Secrecy Evaluation in Physical Layer Secure Systems from Ultra-Wide Band Channel Measurements

Kristian Drizari

MTE2317

Supervisor: Professor Konstantinos Lambrinoudakis

Department of Digital Systems, School of Information and Communication Technologies
Master of Science in Digital Systems Security

This dissertation is submitted for the degree of
Master Of Science (M.Sc)

University Of Piraeus February 2025

"Wisdom begins in wonder."
-Socrates

I would like to dedicate this thesis to my parents, whose courage gave me a chance for a better life, and to my sister. . .

Declaration

I hereby declare that this thesis entitled **"Secrecy Evaluation in Physical Layer Secure Systems from Ultra-Wide Band Channel Measurements"** is the result of my own work and includes nothing that is outcome of work done in collaboration, except where specifically stated. I confirm that all sources of information used have been fully acknowledged and that I have not previously submitted this work, or any part of it, for a degree or diploma at any other institution. This thesis is written in LaTeX environment.

Kristian Drizari
February 2025

Acknowledgements

I wish to express my sincere gratitude to my supervisor, Professor Konstantinos Lambrinoudakis, for his comprehensive supervision and support. I am also deeply grateful to Professor Athanasios Kanatas for his unwavering support, insightful advice and invaluable guidance throughout the development of this thesis, addressing every query related to this work. His provision of the necessary equipment was instrumental in conducting the experiments presented herein. Additionally, I would like to extend my heartfelt thanks to the postdoctoral researchers of the Telecommunications Systems Laboratory at the University of Piraeus for their keen interest in my work and their thoughtful suggestions, which provided valuable insights and bright ideas during the course of this research.

Abstract

The rapid expansion of wireless communication technologies has introduced new challenges in securing data transmissions against eavesdropping and unauthorized access. This thesis investigates the potential of Physical Layer Security (PLS) as a complementary approach to traditional cryptographic methods, leveraging the unique characteristics of wireless channels to enhance communication confidentiality. By combining real world Ultra Wideband (UWB) channel measurements with theoretical modeling, the study evaluates achievable secrecy metrics, including Secrecy Capacity and Secrecy Rate, under various indoor and outdoor scenarios. Using Humatics P442 UWB radios and advanced post-processing techniques, the present work quantifies the impact of environmental factors, interference, and multipath fading on secure communication. The findings demonstrate the effectiveness of UWB technology in achieving robust PLS, particularly in scenarios where its high resolution and wide bandwidth mitigate eavesdropping risks. This work not only bridges the gap between theory and practical implementation but also provides valuable insights into optimizing secure wireless communication systems, paving the way for future advancements in PLS methodologies.

Table of contents

List of figures

List of tables

Nomenclature

Acronyms / Abbreviations

τ_{RMS}	RMS Delay Spread
P_r	Received Power
P_t	Transmitted Power
P_{out}	Outage Probability
5G	Fifth Generation
AWGN	Additive White Gaussian Noise
CDF	Cumulative Distribution Function
CIR	Channel Impulse Response
CSI	Channel State Information
dB	Decibel-Logarithmic Scale
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FSPL	Free Space Path Loss Model
i.i.d	Independent and Identically Distributed
IoT	Internet of Things
LoS	Line of Sight
MPCs	Multipath Components

ns	nanoseconds
PDP	Power Delay Profile
PDP	Power Delay Profile
PL	Path Loss
PLS	Physical Layer Security
pmf	Probability Mass Function
PRF	Pulse Repetition Frequency
Rx	Receiver
SNR	Signal to Noise Ratio
ToF	Time of Flight
Tx	Transmitter
UWB	Ultra-Wideband
VNA	Vector Network Analyzer
WSSUS	Wide-Sense Stationary Uncorrelated Scattering

Chapter 1

Introduction

1.1 Background

Physical Layer Security

Physical Layer Security (PLS) is a security paradigm that leverages the inherent characteristics of the physical medium used for communication to ensure confidentiality [4]. Traditionally, the focus of security has been at higher layers of the communication protocol stack, where cryptographic methods like encryption and authentication are employed. However, with advances in computational power—especially the potential threat posed by quantum computing—there is growing interest in alternative security techniques that do not rely on computational hardness but instead use the physical properties of the communication channel itself. This shift in focus has led to the development of PLS.

The physical layer, which lies at the base of the communication protocol stack, converts bits of information into modulated signals for transmission. Unlike higher-layer techniques, PLS exploits the stochastic nature of wireless communication channels—such as fading, interference, and noise—to provide security. In wireless systems, signals propagate through an open medium, making them inherently vulnerable to eavesdropping. By leveraging the unpredictable behavior of the physical environment, PLS creates an additional layer of protection that complements traditional cryptographic methods.

PLS employs several key techniques:

- Secrecy Coding introduces coding schemes that maximize the uncertainty for eavesdroppers, ensuring that even if the signal is intercepted, decoding it correctly without the knowledge of the channel's properties is virtually impossible [1].

- Artificial Noise Generation involves introducing noise in such a way that only legitimate receivers, who have full channel state information (CSI), can remove it, while eavesdroppers are overwhelmed by the interference.

- Beamforming and Beam-focusing techniques utilize directional antennas to concentrate signal energy toward the intended receiver, reducing the signal's strength in other directions and thereby limiting the possibility of eavesdropping.

The concept of secrecy in PLS is often quantified using metrics such as Secrecy Capacity (C_S) and Secrecy Rate (R_S) [5]. These metrics are directly related to the conditions of the wireless channel, particularly the Signal-to-Noise Ratio (SNR) at the legitimate receiver versus the eavesdropper.

Furthermore, as the world becomes increasingly connected with the advent of technologies like 5G, IoT [6], and Ultra-Wideband (UWB) communications [7], the need for robust security measures at the physical layer becomes even more pressing. These emerging technologies often operate in dynamic and decentralized environments, where traditional security methods may not be sufficient. PLS offers a promising solution, especially in scenarios where low-latency and high-throughput communications are critical, and higher-layer encryption methods might introduce unacceptable overhead. Despite its promise, PLS faces several challenges. The dynamic nature of wireless environments, with frequent changes in channel conditions and network topology, complicates the implementation of such techniques. Moreover, multi-user scenarios introduce additional complexity, as ensuring secrecy for all users simultaneously requires sophisticated coordination. There is also a trade-off between achieving high secrecy rates and maintaining system performance, particularly in terms of bandwidth efficiency and power consumption. Nonetheless, this technology represents an exciting frontier in the quest for secure communication, complementing traditional cryptographic approaches and providing an additional layer of protection against eavesdropping attacks.

1.2 Motivation

The rapid growth of wireless communications has brought about significant challenges in ensuring secure and reliable data transmission. Physical Layer Security offers a promising solution by leveraging the characteristics of the wireless channel itself to secure communication. However, there are several challenges in quantifying how secure these systems are in practical environments. This is particularly crucial because real-world wireless channels exhibit varying properties due to factors like interference, fading, and multipath propagation.

There is a noticeable gap in the literature when it comes to practical channel measurements that inform the achievable secrecy in physical layer systems. While theoretical models of C_S and R_S have been widely explored, there is limited empirical data on how real-world channel characteristics affect these secrecy metrics, especially in dynamic environments. Addressing this gap will enable more accurate predictions of achievable secrecy in real-world systems and guide the design of more secure wireless communication protocols.

The motivation for this research lies in:

- The increasing vulnerability of wireless communications to eavesdropping attacks due to the open nature of the communication medium.
- The limitations of traditional cryptography in wireless networks, particularly as technological advancements pose new threats.
- The lack of empirical data on channel measurements and how these affect secrecy performance in practical systems.

By performing detailed channel measurements and evaluating achievable secrecy in real-world settings, this research aims to provide new insights that can help optimize the design of future secure communication systems.

1.3 Problem Statement

While the concept of PLS offers a promising approach to enhancing wireless communication security, its practical implementation faces significant challenges. In particular, ultra-wideband (UWB) systems, with their unique channel characteristics, introduce new dimensions to how secrecy can be achieved and measured at the physical layer. Theoretical models of secrecy capacity and secrecy rate provide useful benchmarks, but they often rely on idealized conditions that may not fully capture real-world wireless environments. The problem addressed in this thesis is the lack of empirical data linking real-world UWB channel characteristics to achievable secrecy metrics. This gap in the literature limits our ability to design secure communication systems that are resilient to eavesdropping and interference [8]. Therefore, it is necessary to conduct detailed channel measurements in practical UWB scenarios and evaluate how these measurements impact secrecy performance. Specifically, this thesis seeks to identify the conditions under which secrecy can be maximized in realistic environments, accounting for factors like channel fading, interference, and the presence of eavesdroppers.

1.4 Objective

The primary objective of this research is to investigate the security potential of UWB systems at the physical layer by conducting real-world channel measurements and analyzing achievable secrecy metrics. Specifically, the goals are:

- Measure key UWB channel characteristics..
- Calculate secrecy capacity and secrecy rate based on the measured channel data.
- Evaluate how different channel conditions influence the potential for secure communication.
- Provide insights for improving physical layer security in practical UWB environments.

1.5 Contributions

This thesis contributes significantly to the field of Physical Layer Security through several key advances. First, it provides real-world channel measurements in UWB environments, offering empirical data to assess the security potential of such systems. Additionally, it develops and validates models that calculate C_S and R_S based on the measured channel data, making a substantial contribution to the theoretical understanding of PLS. Lastly, it compares empirical results with theoretical models, providing valuable insights into how PLS can be improved in practical wireless communication systems.

Chapter 2

Literature Review

2.1 Progress in Physical Layer Security

Wireless networks, by their very nature, are inherently open and accessible, which makes them particularly susceptible to a variety of malicious activities such as eavesdropping, jamming, and unauthorized access. This openness poses significant challenges to ensuring the confidentiality and integrity of the transmitted data. Consequently, security emerges as a critical aspect in the design and deployment of wireless communication systems. The foundational concept of securing communication at the physical layer was introduced by Claude Shannon, who is widely regarded as the father of information theory. In his seminal work, Shannon [9] defined the notion of 'perfect secrecy,' which refers to a situation where the eavesdropper gains no information about the transmitted message, even with unlimited computational resources (Fig. 2.1). Shannon demonstrated that perfect secrecy can be achieved if and only if the key used for encryption is as long as the message itself and is completely random, a principle that underpins the one-time pad encryption method.

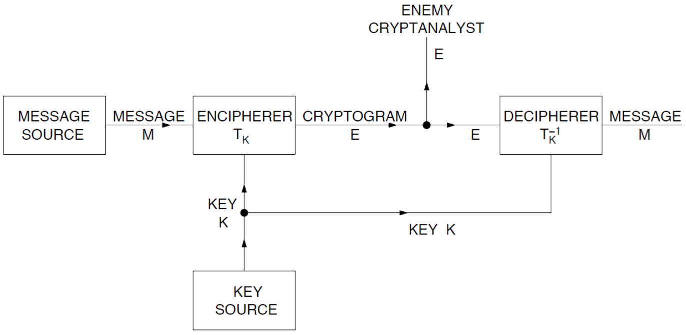


Fig. 2.1 Schematic of a general secrecy system provided from Shannon.

Building upon Shannon's groundbreaking ideas, Aaron Wyner introduced the concept of the wiretap channel (Fig. 2.2), which models the communication scenario involving a legitimate transmitter and receiver, as well as an eavesdropper. In Wyner's model, the main channel refers to the communication link between the source (transmitter) and the intended receiver, while the wiretap channel represents the link between the source and the eavesdropper. Wyner's pivotal work demonstrated that perfect secrecy could be achieved without the need for exchanging secret keys, provided that the wiretap channel has a lower SNR compared to the main channel. This revelation opened new avenues for physical layer security, emphasizing that secure communication is attainable through the inherent properties of the communication channels themselves, without relying solely on higher-layer encryption techniques [1].

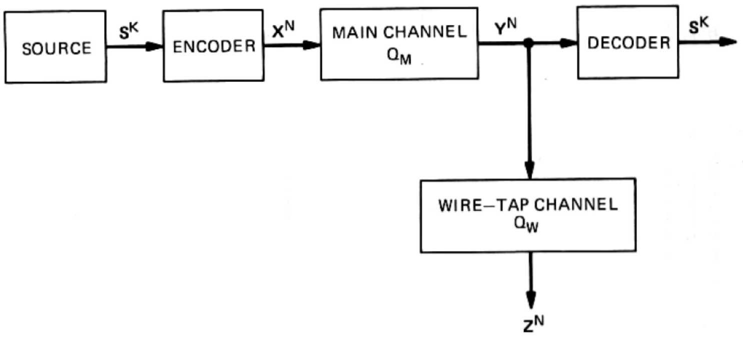


Fig. 2.2 General case of a wiretap channel provided from Wyner.

Wyner's findings were further expanded by subsequent researchers. For instance, Csiszár and Körner generalized Wyner's wiretap channel model by considering more general broadcast channels. They introduced the concept of the secrecy capacity, which quantifies the maximum rate at which information can be securely transmitted over a channel in the presence of an eavesdropper. Their work established that secure communication is possible even when the eavesdropper's channel is not necessarily worse than the main channel [10], provided that certain conditions on the channel statistics are met. Despite these promising developments, Wyner's original model and its extensions come with notable limitations. Two primary constraints hinder the broader applicability of these approaches: the absence of feedback mechanisms and the requirement that the main channel must outperform the wiretap channel in terms of quality (e.g., higher SNR)[2]. The lack of feedback means that the transmitter has no means of adjusting its transmission strategy based on the receiver's feedback, which can be crucial for adapting to varying channel conditions. Additionally, the necessity for the main channel to be inherently better than the eavesdropper's channel limits the scenarios where physical layer security techniques can be effectively applied [11].

In response to these limitations, researchers have explored various strategies to enhance physical layer security. Techniques such as cooperative jamming, where friendly nodes intentionally transmit interference to degrade the eavesdropper's channel[12], and the use of multiple antennas (MIMO systems) to create spatial separation between the legitimate receiver and the eavesdropper[11], have been proposed. These approaches aim to relax the stringent requirements on channel conditions and introduce more flexibility in securing wireless communications.

The primary objective of this study is to maximize the secure transmission rate from the transmitter to the legitimate receiver in the presence of an eavesdropper. This optimal rate is referred to as the secrecy rate, which serves as the key performance metric throughout this thesis. In summary, PLS leverages the physical characteristics of communication channels to provide confidentiality and integrity of transmitted data. Originating from Shannon's concept of perfect secrecy and Wyner's wiretap channel model, the field has evolved to address various challenges and limitations through innovative techniques and strategies.

2.2 UWB Radio Technology

Years now a technology that is thriving in the field of PLS since it has been conducted extended research, is the Ultra Wide-band Radio Technology. Ultra Wideband (UWB) radio technology is a wireless communication method that employs very short pulses spread over a wide frequency spectrum. Unlike traditional narrowband systems that transmit signals within a limited frequency band, UWB transmits over a wide range of frequencies simultaneously. This unique approach allows UWB to offer high data rates, precise positioning capabilities, and low power consumption, making it an attractive option for various applications.

2.2.1 Technical Characteristics

UWB is defined by its extremely wide bandwidth. According to the the Federal Communications Commission (FCC), a UWB signal is one that occupies a bandwidth greater than 500 MHz or has a fractional bandwidth greater than 20% of its center frequency. This extensive bandwidth enables the transmission of large amounts of data at high speeds and provides the ability to resolve multipath components, which is beneficial in cluttered environments. Moreover, some more of the technical characteristics of the UWB Radio are :

- Pulse-Based Transmission: UWB systems typically use very short-duration pulses, nanoseconds or picoseconds. These pulses are transmitted at a low duty cycle, resulting in a signal that has a low power spectral density. The short pulses allow for fine time resolution, which is crucial for high-precision ranging and positioning applications[13].

- Low Power Spectral Density: These type of signals are characterized by their low power spectral density, meaning the power of the signal is spread sparsely across the wide frequency band. This property minimizes the potential for interference with other radio systems operating in the same spectrum. It also contributes to the hidden nature of UWB transmissions, as the signals are difficult to detect without specialized equipment [14]
- High Data Rates and Precise Positioning: Since the wide bandwidth of UWB allows for the transmission of data at very high rates, potentially exceeding hundreds of megabits per second. This makes UWB ideal for applications requiring both high-speed data transfer and accurate localization.

2.2.2 Real-Life Applications of UWB

As mentioned above, UWB has many attractive technical characteristics which makes it suitable for real life scenarios like :

- Short-Range High-Speed Data Transfer
- Indoor Positioning and Localization
- Automotive Applications, for instance , secure key-less entry systems , parking assistance and collision avoidance.
- Medical Applications (Medical imaging and monitoring)

2.2.3 Benefits of UWB for Secure Communications

Its low power spectral density and wide frequency spread make UWB signals difficult to detect and intercept, as they are often covered by noise and not easily identified by conventional receivers. This inherent characteristic provides a level of security against eavesdropping and intentional jamming[13]. Moreover, the stealthy nature of UWB transmissions results in a low probability of detection and intercept. Since the signal energy is spread over a wide bandwidth, it reduces the chance that an unwanted receiver will detect the presence of the transmission, making UWB suitable for secure military communications and secret operations.

2.3 Secrecy Metrics

There are many different approaches to secrecy and therefore many different secrecy definitions, as mentioned above, Shannon and later Wyner built those foundations and the latter introduced what was later called *weak secrecy*.

Weak secrecy, is a weak measure of secrecy which basically limits the rate at which information leaks but the amount of the information which is revealed can still be randomly large. This problem was recognized by a scientist named Ueli M. Mauer when he introduced the *strong secrecy* [15]. First of all , we need to set how we calculate the secrecy. Let's assume that there exists a message **M**, between two parties and there is an eavesdropper whose observation is notated as **Z**. The goal is to make this leakage negligible or, ideally , zero. Mathematically this can be depicted as :

$$I(M;Z) \leq \varepsilon \tag{2.1}$$

where :

- $I(M;Z)$ is the **mutual information** between the message **M** and the eavesdropper's observation **Z** and,
- ε is a small positive constant that bounds the leakage.

In traditional secrecy (weak secrecy) , the mutual information is normalized by the number of symbols n , giving $\frac{1}{n}I(M;Z) \leq \varepsilon$. In strong secrecy , the normalization factor $\frac{1}{n}$ is omitted and we look at the absolute value $I(M;Z)$, aiming to bound the total information leakage directly. However, strong secrecy does not prevent an eavesdropper from determining whether a transmission is taking place or not. And more importantly, it assumes that the messages are uniformly distributed, which prevents from securing each individual message.

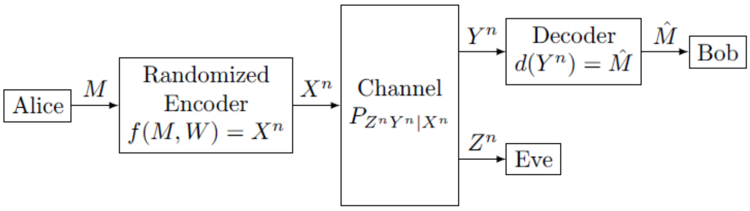


Fig. 2.3 Visual Representation of the Wiretap Channel by Wyner [1].

Throughout the years , Hou and Kramer [16] proposed *effective secrecy* as a more robust secrecy measure than both weak and strong secrecy. This measure includes the idea of *stealth*, where transmissions are concealed such that an eavesdropper cannot detect them. An even stricter level of secrecy is *semantic secrecy*, introduced by Goldwasser and Micali [17] , which ensures the security of each individual message rather than securing all messages simultaneously. Later , Bellare et al.[18] refined these definitions by introducing distinct metrics for evaluating the advantage an attacker might gain.

In this thesis we will mainly study and analyze concepts such as secrecy capacity and secrecy rate. In the next there is a brief introduction on each concept giving some basic examples.

2.3.1 Secrecy Capacity

In the realm of PLS, **secrecy capacity** is a fundamental concept that quantifies the maximum rate at which secure information can be transmitted over a communication channel in the presence of an eavesdropper. It essentially measures the difference in information rates between the legitimate receiver and the eavesdropper, representing the highest data rate at which the transmitter can send information to the intended receiver while ensuring that the eavesdropper gains no useful knowledge about the transmitted messages. The concept of secrecy capacity was first introduced by Wyner [1] through the Wiretap Channel Model (Fig. 2.3). In this model, there are three parties involved :

1. The transmitter (commonly referred to as Alice)
2. The legitimate receiver (Bob)
3. The eavesdropper (Eve)

Wyner demonstrated that if the channel to Bob is better than the channel to Eve, it is possible to transmit information securely without relying on traditional cryptographic methods. This means that the physical properties of the communication channels themselves can be exploited to achieve security. To gain a deeper understanding of this concept let's assume a simple example: Imagine Alice wants to send a confidential message to Bob over a wireless channel, but Eve is trying to intercept the message. If the channel conditions between Alice and Bob are superior (e.g., higher SNR) compared to those between Alice and Eve, Alice can adjust her transmission rate such that Bob can reliably receive and decode the message, while Eve cannot extract any meaningful information due to poorer channel conditions. The significance of secrecy capacity lies in its ability to provide a theoretical limit for secure communication over noisy channels without relying on encryption keys. However, in practical terms, achieving positive secrecy capacity can be challenging due to the dynamic nature of wireless channels and the presence of multiple users and potential eavesdroppers. Although, various techniques have been developed to enhance secrecy capacity, such as introducing artificial noise to degrade the eavesdropper's channel, employing multiple antennas for spatial diversity, and utilizing cooperative relay nodes to assist in secure transmission.

While a detailed mathematical analysis of secrecy capacity will be presented in the next chapter, it's important to recognize its foundational role in PLS. Secrecy capacity provides quantitative measure that helps in assessing the potential for secure communication in different scenarios and guides the development of strategies to mitigate the risks posed by eavesdroppers.

2.3.2 Secrecy Rate

The **secrecy rate** is a fundamental metric in PLS that quantifies the maximum rate at which confidential information can be securely transmitted from a sender to an intended receiver in the presence of an eavesdropper. It represents the achievable data rate at which the legitimate receiver can decode the transmitted messages correctly while ensuring that the eavesdropper gains negligible or no information about the messages. Building upon the concept of secrecy capacity, the secrecy rate focuses on practical scenarios where channel conditions and system constraints play significant roles. It essentially measures the difference between the information rates of the main channel (Alice-Bob channel) and the wiretap channel (Alice-Eve channel). Let's consider a scenario, similar to the one before, where Alice wants to send a confidential message to Bob over a wireless channel, while Eve attempts to eavesdrop on the communication. The capacity of the main channel between Alice and Bob is denoted by C_M and the capacity of the wiretap channel (Alice-Eve) is C_W. The secrecy rate R_S can be expressed mathematically as:

$$R_S = max(C_M - C_W, 0) \tag{2.2}$$

This equation indicates that the R_S is the non-negative difference between the capacities of the main channel and the eavesdropper's channel[5]. The secrecy rate is influenced by various factors, including the quality of the communication channels, signal processing techniques, and the presence of noise and interference. Enhancing the secrecy rate often involves improving the main channel's conditions relative to the eavesdropper's channel. Several strategies can be employed to achieve this:

1. Artificial Noise Generation
2. Beamforming and Multiple Antennas
3. Cooperative Relaying

2.3.3 Helping Interferer or Cooperative jamming

A strategy which is employed to enhance secure communication in wireless networks is **helping interferer** or **cooperative jamming**. This approach involves one ore more friendly nodes in the network, known as helpers or jammers, intentionally transmitting interference or noise to degrade Eve's channel while minimally affecting Bob's channel. By doing so, the secrecy capacity and secrecy rate between Alice and Bob can be significantly improved [19]. How does this mechanism though work? Let's consider the typical scenario where Alice want to exchange confidential information to Bob in the presence of Eve. In cooperative jamming, a helper node, let's call him Freddy, transmits a jamming signal concurrently with Alice's transmission. This jamming signal is desired to interfere with Eve's reception, making it difficult for her to intercept or decode the transmitted message. Since Bob is aware of the presence and characteristics of Freddy's signal, he can employ signal processing techniques to mitigate his impact, ensuring that his reception of Alice's message remains reliable. This method offers several benefits, indicatively the enhancement of secrecy capacity because of the degradation of the C_W, the resource-efficient security enhancement in cases where networks with nodes that have limited computational capabilities and cannot support complex encryption algorithms, and of course the applicability in various networks conditions as it is very beneficial when Eve's channel conditions are similar to or even better that those of Bob's.

However, there are plenty implementation considerations that should be taken into account when applying such security method. First of all, the coordination among nodes as effective cooperative jamming requires precise synchronization and coordination between the transmitter and the helper nodes so as it does not interfere with the legitimate receiver and that the overall communication remains efficient. Moreover, a lot of attention need to be paid when designing a jamming signal since the goal is to maximize the interference at Eve's while minimizing impact on Bob's side. Last but not least, very important is the knowledge of the CSI to both of channels C_M and C_W.

2.4 Previous work

In the literature, there is an abundance of research on physical layer security systems that focus on estimating secrecy capacity and secrecy rate, primarily through theoretical approaches and simulations. Numerous studies have explored various aspects of physical layer security, developing theoretical frameworks and proposing new techniques to enhance secure communications. For instance, researchers have investigated the impact of channel conditions, coding schemes, and signal processing methods on secrecy performance [4]. Similarly, significant work has been conducted on Ultra Wideband (UWB) channel measurements using equipment similar to the kits that will be presented and utilized in this study. These studies often focus on characterizing UWB channels in different environments, analyzing factors such as path loss, multipath propagation, and time-domain characteristics. Such measurements are crucial for designing and optimizing UWB communication systems and have applications in localization and imaging [20].

However, a very limited number of reported works combine real-world UWB channel measurements with the calculation of physical layer communication secrecy. While theoretical models provide valuable insights, they may not capture all the practical aspects and challenges encountered in real environments. The rarity of studies that integrate empirical UWB channel data with physical layer security analysis highlights a gap in the current research landscape.

Chapter 3

Theory and Mathematical Framework

3.1 Wireless Channel Models

Wireless communication channels are complex due to various propagation mechanisms, including reflection, diffraction and scattering. Channel modeling is essential for understanding signal behavior and designing robust communication systems. The channel model can vary significantly depending on the environment(urban, rural, indoor, etc.) and the frequency band used. The general channel model can be expressed as follows :

$$y(t) = h(t) * x(t) + n(t) \tag{3.1}$$

where $y(t)$ is the received signal, $h(t)$ is the channel response, $x(t)$ is the transmitted signal and $n(t)$ is the noise component. A good channel model helps in understanding the limitations of the physical medium, design of the modulation schemes, error-correction algorithms, power control strategies and plays a vital role in system simulation and performance evaluations [21].

Types of Channel Models

Channel models vary depending on the application and environment:

- Free-Space models assume a line-of-sight (LoS) connection between transmitter and receiver.

- Empirical models are based on measurements from specific environments and provide practical, easy to use models that are less complex than theoretical models

- Stochastic models use statistical methods to represent random variations in the channel, accounting for multipath and fading effects
- Deterministic models are based on ray-tracing methods and provide a detailed physical description

Methodology for Channel Modeling

Below it is explained briefly in some steps the basic methodology of performing channel modeling

1. Defining the environment by categorizing it (indoor,urban,rural), as it determines the dominant propagation mechanisms (e.g., reflection, diffraction)
2. Measurements campaigns are performed and parameters like path loss, delay spread, and coherence bandwidth are recorded using specialized equipment (e.g., channel sounders). This data is then processed to create empirical models.
3. Parameter estimation methods are utilized and parameters like path loss exponent, shadowing variance, fading coefficients are extracted from measurements or chosen based on environment characteristics.
4. Channel Impulse Response (CIR), for time-varying channels, the CIR $h(t)$ provides a snapshot of the channel at a specific time

   $$h(t) = \sum_{k=0}^{N-1} \alpha_k \delta(t - \tau_k) \tag{3.2}$$

   where N is the number of multipath components, a_k is the amplitude of each path, and τ_k is the delay.
5. Validation and calibration is performed, i.e, the model is validated by comparing simulated results with real-world measurements. Calibration may involve tuning parameters to improve accuracy in a specific environment.

Sometimes, for simplicity reasons we assume some characteristics for the channel, like, stationarity, Wide-Sense Stationary Uncorrelated Scattering(WSSUS), which means that each multipath component is uncorrelated with others and frequency selectivity because depending on the bandwidth, the channel may exhibit frequency-selective or frequency-flat characteristics, which affects the fading behavior.

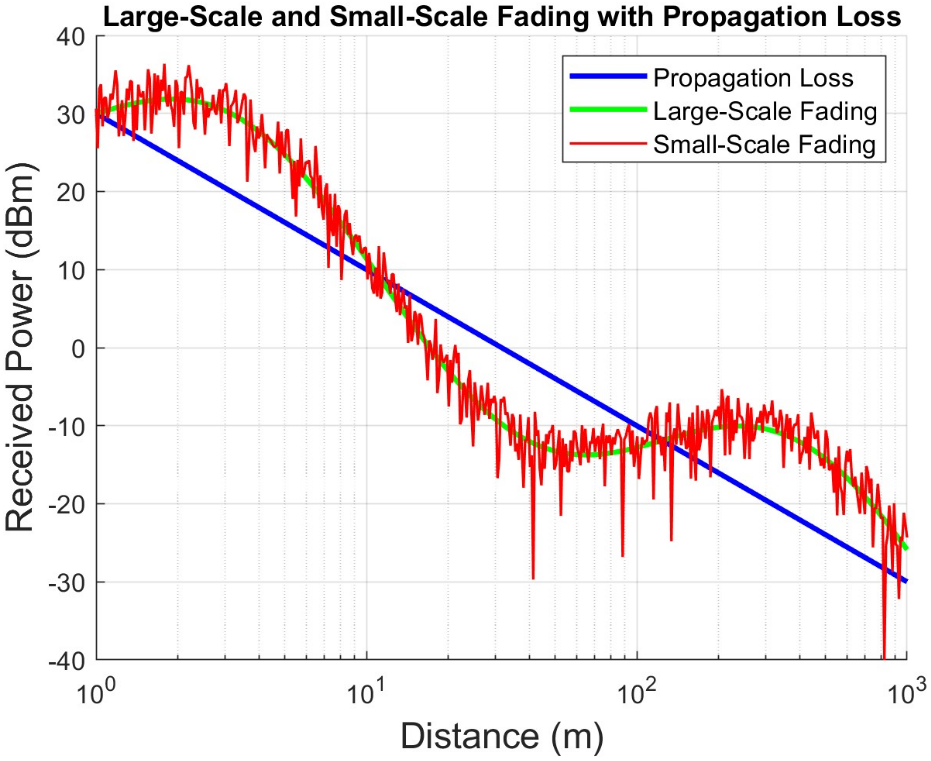


Fig. 3.1 Visual illustration of the effects of path loss, small scale and large scale fading on received power as a function of distance.

3.1.1 Path Loss

In this section we will analyze the Path Loss component in a wireless channel, but first of all we must reply to the simplest question that any reader would come up with, "What is Path Loss?".

Path loss refers to the reduction in signal strength or power density as a signal propagates through space. It is a fundamental concept in wireless communication that quantifies how much the signal weakens as it travels from the transmitter to the receiver. Path loss is influenced by the distance between the antennas, the frequency of the signal, and the environment through which the signal travels (e.g., obstacles, terrain). Accurately calculating path loss is crucial for designing communication systems with sufficient power to reach desired distances or coverage areas. First Path Loss (PL) model to explain is the LOS PL. Let us consider a signal transmitted through a free-space environment from a transmitter to a receiver at a distance d. In this scenario, there are no obstacles between the antennas. The resulting channel model is referred to as LOS. In this model, the signal experiences free space PL as it travels from Transmitter (Tx) to Receiver (Rx). The received signal $r(t)$ is described by the following equation:

$$r(t) = \mathrm{Re}\left\{ \frac{\lambda \sqrt{G_t G_r}\, u(t - \tau_l) e^{-j2\pi d/\lambda}}{4\pi d} \right\} e^{j2\pi f_t t} \tag{3.3}$$

where G_t and G_r are the transmit and receive antenna gains, λ is the wavelength of the transmitted signal, $u(t - \tau_l)$ represents the signal transmission delayed by $\tau_l = \frac{d}{c}$ and the term $e^{-j2\pi d/\lambda}$ accounts for the phase shift due to propagation distance d. In this case G_t and G_r are referenced to isotropic antenna , but in practical applications , T_x and R_x antennas can have directional gains to improve the signal power in specific directions. For example, directional antenna gains can reach up to 2.15 dB for a dipole or even higher for horn or dish antennas. To quantify the relationship between the transmitted and received power in this free-space environment, it is used the **Friis transmission formula**, which provides a direct way to calculate the received power (P_r) at a given distance d from the transmitter with transmit power P_t.

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi d} \right)^2 \tag{3.4}$$

Basically, it captures how received power decreases as the distance between antennas increase, specifically, the term $(\frac{\lambda}{4\pi d})^2$ shows that the received power is inversely proportional to the square of the distance and the square of the frequency.

Received Power in dBm

The received power in dBm is calculated by rearranging Friis equation:

$$P_r\,(\mathrm{dBm}) = P_t\,(\mathrm{dBm}) + 10\log_{10}(G_t G_r) + 20\log_{10}(\lambda) - 20\log_{10}(4\pi) - 20\log_{10}(d) \tag{3.5}$$

Free Space Path Loss Model (FSPL) quantifies the loss of signal strength in free space propagation and is given by:

$$PL(\mathrm{dB}) = 10\log_{10}\left(\frac{P_t}{P_r} \right) = -10\log_{10}\left(G_t G_r \left[\frac{\lambda}{4\pi d} \right]^2 \right) \tag{3.6}$$

It highlights, that the signal decays inversely with the square of the distance between the T_x and R_x [22].

3.1.2 Small Scale Fading

In Figure 3.1 we are able to see an example and a visual illustration of the effects of Path Loss and Fading. Here, we should pay attention because when referring to fading we mean two types of fading : 1) Small scale fading and 2) Large scale fading. The latter usually is referred to as **Shadowing**. In this section the effect of Small Scale Fading will be explained.

Small Scale Fading , occurs due to rapid fluctuations in the received signal's amplitude and phase, caused by interference among multiple signal paths (multipaths) arriving from various directions. These paths are generated due to various electromagnetic propagation mechanisms like diffraction and scattering from obstacles that the signal will interfere with during it's propagation. When modeling the channel it's important to consider this factor and to describe this effect using a statistical distribution. The most common statistical distributions to describe such effect are *Rayleigh* and *Rician* distributions and we refer to them as **Rayleigh Fading** and **Rician Fading**. To give a better understanding of these two fading cases we need to give two simple examples.

3.1.2.1 Rayleigh Fading

Rayleigh Fading is generally considered as a "worse" case fading compared to Rician fading, especially in terms of signal reliability in wireless communication. It occurs in environments with no LOS component between the transmitter and receiver, meaning the signal reaches the receiver purely through scattered or reflected paths. Due to the lack of a strong direct path, the received power fluctuates heavily, often reaching deep fades as the reflected waves interfere destructively. Due to this, Rayleigh fading is quite challenging for reliable communication. So, in this fading model the amplitude α is distributed according to:

$$p_\alpha(\alpha) = \frac{2\alpha}{\Omega} \exp\left(-\frac{\alpha^2}{\Omega}\right), \quad \alpha \geq 0 \tag{3.7}$$

where, $\Omega = E\left[R^2\right] = 2\sigma^2$ is the average power [23].

3.1.2.2 Rician Fading

Rician fading takes place when there is both multiple scattered/reflected paths and a strong LOS path or a strong component (it could be a strong reflection path). As explained in [23] the channel fading amplitude is distributed according to [24]:

$$p_\alpha(\alpha) = \frac{2(1+n^2)e^{-n^2\alpha/\Omega}}{\Omega} \exp\left[-\frac{(1+n^2)\alpha^2}{\Omega}\right] I_0\left(2n\alpha\sqrt{\frac{1+n^2}{\Omega}}\right), \quad \alpha \geq 0 \tag{3.8}$$

where n is the Nakagami-n fading parameter which ranges from 0 to ∞ and is related to Rician K factor $K = n^2$. Another way to depict this would be the following expression [25]:

$$p_r(r) = \frac{r}{\sigma^2} \exp\left(-\frac{r^2 + |c_o|^2}{2\sigma^2}\right) I_0\left(\frac{r|c_o|}{\sigma^2}\right) \tag{3.9}$$

where c_0 is the complex constant which is retrieved from the complex envelope ,

$$c(z) = c_0 + \sum_{i=1}^{N} c_i(z) \tag{3.10}$$

and $I_0(x)$ is the modified Bessel function of first kind and zero order,

$$I_0(x) = \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{x\cos\theta}\, d\theta \tag{3.11}$$

3.1.3 Large Scale Fading

As previously mentioned, Large Scale Fading is also called Shadowing effect. In this case the propagating radiowaves are being shadowed from buildings and other obstacles. This shadowing is neither absolute nor steep, but usually is gradual due to the existence of diffraction mechanism. So the received power practically is a random variable which depends on the number and the electric characteristics of the scatterers, who contribute to the propagation. That is why the random alterations of the received signal are referred to as shadow fading. The most commonly used model for Large Scale Fading is the Log-normal Shadowing Model :

$$PL(d) = PL(d_0) + 10n\log_{10}\left(\frac{d}{d_0}\right) + X_\sigma \tag{3.12}$$

where X_σ is a Gaussian variable with zero mean and standard deviation σ, representing the shadowing effect [25].

3.1.4 UWB channel characteristics

As explained in chapter 2.2, UWB technology is rising through the years. The critical point in designing UWB systems is the deep understanding of UWB propagation channel theory, since there are various differences compared to conventional channels. First of all, if the relative bandwidth is large the propagation processes, and therefore PL and shadowing, become frequency dependent and the well known WSSUS model is not applicable anymore. If the absolute bandwidth is large, the shape of the impulse responses as well as the fading statistics change [7].

To start with, the PL in UWB channels differs significantly from conventional systems. Due to the frequency dependency in PL and shadowing, the higher frequencies within the UWB range experience grater PL than lower frequencies. This phenomenon must be accounted for in UWB channel models to accurately estimate signal attenuation over distance. A common approach to modify the FSPL formula is to include the frequency component explicitly [26] :

$$PL(f,d) = PL(f_0,d_0) + 10n\log_{10}\left(\frac{d}{d_0}\right) + \xi \log_{10}\left(\frac{f}{f_0}\right) \tag{3.13}$$

where ξ is an additional frequency-dependence factor that captures how PL changes with frequency in UWB channels.

Research shows that for UWB signals, higher frequencies within the band tend to suffer more severe path loss than lower frequencies. This is because higher frequencies are more susceptible to absorption and diffraction losses, especially in indoor or cluttered environments [27].

3.1.4.1 Fading in UWB Channels

Fading in UWB channels is also distinct from narrowband fading due to the wide frequency range and short pulse duration of UWB signals. UWB signals are characterized by multipath propagation, where each pulse generates multiple reflected, scattered, and diffracted paths, all arriving at the receiver at slightly different times. This high-resolution multipath structure means that UWB channels experience frequency-selective fading, where different frequency components within the UWB signal can experience different fading characteristics.

As also said in section 3.1 the CIR is given from the formula of $h(t)$. In UWB systems the multipath propagation is represented by the CIR. The amplitude a_k of each multipath component in UWB channels typically follow a log-normal distribution rather than Rayleigh or Rician distributions. This is due to the fine time resolution of UWB signals, which allows individual miltipath components to be resolved more clearly [13]. Since UWB channels exhibit a large number of multipath components, the signal received is a summation of these components, each with different delays and phases. This results in a **fading channel** with **delay spread**, a measure of the spread in arrival times for the multipath components. The delay spread σ_t for UWB is typically larger than for other types of channels, and can be defined as:

$$\sigma_\tau = \sqrt{\sum_{k=0}^{N-1} \alpha_k^2 \tau_k^2 - \left(\sum_{k=0}^{N-1} \alpha_k \tau_k\right)^2} \tag{3.14}$$

N is the number of the multipath component and α_k and τ_k are the amplitude and the delay of the k-th path [28, 29]

A commonly used model to represent UWB channel behavior, especially in indoor environments is the Saleh-Venezuela Model. In this model, multipath components are grouped into clusters of arrivals, with each cluster containing multiple rays. Mathematically this is expressed as :[28]

$$h(t) = \sum_{l=0}^{L-1} \sum_{k=0}^{K-1} \alpha_{l,k} \delta(t - T_l - \tau_{l,k}) \tag{3.15}$$

where, L is the number of clusters, K is the number of rays within each cluster, $\alpha_{l,k}$ is the gain of the k-th array in the l-th cluster, T_l is the delay of the l-th cluster and $\tau_{l,k}$ is the delay of the k-th ray realtive to the l-th cluster arrival time. This model captures both time dispersion (clustered arrivals) and frequency-selective fading effects of UWB channels [30].

3.2 Secrecy Capacity and Secrecy Rate

As discussed in previous chapters in the field of secure wireless communications, the Secrecy Capacity and Secrecy Rate define the limits of data transmission in the presence of potential eavesdroppers. This section builds upon the theoretical frameworks established be Wyner's wiretap model, which first introduced the concept of secrecy capacity in the context of degraded channels, and extends it to fading channels, where channel conditions vary over time. Two primary sources, Barros and Rodrigues [2] on the secrecy capacity of wireless fading channels and Chorti and Poor [12] on helping interferer strategies, are integrated to provide a comprehensive analysis of Secrecy Capacity, practical methods to achieve secrecy, and conditions under which secrecy is maximized. Particularly, the problem setup that we should analyze is depicted in the figure below.

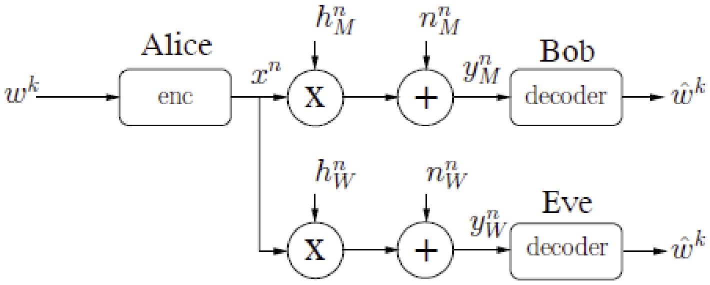


Fig. 3.2 Problem setup of the wiretap channel communication as explained in [2].

In this problem Alice wants to send messages w to Bob. The message block w^k is encoded into codeword $x^n = [x(1), ..., x(i), ..., x(n)]$ to be transmitted over a discrete-time fading channel with output :

$$y_M(i) = h_M(i)x(i) + n_M(i) \tag{3.16}$$

The coefficient $h_M(i)$, also referred to as channel state information (CSI), is independent from the channel output and assumed to be drawn i.i.d according to the probability distribution $p(h_M)$, which is zero-mean complex Gaussian for Rayleigh fading. It should be noted that equation 3.16 represents a narrow-band model, as the equation uses multiplication instead of convolution.

3.2.1 Mathematical Formulations of Secrecy Capacity and Secrecy Rate in the presence of eavesdropper

To understand **Secrecy Capacity** mathematically, we should consider the usual scenario with **Alice**, **Bob**, **Eve** and the main channel in which Alice transmits confidential data to Bob and the wiretap channel in which Eve tries to intercept this data (Figure 3.2). We make an assumption by saying that the channels are subject to quasi-static fading, where the fading coefficients remain constant over a single transmission block. As it is well analyzed in [2] we will go through the analysis of Secrecy Capacity in Additive Gaussian Noise Channels and then in Fading Channels.

For AWGN channels, the C_S is defined as the difference between the capacities of the C_M and the C_W:

$$C_S = max(C_M - C_W, 0) \tag{3.17}$$

where:

$$C_M = \frac{1}{2} log_2 \left(1 + \frac{P}{N_M} \right) \tag{3.18}$$

and

$$C_W = \frac{1}{2} log_2 \left(1 + \frac{P}{N_W} \right) \tag{3.19}$$

Here, P is the transmit power, and N_M, N_W are the noise powers in the main and eavesdropper channels, respectively. When the main channel has a better SNR than the eavesdropper's channel, i.e., $\left(\frac{P}{N_M} > \frac{P}{N_W} \right)$, a positive secrecy capacity exists, enabling secure communication.

Whilst, in fading environments where channel conditions fluctuate, Secrecy Capacity must account for the variations in the channel gain for both the main and eavesdropper channels. Under quasi-static Rayleigh fading, the Secrecy Capacity can be expressed as:

$$C_s = \begin{cases} \log_2(1+\gamma_M) - \log_2(1+\gamma_W), & \text{if } \gamma_M > \gamma_W \\ 0, & \text{otherwise} \end{cases} \tag{3.20}$$

where :

- $\gamma_M = \frac{P|h_M|^2}{N_M}$
- $\gamma_W = \frac{P|h_W|^2}{N_W}$
- h_M and h_W are the fading coefficients for the main and the eavesdropper channels, respectively.

The quasi-static fading condition assumes that h_M and h_W are constant within a transmission block but vary independently across blocks. The C_S becomes positive only when the instantaneous SNR of the C_M exceeds that of the wiretap channel, $\gamma_M > \gamma_W$. Thus, fading can enhance secrecy by occasionally degrading the wiretap channel more than the main one, a phenomenon referred to as **fading-induced secrecy**.

3.2.1.1 Example Calculation

Consider a Rayleigh fading scenario with average SNRs $\bar{\gamma}_M$ and $\bar{\gamma}_W$ for the main and wiretap channel, respectively. The probability of achieving a positive C_s (i.e., $\gamma_M > \gamma_W$) is given by:

$$P(\gamma_M > \gamma_W) = \frac{\bar{\gamma}_M}{\bar{\gamma}_M + \bar{\gamma}_W}$$

If $\bar{\gamma}_M = 10dB$ and $\bar{\gamma}_W = 5dB$, ($\bar{\gamma}_M = 10^1 = 10, \bar{\gamma}_W = 10^{0.5} \simeq 3.16$) then :

$$P(\gamma_M > \gamma_W) = \frac{10}{13.16} \simeq 0.76$$

which means that there is a 76% chance that the main channel SNR exceeds the wiretap's SNR, thereby enabling secure communication.

3.2.2 Conditions in which secrecy is maximized

Maximizing secrecy in wireless channels involves optimizing system parameters to increase the likelihood of secure transmission. Here, we consider factors such as signal jamming and user placement to enhance secrecy capacity.

3.2.2.1 Helping Interferer Strategy

One effective approach is the helping interferer strategy, where a friendly node transmits noise-like interference to degrade the eavesdropper's channel without significantly affecting the main channel. This interference is carefully designed to have a **pmf** similar to the actual data signal, ensuring minimal impact on the legitimate receiver while maximizing confusion at the eavesdropper's end. For example, in a Binary Phase Shift Keying (BPSK) system with a helping interferer, the bit error rate (BER) at the eavesdropper can be expressed as [12] :

$$P_b = \frac{1}{2}\,\mathrm{erfc}\left(\frac{d_{\min}/2}{\sqrt{2(\sigma_i+\sigma_n)}}\right) \tag{3.21}$$

d_{min} is the minimum distance in the BPSK constellation, σ_ι and σ_n are the noise variances due to interference and the channel, respectively. The effectiveness of this strategy is enhanced in low and medium SNR schemes, where the presence of a carefully constructed jamming signal significantly increases the eavesdropper's BER, thereby protecting the confidentiality of the transmission.

3.2.2.2 Optimal Power Allocation

Another condition to maximize secrecy involves optimal power allocation between the data signal and the jamming signal. If the transmit power budget **P** is split optimal between the data and interference signals, the R_S can be maximized. The R_s in the presence of interference is given by :

$$R_s = \left(\log_2\left(1+\frac{P_d|h_M|^2}{N_M}\right) - \log_2\left(1+\frac{P_i|h_W|^2}{N_W}\right)\right)^+ \tag{3.22}$$

(P_d, P_i, powers allocated to data and interference respectively). Finally, $(.)^+$ denotes the positive part function ensuring that R_S is non-negative.

3.2.3 Outage Secrecy Capacity

In fading channels, the secrecy rate may vary due to fluctuations in channel quality. Outage secrecy capacity quantifies the highest secrecy rate achievable with a probability that the rate falls below a target value. This concept, introduced by Barros and Rodrigues [2], defines the probability of an outage, where the C_S drops below a target rate R_s:

$$P_{out}(R_S) = P(C_s < R_s) \tag{3.23}$$

By adjusting R_s and power allocation, it is possible to balance between the desired R_s and the tolerable P_{out}, achieving a robust level of security even in adverse fading conditions.

Chapter 4

Measurements Methodology

This chapter provides a comprehensive outline of the methodology used for channel measurements in UWB systems using a specific radio module, covering the setup, procedures, and data processing steps necessary for obtaining accurate channel characteristics. The measurements in this study were performed with Humatics P442 UWB radios and BroadSpec™ antennas. Various aspects, such as antenna performance and calibration, are detailed to ensure replicability and reliability.

4.1 Channel Measurements Setup

In this section, we discuss the overall setup used for the UWB channel measurements, including descriptions of the equipment and environment, measurement procedures, the antenna measurement and calibration, and the data collection to be processed. The setup of the equipment used is depicted in the figure below:

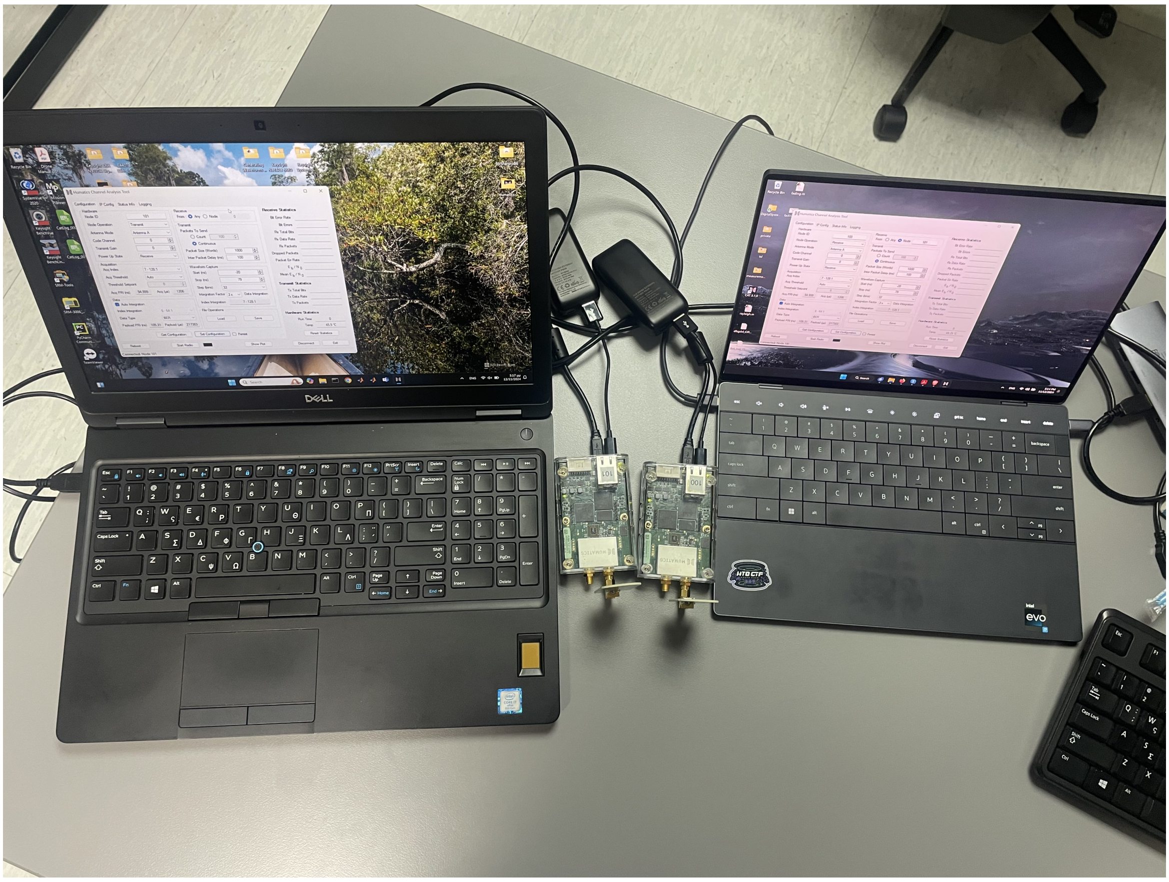


Fig. 4.1 Picture of the setup environment and the control software provided by Humatics [3].

4.1.1 Description of UWB Radios used

The Humatics P442 UWB radio module forms the core of the channel measurement setup, providing a versatile and robust platform for UWB signal transmission and reception. This module, part of the P4xx series, is designed to operate across a frequency range of 3.4 to 4.8 GHz with a central focus on high-precision distance and positioning measurements. Here, we will explore the radio's capabilities, configuration, and transmission characteristics in detail.

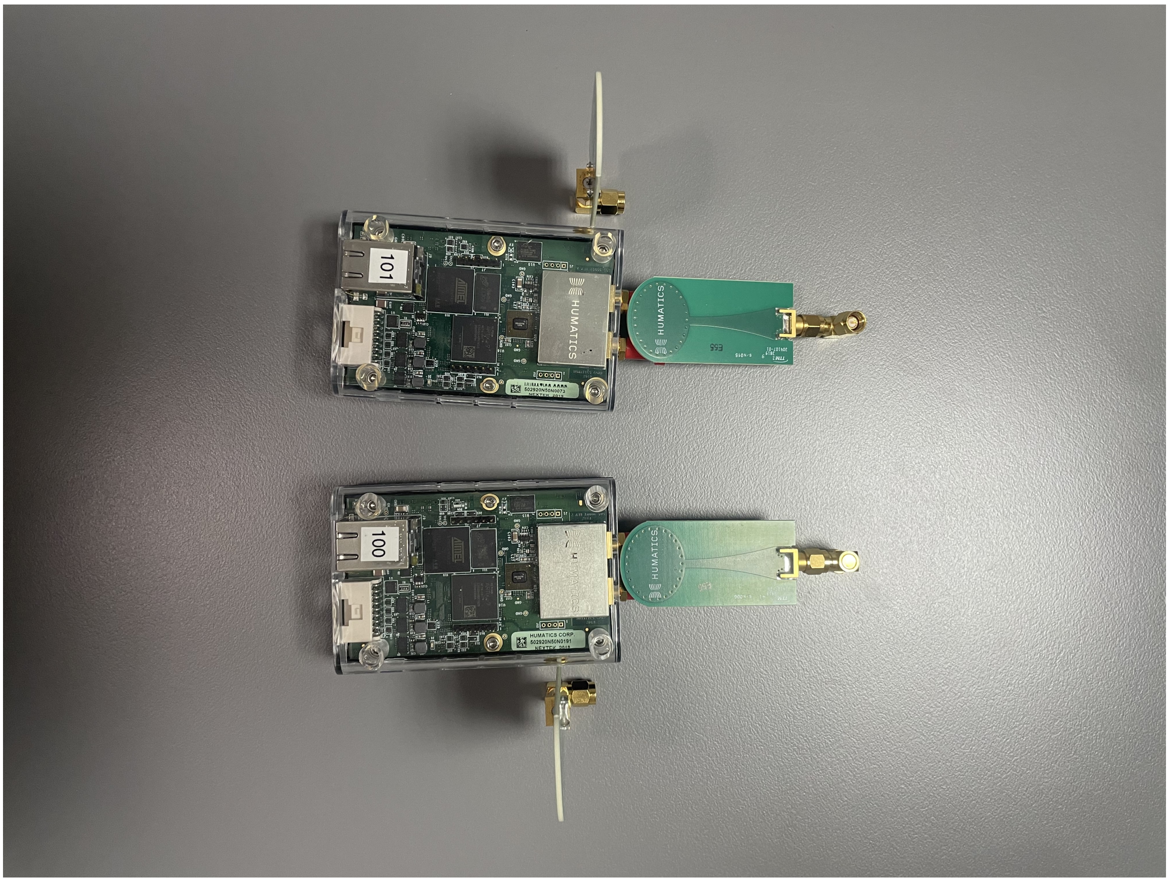


Fig. 4.2 Picture of the radio modules (Tx and Rx) and their antennas.

4.1.1.1 Overview of Transmission Capabilities

The Time Domain P442 radio is capable of transmitting UWB pulses with adjustable power levels. The radio operates within the power limits specified by the FCC and ETSI for UWB devices [31], ensuring compliance across indoor and outdoor environments. It can emit up to approximately -14.5 dBm per MHz, making it suitable for various applications that require accurate short-range measurements and minimal interference with other narrowband communications. This module supports a range of transmission settings, allowing users to adjust parameters such as the pulse repetition frequency (PRF) and transmission power, which are critical in configuring the system to balance range, accuracy, and power consumption. The transmitted pulse repetition rate is 10.1 MHz. There is no need for physical synchronization between the transmitter and the receiver. A rake receiver is used for collection of MPCs at the receiver with an adjustable sampling rate. To group up everything that was referred, the measurement process of the module follows these primary steps:

1. Transmission of Pulses: It emits ultra-short pulses that travel from Tx antenna to the Rx antenna. These pulses are transmitted at regular intervals (Pulse Repetition Rate), which can be set depending on the desired measurement frequency and environment.

2. Reception and Sampling: At the Rx, the signal is captured and sampled using a rake receiver configuration, which collects and aligns multiple signal components that may have taken different paths.

3. Time-of-Flight Measurements: The Rx calculates the ToF of each pulse, leveraging the high resolution of UWB signals to achieve accurate distance measurements with up to centimeter-level precision. This ToF data is then used in further analyses to derive channel characteristics, such as PL.

4.1.2 Description of the Antennas and calibrated measurement

The P442 module uses the Broadspec™ antenna, a wideband antenna designed to operate effectively across the 3.1 to 5.3 GHz frequency range, which aligns with the ultra-wideband (UWB) spectrum utilized by the device. This antenna features a nominal impedance of 50 ohms and provides linear polarization. Its radiation pattern in the azimuth plane is nearly omnidirectional, offering uniform coverage around the antenna with minimal signal strength variation. In the elevation plane, the antenna exhibits a dipole-like pattern, meaning the signal strength varies with the elevation angle, typically being strongest perpendicular to the antenna axis. With a nominal gain of approximately 3 dBi, this antenna contributes to effective signal propagation for short-range communication and precise ranging applications. Its design makes it well-suited for the P442's operations in high-resolution distance measurements and radar sensing, providing reliable performance in various environments. The antenna got measured in a Keysight N5221A VNA with proper calibration, to check it's characteristics such as S11 pattern. This step is not mandatory but still is crucial for minimizing measurement errors and ensure that antenna performance aligns with the system's design specification.

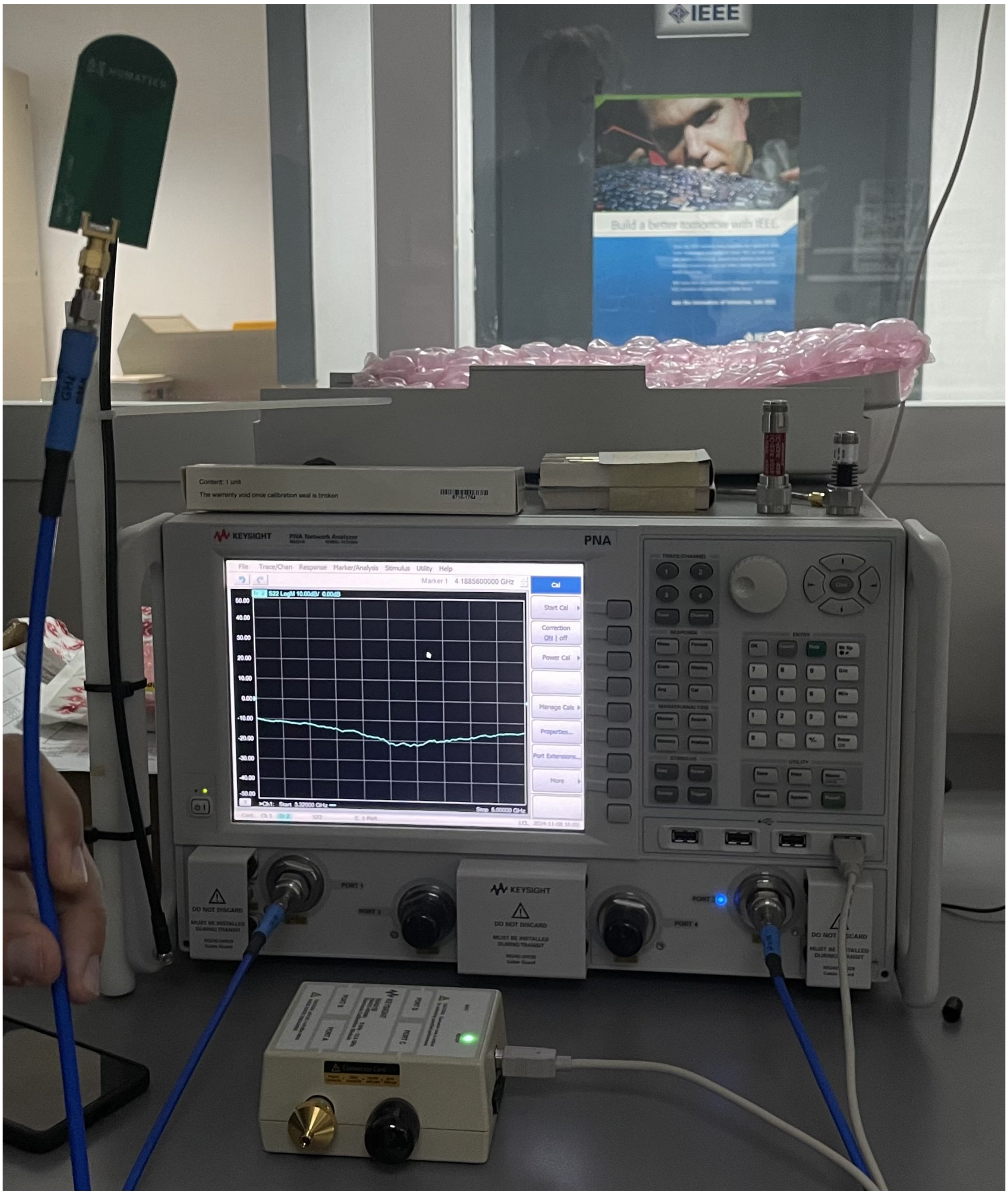


Fig. 4.3 Antenna Measurement and Calibration with Keysight N5221A VNA.

In the figure below it's a clear plot of the S_{11} parameters of the antenna in it's wide range of operation. The antenna seems to have an excellent behavior in the whole range and it confirms its ultra-wide BW, which is greater than 2.5GHz measured measured at -10dB< .

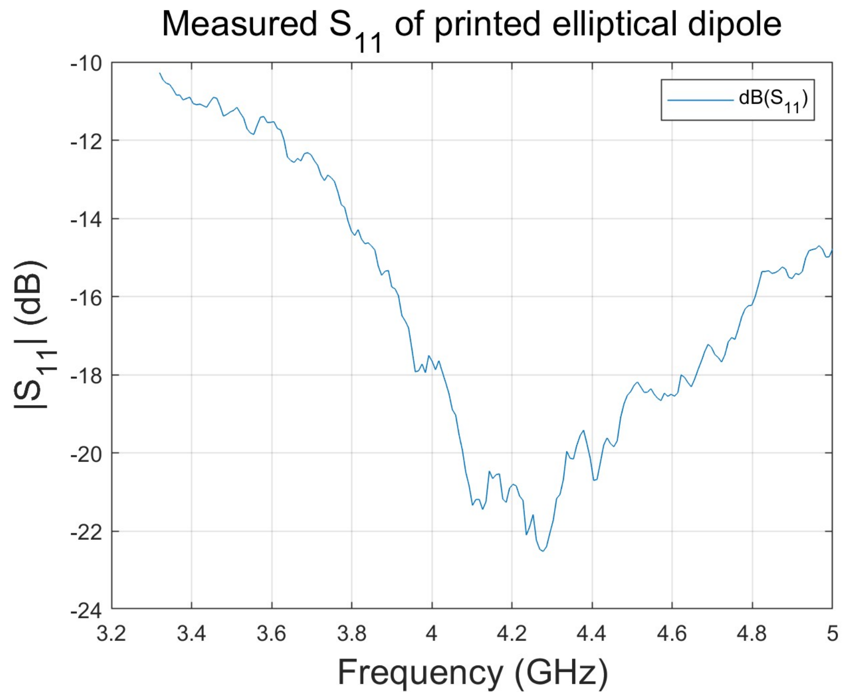


Fig. 4.4 Plot of the S-parameters from the calibrated antenna measurements.

4.1.3 Measurement Environment

The measurements were conducted in both indoor and outdoor environments to capture a wide range of scenarios:

- Indoor: Measurements were taken in controlled lab environments, where conditions allowed for both LOS and NLOS paths

- Outdoor: Tests in open areas enabled long-rage measurements under dynamic environment, facilitating analysis of enviromental impacts on signal attenuation and delay.

The selection of both LOS and NLOS scenarios is critical to understanding how physical obstructions and multi-path reflections influence signal behavior in UWB channels. In particular, the impact of signal reflections and diffractions is more pronounced in indoor environments with walls and metallic objects, while outdoor measurements emphasize the effect of distance and open-space fading.

4.1.4 Measurement Procedure

The measurement procedure is divided into two main steps: equipment setup and data acquisition.

1. Equipment Setup: The P442 modules were configured through the CAT software interface, where key parameters such as transmission power, integration index, and antenna configurations were adjusted. The BroadSpec™ antennas were mounted at specific heights and orientations, optimized according to the guidelines provided in the user documentation [3].

2. Data Acquisition: Once the setup was complete, measurements were conducted by logging the channel impulse responses using the CAT software. Data was collected in CSV format for ease of processing in software such as MATLAB.

3. Data post-processing: After the collection of the data, MATLAB scripts provided by Humatics were used to calculate and plot CIR, by implementing the CLEAN algorithm [32].

4.1.5 Data Post Processing

The CLEAN algorithm is a signal processing technique commonly used in applications such as radar, and UWB systems, to resolve MPCs in time-domain or frequency-domain measurements. It deconvolves the received signal with a known transmitted waveform (template) to identify and separate individual MPCs, which are typically closely spaced in time and overlapping due to the channel's multipath nature. It iteratively refines the received signal by identifying and subtracting the dominant contributions of MPCs.

For example let's consider a received signal which contains contributions from MPCs, $r(t)$ and a template signal as reference, $p(t)$. Basically to detect the MPCs it performs cross-correlation between the two signals :

$$\rho(\tau) = \int r(t)p(t-\tau)\,dt \tag{4.1}$$

Then, you estimate the strongest MPC, which is the one with the largest peak and it's characterized by its amplitude A_k and delay τ_k. After estimating it, we subtract it from the template as : $m_k(t) = A_k p(t-\tau_k)$ and we create the new received signal: $r'(t) = r(t) - m_k(t)$. The algorithm outputs a list of MPCs, characterized by the amplitude, delay, and potentially its phase.

These parameters are used to construct a Power Delay Profile (PDP) or a detailed CIR :

$$h(t) = \sum_{k=0}^{N-1} A_k \delta(t - \tau_k) \tag{4.2}$$

4.2 Secrecy Calculations

The last step for the desired results is to calculate the Secrecy Metrics. For this step, we need to design an algorithm which will be consisted of several steps and will eventually calculate the Secrecy Capacity and Secrecy Rate for every scenario. The steps of the algorithm are described below :

1. **Input Channel Data**

   Load the CIR data from measurements, to the post processing scripts for both the main and the wiretap channels.

2. **Extract Channel Parameters**

   Compute the received power P_r using the PL and fading coefficients.

   Calculate the noise power N based on the measurement environment.

3. **Compute SNR**

   For the main channel γ_M.

   For the wiretap channel γ_W.

4. **Calculate Secrecy Metrics**

   Compute C_M, C_W, C_S from the formulas given in chapter 3.2.1.

   Evaluate the secrecy rate R_S.

5. **Output Results**

   Generate plots depicting the Capacities and achievable Rate.

For our ease, Humatics software computes directly the instantaneous SNR and so we are able to calculate the total average SNR for all the snapshots, without extracting the needed Channel Parameters.

Chapter 5

Results and Analysis

5.1 Measurement Scenarios

As mentioned previously, the channel measurements will take place both on indoor and outdoor environments. For each one of the scenarios schematic figures are provided that map the territory in which the measurements take place and realistic photos that depict the placement of the equipment, are given.

5.2 Indoor Scenario

To start with, the indoor measurements took place in a controlled laboratory environment, specifically in Telecommunication Systems Laboratory at University of Piraeus, Piraeus, Greece. The first measurement scenario is a simple one, in which Alice and Bob are in the same room and Eve is located near, but outside of the room so there is a wall in between Alice and Eve. First scenario is depicted in a schematic form in figure 5.1.

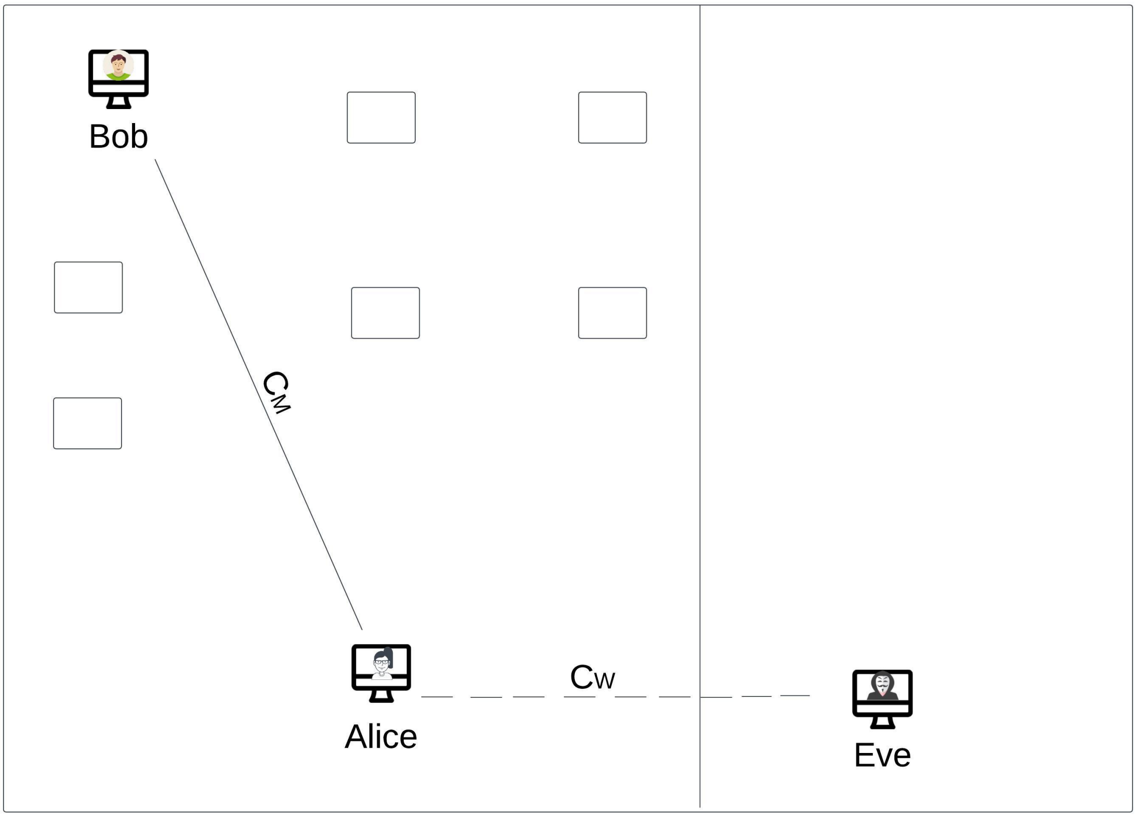


Fig. 5.1 Depiction of the first scenario.

In between the 2 parties (Alice and Bob) there are some objects which contribute to the propagation and affect the channel conditions but generally this case is considered ideal, and for an office environment is considered a LoS connection. The distance between Alice and Bob (d_M) is approximately 6 meters and the distance between Alice and Eve (d_W) is approximately 3 meters. In the figures 5.2 and 5.3 it is depicted the real positions of Alice, Bob, and Eve while conducting the measurement experiment.

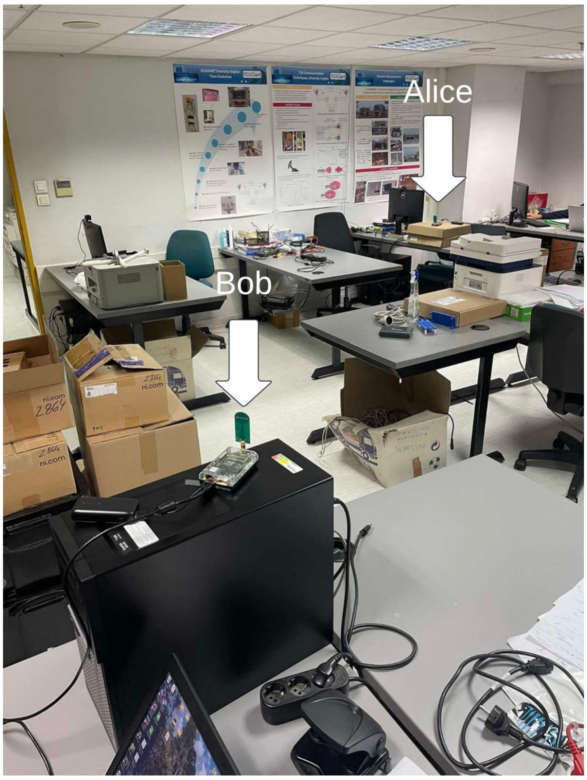


Fig. 5.2 Alice and Bob Positions.

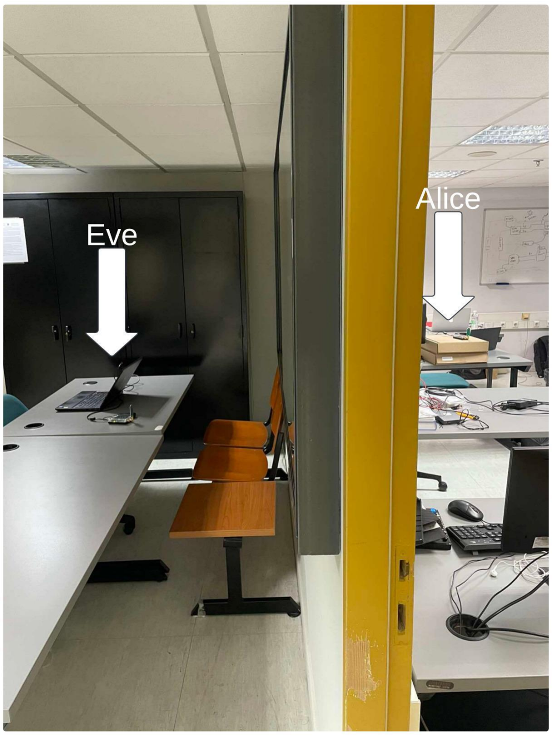


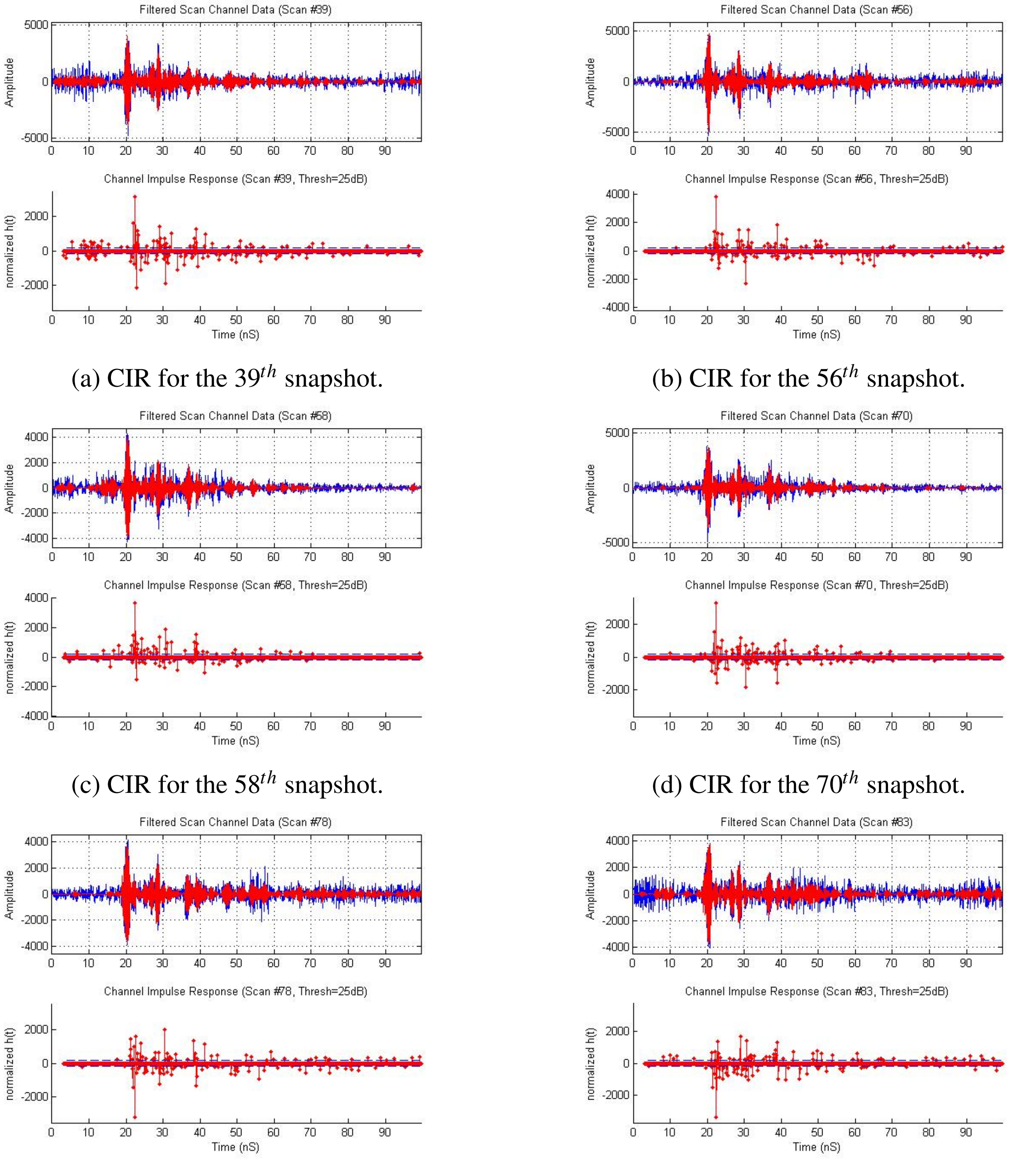
Fig. 5.3 Alice and Eve Positions.

All of the three users in this scenario are static, so the distances do not change. Here the goal is to evaluate the Secrecy that is achieved in the communication of Alice and Bob, through the metrics that were analyzed in previous chapters.

5.2.1 Channel Characteristics and Secrecy Calculation

The channel characteristics for the indoor measurement scenario are evaluated based on the metrics derived from the CIR data. The primary focus is on the RMS Delay Spread, Mean Delay, and Excess Delay, which quantify the temporal dispersion of the channel. Additionally, the Power Delay Profile is provided.

To start with, we need to present the CIR results we retrieved from the CLEAN algorithm. Below there are two figures of the CIRs one for the C_M and the other for the C_W respectively. During the measurements through the CAT software several snapshots of the channels were taken and analyzed, so below there are depicted some snapshots for the C_M and C_W respectively.



(a) CIR for the 39^{th} snapshot.

(b) CIR for the 56^{th} snapshot.

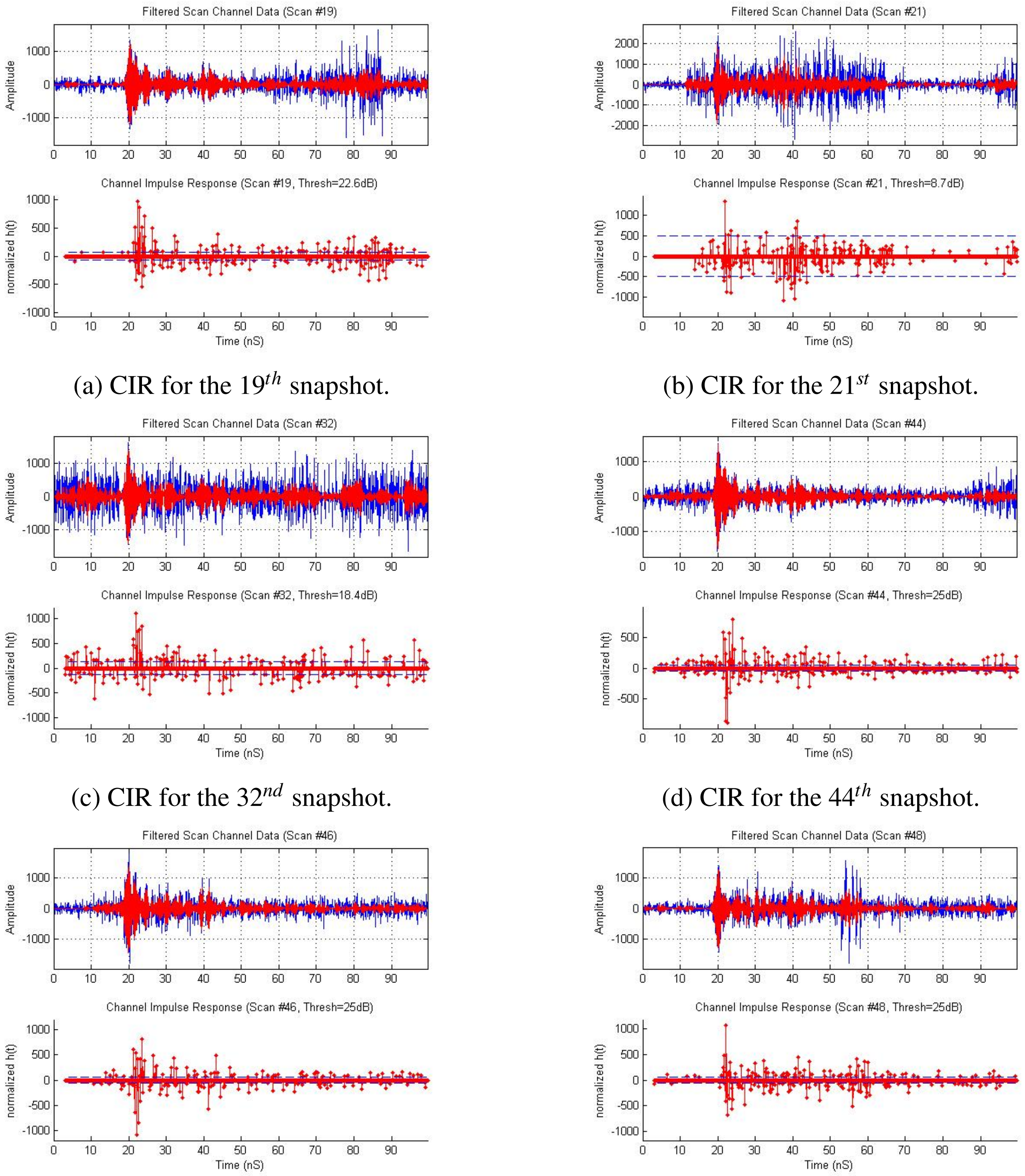
(c) CIR for the 58^{th} snapshot.

(d) CIR for the 70^{th} snapshot.

(e) CIR for the 78^{th} snapshot.

(f) CIR for the 83^{rd} snapshot.

Fig. 5.4 Channel Impulse Response for some snapshots of the C_M.



(a) CIR for the 19^{th} snapshot.

(b) CIR for the 21^{st} snapshot.

(c) CIR for the 32^{nd} snapshot.

(d) CIR for the 44^{th} snapshot.

(e) CIR for the 46^{th} snapshot.

(f) CIR for the 48^{th} snapshot.

Fig. 5.5 Channel Impulse Response for some snapshots of the C_W.

Figure 5.4 shows the normalized amplitude of the raw received pulses in blue. The waveforms in red are the reconstructed ones by convolving the CIR with the template waveform (Figure 5.6). The second histogram in Figure 5.4 is the CIR of the received waveform obtained by performing deconvolution of the received waveform with the template waveform. The dashed blue lines show the threshold that is being set at 10% of input signal, where all CIR samples below the threshold are discarded. The same apply to the results depicted in fig. 5.5.

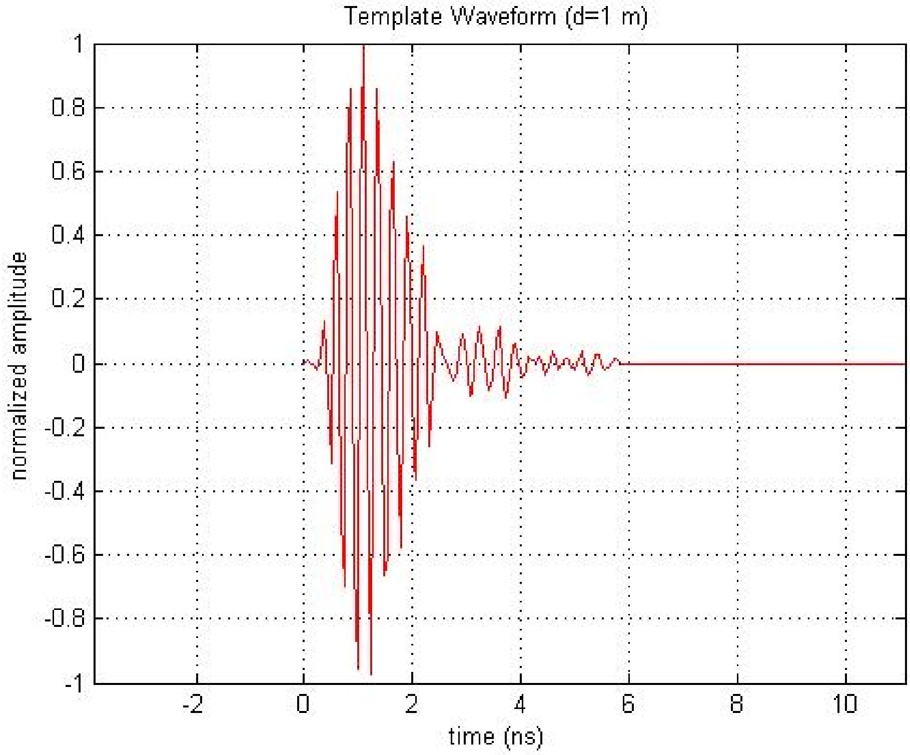


Fig. 5.6 Template Waveform used in C_W and C_M.

5.2.1.1 Power Delay Profile

The Power Delay Profile (PDP) characterizes the temporal distribution of signal power received through multiple propagation paths (multipath components) at the receiver. It provides insights into how the power of the signal is distributed over time delays caused by multipath reflections, diffractions, and scattering.

The PDP is derived from the CIR and represents the squared magnitude of the CIR values at different time delays. Mathematically, the PDP can be expressed as:

$$PDP(t) = |CIR(t)|^2 \tag{5.1}$$

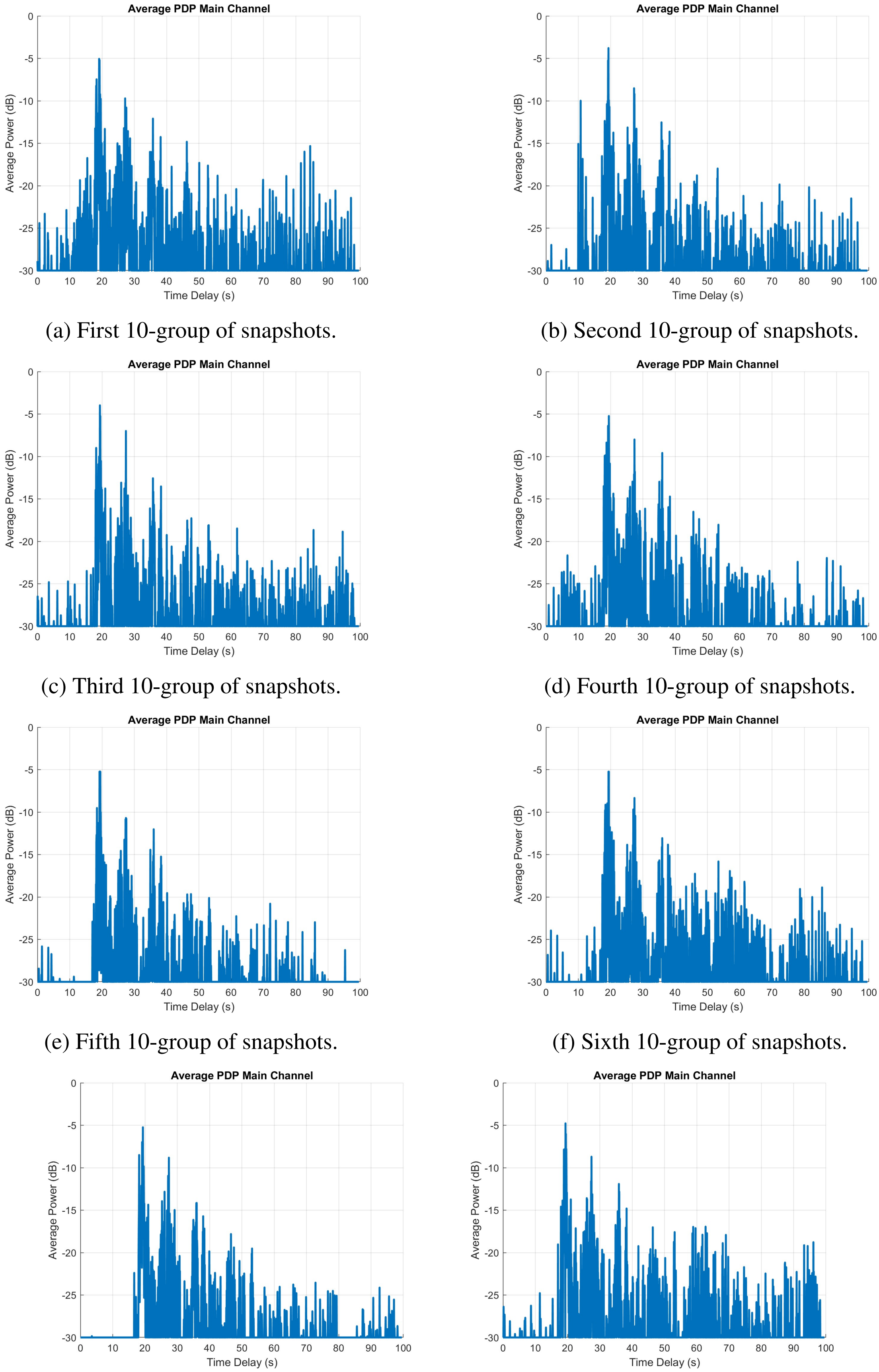
Here :

- t: Time delay (in nanoseconds).
- $CIR(t)$: Amplitude of the CIR at a given time delay.

The PDP is computed by squaring the amplitude of the CIR for each time bin:

1. Extract the CIR data for a specific scan.
2. Square the absolute values of the CIR to compute power at each time delay.
3. Normalize the PDP to its maximum value for visualization.

Below are the PDP plots for the Main Channel. The PDPs shown below are calculated as an average of a group of 10 snapshots.



(a) First 10-group of snapshots.

(b) Second 10-group of snapshots.

(c) Third 10-group of snapshots.

(d) Fourth 10-group of snapshots.

(e) Fifth 10-group of snapshots.

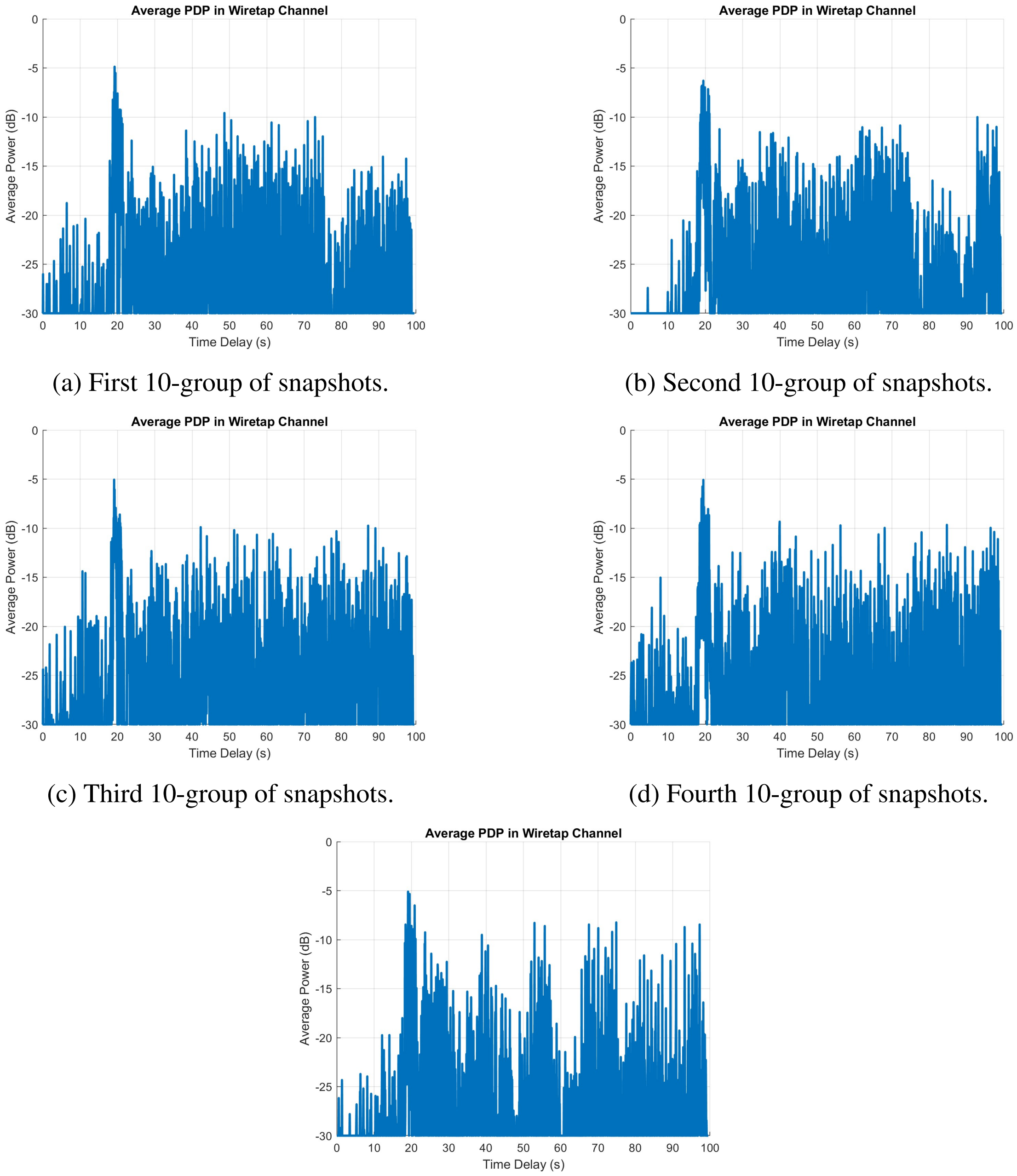
(f) Sixth 10-group of snapshots.

(g) Seventh 10-group of snapshots.

(h) Eighth 10-group of snapshots.

Fig. 5.7 Power Delay Profile (PDP) in group of 10 snapshots for each PDP plot. Each plot shows the power in dB as a function of time delay (ns).

Same for the Wiretap Channel:



(a) First 10-group of snapshots.

(b) Second 10-group of snapshots.

(c) Third 10-group of snapshots.

(d) Fourth 10-group of snapshots.

(e) Fifth 10-group of snapshots.

Fig. 5.8 Power Delay Profile (PDP) in group of 10 snapshots for each PDP plot. Each plot shows the power in dB as a function of time delay (ns).

These PDPs reveal the multipath propagation characteristics of the channel under observation. Each plot shows several prominent peaks at specific time delays, corresponding to the strong multipath components (siganl reflections) arriving at the receiver. These peaks indicate the presence of reflectors or scatterers in the environment, which produce significant delayed copies of the transmitted signal. These peaks close to 0 ns likely represent the LoS component (for example at the C_M), while peaks at larger time delays correspond to reflections from obstacles further away. Moreover, it's significant to note that the distribution of peaks over time delay suggests the time dispersion of the channel. In some plots , such as Figure 5.7 a, b, these peaks are clustered towards the start of the time axis, indicating fewer significant multipath reflections and a more concentrated energy profile. On the other hand, other plots show a wider spread of peaks, indicating increased multipath propagation and reflections arriving over a larger delay spread. The power of the delayed signal components decreases with time, which is a typical behavior in multipath channels. The signal strength diminishes as the delay increases due to longer travel paths, greater attenuation, and reflection losses.

5.2.1.2 Main Channel Delay Spread Analysis

In this section, we evaluate the delay spread characteristics of the indoor channel scenario. The delay spread analysis provides insights into the temporal dispersion of the signal as it propagates through the environment, influenced by multipath propagation due to the reflective surfaces and obstacles in the laboratory. To perform a Delay Spread Analysis, a statistical analysis was performed over all snapshots by generating generating histograms (fig. 5.9) for each delay spread metric to visualize the distribution of delay values and plotted the CDF .

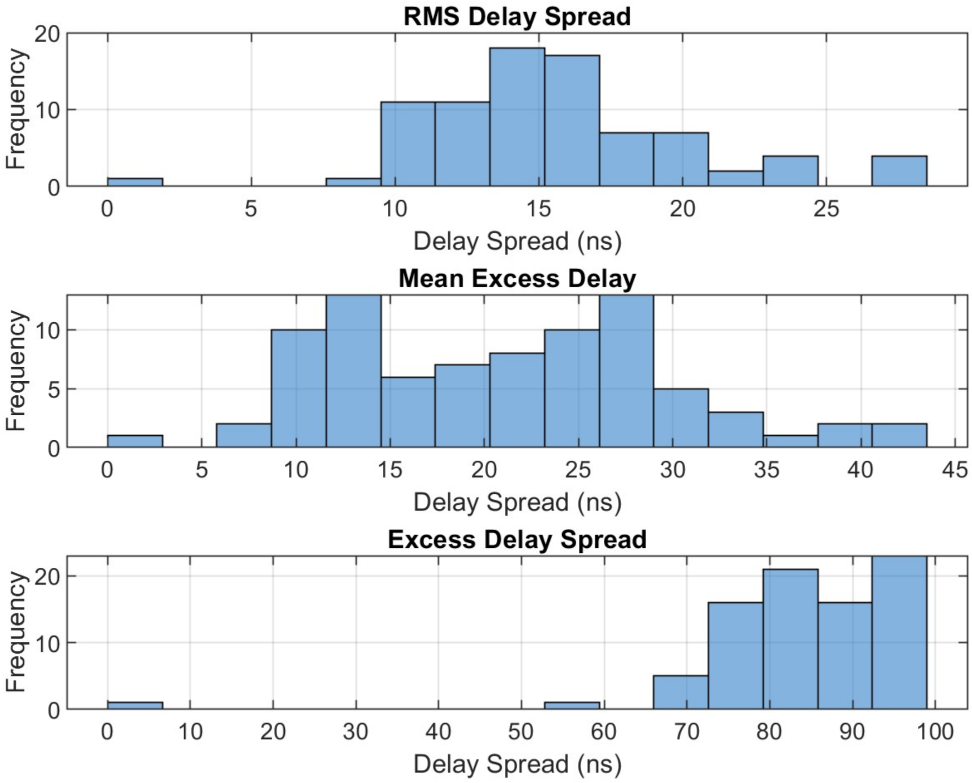


Fig. 5.9 Statistical Delay Spread Analysis for the C_M.

Above we can see the generated histograms for each metric, RMS , Mean Excess and Excess Delay Spread. Here, it should be mentioned that the y-axis labeling "Frequency" corresponds to the statistical meaning of frequency which is **Number of Ocurrences** and it should not be confused with the actual frequency in which the system operates.

Excess Delay

The Excess Delay, measures the delay relative to the first arriving component. It quantifies how far the multipath components are spread out in time beyond the main (first) signal arrival. In this case it is observed that most values are concentrated between 70 and 100 ns, with significant peaks around 90 ns and 100 ns. Very few values fall below 70 ns, and there is a notable gap between 0 and 60 ns. All in all, a high excess delay spread shows **a highly dispersive channel** where many reflected paths arrive well after the direct path, and this is typical in environments with significant scattering, such as urban or indoor areas with multiple obstacles causing reflection.

To calculate the Excess Delay Spread you need to:

- Obtain the PDP.
- Determine the threshold for significant power (apply a noise floor, so as to ignore noise or weak multipaths).
- Find the minimum and maximum delays , $\tau_{\text{min}}, \tau_{\text{max}}$.
- Subtract the two delays as : $\tau_{\text{max}} - \tau_{\text{min}}$.

From table 5.1 we see the analytical statistic analysis. In the Excess Delay Spread the mean value is equal to 84.35 ns which indicates the highly dispersive channel and confirms rich multipath propagation. The median value of 84.50 ns is very close to the mean, suggesting that the distribution of excess delay spread values is fairly symmetric, so no extreme outliers dominte the data measurements. Finally, the standard deviation is equal to 12.82 ns, which indicates moderate variability in the excess delay spread. The mean and median may be around 84 ns but some snapshots exhibit slightly lower or higher values, which can be caused by dynamic changes in the propagation enviroment.

Mean Excess Delay

The Mean Excess Delay represents the average time of arrival of the multipath components weighted by their power. It gives insight into the "center of mass" of the PDP. It is observed that the values are concentrated in the range of 10 to 30 ns, with a peak around 25 ns. This means that the channel seems to have moderate multipath propagation, where significant reflected components take some time to arrive but are not excessively delayed. This result can be easily verified from the mean and median values of Table 5.1 and also we can understand that the significant multipath components arrive with a delay of approximately 21 ns relative to the first arriving path. Mathematically Mean Excess Delay is given by [25] :

$$\overline{\tau} = \frac{\sum_i \tau_i P(\tau_i)}{\sum_i P(\tau_i)} \tag{5.2}$$

where ,

- τ_i : The delay of the *i*-th multipath component.
- $P(\tau_i)$: Power of the received signal at delay τ_i.

RMS Delay Spread

The Root Mean Square (RMS) Delay Spread quantifies the spread of signal energy in time and is a critical parameter for understanding the channel's multipath nature [21]. As observed in the results in Figure 5.9, most values of RMS delay spread are concentrated between 10 ns and 20 ns , a few values fall below 10 ns and above 20 ns, but these are less frequent, this suggests that, for most scans, the channel's energy is relatively concentrated, with moderate time dispersion. Important step to fully understand this analysis is to interpret these observations. A low RMS delay spread indicates a **non-dispersive channel** where most of the signal energy arrives within a short time. Higher values (e.g., near 25 ns) suggest the presence of stronger multipath components with delays farther from the main arrival time. Generally, RMS delay spread, symbolized as τ_{RMS} is defined as the mean square of the delay values relative to the mean excess delay, mathematically [25]:

$$\tau_{\text{RMS}} = \sqrt{\overline{\tau^2} - (\overline{\tau})^2} \tag{5.3}$$

where,

- $\overline{\tau^2}$ is the second moment of the delay spread.
- $\overline{\tau}$ is the mean excess delay (the first moment).

From the values of the Statistical Delay Spread Analysis below, there are the values of Mean RMS 15.67 ns , Median value 15.2 and Standard Deviation of 4.74 ns. The information that can be extracted from these values are, that the signal energy in the channel is dispersed across approximately 15.67 ns, which indicates that most of the received signal energy is arriving within a short time window.

Table 5.1 Statistical Delay Spread Analysis.

Metric	Mean (ns)	Median (ns)	Standard Deviation (ns)
RMS Delay Spread	15.67	15.20	4.74
Mean Excess Delay	20.96	21.40	8.80
Excess Delay Spread	84.35	84.50	12.82

In Figure 5.10 , the cumulative distribution functions (CDFs) of the delay spread metrics illustrate how the RMS delay spread, mean excess delay, and excess delay spread are distributed across the measured snapshots. The curve rises gradually, indicating a smooth distribution and confirming that the signal power is largely concentrated around a short time window, as previously observed. In the second plot, the mean excess delay seems to have a relatively uniform distribution. The CDF rises steadily, showing that most of the power-weighted delays are concentrated between 20 ns and 30 ns. The third plot shows the excess delay spread, which has a distinct behavior compared to the other two metrics. The excess delay spread ranges from approximately 60 ns to 100 ns, with a sharp rise in the CDF starting at 70 ns and plateauing around 100 ns. This behavior highlights the presence of weak but significantly delayed multipath components that extend the temporal spread of the signal. While the RMS and mean excess delay spreads show a more compact distribution, the excess delay spread reveals a highly dispersive nature of the channel when considering late-arriving reflections.

Together, these plots reinforce the earlier observations: the channel exhibits limited dispersion for stronger components (small RMS delay spread), while the presence of delayed weaker components (large excess delay spread) significantly increases the overall temporal dispersion.

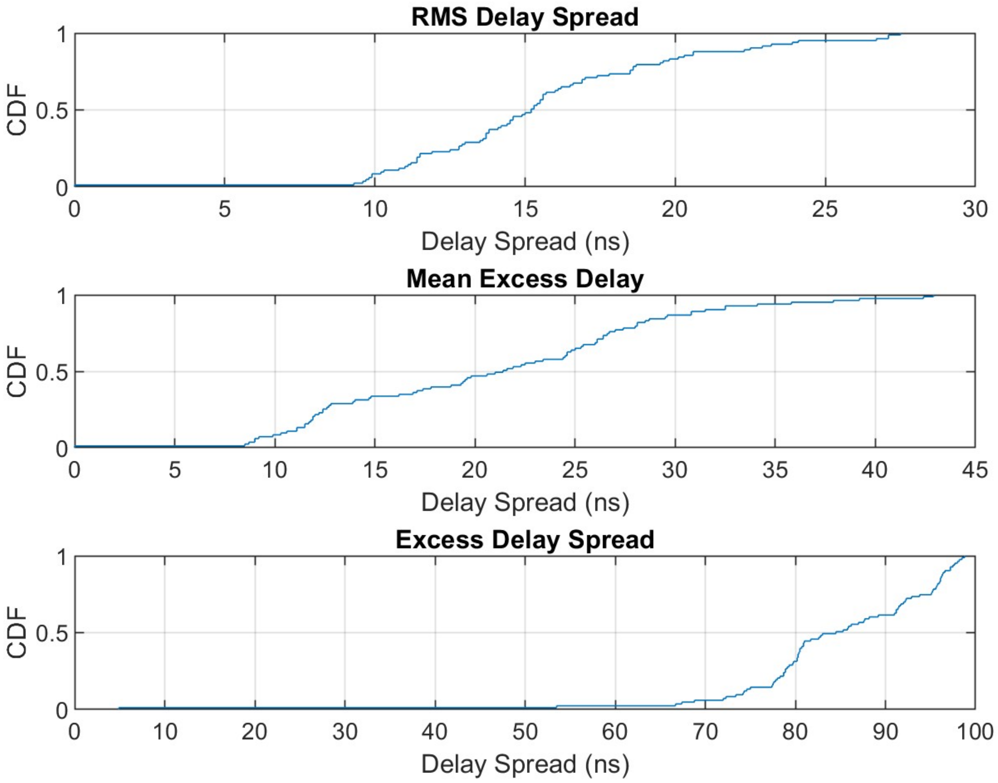


Fig. 5.10 Cumulative Density Functions C_M.

5.2.1.3 Wiretap Channel Delay Spread Analysis

In this section, as also previously analyzed, we will perform Channel Delay Spread Analysis for the C_W. Reminder that in this case Eve may be located nearer to Alice but a wall is separating them, so there is no LoS link between them.

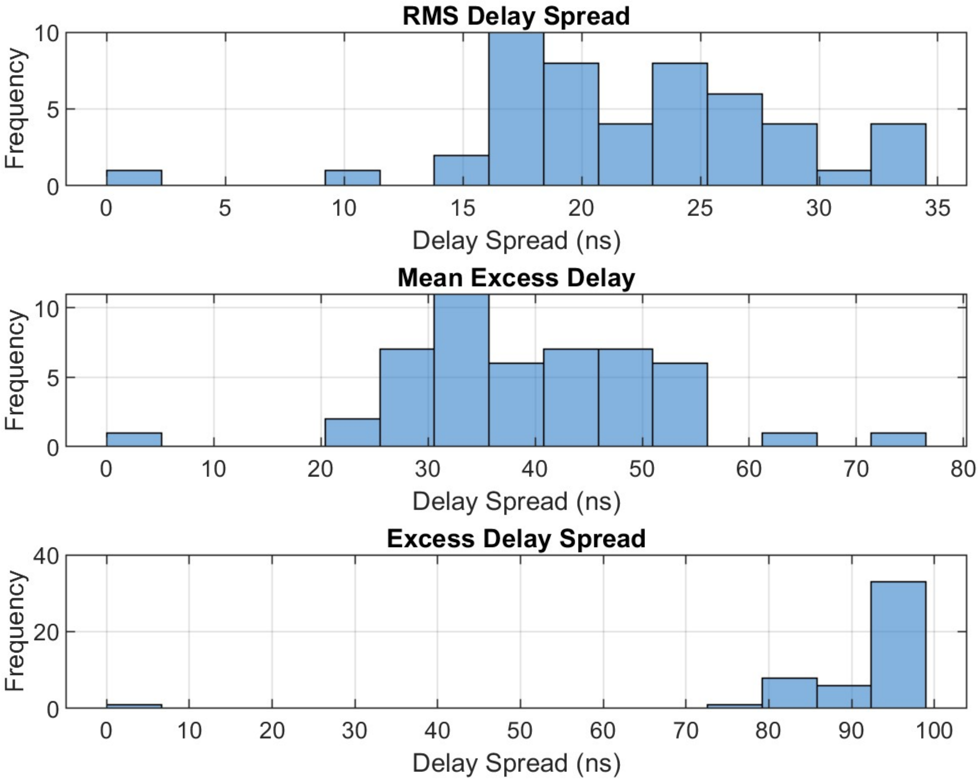


Fig. 5.11 Statistical Delay Spread Analysis for the C_W.

The analysis of the RMS delay spread, mean excess delay, and excess delay spread, as presented in the histograms (Figure 5.11) and statistical summary table (Table 5.2), provides a comprehensive understanding of the channel's temporal dispersion. The RMS delay spread, with a mean of 22.11 ns, a median of 21.20 ns, and a standard deviation of 6.37 ns, indicates that most of the signal power is concentrated around a relatively narrow time window, as reflected by the histogram where the majority of values lie between 15 ns and 30 ns. This suggests that the channel exhibits moderate time dispersion for the stronger multipath components. In contrast, the mean excess delay shows a higher average value of 39.62 ns, with a larger spread as demonstrated by the standard deviation of 12.23 ns. The corresponding histogram highlights that the mean excess delay values are more widely distributed, ranging between 20 ns and 60 ns, indicating that significant portions of the signal power arrive with moderate delays relative to the first path. The excess delay spread further emphasizes the dispersive nature of the channel, with a mean of 91.10 ns, a median of 96.00 ns, and a standard deviation of 14.20 ns. The histogram for the excess delay spread shows a significant concentration of values at the upper range, between 90 ns and 100 ns, which reflects the presence of weak but highly delayed multipath components that extend the overall temporal spread. These results suggest that while the main signal power arrives within a moderate window, the overall channel exhibits a highly dispersive nature due to late-arriving multipath components, which is a typical characteristic of rich multipath environments in UWB systems, in indoor environments with multiple scatterers.

Table 5.2 Statistical Analysis of Delay Spread Metrics for Wiretap Channel.

Metric	**Mean (ns)**	**Median (ns)**	**Standard Deviation (ns)**
RMS Delay Spread	22.11	21.20	6.37
Mean Excess Delay	39.62	38.40	12.23
Excess Delay Spread	91.10	96.00	14.20

In Figure 5.12 are depicted the CDF plots for the RMS, Mean Excess and Excess delay spread. Also here, like in the histogram, we can understand from the distribution the signal energy is contained to a narrow range between 15 ns and 30 ns. While the mean excess delay and excess delay confirm the outcomes of the high dispersion and the late arriving multipath components.

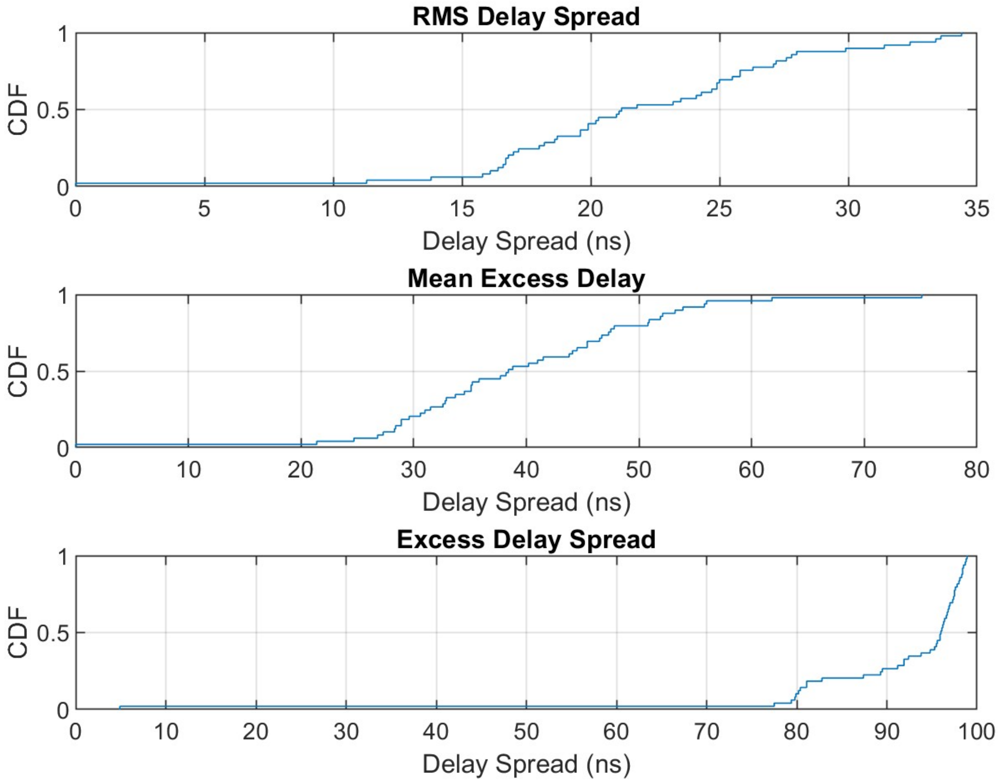


Fig. 5.12 Cumulative Density Functions C_W.

5.2.1.4 Secrecy Metrics

After analyzing the channel characteristics and giving a clear view of the channel situation, the next step is to calculate the needed Secrecy Metrics so as to estimate the achievable existing secrecy. We shall start with the calculation of the Secrecy Capacity, $\mathbf{C_S}$, but first it's mandatory to calculate the two Channel Capacities ($\mathbf{C_M}$, $\mathbf{C_W}$) independently. As explained in equations (3.17)-(3.20) the Secrecy Capacity is the difference between the main's channel capacity and wiretap's channel capacity. And from equations (3.18), (3.19) and (3.20) we can determine the γ_M and γ_W, which are the corresponding SNRs. The logging capability of UWB's kit has the opportunity of offering real time E_b/N_0 and also calculate and log the Linear SNR for each snapshot of the channel measurement. So, in such case the calculation of the Channel Capacity is quite simple. Each given value of linear SNR is the instantaneous SNR, so by summing and dividing with the total number of snapshot we should get the average SNR value of the channel. In other words :

$$\overline{\gamma}_{M,W} = \frac{\sum_{i=1}^{N} \gamma_{M,W|i}}{N} \tag{5.4}$$

N is the total number of the captured snapshots. From this formula (5.4) the average SNR at the transmitter and at the receiver respectively is calculated as :

- $\overline{\gamma}_M$ = 21 dB
- $\overline{\gamma}_W$ = 16 dB

And now we can easily calculate the capacities :

$$C_S = C_M - C_W \Rightarrow B * log_2(1 + \overline{\gamma}_M) - B * log_2(1 + \overline{\gamma}_W)$$

For $B = 1.4$ GHz we calculate the capacities as :

$$C_M \approx 9.78 \text{ Gbps}$$

$$C_W \approx 7.49 \text{ Gbps}$$

Finally the available Secrecy Capacity is equal to :

$$C_S = 9.78 - 7.49 = 2.29 \text{ Gbps} \tag{5.5}$$

The calculated Secrecy Capacity of 2.29 Gbps indicates that secure communication is achievable at this rate, ensuring confidentiality against eavesdropping, as also proven in [2] . This result demonstrates the advantage of the legitimate receiver's channel over the eavesdropper's channel under the given system parameters, such as bandwidth and SNR ratios. The positive C_S (since $C_M > C_W$), highlights the robustness of the PLS scheme, enabling secure transmission without relying entirely on cryptographic techniques. Moreover, this result underscores the importance of maintaining a significant channel advantage to achieve secure communication in practical wireless systems.

However the Secrecy Rate (R_S), which represents the actual data achievable for secure communication, is bounded by the C_S. In this case, the latter was calculated to be 2.29 Gbps, indicating that secure communication can occur at any rate $R_S \leq 2.29$Gbps. This result highlights the advantages of using UWB systems, since they are well-suited for achieving higher secrecy rates due to their wide BW. Also the broad spectrum enables UWB signals to exhibit low power spectral densities, making them less detectable and harder to intercept. The R_S depends on the system design and application requirements, with R_S typically chosen to maximize the secure transmission rate while considering practical constraints such as coding overhead and channel conditions.

5.2.2 Non Achievable Secrecy Case

Now let's consider that Eve changes her position and moves towards Alice ,while the main channel's communication link is still alive and remained stable, and approaches at a close distance like shown below at figure 5.13. The distance between Alice and Eve now is approximately 1 meter.

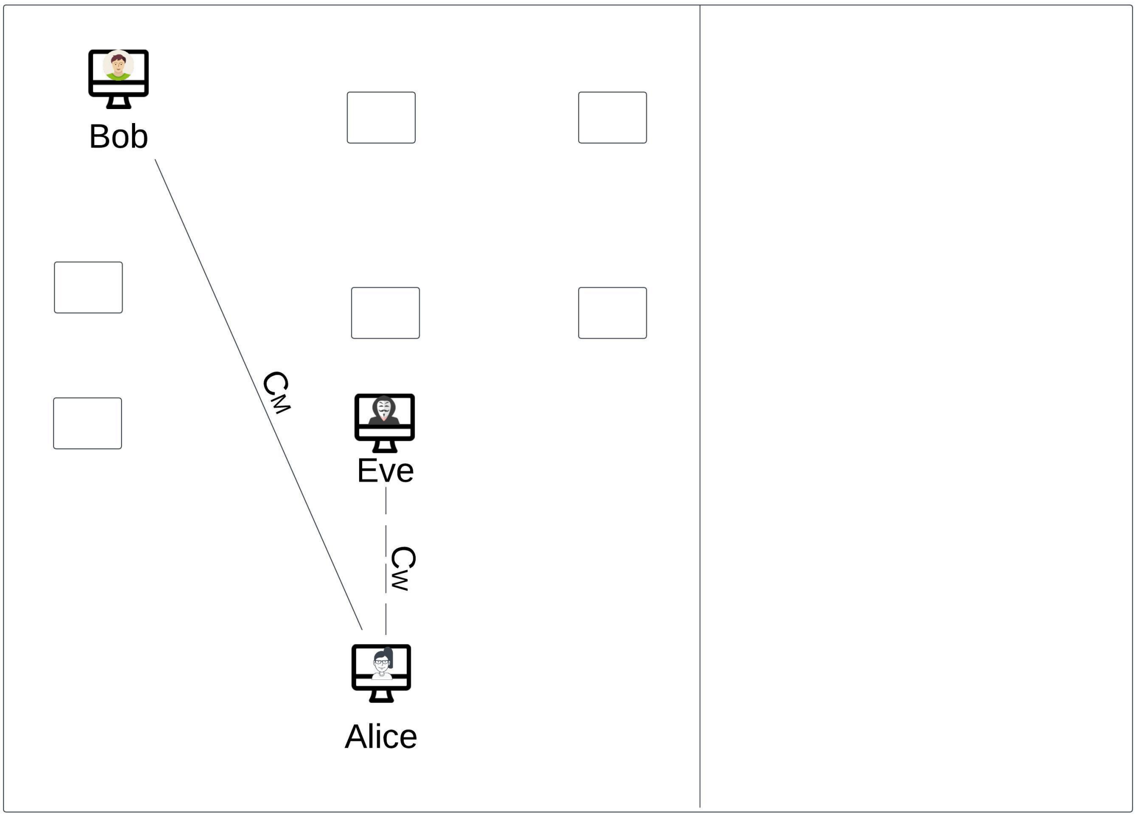
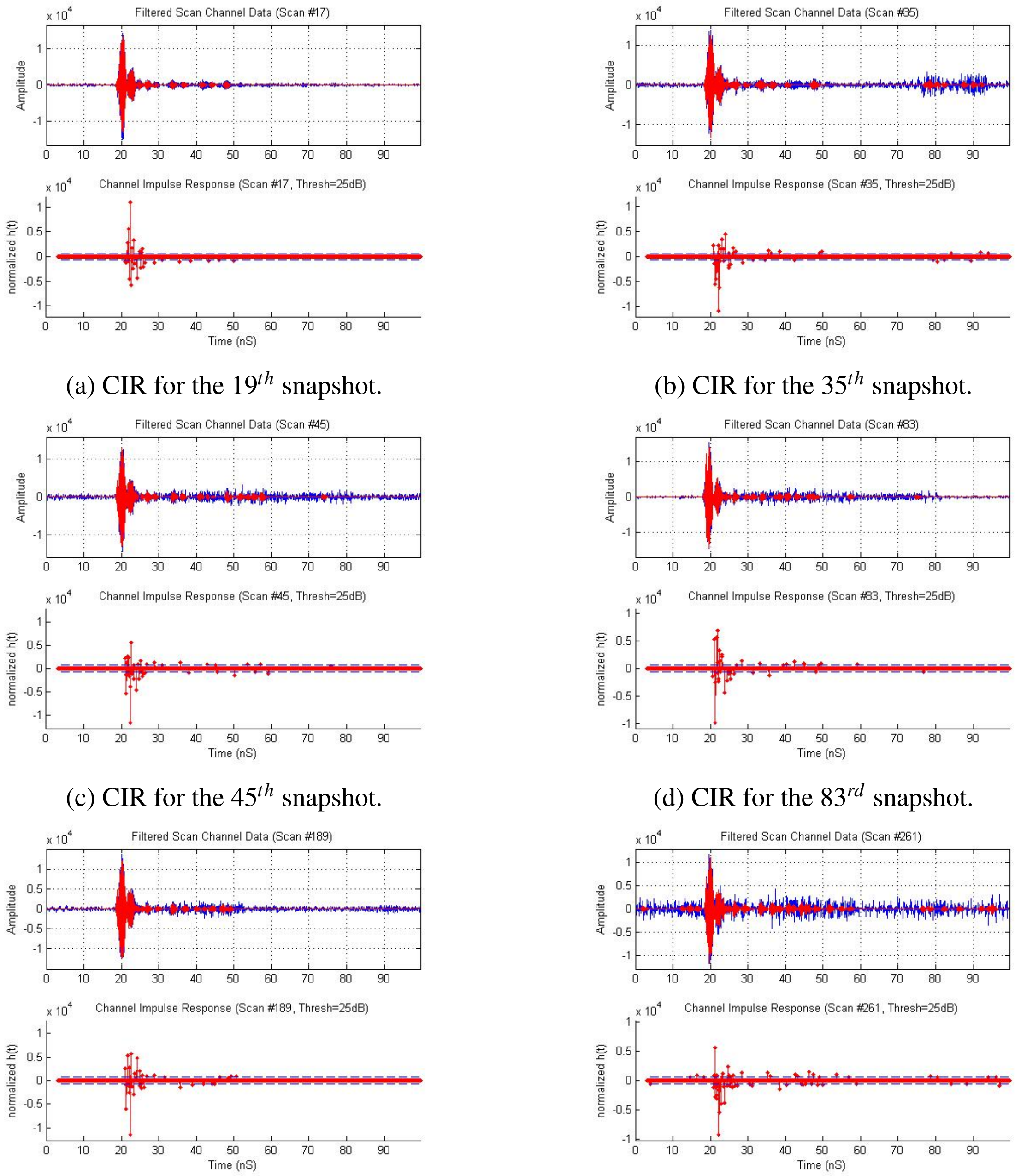


Fig. 5.13 Depiction of the case in which Eve approaches Alice at a very close distance.

Some of the CIR snapshots of the C_W in this case are shown in figure 5.14, in which shows like in previous figures (Fig 5.4 and Fig 5.5) the filtered channel measurements and their respective CIRs for different snapshots in time.



(a) CIR for the 19^{th} snapshot.

(b) CIR for the 35^{th} snapshot.

(c) CIR for the 45^{th} snapshot.

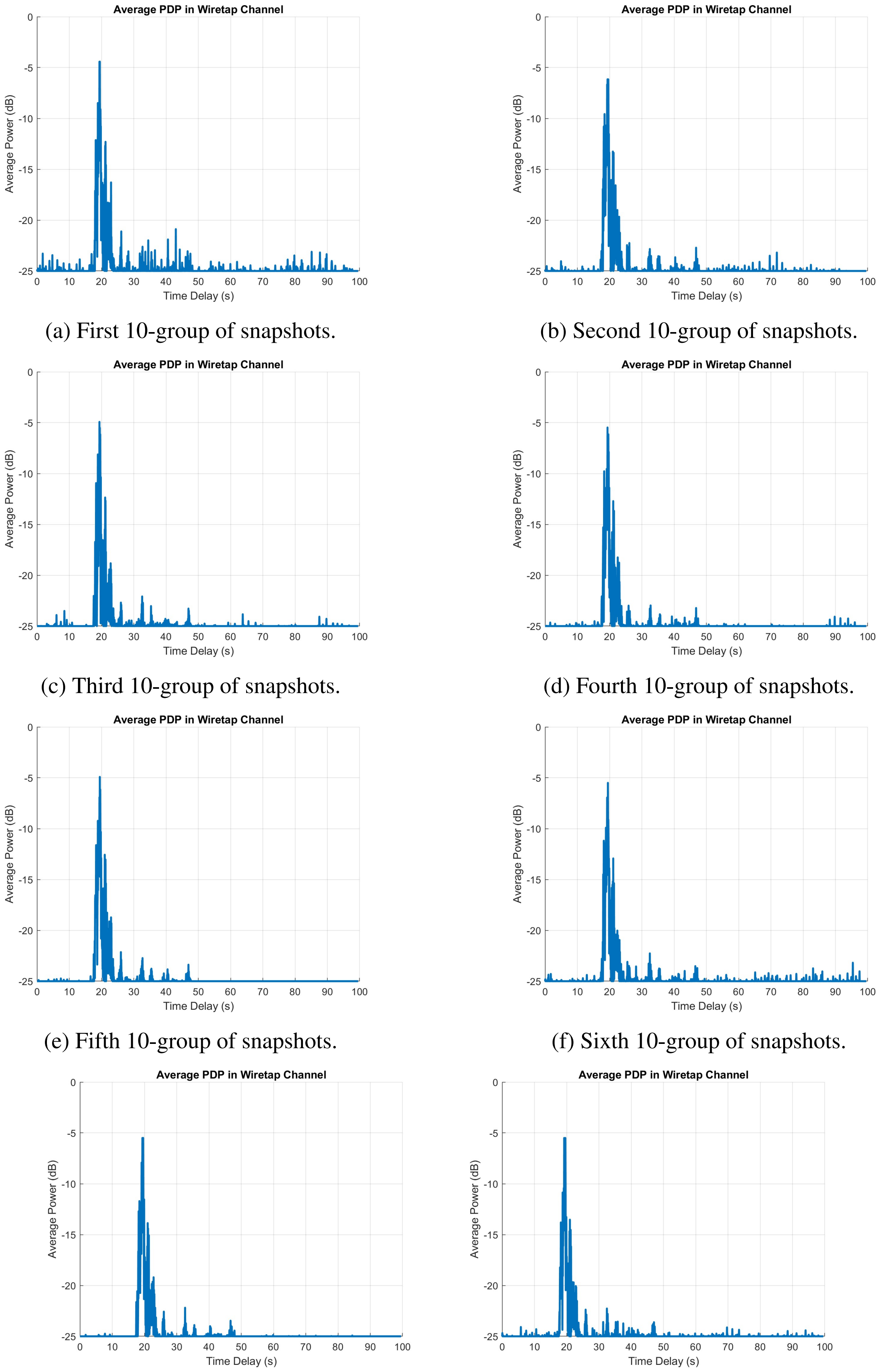
(d) CIR for the 83^{rd} snapshot.

(e) CIR for the 189^{th} snapshot.

(f) CIR for the 261^{st} snapshot.

Fig. 5.14 Channel Impulse Response for some snapshots of the C_W.

Here the CIR exhibit subtle variations in amplitude, some sort of noise level and a bit of temporal spread. It's obvious that there is a clear main peak followed by some minor reflections and this indicates that there are not significant multipaths since the overall "energy tail" is not especially long. Moreover, the PDP plots of the channel calculated as an average of a group of 25 snapshots are depicted below.



(a) First 10-group of snapshots.

(b) Second 10-group of snapshots.

(c) Third 10-group of snapshots.

(d) Fourth 10-group of snapshots.

(e) Fifth 10-group of snapshots.

(f) Sixth 10-group of snapshots.

(g) Seventh 10-group of snapshots.

(h) Eighth 10-group of snapshots.

Fig. 5.15 Power Delay Profile (PDP) of the second case C_W in group of 25 snapshots for each PDP plot.

The Power Delay Profile (PDP) plots for the C_W, shown in groups of 25 snapshots, provide insight into the temporal dispersion and power distribution in a scenario where Alice and Eve have a line-of-sight (LoS) connection with no objects obstructing their link. Across all groups, the PDPs exhibit a dominant peak around the 20 ns mark, corresponding to the strong LoS component that arrives first with the highest power. This is expected in LoS conditions, where the direct path dominates the channel. Beyond the primary peak, there is a sharp decay in power, with later arriving multipath components showing significantly lower power levels. These weaker components likely result from minor reflections from distant surfaces, as the absence of obstructions minimizes scattering. The consistency of the dominant peak across all groups indicates a stable channel over time, with negligible temporal dispersion due to the predominance of the direct LoS path. This compact power concentration around the first arrival demonstrates that the channel provides a clear and direct communication link between Alice and Eve, minimizing inter-symbol interference and further emphasizing the impact of their proximity and unobstructed LoS connection.

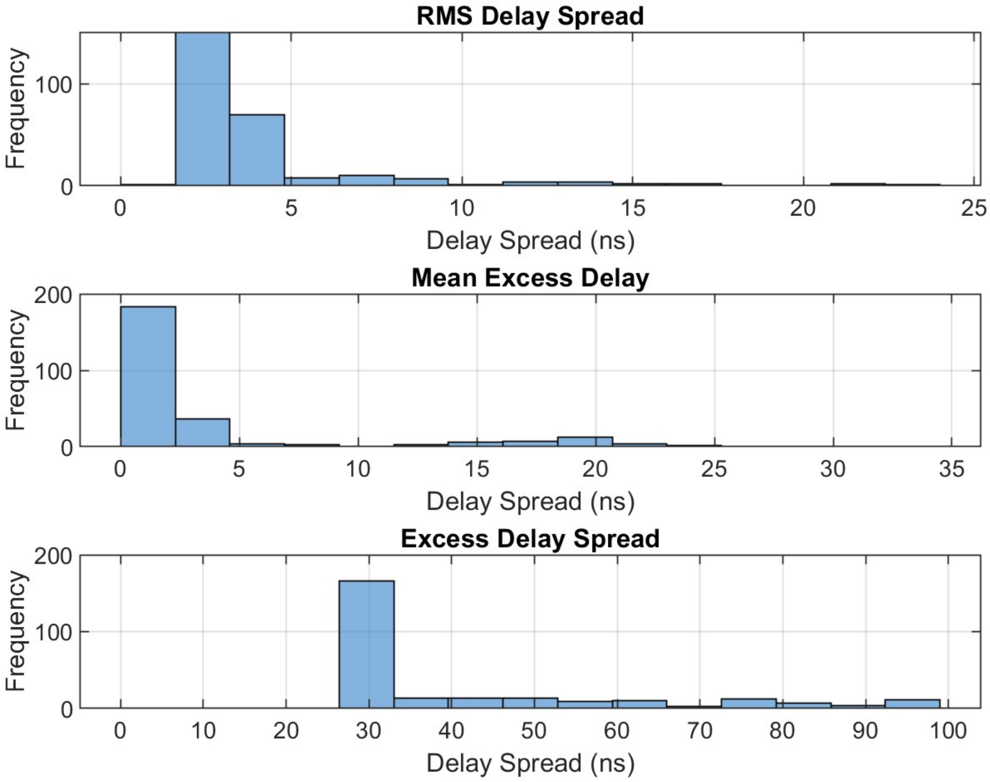


Fig. 5.16 Delay Spread Analysis of the second case C_W.

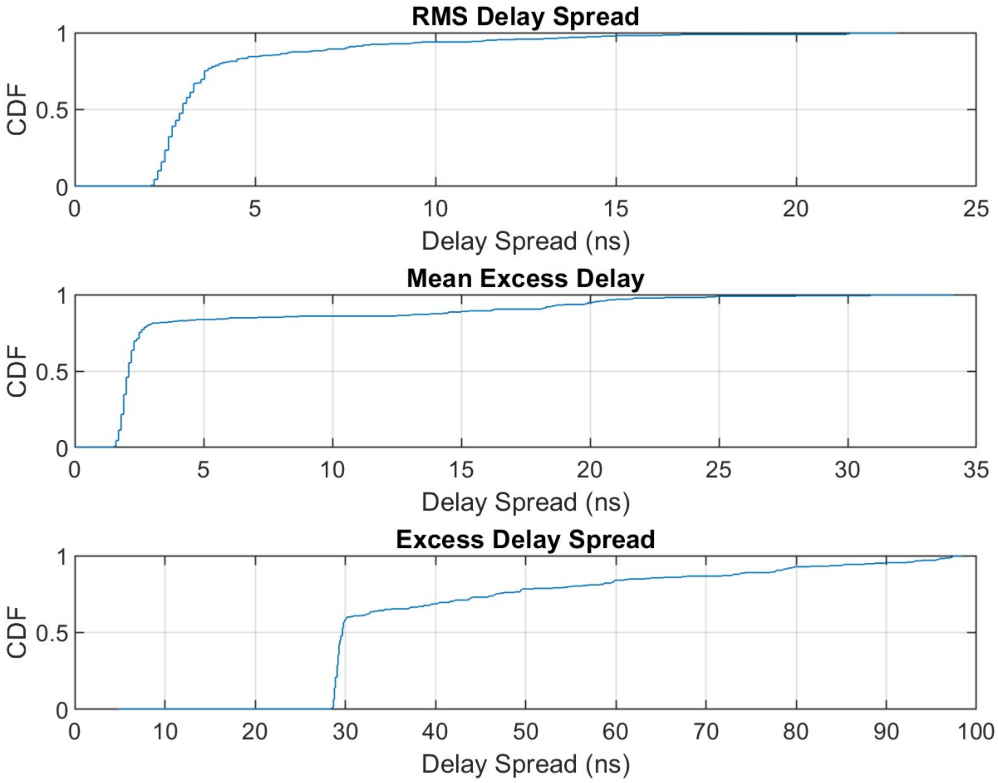


Fig. 5.17 CDF of the second case C_W.

In Figure 5.16 the histograms for the RMS delay spread, mean excess delay, and excess delay spread reflect the expected behavior of the channel under a LoS scenario with no obstructions between Alice and Eve. The RMS delay spread and mean excess delay are predominantly concentrated below 5 ns, indicating that the direct path dominates, with minimal contribution from weak and closely spaced multipath components. The excess delay spread, while slightly broader, primarily ranges below 30 ns, confirming that even the delayed multipath components arrive within a relatively short time frame. These results are consistent with the characteristics of an LoS channel, where minimal scattering and strong dominance of the direct path lead to limited temporal dispersion. The distributions validate the low dispersive nature of the channel, as expected in this controlled environment. In Figure 5.17 are depicted the CDFs for each one of the calculated Delay Spreads. The statistical analysis of the Delay Spreads is shown at Table 5.3.

Table 5.3 Statistical Analysis of Delay Spread Metrics for second case Wiretap Channel.

Metric	**Mean (ns)**	**Median (ns)**	**Standard Deviation (ns)**
RMS Delay Spread	4.08	3.00	3.26
Mean Excess Delay	4.63	2.10	6.26
Excess Delay Spread	41.10	29.70	19.83

The next step is to calculate the new SNR at Alice and determine if it is able to achieve secrecy and at which rate in this scenario. So, from equation (5.4) the SNR at Alice is equal to 35dB which means that the $C'_W \approx 16.28$ Gbps. So, the overall Secrecy Capacity in this scenario is negative since, the C_M capacity equals to 9.78 Gbps, and it is not possible to be achieved any secrecy rate here, so as shown in [2] since $C_M < C'_W$ we cannot achieve a positive R_S. Although, it's possible to determine the probability of existence of a positive C_S like shown below :

$$\begin{aligned}\mathscr{P}(C_S > 0) &= \mathscr{P}(\gamma_M > \gamma_W)\\ &= \frac{\overline{\gamma}_M}{\overline{\gamma}_M + \overline{\gamma}_W}.\end{aligned}$$

Like already calculated in the example at Chapter 3. All in all, from this experiment we conclude that when $\gamma_M >> \gamma_W$ (or $d_M << d_W$) then $\mathscr{P}(C_S > 0) \approx 1$ and on the other hand when $\gamma_M << \gamma_W$ (or $d_M >> d_W$) then $\mathscr{P}(C_S > 0) \approx 0$.

5.3 Outdoor Scenario

The outdoor measurements took place at Odyssea Androutsou and Vasileos Georgiou Street, Piraeus creating a possible scenario between the parties, Alice, Bob and Eve. More specifically, Alice is communicating with Bob through the main channel C_M while Bob is crossing the distance d_1 and Eve tries to "listen" the communication through the wiretap channel C_W.

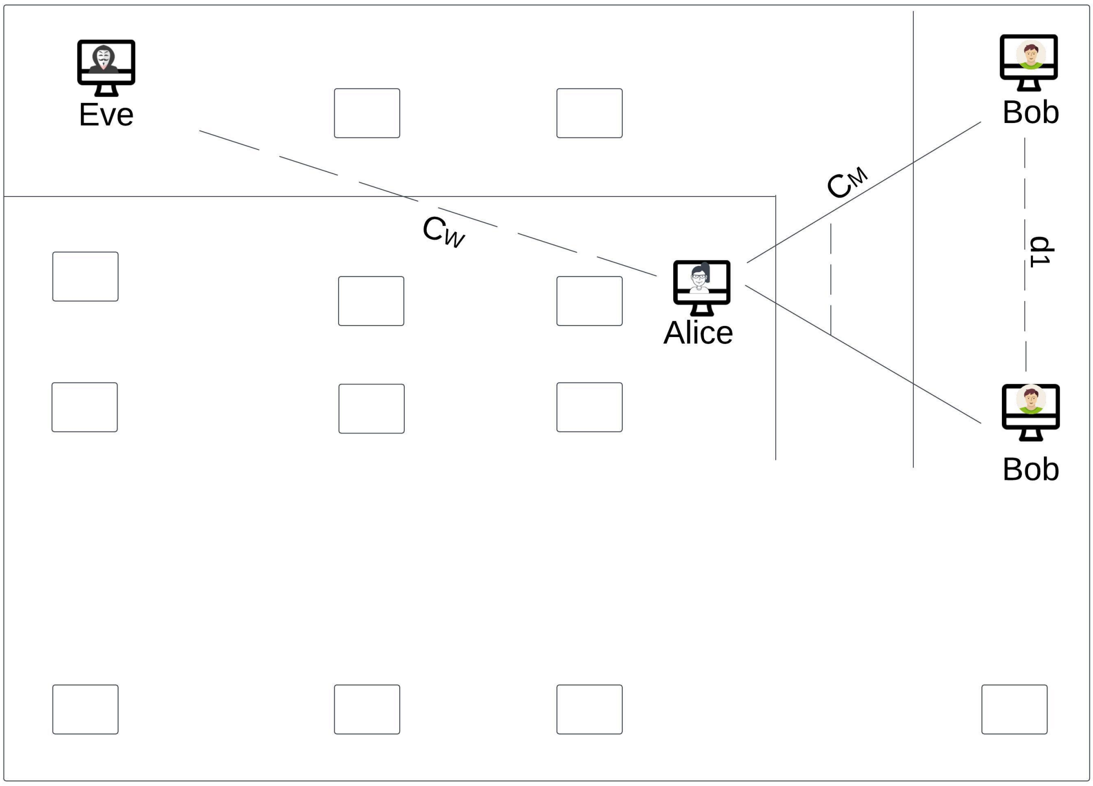


Fig. 5.18 Depiction of the outdoor scenario.

At figure 5.18 is a schematic depiction of the setup experiment showing the position of the parties and the the distance that Bob is crossing.

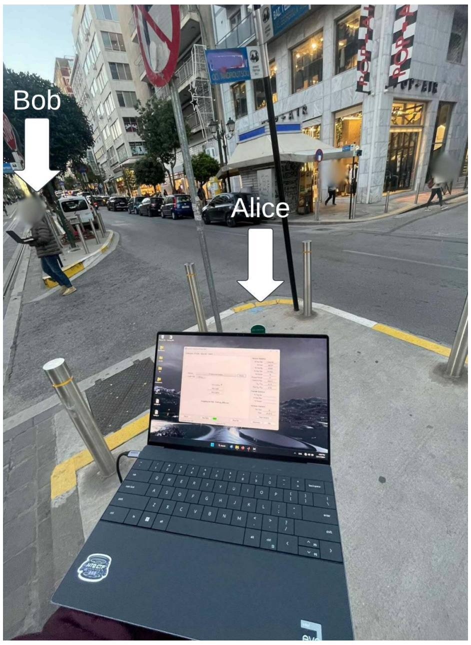


Fig. 5.19 Alice and Bob's initial position.

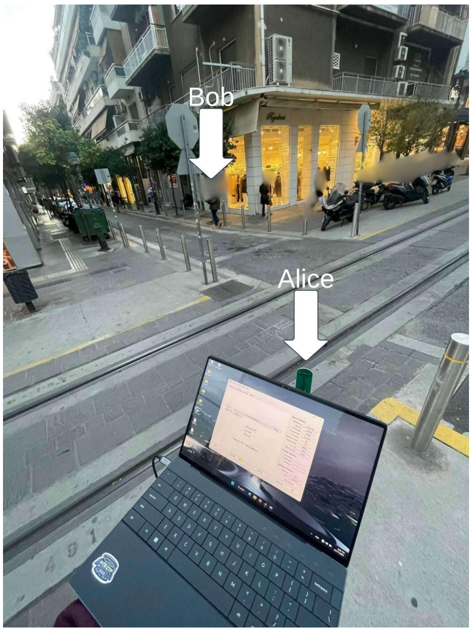


Fig. 5.20 Alice and Bob's final position after crossing distance d_1.

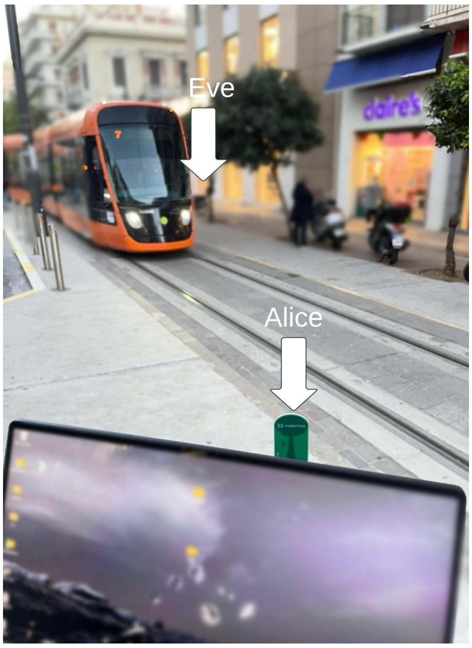
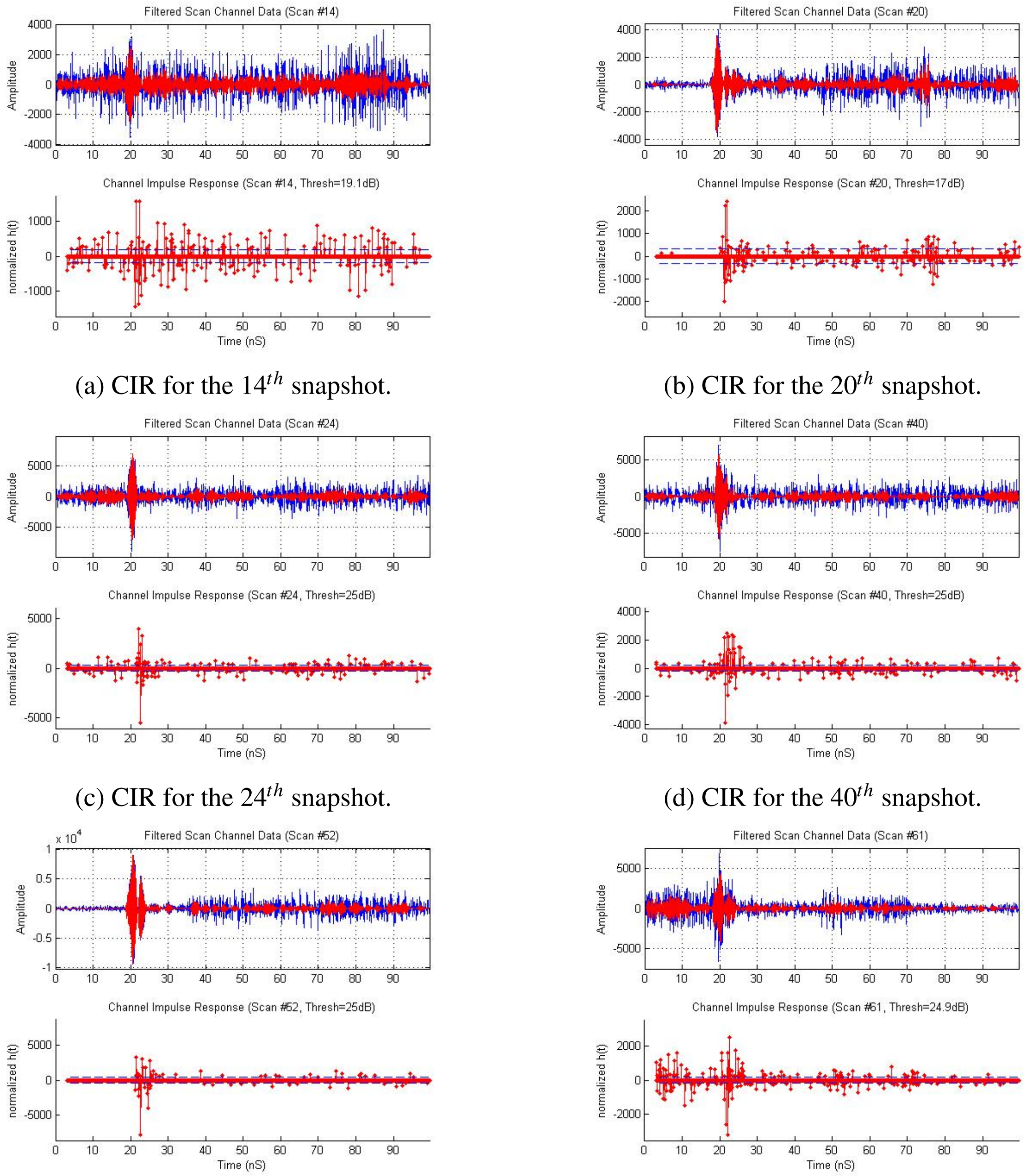


Fig. 5.21 Alice and Eve positions.

From figures 5.19 - 5.21 it's clear that Bob and Alice are separated at a distance of approximately 7-15 meters while Bob is moving and crossing a distance of 10 meters along the road. On the other hand, Eve is hidden at the end of the road behind the tram, at a distance of 20 meters separated from Alice.

5.3.1 Channel Characteristics and Secrecy Calculation

Like the the previous indoor case, the channel characteristics for this experiment setup are evaluated based on the derived CIR data. The main focus is on the Delay Spread Analysis and the Power Delay Profile. Below in Fig. 5.22 are shown some CIRs of the collected snapshots. Specifically are depicted six snapshots which illustrate the temporal behavior of the channel under varying conditions. In these plots, the primary peak corresponds to the LoS component or the strongest multipath component, while subsequent smaller peaks represent reflections and scattering from surrounding objects (buildings, vehicles or even the ground). The temporal spread of the multipath components also highlight the delay spread dispersion of the channel which is critical in potential inter-symbol interference. These CIR snapshots also allow for an assessment of channel variability over time, as differences in the amplitude and delay of multipath components across the snapshots confirms the changes in the environment, such as the moving objects and the varying distances between Alice and Bob. Similarly, Fig. 5.23 depicts the CIR of six snapshots of the C_W. It is obvious from the presented graphs that the wiretap channel suffers more from multipath components since more moving objects (like the tram shown in Fig. 5.21) contribute to the multipath propagation and as a result in most of the graphs it is obvious a "tail" of energy after the first strong component.



(a) CIR for the 14th snapshot.

(b) CIR for the 20th snapshot.

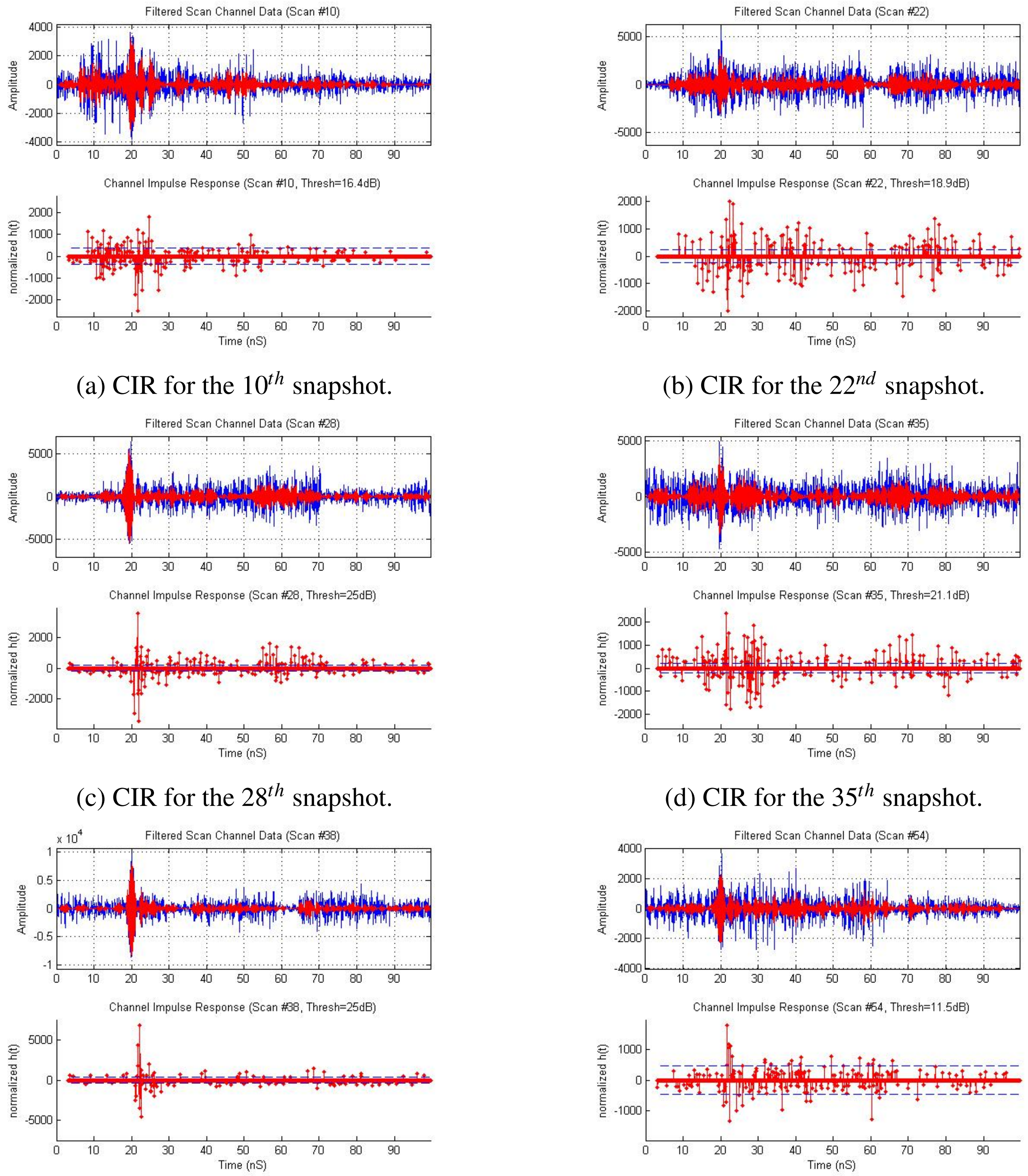
(c) CIR for the 24th snapshot.

(d) CIR for the 40th snapshot.

(e) CIR for the 52nd snapshot.

(f) CIR for the 61st snapshot.

Fig. 5.22 Channel Impulse Response of the C_M for outdoor measurements.



(a) CIR for the 10^{th} snapshot.

(b) CIR for the 22^{nd} snapshot.

(c) CIR for the 28^{th} snapshot.

(d) CIR for the 35^{th} snapshot.

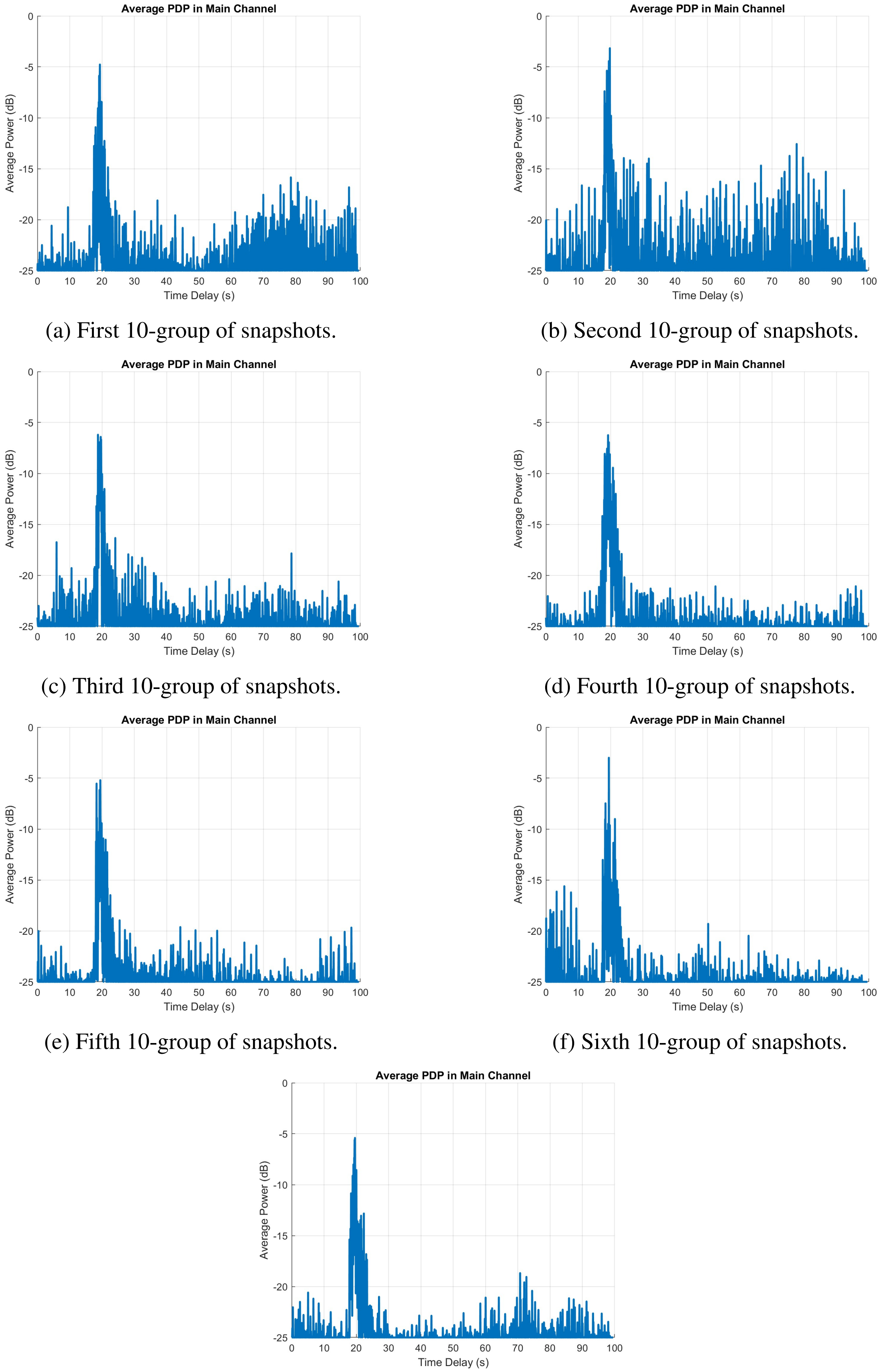
(e) CIR for the 38^{th} snapshot.

(f) CIR for the 54^{th} snapshot.

Fig. 5.23 Channel Impulse Response of the C_W for outdoor measurements.

5.3.1.1 Power Delay Profile

Below on Fig. 5.24 and Fig. 5.25 are depicted the PDPs of the C_M and C_W respectively.



(a) First 10-group of snapshots.

(b) Second 10-group of snapshots.

(c) Third 10-group of snapshots.

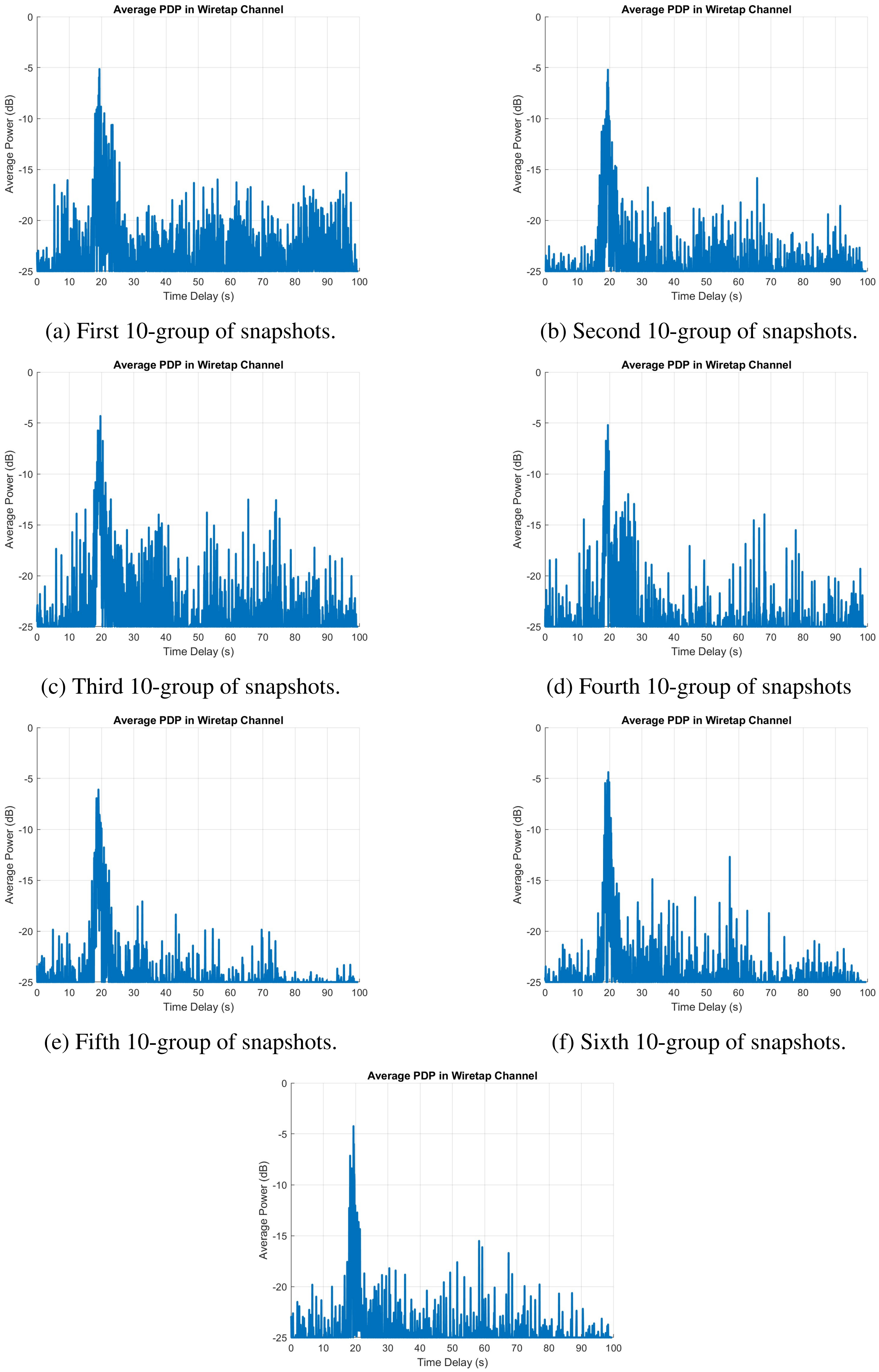
(d) Fourth 10-group of snapshots.

(e) Fifth 10-group of snapshots.

(f) Sixth 10-group of snapshots.

(g) Seventh 10-group of snapshots.

Fig. 5.24 Power Delay Profile (PDP) of the C_M outdoor measurements.



(a) First 10-group of snapshots.

(b) Second 10-group of snapshots.

(c) Third 10-group of snapshots.

(d) Fourth 10-group of snapshots

(e) Fifth 10-group of snapshots.

(f) Sixth 10-group of snapshots.

(g) Seventh 10-group of snapshots.

Fig. 5.25 Power Delay Profile (PDP) of the C_W outdoor measurements.

The PDPs for the C_M in the outdoor measurement scenario, calculated as an average over groups of 10 snapshots, reveal key insights into the multipath propagation characteristics of the channel. The PDPs consistently exhibit a dominant peak at the earliest time delay, corresponding to the strong LoS component between Alice and Bob. This is expected given their varying distance of 7 to 15 meters, which ensures a strong direct signal. Beyond the primary peak, there are several smaller peaks at later time delays, representing reflected and scattered multipath components caused by interactions with surrounding objects such as buildings, the ground, or other surfaces in the outdoor environment. The relative amplitude of these secondary peaks is notably lower compared to the LoS component, indicating that while multipath propagation is present, the LoS component is the dominant contributor to the received signal power. The temporal spread of the PDPs confirms the characteristics of an outdoor measurement environment, where the lack of significant obstructions allows for distinct and less attenuated reflections from far-field scatterers. Furthermore, the grouping and averaging of snapshots highlight the temporal stability of the main channel, as the general structure of the PDPs remains consistent across different groups. This stability is a result of the relatively stationary nature of the outdoor environment during the measurements and the controlled motion of Bob within the predefined distance range. Overall, these PDPs validate the measurement setup and confirm the influence of multipath propagation, as expected in a typical outdoor wireless communication scenario.

The PDPs of the C_W, averaged over groups of 10 snapshots, exhibit characteristics that are comparable to those of the main channel. While Eve is positioned farther from Alice 20 meters compared to Bob's varying distance of 7–15 meters, the wiretap channel PDPs still display a dominant peak corresponding to the LoS component, with multipath components that appear relatively strong. This suggests that environmental factors, such as reflective surfaces or scatterers, contribute significantly to the wiretap channel's multipath strength, partially offsetting the increased free-space path loss due to Eve's greater distance. The multipath components in the wiretap channel are distributed over a slightly broader delay range, as seen in the temporal spread of the PDPs, but their amplitudes remain comparable to those observed in the main channel. This broader spread indicates that the signal experiences longer propagation delays in the wiretap channel, likely due to the increased distance and the influence of environmental scatterers. However, the strength of the multipath components suggests that Eve's channel still benefits from significant multipath contributions, similar to the C_M.

5.3.1.2 Main Channel Delay Spread Analysis

The delay spread analysis of the C_M, as depicted in Fig. 5.26, provides insights into the dispersion of the received signal. The RMS delay spread, is distributed between 10 and 25 ns, indicating a moderately dispersive channel. The mean excess delay, is concentrated around 20 to 40 ns, further confirming the significant contribution of early arriving multipaths. Finally, the excess delay spread exhibits values distributed up to 100 ns, depicting thew presence of extended multipaths caused by the outdoor environments' scatterers. The calculated metric values of the Mean, Median and Standard Deviation are shown in Table 5.4.

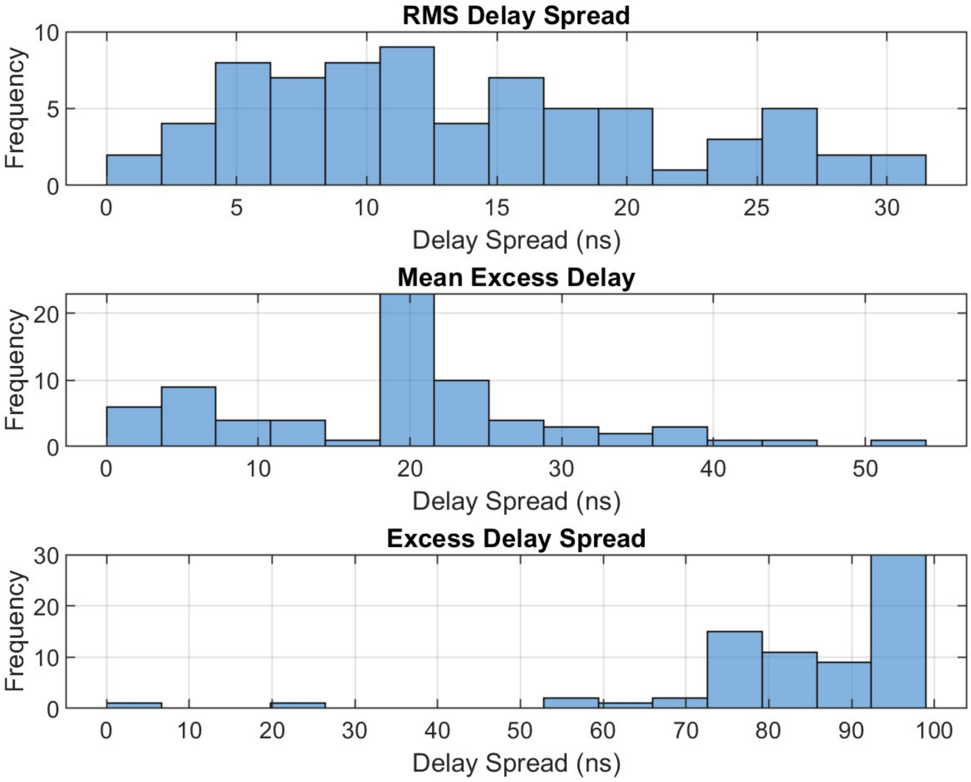


Fig. 5.26 Delay Spread Analysis of the C_M for the outdoor measurements.

Table 5.4 Statistical Analysis of Delay Spread Metrics for outdoor C_M.

Metric	**Mean (ns)**	**Median (ns)**	**Standard Deviation (ns)**
RMS Delay Spread	13.65	11.85	7.66
Mean Excess Delay	19.02	19.80	11.18
Excess Delay Spread	84.47	88.05	16.36

Figure 5.27 depicts the RMS delay spread which exhibits a steady increase, with most values falling below 30 ns, indicating the dispersion of the channel. The mean excess shows a similar behavior, showing the influence of the early arriving multipaths. The excess delay spread indicates a broader distribution, with values reaching up to 100 ns.

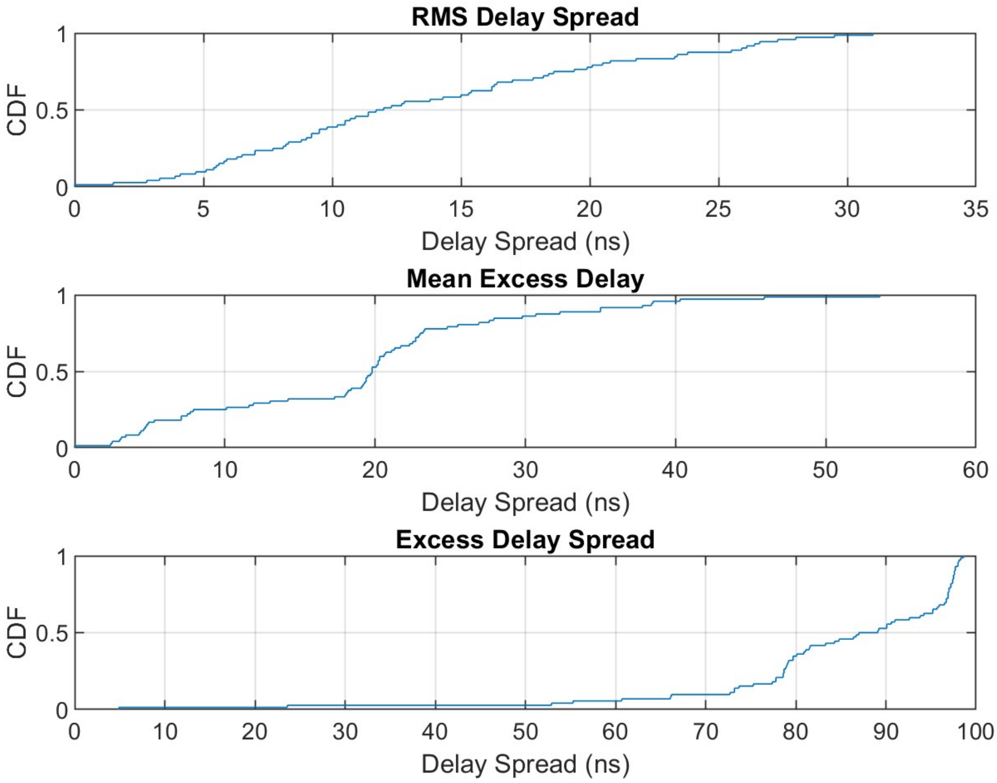


Fig. 5.27 CDF of the C_M for the outdoor measurements.

5.3.1.3 Wiretap Chanel Delay Spread Analysis

As explained in the previous section, also here the Delay Spread analysis shows the dispersion of the channel and it can be easily understood that the behavior of the C_W regarding the delay spread is similar to the C_M. Table 5.5 shows the statistical values of the Delay Spread Analysis and Figure 5.29 the corresponding CDF.

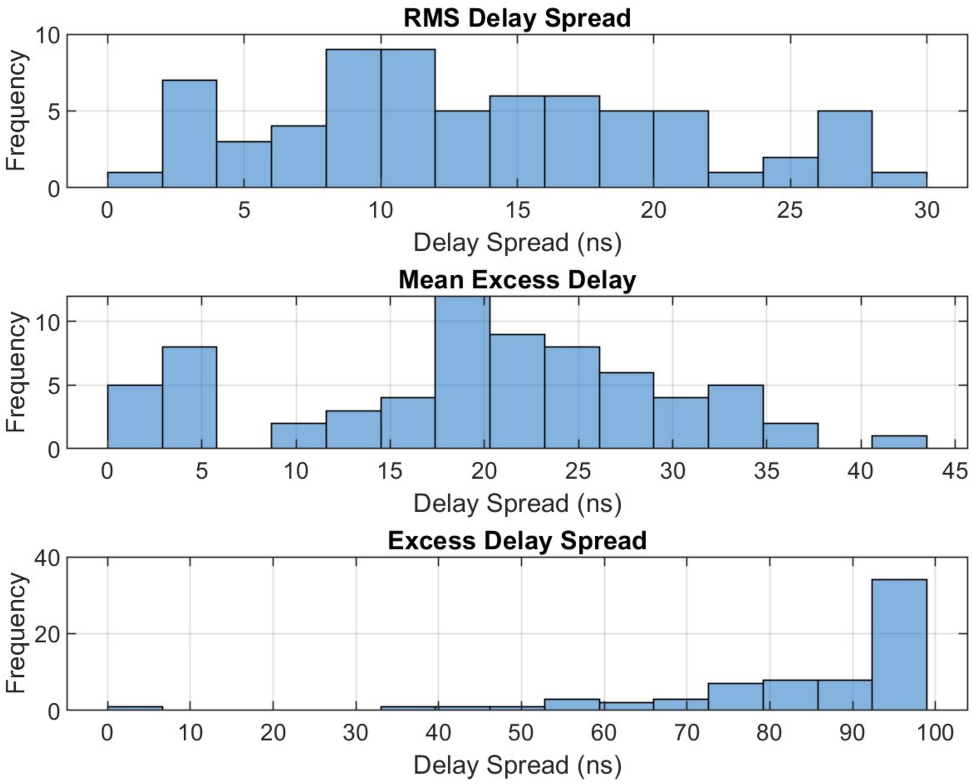


Fig. 5.28 Delay Spread Analysis of the C_W for the outdoor measurements.

Table 5.5 Statistical Analysis of Delay Spread Metrics for outdoor C_W.

Metric	Mean (ns)	Median (ns)	Standard Deviation (ns)
RMS Delay Spread	13.62	13.0	7.30
Mean Excess Delay	19.82	20.50	10.18
Excess Delay Spread	83.98	92.30	17.52

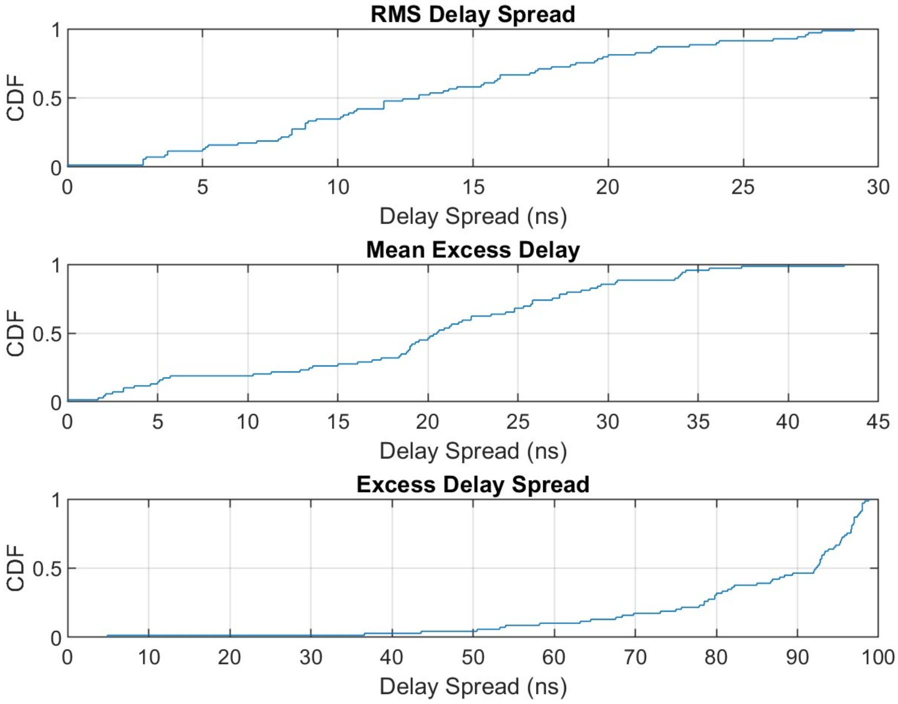


Fig. 5.29 CDF of the C_W for the outdoor measurements.

5.3.1.4 Secrecy Metrics

To calculate the possible Secrecy Capacity and achievable Secrecy Rate, the same process as in the previous cases should be followed. The SNR at Bob $\overline{\gamma}_M$, calculated by the instantaneous SNR's per snapshot is equal to 24.69 dB. While the SNR at Eve $\overline{\gamma}_W$ is equal to 24.21 dB. As explained 5.2.2 it's proven that when $\gamma_M > \gamma_W$ then $\mathscr{P}(C_S > 0) \approx 1$. In particular, the capacities are :

$$C_M = Blog_2(1+\overline{\gamma}_M) \approx 11.49 \text{ Gbps}$$

$$C_W = Blog_2(1+\overline{\gamma}_W) \approx 11.27 \text{ Gbps}$$

So, the available $C_S = C_M - C_W \approx 222.43$ Mbps. To conclude, the achievable R_S here can occur at any rate $R_S \leq 222.43$ Mbps. The Achievable Secrecy Rate at this case is very low, since the channels are very similar due to the near distances of the parties and the common environment that are located. So in this case Eve has a great link through the wiretap channel but even so, the distance that separates Eve and Alice compared to the dynamic distance between Alice an Bob plays significant role in achieving a possible Secrecy Rate.

5.4 Theoretical Study

In this section various simulations on MATLAB will be evaluated, mostly to check the UWB effect on the Secrecy Capacity and how Secrecy Capacity changes over different values of transmitted power. In this scenario we assume that there are the parties Alice, Bob, Eve and Alice reaches Bob through a relay.

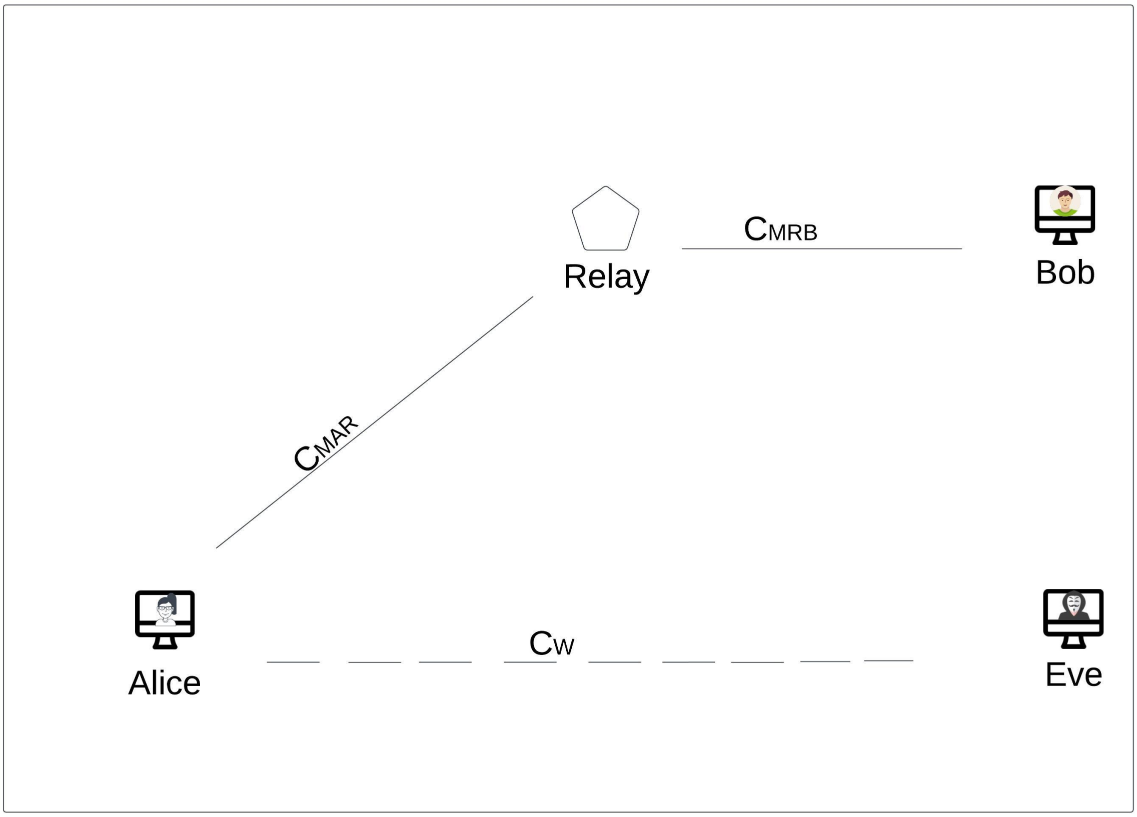


Fig. 5.30 Evaluation of C_S in an outdoor relay assisted communication.

In Fig. 5.30 is depicted a possible scenario in which Alice uses the offered Relay in the network to reach Bob, since there is no LoS link between them, while Eve is positioned somewhere in the area trying to "listen" to their communication. We consider that both channels suffer from fading, in the simulation is modeled using Rayleigh fading as a worst case scenario. The transmit power here follows the power limit specified by ETSI [31] for UWB devices, adjusting the transmit power on a range of -30dBm to 14.5dBm. The offered bandwidth of the system is parameterized for different values across the range of 1GHz - 5GHz.

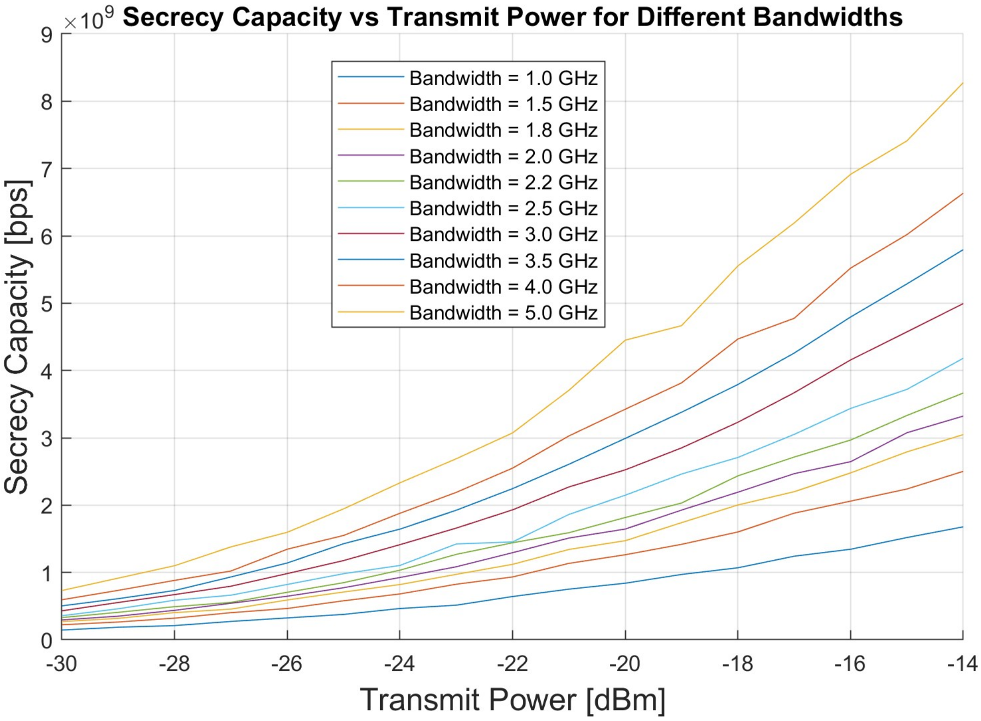


Fig. 5.31 Simulation of the calculated Secrecy Capacity versus Transmit Power for Different Bandwidths.

The Fig. 5.31 illustrates the variation of secrecy capacity as a function of global transmit power for different system bandwidths. Secrecy capacity, a critical performance metric in secure communication systems, increases with higher transmit power and larger bandwidth. The plot clearly shows that at lower transmit power, the secrecy capacity is almost identical across different bandwidths due to the limited available signal energy. However, as the transmit power increases, the secrecy capacity exhibits a steeper growth for larger bandwidths, highlighting the enhanced secure communication potential provided by UWB communications. For example, at a transmit power of -15 dBm, a system with 5 GHz bandwidth achieves a significantly higher secrecy capacity compared to one with 1 GHz bandwidth. This demonstrates the importance of bandwidth in maximizing secrecy capacity, especially in high-power transmission scenarios.

Chapter 6

Conclusion

6.1 Implications

The results obtained from the channel measurements and secrecy capacity calculations have significant implications for the design of secure physical layer systems. By evaluating the achievable secrecy rates under different scenarios, we gain valuable insights into the dynamics of secure communication over wireless channels and the factors that influence their performance.

Firstly, from the indoor measurements we understand that LoS link may not be always available for an eavesdropper when trying to hide its presence, so preventing wiretapping in such cases could be easier since the Wiretap Channel will be way more degraded than the main channel between the two legitimate parties who may have LoS link.

Secondly, from the outdoor measurements we come up with several results. Due to the fact that the radio modules that are used are for short range transmission, the scenario was built for a short range wiretap channel communication. We can clearly understand that in such cases both channels seem to have similar behavior due to the fact that they share common environment. Even though, the distance between the parties, which is the most important factor in this case, allows for a secure communication but with a relatively limited Secrecy Rate. In such cases, furthermore techniques, like the ones proposed in the second section of the third chapter could be applied to adapt to the system model in order to increase the possible Secrecy Capacity and achieve higher Secrecy Rate. Such techniques include friendly jamming nodes allocated along the network, artificial noise generation and optimal power allocation between the actual signal and the interference signal.

Last but not least, the theoretical study that was concluded at 5.4 draws significant conclusions for UWB communications by comparing different achievable Secrecy Capacities, and so Secrecy Rates, with different bandwidths for possible transmit powers that are allowed for such UWB modules.

6.2 Summary

In conclusion, the continuous evolution of wireless communication systems and the rising threats to data confidentiality underscore the critical need to evaluate secrecy metrics when designing modern wireless networks. By quantifying how securely information can be transmitted over a given channel, these metrics provide valuable insights that guide the selection of system parameters, coding schemes, and resource allocation strategies to ensure robust protection against eavesdropping. Physical Layer Security further strengthens this defense by leveraging the unique statistical properties of the wireless channel, reducing the reliance on higher-layer cryptographic techniques. UWB technology, in particular, emerges as a strong candidate for PLS applications, thanks to its broad frequency spectrum, low power requirements, and inherent resilience to multipath interference. Together, these features enable high data rates, precise localization, and minimal detectability, crucial factors in achieving enhanced secrecy rates and secrecy capacities. Consequently, adopting UWB for PLS can be pivotal in meeting the growing demand for secure and efficient communication in today's interconnected world.

6.3 Future Work

There are a number of interesting topics related to Physical Layer Secure Systems, to enhance and proceed the research work that is being conducting nowadays on the scientific society and academia. Some interesting ideas to enhance this present work could be:

- **Experimental Validation of Cooperative Jamming Approaches.**

  Conduct real-life measurements in controlled and outdoor scenarios to evaluate the performance of cooperative jamming techniques. This could involve using programmable hardware platforms (e.g., USRPs) to study the trade-off between jamming effectiveness and communication quality in various channel conditions.

- **Machine Learning for Adaptive Physical Layer Security**

  Explore machine learning and deep learning models for real-time adaptation of transmission parameters (e.g., power, beamforming patterns) to maximize secrecy rates. This may involve designing algorithms that can predict eavesdropping conditions.

- **MIMO System Design for Enhanced PLS**

  Investigate how multi-antenna configurations can be leveraged for improved secrecy. Research could focus on exploiting spatial diversity to implement beamforming and spatial filtering techniques that significantly raise the eavesdropper's uncertainty, while minimizing power consumption.

- **Integration of UWB Based Localization and Security**

  Examine the combined benefit of high precision UWB localization with PLS strategies. For instance, the system could adjust transmission parameters based on real-time distance and CSI to maximize secrecy capacity in time-varying environments.

References

[1] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[2] Joao Barros and Miguel R. D. Rodrigues. Secrecy capacity of wireless channels. In *2006 IEEE International Symposium on Information Theory*, pages 356–360, 2006.

[3] TDSR. *P440 Data Sheet & User Guide*, March 2021. Accessed: 2024-11-06.

[4] Amitav Mukherjee, S. Ali A. Fakoorian, Jing Huang, and A. Lee Swindlehurst. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys & Tutorials*, 16(3):1550–1573, 2014.

[5] Matthieu Bloch and Joao Barros. *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[6] Yulong Zou, Jia Zhu, Xianbin Wang, and Lajos Hanzo. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9):1727–1765, 2016.

[7] Andreas F. Molisch. Ultra-wide-band propagation channels. *Proceedings of the IEEE*, 97(2):353–371, 2009.

[8] Mahdi Shakiba-Herfeh, Arsenia Chorti, and H. Vincent Poor. *Physical Layer Security: Authentication, Integrity, and Confidentiality*, pages 129–150. Springer International Publishing, Cham, 2021.

[9] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.

[10] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *IEEE transactions on information theory*, 24(3):339–348, 1978.

[11] Frederique Oggier and Babak Hassibi. The mimo wiretap channel. In *2008 3rd International Symposium on Communications, Control and Signal Processing*, pages 213–218, 2008.

[12] Arsenia Chorti and H. Vincent Poor. Achievable secrecy rates in physical layer secure systems with a helping interferer. In *2012 International Conference on Computing, Networking and Communications (ICNC)*, pages 18–22, 2012.

[13] M.Z. Win and R.A. Scholtz. Impulse radio: how it works. *IEEE Communications Letters*, 2(2):36–38, 1998.

[14] Andreas F. Molisch, Dajana Cassioli, Chia-Chin Chong, Shahriar Emami, Andrew Fort, Balakrishnan Kannan, Johan Karedal, Juergen Kunisch, Hans Gregory Schantz, Kazimierz Siwiak, and Moe Z. Win. A comprehensive standardized model for ultra-wideband propagation channels. *IEEE Transactions on Antennas and Propagation*, 54(11):3151–3166, 2006.

[15] Ueli M. Maurer. *The Strong Secret Key Rate of Discrete Random Triples*, pages 271–285. Springer US, Boston, MA, 1994.

[16] Jie Hou and Gerhard Kramer. Effective secrecy: Reliability, confusion and stealth. In *2014 IEEE International Symposium on Information Theory*, pages 601–605, 2014.

[17] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[18] Mihir Bellare, Stefano Tessaro, and Alexander Vardy. Semantic security for the wiretap channel. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, pages 294–311, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[19] Satashu Goel and Rohit Negi. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, 7(6):2180–2189, 2008.

[20] Wahab Khawaja, Ismail Guvenc, and David Matolak. Uwb channel sounding and modeling for uav air-to-ground propagation channels. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–7, 2016.

[21] David Tse and Pramod Viswanath. *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[22] Andrea Goldsmith. *Bibliography*, page 605–632. Cambridge University Press, 2005.

[23] Simon. *Fading Channel Characterization and Modeling*, chapter 2, pages 17–43. John Wiley & Sons, Ltd, 2004.

[24] Minoru Nakagami. The m-distribution—a general formula of intensity distribution of rapid fading. *Conference on Statistical Methods in Radio Wave Propagation*, pages 3–36, 1960.

[25] Athanasios G. Kanatas Filippos Konstantinou. *Mobile Comunication Systems, 2nd Edition*. University Publications of Crete, Athens, Greece, 2012.

[26] Nektarios Moraitis, Lefteris Tsipi, and Demosthenes Vouyioukas. Machine-learning-based path loss prediction for in-cabin wireless networks. In *2024 IEEE International Conference on Machine Learning for Communication and Networking (ICMLCN)*, pages 393–398, 2024.

[27] A.F. Molisch. Ultrawideband propagation channels-theory, measurement, and modeling. *IEEE Transactions on Vehicular Technology*, 54(5):1528–1545, 2005.

[28] A.A.M. Saleh and R. Valenzuela. A statistical model for indoor multipath propagation. *IEEE Journal on Selected Areas in Communications*, 5(2):128–137, 1987.

[29] D. Cox. Delay doppler characteristics of multipath propagation at 910 mhz in a suburban mobile radio environment. *IEEE Transactions on Antennas and Propagation*, 20(5):625–635, 1972.

[30] Arjan Meijerink and Andreas F. Molisch. On the physical interpretation of the saleh–valenzuela model and the definition of its power delay profiles. *IEEE Transactions on Antennas and Propagation*, 62(9):4780–4793, 2014.

[31] ETSI. Electromagnetic compatibility and radio spectrum matters (erm); short range devices (srd); ultra wide band (uwb) devices in the 6-8.5 ghz frequency range; part 1: Technical characteristics, test methods and limits. Technical Report ETSI EN 302 065-1 V2.1.0, European Telecommunications Standards Institute (ETSI), 2020. Accessed: 2024-11-06.

[32] S Park, H Chao, HR Arabnia, and Neil Y Yen. Advanced multimedia and ubiquitous engineering. *Lecture notes in electrical engineering*, 448:269–276, 2017.