel obfuscation technique that uses a time-varying filter. This technique can reduce the eavesdropper's sensing accuracy to below 50% while maintaining a legitimate sensing performance above 90%. However, this is limited in that an attacker cannot observe the signal for an extended period to discern the statistical characteristics of the time-varying filter.

Ghiro et al. [13] implemented an obfuscation technique for 802.11a/g/h and 802.11n systems in open Wi-Fi environments. This technique injects pseudo-random patterns into the transmitter's CSI of the Wi-Fi signal to conceal location information. This was achieved by implementing the obfuscation technique in a real open Wi-Fi environment and verifying its practicality and performance. However, it does not consider that an attacker can estimate obfuscation masking by mimicking the method used to generate a transmitted signal.

To address these limitations, this study proposes an attack method for conventional Wi-Fi sensing obfuscation techniques designed to prevent location estimation and object detection while maintaining the information transmission performance of Wi-Fi signals. Through this approach, we aimed to analyze the vulnerabilities.

3 Background

This study aimed to verify the feasibility of CSI reconstruction attacks by selecting the obfuscated masking technique proposed by Ghiro et al. [13] as the target model. The obfuscation method employed in this study modulates the amplitude of each subcarrier, as described by Equations (1) and (2) [13].

$$R_K = e^{-\alpha\Delta t} R_{K-1} + R_{new} \tag{1}$$

$$A_0 = clip\left(1 + R_k, \left[clip_{min,} clip_{max}\right]\right) * \theta_C \tag{2}$$

All variable values were set to match those defined by Ghiro et al. [12]. Here, k is the index of the packets transmitted in chronological order. Equation (1) represents the step of generating the random number pattern set R_K required to generate the masking coefficient for each packet, which reflects the temporal correlation. When generating R_K, it mimics the actual communication environment by incorporating the temporal correlation of the previous packet by $e^{-\alpha\Delta t}$ from R_{K-1}. This protects the communication performance of legitimate receivers and increases the attackers' difficulty in identifying the CSI. Here, α is the coefficient determining the rate at which temporal correlation with the previous frame decreases, set to 0.2, and Δt denotes the time interval between packets. If Δt exceeds a certain threshold, the value $e^{-\alpha\Delta t}$ approaches zero, eliminating temporal correlation with the previous packet. R_{new} is a value randomly selected from the interval [-0.3, 0.3]. Equation (2) describes the process of generating the masking vector value, A_0, which is multiplied by the actual subcarrier. $1 + R_k$ is clipped within the ranges $\left[clip_{min,} clip_{max}\right]$ to prevent the values from being excessively small or large, with a clipping range of [0.1, 1.9]. Subsequently, θ_C undergoes convolution with an FIR filter to achieve smoothing between adjacent subcarriers, generating a gradual masking pattern in the frequency domain.

4 De-obfuscation Attack Scenario on Wi-Fi Sensing

Figure 1 illustrates two attack scenarios for reconstructing the obfuscated signal.

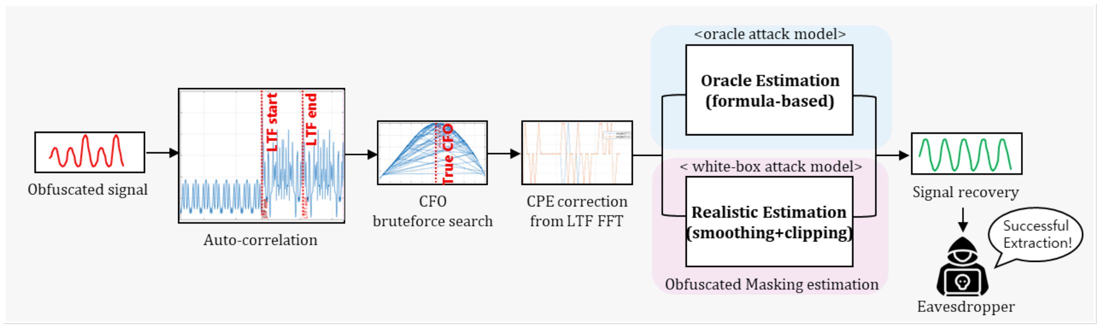
Obfuscated signal
LTF start
LTF end
Auto-correlation
True CFO
CFO bruteforce search
CPE correction from LTF FFT
<oracle attack model>
Oracle Estimation (formula-based)
< white-box attack model>
Realistic Estimation (smoothing+clipping)
Obfuscated Masking estimation
Signal recovery
Successful Extraction!
Eavesdropper

Figure 1 : Two Attack Scenarios

In this experiment, because the target model used an amplitude modulation masking technique, the symbol timing offset (STO), which caused phase errors, was assumed to be zero. First, both attack scenarios utilized the repetitive structure of the STF in the received obfuscated signal. According to the IEEE 802.11 standard, STF is repeated every 10 samples, whereas LTF is repeated after every two samples. The starting interval of the STF was identified by multiplying the repeating patterns within the signal and comparing the maximum values, as shown in Equations (3), (4), (5) [14].

$$P(d) = \sum_{n=0}^{L-1} x_1(n) x_2{}^*(n) \tag{3}$$

$$R(d) = \sum_{n=0}^{L-1} |x_2(n)|^2 \tag{4}$$

$$M(d) = \frac{|P(d)|^2}{(R(d))^2} \tag{5}$$

Here, $x_1(n)$ and $x_2(n)$ represent the first and second STF segments of the received signal, respectively, and L denotes the repeating length of the STF. $P(d)$ is the value calculated from the cross-correlation of the first and second STF segments. Meanwhile, $R(d)$ is calculated from the power of the $x_2(n) \times segment$. If only $P(d)$ is used as the STF detection criterion, it is difficult to distinguish cases where the signal size is large, even if the similarity between two repeating segments is high. Therefore, it was normalized using $R(d)$ to reduce the influence of the signal size. Therefore, $M(d)$ is calculated as the ratio of $P(d)$ to $R(d)$ and is used as an indicator to detect the starting point of the STF. Next, the starting position of the LTF is determined based on the STF length. Subsequently, candidate carrier frequency offsets (CFO) within the range [-0.5, 0.5] are randomly assigned to the signal. The symbol rate obtained from the LTF interval is then calculated using Equations (6) and (7).

$$z[k] = \frac{Y[k]}{X[k]}\ ,\ k \in\ A \tag{6}$$

$$Z =\ \sum_{k\in A}\{z[k]\}^2 \tag{7}$$

Here, k is the subcarrier index belonging to the active subcarrier set A and $Y[k]$ is the LTF symbol obtained by applying a fast Fourier transform (FFT) after the signal is corrected for the candidate CFO at the receiver. $X[k]$ is the standard LTF symbol in BPSK modulation format, consisting of ±1, known at the transmitter. Therefore, $z[k]$ represents the ratio of the transmitted symbol to the received symbol for each k index. When the CFO is corrected precisely, $z[k]$ should be close to the real axis. Therefore, the candidate CFO that minimizes the sum of the squares of the imaginary components for all active subcarriers is selected as the optimal value. Subsequently, to correct minor errors in the CFO candidate search, the LTF is converted into a FFT to correct the common phase error (CPE).

Subsequently, the oracle and white-box attack models estimate masking based on the signal model, as presented in Equation (8).

$$y = MFx + n \tag{8}$$

Here, y is the signal observed at the receiver, M denotes the amplitude masking, F denotes CFO, x is the transmit preamble vector defined in IEEE 802.11, and n denotes the artificial noise. Therefore, signal y, received by the attacker, is the result of multiplying the standard preamble vector by the masking and CFO, and then adding artificial noise. The oracle attack model assumes an ideal scenario with no noise. If an attacker can precisely remove the CFO from $y = MFx$, they can calculate y divided by x to obtain only the positive real part, thereby determining the masking value. Conversely, the white-box attack model assumes a realistic scenario in which the attacker knows how the transmit signal is generated and whether noise is present. Therefore, dividing y by x yields a signal in which the masking value is mixed with the noise. To correct the error caused by this noise, the attacker replicates the clipping and smoothing steps of the transmission signal generation process. First, negative values of $\frac{y}{x}$ are eliminated. The smoothing process then averages the adjacent subcarriers to reduce the abrupt signal fluctuations caused by noise. Subsequently, the values are clipped within the range defined by the transmitter $[clip_{min,}\ clip_{max}]$ to derive valid masking values. Through this process, the attacker reduces the estimation errors caused by noise.

5 Evaluation

An experiment was conducted using a MATLAB-based simulation that implemented the preamble structure of the IEEE 802.11 OFDM physical layer standard. The evaluation was performed by repeating the simulation 1,000 times. In addition, an initialization interval was defined to control the temporal correlation of the masking coefficients. The initialization interval determines the number of packets to pass before the initialization R_{K-1}. As mentioned in Equation (1), R_{K-1} is a variable used to reflect the temporal correlation of a previous packet during the masking coefficient generation. A larger value indicates that the temporal correlation between the packets persists for a longer duration.

The selected evaluation metrics were the normalized subcarrier error rate (NSER) and masking estimation accuracy (MEA). NSER represents the sum of the masking estimation error rates per subcarrier unit and is given by Equation (9). The MEA indicates how accurately the masking of all subcarriers is estimated and is given by Equation (10):

$$NSER \;=\; \sum_k \frac{|M_{est}[k]-M_{real}[k]|^2}{[M_{real}[k]]^2},\; k \in A \tag{9}$$

$$MEA = 100 \times (1 - \overline{NSER}) \tag{10}$$

The denominator $[M_{real}[k]]^2$ in Equation (9) represents the actual masking value, whereas the numerator $|M_{est}[k] - M_{real}[k]|^2$ denotes the difference between the masking value estimated by the attacker and the actual masking value. The NSER was calculated from the normalized mean squared error (NMSE), defined as the squared difference between the actual and estimated masking values divided by the squared actual masking value. The MEA was calculated by averaging the NSER and converting it into a percentage.

Figure 2 compares the MEA of the oracle and white-box attack models as the SNR increases.

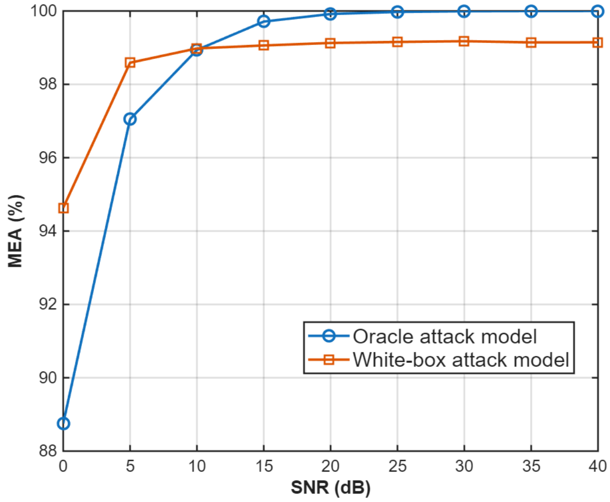

Figure 2: MEA of the white-box and oracle attack models

When the SNR was < 10 dB, the white-box attack model achieved a higher MEA value than the oracle attack model. This indicates that, even in unstable channel environments, attackers can sufficiently estimate a portion of the masking values using the white-box attack model. Conversely, when the SNR is 10 dB or higher, the white-box attack model maintains an MEA value of approximately 99%. In comparison, the oracle attack model increased by 1% up to an SNR of 25 dB and then maintained an MEA value of 100%. This indicates that both the oracle and white-box attack models can partially determine the masking value, even in noisy environments. Therefore, the conventional obfuscation methods are vulnerable to reconstruction attacks.

Figure 3 shows the MEA results for the oracle and white-box attack models as the reset interval varies in an environment where the SNR is fixed at 30 dB.

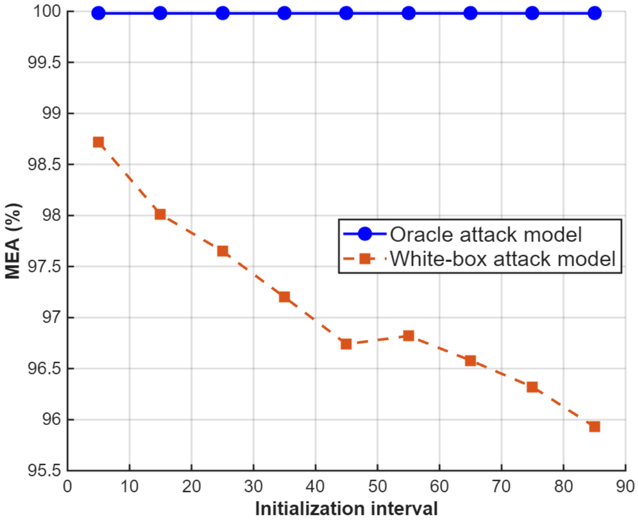

Figure 3: MEA over various initialization interval

The oracle attack model maintained an MEA of 99.98%, regardless of changes in the reset interval. However, the white-box attack model achieved an MEA of 98.72% when the reset interval was five days, and the MEA decreased by an average of approximately 0.15% for each 5-day increase in the reset interval. This indicates that from an attacker's perspective, longer reset intervals make masking more difficult to estimate. Nevertheless, the white-box attack model maintained an MEA greater than 90%. Therefore, even when increasing the reset interval, some masking can still be estimated, demonstrating the limitations of the obfuscation techniques.

6 Conclusion

Wi-Fi sensing utilizes the CSI information from Wi-Fi signals to identify the location of objects or people and detect their movements. This technology can be applied to fall detection, smart home control, digital healthcare, and indoor location-based services, thereby enhancing industrial efficiency and making personal life more convenient. However, it also has limitations, as it can intentionally or unintentionally leak private information to third parties. Consequently, previous studies have proposed various Wi-Fi sensing obfuscation techniques that artificially modify transmitted signals to de-identify the CSI information. However, existing methods struggle to apply strong masking without compromising communication quality with legitimate receivers and fail to fully guarantee the confidentiality of CSI.

Therefore, this study presents two attack scenarios that utilize the preamble information and autocorrelation characteristics defined in the IEEE 802.11 standard to reconstruct the masking coefficients proposed in conventional Wi-Fi sensing obfuscation techniques. According to the experimental results, both the oracle and white-box attack models achieved MEA values of 97.05% and 98.59%, respectively, even in a noisy environment with an SNR of 5 dB. Furthermore, in environments with SNR $\leq$ 10, the white-box attack model achieved a higher MEA than the oracle attack model. This indicates that the white-box attack model is a more realistic approach for estimating masking coefficients in noisy environments. Furthermore, although longer reset intervals increase the difficulty of estimating attacker masking, the white-box attack model maintained an MEA above 90%. This result indicates that the security of the existing obfuscation techniques is insufficient. Future research should aim to develop countermeasures that address the vulnerabilities of the conventional obfuscation techniques analyzed in this study. Specifically, we propose generating preamble patterns that differ from the IEEE 802.11 standard while maintaining compatibility, thereby preventing third parties from reconstructing the CSI.

Acknowledgments

This work was supported by the Ministry of Trade, Industry and Energy (MOTIE) under Training Industrial Security Specialist for High-Tech Industry (RS-2024-00415520) supervised by the Korea Institute for Advancement of Technology (KIAT), and the Ministry of Science and ICT (MSIT) under the ICAN (ICT Challenge and Advanced Network of HRD) program (IITP-2022-RS-2022-00156310) and Information Security Core Technology Development (RS-2024-00437252) supervised by the Institute of Information & Communication Technology Planning & Evaluation (IITP).

References

Business Research Insights. (2025, August 25). *Integrated Sensing and Communication (ISAC) Market Size, Share, Growth, and Industry Analysis, By Type (Semi-ISAC, UAV-enabled ISAC, Other), By Application (Car, Drone, Other), and Regional Forecast to 2033 (Report No. BRI120298).* Retrieved September 9, 2025, from https://www.businessresearchinsights.com/market-reports/integrated-sensing-and-communication-isac-market-120298

Ma, H. (2024). Integrated sensing and communication - The ISAC technology. In *Proceedings of the 2024 IEEE 2nd International Conference on Sensors, Electronics and Computer Engineering (ICSECE)* (pp. 225–229). Jinzhou, China: IEEE.

Ge, Y., et al. (2023). Contactless Wi-Fi sensing and monitoring for future healthcare – Emerging trends, challenges, and opportunities. *IEEE Reviews in Biomedical Engineering, 16,* 171–191.

Ma, Y., Zhou, G., & Wang, S. (2019). Wi-Fi sensing with channel state information: A survey. *ACM Computing Surveys, 52*(3), Article 46, 36 pages.

Quy, T. D., Lin, C.-Y., & Shih, T. K. (2025). Enhanced human activity recognition using Wi-Fi sensing: Leveraging phase and amplitude with attention mechanisms. *Sensors, 25*(1038).

Alghisi, G. A., Gringoli, F., Cominelli, M., Raza, S., & Cigno, R. L. (2025). For your eyes only: Bridging privacy and sensing in Wi-Fi networks through CSI obfuscation. In *Proceedings of the 2025 23rd Mediterranean Communication and Computer Networking Conference (MedComNet)* (pp. 1–6). Cagliari, Italy: IEEE.

Shi, Y., Zhang, X., Fu, L., & Zhang, H. (2024). An investigation of the private-attribute leakage in Wi-Fi sensing. *High-Confidence Computing, 4*(4), 100209. https://doi.org/10.1016/j.hcc.2024.100209.

Gu, Y., et al. (n.d.). CSIPose: Unveiling human poses using commodity Wi-Fi devices through the wall. *IEEE Transactions on Mobile Computing.*

Meng, Y., Li, J., Zhu, H., Liang, X., Liu, Y., & Ruan, N. (2020). Revealing your mobile password via Wi-Fi signals: Attacks and countermeasures. *IEEE Transactions on Mobile Computing, 19*(2), 432–449.

Asadi, A. (2021). IEEE 802.11 CSI randomization to preserve location privacy: An empirical evaluation in different scenarios. *Computer Networks, 191,* 107970. https://doi.org/10.1016/j.comnet.2021.107970.

Marcello, F., Pettorru, G., Martalò, M., & Pilloni, V. (2024). Preserving privacy in CSI-based human activity recognition: A data obfuscation case study. In *Proceedings of the IEEE Global Communications Conference (GLOBECOM 2024)* (pp. 2822–2827). Cape Town, South Africa: IEEE.

Chu, Z., Li, G., Meng, Q., Li, H., & Zeng, Y. (2025). Privacy-preserving Wi-Fi sensing in WSNs via CSI obfuscation. *Computers & Security, 157,* 104594. https://doi.org/10.1016/j.cose.2025.104594.

Ghiro, L., Cominelli, M., Gringoli, F., & Cigno, R. L. (2023). Wi-Fi localization obfuscation: An implementation in OpenWi-Fi. *Computer Communications, 205,* 1–13. https://doi.org/10.1016/j.comcom.2023.03.026.

Schmidl, T. M., & Cox, D. C. (1997). Robust frequency and timing synchronization for OFDM. *IEEE Transactions on Communications, 45*(12), 1613–1621.