



UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

DIPARTIMENTO DI INGEGNERIA
DELL'INFORMAZIONE

Dottorato di ricerca in Ingegneria dell'informazione

Ph.D Thesis

**CSI-BASED WIRELESS SENSING AND
LOCALIZATION WITH NEXT-GENERATION
WI-FI: PERFORMANCE AND PRIVACY
ASPECTS**

Supervisor:
Ch.mo Prof. Francesco Gringoli

Author:
Dott. Shabbir Raza Baloch

**Academic Year 2024/2025
XXXVIII Cycle**

Bonafide Certificate

This is to certify that the topic entitled “**CSI-Based Wireless Sensing and Localization with Next-Generation Wi-Fi: Performance and Privacy Aspects**” is the bona fide work carried out by **Shabbir Raza**, a PhD student in the Department of **Information Engineering, (DII)** at the **University of Brescia (Italy)**, in partial fulfillment of the requirements for the award of the degree of PhD in Information Engineering.

Signature of the Supervisor:

Name of the Supervisor: Prof. Francesco Gringoli

Place: Brescia, Italy

Date:

Abstract

This dissertation studies the correlation between wireless sensing capabilities and privacy protection within the context of next-generation Wi-Fi networks, while discovering the latest wireless mesh networking techniques for Internet of Things (IoT) applications. The pervasive adoption of IEEE 802.11 standards, specifically the improvements toward Wi-Fi 7 (802.11be), has revealed an opportunistic horizon for fine-grained environmental sensing through Channel State Information (CSI) analysis. However, the same capabilities that enable powerful sensing applications introduce significant privacy risks, as unauthorized users can extract and utilize sensitive information about human activities and presence without needing an active participation from targets.

This study has four major contributions. First, we perform an empirical validation concerning the influence of IEEE 802.11be's on CSI-based sensing by developing a Software-Defined Radio (SDR) framework capable of emulating 320 MHz Wi-Fi frames and systematically analyzing the relationship between bandwidth and localization accuracy. Our findings show that wider channels, facilitated by modern Wi-Fi standards, offer not just increased data capacity but also provide the probability of capturing frequency components essential for sensing tasks.

Second, we investigate the privacy-sensing paradigm by validating a practical implementation of CSI obfuscation and de-obfuscation techniques. With the help of experimental validation, we show that authorized users can recover sensing capabilities even when the signals have been intentionally distorted for privacy protection.

Third, a fundamental tradeoff between privacy strength and de-obfuscation fidelity is revealed by identifying and characterizing the "notch phenomenon," where mask coefficients with near-zero amplitudes introduce error amplification during de-obfuscation and become more challenging to perform sensing.

Finally, we investigate how CSI-based sensing can be integrated with infrastructure-less mesh networking: the idea is to consider a dense infrastructure dedicated to sensing, in order to improve its accuracy, composed of tens if not hundreds of nodes that are able to sense the environment on their own by processing information locally. To disseminate the sensed information to a central repository, an OpenThread-based mesh network can be used: this enables flexible sensor deployment without the need for costly network infrastructure.

The research manifests that sensing and communication capabilities in modern wireless networks should not be treated as competing objectives but rather as complementary aspects that may be balanced through suitable technical methods. Our findings offer key insights for developing next-generation wireless systems where privacy protection and sensing coexist, enabling the effective deployment of ubiquitous sensing technologies while protecting users' privacy at the physical layer.

Abstract

(Italian)

Questa tesi studia come le tecniche di sensing wireless e la protezione della privacy possano coesistere nelle reti Wi-Fi di nuova generazione, affrontando anche il tema delle reti mesh wireless per applicazioni IoT. L'evoluzione degli standard IEEE 802.11, in particolare verso il Wi-Fi 7 (802.11be), ha reso possibile estrarre informazioni ambientali sempre più dettagliate a partire dalle CSI. Se da un lato ciò abilita nuove applicazioni di sensing, dall'altro introduce rischi rilevanti per la privacy, poiché tali informazioni possono essere utilizzate anche da soggetti malevoli per dedurre la presenza e le attività umane in ambienti serviti da una rete Wi-Fi.

Il lavoro si concentra su quattro contributi principali. Il primo riguarda la valutazione sperimentale dell'impatto del Wi-Fi 7 sul sensing basato su CSI. A questo scopo è stato sviluppato un framework che, grazie all'uso di dispositivi SDR, supporta trasmissioni Wi-Fi con larghezze di banda fino a 320 MHz. L'analisi dei risultati mostra che l'uso di canali più ampi non comporta solo un aumento della capacità trasmissiva, ma migliora anche l'efficacia del sensing, grazie a una rappresentazione spettrale più ricca e informativa.

Il secondo contributo affronta il problema della privacy, analizzando in modo specifico tecniche di offuscamento della CSI volte a nascondere e proteggere le informazioni che descrivono l'ambiente circostante dagli utenti non autorizzati, nonché le corrispondenti tecniche di de-offuscamento che ne consentono l'estrazione selettiva da parte dei soli utenti autorizzati. Gli esperimenti condotti dimostrano, per la prima volta, che le informazioni di sensing possono essere efficacemente ripristinate esclusivamente dai nodi autorizzati.

In questo contesto emerge un compromesso fondamentale tra il livello di protezione della privacy e la qualità del recupero dell'informazione ambientale. Tale compromesso è attribuito al cosiddetto notch phenomenon, per cui coefficienti di mascheramento di ampiezza molto ridotta causano un'amplificazione dell'errore nella fase di de-offuscamento, rendendo il sensing meno affidabile.

Infine, si analizza come il sensing basato su CSI possa essere integrato con reti mesh prive di infrastruttura. L'idea è quella di adottare un dispiegamento massivo di nodi di sensing, composto da decine o centinaia di dispositivi autonomi che osservano

l'ambiente ed elaborano localmente i dati, migliorando così l'accuratezza complessiva del sistema. Per la disseminazione delle informazioni rilevate verso un repository centrale, può essere utilizzata una rete mesh basata su OpenThread; ciò consente un dispiegamento flessibile dei sensori senza la necessità di una costosa infrastruttura di rete.

Nel complesso, i risultati mostrano che comunicazione e sensing possono essere integrati in modo equilibrato attraverso opportune scelte progettuali. La tesi contribuisce così allo sviluppo di reti wireless di nuova generazione capaci di supportare funzionalità di sensing avanzate, garantendo al tempo stesso un adeguato livello di protezione della privacy a livello fisico.

Preface

This doctoral thesis summarizes my Ph.D work as a student at the University of Brescia (Italy) under the supervision of Prof. Francesco Gringoli. The thesis focuses on wireless sensing, privacy preservation at the physical layer, and the performance analysis of modern wireless communication and networking technologies.

Parts of this thesis are based on the author's previously published research work. In particular, selected content included in Chapter 3 and Chapter 4 extends, summarizes, and clarifies the findings originally published in peer-reviewed conference proceedings co-authored by the candidates mentioned in the proceedings. These contributions are clearly cited throughout the manuscript and have been integrated to ensure transparency, coherence, completeness, and continuity of the doctoral research narrative.

The publications on which parts of this thesis are based include:

[1] Marco Cominelli, Shabbir Raza, Renato Lo Cigno, and Francesco Gringoli. A glimpse into ieee 802.11be channels: Can they improve csi-based sensing? In 2025 IEEE Wireless Communications and Networking Conference (WCNC), pages 1–6, 2025.

[2] Giovanni Angelo Alghisi, Francesco Gringoli, Marco Cominelli, Shabbir Raza, and Renato Lo Cigno. For your eyes only: Bridging privacy and sensing in wi-fi networks through csi obfuscation. In 2025 23rd Mediterranean Communication and Computer Networking Conference (MedComNet), pages 1–6, 2025.

Shabbir Raza Baloch
January, 23rd 2026

Acknowledgements

قَالَ لَا تَخَافُ إِنِّي مَعَكُمْ أَسْمَعُ وَأَرَى

Meaning: ‘[Allah] said, “Fear not. Indeed, I am with you both; I hear and I see.”
[Surah Taha, 20:46] [Quran]

I am extremely thankful to Almighty ALLAH for keeping me in good health for the completion of this work and my Ph.D.

First and foremost, I would like to thank my supervisor, Professor Francesco Gringoli, whose expertise was invaluable in formulating the research questions and methodology. Your insightful feedback pushed me to sharpen my thinking and brought my work to a higher level. I would like to express my sincere gratitude to all those who supported and contributed to the completion of this doctoral research.

In addition, I would like to thank my parents for their wise counsel and sympathetic ear. Specially my Father, Haji Raza Muhammad, and my Mother, Mehrun-nisa, were always there for me. Finally, I could not have completed this thesis without the support of my Wife Samreen, and my sincere friends and family, who provided stimulating discussions as well as happy distractions to rest my mind outside of my research.

I would be forever indebted to the University of Brescia for striving to provide me with this excellent opportunity to pursue a doctoral degree.

Contents

1	Introduction	5
1.1	The Evolving Landscape of Wireless Technologies and Sensing . . .	5
1.2	The Imperative for Robust Indoor Localization	6
1.3	Sensing Potential with Next-Gen Wi-Fi IEEE 802.11-be	6
1.4	Navigating the Privacy Paradox in Ubiquitous Wireless Sensing . . .	7
1.5	Research Gaps and Thesis Contributions	7
1.6	Thesis Structure	9
2	Background and IEEE 802.11 Architecture	11
2.1	Overview of Channel State Information (CSI)	12
2.1.1	Mathematical Representation of CSI in IEEE 802.11 OFDM Systems	13
2.1.2	CSI data acquisition	15
2.2	CSI-Based Sensing and Localization	15
2.2.1	Applications of CSI-Based Sensing	17
2.2.2	CSI Based Localization Techniques	17
2.3	Privacy Concerns in Wireless Sensing	19
2.4	IEEE 802.11 Standards Evolution	20
2.4.1	IEEE 802.11 Layers	22
2.4.2	Physical (PHY) Layer	22
2.4.3	Medium Access Control (MAC) Layer	23
2.5	Thread and OpenThread Architecture	24
2.5.1	Comparison with Zigbee and Wi-Fi	25
3	CSI-Based Localization with IEEE 802.11be	27
3.1	Emulating IEEE 802.11be Transmissions: The SDR framework . . .	28
3.2	Other considerations and Limitations	31
3.3	Sensing Architecture for Device Free Positioning	32
3.4	Experimental Setup and Data Collection	33
3.5	Experimental Results and Analysis	34

3.5.1	Impact of Wi-Fi Bandwidth and Standard on Localization Accuracy	35
3.5.2	Influence of Sub-Channels and Spectral Position on Sensing Performance	36
3.5.3	Effect of Training Data Size on Model Performance	37
3.5.4	Impact of Data Collection Duration on Sensing Accuracy	38
3.6	Discussion	42
4	CSI Obfuscation and De-obfuscation for Privacy Protection	43
4.1	The Emerging Privacy Concerns in CSI-based Sensing	44
4.2	Proposed Solution: CSI Obfuscation and Deobfuscation	44
4.3	Existing Privacy-Preserving Methods in Wireless Sensing	46
4.4	The Research Gap: Practical Feasibility of CSI De-obfuscation	46
4.5	Primer on CSI-Based Sensing	47
4.5.1	Analysis on CSI Obfuscation	48
4.5.2	Analysis on CSI De-Obfuscation	48
4.5.3	Towards a Practical De-obfuscation Protocol	50
4.6	Methodology	51
4.6.1	Case Study: Device-Free Localization	51
4.6.2	Experimental Setup	51
4.6.3	Data Collection	52
4.6.4	Transmitter and receiver setup	53
4.7	Design and Implementation of Obfuscation Masks	54
4.7.1	Sinusoidal-based Mask	54
4.7.2	Reflection-based Mask	54
4.7.3	Dynamic Evolution of Mask Parameters	55
4.7.4	Transmission and masking strategy	56
4.7.5	The neural network architecture and data processing for localization	56
4.8	Experimental results and Discussion	58
4.8.1	Baseline localization accuracy	58
4.8.2	Effectiveness of obfuscation in degrading unauthorized sensing	60
4.8.3	Performance of de-obfuscation in restoring legitimate sensing	61
4.8.4	Impact of obfuscation strength on de-obfuscation accuracy	61
4.9	Summary of key findings	62
5	An Extension Toward Low-Power IoT Sensing and Networking	63
5.1	Overview of Thread	64
5.1.1	Device Roles and Types	65
5.1.2	Thread Network Stack	66
5.2	Methodology	68
5.2.1	Experimental Setup	68
5.2.2	Experimental Infrastructure and Architecture	69
5.3	Hardware and Software Implementation	70

5.3.1	Core Network Hardware	70
5.3.2	OpenThread Firmware Configurations	71
5.4	Connectivity and RTT Measurement	71
5.4.1	UDP Throughput Measurement	71
5.5	Experimental Considerations: Interference and Multi-Hop Overhead	72
5.5.1	The Impact of Environmental Interference	72
5.5.2	Multi-Hop Performance Degradation	72
5.6	Empirical Results	73
5.6.1	RTT Performance in Controlled Environments	73
5.6.2	Impact of Interference and Human Presence	75
5.7	Key Findings	76
6	Conclusions	77
	 List of Symbols	 85

List of Acronyms

6LoWPAN IPv6 over Low-Power Wireless Personal Area Networks. 67, 68, 72, 73

A/D Analog to Digital. 17, 28

AI Artificial Intelligence. 47, 58

AmpFi Amplitude-Based Fingerprinting. 18

AoA Angle of Arrival. 12, 18

AoD Angle of Departure. 12

AP Access Point. 13, 18, 21, 22, 25, 26, 53

BR Border Router. 24, 64, 65, 70

BSS Basic Service Set. 21

CDFs Cumulative Distribution Functions. 70

CNN Convolutional Neural Network. 17, 32, 34

CoAP Constrained Application Protocol. 24, 65

COTS Commercial Off-The-Shelf. 5, 12, 19, 44, 51, 53

CSI Channel State Information. 5–9, 11–19, 27, 28, 31, 32, 34–40, 42–53, 56–58, 60–62, 77–79, 81, 82

CSMA/CA carrier Sense Multiple Access with Collision Avoidance. 23, 71–73

D/A Digital to Analog. 28

DCF Distributed Coordination Function. 21, 23

DFP Device Free Passive. 18

DNS Domain Name System. 65

- DS** Distribution System. 21
- DSSS** Direct Sequence Spread Spectrum. 23
- DTLS** Datagram Transport Layer Security. 24, 65
- EDs** End Devices. 64, 66
- ESS** Extended Service Set. 21
- FED** Full End Device. 66
- FFT** Fast Fourier Transform. 17, 30
- FTD** Full Thread Device. 65, 66, 68, 71
- GPS** Global Positioning System. 6, 15, 17, 27
- IBSS** Independent Basic Service Set. 21
- ICMPv6** Internet Control Message Protocol version 6. 65, 71
- IETF** Internet Engineering Task Force. 67
- IFFT** Inverse Fast Fourier Transform. 17
- IoT** Internet of Things. 5, 7, 9, 10, 24, 25, 27, 42, 64, 65, 73, 79
- IPv6** Internet Protocol Version 6. 24, 64, 66–68, 72, 73
- ISAC** Integrated Sensing and Communication. 6, 8, 43–45, 61, 78, 79
- ISM** Industrial, Scientific and Medical. 72
- LAN** Local Area Network. 11, 25
- LoWPAN** Low-Power Wireless Personal Area Networks. 24
- LTF** Long Training Field. 15
- LTS** Long Training Symbols. 15
- MAC** Medium Access Control. 9, 11, 20, 22, 23, 25, 53, 65, 67, 70–72
- MED** Minimal End Device. 66
- MIMO** Multiple Input Multiple Output. 13, 16, 18, 20, 42, 78
- MLE** Multicast Listener Extension. 67
- MTD** Minimal Thread Device. 65, 66

- NIC** Network Interface Card. 15, 16
- NN** Neural Networks. 57
- NTP** Network Time Protocol. 65
- OFDM** Orthogonal Frequency Division Multiplexing. 6, 8, 13, 14, 16, 17, 23, 25, 29, 30, 42, 47, 53, 77, 81
- OT** OpenThread. 11, 64, 71–73
- OTBR** OpenThread Border Router. 68, 70
- PAN** Personal Area Network. 25
- PCF** Point Coordination Function. 23
- PHY** Physical. 7, 9, 11, 13, 19, 20, 22, 23, 25, 46, 47, 65–67, 70, 72
- PLCP** Physical Layer Convergence Procedure. 22
- PLR** Packet Loss Rate. 71
- PMD** Physical Medium Dependent. 22
- QAM** Quadrature Amplitude Modulation. 16
- QPSK** Quadrature Phase Shift Keying. 16
- REED** Router Eligible End Devices. 64, 66
- RIS** Reflective Intelligent Surfaces. 46
- RNN** Recurrent Neural Networks. 17
- RPL** Routing Protocol for Low-Power and Lossy Networks. 64, 67, 72
- RSS** Radio Signal Strength. 12, 16
- RSSI** Received Signal Strength Indicator. 5, 12, 16
- RTT** Round Trip Time. 69–73
- SDR** Software-Defined Radio. 5, 7–9, 15, 28–30, 46, 51, 53, 77–79, 81
- SDRs** Software-Defined Radios. 27, 31, 42
- SED** Sleepy End Device. 66
- SoC** System-on-Chip. 70
- STC** Space-Time Coding. 20

ToF Time of Flight. 12, 18

UDP User Datagram Protocol. 24, 65, 71–73

USRP Universal Software Radio Peripheral. 15

WARP Wireless Open-Access Research Platform. 15

WLAN Wireless Local Area Networks. 5, 11, 20, 22, 65

WSN Wireless Sensor Networks. 19

Chapter 1

Introduction

1.1 The Evolving Landscape of Wireless Technologies and Sensing

In contemporary times, the adoption of Wi-Fi is increasingly defined by the growing ubiquity and presence of wireless communication technologies, particularly those based on the IEEE 802.11 family of standards [1]. Initially, Wi-Fi-based solutions were used and developed for Wireless Local Area Networks (WLAN) but are now emerging as a viable choice for indoor monitoring using Wi-Fi signals for tasks such as activity and gesture recognition.

Wi-Fi-based devices have been widely adopted in residential settings, including smart homes and care facilities that assist in living facilities. Wi-Fi CSI may be accurately extracted using Commercial Off-The-Shelf (COTS) equipment or custom hardware thanks to advanced signal processing techniques. This covers phase variations, frequency shifts, and signal levels [2]. The widespread use and continued technological evolution highlight the underlying centrality of Wi-Fi's to both connectivity and advanced sensing capabilities. A tech insights report reveals a continuous increase in IoT and connected devices by 8% per year, which is expected to reach 46 billion by 2028, and the majority of devices will use Wi-Fi as their primary wireless broadband technology. This pattern highlights the broadening role of Wi-Fi, not only as a data source, but also as a part of the massive sensor network [3]. Beyond traditional signal strength indicators such as Received Signal Strength Indicator (RSSI), Wi-Fi provides access to CSI, enabling advanced applications such as sensing, localization, and motion detection. CSI tells us how a Wi-Fi signal travels from the transmitter to the receiver and helps in understanding its interaction with the environment, capturing intricate amplitude and phase shifts across multiple sub-carriers and antenna pairs. A more detailed discussion about CSI can be found in Section 2.1.

The combination of communication and sensing capabilities within a single system

is referred to as Integrated Sensing and Communication (ISAC), which represents an emerging framework for future wireless networks. Since the introduction of IEEE 802.11a/n, Orthogonal Frequency Division Multiplexing (OFDM) has been the foundation of Wi-Fi technology, operating at 2.4 or 5 GHz, and currently even at 6 GHz, which are particularly well suited for ISAC. This is due to the inherent availability of CSI, which is computed starting from the training symbols in the Wi-Fi preamble, which is then modulated using OFDM. CSI captures key characteristics of the wireless channel, including amplitude and phase information across different subcarriers, which are essential for fine-grained sensing. This highlights that CSI is derived directly from standard communication protocols and training symbols such as the preambles [4].

ISAC in the context of 6G, underlines that communication and sensing will coincide and be fully integrated. The author in [5] discusses how ISAC systems could provide both device-based and device-free localization services for 6G that feature networked sensing capabilities, denser antenna arrays, and frequency bands that enable the integration of wireless sensing. Experts have successfully reused Wi-Fi as a sensing platform beyond its traditional use as a pure communication medium, thus giving birth to the concept of ISAC with Wi-Fi. It also highlights that the deliberate recognition of ISAC can improve spectrum efficiency and reduce hardware costs, indicating a planned integration rather than mistaken convergence. The paper also mentions the IEEE 802.11bf standardization group, which further solidifies the trend toward formal adoption of sensing in Wi-Fi [6].

1.2 The Imperative for Robust Indoor Localization

Wireless signals have emerged as a promising alternative to traditional localization methods, especially due to the limitations of Global Positioning System (GPS) signals in indoor scenarios, making it more challenging to perform accurate indoor positioning. In contrast, the availability of CSI from Wi-Fi signals enables a better approach, offering a richer, more granular view of the wireless environment. This detailed form of data opens the door to accurate device-free localization, enabling the detection of people and objects in complex environments without the need to carry any dedicated sensors. Despite these advancements in the field, a strong need remains for robust and accurate solutions in real-world indoor environments, especially as new wireless standards continue to emerge.

1.3 Sensing Potential with Next-Gen Wi-Fi IEEE 802.11be

Next-generation Wi-Fi standards, such as IEEE 802.11be (Wi-Fi 7), provide deep fascinations in wireless communication capabilities, introducing wider channel capacities and bringing more dense subcarriers. These technical advancements are not

only limited to increased data throughput, but in fact offer a rich source of CSI, thereby holding immense, yet largely unexplored, potential for revolutionizing wireless sensing applications. An important gap in current studies lies with the empirical validation to see how these innovations in the latest Wi-Fi can truly impact sensing precision, particularly in device-free positioning. Furthermore, the unavailability of CSI extraction tools from the advanced 802.11be systems requires detailed examination. The thesis is motivated by the need to fill this gap, providing the necessary tools and development of the system using SDR and providing empirical evidence to understand and leverage the full sensing capabilities of Wi-Fi 7.

1.4 Navigating the Privacy Paradox in Ubiquitous Wireless Sensing

The distinct features that make CSI-based sensing more powerful are its granularity, ubiquitous availability, and device-free operations, which expose users to substantial privacy threats. The ability to spy on sensitive information, such as human detection, or even daily activities, from Wi-Fi signals, without the need for carrying any specialized devices or sensors, presents a significant ethical and security risk. Traditional cryptographic protections, which operate at higher network layers, often fall short in mitigating these Physical (PHY) information leakages. This inherent conflict between the utility of pervasive sensing and the imperative of user privacy necessitates novel, fundamental solutions. This research stems from the pressing demand to develop practical and effective countermeasures that can protect the privacy of users at the PHY level, ensuring that the benefits of pervasive wireless sensing can be realized responsibly and securely.

1.5 Research Gaps and Thesis Contributions

With the advancement in wireless sensing, there are still many important research gaps, particularly regarding the integration of the next generation Wi-Fi and the need for protection of privacy. This thesis identifies and addresses the possible gaps through some contributions that push the boundaries of the field.

a) IEEE 802.11be’s Impact on Device-Free Localization: Although IEEE 802.11be (Wi-Fi 7) introduces support for up to 4096 subcarriers and a wider channel width, its actual impact on CSI based sensing remains mainly unexplored. Therefore, it’s important to isolate and understand the impact of the bandwidth on sensing performance; existing studies often confuse it with other factors, such as different frequency band variations and ambient environmental noise.

This thesis presents an innovative analysis that practically demonstrates the correlation between Wi-Fi bandwidth and the accuracy of device-free positioning systems. It highlights the considerable performance improvements that are achievable

with IEEE 802.11be’s wider OFDM capabilities with increased channel width, showing consistent improvement. A key aspect of this research is its ability to isolate the bandwidth impact, a novel contribution in a field where previous studies often blended bandwidth effects with other variables, such as differences in frequency bands or noise. The evolution of Wi-Fi standards, specifically the shift toward wider channels with more subcarriers in 802.11be, is not limited only to better communication throughput but instead to improving the sensing capacity of the wireless medium. The design of new Wi-Fi standards directly increases the granularity and volume of CSI data, which in turn improves the precision of sensing applications based on CSI such as localization. This suggests that the development of communication standards is now implicitly driving advances in sensing, and future Wi-Fi standards will likely be co-designed with sensing capabilities in mind.

b) SDR Framework for 802.11be CSI Sensing: To address the scarcity of 802.11be CSI extraction tools, this thesis details the development and public release of a custom SDR framework, which was built using two Ettus X-310 SDR motherboards configured as a pair of transmitter and receiver, and MATLAB software. This framework enables 802.11be transmission emulation, supports bandwidths up to 320 MHz, and enables precise CSI acquisition. This development fills a critical gap for the research community, providing a valuable tool that fosters reproducible research in a field where proprietary tools are common.

c) ISAC Privacy for CSI Obfuscation and De-obfuscation: This study addresses a practical demonstration of the feasibility of de-obfuscating the signal on the receiver side at legitimate sensing devices that were intentionally obfuscated at the transmitter side. Experimental findings categorically verified that only authorized users can successfully recover original CSI features, achieving localization accuracy levels comparable to those obtained with clear (un-obfuscated) transmitted frames. This resolves the fundamental issue between privacy concerns and the utility of CSI for sensing. The work analyzes two different types of obfuscation masks, sinusoidal-based masks and reflection-based masks, which evaluate three levels of distortion strength, weak, medium, and strong, providing empirical evidence of their effectiveness in both degrading unauthorized sensing and enabling legitimate sensing restoration.

d) Obfuscation vs. De-obfuscation Trade-offs in ISAC: The study reveals a transparent trade-off: Although stronger signal distortions enhance protection against illegal sensing, they simultaneously limit the ability of legitimate users to accurately reverse the obfuscation process. A key insight is the discovery of the “notch” phenomenon, where coefficients in the obfuscation mask with near-zero amplitudes significantly amplify errors during the de-obfuscation process. As a result of this measurement noise amplification, the recovered CSI fidelity noticeably decreases, further reducing the sensing accuracy for legitimate applications. This

shows that it is not merely about applying any signal distortions, but rather designing sophisticated masks that minimize error amplification during the signal reversal process. This hinders the need for a new class of obfuscation algorithms that are “de-obfuscation friendly” while still maintaining privacy.

1.6 Thesis Structure

The thesis is structured into five chapters, which offer a comprehensive and in-depth analysis of CSI based wireless sensing, exploring its recent advancements, and the privacy concerns related to it. The fifth chapter broadens the scope by introducing IEEE 802.15.4-based low-power, low-latency mesh networks, highlighting their significant importance and potential for secure, efficient, and reliable IoT for device-to-device communications.

Chapter 2 - Background and IEEE 802.11 Architecture: This chapter establishes and explores the understanding that is important for the subsequent discussions. It starts by providing a thorough overview of CSI, including its mathematical representation and CSI data acquisition methods, applications, and techniques within the wireless communication systems. The chapter further explores the evolution of IEEE 802.11 standards, with a particular focus on the PHY and Medium Access Control (MAC) layers, which are crucial for CSI extraction. Additionally, it introduces the architecture of Thread and OpenThread, demonstrating its suitability for low-power mesh networks and their potential for low-power IoT applications.

Chapter 3 - CSI-Based Localization with IEEE 802.11be: This chapter discusses the study’s experimental work, focusing on device-free localization using next-generation Wi-Fi, specifically IEEE 802.11be (Wi-Fi 7). It describes the SDR framework to simulate 802.11be transmissions and examines how localization accuracy is affected by wider channels, such as in this case of 4096 subcarriers in this instance. The chapter concludes with some preliminary recommendations for maximizing sensing performance in these advanced Wi-Fi environments.

Chapter 4 - CSI Obfuscation for Privacy Protection: This chapter highlights the important privacy issues necessary for CSI-based sensing applications. It verifies a new initiative: CSI obfuscation and de-obfuscation experimentally. To show how legal sensing capabilities can successfully be restored for authorized sensing while maintaining privacy for unauthorized access. The chapter examines several mask types and distortion strengths, including weak, median, and strong, demonstrating how legitimate sensing capabilities could be helpful.

Chapter 5 - IEEE 802.15.4 Low Power Mesh Networking for IoT: This chapter addresses the discussion of wireless mesh networks based on IEEE 802.15.4 radio that operates at 2.4 GHz to explore its applicability and suitability within

Thread-based IoT mesh networks. It explores the difficulties and possibilities of using CSI sensing concepts in mesh-networked, low-power IoT applications. This study contributes to techniques initially created for Wi-Fi sensing could be used to numerous other wireless protocols, especially low-power, low-cost IoT applications.

Chapter 2

Background and IEEE 802.11 Architecture

In this chapter, we summarize and report the fundamental standards and technology that support CSI-based sensing and localization. We start with the introduction of CSI, focusing on its importance in modern wireless communication systems. The latest developments and techniques in CSI-based sensing and localization are explored, including engineered methods that benefit from the rich information embedded in wireless channels. In addition, increasing risks to privacy that occur from the use of CSI data, specifically in sensitive or personal environments. Then the IEEE 802.11 standards, which regulate WLAN, popularly referred to as Wi-Fi, were developed. The PHY and MAC layers are given particular attention because they are crucial to comprehending the extraction of CSI. The chapter concludes with the designs of Thread and OpenThread (OT) provided, emphasizing their suitability and applicability to create scalable low-power mesh networks that can accommodate CSI-based applications in embedded and distributed environments.

Wireless technologies have emerged substantially in modern times, introducing numerous applications from basic communication to refined sensing and localization systems. Among these technologies, the IEEE 802.11 family of standards, commonly known as Wi-Fi, stands out due to its widespread adoption and continuous evolution. Wi-Fi originally developed for wireless Local Area Network (LAN)s, the underlying signal characteristics of Wi-Fi, particularly CSI, have shown significant capabilities for advanced applications beyond simple connectivity. This chapter serves as the foundation for CSI within the context of IEEE 802.11 architecture, analyzing its fundamental concepts, evolution within the 802.11 standards, and its transformative role in wireless sensing and localization. Furthermore, as these potential capabilities become more prevalent, the associated privacy concerns require careful consideration, which will also be addressed in this chapter. The objective is to provide a comprehensive background that will serve as a basis for further discussion

and analysis within this thesis.

2.1 Overview of Channel State Information (CSI)

CSI, which helps in characterizing the Phase and Amplitude of Wi-Fi signals, may be used to predict signal parameters, such as Angle of Arrival (AoA), Angle of Departure (AoD), Time of Flight (ToF), and has significantly advanced indoor localization based on Wi-Fi signals in recent years [7]. The two forms of wireless signals that are typically used in detection based on Wi-Fi are CSI and Radio Signal Strength (RSS). While RSS offers coarse-grained information about communication links, CSI provides fine-grained information about the state of the channel in much detail [8].

In recent years, some RSSI-based methods have been proposed for human motion detection and localization. Due to the instability of RSSI caused by environmental changes, which results in erroneous detections, RSSI-based methods have various drawbacks [9]. The emerging approach to device-free sensing has attracted more attention due to its ability to use COTS commodity devices Wi-Fi and the rich information provided by the channel state information (CSI).

Channel State Information (CSI) typically refers to the detailed data on how a Wi-Fi signal travels between a transmitter and receiver, capturing signal strength, phase, and distortions. It helps in localization, motion detection, and wireless sensing by analyzing how signals change due to obstacles or movement. This interest is further supported by the availability of a wide range of open-source tools such as Atheros-CSI-Tool, an extraction suite for Atheros 802.11n Wi-Fi hardware; this tool is supposed to support all types of Atheros 802.11n Wi-Fi chipsets, including Atheros AR9580, AR9590, AR9344, and QCA9558 [10]; CSI-Kit [11], which provides a command-line tool for parsing, processing, converting, and visualization of CSI data, as well as libraries for use in other Python applications such as those working with TensorFlow and PyTorch; Feit-CSI [12], the first open-source tool that enables CSI extraction and frame injection for all formats (802.11a/g/n/ac/ax) and bandwidths (20/40/80/160 MHz) using commodity Intel NICs (AX200/AX210); and nexmon-CSI [13], an extraction suite for a range of Broadcom Wi-Fi hardware for CSI extraction and analysis.

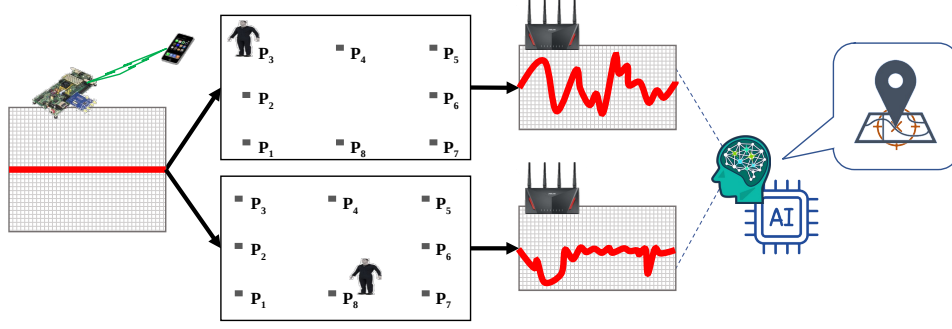


Figure 2.1: CSI changes as the target moves from one place to another.

The way in which a wireless communication system gathers CSI in several spatial locations is depicted in Figure 2.1. CSI describes how a signal behaves as it moves through the environment, taking into account variations in the signal's phase and amplitude caused by movement or environmental changes. The CSI readings change as an individual changes positions. Without the need for visual or physical touch, it is now feasible to precisely identify, locate, and categorize activities or environmental changes by evaluating these variances using machine learning algorithms.

In recent years, the integration of CSI has become a valuable addition to indoor location and detection techniques. CSI provides crucial information on the state of the wireless communication channel, offering details on signal quality, multipath effects, and interference levels. This real-time information on the channel conditions between Access Point (AP) and mobile devices can be used to improve the precision and robustness of indoor localization systems.

2.1.1 Mathematical Representation of CSI in IEEE 802.11 OFDM Systems

Advanced PHY techniques like Multiple Input Multiple Output (MIMO) and OFDM are used in modern wireless networks that follow the IEEE 802.11 standard. These methods are designed to increase the orthogonality of the channel and the data capacity in multipath propagation conditions. CSI offers comprehensive details on the phase shift and amplitude attenuation that the signal experiences over several pathways for each subcarrier for each pair of transmitter and receiver antenna [14]. The Wi-Fi channel can be modeled as:

$$y = Hx + n, \quad (2.1)$$

where y is the received signal, x is the transmitted signal, H is the complex matrix CSI and n is the signal noise factor.

Each element of the CSI captures the channel frequency response that is given by:

$$H(f, t) = \sum_{n=1}^N a_n(t) e^{-j2\pi f \tau_n(t)}, \quad (2.2)$$

where $H(f, t)$ [15] is the channel frequency response, $\sum_{n=1}^N$ is the summation of all multipath components, $a_n(t)$ is the amplitude strength factor, and $e^{-j2\pi f \tau_n(t)}$ represents the phase change due to delay $\tau_n(t)$.

At the receiving end, CSI is calculated using the previously defined sent signal and the received signal y after processing and cyclic prefix removal. The CSI is a three-dimensional matrix that may be written as

$$\mathbf{CSI} = \{H_{i,j,k}\} \quad (2.3)$$

$$\mathbf{H}_k = \begin{bmatrix} H_{1,1,k} & H_{1,2,k} & \cdots & H_{1,N_t,k} \\ H_{2,1,k} & H_{2,2,k} & \cdots & H_{2,N_t,k} \\ \vdots & \vdots & \ddots & \vdots \\ H_{N_r,1,k} & H_{N_r,2,k} & \cdots & H_{N_r,N_t,k} \end{bmatrix} \quad (2.4)$$

where $i = 1, \dots, N_r$ (receiving antennas), $j = 1, \dots, N_t$ (transmitting antennas), $k = 1, \dots, K$ (subcarriers), H_k [16] is the channel matrix of N_r, N_t dimensional and is known as CSI for the i -th subcarrier. Matrix H_i can be represented as shown in eq. (2.4).

For OFDM systems, which divide the available bandwidth into multiple subcarriers, the CSI is often represented as a matrix of complex values. Each entry in this matrix corresponds to a specific subcarrier and captures both the amplitude and phase shift calculated by the signal on that subcarrier as it travels from a particular transmit antenna to a particular receive antenna.

The measured CSI in real-world systems is not ideal and is influenced by a multitude of factors beyond the intrinsic channel characteristics. These include multi-path effects, the signal processing techniques employed by the transmitter and receiver, and various imperfections in the hardware and software components of the communication system.

A more comprehensive mathematical model of the measured baseband-to-baseband CSI is given by; [15]

$$H_{i,j,k} = \sum_{n=1}^N a_n e^{-j2\pi \frac{d_{i,j,n} f_k}{c}} e^{-j2\pi \tau_i f_k} e^{-j2\pi \rho f_k} e^{-j2\pi \eta \left(\frac{f'_k}{f_k} - 1 \right) f_k} q_{i,j} e^{-j2\pi \zeta_{i,j}} \quad (2.5)$$

Here, $d_{i,j,n}$ is the path length, f_k is the carrier frequency for the k -th subcarrier, c is the speed of light, τ_i represents the phase offset due to Cyclic Shift Diversity (CSD), ρ is the Sampling Time Offset (STO), η is the Sampling Frequency Offset (SFO), and $\zeta_{i,j}$ accounts for phase offsets due to beamforming.

Understanding these mathematical representations is fundamental to analyzing and utilizing CSI for both enhancing communication and enabling sensing applications.

2.1.2 CSI data acquisition

The process of CSI data acquisition generally involves the receiver that estimates the characteristics of the channel based on the receiving signal. Typically, pilot signals or training sequences encoded in the transmitted data packets are used to carry out this estimation in IEEE 802.11 systems. The Long Training Symbols (LTS) that are part of the preamble of 802.11 packets are a prime example of such pilot signals. Both the transmitter and the receiver are aware of the predetermined sequences contained in these Long Training Field (LTF)s. The receiver can determine the CSI by comparing the received LTF sequence with the original and estimating the impact of the channel on the signal at various frequencies (subcarriers).

However, this process is the basis for communication; the current IEEE 802.11 standard does not directly support sensing applications [17]. Thus, researchers have developed different ways to acquire CSI for sensing purposes. These methods include using specialized hardware such as channel sounders, which transmit custom waveforms specifically designed for accurate CSI estimation. Another approach involves extracting CSI from regular data traffic using modified drivers for commodity Wi-Fi Network Interface Cards (NICs) [18]. Several tools were introduced to propose this, such as the Intel 5300 Network Interface Card (NIC) Tool [19], the Atheros CSI Tool [10], and the Nexmon CSI Tool [13] for extracting the channel information from mobile devices like smartphones and embedded systems like Raspberry Pi. Additionally, SDR platforms like Wireless Open-Access Research Platform (WARP) and Universal Software Radio Peripheral (USRP) offer reasonable platforms for CSI acquisition across various frequency bands [18]. These diverse methods highlight the ongoing efforts to leverage CSI for a wide range of applications beyond traditional Wi-Fi communication.

2.2 CSI-Based Sensing and Localization

The importance of Wi-Fi signals has grown with the quick development of wireless technologies. These signals are always present in our environment, no matter where we are, hence they can be used to track, identify, and analyze human actions and behaviors. Remarkably, common commercial Wi-Fi equipment may be used for such sensing and localization tasks. One of the most crucial elements of mobile wireless applications is localization and sensing. Due to the weakening of the signals caused by building materials, GPS frequently functions poorly indoors. Achieving precise

indoor localization, therefore, remains a research challenge, with potential uses in asset monitoring, patient tracking, elder care, and other fields.

The issue of indoor localization has been the subject of numerous studies. The RSSI, which indicates the received power level at the receiver, is used by several range-based localization protocols to calculate positions. RSSI data are also the basis for current radio frequency (RF)-based indoor localization [20]. Using the strength of received signals, RSSI-based localization calculates the distance between nodes, which localization algorithms subsequently utilize to establish node locations. Nevertheless, there are two primary issues with this approach: precise model parameter determination is challenging because of environmental variability, and wireless environments, particularly indoors or in crowded outdoor areas, cause signal fluctuations due to interference and multipath effects, rendering distance estimation unreliable. Using anchor nodes at known locations to build a signal strength map, RSSI profiling techniques are employed to increase accuracy. The closest match is used to approximate the position of unknown nodes during localization by comparing their current RSSI values with this map [21]. Therefore, localization that is based on RSSI could lead to unsatisfactory performance.

CSI, as opposed to RSS, includes link information at the granularity of a single MIMO-OFDM subcarrier. As a result, it can lead to more precise indoor localization. We are now able to aggregate the amplitude and phase information for every MIMO-OFDM subcarrier, and thanks to the availability of the CSI tool for Intel Wi-Fi Link 5300 wireless NIC commodity Wi-Fi cards [22].

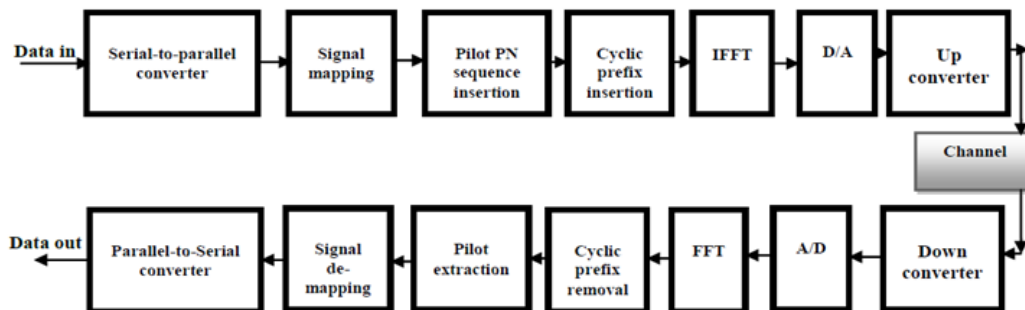


Figure 2.2: Block Diagram of OFDM transceiver[23]

OFDM has been a paradigm in today's wireless systems due to its ability to manage frequency-selective fading in multipath environments, explicitly in wireless standards such as IEEE 802.11a/g/n/ac/ax/be. As illustrated in Figure 2.2 on the Tx starts by sending the incoming serial data into parallel data streams. After that, each stream is modulated using Quadrature Phase Shift Keying (QPSK) or Quadrature Amplitude Modulation (QAM) schemes. To facilitate channel estimation at the receiver, pilot sequences are added into the stream, then a cyclic prefix, extracted

from the end of each OFDM symbol, a part of the signal is added at the beginning to reduce interference caused by signal reflections. After the signal is converted to the time domain by an Inverse Fast Fourier Transform (IFFT), the data is upsampled and converted from digital to analog before being sent.

The operations at the receiver are the reverse of the ones performed at the transmitting side. Firstly, the signal is downsampled and converted from Analog to Digital (A/D). After that, the cyclic prefix is removed, and the Fast Fourier Transform (FFT) is applied to shift the signal into the frequency domain. After the data is demodulated, the receiver then extracts the pilot tones. Finally, a single serial stream is created by combining the parallel streams once more. With this simple OFDM transceiver architecture, wireless systems can achieve good performance and reliability even in high multipath effect scenarios.

2.2.1 Applications of CSI-Based Sensing

The rich and detailed information that CSI provides has enabled a wide variety of sensing applications. One of the most salient applications is to detect human presence in complex indoor environments, where the variations in CSI amplitude over time can identify whether a person is in the proximity. Similarly, motions can be detected by analyzing the temporal changes in the channel. More complex applications include human activity recognition, on how specific patterns in CSI variations can be associated with activities like gesture, running, walking, or even falling. CSI can also be used for health monitoring, such as evaluating breath and heart rate, by detecting sophisticated changes in the wireless signals caused by these physiological movements. Furthermore, CSI can be used for object detection and even for specialized applications like in-car activity recognition. For instance, variations in CSI amplitude over time can indicate the presence and movement of a person, while phase shifts in the spatial and frequency domains can provide information about the direction and distance of movement.

2.2.2 CSI Based Localization Techniques

One of the important uses of CSI is indoor localization, which provides a more affordable and private option than other techniques, particularly in areas where GPS signals are not available. The widening reach of large datasets and advancements in computational power have also led to the broad acceptance of machine learning and deep learning techniques, such as Convolutional Neural Network (CNN) and Recurrent Neural Networks (RNN), to automatically extract complex features from CSI data and achieve higher localization accuracy and robustness in various indoor environments [18]. One famous technique is the Fingerprinting-based localization, which typically consists of two stages: the offline phase (also called the training phase) and the online phase (which is called the test phase). In the training phase, survey data is used and preprocessed. In the offline training stage, machine learning

methods can be applied to train fingerprints instead of storing all the received signal strength (RSS) data [24].

The author in [25] designed two CSI fingerprinting approaches called Amplitude-Based Fingerprinting (AmpFi) and FuFi (complete CSI fingerprinting), respectively. AmpFi uses a weighted KNN in the online phase to match a new CSI snapshot to the nearest fingerprint after recording the amplitude of each CSI subcarrier at reference points (off-line). FuFi goes one step further and uses the whole channel state for localization by using the normalized amplitudes of all subcarriers across the MIMO antennas as the fingerprint. Another category is Model-based that uses physical models of signal propagation to compute location from CSI without relying on a training map. For example, the authors in [26] proposed a multipath-assisted localization system using a single Wi-Fi receiver. They exploit CSI's phase and timing, where first they build a geometric model that associates the target's position and surrounding scatterers via ToF and AoA differences. Through a search (particle swarm optimization), they estimate the target and obstacle positions by comparing the measured ToF gaps between the direct path and reflections and using the measured AoA. With just one receiver, their model-based method achieved meter-level accuracy by directly calculating position using CSI's fine-grained phase and delay information.

Another interesting technique of Device Free Passive (DFP) localization was introduced by the authors in [27] from the Department of Computer Science at the University of Maryland, in which the entity does not require carrying any device or sensor to participate actively in the localization algorithm. This concept is to use preinstalled wireless networks to identify changes in the environment and track the location of entities passively without needing the entity to carry any device. The DFP idea depends on the reality that RF signals are impacted by environmental factors, particularly concerning the frequency ranges of the common wireless data networks that are either in use today, like Wi-Fi, or envisioned, such as WiMax. DFP may predict changes in the environment and link them with entities and their positions by setting up monitoring stations that continuously record physical qualities, which include signal strength and ToF.

The authors in [28] proposed an unsupervised view selective deep learning approach where they collected CSI from multiple AP, considering multiple views/angles where they automatically select the most salient CSI stream for training. A deep regression model is then trained on the chosen CSI view to map CSI directly to coordinates. Thus, without the need for a definite geometric model, the neural network starts learning the complicated mapping from high-dimensional CSI to location. They achieve extremely high localization accuracy in crowded indoor environments by employing deep learning and focusing on the strongest CSI view.

2.3 Privacy Concerns in Wireless Sensing

Automation, healthcare, home, and elderly monitoring are just a few of the many beneficial applications that have been made possible by the development and expansion of wireless sensors, particularly the device-free variety, which has greatly simplified daily life. However, these also pose significant privacy risks, particularly in indoor settings. With the aid of CSI and readily available COTS technology that may expose motions, gestures, presence, etc., there could be major active and passive attacks. This always makes wireless sensing both useful and dangerous, without requiring the subject to carry any device or wearables.

The potential of CSI, in particular its usage for decoding and equalization in wireless communication, to collect valuable PHY information about users that may pose significant privacy hazards has been the subject of numerous studies. In 2022, [29] investigation of CSI data allows unauthorized users to interfere with people's identification, presence, and movements by examining electromagnetic (EM) reflections embedded in the channel transfer function, $H(f, t)$. Even in encrypted signals, these reflections can be used for active injection or passive eavesdropping attacks, which completely circumvent upper-layer cryptographic safeguards. This leak is particularly challenging to prevent using traditional techniques because, in contrast to application-layer vulnerabilities, it is firmly anchored in the physics of wireless transmission.

The wired networks are more exposed to eavesdropping as compared to the wireless connections, it is because a wireless network uses air-borne radio frequencies to exchange information. On the other end, wireless networks, specifically those that are not reasonably secure, are more susceptible to data theft by unauthorized users. This is due to the fact that a wired network transmits and receives data via shielded copper wire or fiber optic cables, making it more difficult for an unauthorized user to perform eavesdropping, steal, or alter information that are being communicated, but a wireless network transmits data via radio frequency, which travels in the air, which makes its easy for unauthorized individuals to intercept the radio frequency and steal the information easily if the connection is not properly protected [30].

However, Wireless Sensor Networks (WSN) are frequently installed in remote or unattended locations, particularly in critical domains like healthcare and industrial settings, and they are constantly vulnerable to security threats. These systems can be the target of a variety of active and passive attacks, including denial-of-service attacks, illegal data alteration, and signal interception. Passive attacks are relatively difficult to detect, yet they can secretly collect important data without interfering with network operations. However, active attackers can compromise data integrity and system operation by interfering with communication channels, injecting malicious packets, or impersonating reliable nodes [31].

2.4 IEEE 802.11 Standards Evolution

WLAN, have expanded significantly over the past 20 years and are now a necessary part of human life since the IEEE standard 802.11 was originally published in 1997, as depicted in Table 2.1. The IEEE 802.11 standards specify the MAC and PHY requirements for local networks, laying out the guidelines and technical prerequisites for proper device cooperation and communication inside a single network. From the "legacy" 2 Mbit/s IEEE 802.11-1997 to the 11 Mbit/s of 802.11b, the 54 Mbit/s of 802.11a/g, the 600 Mbit/s of 802.11n, the 6.9 Gbit/sec of 802.11ac, and the above 30 Gbit/s rates of the upcoming latest 802.11be, the standards' evolution demonstrates a significant increase in nominal data rates.

Wider channels, quicker modulation and coding techniques, and the use of MIMO technologies have all been used to achieve these Wi-Fi rates [32]. MIMO technology is the primary new feature, enabling multiple data streams to attain raw data speeds of up to 600 Mbps in both the 2.4 and 5.2 GHz bands. The advent of multi-antenna streaming, which makes use of MIMO and Space-Time Coding (STC), signaled this important advancement in wireless communications. The STC is a coding technique that allows the separation of many data streams transmitted simultaneously with coding, and adaptive antenna arrays that may be intelligently directed to receiving devices allow the transmission beam to be focused more accurately[33].

To achieve multi-gigabit speeds with 802.11ac and 802.11ax, the emphasis switched toward greater spectral efficiency using methods like MU-MIMO, OFDMA, and bigger channel bandwidths (up to 160 MHz). By enabling up to 320 MHz channels, 4096-QAM modulation, and multi-link operation, the next 802.11be standard—also known as Wi-Fi 7 pushes the envelope even farther and aims for peak data rates beyond 30 Gbps. Higher capacity, reduced latency, and enhanced reliability in dense environments are all made possible by PHY innovations, especially the integration of multiple-antenna systems, adaptive beamforming, and complex coding techniques like STC. When taken as a whole, these characteristics demonstrate the continuous endeavor to improve WLAN performance in response to contemporary bandwidth-intensive applications like industrial automation, augmented reality (AR), and 4K/8K video streaming.

Standard	Year	Max Rate	Freq. Band	Modulation	Channel Width
802.11	1997	2 Mbps	2.4 GHz	DSSS / FHSS	20 MHz
802.11b	1999	11 Mbps	2.4 GHz	DSSS	20 MHz
802.11a	1999	54 Mbps	5 GHz	OFDM	20 MHz
802.11g	2003	54 Mbps	2.4 GHz	OFDM	20 MHz
802.11n	2009	600 Mbps	2.4 / 5 GHz	MIMO-OFDM	20 / 40 MHz
802.11ac	2013	6.9 Gbps	5 GHz	MU-MIMO, OFDM	20 / 40 / 80 / 160 MHz
802.11ax	2019	9.6 Gbps	2.4 / 5 / 6 GHz	OFDMA, MU-MIMO	20–160 MHz
802.11be	Upcoming	>30 Gbps	2.4 / 5 / 6 GHz	OFDMA, 4096-QAM, MU-MIMO	20–320 MHz

Table 2.1: Evolution of IEEE 802.11 Wi-Fi standards with increasing throughput, advanced modulation, and wider channel support.

The Independent Basic Service Set (IBSS) and Basic Service Set (BSS) are two distinct designs defined by IEEE 802.11. Multiple wireless devices, called stations (STAs), are connected to a central AP in a BSS, and all communication takes place via this AP. An IBSS, on the other hand, enables direct communication between stations as long as they are within the transmission range of one another. With this architecture, a wireless ad hoc network can be established independently of any preexisting infrastructure. To create a bigger network known as a Extended Service Set (ESS), several BSSs can be connected via a Distribution System (DS)[34]. Figure 2.3 illustrates the architecture of IEEE 802.11.

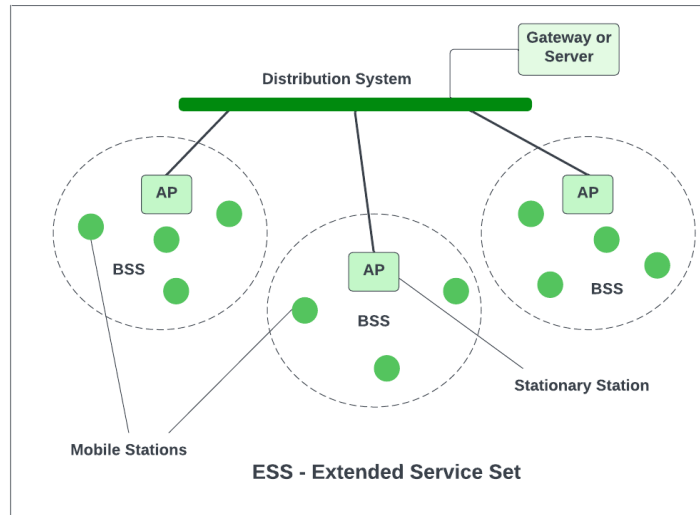


Figure 2.3: IEEE 802.11 Architecture[35]

IEEE 802.11 employs the Distributed Coordination Function (DCF), a contention-based technique. Using this technique, the STA connected to the AP checks the

air interface for available channels. The station utilizes the AP to transfer data to the destination if the interface is not in use. However, a collision occurs if the air interface is congested or if multiple STAs attempt to reach the same AP [36].

2.4.1 IEEE 802.11 Layers

The PHY and MAC Layers, which are the fundamental elements of the IEEE 802.11 standard, are continuously being improved with the newer technologies to provide end user faster and more seamless connections. The IEEE 802.11 standard specifies the protocols that control wireless communication in the lower layers of the network stack [37].

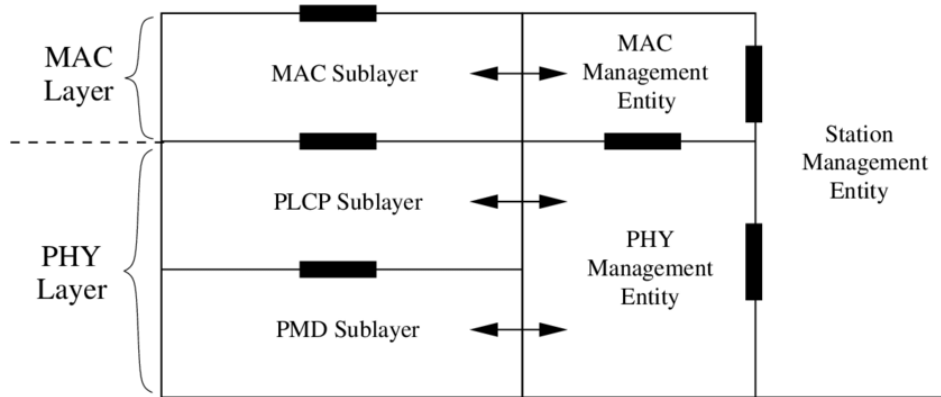


Figure 2.4: IEEE 802.11 PHY and MAC Layers

2.4.2 Physical (PHY) Layer

The PHY layer of the IEEE 802.11 protocol, that is known as Wi-Fi, is essential to control data transmission and reception through electromagnetic waves. To facilitate reliable transmission over tangible media such as radio frequency or infrared channels, it handles the conversion of digital data into radio signals and vice versa. The IEEE 802.11 PHY layer can further be divided into three sub-layers. The Physical Layer Convergence Procedure (PLCP) PHY sublayer holds the responsibility of obtaining the Clear Channel Assessment (CCA) to identify if the wireless medium is available for data transmission. The Physical Medium Dependent (PMD) sublayer is responsible for handling the interface between the wireless and PHY medium, and also manages the actual transmission and reception of the signal bits, including the processes of modulation (converting digital data into radio waves) and demodulation (converting received radio waves back into digital data). Finally, the PHY Management layer oversees the operation of the PHY, dealing with tasks such as selecting the appropriate channel for communication and controlling the transmit power [38].

Table 2.2 lists the three PHY layers that are accessible for the IEEE 802.11 WLAN.

Standard	PHY Layer	Freq. Band	Modulation	Channel Width	Data (Mbps)	Rates
802.11a	OFDM	5 GHz	BPSK, QPSK, 16-QAM, 64-QAM	20 MHz	6, 9, 12, 18, 24, 36, 48, 54	
802.11b	IR / FH / DSSS	2.4 GHz	CCK, DQPSK	20 MHz	1, 2, 5.5, 11	
802.11g	OFDM	2.4 GHz	BPSK, QPSK, 16-QAM, 64-QAM	20 MHz	1, 2, 5.5, 6, 9, 11, 12, 18, 22, 24, 33, 36, 48, 54	

Table 2.2: Characteristics of various PHY layers in the IEEE 802.11 standard.

Whereas IEEE 802.11a radios use OFDM to transmit at 5 GHz and carry data up to 54 Mbps, IEEE 802.11b radios make use of a Direct Sequence Spread Spectrum (DSSS), infrared (IR), and frequency hopping (FH) to broadcast at 2.4 GHz and transmit data up to 1 or 11 Mbps. Through an enhanced PHY layer known as the extended rate PHY layer (ERP), the IEEE 802.11g standard pushes the data-rate of the IEEE 802.11b to 54 Mbps in an upgraded PHY layer named as extended rate PHY layer (ERP) [39].

2.4.3 Medium Access Control (MAC) Layer

The MAC, which is situated above the PHY layer as shown in Figure 2.4, controls how devices access the physical channel for all upper layers and is responsible for managing how devices access and share the wireless communication medium, which basically provides two fundamental services: the MAC data service and the MAC management service [40]. The two medium access techniques are included in the IEEE 802.11 standard for wireless networks are: the mandatory DCF method and the optional Point Coordination Function (PCF) method [41]. The DCF is the main component of the IEEE 802.11 MAC protocol and operates via an Ethernet-like carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) method. After determining if the channel is available for transmission, a node waits for a random backoff time chosen from the interval

$$[0, CW...1]$$

, where CW is the contention window. A data packet is sent by the node when the timer hits zero. The process concludes when the recipient acknowledges (ACK). The sender chooses a new backoff, doubles CW, and tries again if not. Upon multiple unsuccessful attempts the packet is dropped. RTS/CTS (Request To Send/Clear To Send) frames are an optional way to reduce accidents on longer broadcasts. Since PCF, which is also defined by the MAC, is rarely supported and usually performs poorly, this work only concentrates on DCF [42].

2.5 Thread and OpenThread Architecture

Thread is a wireless mesh networking protocol that is designed for low-power, low-cost IoT devices. The Thread uses a two-layer approach. At the bottom, Thread uses the IEEE 802.15.4 radio that operates at (2.4 GHz, 250 kb/s), designed for low-power, low-latency communication. And on top of 802.15.4, Thread implements IPv6 over Low-Power Wireless Personal Area Networks (LoWPAN) to carry out Internet Protocol Version 6 (IPv6) packets. Each node in the Thread network can have one or more standards of IPv6 addresses [43, 44]. Thread is seamlessly capable of connecting to any IP-based network, including Ethernet, Wi-Fi, and the Internet in general, without the need for a single point of failure. This is done with the employment of an IPv6 over LoWPAN layer, which enables IPv6 packets to be routed back and forth using familiar IP protocols (User Datagram Protocol (UDP), Constrained Application Protocol (CoAP), Datagram Transport Layer Security (DTLS), etc), over any IEEE 802.15.4 network.

A Thread mesh network can have one or more Border Router (BR) which function as a bridge between the Thread network and the outer Thread network, like Wi-Fi, which offer routing services to other network devices [45]. The thread categorizes devices into two categories: end devices, which are battery-powered nodes that connect to a parent router, and routers, which are always-on, mains-powered nodes that maintain routes and transmit messages. While several Border Routers (often on Ethernet or Wi-Fi) connect the Thread mesh to the larger Internet, where one router is dynamically chosen as the Leader to coordinate network parameters. As a result, the network automatically reconfigures without a single point of failure if devices join, depart, or malfunction, creating a self-forming, self-healing IPv6 mesh [46]. To ensure security, Thread also has built-in security features where all traffic is encrypted with AES-128, and devices must authenticate (via DTLS and elliptic-curve key exchange) before being connected to the network, ensuring a trusted, secure mesh topology. In summary, Thread provides a secure, IP-based mesh over 802.15.4 with low-duty cycling, full IPv6 addressing, and dynamic routing, and this credential confinement prevents any external device from obtaining the network credentials, which ensures the confidentiality [47].

The Thread is specifically designed for home and building automation. It supports common smart-home devices, such as lighting controls, door locks, thermostats, sensors, smart speakers, etc. For example, the work presented in [48] provides a detailed system-level model analyzing latency within Thread mesh networks, particularly in the context of proximity services in smart homes and building automation. It inspects delays across various layers from application to physical and evaluates Thread's suitability for user-friendly and safety-critical applications in home and building automation. A comparative study carried out between Thread and Zigbee protocols about their implementation in home and commercial building automation is presented in [49]. It features Thread's advantages, such as its IPv6-based mesh

networking, low power consumption, and scalability. The document explores how Thread's design enables effortless connectivity and integration of devices, which enhances network reliability and supports future-proofing through compatibility with various application protocols.

2.5.1 Comparison with Zigbee and Wi-Fi

Architecture

Despite having different layers, Thread and Zigbee both enable mesh architecture and operate on 802.15.4 radios. Every node in Thread is IP-addressable and has inherent packet forwarding native capabilities because it uses 6LoWPAN/IPv6 as its network layer. The address of a Zigbee node must be converted to IP via a gateway, as Thread defines its own network and application layers using 16-bit addresses [43, 45, 49]. Wi-Fi by comparison is a family of wireless network protocols based on IEEE 802.11 that uses entirely different PHY MAC and typically operates a star topology: Wi-Fi assumes all devices are IP-capable, and uses high-rate OFDM links with AP, rather than a multi-hop 802.15.4 mesh [50]. Ultimately, Thread is a low-power IP LAN over 802.15.4, while Zigbee is a proprietary 802.15.4 Personal Area Network (PAN) stack with translation to IP, and Wi-Fi is a high-speed IP LAN over 802.11.

Power Efficiency

Zigbee and Thread are made to run on little power. Both employ duty cycling to allow battery-operated end devices to slumber for most of the day. The Thread is especially well-optimized: gadgets use "low duty cycle, sleeping nodes, and energy-efficient routing" to reduce power consumption, allowing sensors to have multi-year battery life.

Additionally, Thread supports sleepy end devices, which turn down their radios and only activate in response to an event. The Thread employs the optimal path while routing, resulting in low power consumption [51]. Zigbee 802.15.4 technology also supports sleeping modes, though its larger software stack may consume more memory. For the motes to spend the majority of their time in a low-power (sleepy state) their activities must be minimised. Thus, all a mote needs to do is awaken to detect and send the information for a small fraction of time [52]. Wi-Fi radios typically utilize more power, because keeping a Wi-Fi link up needs continuous radio activity and high data rates, so Wi-Fi IoT devices require regular wake-ups or main power.

Scalability

Thread networks can scale up to hundreds of devices, and in general, a Thread network can support up to 16,384 addressable devices (1 Leader, 32 active routers with 511 children or end devices each). Each Thread router can hold the full topology, so routing capability remains efficient at a large scale. Zigbee also supports mesh

expansion via routers, but commercial Zigbee systems typically handle far fewer nodes (often just dozens to a few hundred), since a central coordinator often limits size. A thread network can be initiated as a Router-Eligible-End-Device (REED), meaning that if it does not find any network so it can join the existing network as the Leader and to which other devices may connect through some standard joining and commissioning procedure [46, 49]. Wi-Fi networks scale very differently, where a single Wi-Fi AP is capable of maintaining stable services for a few dozen clients. However, every Wi-Fi device carries the full 802.11 overhead, and extending range requires separate APs [50].

Chapter 3

CSI-Based Localization with IEEE 802.11be

The growing interest in wireless sensing, highlighting specific methods that exploit CSI, marks a key edge to improve applications with contextual information, especially in the evolving context of 6G and next-generation Wi-Fi standards [53, 54]. This relies on the fundamental concepts of CSI-based sensing and localization previously described in Chapter 2 Section 2.2, which emphasized the critical role of fine-grained channel information. Device-free sensing, in particular, is gaining prominence across smart homes, healthcare, and general IoT applications, offering a non-intrusive means of gathering environmental intelligence. However, achieving high precision in indoor locations remains a considerable challenge, largely due to the inherent unreliability of traditional GPS signals within enclosed spaces. An essential scientific exploration driving current research revolves around the influence of emerging Wi-Fi technologies on sensing precision. This chapter specifically addresses this question in the context of the forthcoming IEEE 802.11be standard, commonly known as Wi-Fi 7.

Wi-Fi 7 promises major improvements, including wider channels up to an increased bandwidth of 320 MHz and providing an incomparably higher number of subcarriers, reaching 4096 per spatial stream. However, researchers still have limited access to CSI extraction tools for such systems. To fill this necessary gap, this chapter presents several key contributions. First, it details the design and public release of an open-source framework built upon Software-Defined Radios (SDRs), to investigate the potential impact of new Wi-Fi features, namely the wider channels and the higher number of subcarriers, on a device-free positioning system based on positioning fingerprinting. Second, it provides a comprehensive analysis of the impact and performance variations of this new technology across diverse bandwidths and frequency sub-bands within a device-free position classification system. Lastly, the results provide initial recommendations, clearly defining a path for further studies

focused on maximizing the use of more recent Wi-Fi channels for improved sensing. The SDR framework, the sensing architecture, the experimental setting, and a comprehensive analysis of the findings will be covered in detail in the sections that follow.

3.1 Emulating IEEE 802.11be Transmissions: The SDR framework

Employing the SDR approach was a necessary choice for this work, in order to mitigate the limitations of commercial CSI extraction tools that are compatible with the latest IEEE 802.11be standard. Some solutions exist, such as closed-source software like PicoScenes [55] or some custom implementation. CSI extractors that work also on commercial systems are limited to the IEEE 802.11ax standard (e.g., again PicoScenes for Intel network cards or AX CSI [56] on Broadcom cards). Older CSI extractors are still popular today, with the Linux 802.11n CSI Tool [10] is still widely used today for Wi-Fi sensing activities [57]

In this work, we adopt a custom SDR implementation based on Ettus devices and supported by Matlab. On the transmitter side, the IQ samples corresponding to a transmission frame are prepared in Matlab and then passed to the Ettus device that implements the Digital to Analog (D/A) and the transmission on-air; on the receiver side, the Ettus device implements the antenna front-end and the A/D, and the Matlab script recovers the received frames from the received sampled radio signals. In the rest of the work, we explore the impact of the bandwidth of the Wi-Fi signals on the performance of a target sensing application, specifically, a simple device-free localization algorithm described in Section 3.3.

The methodology proposed in this work uses two MATLAB instances. One instance is dedicated to the precise generation of In-phase and Quadrature (IQ) samples, corresponding to well-formed IEEE 802.11be frames, at the transmitter side. The other instance is responsible for extracting and processing the CSI from each received frame at the receiver. These Wi-Fi frames are then exchanged over the air using wideband SDR platforms.

Hardware and Software components

The experimental setup consists of two Ettus X310 SDR motherboards, configured as a pair of Tx and Rx. Each X310 is equipped with a pair of integral UBX 160 daughterboards that divide the signal into two parts, upper and bottom, to the system's signal processing capabilities. The MATLAB WLAN toolbox is used as the basic software for useful CSI extraction and Wi-Fi frame creation. In addition, C++ software was created to control the synchronized transmission and receiving of 320 MHz signals, which was necessary for an effective experimental setup.

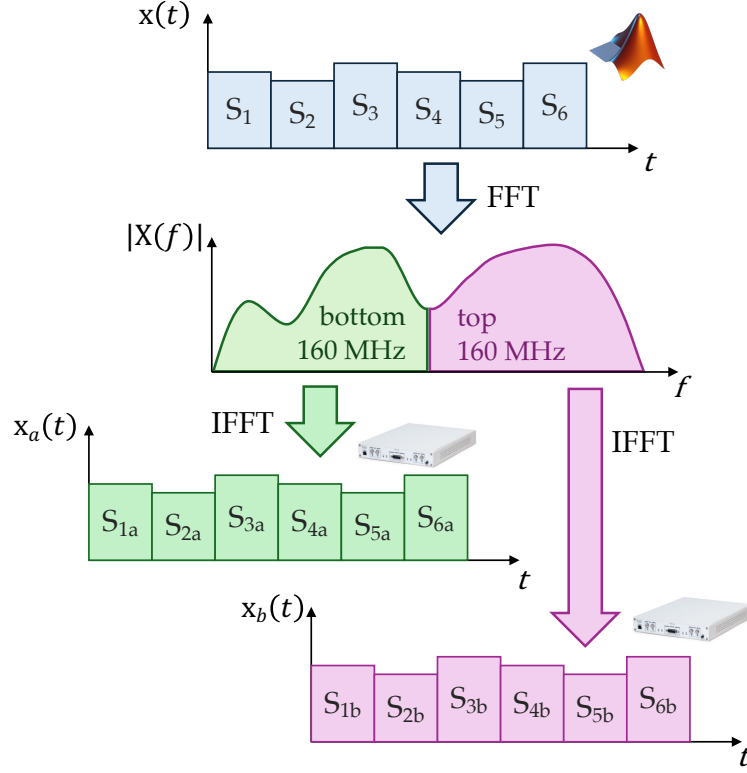


Figure 3.1: Illustration of the procedure used to split a 320-MHz signal generated by MATLAB into two halves (each of 160 MHz) that are compatible with the SDR front end. Each OFDM symbol from the original signal at 320 MHz is processed in the frequency domain to create the corresponding copies and generate the two signals carrying the bottom and top parts of the original spectrum. Here we emphasise the process for symbol s_4 .

The Wi-Fi frames are exchanged over the air using wideband SDR platforms. Specifically, we used two Ettus X310 SDR motherboards (one for transmitting and one for receiving), each equipped with a pair of UBX 160 daughterboards. Even though the UBX 160 daughterboards have a maximum bandwidth of 160 MHz, we can successfully transmit and receive 320 MHz Wi-Fi frames by splitting the signals into two halves, each transmitted by a separate daughterboard. This process, shown in Figure 3.1 and key to experiment with 320 MHz bandwidth, is now explained in detail.

Transmitting Operations(Generating 320 MHz signals)

The ideal task in the model is to split the wideband signal into two parts, each 160 MHz, which is essential because the UBX 160 daughterboards have a band limit that could support up to 160 MHz. The process begins with the generation of a

sequence of IQ samples in MATLAB, corresponding to a well-formed Wi-Fi frame. This resultant is a complex signal in the time domain, sampled at 320 MSample/s. From the time domain signal, the sequence of OFDM symbols is recovered by reversing the signal construction process of the EHT-PHY specification ([58], Chapter 36). Specifically, the WLAN toolbox is first used to identify the OFDM symbols' boundaries; then the windowing and the Guard Interval (GI) are removed, and the FFT is applied to each OFDM symbol to obtain all its subcarrier coefficients, that is, its spectral content. In the case of 320-MHz 802.11be frames, every OFDM symbol consists of 4096 subcarriers, equally spaced by 78.125 kHz.

This processing step is illustrated in the first part in Figure 3.1, where each OFDM symbol signal generated by MATLAB in the time domain is transformed into its corresponding representation in the frequency domain. The 4096 OFDM subcarriers are split into two equal parts: top and bottom, each with 2048 subcarriers. Then, each part is processed with the same operations in reverse order to obtain two signals in the time domain, sampled at 160 MSample/s, corresponding to the top and bottom halves of the original signal's spectrum. The top and bottom parts of the 320 MHz signal are sent to the two daughterboards mounted on the transmitter after an upsampling operation that matches the signal bandwidth to the rate of the master clock on the X310 SDR, which is 200 MHz. The two daughterboards are tuned at ± 80 MHz from the central frequency of the Wi-Fi channel and are connected to an RF multiplexer so that the resulting 320 MHz signal is transmitted from a single antenna as if a single device generated it.

It is important to note that the double-radio approach described so far splits the wideband signal over two carriers, thus introducing a double hump shape in the signal's spectrum, with the two peaks centered around -80 MHz and 80 MHz, that is, the central frequencies of the two daughterboards. To mitigate this effect, we apply a pre-equalization mask to the signals fed to the two transmit daughterboards. The specific shape of the pre-equalization masks are determined before the on-air experiments are run. Its actual design is derived empirically, equalizing the spectral content of frames' preambles transmitted over a coaxial cable so that it results flat spectrum on the entire 320 MHz channel.

Receiving Operations(Reconstructing 320 MHz CSI)

The operations in the receiver are the inverse of those performed at the transmitter, designed for precise signal recovery. Firstly, the 320 MHz radio signal is captured by a single antenna, and then it is fed into a splitter, which generates two replicas without any power loss. These replicas of the signal are then sent to the two daughterboards mounted onboard on the receiving X310 SDR. The daughterboards are accurately tuned at the same ± 80 MHz frequencies as their transmitting counterparts, allowing each to capture either the lower or upper part of the original signal's spectrum. The daughterboards work at 200 MSsample/s, so each of the portions of the spectrum must be properly and accurately filtered to retain exactly the 160 MHz top or bottom part of the spectrum respectively. Following this, then they are

up-sampled at 320 MSsample/s and the two signals are shifted at the proper frequency and added together to get the original 320 MHz Wi-Fi frame. Finally, the MATLAB WLAN toolbox extracts the CSI.

3.2 Other considerations and Limitations

Accurate synchronization between the transmitting and receiving X310 SDRs is highly important for the robustness and effectiveness of the experimental setup. This was made possible through the use of an Ettus Octoclock that provides a Pulse-Per-Second (1 PPS) and 10 MHz reference signals. This synchronization emphasizes having multiple purposes: that includes allowing the receiver to capture samples only when the transmitter is active, effectively reducing the storage required for each experiment. Furthermore, it speeds up processing by eliminating the need for the receiver to search for frame boundaries, as the timing is highly aligned. To achieve this second goal, we developed custom C++ software to control the synchronized transmission and reception of 320 MHz signals. To the best of our current information, no other open source code offers the capability to collect and analyze 320 MHz Wi-Fi frames (PicoScenes supports 802.11be frames but is mostly closed source), which highlights the potential contribution to shift research practices that foster reproducible research in a field where proprietary tools are common. Second, a practical limitation of the X310 SDRs, which cannot work above 6 GHz, is in the spectrum slab actually assigned to 802.11be. Hence, we must work on lower frequencies during our experiments. Given the central frequency of the 320 MHz Wi-Fi channel, we analyze all possible subchannels as shown in Figure 3.2. This segmentation of the Wi-Fi channels can be used to examine the impact of different bandwidths on the sensing performance and compare the sensing performance when using data from different subchannels.

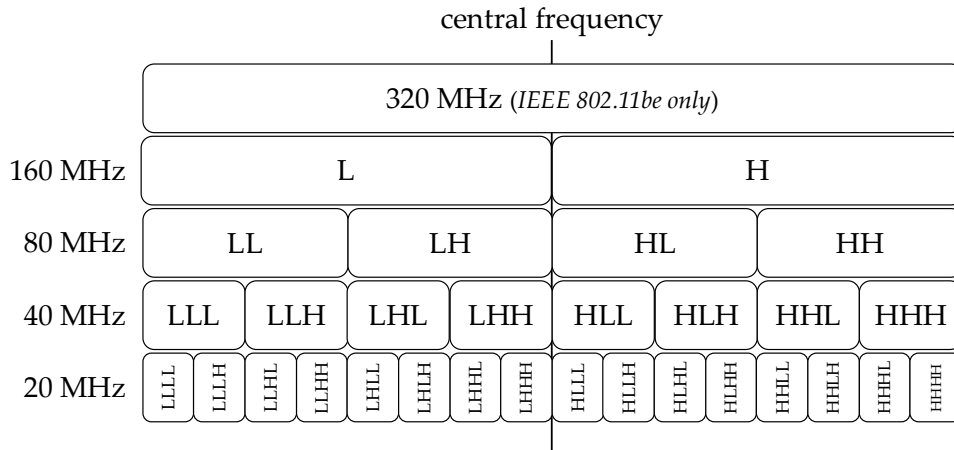


Figure 3.2: Visualization of the relation between standard Wi-Fi channels and naming scheme used in the experiments for each bandwidth.

3.3 Sensing Architecture for Device Free Positioning

Several CSI-based sensing architectures and methods have been considered by the research community in the last few years. In this work, a device-free positioning was chosen, which employed a fingerprinting approach [59] based on a CNN. This method was selected, which has the merit of being simple and allowing easy adjustments of parameters. A more detailed background on CSI-based localization techniques, including the principles of fingerprinting, can be found in Chapter 2, Section 2.2.2. Moreover, the focus of the work is not on the sensing algorithm, and we think that the impact of different bandwidths is similar on most algorithms, unless they are specifically tuned based on a particular bandwidth and signal structure.

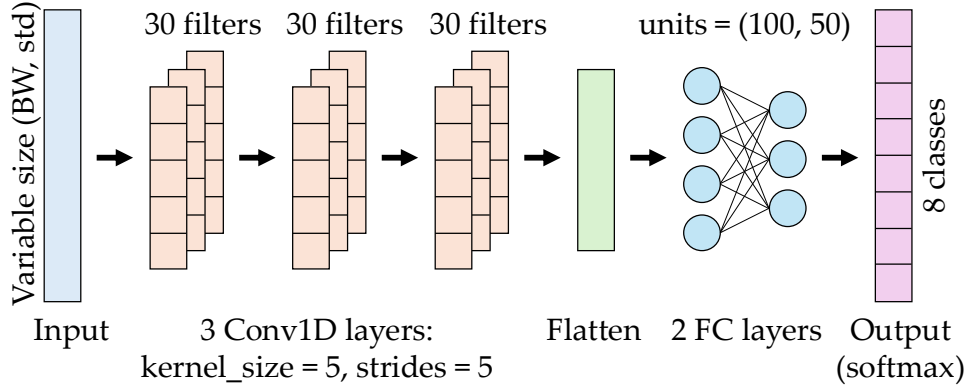


Figure 3.3: Architecture of the neural network for the positioning task. All the hidden layers use a ReLU activation function.

Convolutional Neural Network (CNN) Architecture

The ideal component of a positioning classification system is the CNN, which maps each input CSI to one of the eight predefined target positions to solve a classification problem. Figure 3.3 shows the architecture of the CNN employed in this work. In short, CNN is utilized to solve a classification problem where every input CSI is mapped onto one of eight target positions. The CNN has a straightforward structure that comprises three convolutional layers that are followed by a flattening layer that transforms the multidimensional output into a single vector. This flattened vector is then processed by two fully connected (FC) layers. The activation function in all the hidden layers is a Rectified Linear Unit (ReLU) function, while the output layer uses a Softmax activation function. The number and shape of the hidden layers are fixed; the only variable in the definition of the CNN architecture is the size of the input layer, which depends on the bandwidth of the input CSI and on the Wi-Fi standard considered.

System Configuration (SISO)

This work considers only Single-Input Single-Output (SISO) systems, allowing us to focus only on the signal bandwidth as the primary variable of our analysis, leaving out the effects caused by multiple spatial streams and different antenna patterns that may influence the sensing performance. These findings may shed more light on how sensing performance could be affected only by the bandwidth factor.

3.4 Experimental Setup and Data Collection

All of the experimental work was carried out in the Advanced Networking Group (ANS) telecommunication laboratory, an integral part of the Information Engineering Department at the University of Brescia. Figure 3.4 displays the layout of the site for the experiments, highlighting the location of the transmitter (TX) and the receiver (RX), which were placed at fixed locations. Additionally, eight distinct target positions were established, which are labeled from P1 to P8. The positions acted as the basis for the performance evaluation of the device-free positioning system.

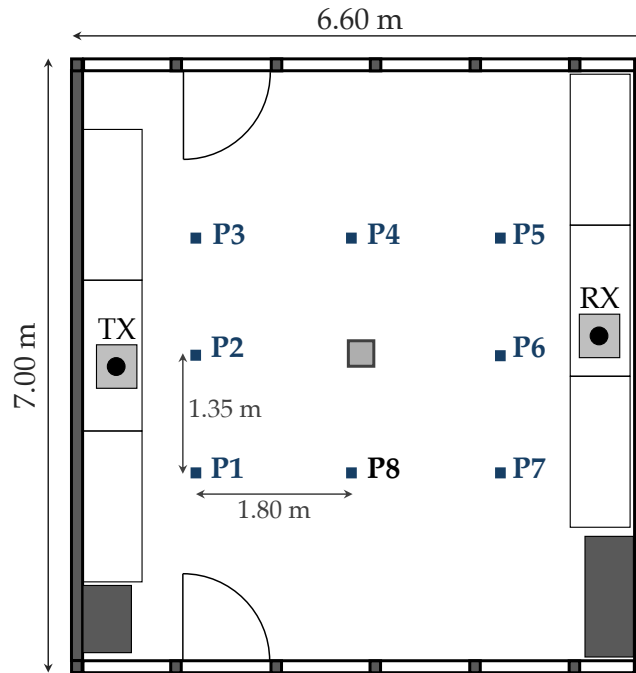


Figure 3.4: Layout of the experimental setup.

Data Collection Methodology

The data were gathered extensively covering a range of bandwidths, which can be visualized in Figure 3.2, which includes 20, 40, 80, 160, and 320 MHz. Additionally, experiments included frames from two different IEEE 802.11 standards: named as

IEEE 802.11ac and IEEE 802.11be. We deliberately included smaller bandwidths, such as 10 MHz bandwidth, generally associated with the IEEE 802.11p standard that is used for vehicular communications, only to discover any trend in the relation between the bandwidth and sensing accuracy. The data collection procedure was standardized to ensure consistency and comparability. During each session of data collection, a person stood on each of the eight target positions. While the person was in position, the transmitter (TX) began transmitting 800 Wi-Fi frames at a constant rate of 100 frames per second.

Hence, during each data collection session, the system recorded a total of 6400 CSI data points, over a complete round for eight targeted positions, meaning 800 samples were collected for each of the positions. This is repeated twice for every band and Wi-Fi standard under analysis, with each collection session separated by at least 10 minutes. The data collected during the first run is used to train the CNN in the positioning system, and the other dataset is used to test the accuracy of the positioning framework. In this way, training and testing samples do not contain CSI data collected from the same round of experiments but are collected in two separate phases, ensuring that the accuracy is not biased because the samples for training and testing are collected during a single session. This is inspired by a realistic application scenario in which someone wants to first train the localization framework and then use it to actually localize a person in a room at a later time. As shown in Figure 3.3, the CSI are processed independently one at a time, and each CSI has attached the ground truth label that is the index of the corresponding position. The experimental parameters are summarized in the Table 3.1 below for quick reference to readers.

3.5 Experimental Results and Analysis

The main objective of this work is to thoroughly assess the accuracy of the device-free sensing framework as a function of various Wi-Fi bandwidths. To the best of our knowledge, the question about possible correlations between Wi-Fi bandwidth and sensing accuracy has not been tackled yet, and even recent surveys [15, 60] do not mention studies in this direction. Although many scholars expect that an increased bandwidth can improve sensing accuracy. Only [61] very recently explored the effect of different channels (namely channel 6 with 20 MHz on the 2.4 GHz band and channel 36 with 80 MHz on the 5 GHz band), found a 6% increase in accuracy using channel 36 when the goal is to count people in a room. However, the authors did not perform experiments to distinguish whether the effect is due to the different bandwidth, the different frequency band, or simply less noise and interference in the 5 GHz band.

Parameter	Description
Location of Experiment	ANS Telecommunication Laboratory, University of Brescia
TX/RX Hardware	Ettus X310 SDRs equipped with UBX 160 daughter-boards
Number of Positions	8 (labeled P1 to P8)
Wi-Fi Standards Tested	IEEE 802.11ac, IEEE 802.11be, IEEE 802.11p (for 10 MHz bandwidth)
Bandwidths Tested	10 MHz, 20 MHz, 40 MHz, 80 MHz, 160 MHz, 320 MHz
Frames per Position (per Session)	800
Frame Transmission Rate	100 fps
Total CSI Data Points per Session	6400 (800 frames $\times$ 8 positions)
Training Data Methodology	Data collected during the first experiment run
Testing Data Methodology	Data collected during the second experiment run
Time Between Sessions	10 minutes

Table 3.1: Summary of experimental parameters used in the data collection

3.5.1 Impact of Wi-Fi Bandwidth and Standard on Localization Accuracy

The findings demonstrate the analysis on the performance comparison across different Wi-Fi bandwidths using both IEEE 802.11be and 802.11ac frames, as illustrated in Figure 3.5. The results report the average accuracy over ten repetitions, where vertical bars indicate the standard deviation, providing the reliability of consistent performance. An observation of note is the clear correlation between increased bandwidth and improved positioning accuracy. Specifically, transmissions that utilize 320 MHz consistently yielded the best results, achieving a perfect or near-perfect 100% positioning accuracy in the conducted experiments. However, using very large channels to get good results is unnecessary, and 80 MHz channels are likely sufficient in the simple scenario that we considered. Additionally, 20 MHz transmissions showed excellent performance, consistently maintaining an average accuracy above 80%. Second, the localization with 802.11be frames performs better than that with 802.11ac frames. This is somewhat expected, as 802.11be CSI data has four times the size of the corresponding 802.11ac CSI, and thus can potentially provide more information for the localization task, but the difference is not striking. The second important conclusion indicates that localization performed with 802.11be frames generally shows higher precision than with 802.11ac frames. This performance discrepancy is explained by the fact that 802.11be CSI data is four times greater than

its 802.11ac counterpart within the same bandwidth. This larger data size potentially provides more information for the localization task, although the difference was described as "not striking" when ample training data was readily available.

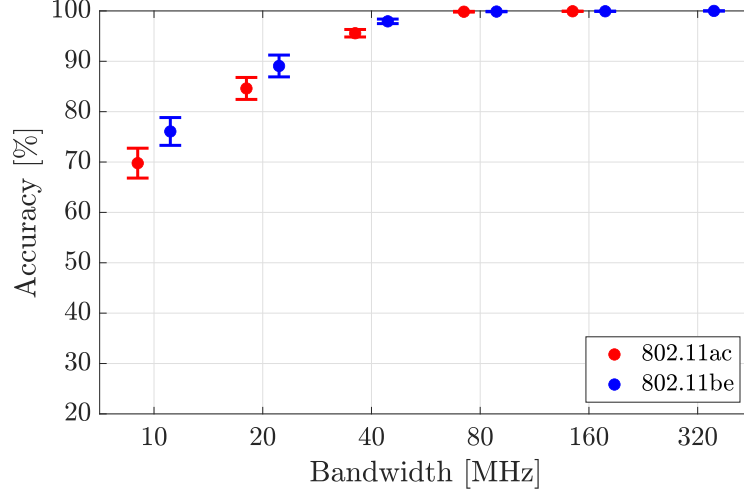


Figure 3.5: Performance comparison for different Wi-Fi bandwidths using 802.11ac and 802.11be frames. Dots indicate average results over 10 repetitions; vertical bars represent standard deviation. Both training and testing are done, collecting 800 CSI per position. Training and testing experiments are separated by at least 10 minutes.

3.5.2 Influence of Sub-Channels and Spectral Position on Sensing Performance

An important aspect of the analysis involves investigating the influence of various Wi-Fi channels that share the same Wi-Fi bandwidth, but occupy different positions in the spectrum. The goal is to determine whether the specific frequencies have an impact on the CSI data. Our experimental findings revealed substantial variance that was obtained with 10-MHz subchannels, where the accuracy varied greatly, ranging from a minimum of 38.75% (on channel HLLLH) to a maximum of 96.0% (on channel LLHLH). In General, we found that this variance steadily dropped as the total bandwidth rose. A possible reason could be that the specific sensing information is not equally distributed across the entire frequency spectrum; instead, it might be localized or concentrated in specific frequency bands. For narrower channels, there is a high risk of selecting a subband that lacks these crucial features, leading to significant performance degradation. This suggests again that CSI sensing on wider Wi-Fi channels can produce better and more stable results, while using narrower channels can miss some details and quickly lead to overfitting problems during the training phase. This also indicates that the information embedded into a larger-bandwidth signal is not necessarily more or better, but that on a larger bandwidth, there are higher chances to hit the specific frequency that carries the

information the localization system is trying to single out.

3.5.3 Effect of Training Data Size on Model Performance

Continuing our analysis, we further investigated how training a model on a limited number of CSI data samples affects sensing performance. Thus, we started the training dataset by reducing the dataset to 200 CSI samples per target position, as shown in Figure 3.6, showing a reduction in positioning accuracy. This is expected for data-driven models like CNN, used in this work, which need to be trained on large datasets. However, the results consistently confirmed that positioning performed with 802.11be frames maintained higher accuracy than with 802.11ac frames, and it was proven that the strong correlation between bandwidth and positioning accuracy is highly significant.

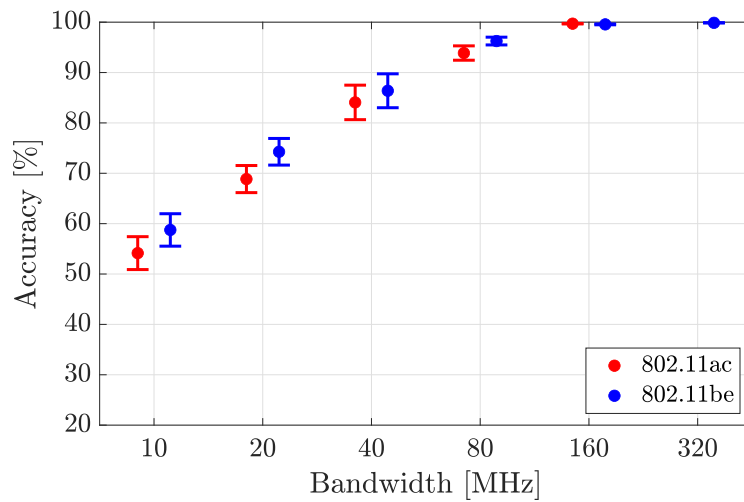


Figure 3.6: Performance comparison when training the localization model with only 200 samples per position.

However, in this scenario, the use of 80 MHz frames was not sufficient to achieve almost perfect positioning. Moreover, we observed a decline in accuracy with narrower bands. For example, the accuracy of the model using 40 MHz channels and 802.11ac frames dropped from approximately 95% to 85% on average, while the accuracy of the 10-MHz 802.11ac model decreased from 70% to 55%. We recall that these are aggregated results obtained by averaging over all the possible sub-bands and multiple repetitions of the experiments.

Finally, we evaluate what happens to the sensing framework when we reduce the number of training samples even further. Figure 3.7 shows the positioning accuracy when only 25 CSIs for each position are considered to train the CNN. Even in this case, the relation between bandwidth and positioning accuracy is confirmed.

Models trained using 160-MHz and 320-MHz frames still perform the best, with accuracy well above 90%. In addition, models based on 802.11be frames provide more information for device-free positioning than 802.11ac frames.

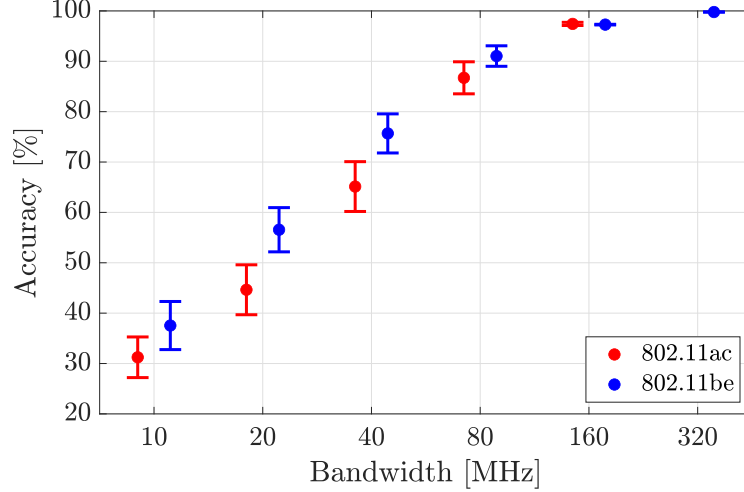


Figure 3.7: Performance comparison when training the localization model with only 25 CSI per position.

3.5.4 Impact of Data Collection Duration on Sensing Accuracy

We have experimentally verified that the number of OFDM subcarriers directly impacts the sensing accuracy for simple data-driven models. In addition, the number of training samples can greatly affect the sensing performance. Another aspect we would like to verify with our experiments is whether it is better to collect CSI data in quick bursts or over longer periods of time. To this end, we again consider only 200 CSI samples per position to train the positioning model, but in one case they are taken in a short period of 2 seconds while in another case they are taken over 8 seconds (i.e., with a sampling frequency of 25 CSI per second). In Figure 3.9 and Figure 3.8, we report the classification performance obtained while testing the positioning with 802.11ac frames at 40 MHz. The confusion matrices show that capturing the CSI for longer periods of time is better than short bursts. Indeed, taking several CSI measurements in short time periods may miss features that instead are clear on a longer time scale. This shows that a longer observation window allows the model to capture a more diverse and representative range of channel variations, including subtle, slower-changing features. A summary of key accuracy results in various conditions is provided in the Table 3.2 below:

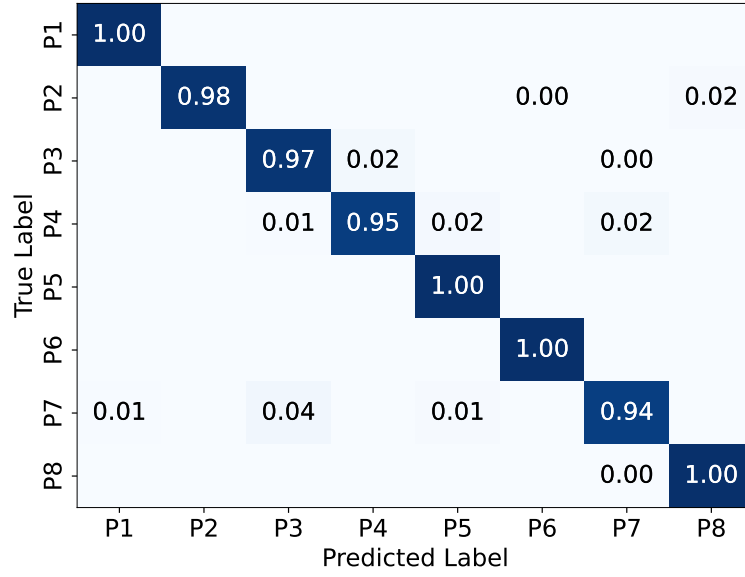


Figure 3.8: Confusion matrix obtained by training the positioning model with 40-MHz 802.11ac frames. Only 200 training CSI samples have been used, distributed equally over the entire time frame of the experiment of 8 seconds.

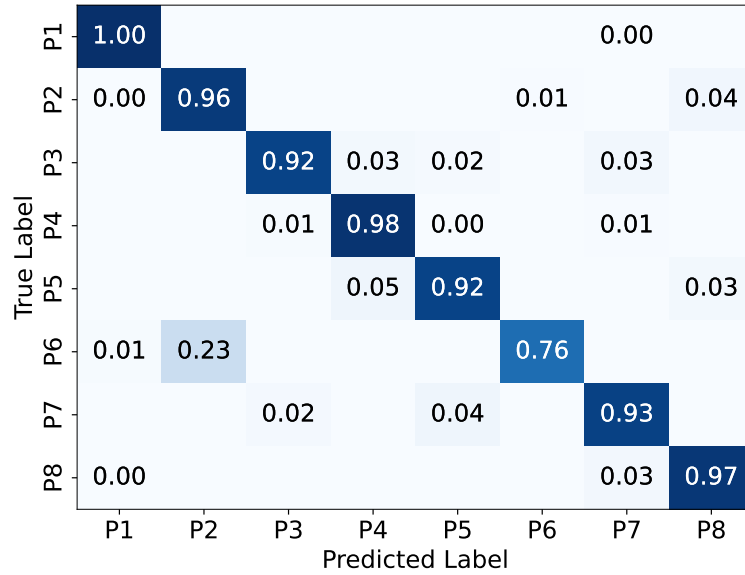


Figure 3.9: Confusion matrix obtained by training the positioning model with 40-MHz 802.11ac frames. Only 200 training CSI samples have been used, restricted only at the beginning of the experiment lasting for only 2 seconds.

Band (MHz)	Wi-Fi Std	Training Samples	Avg. Accuracy (%)	Std. Dev
<i>Full Dataset (800 samples)</i>				
320	802.11be	800	100	Low
160	802.11be	800	~98	Low
80	802.11be	800	~95	Low
40	802.11be	800	~92	Low
20	802.11be	800	~85	Low
10	802.11be	800	~75	High
160	802.11ac	800	~95	Low
80	802.11ac	800	~90	Low
40	802.11ac	800	~88	Low
20	802.11ac	800	~82	Low
10	802.11ac	800	~65	High
<i>Reduced Dataset (200 samples)</i>				
320	802.11be	200	~98	Low
160	802.11be	200	~95	Low
80	802.11be	200	~88	Low
40	802.11be	200	~88	Low
10	802.11be	200	~65	High
40	802.11ac	200	~85	Low
10	802.11ac	200	~55	High
<i>Minimal Dataset (25 samples)</i>				
320	802.11be	25	>90	Low
160	802.11be	25	>90	Low
160	802.11ac	25	>90	Low

Table 3.2: Classification accuracy for different bandwidths, Wi-Fi standards, and sample sizes. Accuracy values are approximate based on visual interpretation; standard deviation is categorized as Low or High.

The experimental results shown in Figure 3.10 and Figure 3.11 evaluation demonstrate that IEEE 802.11-be significantly improved CSI based sensing accuracy compared to IEEE 802.11-ac. This improved accuracy remained consistent across varying bandwidths (20 – 160 MHz) and CSI sampling strategies tested in this work, with effective performance achieved using equally distributed CSI with high sampling density.

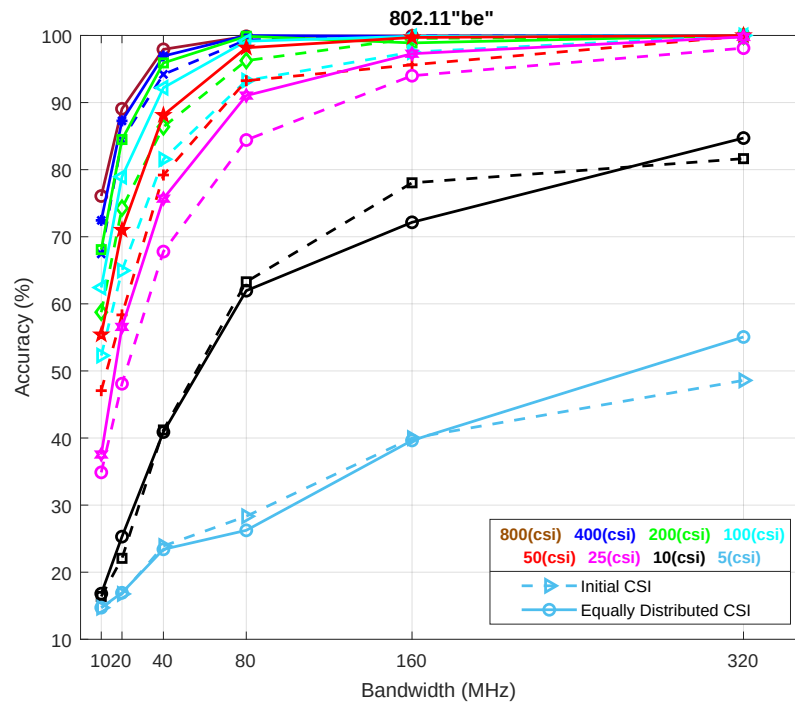


Figure 3.10: IEEE 802.11-be Overall Accuracy Results

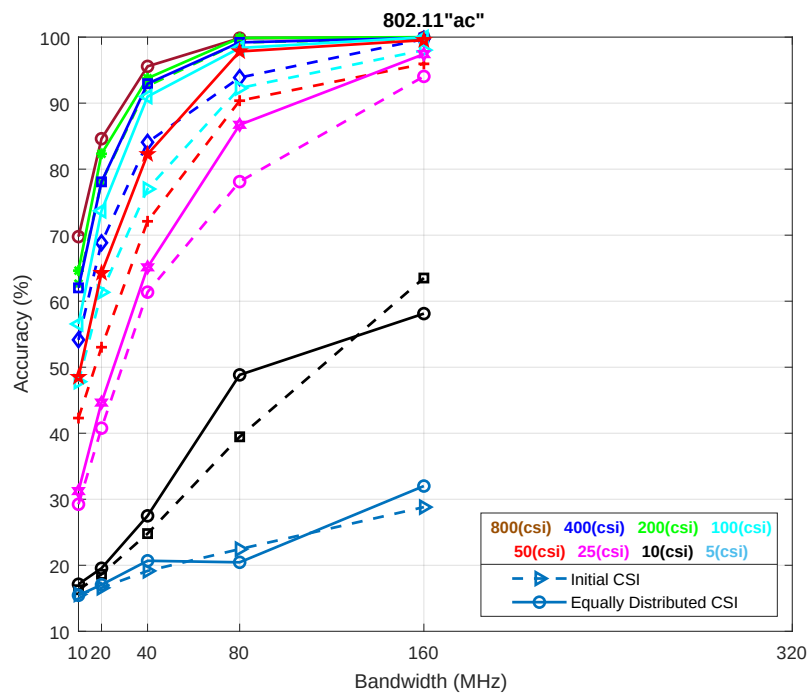


Figure 3.11: IEEE 802.11-ac Overall Accuracy Results

3.6 Discussion

The results presented in this chapter highlight a clear relationship between the bandwidth of Wi-Fi signals and the accuracy attainable in device-free positioning applications. Wider channels, such as 320 MHz featuring IEEE 802.11be, consistently provided better sensing performance. This performance improvement is not exclusive to an increased quantity of data, but in fact is the higher probability of capturing the specific frequency components that are most selective for sensing. The larger CSI data size of IEEE 802.11be frames is a result of the increased OFDM subcarrier density, which positively contributes to better performance compared to IEEE 802.11ac. This turns out to be an advantage under conditions where training data are limited, emphasizing IEEE 802.11be’s robustness for data-driven sensing models. Another important discovery is a key to data collection strategy: if we collect CSI samples over a longer period of time, even with the same number of samples, it captures a more comprehensive view of channel interactions, leading to more robust and reliable models. This guarantees that the model learns widespread features contaminated in the channel and which helps in avoiding overtraining to temporary channel variations. Moreover, the observed spectral nonuniformity of sensing features suggests that, although some crucial features for localization may be concentrated in specific subbands, spanning a wider bandwidth spectrum effectively reduces the risk of missing this important information. As a result, the sensing results are more consistent across different channel conditions.

This makes our findings a novel contribution to the field, whereas many other previous studies blended effects of the bandwidth with the differences in frequency bands or noise, whilst this study isolates the bandwidth impact. The benefits of using Wi-Fi 7 (IEEE 802.11be) for localization are profound, but it cannot be termed as an evolution of communication throughput, but rather a decisive technology that helps to enhance capabilities for advanced sensing applications, specifically in environments such as smart homes, healthcare monitoring, and IoT applications in general.

This work, therefore, establishes a firm foundation for future findings on the potential use of Wi-Fi sensing. From the results, it is obvious that using IEEE 802.11be provided very good results, but the investigations also provided insights that if we use 80 MHz channels, they might be sufficient for sensing. However, the focus of the work was solely on Device Free Localization (DFL) sensing and was limited to Single-Input Single-Output (SISO) systems, which indicates that the bandwidth that we observed might vary when more complex algorithms such as MIMO or different antenna patterns are employed. Furthermore, there are some limitations of the hardware that we considered in this work, where the chosen SDRs do not support bandwidth above 6 GHz; therefore, the experiments were conducted mainly at lower frequencies.

Chapter 4

CSI Obfuscation and De-obfuscation for Privacy Protection

This chapter demonstrates the importance of privacy and environmental sensing in Wi-Fi-enabled networks, with a particular attention on susceptibilities induced by CSI and a novel initiative based on CSI obfuscation and de-obfuscation. While the ubiquity of Wi-Fi traffic and its inherent CSI enable a wide range of environmental sensing applications such as device-free localization and human activity recognition, this capability simultaneously presents significant privacy risks due to the potential for unauthorized surveillance. To address these concerns, the work proposes an active defense mechanism that performs distortion to the Wi-Fi signals at the transmitter side (obfuscation) to prevent the process of harmful sensing, while only allowing authorized users to perform the reverse operation known as distortion (de-obfuscation) and restoring the legitimate sensing capabilities. As a case study, we analyze device-free localization, involving two distinct obfuscation patterns and three levels of distortion strength, verifying that stronger distortion is more effective but harder to reverse. In general, proper de-obfuscation can almost completely restore localization accuracy; however, it becomes more challenging when obfuscation patterns introduce notches in the CSI, i.e., when some subcarriers reach near-zero.

ISAC capabilities represent a transformative paradigm that is attracting attention for its potential to revolutionize services with the integration of communication and environmental sensing within a single infrastructure, thereby enabling a new generation of intelligent services. Today, Wi-Fi technology is particularly the best suited for ISAC, owing to the availability of CSI derived from preambles embedded in every Wi-Fi frame, including beacons. These features ideally link the communication and sensing in Wi-Fi, positioning it as both a current enabler and a key testbed for ISAC applications. Furthermore, the well-established Wi-Fi infrastructure enables

a valuable addition for shaping the design of future wireless standards, such as 6G, where pilot signals are expected to allow comparable sensing in cellular systems such as LTE.

4.1 The Emerging Privacy Concerns in CSI-based Sensing

Despite these advancements offered by CSI-based sensing, they also introduce significant privacy concerns. For example, an attacker can exploit the available CSI to monitor individuals' activities [62], potentially leading to unauthorized access to the information. For instance, a neighbor could easily intercept wireless frames from your home Access Point (AP) and can analyze the CSI data to determine whether you are at home, or your specific activities like walking or sleeping, and other details about your daily routine. An important aspect of this kind of threat is accessibility: because such exercises can be done using readily available devices [63]. The privacy threat is very common and does not only affect highly skilled individuals due to its ease of access. We categorize these threats into two main types: active attacks, where attackers generate Wi-Fi signals using their own devices, thus having full control over the data collection; and passive attacks, where malicious users exploit ongoing transmissions to collect the data [62]. In this work, we specifically focused on the second type of attacks. The focus on passive attacks is important because it means individuals are at risk simply by using their Wi-Fi networks, even if they are not the target of malicious transmissions. This makes the risk of privacy nearly unavoidable without any specific countermeasure. The combination of low-cost COTS tools and passive attack transforms privacy leaking from a theoretical issue into an immediate necessity for the widespread adoption of ISAC.

4.2 Proposed Solution: CSI Obfuscation and Deobfuscation

To address these necessary privacy concerns, a preventive measure is transmitter-side obfuscation. This technique involves intentionally adding distortions into the transmitted Wi-Fi signals to hide the ambient-induced distortions in the CSI that sensing algorithms typically exploit. This can be implemented by pre-filtering time-domain signals with an artificial channel response [64], or by multiplying the modulated Wi-Fi subcarriers by time-varying weights in the frequency domain to generate the obfuscated symbols [65, 66]. While the receiver can still correctly decode the communication data if the same distortion is applied to the entire frame on a per-frame basis; however, the CSI changes randomly over time, making it significantly more challenging to differentiate the effects of the physical channel from those induced by the obfuscation technique itself.

While obfuscation effectively protects privacy, but also disrupts unauthorized sens-

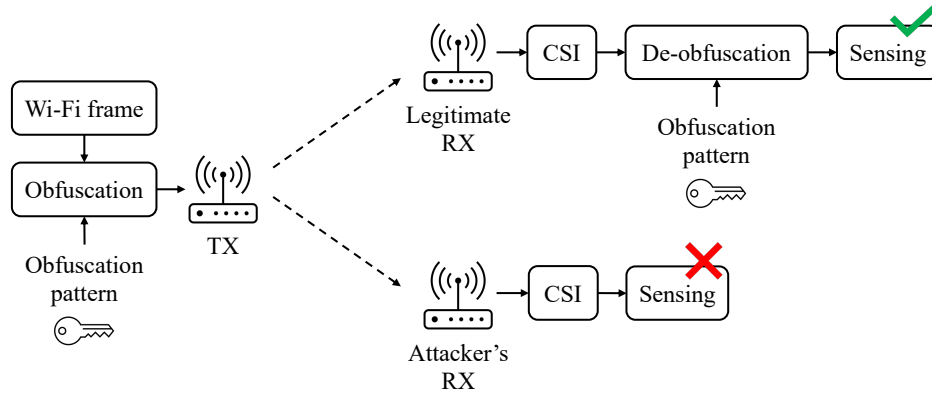


Figure 4.1: High-level obfuscation and de-obfuscation scheme.

ing, and it also inherently hinders legitimate sensing capabilities, limiting the system’s ability to perform authorized tasks within the ISAC infrastructure. Instead, the ultimate goal is to block malicious sensing operations from unauthorized users while ensuring proper functionality for legitimate devices. To overcome this trade-off, in this work we adopt an approach described in Figure 4.1. In particular, if trusted nodes possess the prior knowledge of the pre-distortion applied during transmission, they can accurately compensate for its effects and recover the sensing features of the CSI. Thus, in this context, the obfuscation pattern plays a role that resembles that of a key used to protect the CSI. We refer to this approach as de-obfuscation. Although the concept of de-obfuscation is not entirely novel [67, 68], there is still no evidence of its effectiveness in real-world scenarios. This work directly addresses this research gap by showing that the de-obfuscation can successfully restore sensing capabilities for authorized devices with a real implementation. The security of the de-obfuscation process entirely depends on the confidentiality and unpredictability of this “key.” If an unauthorized entity is able to gain access to the pattern of obfuscation, then the privacy protection is compromised. This suggests that practical implementations would necessitate robust key management protocols, potentially integrating with existing security frameworks for secure distribution of obfuscation parameters. As a case study, we examine a device-free localization problem involving a person inside a room. In particular, we evaluate the localization accuracy when a legitimate node removes CSI obfuscation. The experimental results highlight the feasibility of this approach and offer insights into its practical applicability and limitations.

4.3 Existing Privacy-Preserving Methods in Wireless Sensing

Despite several Wi-Fi sensing solutions have been presented in the literature [15], however, awareness of PHY privacy threats remains limited, with relatively little attention given to the environmental information leakage [62]. One of the early efforts to address this issue includes proposals for relay nodes that introduce dynamic variations in multipath components of a signal, thus interfering with CSI-based sensing [69]. This solution requires an additional device that receives, modifies, and retransmits the wireless signals, making it appear as a natural multipath component. A natural evolution of this approach is the use of Reflective Intelligent Surfaces (RIS). This idea was explored in [70], where the authors used a SDR to simulate the behavior of an Reflective Intelligent Surfaces (RIS) and counter localization. Similarly, and almost at the same time [71], showed that an actual RIS can conceal a moving person inside a room.

These solutions mitigate both passive and active attacks but require additional hardware (a RIS). This introduces significant deployment costs and complexity, potentially limiting their widespread adoption in existing Wi-Fi ecosystems. In contrast, the approach of pre-distorting signals upon transmission addresses only passive attacks, without necessitating any additional infrastructure. This strategy, as shown in [65, 66], is effective for privacy protection in device-free localization. This highlights a crucial design trade-off in privacy solutions: software-defined or the transmitter-side approaches are cost-effective and applicable, while hardware-based methods provide comprehensive protection but at a higher cost. Since the selection of countermeasures often depends on the individual threat model and resource constraints of the deployment environment, making the transmitter-side obfuscation particularly best-suited for scenarios where infrastructure modification is difficult or undesirable.

4.4 The Research Gap: Practical Feasibility of CSI De-obfuscation

The transmission-side obfuscation technique has been considered to be effective for privacy protection in device-free localization; the challenge of restoring valid sensing capabilities has not gotten so much empirical validation. Previous studies [67, 68] have proposed protocols to support de-obfuscation; however, these proposals have lacked formal proof or implementations to demonstrate their practical feasibility. The lack of practical support represents a serious gap in current research. In wireless communication systems, theoretical approaches often overlook the challenges raised by the real-world environments, including hardware limitations, environmental noise, and complex protocol behaviours. As a result, validating the practical feasibility through real-world implementations becomes paramount to prove their reliability and applicability. This work addresses this gap by providing a real implementation

and experimental validation of CSI de-obfuscation.

4.5 Primer on CSI-Based Sensing

The core principle of CSI-based sensing is straightforward: physical objects and environmental features such as walls, objects, and people interact with propagating wireless signals by introducing scattering and reflections. The analysis of these interactions alters the reliable inference of environmental conditions. The CSI serves as a unique fingerprint of the wireless channel, capturing how the environment affects transmitted signals. In the context of modern Wi-Fi, which utilizes OFDM transmissions, including modern Wi-Fi, CSI is crucial for signal equalization and data decoding.

It consists of a set of complex values, one per subcarrier, that measure the channel-introduced distortion.

These complex values are estimated using a prior knowledge of the OFDM preambles in the PHY header. By comparing the known and measured values per subcarrier, the CSI is derived directly. Formally, let $H_c(f, t)$ be the channel frequency response, and $S_t(f, t)$, $S_r(f, t)$ the transmitted and received OFDM spectra, respectively, then:

$$S_r(f, t) = H_c(f, t) S_t(f, t). \quad (4.1)$$

If the receiver possess the knowledge of $S_t(f, t)$, the estimation of $H_c(f, t)$ becomes a direct process.

While both the amplitude and phase components of CSI are theoretically influenced by environmental changes, practical sensing systems primarily rely on amplitude information. Even though phase values theoretically carry useful information for sensing, practical limitations arise from real-world devices, which introduce significant errors into phase values, rendering them unreliable for sensing applications [72]. Thus, the analysis of $|H_c(f, t)|$ makes it possible to collect information on the environment.

CSI-based sensing can be conceptualized as the process of finding a function that maps CSI measurements to environmental information. Given that the mathematical characterization and stochastic properties of this mapping remain an open problem, most sensing systems frequently rely on Artificial Intelligence (AI) algorithms for this purpose [15, 59]. The use of AI implies that CSI sensing is mainly empirical, which makes it vulnerable to distortions (obfuscation) since AI models are sensitive to changes in the distribution of input data. On the other hand, this also suggests that de-obfuscation must return the CSI to a state that is noticeably comparable to the clear CSI for the AI algorithm, rather than exactly the same, which could provide some margin for error.

4.5.1 Analysis on CSI Obfuscation

CSI obfuscation is a strategy designed to mitigate the risk of malicious actors that sense the environment through CSI by intentionally distorting the signal. The objective is to obscure the ambient-induced distortion, which is what sensing algorithms typically exploit. This concept is formalized by introducing an artificial distortion.

$$S_r(f, t) = H_c(f, t) O(f, t) S_t(f, t), \quad (4.2)$$

where $O(f, t)$ is the artificial distortion. From the perspective of the receiver, $O(f, t) H_c(f, t)$ appears as a normal channel response, denoted $H_o(f, t)$, that combines real environmental data with obfuscation effects. This makes it harder to distinguish ambient-induced features in the CSI. This work specifically focuses on a transmitter-side obfuscation system, where the distortion element $O(f, t)$ is applied by multiplying each subcarrier of the OFDM symbols within the Wi-Fi frame before transmission.

For obfuscation to be effective and robust, several design considerations are paramount [29]. Firstly, the obfuscation pattern $O(f, t)$ must evolve randomly over time to effectively mislead sensing algorithms. However, excessive randomness, such as white noise, must be avoided, as attackers might be able to filter it out over extended observations. Secondly, if the distortion is constant within a single frame and is excessively strong, it allows the receiver to still correctly decode the signal. Thirdly, and critically for security, $O(f, t)$ must be designed to mimic a physically realizable channel response and to be non-invertible, preventing attackers, even with extended observations and high computational power, from reconstructing $O(f, t)$ in a reasonable time.

The attackers are not able to reverse the $O(f, t)$ while only authorized users are able to perform a reversible operation, which presents a unique challenge. One way to address this is to observe that, for an attacker, non-invertibility arises either from computational infeasibility or from the absence of the required key. It cannot be inferred by unauthorized parties that are unaware of the particular $O(f, t)$ sequence or the pseudo-random seed that was used to generate it. However, only authorized users have access to this key for producing $O(f, t)$, which allows them to carry out the opposite operation. This difference is very important: the difficulty for an unauthorized party to find $O(f, t)$ or its generation parameters is what gives the obfuscation its strength, not the mathematical complexity of the inverse of $O(f, t)$. This highlights the significance of secure key exchange and synchronization protocols in a real-world system and supports the "key" analogy.

4.5.2 Analysis on CSI De-Obfuscation

While obfuscation effectively conceals CSI to prevent unauthorized sensing, legitimate nodes must retain the ability to extract meaningful channel information for

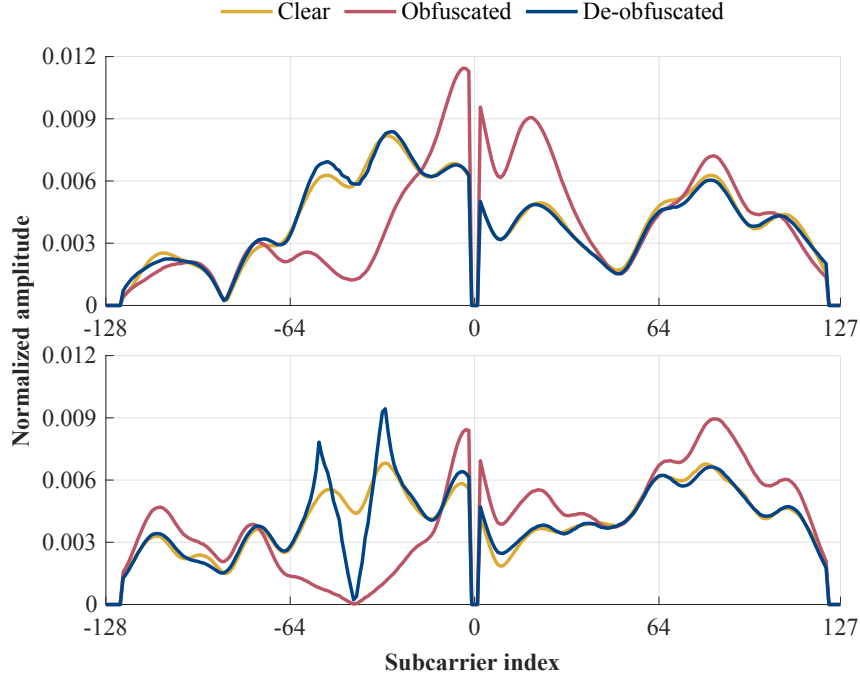


Figure 4.2: Two examples of CSI de-obfuscation. The top plot illustrates a good result that was obtained; the bottom one highlights the error amplification issue, which arises for subcarriers whose mask amplitude approaches zero.

authorized applications. This is achievable if authorized devices have prior knowledge of the obfuscation mask $O(f, t)$, allowing them to remove its effect and recover the original CSI.

The de-obfuscation process can be expressed as:

$$H_d(f, t) = O(f, t)^{-1} H_o(f, t) \quad (4.3)$$

$$= O(f, t)^{-1} H_c(f, t) O(f, t), \quad (4.4)$$

where $H_d(f, t)$ is the estimated CSI after removing the obfuscation factor and should ideally match $H_c(f, t)$, enabling authorized nodes to perform sensing.

The upper plot in Figure 4.2 illustrates an example of effective de-obfuscation, where the de-obfuscated CSI closely matches the clear one, while the lower plot shows a case when the de-obfuscation process is affected by significant errors. We attribute this issue to the assumption made in eq. (4.3), which neglects the possibility of errors in the CSI extraction process.

Let's define $\tilde{H}_c(f, t)$, $\tilde{H}_o(f, t)$, and $\tilde{H}_d(f, t)$ as the clear, obfuscated, and de-obfuscated CSI values respectively. The assumption is that all three terms correspond to the same environmental configuration, meaning they represent the channel response un-

der the same physical conditions. Thus, it is reasonable to assume that:

$$\tilde{H}_c(f, t) = H_c(f, t) + \epsilon_c(f, t) \quad (4.5)$$

$$\begin{aligned} \tilde{H}_o(f, t) &= H_o(f, t) + \epsilon_o(f, t) \\ &= H_c(f, t) O(f, t) + \epsilon_o(f, t) \end{aligned} \quad (4.6)$$

$$\begin{aligned} \tilde{H}_d(f, t) &= O(f, t)^{-1} \tilde{H}_o(f, t) \\ &= O(f, t)^{-1} [H_c(f, t) O(f, t) + \epsilon_o(f, t)] \end{aligned} \quad (4.7)$$

where $\epsilon_c(f, t)$ and $\epsilon_o(f, t)$ denote impairments in CSI introduced by environmental noise and the CSI extraction process.

The de-obfuscation effectiveness is given by the absolute value of the difference between $\tilde{H}_c(f, t)$ and $\tilde{H}_d(f, t)$. After some algebraic manipulation, we obtain:

$$|\tilde{H}_c(f, t) - \tilde{H}_d(f, t)| = |\epsilon_c(f, t) - O(f, t)^{-1} \epsilon_o(f, t)|. \quad (4.8)$$

With this equation, we can understand the issue in Figure 4.2: de-obfuscation can amplify the $\epsilon_o(f, t)$ term if the mask approaches zero, increasing the gap between the clear and de-obfuscated CSI, potentially interfering with sensing algorithms. This suggests a trade-off: limiting the amplitude of the mask may reduce errors, but can also weaken obfuscation.

4.5.3 Towards a Practical De-obfuscation Protocol

A key challenge in designing a practical de-obfuscation system is ensuring that only legitimate nodes can securely access the obfuscation mask $O(f, t)$. We proposed an approach that leverages the synchronization mechanisms inherent in modern Wi-Fi systems, where, specifically, timestamps in beacon frames could be used to coordinate the evolution of the mask. This approach is considered more robust in real-world scenarios than relying solely on frame numbers, which can lose synchronization due to frame drops.

The protocol envisions an initial association phase during which the transmitter and receiver agree on pseudo-random seeds. These seeds would then be used to generate the mask coefficients over time. The distortion can be updated periodically (e.g., every 100 ms), with the interval of change defined during this initial phase. It is important to note that in this preliminary work, we focus on demonstrating the fundamental knowledge of the mask at the receiver, which can restore sensing accuracy for legitimate nodes, without implementing the full, real-time de-obfuscation protocol. This distinction is crucial: while the core technical feasibility is proven, the practical challenges of secure key exchange, robust synchronization, and dynamic mask management in a real-world, large-scale deployment remain open research questions requiring further development.

4.6 Methodology

A thorough experimental methodology was created in order to empirically verify the viability and efficacy of CSI de-obfuscation. This included a particular case study, a thorough hardware and software configuration, the application of different obfuscation masks, and a reliable data processing and neural network framework for localization.

4.6.1 Case Study: Device-Free Localization

To demonstrate the effectiveness of the de-obfuscation method discussed in Section 4.5.2 was evaluated within a device-free localization scenario. This involved a person moving within a room, serving as the environmental change to be sensed. The experiments were conducted in the University building at the Advanced Networking Systems (ANS) laboratory at the University of Brescia. The setup consists of a single transmitter (TX) and two receivers named as RX1 and RX2. During data collection, a participant in the laboratory progressively stood at eight designated pre-defined positions, ensuring a controlled and repeatable environment for localization. Device-free localization is a popular and widely recognized use of CSI sensing, which makes it an appropriate standard for assessing the effects of obfuscation and de-obfuscation. Although localization is a powerful proof-of-concept, the ideas presented here may also apply to other sensing tasks, like identifying human activity; however, additional testing in a variety of settings would increase the findings' generalizability.

4.6.2 Experimental Setup

The experimental setup combined flexible SDR capabilities with COTS Wi-Fi hardware to balance control and realism.

The localization accuracy and obfuscation effectiveness depend on the location of the receiver [66], so we designed the setup accordingly. Each device captures CSI through four antennas spaced at a half-wavelength distance. As explained in section 4.6.4, this configuration provides eight antennas in total, increasing data diversity and improving the robustness of our analysis.

Unlike other approaches that distinguish between legitimate devices and attackers, our setup uses the same equipment to implement both authorized users and potential adversaries. This design choice ensures that the results are directly comparable, with any performance variations attributed solely to the obfuscation system rather than device characteristics or placement.

To evaluate the effectiveness of the de-obfuscation process, we follow these conceptual steps:

1. Examine the performance without obfuscation (clear), which serves as the basis for subsequent comparisons;

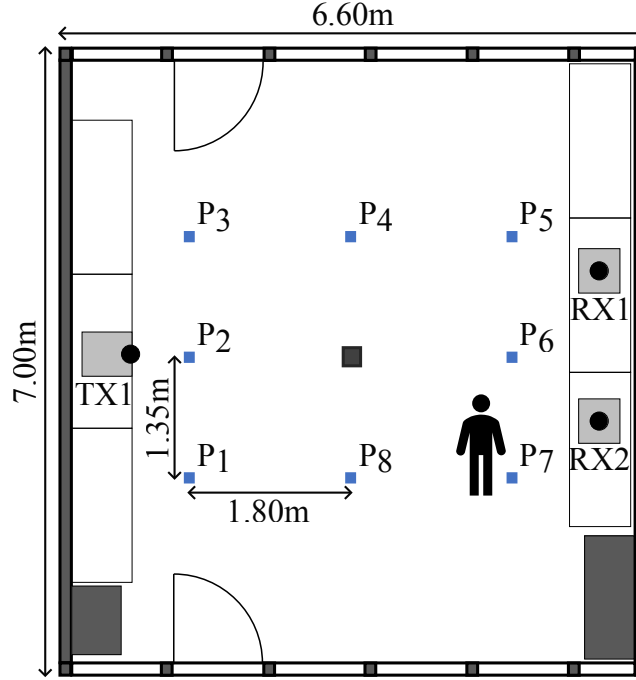


Figure 4.3: Map of the testing scenario in the ANS laboratory at the University of Brescia. A participant sequentially stands at the eight marked positions.

2. Assess the effectiveness of the obfuscation system in preventing unauthorized sensing by adversaries;
3. Remove virtual distortions from the obfuscated CSI and compare the performance with the clear case to determine whether it is possible to restore comparable levels of accuracy.

We use a neural network, presented in Section 4.7.5, to localize the user, with localization accuracy (correct guesses to total guesses ratio) as a performance metric.

4.6.3 Data Collection

The data collection process follows a structured procedure. Before sending Wi-Fi frames, a person makes sure to stand still at one of the eight designated positions within the experimental environment, while CSI samples are continuously recorded. Once we have recorded and collected samples at one position, we then wait for approximately 2 minutes, and we move to the next position, and the same procedure is repeated until data has been collected from all eight predefined spots.

As described in section 4.7, our experimental analysis includes the evaluation of different masking approaches and the impact of multiple realizations, generated using stochastic processes to introduce controlled randomness. For any combination of mask type and stochastic realization, we collect a total of 450 CSI frames at each

position, ensuring sufficient data for robust training and evaluation. The entire data collection campaign is divided into two separate and independent cycles, labeled (P_1 to P_8). The first cycle is exclusively used for training purposes, while the second cycle is reserved for testing, allowing us to validate the generalization capability of our models under consistent yet independently acquired conditions.

4.6.4 Transmitter and receiver setup

The transmitter is an Ettus USRP N300 SDR, which provided precise control over the generation of each Wi-Fi frame. A MATLAB script executed on a connected PC was responsible for crafting and applying the pre-distortion (obfuscation) to the signals. This involved the following:

1. The WLAN Toolbox in MATLAB is used to generate a base-band time-domain signal of a Wi-Fi frame;
2. For each frame, the sequence of OFDM symbols in the time domain is extracted and transmitted in the frequency domain via FFT;
3. The selected obfuscation mask is applied to all the OFDM symbols in the frame;
4. Each obfuscated symbol is retransformed in the time domain via IFFT;
5. The signal is normalized to its highest value to use the entire range of the SDR;
6. The IQ values of the symbols are sent to the SDR for transmission.

On the opposite of the room, that is the receiving side, two Asus RT-AX82U APs running Nexmon [63] were deployed as RX1 and RX2. Each AP was equipped with four distinct antennas, and each of them was capable of independently extracting CSI samples. This configuration provided us with a total of eight antennas, increasing data diversity and strengthening the robustness of the analysis. Since the choice of COTS APs for reception ensures that the results are relevant to real-world Wi-Fi deployments, accounting for the imperfections and characteristics of commercial devices. In order to guarantee direct comparison of findings, authorized users and possible adversaries were implemented using the same equipment, and any performance variations were solely due to the obfuscation system rather than device characteristics or placement.

To prevent signal collisions, especially since the SDR did not run a MAC algorithm, the transmissions were conducted at a central frequency of 5775 MHz (Wi-Fi channel 157), which is not typically used in our university environment. For data collection, 450 Wi-Fi frames were recorded per designated position, for all eight positions. The experiments consisted of two separate cycles of data collection across these eight positions: the first cycle was allocated for training the localization model, and the second for testing its performance.

4.7 Design and Implementation of Obfuscation Masks

We compare in the study two distinct types of obfuscation masks: a sinusoidal-based approach and a reflection-based approach. i.e., two different strategies to derive $O(f, t)$ for different subcarriers and their evolution over time. Each mask introduces variations as a function of the transmitted frame index k , ensuring that its obfuscating effect evolves dynamically over time.

4.7.1 Sinusoidal-based Mask

The sinusoidal mask was generated by superimposing $N = 3$ sine waves. Each component possesses an amplitude $a_n(k)$ and a phase $\phi_n(k)$. The resulting obfuscation function is mathematically expressed as:

$$O_{\sin}(f, k) = \left[1 + \sum_{n=1}^N a_n(k) \sin \left(\frac{n 2\pi}{BW} f + \phi_n(k) \right) \right]_{O_{\min}}^{O_{\max}} \quad (4.9)$$

Here, BW denotes the system bandwidth, and the $[\cdot]_{O_{\min}}^{O_{\max}}$ operator clips the modulo within a defined range of $[0.1, 0.9]$ to prevent excessive distortions that could disrupt communication. Three intensity levels (weak, medium, and strong) were defined based on the range of values allowed for the amplitude parameter. Higher values correspond to stronger distortions. For the weak level, $a_{1,2,3} \in [0.1, 0.2]$; for medium, $a_{1,2,3} \in [0.2, 0.3]$; and for strong, $a_{1,2,3} \in [0.3, 0.4]$. The phase ϕ_k for all levels ranged from $[-\pi, +\pi]$.

Sinusoidal mask		
$N = 3, \alpha = 0.025, \beta = 0.0025, O \in [0.1, 1.9]$		
Weak	$a_{1,2,3} \in [0.1, 0.2]$	$\phi_{1,2,3} \in [-\pi, +\pi]$
Medium	$a_{1,2,3} \in [0.2, 0.3]$	$\phi_{1,2,3} \in [-\pi, +\pi]$
Strong	$a_{1,2,3} \in [0.3, 0.4]$	$\phi_{1,2,3} \in [-\pi, +\pi]$

Table 4.1: Sinusoidal mask parameters at different strengths

4.7.2 Reflection-based Mask

The reflection-based mask was designed to reproduce the effect of objects moving within the environment by introducing virtual reflections. In this case, $N=2$ components were used, each characterized by its intensity $a_n(k)$ and a distance $\delta_n(k)$, representing an extra path length traveled by the signal due to the virtual reflection effect. The obfuscation function is expressed as

$$O_{\text{ref}}(f, k) = \left[1 + \sum_{n=1}^N a_n(k) e^{-j2\pi f \delta_n(k) c^{-1}} \right]_{O_{\min}}^{O_{\max}} \quad (4.10)$$

where c is the speed of light, and O is the clipping range from $[0.1, 1.9]$ was also applied. Similar to the sinusoidal mask, three strength levels were defined. For the weak level, the distance parameters are $a_1 \in [0.2, 0.4]$, $a_2 \in [0.1, 0.2]$, for medium $a_1 \in [0.4, 0.6]$, $a_2 \in [0.2, 0.3]$, and for strong $a_1 \in [0.6, 0.8]$, $a_2 \in [0.2, 0.4]$.

Reflection mask				
$N = 2, \alpha = 0.025, \beta = 0.0025, O \in [0.1, 1.9]$				
Weak	$a_1 \in [0.2, 0.4]$	$a_2 \in [0.1, 0.2]$	$\delta_1 \in [3, 3 + \lambda]^*$	$\delta_2 \in [9, 9 + \lambda]^*$
Medium	$a_1 \in [0.4, 0.6]$	$a_2 \in [0.2, 0.3]$	$\delta_1 \in [3, 3 + \lambda]^*$	$\delta_2 \in [9, 9 + \lambda]^*$
Strong	$a_1 \in [0.6, 0.8]$	$a_2 \in [0.2, 0.4]$	$\delta_1 \in [3, 3 + \lambda]^*$	$\delta_2 \in [9, 9 + \lambda]^*$

* λ denotes the wavelength at the central frequency of the desired channel.

Table 4.2: Reflection mask parameters at different strengths

For both types of distortions, we consider three different intensity levels: weak, medium, and strong. The strength is determined by the range of values allowed for the parameter a_n , which defines the amplitude of any masking component. Higher values correspond to stronger distortions, whereas lower ones to milder perturbations. This distinction allows the evaluation of how different levels of obfuscation impact the system's ability to restore accurate localization information.

4.7.3 Dynamic Evolution of Mask Parameters

For both mask types, the variables defining their functions, i.e., $a_n(k)$, $\phi_n(k)$, and $\delta_n(k)$, were designed to evolve dynamically with respect to the transmitted frame index k .

These variables were generated as realizations of a stochastic Markovian process. Specifically, each follows a Markovian process with an exponential decay filter applied to ensure smooth variations over time. To simplify the notation, we hereafter refer to them generically as $x(k)$. The Markovian behavior can be expressed as:

$$x_{\text{raw}}(k) = \left[x_{\text{raw}}(k-1) + \alpha U_{[-1,1]} \frac{x \Delta}{2} \right]_{x_{\min}}^{x_{\max}} \quad (4.11)$$

where:

- α represents a scaling parameter that controls the intensity of variations;

- $U_{[-1,1]}$ is a uniform random variable in $[-1, 1]$;
- $x_{\Delta} = (x_{\max} - x_{\min})$ is the allowed range for x_{raw} ;
- $[\cdot]_{x_{\min}}^{x_{\max}}$ clips x_{raw} within the bounds $[x_{\min}, x_{\max}]$.

To smooth $x_{\text{raw}}(k)$, the following filter is applied afterward:

$$x(k) = (1 - \beta) \cdot x(k - 1) + \beta \cdot x_{\text{raw}}(k) \quad (4.12)$$

where β controls the smoothing intensity.

Tables 4.1 and 4.2 summarize the parameters for the sinusoidal and reflection masks. Since their generation is stochastic, realizations vary across experiments, leading to performance fluctuations even for the same type and intensity. To ensure statistical robustness, we generate eight independent realizations per mask-intensity combination, thus reducing the influence of any single evolution instance.

4.7.4 Transmission and masking strategy

We split the experimental procedure into two phases: the first phase utilizing sinusoidal masks, followed by the second employing virtual reflection masks. During each phase, for every sequentially generated frame in MATLAB, a clear (unobfuscated) version was transmitted, and this was followed by frames corresponding to every mask strength (weak, medium, strong) and each of the eight random process instances.

This information, which uniquely identifies each CSI sample at the receiver for post-processing, specific information was encoded into the MAC address 3 field: The first 10 hexadecimal digits were used for the cycle number, the 11th for the mask strength, and the 12th for the instance of realization. Consequently, each applied mask was meticulously stored in a data structure, indexed by its cycle number, strength, and instance reference. This systematic storage approach allowed the accurate identification of the distortion applied to each received frame during post-processing, which was important for enabling the de-obfuscation operation. This simple, straightforward approach facilitated a preliminary study of de-obfuscation effectiveness without needing the implementation of a full, complex real-time protocol discussed in Section 4.5.3.

Although the feasibility of de-obfuscation has been explained quite well, the offline nature of this process, where mask information is encoded and saved for post-processing which highlights the future development that still requires addressing the real-time difficulties of mask synchronization and safe key exchange.

4.7.5 The neural network architecture and data processing for localization

To evaluate localization accuracy, a lightweight neural network was employed in the work. The choice of a superficial architecture was intentional, aiming to reduce

parameters and speed up the training process, as the main goal of this work was to manifest the practicability of de-obfuscation rather than to develop advanced AI algorithms for sensing.

a) CSI preconditioning steps In this work the Neural Networks (NN) processed 802.11ac frames transmitted over 80 MHz channels with a single spatial stream. Each raw CSI sample consisted of 256 complex values, one for each subcarrier. However, due to inherent device imperfections in real-world scenarios, phase values often exhibit significant errors, as discussed in [72] analysis, so only the amplitude component of the CSI was utilized.

During pre-processing, the pilot and unused subcarriers were discarded in accordance with the 802.11ac standard, leaving the number of values from 256 to 242. The two outermost subcarriers (the low and high ends of the channel) were also suppressed to ensure the remaining count was a multiple of 5, further reducing the total to 240 values. Finally, groups of 5 adjacent subcarriers were averaged, resulting in a downsampled feature set of 48 values. This downsampling provided a more compact yet representative feature set for the neural network. To standardize the data and improve the convergence of the neural network during training, z-score normalization was applied, ensuring a mean of 0 and a standard deviation of 1 while preserving its original data shape. This step helps improve the convergence of the neural network during training.

b) Neural network design The neural network, developed in MATLAB, featured a shallow architecture optimized for CSI-based classification. The input layer was configured to process the preconditioned, downsampled CSI based samples as a 1D vector of 48 values. This input layer was connected to a fully connected layer comprising 8 neurons, related directly to the eight target localization classes (i.e., the eight distinct positions in the indoor laboratory where the participant sequentially stood one after the other). A softmax layer followed, outputting a probability distribution across all these classes, with the predicted class being the one exhibiting the maximum probability value.

c) Training and testing strategy The network was trained using the Adam optimizer, with cross-entropy loss serving as the objective function. A mini-batch size of 5 was employed, and an initial learning rate of 0.001 was set. Training was performed for 15 epochs, with data shuffled between each epoch to improve generalization and prevent overfitting. Performance was finally evaluated based on classification accuracy, defined as the ratio of correct guesses to total guesses.

A fundamental technique for the chosen work was the thorough separation of training and testing. Training and testing were conducted independently for three distinct scenarios as previously discussed in Section 4.7: clear (without obfuscation), obfuscated, and de-obfuscated. This separation was also applied for each obfuscation pattern (sinusoidal and virtual reflection) and for each realization instance of the

stochastic process. Training of the clear frames and testing it on obfuscated or de-obfuscated frames was explicitly avoided because it would make no sense in a real-world scenario and does not provide any meaningful results (testing is equivalent to a random guess).

This research approach significantly impacts the study’s accuracy, for the validity of the de-obfuscation results, ensuring that the neural network learns to localize specifically from the type of CSI it receives (clear, obfuscated, or de-obfuscated). This implies that for a legitimate sensing system using de-obfuscation, the AI model would need to be trained on de-obfuscated CSI. To mitigate the impact of weight initialization variability on model performance, we trained each model for a total of five times. And the final localization accuracy was computed as the average across these five trained models.

4.8 Experimental results and Discussion

The experimental findings provided strong evidence for the feasibility of CSI de-obfuscation, illustrating the trade-offs between privacy protection and legitimate sensing fidelity. The results which we obtained are shown in Figure 4.4 compactly, using boxplots with the median, 25 and 75 percentiles (box), outliers as single points, and whiskers reach the most distant non-outlier data points.

4.8.1 Baseline localization accuracy

As a foundational benchmark, the localization system’s performance without obfuscation (clear case) was evaluated. In this case, the accuracy proved to be consistently high, with a median correct classification rate of 94.1% and 93.7% for the first test that involves (sinusoidal masks) and for the second involving (virtual reflection masks) tests.

Both cases exhibited limited dispersion in their results, which aligns well with findings from previous studies on CSI-based localization [66]. This higher accuracy supports the idea of CSI-based localization itself, which is a premise that CSI is a powerful sensing modality. The high accuracy further demonstrates how serious concern is the privacy threat is: if CSI can be so accurately useful for localization without needing any countermeasures, then it raises an important question: how can we protect the privacy? Although both scenarios yielded similar median accuracies, the boxplot for sinusoidal masks revealed an outlier. A closer analysis shows that these results were attributable to a specific antenna, possibly in an unfortunate receiving location. This observation suggests that the outlier was a localized hardware/environmental issue rather than a systemic flaw in the localization method itself.

Table 4.3 provides a summary of the localization accuracy results, highlighting the performance across clear, obfuscated, and de-obfuscated scenarios for different mask types and strengths.

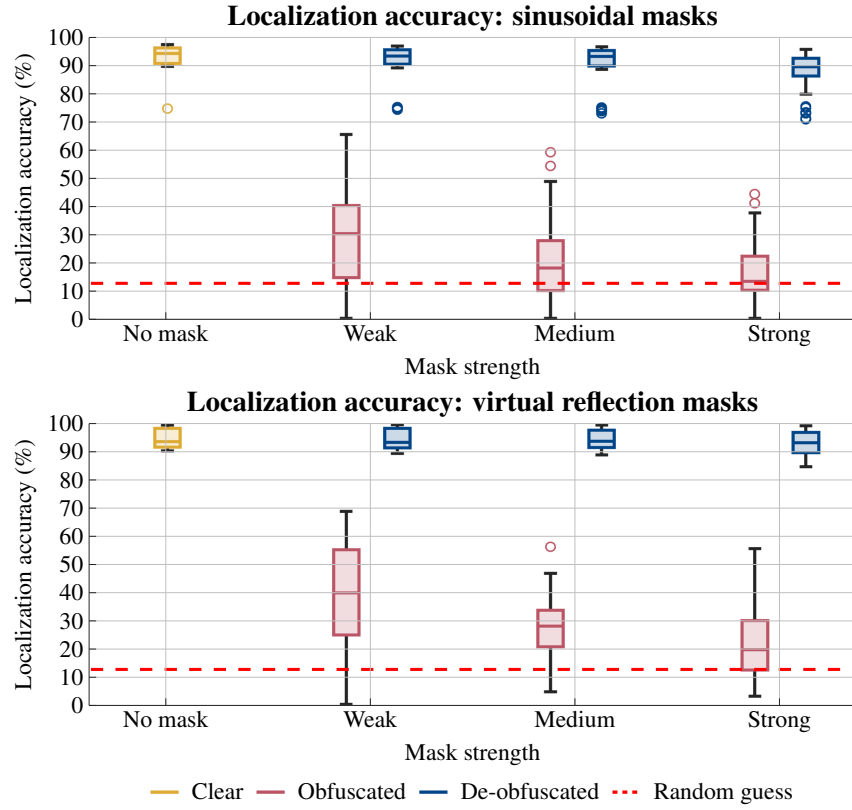


Figure 4.4: Localization accuracy across obfuscation levels. The top plot shows results for the sinusoidal mask, the bottom for the virtual reflection-based one. Data is aggregated across all antennas and multiple instance evolution per obfuscation level.

Mask Type	Strength	Clear Accuracy (%)	Obfuscated Accuracy	De-obfuscated Accuracy	IQR (De-obfuscated)
<i>Sinusoidal Mask</i>					
No mask	–	94.1	N/A	N/A	N/A
Weak	Weak	N/A	Very Low	High	Low
Medium	Medium	N/A	Very Low	High(Slightly Lower-than-Clear)	Medium
Strong	Strong	N/A	Extremely Low	Moderate	High
<i>Virtual Reflection Mask</i>					
No mask	–	93.7	N/A	N/A	N/A
Weak	Weak	N/A	Very Low	High	Low
Medium	Medium	N/A	Very Low	High(Slightly Lower-than-Clear)	Medium
Strong	Strong	N/A	Extremely Low	Moderate	High

Table 4.3: Summary of localization accuracy results under various masking conditions. Clear = no masking; Obfuscated = with mask applied; De-obfuscated = recovered accuracy. IQR: Interquartile Range.

4.8.2 Effectiveness of obfuscation in degrading unauthorized sensing

Next, taking into account the primary goal of obfuscation, which is to reduce the precision of unauthorized sensing. The experimental findings verified that the proposed obfuscation masks successfully reduced the localization system’s accuracy in both sinusoidal and reflection-based scenarios. This demonstrates that they were successful in introducing a significant amount of uncertainty to the CSI measurements, while maintaining privacy.

As expected, a direct relationship between the degree of obfuscation efficacy and different distortion intensities (weak, medium, and strong) and the level of obfuscation effectiveness was observed. Stronger distortions led to lower localization accuracies for the obfuscated signals, provided that the increased obfuscation strength provides greater privacy protection. Furthermore, a comparison of the two masks showed that the sinusoidal mask outperformed the reflection-based mask in terms of lowering localization accuracy, exhibiting a lower median accuracy for unauthorized sensing. This implies that effective privacy protection relies on the type of distortion, not

just its size, and provides information for improving obfuscation strategies in the future.

4.8.3 Performance of de-obfuscation in restoring legitimate sensing

The key finding of this study is the successful restoration of legitimate sensing functionalities through de-obfuscation. The findings clearly demonstrate that localization accuracy was effectively restored to clear-state levels across all strengths comparable to unobfuscated state, across all obfuscation intensities, including weak, medium, and strong. This gives strong evidence that the de-obfuscation approach can reliably reinstate sensing performance for authorized users, regardless of the presence of obfuscation mechanisms.

This shows that sensing and privacy do not have to conflict; a system can be designed to provide robust privacy protection against unauthorized users while maintaining its full functionality for approved applications. This is a critical enabler for the widespread adoption of ISAC in privacy-sensitive environments. It was also observed that the outliers previously identified in the sinusoidal case, which arose from the problematic antenna in the clear condition, persisted in the de-obfuscated results. Therefore, they did not indicate performance degradation caused by the de-obfuscation process itself, as their results remained comparable to those observed in the clear case for that specific antenna. This supports the idea that the original channel information can successfully be recovered using the de-obfuscation process.

4.8.4 Impact of obfuscation strength on de-obfuscation accuracy

While de-obfuscation largely restored accuracy, we also observed that accuracy generally worsens as the obfuscation level increases. Specifically, the median localization accuracy of de-obfuscated results deviated more from the clear state for strong masks compared to weak ones. A similar trend was observed in the dispersion of results, with stronger masks leading to increased variability.

We believe that failure to recover the user’s position mainly stems from the error amplification effect discussed in Section 4.5.2. Figure 4.5 shows that the phenomenon predominantly affects subcarriers with lower mask amplitudes. The figure highlights that large mask amplitudes exhibit results in absolute errors that are smaller compared to those derived from small mask amplitudes. Consequently, this leads to larger de-obfuscation errors and, in turn, reduced performance.

Moreover, just as obfuscation effectiveness varies randomly across antennas, error amplification does not cause a uniform accuracy drop. Although affected subcarriers are consistent for all antennas (since they derive from the same mask structure), their impact depends on whether the errors affect critical portions of the CSI of the specific receiver and neural network model. This observation is further supported by the fact that, when analyzing the per-antenna difference between clear-state and de-obfuscated accuracy for the same mask realization, the maximum observed error reaches 13.5% and 7.2% for the sinusoidal and virtual reflection cases, respectively.

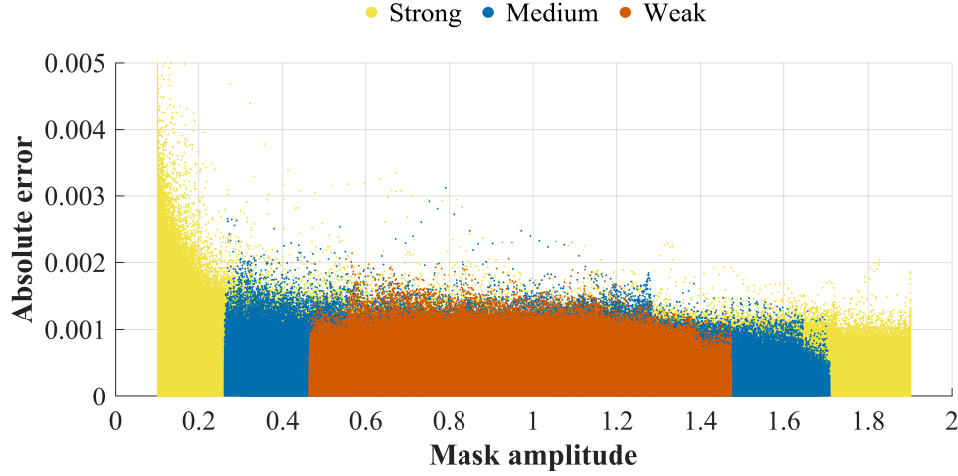


Figure 4.5: Qualitative analysis of the relationship between the mask amplitude and the de-obfuscation absolute error for any single subcarrier. In this figure, we only consider pairs of clear and de-obfuscated CSI extracted from frames with the same sequential number. Data shown are from one antenna and one sinusoidal mask instance; similar trends hold in other cases.

4.9 Summary of key findings

The novelty of this study is associated by showing a significant step forward by demonstrating, for the first time, that it is practically feasible to de-obfuscate the signal at the transmitter side at the legitimate sensing devices. The experimental results unequivocally confirmed that it is possible for authorized users to recover original CSI features, thereby leading to localization accuracy levels that are comparable to those obtained with clear transmitted frames (un-obfuscated CSI). This addresses the basic issue between the privacy problems associated with the usefulness of CSI.

A transparent trade-off was identified: where stronger distortions yielded improved privacy protection, and they make the de-obfuscation process more challenging for legitimate receivers. The fundamental factor contributing to performance degradation in legitimate sensing is attributed to the presence of near-zero amplitude values within the mask coefficients. These "notches" in the obfuscation pattern greatly increase distortions in the recovered CSI, leading to a noticeable decline in sensing fidelity.

Chapter 5

An Extension Toward Low-Power IoT Sensing and Networking

The activities presented in the first part of this thesis, focused on joint communication and sensing, naturally converge toward a distributed system perspective that motivates the work discussed in this final chapter. In particular, the analysis of sensing accuracy as a function of physical-layer parameters—such as bandwidth—highlights how sensing capabilities can be embedded into devices whose primary function is communication, without requiring dedicated sensing infrastructure. This observation enables a paradigm in which sensing is performed locally, close to where data is generated, leveraging ambient wireless traffic and on-device processing to extract meaningful features. Within this context, the adoption of a mesh networking solution based on OpenThread represents a complementary and enabling technology: rather than transmitting raw sensing data over a centralized or wired backhaul, nodes can disseminate pre-processed sensing results through a self-organizing, low-cost mesh network. This architectural choice decouples sensing performance from infrastructure constraints, allowing sensors to be deployed flexibly and opportunistically while relying on the mesh network for resilient and scalable data delivery. As a result, the two research directions addressed in this thesis can be interpreted as components of a unified framework for distributed sensing systems, where physical-layer-aware sensing and infrastructure-less networking jointly contribute to the realization of cost-effective, adaptable, and easily deployable wireless sensing platforms.

5.1 Overview of Thread

Thread, an open-source implementation of OpenThread, is a robust and reliable protocol designed for mesh networking among the IoT nodes, actuators, or sensors. It enables device-to-device and device-to-cloud communication and prevents a single point of failure. Broadening the IoT networks by integrating resource-constrained nodes, such as embedded sensors, over multiple wireless hops, is crucial for the continued development of the future of IoT. Thread enabled IPv6, engineered for low-power IoT devices, enabling efficient communication, networking, and seamless connectivity for sensors or actuator devices. It has some primary variations that differentiate it from other 802.15.4-based protocols, aiming to reduce overall power consumption while maintaining the resilient network performance. Unlike Routing Protocol for Low-Power and Lossy Networks (RPL), Thread offers a unique approach to multi-hop networking, providing simplicity, security, reliability, efficiency, and scalability, which make it suitable for the future Internet. It makes use of IPv6 connectivity and is made up of one or more devices, including End Devices (EDs), Router Eligible End Devices (REED), BR, and Leader. The BR establishes the connection between the IEEE 802.15.4 internal thread network to a non-thread outer network for external connectivity, such as Wi-Fi or Ethernet, as illustrated in Figure 5.1.

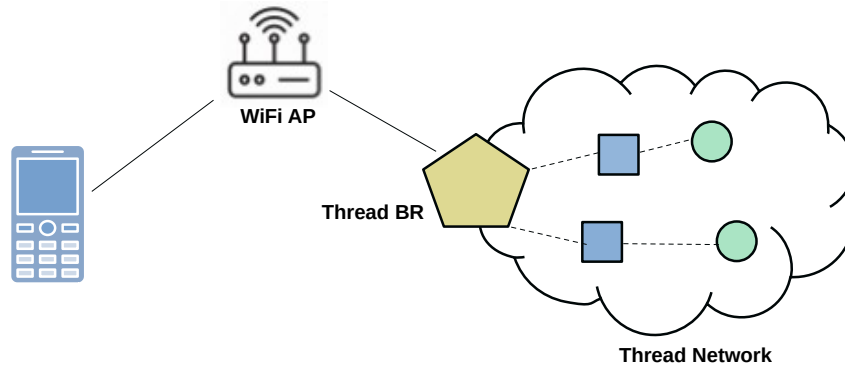


Figure 5.1: System Model: Wireless Mesh Networking via Thread Border Router

With the help of IPv6 addresses, we can differentiate among nodes. Link Local, use the prefix $\text{fe80::}/16$, allowing communication within a single link. Mesh Local with the prefix $\text{fe80::}/8$, where all nodes are accessible across the same Thread network, where global addresses with the prefix $\text{2000::}/3$ can be reached outside of the Thread network [73]. In particular, thread devices running OT firmware may face compatibility and adaptability issues preventing direct communications. As a result, they are forced to partition the network with their own leaders until they are within the range of sensing. A thread network is restricted to a single leader and 32 routers, each of which may be connected to 511 endpoints.

$$N_{\max} = 32 \times 511 + 32 = 16,384 \text{ nodes} \quad (5.1)$$

$N_{\max}$ = Maximum theoretical network size

Thread [74] solves several issues with wireless sensor networks and is made to meet the needs of short-range, low-power, and low-data applications, such as home and building automation, with features like end-to-end encryption, low battery consumption, and eliminating the traditional single point failure. Through a gateway known as a BR, which offers access via WLAN, the Thread IoT network can be linked to the global Internet[51]. Thread provides full support for UDP and Internet Control Message Protocol version 6 (ICMPv6) at the transport layer. Thus, application-layer protocols include Network Time Protocol (NTP), Domain Name System (DNS), and CoAP. At the PHY and MAC, Thread relies on IEEE 802.15.4 radio technology, which operates in the 2.4 GHz frequency band with a data rate of 250 kbps. Consequently, an IEEE 802.15.4 network's framework is followed by a Thread implementation [75]. The IEEE 802.15.4 standard includes AES encryption as a built-in feature to assure communication security. A pre-shared network key is required for authentication before new nodes can join the network.[76]. Thread [73] utilizes a set of sub-protocols referred to as commissioning protocol (MeshCoP), which involves assigning one device the role of Commissioner and another the role of Joiner to facilitate secure authentication. MeshCop that uses DTLS consists of three main components: the Joiner (it manages a secure onboarding for a new node), Commissioner (which handles the control of admission), and Thread management protocol (which facilitates overall network management tasks during commissioning)[77].

5.1.1 Device Roles and Types

The Thread is capable of adopting many device roles and types depending on the configurations, shown in Figure 5.2. Every Thread node can function as Minimal Thread Device (MTD) or a Full Thread Device (FTD), based on its capabilities and role within the network.

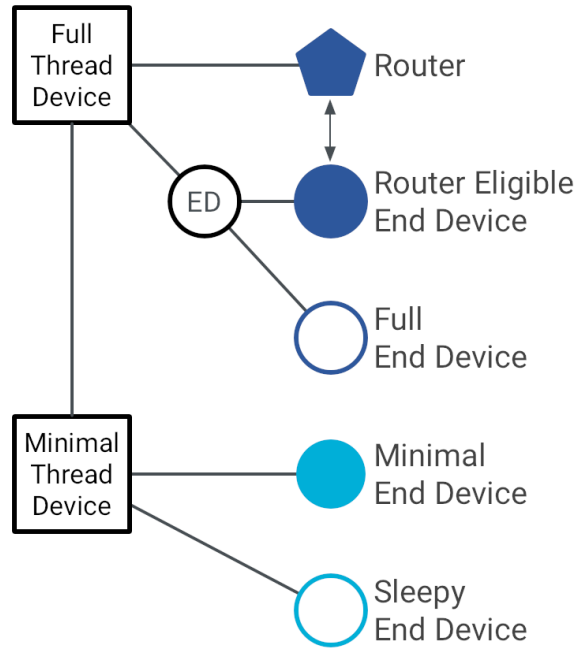


Figure 5.2: Roles of Devices in a Thread Mesh Network

A FTD can keep its radios always active, managing multicast addresses for all routers, and ensures the IPv6 connectivity. FTD can elevate itself to a router or a REED. In contrast, a Full End Device (FED) can not transition into a router. However, a REED has the suitability to change its state to a router due to its eligibility. A minimal thread device routes all communication to its parent instead of participating in the all-router multicast address. MTDs are categorized into two.

Minimal End Device (MED) — keeps its transceiver continuously on, does not require polling for messages from its parent.

Sleepy End Device (SED), in other words, (child) — disabled most of the time, but wakes up on occasions to look up messages from its parent.

The Thread Leader is a key router that oversees the network's routing operations. It is chosen automatically and determines which nodes are eligible to become Thread Routers. Additionally, it is responsible for assigning network credentials to both routers and EDs.

5.1.2 Thread Network Stack

The performance of the Thread network operates under a multi-level constraint framework of its protocol stack, as illustrated in Figure 5.3.

- PHY and MAC Layer (IEEE 802.15.4): Thread fundamentally operates on

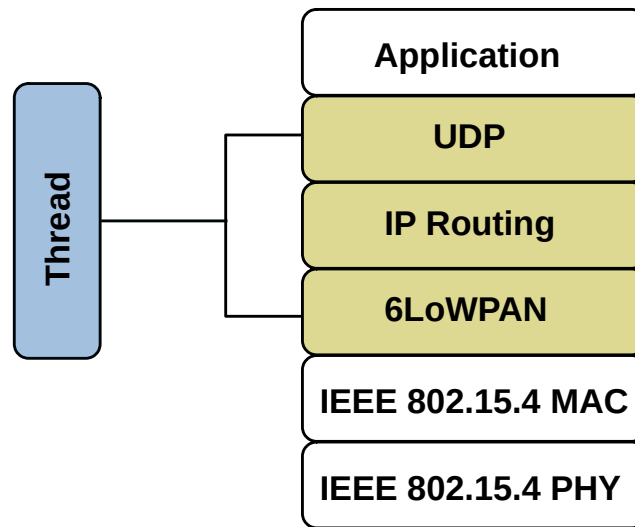


Figure 5.3: Thread Stack

the IEEE 802.15.4 standard, which specifies the PHY and MAC layers. The standard regulates operation primarily in the 2.4 GHz ISM band, which is also utilized by Wi-Fi (802.11), that is the primary source of external interference. The 802.15.4 protocol is limited by a relatively low data rate of 250 kbps and a fixed maximum frame size (MPDU) of 127 bytes.

- (6LoWPAN): The IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) layer is required to support large IPv6 packets over IEEE 802.15.4 networks due to limited maximum frame size of underlying PHY layer. An IEEE 802.15.4 link offers a maximum PHY frame size of 127 bytes, of which approximately 81 bytes remain available for payload after accounting for MAC headers and optional link-layer security overhead, as specified by the Internet Engineering Task Force (IETF) 6LoWPAN standard specifications [78]. To overcome this constraint, this layer provides fragmentation and reassembly services in addition to the header compression. This layer imposes a significant design limitation: the maximum application payload that can be transferred without requiring 6LoWPAN fragmentation is strictly limited to 63 bytes. Any application data exceeding this threshold must be divided into segments.
- Thread uses a mesh-based routing design at the routing layer that incorporates techniques inspired by the RPL and is closely aligned with IPv6 concepts. The Multicast Listener Extension (MLE) protocol, which enables adjacent nodes to share link quality information and preserve routing links, is principally responsible for path establishment and maintenance. Thread is a fully IPv6-compliant protocol that utilizes DHCPv6 to assign router addresses and supports IPv6 addressing. Compared to IPv4, IPv6

packets have a much bigger address space since they have a 40-byte header with 128-bit address fields. Routing tables maintain routers' mesh-local IPv6 addresses, guaranteeing constant connectivity and the availability of numerous forwarding paths. To minimize control overhead and enable the network to adjust to topology changes, Thread uses a distance-vector routing technique that effectively distributes routing information across nodes [51].

5.2 Methodology

The work presented in this study is based on OpenThread 1.2, the open-source implementation of the Thread protocol. This version introduces several enhancements focused on scalability and network density, making it particularly suitable for large-scale building automation.

A Thread mesh network is created, consisting of 16 nodes, one acts as the network Leader and operates as an OpenThread Border Router (OTBR). This OTBR is implemented using a Raspberry Pi running the Thread stack, integrated with a Nordic Development kit (nRF52833) configured as a Radio Co-Processor, functioning as an IEEE 802.15.4 transceiver. And the remaining 15 nodes functioning as FTDs resulting in a network where every node operates as an FTD described in section 5.1.1). In this way, the Thread stack will run on the Raspberry Pi, and the Dongle will act as an IEEE 802.15.4 transceiver. The Raspberry Pi host needs to run two services specifically OTBR-agent and OTBR-web, while the Nordic Dongles handle the radio communication. Since Thread is a mesh protocol designed for redundancy and self-healing, an important part of this work involves deploying the Thread nodes in the offices of the university building and letting them create the natural mesh topology, which allows the devices to communicate in a fully connected mesh setup. This method enables us to perform a precise analysis of the overall cost associated with routing, channel access, and 6LoWPAN fragmentation as the communication path length is intentionally maximized with increasing hop counts to essentially study the known performance degradation of IEEE 802.15.4-based mesh protocols with increasing hop counts.

5.2.1 Experimental Setup

To access the operational considerations and latency distribution characteristics of Thread Mesh Network, an accurate experimental methodology was implemented within an active university environment. The reliability and the latency of the Thread network are highly dependent on the physical environment in which it is deployed; therefore, a total of 16 Thread devices were carefully distributed across faculty offices as shown in Figure 5.4, making a consistent inter-node distance of approximately 10 meters. This spatial configuration was chosen to design a dense, real-world office environment rather than a fixed lab setup. This study successfully isolates the performance variables associated with multi-hop mesh topologies and

temporal interference patterns.

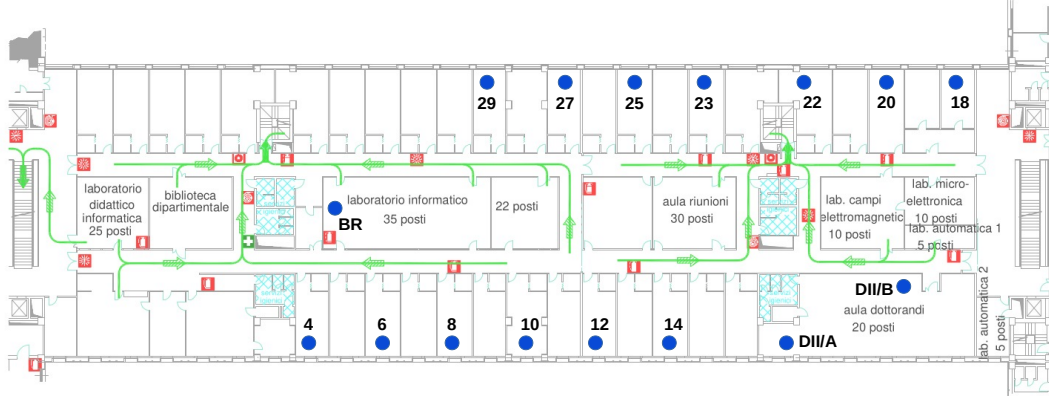


Figure 5.4: Map of the testing scenario in the Department of Information Engineering, First Floor. Blue dots represent the devices, and the number corresponds to the office location.

5.2.2 Experimental Infrastructure and Architecture

The experimental framework was organized into a four-layer architecture, ensuring remote login into the Border Router, network operations, and statistical analysis as illustrated in Figure 5.5.

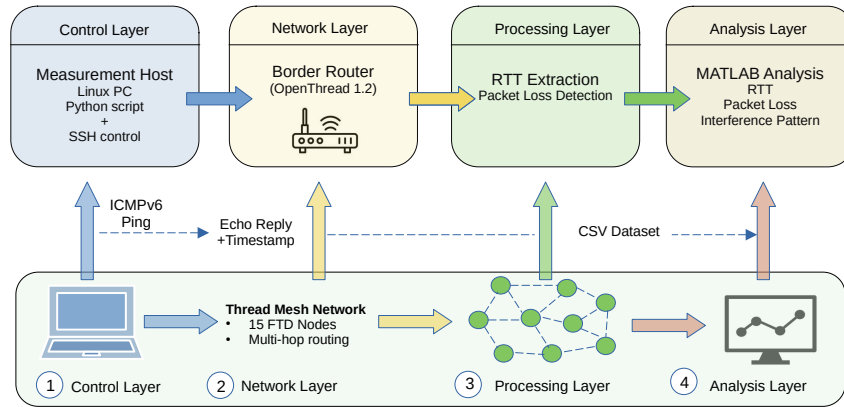


Figure 5.5: Experimental framework organized into a four-layer architecture.

- **Control Layer:** This layer served as the organizer of the experiment. A Linux-based measurement host utilized Python scripts to initiate ICMPv6 echo requests through SSH control. The scripts were designed to target specific nodes at defined intervals, simulating real-world sensing traffic while recording high-resolution timestamps for Round Trip Time (RTT) calculation.

- **Network Layer:** The physical mesh network consisted of 15 nRF52840-based nodes and one nRF52833-based Border Router. The BR acted as the bridge between the infrastructure Ethernet/Wi-Fi network and the low-power 802.15.4 mesh.
- **Processing Layer:** Following the conclusion of each trial, the processing layer performed automated RTT extraction and packet loss detection. This involved parsing the capture files generated by the control layer to match echo requests with their corresponding replies, thereby identifying timeouts and sequence discontinuities.
- **Analysis Layer:** The final stage utilized MATLAB to perform the analysis on the resulting CSV datasets. This included the generation of Cumulative Distribution Functions (CDFs) to visualize latency spread and the calculation of packet success rates across varying environmental conditions.

5.3 Hardware and Software Implementation

5.3.1 Core Network Hardware

The work relies on the Nordic Semiconductor (nRF54840) System-on-Chip (SoC) hardware, serving as the primary Thread device. The particular SoC is chosen for its affordability, low-power consumption, and integration of 2.4 GHz radio, which fully supports the IEEE 802.15.4 communication protocol, and is also the foundation of PHY and MAC for the Thread protocol. In addition to the USB dongles, the setup incorporates one nRF52833 development kit connected to a small Linux-based computer (Raspberry Pi device) installed OTBR to activate the web interface and to visualize the network topology on the web. The remote capabilities of these small Linux computers (Raspberry Pis) allow the nRF hardware to remotely flash, configure, and execute network performance tests, and can be monitored directly via serial interfaces. This integration enables automated deployment of Thread firmware as well as controlled execution of multi-hop network performance tests across the entire mesh topology.

Feature	nRF52840 (Mesh Node)	nRF52833 (Border Router)
Processor	64 MHz ARM Cortex-M4 (FPU)	64 MHz ARM Cortex-M4 (FPU)
Flash / RAM	1 MB / 256 KB	512 KB / 128 KB
802.15.4 Sensitivity	-100 dBm	-100 dBm
Max TX Power	+8 dBm	+8 dBm
Hardware Security	CryptoCell 310 (AES-128)	128-bit AES/ECB/CCM
Protocol Support	Thread, Zigbee, BLE, 2.4GHz	Thread, Zigbee, BLE, 2.4GHz

Table 5.1: Key Hardware Features of the Mesh Nodes and Border Router

5.3.2 OpenThread Firmware Configurations

The OT source code is built with specific compilation flags, detailed in the deployment of the automated script outlined in this work, to tailor the firmware for the experimental objectives:

The main flashing command is:

```
-DOT_BOOTLOADER=USB -DOT_THREAD_VERSION=1.2
-DOT_MAC_FILTER=ON -DOT_APP_CLI=ON -DOT_FTD=ON
-DOT_MTD=OFF -DOT_APP_NCP=OFF -DOT_APP_RCP=OFF
-DOT_RCP=OFF
```

- **Thread Version 1.2:** The firmware is compiled with `-DOT_THREAD_VERSION=1.2`, enabling the latest features of the Thread standard.
- **Full Thread Devices:** All of the 16 devices are compiled as FTD (`-DOT_FTD=ON` and `-DOT_MTD=OFF`), making them eligible to become Routers and participate fully in the mesh routing and forwarding process. The experiment specifically deploys a network consisting solely of Router-eligible devices to maximize the integrity of the routing path.

5.4 Connectivity and RTT Measurement

The network's stability and latency performance are estimated using the standard ICMPv6 Ping utility, which is executed through the CLI interface on the two end-point devices.

- **Stability check:** An initial ping loop verifies the stable connectivity between the two end devices, ensuring the multi-hop path between the nodes.
- **Multi-Hop RTT Analysis:** The automated script uses the `ping6` command to send N ICMPv6 data packets between the two end devices, and also between the intermediate dongles. This measures the RTT and the Packet Loss Rate (PLR) as a function of the hop count. RTT in OT can vary widely, from 10 ms in single-hop scenarios to potentially over 100 ms in multi-hop paths, particularly under real-world interference.
- **Impact of Hop Count:** Since the topology is a mesh, RTT is expected to increase as the hop count increases, driven by the overhead of the CSMA/CA mechanism at the 802.15.4 MAC layer.

5.4.1 UDP Throughput Measurement

Throughput is measured using custom UDP client/server applications (`udpperf6` and `udpserver6`) for various payload sizes between the various end-points in the

mesh network. UDP is the recommended transport protocol for many constrained Thread applications.

- **Test Parameters:** In this work, throughput is measured across various payload sizes (PERFLENGTH) of 50, 100, 200, 300, 400, 500 bytes running for a duration of 40 seconds (PERFDURATION).
- **Packet Fragmentation Analysis:** The selection of these packet sizes directly targets the 6LoWPAN adaptation layer. The 802.15.4 PHY layer limits the maximum packet size to 127 bytes. Given the IPv6 and UDP header overhead, the effective application payload capacity for a single 802.15.4 frame is typically around 80 to 100 bytes (depending on header compression).

5.5 Experimental Considerations: Interference and Multi-Hop Overhead

The deployment of Thread networks within a building introduces significant challenges, providing a realistic test bed for industrial and smart-building applications.

5.5.1 The Impact of Environmental Interference

As the nRF52840 devices also operate in the same unlicensed 2.4 GHz Industrial, Scientific and Medical (ISM) band, the network is exposed to interference from co-located wireless technologies, primarily Wi-Fi. Prior research in similar indoor office environments shows that co-located IEEE 802.11 (Wi-Fi) interference significantly increases packet loss and RTT in IEEE 802.15.4 (Zigbee) networks by disturbing MAC layer operations [79]. Detailed reviews of cross-technology interference in the ISM band suggest that such interferences introduce packet loss, retransmissions, where latency jumps from below 10% to as high as 90%, particularly for low-power networks like IEEE 802.15.4 when operating alongside high-power Wi-Fi traffic [80].

5.5.2 Multi-Hop Performance Degradation

The mesh topology, with up to 16 hops, is a purposeful stress test of the Thread protocol's routing efficiency. While Thread is based on IPv6 routing (which may use the Routing Protocol for RPL, the latency accumulates primarily due to the repeated operations required at the 802.15.4 MAC layer at each hop. The cumulative effect of the following operations is maximized across the full chain:

- In multi-hop 802.15.4 networks such as those used by OT, each router must suspend its transmission until the wireless medium is clear, due to the CSMA/CA mechanism. This necessary backoff period increases along multi-hop paths, especially under dense and high interference conditions. Additional delay is introduced at every forwarding node because routers must perform routing-table lookups, process metadata, and re-encapsulate packets before sending them to

the next hop, which increases end-to-end latency in dense or environmentally noisy deployments [81][82].

- Furthermore, when larger IPv6/UDP datagrams exceed the IEEE 802.15.4 frame size, 6LoWPAN fragmentation is required. In route-over designs such as those used by Thread, each hop must receive, buffer, and reassemble fragments before forwarding them, which greatly increases delay and the likelihood of packet loss as the hop count grows significantly. Previous research demonstrated that the overhead of fragmentation becomes increasingly problematic in lossy or interference-heavy scenarios, as nodes must track multiple fragment states while competing for limited memory and link capacity [83][84].

The planned experimental evaluation will therefore yield practical insights into how reliability and efficiency degrade in OT multi-hop routes when both hop distance and channel interference intensify. These empirical results will help clarify the operational limits of Thread-based IoT networks under realistic environmental scenarios.

5.6 Empirical Results

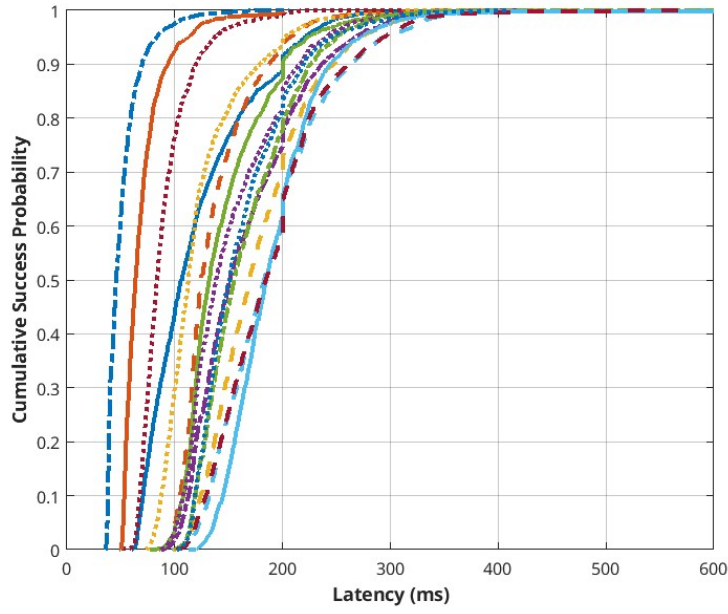
To establish a baseline for Thread mesh performance, the first experiment was conducted on non-working days (weekends). This phase aimed to characterize the network in a "quiet" radio environment with minimal human presence and low Wi-Fi activity. And the second phase of experiments was conducted during regular working days, during which the network was exposed to a higher level of ambient noise and interference associated with a fully occupied office environment.

5.6.1 RTT Performance in Controlled Environments

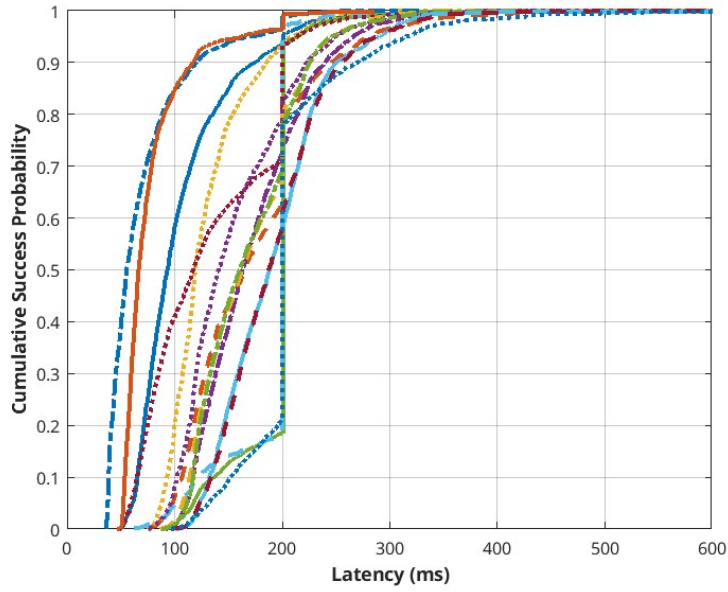
The results shown in Figure 5.6(a) & (b), which comprised of 37,583 total ICMPv6 pings in a (a) non-working scenario and 35824 ICMPv6 respectively, during (b) regular working days, demonstrated the exceptional stability of the Thread protocol under controlled conditions. The overall success rate was measured at 97.35%, with a mean RTT across all devices of 141.37 milliseconds in the first phase of the non-working scenario and 83.56% overall success with a mean RTT of 148.07 in a regular working environment, respectively.

The latency distribution, visualized through Cumulative Success Probability (CSP) charts, showed a high degree of predictability. For the best-performing device, DII/4, the RTT was exceptionally low, averaging only 51.05 ms. The worst-performing device, DII/18, still maintained a respectable mean RTT of 190.70 ms, which is well within the acceptable limits for most industrial sensing applications.

The baseline data verifies that in the absence of external stressors, the OpenThread 1.2 stack efficiently handles multi-hop routing and 6LoWPAN fragmentation with minimal overhead. The RTT which is observed is largely a function of the number of hops, and the CSMA/CA backoff intervals inherent in the 802.15.4 standard [48].



(a) Non-Working Days



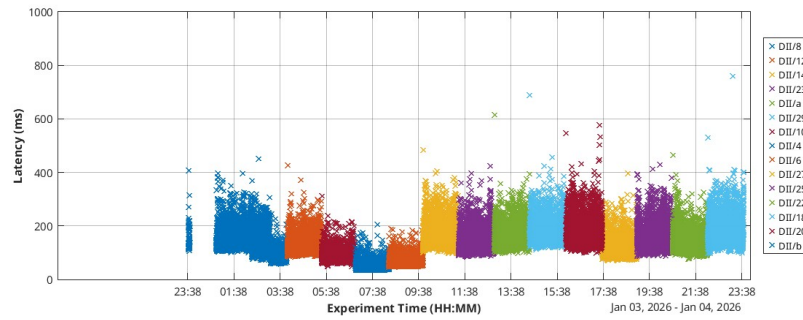
(b) Regular Working Days

Figure 5.6: Comparison of RTT results for different deployment scenarios

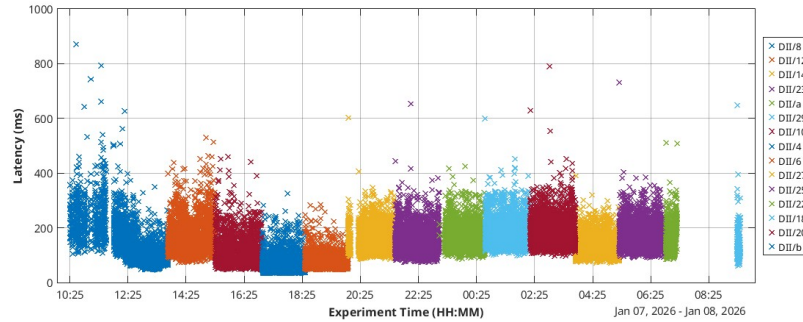
5.6.2 Impact of Interference and Human Presence

The primary source of performance degradation on regular working days is the presence of interference from the department's Wi-Fi infrastructure and personal electronic devices. Wi-Fi (IEEE 802.11) typically transmit signals at significantly higher power levels (up to 20 dBm) compared to Thread's (max 8 dBm) [85]. This power imbalance, combined with the wider bandwidths of Wi-Fi channels, (22 MHz for 802.11b/g compared with 2 MHz for 802.15.4), creates a "hidden node" issue where Thread nodes might not be able to initiate a particular Wi-Fi access points, Clear Channel Assessment (CCA) which might lead to frequent packet collisions [86].

Experimental results showed a significant decrease in the overall success rate to 83.56%, a drop of about 14% from the baseline can be seen in Table 5.2. Although the mean RTT increased slightly to 148.07 ms, this average masks the significant increase in jitter and high-latency outliers. Interference results for the second phase of regular working days showed a series of dense latency "bursts" during typical office hours (09 : 45 – 18 : 00), which can be seen in Figure 5.7(b) correlating perfectly with the arrival and activity of staff and students.



(a) Non-Working Days



(b) Regular Working Days

Figure 5.7: Comparison of Interference for different deployment scenarios

Metric	Non-working Days	Regular Working Days	Delta
Total Success Rate	97.35%	83.56%	-13.79%
Mean RTT (avg)	141.37 ms	148.07 ms	+6.70 ms
Best Device RTT	51.05 ms (DII/4)	66.99 ms (DII/4)	+15.94 ms
Worst Device RTT	190.70 ms (DII/18)	218.95 ms (DII/b)	+28.25 ms

Table 5.2: Comparative Analysis between Non-Working and Regular Working Days

5.7 Key Findings

The experimental analysis conducted at the University of Brescia Engineering building reveals that, despite being a robust Thread protocol, it's still vulnerable to the complex interference and physical barriers present in modern office settings. The transition from non-working to regular working days resulted in a measurable decrease in network reliability, with packet success rates falling to 83.56% and latency distributions becoming significantly more unpredictable.

The study demonstrated that the performance of a Thread Network is highly dependent on the hierarchical structure and the number of hops. Nodes much farther from the originator of data packets suffer the impact of interference-induced delays and packet loss. To maximize the performance of Thread in Industrial and academic settings, coexistence techniques and deliberate frequency planning must take into consideration to mitigate the effects of high power Wi-Fi networks that share the same spectrum.

Chapter 6

Conclusions

This doctoral dissertation has investigated the dual role of modern wireless networks as both communication and sensing platforms, with particular attention on CSI-based sensing, localization performance, and privacy protection. The work was driven by the fast-paced evolution of IEEE 802.11 wireless standards toward Wi-Fi 7 (IEEE 802.11be), which introduces wider bandwidths and spectral resolution, and by the growing need to cross-functional alignment of advanced sensing capabilities with user privacy at the physical layer. In addition, the thesis explored the applicability of CSI-inspired concepts in low-power mesh networking environments, broadening the scope beyond traditional Wi-Fi deployments.

The first major contribution of this thesis concerns the empirical evaluation of CSI-based device-free localization using next-generation Wi-Fi. By developing an open and flexible Software-Defined Radio (SDR) framework capable of emulating IEEE 802.11be transmissions up to 320 MHz. This contribution offers an innovative analysis that experimentally shows a strong correlation between the bandwidth of the Wi-Fi signal and the accuracy of device-free positioning systems. The study highlights the importance of the performance improvements achievable with IEEE 802.11be's wider OFDM capabilities with an increased channel width. An important contribution of the work is the development of an open-source release of a custom SDR framework, which fills a necessary gap in available tools for the research community, allowing for emphasizing different aspects of future research in 802.11be CSI sensing. The findings also demonstrated that IEEE 802.11be's CSI contributes significantly when training data is limited, because of the rich information present per sample, and that collecting CSI over longer durations, even with the same number of samples, is beneficial. Future work should investigate beyond simple device-free positioning to other CSI-based sensing algorithms and applications (for example, activity and gesture recognition) to confirm whether i) bandwidth does influence sensing accuracy in other scenarios or ii) some classes of algorithms are more sensitive than others to the bandwidth. We believe that alternative ways to explore the time correlation

of CSI is also recommended. Broadening the scope of work should include MIMO and multi-spatial stream configurations, which we did not consider in this study, would deliver a more generalized picture of 802.11be sensing capabilities. Further, validation of the results in different propagation scenarios should therefore be carried out in the actual 6 GHz band assigned to IEEE 802.11be, given the limitations of the current SDR configuration. Lastly, the practical usefulness of this research depends on testing the developed framework and validating the results in more complex, dynamic, and varied real-world scenarios outside of controlled laboratory settings.

The second core contribution addressed the privacy risks inherent in CSI-based sensing. While CSI enables fine-grained and device-free monitoring, it also exposes users to unauthorized inference of presence, motion, and activities. To address this challenge, the thesis proposed and experimentally validated a practical framework for CSI obfuscation and de-obfuscation at the physical layer. This study fills an important gap in the current body of knowledge by showcasing practical validation, through a real-world implementation and performing an extensive amount of experiments, for the reversibility of the obfuscation process. This evidence is a tremendous step towards integrating secure CSI-based sensing techniques into a wide range of ISAC world. The successful implementation of de-obfuscation simply means that ISAC systems can be designed to be powerful enough for legitimate sensing, in addition to helping us with robust privacy-preserving techniques against any unauthorized malicious users.

Enabling Wi-Fi sensing to operate in parallel with the privacy protection concern is essential for the broader adoption of ISAC technologies, ensuring that privacy-related concerns do not become obstacles to innovation in sensing-driven applications. Moreover, the findings also provide valuable insights that direct future development of obfuscation systems, particularly in defining the desirable characteristics of the obfuscation mask itself. The identification of the "notch" issue and its impact on how de-obfuscation accuracy offers a clear path for creating more sophisticated mask generation strategies that strike a balance between strong privacy and high de-obfuscation fidelity.

This work demonstrates, for the first time, the feasibility of de-obfuscation at legitimate sensing devices of signals obfuscated at the transmitter. Obfuscation methods and analysis can significantly improve accuracy and privacy, but a more comprehensive analysis is needed to thoroughly evaluate the impact of the error amplification phenomenon across a wider range of obfuscation strategies and for diverse sensing tasks beyond localization. Experimental results confirm that it is possible to recover CSI features for accurate sensing, achieving localization accuracy close to sensing with clear CSI. Moreover, in our experiments using two types of obfuscation at different intensities, we verify that stronger distortions indeed offer better privacy, but on the downside, they make de-obfuscation harder.

In conclusion, future work fills a gap in the state-of-the-art by demonstrating with an implementation and experiments for the reversibility of the obfuscation process.

According to the analysis, significant degradation in performance was observed in legitimate sensing. It is recognized that the current experimental setup did not fully implement the practicability of the de-obfuscation protocol, required to demonstrate its effective feasibility in real-world scenarios such as real-time mask synchronization and secure key exchange mechanisms. Therefore, a crucial next step involves addressing these engineering challenges to transition from a proof-of-concept to a truly deployable system. This includes integrating secure CSI-based sensing techniques into the ISAC landscape. It also provides valuable insights to improve the design of obfuscation systems, particularly the characteristics of the mask. We plan to explore these further in future research, collecting more data with several obfuscation strategies to proceed with a statistical characterization of these errors and their effects on sensing.

The work in Chapter 5 offered insights into the discussion of ISAC to low-power mesh networking scenarios, by experimentally analyzing Thread-based IEEE 802.15.4 networks, evaluating its connectivity, latency, and multi-hop performance under real interference and deployment conditions. While Thread does not expose CSI with the same granularity as Wi-Fi, the study demonstrated that principles driven by the CSI-based sensing, such as sensitivity to environmental changes and multi-hop performance degradation, remain relevant in low-power IoT networks. This exploration lays the groundwork for future ISAC perspectives that extend beyond high-throughput Wi-Fi systems to energy-constrained, low-power, and low data-rate distributed IoT deployments.

Overall, the findings of this thesis show that sensing and communication should be regarded as complementary functionalities rather than conflicting goals in modern wireless systems. Through physical-layer design, it is feasible to improve sensing performance while preserving user privacy and maintaining reliable communication. The developed SDR framework, empirical analyses, and privacy-preserving mechanisms provide valuable tools and insights for both the research community and system designers.

List of Figures

2.1	CSI changes as the target moves from one place to another.	13
2.2	Block Diagram of OFDM transceiver[23]	16
2.3	IEEE 802.11 Architecture[35]	21
2.4	IEEE 802.11 PHY and MAC Layers	22
3.1	Illustration of the procedure used to split a 320-MHz signal generated by MATLAB into two halves (each of 160 MHz) that are compatible with the SDR front end. Each OFDM symbol from the original signal at 320 MHz is processed in the frequency domain to create the corresponding copies and generate the two signals carrying the bottom and top parts of the original spectrum. Here we emphasise the process for symbol s_4	29
3.2	Visualization of the relation between standard Wi-Fi channels and naming scheme used in the experiments for each bandwidth.	31
3.3	Architecture of the neural network for the positioning task. All the hidden layers use a ReLU activation function.	32
3.4	Layout of the experimental setup.	33
3.5	Performance comparison for different Wi-Fi bandwidths using 802.11ac and 802.11be frames. Dots indicate average results over 10 repetitions; vertical bars represent standard deviation. Both training and testing are done, collecting 800 CSI per position. Training and testing experiments are separated by at least 10 minutes.	36
3.6	Performance comparison when training the localization model with only 200 samples per position.	37
3.7	Performance comparison when training the localization model with only 25 CSI per position.	38
3.8	Confusion matrix obtained by training the positioning model with 40-MHz 802.11ac frames. Only 200 training CSI samples have been used, distributed equally over the entire time frame of the experiment of 8 seconds.	39

3.9	Confusion matrix obtained by training the positioning model with 40-MHz 802.11ac frames. Only 200 training CSI samples have been used, restricted only at the beginning of the experiment lasting for only 2 seconds.	39
3.10	IEEE 802.11-be Overall Accuracy Results	41
3.11	IEEE 802.11-ac Overall Accuracy Results	41
4.1	High-level obfuscation and de-obfuscation scheme.	45
4.2	Two examples of CSI de-obfuscation. The top plot illustrates a good result that was obtained; the bottom one highlights the error amplification issue, which arises for subcarriers whose mask amplitude approaches zero.	49
4.3	Map of the testing scenario in the ANS laboratory at the University of Brescia. A participant sequentially stands at the eight marked positions.	52
4.4	Localization accuracy across obfuscation levels. The top plot shows results for the sinusoidal mask, the bottom for the virtual reflection-based one. Data is aggregated across all antennas and multiple instance evolution per obfuscation level.	59
4.5	Qualitative analysis of the relationship between the mask amplitude and the de-obfuscation absolute error for any single subcarrier. In this figure, we only consider pairs of clear and de-obfuscated CSI extracted from frames with the same sequential number. Data shown are from one antenna and one sinusoidal mask instance; similar trends hold in other cases.	62
5.1	System Model: Wireless Mesh Networking via Thread Border Router	64
5.2	Roles of Devices in a Thread Mesh Network	66
5.3	Thread Stack	67
5.4	Map of the testing scenario in the Department of Information Engineering, First Floor. Blue dots represent the devices, and the number corresponds to the office location.	69
5.5	Experimental framework organized into a four-layer architecture. . .	69
5.6	Comparison of RTT results for different deployment scenarios	74
5.7	Comparison of Interference for different deployment scenarios	75

List of Tables

2.1	Evolution of IEEE 802.11 Wi-Fi standards with increasing throughput, advanced modulation, and wider channel support.	21
2.2	Characteristics of various PHY layers in the IEEE 802.11 standard. .	23
3.1	Summary of experimental parameters used in the data collection . .	35
3.2	Classification accuracy for different bandwidths, Wi-Fi standards, and sample sizes. Accuracy values are approximate based on visual interpretation; standard deviation is categorized as Low or High. . .	40
4.1	Sinusoidal mask parameters at different strengths	54
4.2	Reflection mask parameters at different strengths	55
4.3	Summary of localization accuracy results under various masking conditions. Clear = no masking; Obfuscated = with mask applied; De-obfuscated = recovered accuracy. IQR: Interquartile Range.	60
5.1	Key Hardware Features of the Mesh Nodes and Border Router . . .	70
5.2	Comparative Analysis between Non-Working and Regular Working Days	76

List of Symbols

Symbol	Description
y	Received signal vector
x	Transmitted signal vector
H	Channel matrix (CSI)
n	Noise vector
f	Carrier frequency
t	Time
$H(f, t)$	Channel frequency response
$a_n(t)$	Amplitude attenuation on the n -th path
$\tau_n(t)$	Propagation delay on the n -th path
$d_{i,j,n}$	Path length
f_k	Frequency of k -th subcarrier
c	Speed of light
τ_i	Phase offset due to Cyclic Shift Diversity (CSD)
ρ	Sampling Time Offset (STO)
η	Sampling Frequency Offset (SFO)
f'_k	Sampling frequency
$q_{i,j}$	Beamforming gain
$\zeta_{i,j}$	Beamforming phase offset
N	Number of multipath components
N_r	Number of receive antennas
N_t	Number of transmit antennas
K	Number of subcarriers
$O(f, t)$	Obfuscation mask applied to the CSI
$H_c(f, t)$	Clean CSI (original channel state)
$H_o(f, t)$	Obfuscated CSI
$H_d(f, t)$	De-obfuscated CSI
$a_n(k)$	Amplitude of the n -th component in the mask
$\phi_n(k)$	Phase of the n -th component (sinusoidal mask)
$\delta_n(k)$	Delay in reflection mask
α	Markov scaling parameter

Symbol	Description
β	Smoothing coefficient
$x(k)$	Smoothed mask parameter
$x_{raw}(k)$	Raw (unfiltered) mask value
x_{min}, x_{max}	Lower and upper bounds for parameter clipping
$U[-1, 1]$	Uniform random value in $[-1, 1]$
BW	Bandwidth of the Wi-Fi signal
λ	Wavelength of center frequency
s_n	OFDM symbol or subcarrier index
$FFT, IFFT$	Fourier transforms (forward and inverse)
k	Frame index

Bibliography

- [1] Jesus A. Armenta-Garcia, Felix F. Gonzalez-Navarro, and Jesus Caro-Gutierrez. Wireless sensing applications with wi-fi channel state information, preprocessing techniques, and detection algorithms: A survey. *Computer Communications*, 224:254–274, 2024.
- [2] Bo Tan, Qingchao Chen, Kevin Chetty, Karl Woodbridge, Wenda Li, and Robert Piechocki. Exploiting wifi channel state information for residential healthcare informatics, 2017.
- [3] TechInsights. Global connected and iot device installed base forecast 2018–2028. <https://www.techinsights.com/blog/global-connected-and-iot-device-installed-base-forecast-2018-2028>, May 2024. Accessed: July 10, 2025.
- [4] Marco Cominelli, Francesco Gringoli, and Francesco Restuccia. Exposing the csi: A systematic investigation of csi-based wi-fi sensing capabilities and limitations. In *2023 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 81–90. IEEE, 2023.
- [5] Danny Kai Pin Tan, Jia He, Yanchun Li, Alireza Bayesteh, Yan Chen, Peiying Zhu, and Wen Tong. Integrated sensing and communication in 6g: Motivations, use cases, requirements, challenges and future directions. In *2021 1st IEEE International Online Symposium on Joint Communications and Sensing (JC&S)*, pages 1–6, 2021.
- [6] Hai Zhu, Enlai Dong, Mengmeng Xu, Hongxiang Lv, and Fei Wu. Commodity wi-fi-based wireless sensing advancements over the past five years. *Sensors*, 24(22), 2024.
- [7] Runming Yang, Xiaolong Yang, Jiachen Wang, Mu Zhou, Zengshan Tian, and Lingxia Li. Decimeter level indoor localization using wifi channel state information. *IEEE Sensors Journal*, 22(6):4940–4950, 2022.
- [8] Zhengjie Wang, Kangkang Jiang, Yushan Hou, Wenwen Dou, chen2023ngming Zhang, Zehua Huang, and Yinjing Guo. A survey on human behavior recognition using channel state information. *IEEE Access*, 7:155986–156024, 2019.

- [9] Mohammed A. A. Al-qaness, Mohamed Abd Elaziz, Sunghwan Kim, Ahmed A. Ewees, Aaqif Afzaal Abbasi, Yousif A. Alhaj, and Ammar Hawbani. Channel state information from pure communication to sense and track human motion: A survey. *Sensors*, 19(15), 2019.
- [10] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. Tool release: Gathering 802.11n traces with channel state information. *Computer Communication Review*, 41:53, 01 2011.
- [11] G. Zars. Csikit: A toolkit for parsing and visualizing csi data. <https://github.com/Gi-z/CSiKit>, 2021.
- [12] Kuskosoft. Feitcsi: High-performance csi extraction framework. <https://feitcsi.kuskosoft.com/>, 2022.
- [13] Seemoo Lab. Nexmon csi: Extract csi on broadcom wi-fi chips. https://github.com/seemoo-lab/nexmon_csi, 2021.
- [14] Jaeseong Son and Jaesung Park. Channel state information (csi) amplitude coloring schenme for enhancing accuracy of an indoor occupancy detection system using wi-fi sensing. *Applied Sciences*, 14(17), 2024.
- [15] Yongsen Ma, Gang Zhou, and Shuangquan Wang. Wifi sensing with channel state information: A survey. *ACM Comput. Surv.*, 52(3), June 2019.
- [16] Kazuya Ohara, Takuya Maekawa, and Yasuyuki Matsushita. Detecting state changes of indoor everyday objects using wi-fi channel state information. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 1(3), September 2017.
- [17] MINTS Project. Beyond 5g networks: How will our future look like? <https://b5g-mints.eu/beyond-5g-networks-how-will-our-future-look-like/>, 2023. [Online; accessed 16-May-2025].
- [18] Frederik Zumegen and Christoph Studer. A software-defined and distributed wi-fi channel-state information acquisition testbed. *arXiv preprint arXiv:2412.07588*, 2024.
- [19] Daniel Halperin et al. Linux 802.11n csi tool for intel 5300. <https://dhalperi.github.io/linux-80211n-csitool/>, 2011.
- [20] Kaishun Wu, Jiang Xiao, Youwen Yi, Dihua Chen, Xiaonan Luo, and Lionel M. Ni. Csi-based indoor localization. *IEEE Transactions on Parallel and Distributed Systems*, 24(7):1300–1309, 2013.
- [21] Anup Kumar Paul and Takuro Sato. Localization in wireless sensor networks: A survey on algorithms, measurement techniques, applications and challenges. *Journal of Sensor and Actuator Networks*, 6(4), 2017.
- [22] Shuyu Shi, Stephan Sigg, Lin Chen, and Yusheng Ji. Accurate location tracking

- from csi-based passive device-free probabilistic fingerprinting. *IEEE Transactions on Vehicular Technology*, 67(6):5217–5230, 2018.
- [23] Arun Agarwal and Saurabh N. Mehta. Combined effect of block interleaving and fec on ber performance of ofdm based wimax (ieee 802.16d) system. *American Journal of Electrical and Electronic Engineering*, 3(1):4–12, 2015.
- [24] Xuyu Wang, Lingjun Gao, Shiwen Mao, and Santosh Pandey. Csi-based fingerprinting for indoor localization: A deep learning approach. *IEEE Transactions on Vehicular Technology*, 66(1):763–776, 2017.
- [25] Rongjie Che and Honglong Chen. Channel state information based indoor fingerprinting localization. *Sensors*, 23(13), 2023.
- [26] Ze Li, Zengshan Tian, Zhongchun Wang, and Zhenyuan Zhang. Multipath-assisted indoor localization using a single receiver. *IEEE Sensors Journal*, 21(1):692–705, 2021.
- [27] Moustafa Youssef, Matthew Mah, and Ashok Agrawala. Challenges: device-free passive localization for wireless environments. In *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking, MobiCom '07*, page 222–229, New York, NY, USA, 2007. Association for Computing Machinery.
- [28] Minseuk Kim, Dongsoo Han, and June-Koo Kevin Rhee. Unsupervised view-selective deep learning for practical indoor localization using csi. *IEEE Sensors Journal*, 21(21):24398–24408, 2021.
- [29] Renato Lo Cigno, Francesco Gringoli, Marco Cominelli, and Lorenzo Ghio. Integrating csi sensing in wireless networks: Challenges to privacy and countermeasures. *IEEE Network*, 36(4):174–180, 2022.
- [30] Yong Weixiong, Robin Lee, Alvin Kon Soon Seng, et al. Security and privacy concerns in wireless networks - a survey. TechRxiv, preprint, May 2020.
- [31] K N SunilKumar and Shivashankar. A review on security and privacy issues in wireless sensor networks. In *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, pages 1979–1984, 2017.
- [32] Evgeny Khorov, Anton Kiryanov, Andrey Lyakhov, and Giuseppe Bianchi. A tutorial on ieee 802.11ax high efficiency wlans. *IEEE Communications Surveys & Tutorials*, 21(1):197–216, 2019.
- [33] Angela Ambrosin. The evolution of wi-fi networks: A comprehensive study of the ieee 802.11 standards with a focus on the upcoming ieee 802.11be version. https://thesis.unipd.it/retrieve/a6020dd3-ea46-44fb-921a-082bd1a7b97a/Ambrosin_Angela.pdf, 2023. Thesis, University of Padova.

- [34] Jahanzeb Farooq and Bilal Rauf. An overview of wireless lan standards ieee 802.11 and ieee 802.11 e. *Department of Computing Science. Umeå University Sweden.[online]. Available from World Wide Web:< URL: http://heim.ifi.uio.no/~paalee/referencing_publications/ref-wlanmodel-farooqthesis-2006.pdf*, 2006.
- [35] GeeksforGeeks. Ieee 802.11 architecture. <https://www.geeksforgeeks.org/ieee-802-11-architecture/>, 2021. Accessed: 2025-05-05.
- [36] Sourangsu Banerji and Rahul Singha Chowdhury. On ieee 802.11: wireless lan technology. *arXiv preprint arXiv:1307.2661*, 2013.
- [37] Imran Ali Qureshi and Sohail Asghar. A systematic review of the ieee-802.11 standard’s enhancements and limitations. *Wireless Personal Communications*, 131(4):2539–2572, 2023.
- [38] Tektronix. Wi-fi overview: 802.11 physical layer and transmitter measurements. <https://www.tek.com/en/documents/primer/wi-fi-overview-80211-physical-layer-and-transmitter-measurements>, 2020. [Online; accessed 19-May-2025].
- [39] Mohammad Hossein Manshaei. *Cross layer interactions for adaptive communications in IEEE 802.11 wireless LANs*. Theses, Université Nice Sophia Antipolis, December 2005.
- [40] Luiz Oliveira, Joel J. P. C. Rodrigues, Sergei A. Kozlov, Ricardo A. L. Rabêlo, and Victor Hugo C. de Albuquerque. Mac layer protocols for internet of things: A survey. *Future Internet*, 11(1), 2019.
- [41] Chul Geun Park, Dong Hwan Han, and Seong Joon Ahn. Performance analysis of mac layer protocols in the ieee 802.11 wireless lan. *Telecommunication Systems*, 33(1):233–253, 2006.
- [42] Hongqiang Zhai, Xiang chen2023n, and Yuguang Fang. How well can the ieee 802.11 wireless lan support quality of service? *IEEE Transactions on Wireless Communications*, 4(6):3084–3094, 2005.
- [43] Wikipedia contributors. Thread (network protocol). [https://en.wikipedia.org/wiki/Thread_\(network_protocol\)](https://en.wikipedia.org/wiki/Thread_(network_protocol)), 2024. Accessed: 2025-05-23.
- [44] Texas Instruments. Understanding thread: A low-power mesh networking protocol for iot. Technical report, Texas Instruments, 2015. Accessed: 2025-05-23.
- [45] Georgios Kambourakis, Constantinos Kolias, Dimitrios Geneiatakis, Georgios Karopoulos, Georgios Michail Makrakis, and Ioannis Kounelis. A state-of-the-art review on the security of mainstream iot wireless pan protocol stacks. *Symmetry*, 12(4), 2020.

-
- [46] Thread Group. Thread network fundamentals. Technical report, Thread Group, September 2022. Accessed on May 27, 2025.
 - [47] Pankaj Upadhyay, Subodh Sharma, and Guangdong Bai. Symbolic security verification of mesh commissioning protocol in thread (extended version). *arXiv preprint arXiv:2312.12958*, 2023.
 - [48] Dapeng Lan, Zhibo Pang, Carlo Fischione, Yu Liu, Amir Taherkordi, and Frank Eliassen. Latency analysis of wireless networks for proximity services in smart home and building automation: The case of thread. *IEEE Access*, 7:4856–4867, 2019.
 - [49] Texas Instruments. Exploring thread and zigbee for home and building automation. White Paper SWAY034, Texas Instruments, April 2021.
 - [50] Wikipedia contributors. Wi-Fi — Wikipedia, The Free Encyclopedia. <https://en.wikipedia.org/wiki/Wi-Fi>, 2025. [Online; accessed 3-June-2025].
 - [51] Sohaib Bin Altaf Khattak, Moustafa M. Nasralla, Haleem Farman, and Nikumani Choudhury. Performance evaluation of an ieee 802.15.4-based thread network for efficient internet of things communications in smart cities. *Applied Sciences*, 13(13), 2023.
 - [52] Eduardo Casilari, Jose M. Cano-García, and Gonzalo Campos-Garrido. Modeling of current consumption in 802.15.4/zigbee sensor motes. *Sensors*, 10(6):5443–5468, 2010.
 - [53] Isura Nirmal, Abdelwahed Khamis, Mahbub Hassan, Wen Hu, and Xiaoqing Zhu. Deep learning for radio-based human sensing: Recent advances and future directions. *IEEE Comm. Surv. & Tutorials*, 23(2), 2 2021.
 - [54] Renato Lo Cigno, Francesco Gringoli, Marco Cominelli, and Lorenzo Ghiro. Integrating CSI Sensing in Wireless Networks: Challenges to Privacy and Countermeasures. *IEEE Network*, 36(4):174–180, 8 2022.
 - [55] Zhiping Jiang, Tom H. Luan, Xincheng Ren, Dongtao Lv, Han Hao, Jing Wang, Kun Zhao, Wei Xi, Yueshen Xu, and Rui Li. Eliminating the barriers: Demystifying wi-fi baseband design and introducing the picoscenes wi-fi sensing platform. *IEEE Internet of Things Jou.*, 9(6):4476–4496, 2022.
 - [56] Francesco Gringoli, Marco Cominelli, Alejandro Blanco, and Joerg Widmer. Ax-csi: Enabling csi extraction on commercial 802.11ax wi-fi platforms. In *15th ACM Wrks on Wireless Network Testbeds, Experimental Evaluation & CHaracterization (WiNTECH)*, WiNTECH '21, pages 46–53. Association for Computing Machinery, 2021.
 - [57] Jun Wan, Ting Jiang, Xinyi Zhou, and Danlan Huang. Wi-locind: Location-independent respiration sensing based on wifi csi. In *2024 IEEE Wireless Communications and Networking Conference (WCNC)*, 2024.

- [58] IEEE 802.11 Working Group. Ieee draft standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment: Enhancements for extremely high throughput (eht). *IEEE P802.11be/D3.0, January 2023*, pages 1–999, 2023.
- [59] Chenwei Cai, Li Deng, Mingyang Zheng, and Shufang Li. Pilc: Passive indoor localization based on convolutional neural networks. In *2018 Ubiquitous Positioning, Indoor Navigation and Location-Based Services (UPINLBS)*, pages 1–6, 2018.
- [60] Chen Chen, Gang Zhou, and Youfang Lin. Cross-domain wifi sensing with channel state information: A survey. *ACM Comput. Surv.*, 55(11), February 2023.
- [61] Haobin Guan, Aryan Sharma, Deepak Mishra, and Aruna Seneviratne. Experimental accuracy comparison for 2.4ghz and 5ghz wifi sensing systems. In *ICC 2023 - IEEE International Conference on Communications*, pages 4755–4760, 2023.
- [62] Renato Lo Cigno, Francesco Gringoli, Marco Cominelli, and Lorenzo Ghiro. Integrating csi sensing in wireless networks: Challenges to privacy and counter-measures. *IEEE Network*, 36(4):174–180, 2022.
- [63] Francesco Gringoli, Matthias Schulz, Jakob Link, and Matthias Hollick. Free your csi: A channel state information extraction platform for modern wi-fi chipsets. In *Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*, pages 21–28, 2019.
- [64] Xianjun Jiao, Michael Mehari, Wei Liu, Muhammad Aslam, and Ingrid Morerman. Openwifi csi fuzzer for authorized sensing and covert channels. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 377–379, 2021.
- [65] Marco Cominelli, Felix Kosterhon, Francesco Gringoli, Renato Lo Cigno, and Arash Asadi. Ieee 802.11 csi randomization to preserve location privacy: An empirical evaluation in different scenarios. *Computer Networks*, 191:107970, 2021.
- [66] Marco Cominelli, Francesco Gringoli, and Renato Lo Cigno. On the properties of device-free multi-point csi localization and its obfuscation. *Computer Communications*, 189:67–78, 2022.
- [67] Lorenzo Ghiro, Marco Cominelli, Francesco Gringoli, and Renato Lo Cigno. On the implementation of location obfuscation in openwifi and its performance. In *2022 20th Mediterranean Communication and Computer Networking Conference (MedComNet)*, pages 64–73, 2022.

-
- [68] Lorenzo Ghiro, Marco Cominelli, Francesco Gringoli, and Renato Lo Cigno. Wi-fi localization obfuscation: An implementation in openwifi. *Computer Communications*, 205:1–13, 2023.
 - [69] Yue Qiao, Ouyang Zhang, Wenjie Zhou, Kannan Srinivasan, and Anish Arora. {PhyCloak}: Obfuscating sensing from communication signals. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, pages 685–699, 2016.
 - [70] Marco Cominelli, Francesco Gringoli, and Renato Lo Cigno. Antisense: Standard-compliant csi obfuscation against unauthorized wi-fi sensing. *Computer Communications*, 185:92–103, 2022.
 - [71] Paul Staat, Simon Mulzer, Stefan Roth, Veelasha Moonsamy, Markus Heinrichs, Rainer Kronberger, Aydin Sezgin, and Christof Paar. Irshield: A countermeasure against adversarial physical-layer wireless sensing. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1705–1721. IEEE, 2022.
 - [72] Hongzi Zhu, Yiwei Zhuo, Qinghao Liu, and Shan Chang. π -splicer: Perceiving accurate csi phases with commodity wifi devices. *IEEE Transactions on Mobile Computing*, 17(9):2155–2165, 2018.
 - [73] OpenThread. Node roles and types. <https://openthread.io/guides/thread-primer/node-roles-and-types>. Accessed: 2025-02-18.
 - [74] Srikanth Sistu, Qingzhi Liu, Tanir Ozcelebi, Esko Dijk, and Teresa Zotti. Performance evaluation of thread protocol based wireless mesh networks for lighting systems. In *2019 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–8, 2019.
 - [75] Tomás Herrera and Felipe Núñez. Design and prototyping of a thread border router based on a non network-co-processor architecture. *IEEE Access*, 8:60613–60625, 2020.
 - [76] Wojciech Rzepecki and Piotr Ryba. Iotsp: Thread mesh vs other widely used wireless protocols – comparison and use cases study. In *2019 7th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 291–295, 2019.
 - [77] Pankaj Upadhyay, Subodh Sharma, and Guangdong Bai. Symbolic security verification of mesh commissioning protocol in thread (extended version), 2023.
 - [78] Gabriel Montenegro, Christian Schumacher, and Nandakishore Kushalnagar. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. RFC 4919, August 2007.
 - [79] M. Danilo Abrignani, Chiara Buratti, Lindsay Frost, and Roberto Verdone.

- Testing the impact of wi-fi interference on zigbee networks. In *2014 Euro Med Telco Conference (EMTC)*, pages 1–6, 2014.
- [80] Phuong Luong, Tri Minh Nguyen, and Long Bao Le. Throughput analysis for coexisting ieee 802.15. 4 and 802.11 networks under unsaturated traffic. *EURASIP Journal on Wireless Communications and Networking*, 2016(1):127, 2016.
- [81] Samer AB Awwad, Nor K Noordin, Borhanuddin Mohd Ali, Fazirulhisyam Hashim, and Nurul Halimatul Asmak Ismail. 6lowpan route-over with end-to-end fragmentation and reassembly using cross-layer adaptive backoff exponent. *Wireless Personal Communications*, 98(1):1029–1053, 2018.
- [82] Thread Group. Thread Technical Overview, 2024. Accessed: March 4, 2025.
- [83] Georgios Z. Papadopoulos, Pascal Thubert, Sotirios Tsakalidis, and Nicolas Montavont. Rfc 4944: Per-hop fragmentation and reassembly issues. In *2018 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 1–6, 2018.
- [84] Martine S Lenders, Thomas C Schmidt, and Matthias Wählisch. A lesson in scaling 6lowpan—minimal fragment forwarding in lossy networks. In *2019 IEEE 44th Conference on Local Computer Networks (LCN)*, pages 438–446. IEEE, 2019.
- [85] Jan-Hinrich Hauer, Vlado Handziski, and Adam Wolisz. Experimental study of the impact of wlan interference on ieee 802.15. 4 body area networks. In *European Conference on Wireless Sensor Networks*, pages 17–32. Springer, 2009.
- [86] Chieh-Jan Mike Liang, Nissanka Bodhi Priyantha, Jie Liu, and Andreas Terzis. Surviving wi-fi interference in low power zigbee networks. In *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*, SenSys ’10, page 309–322, New York, NY, USA, 2010. Association for Computing Machinery.