UCLouvain

École polytechnique de Louvain

Integrated Sensing and Communication: a Wi-Fi 6 USRP-based Experimental Setup

Author: **Jérôme LAFONTAINE**
Supervisors: **Prof. Claude OESTGES, Prof. Luc VANDENDORPE**
Readers: **Prof. Jérôme LOUVEAUX, François DE SAINT MOULIN, Martin WILLAME**
Academic year 2023–2024
Master [120] in Electrical Engineering

Abstract

In recent years, there has been an increasing interest in Integrated Sensing and Communication systems (ISAC). Such systems are capable of both sensing and communicating. Their use could be beneficial in a wide range of applications, including autonomous driving, smart cities, and the Internet of Things (IoT), with the potential to reduce the cost, size, and power consumption of the system by combining both functionalities. Existing systems could be upgraded to achieve this goal. The mobile network or the Wi-Fi standard can be mentioned. This work focuses on the development of an experimental setup that can perform communication and sensing tasks with an OFDM signal using the Wi-Fi 6 standard. For this purpose, the question of synchronization of the communication system is also discussed for the case of OFDM.

Acknowledgments

I would like to take a moment to express my heartfelt gratitude to all the people who helped me complete this thesis.

First and foremost, I would like to thank my supervisors, Prof. Claude Oestges, Prof. Luc Vandendorpe, François De Saint Moulin and Martin Willame for their guidance throughout this year. Their expertise, knowledge, and feedback have been invaluable in helping me to complete this thesis. I would like to extend a big thank you to François De Saint Moulin for all his help, support, and patience. He's been a great help to me in achieving this goal, and I'm really grateful for all his time and effort.

I would also like to extend my gratitude to Hasan Can Yildirim for his invaluable assistance in grasping the system, interfacing the hardware, and for his willingness to address my questions.

I would also like to thank Prof. Jérôme Louveaux for taking the time to read and evaluate this thesis.

Finally, I would like to take a moment to thank my family, my roommates, the fellow members of the B.232 room, my friends, who I have met at UCLouvain and before, as well as all the people whose names are embedded in the heart of the USRPs for I hope many years. A special thank you to Baptiste Sambon and Samuel Ahou for your help, support and motivation you gave me throughout this year. All those moments at the lab have been wonderful! And finally, I want to thank my parents, my brother, and Ollie for always being there for me throughout those years before I started my studies, during my time at UCLouvain, and for all the years to come.

ChatGPT[1], *Deepl*[2] and *GitHub Copilot*[3] were used to assist in the writing process.

Contents

Abstract i

Acknowledgments ii

List of Acronyms v

Introduction 1

1 State of the Art - Joint Communication and Sensing 3
- 1.1 General State of the Art . . . 3
  - 1.1.1 Radar-Centric Design . . . 3
  - 1.1.2 Communication-Centric Design . . . 6
  - 1.1.3 Joint Design . . . 7
  - 1.1.4 Comparison of the Different Designs . . . 9
- 1.2 OFDM Communication and Sensing . . . 10
  - 1.2.1 Communication . . . 10
  - 1.2.2 Sensing . . . 17

2 Wi-Fi Standard - IEEE 802.11 25
- 2.1 IEEE 802.11ax . . . 26
  - 2.1.1 Presentation of the Standard . . . 26
  - 2.1.2 Preamble and Tailing . . . 28
- 2.2 IEEE 802.11bf . . . 31
  - 2.2.1 PHY Layer . . . 31
  - 2.2.2 Sensing Configurations . . . 32
  - 2.2.3 Sensing Procedure . . . 33

2.3 Scenario . . . 35
2.4 Summary of the Wi-Fi Standard - IEEE 802.11 . . . 36

3 Experiment Setup 37
3.1 USRP - 2944R . . . 37
3.2 OctoClock - CDA-2990 . . . 40
3.3 Switch - CPS-8910 . . . 40
3.4 First Generation Setup . . . 41
3.5 Second Generation Setup . . . 43
3.6 Benchmarking . . . 44
3.7 Time Domain Representation of the Waveforms . . . 45
3.7.1 Communication . . . 45
3.7.2 Sensing . . . 47
3.8 Summary of the Experimental Setup . . . 48

4 Synchronization 49
4.1 Time Synchronization . . . 49
4.1.1 Correlation . . . 50
4.1.2 Schmidl & Cox Method . . . 50
4.1.3 Simulation Results . . . 52
4.2 Frequency Synchronization . . . 54
4.2.1 Classical Communication Algorithm . . . 54
4.2.2 JCAS Algorithm . . . 55
4.2.3 Simulation Results . . . 57
4.3 Summary of the Synchronization . . . 58

5 OFDM - Joint Radar and Communication 60
5.1 Communication . . . 60
5.2 Radar . . . 66
5.3 Summary of the OFDM - Joint Radar and Communication . . . 70

6 Experimental Results 72
6.1 Communication Performance . . . 72
6.2 Sensing Performance . . . 74
6.2.1 Clutter-Free Environment - Anechoic Chamber . . . 74
6.2.2 Laboratory Environment . . . 84
6.2.3 Outdoor Environment . . . 90
6.3 Summary of the Results . . . 99

Conclusion 100

Bibliography 102

List of Acronyms

10 GbE	10 Gigabit Ethernet
4G	Fourth generation of broadband cellular network technology
5G	Fifth generation of broadband cellular network technology
ADC	Analog to Digital Converter
AP	Access Point
API	Application Programming Interface
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
CA-CFAR	Cell Averaging Constant False Alarm Rate
CDMA	Code Division Multiple Access
CFAR	Constant False Alarm Rate
CFO	Carrier Frequency Offset
CPU	Central Processing Unit
CR	Clutter Removal
CSI	Channel State Information
DAC	Digital to Analog Converter
DC	Direct Component
DDC	Digital Down-Converter
DFE	Decision Feedback Equalizer
DFT	Discrete Fourier Transform
DLC	Delay Line Canceller

DOA	Direction of Arrival
DUC	Digital Up-Converter
ECA	Extended Cancellation Algorithm
ESPRIT	Estimation of Signal Parameters via Rotational Invariance Techniques
FAR	Frequency Agile Radar
FFT	Fast Fourier Transform
FMCW	Frequency Modulated Continuous Wave
FPGA	Field-Programmable Gate Array
GMM	Gaussian Mixture Model
GPS	Global Positioning System
HE	High Efficiency
HE-LTF	High Efficiency Long Training Field
HE-STF	High Efficiency Short Training Field
HE-SIG-A	High Efficiency Signal field A
ICI	Inter-Carrier Interference
IDFT	Inverse Discrete Fourier Transform
IEEE	Institute of Electrical and Electronics Engineers
IFFT	Inverse Fast Fourier Transform
IoT	Internet of Things
IQ	In-phase and Quadrature components
ISAC	Integrated Sensing and Communication
ISI	Inter-Symbol Interference
JCAS	Joint Communication and Sensing Systems
L-LTF	Legacy Long Training Field
LNA	Low Noise Amplifier
LTF	Long Training Field
MAC	Medium Access Control
MI	Mutual Information
MIMO	Multiple Input Multiple Output
ML	Maximum Likelihood
MMSE	Minimum Mean Square Error
MRT	Maximum Ratio Transmission

MU-MIMO	Multi-User MIMO
MUSIC	Multiple Signal Classification
NDP	Null Data Packet
NDPA	Null Data Packet Announcement
NI	National Instruments
NTB	Non-Trigger Based
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
PCIe	Peripheral Component Interconnect Express
PHY	Physical Layer
PPDU	Physical Protocol Data Unit
PPS	Pulse Per Second
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RAM	Random Access Memory
RL-SIG	Repeated Legacy Signal Field
RMA	Recursive Moving Average
RX	Receiver
SDR	Software Defined Radio
SIG	Signal Field
SISO	Single Input Single Output
SNR	Signal to Noise Ratio
SSD	Solid State Drive
STF	Short Training Field
TB	Trigger Based
TF	Trigger Frame
TX	Transmitter
UE	User Equipment
UHD	USRP Hardware Driver
ULB	Université Libre de Bruxelles
USRP	Universal Software Radio Peripheral

WLAN	Wireless Local Area Network
ZF	Zero Forcing
ZP	Zero Padding

Introduction

In recent years, there has been an increasing interest in integrated sensing and communication systems, also known as Joint Communication and Sensing (JCAS) systems. Those systems are capable of performing both communication and sensing tasks. Such applications could be used in a multitude of contexts, including autonomous driving, smart cities, and IoT. In the context of future automotive applications, the sensing capabilities provided by radar could facilitate precise detection of objects in poor weather conditions, with the potential to be employed in automated vehicles[4]. The joint implementation of radar and communication systems would reduce the need for separate components, thus reducing the cost, size, and power consumption of such system. Moreover, as the frequency spectrum is a scarce resource, the joint implementation of radar and communication would allow for more efficient use of this resource and help to address the problem of spectrum scarcity[5].

Existing communication systems could benefit from upgrades that would enable them to perform sensing tasks. The new Wi-Fi standard, IEEE 802.11bf, is the first amendment that focuses on the sensing capabilities of the Wi-Fi. This new standard allows to perform sensing tasks with the Wi-Fi signal. This standard is a good candidate for sensing as it is already widely deployed and the hardware is already available[6]. Indeed, with more than 3 billions new devices shipped every year. Moreover, those devices are present in most homes[7]. Wi-Fi sensing could be used in a wide range of applications, such as smart homes, where fall detection[8] or monitoring the breathing rate of a person[9] in remote healthcare scenarios could take place.

Another system that could potentially benefit from such upgrades is the mobile

network. [10] proposes the creation of a perceptive mobile network that would benefit from the larger capabilities than the Wi-Fi. Indeed the mobile network has access to larger bandwidth, more antennas, and more computational power. Such a network would be capable of performing more complex sensing tasks, including environmental sensing (e.g., animal migration, rainfall monitoring,etc) and be used in smart cities (e.g., crowd management, automatic street lighting systems,etc).

This study is concerned with the development of an experimental setup that can perform communication and sensing tasks with an OFDM signal in accordance with the Wi-Fi standard.

Contributions The objective of this research is to develop an experimental JCAS setup that can perform communication and sensing tasks with an OFDM signal. One of the key contributions is the design and evaluation of this setup. This setup has been studied in the context of the new Wi-Fi standard, IEEE 802.11bf. Another contribution is the comparison of timing and frequency synchronization methods for OFDM systems.

Outline The report is structured as follows. The state of the art of JCAS systems is presented in Chapter 1 with a broad overview, as well as a focus on the OFDM JCAS systems. Chapter 2 presents the Wi-Fi standard and the new IEEE 802.11bf amendment. It is also in this chapter that the scenario of the tested experimental setup is presented. The experimental setup used in this work is presented in Chapter 3 with some details on the hardware and software used. Chapter 4 compares time and frequency synchronization methods in the context of OFDM systems. The system and the different blocks that compose it are presented in Chapter 5. Finally, the experimental results for the communication and the sensing are presented in Chapter 6.

CHAPTER 1

State of the Art - Joint Communication and Sensing

The objective of this chapter is to conduct a review of the state of the art of JCAS systems, with a focus on their general characteristics and the various design approaches that have been employed in this domain. This review is divided into two sections. The first section presents an overview of the current state of JCAS systems and their associated designs, and provides a comparative analysis between these approaches. The second section is devoted to the study of OFDM systems within the context of JCAS. OFDM is employed in contemporary communication systems, including 4G, 5G, and Wi-Fi. This section is divided into two parts. The first is dedicated to OFDM communication, while the second is dedicated to OFDM sensing.

1.1 General State of the Art

It is possible to employ a number of different techniques in order to achieve communication and sensing simultaneously. [10] identifies three main categories of design: radar-centric, communication-centric, and joint design. This section presents the different design techniques and compares them.

1.1.1 Radar-Centric Design

A radar-centric focus on the radar function with an additional capability for communication. The main objective of such design is to optimize the radar part of the

system. [4] provides two different examples of such system.

FMCW The first system implements communication capabilities on a Frequency Modulated Continuous Wave (FMCW) radar. The emitted waveform for one pulse of a FMCW signal is represented by

$$s_m(t) = e^{j2\pi f_c t + j\pi\gamma t^2}, t \in [mT_{\text{PRI}}, (m+1)T_{\text{p}}], \tag{1.1}$$

where f_c is the carrier frequency, γ is the chirp rate, T_{PRI} is the pulse repetition interval, T_p is the duration of a chirp and m is the pulse index. The FMCW radar waveform is represented in Figure 1.1. In this figure, 3 pulses (chirps) are transmitted. Each chirp is constituted by a signal exhibiting an increasing frequency over a specific bandwidth, f_{BW}. In the figure, the pulse repetition interval T_{PRI} is equivalent to the duration of a chirp T_p.

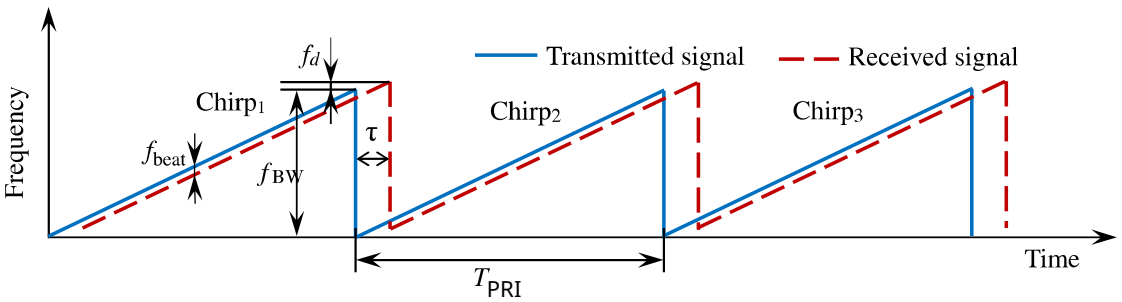


Figure 1.1: FMCW Radar waveform[11] - The blue curve represents the emitted chirps, while the red dashed curve represents the received chirps.

Following the alteration of the signal by the environment, a delay and a Doppler shift are introduced, resulting in the received chirps, represented in Figure 1.1. The delay is represented by τ and the Doppler shift by f_d. If there are K targets present in the scene, the received signal is given by

$$y(t) = \sum_{k=1}^{K} \alpha_k s(t - \tau_k) + w(t), \tag{1.2}$$

where,

$$\tau_k = \frac{2(r_k + v_k t)}{c}. \tag{1.3}$$

In (1.3), r_k represents the distance between the radar and the k^th target, v_k is the velocity of the k^{th} target, c is the speed of light, α_k is the attenuation due to the

k^{th} target, $s(t)$ is the emitted signal and $w(t)$ is the noise. The received signal is then processed in order to estimate the range and the Doppler effect of the targets. If the expression is developed, the received signal is given by

$$y(t) = \sum_{k=1}^{K} \tilde{\alpha_k} e^{-j2\pi(\frac{2\gamma r_k}{c} + \frac{2v_k f_c}{c})t} + w(t), \tag{1.4}$$

where $\tilde{\alpha_k} = \alpha_k e^{-j2\pi c \frac{2r_k}{c}}$.

The presented equations are for a Single-Input Single-Output (SISO) system. The addition of multiple antennas on the receiver side would allow the system to estimate the angle of arrival of the arriving signal after being reflected on the targets. In such systems, the range and the Doppler effect can be estimated by using the discrete Fourier transform (DFT). However, both the Delay and the Doppler effect are coupled.

As this waveform was originally designed for radar applications, its processing is well known. To implement the communication capabilities in this system, [4], proposes to use the phase of the waveform to encode the data. Equation (1.1) then becomes

$$s_{m,new}(t) = s_m(t) e^{j\phi_m}, \tag{1.5}$$

where ϕ_m is the phase that is used to encode the data. To enhance the data rate of such system, it is proposed to use multiple orthogonal waveforms and beamforming techniques. The data is then modulated on the phase of the waveforms.

Index Modulation The second example of radar-centric design is the implementation of communication capabilities with a frequency agile radar (FAR). [12] presents the FAR as a necessity for the increasingly congested environment that we live in. The frequency use by the FAR is not fixed and changes randomly to counter this jamming. This system can be tuned to perform a communication system. Indeed, instead of randomly changing the frequency used by the FAR, it can be used to encode data. Figure 1.2 presents such a system, where the two transmitters are used to send a message. To encode the data, the transmitters will use combinations of carrier frequencies from a predefined dictionary, linking the transmitted bits to the frequencies used. A more visual explanation of the system is presented in the figure, with the emission of the sequence "110" by having the first transmitter using the frequency f_2 and the second transmitter using the frequency f_3.

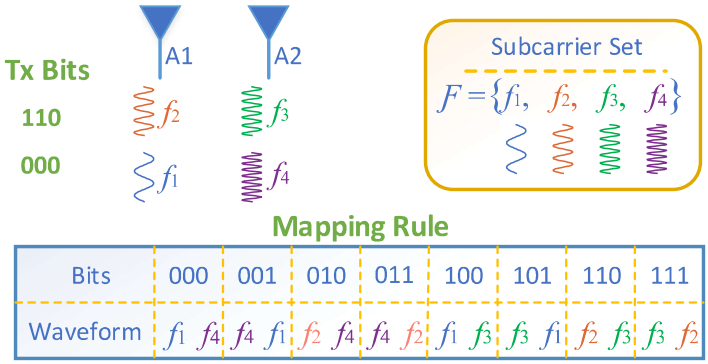


Figure 1.2: Frequency agile radar example[4].

For a single antenna system, the mth transmitted signal is expressed as

$$s_m(t) = e^{j2\pi f_m t}, \tag{1.6}$$

where f_m is the frequency used by a transmitter. It is selected from a dictionary of N frequencies. The received signal, in a scene with K targets, is given by

$$y_m(t) = \sum_{k=1}^{K} \alpha_k e^{j2\pi f_m \frac{2r_k}{c} - j2\pi f_m \frac{2v_k(m-1)T_{\text{PRI}}}{c}} + w(t). \tag{1.7}$$

After performing a Delay-Doppler process, the range and speed of the targets can be estimated. In the event of communication, the carrier frequency can be retrieved, allowing for the decoding of the information.

1.1.2 Communication-Centric Design

The communication-centric design uses an existing communication system and introduces the capability to perform sensing. One example of such systems is the OFDM system. One possible use of the OFDM for both communication and sensing is presented in subsection 1.2.

[13] presents other examples of the utilization of communication centric design. These examples can be based on the division between radar and communication systems. Non-overlapped resource allocations are widely used in communication systems and are well known in the context of multi-user environments. If used in the context of JCAS, some resources are allocated to the radar and some to the communication system. The radar waveform can be a traditional radar waveform, and it is separated from the communication one by using an orthogonal resource. Some of those techniques are the following :

- **Time Division**: The time is divided between the radar and the communication system. Some time frames are allocated for the radar to use, while the communication system is not using it and inversely. The number of time slots as well as their duration can be fixed or variable.
- **Frequency Division**: The frequency is divided between the radar and the communication systems. Those resources can be OFDM subcarriers or separate frequency bands. In this case, some subcarriers may be allocated to sensing capabilities and others to communication. This kind of division is not addressed in the previously referenced section.
- **Code Division**: The radar and the communication system may use different codes to transmit their respective information. This approach is used for communication in CDMA systems. The signal is spread with a different code for the radar and the communication system. This renders the signal of the radar and the communication system orthogonal if the codes are carefully selected, thus orthogonal.
- **Space Division**: The radar and the communication system may use different antennas. This can be used in MIMO systems. The radar and the communication systems may use the same frequency and time resources, yet the antennas may be different and beamforming techniques may be employed to separate the signals.

1.1.3 Joint Design

The objective of the joint design is to optimize both the radar and the communication system without relying on an existing one. This should provide greater flexibility to the design as it is not constrained by predefined systems. [14] presents different techniques in MIMO that can be used to perform this. Firstly, the two received signals are presented as

$$\mathbf{y}_R = \mathbf{H}_R\mathbf{x} + \mathbf{w}_R, \tag{1.8}$$

for the radar system and

$$\mathbf{y}_C = \mathbf{H}_C\mathbf{x} + \mathbf{w}_C, \tag{1.9}$$

for the communication system. In (1.8) and (1.9), $\mathbf{y}$ is the received signal, $\mathbf{H}$ is the channel matrix, $\mathbf{x}$ is the transmitted signal and $\mathbf{w}$ is the noise. A subscript R linking those variable to the radar, while a C to the communication. The objective is to find an optimal transmit signal, $\mathbf{x}$, to optimize both radar and communications performance.

The first method proposed is based on spatial precoding. In this case, a precoding matrix denoted $\mathbf{P}$ is optimized, and an objective function $\lambda(\mathbf{P})$ is defined. The optimization can be presented as follows:

$$\mathbf{P}^* = \arg\max_{\mathbf{P}} \lambda(\mathbf{P}) \qquad \text{s.t. Constraints,} \tag{1.10}$$

where the constraints are related to the power of the transmitted signal, the orthogonality of the precoding matrix, and the power of the noise, etc. The optimal precoding matrix is denoted $\mathbf{P}^*$.

Mutual Information In order to define the objective function and perform the optimization, [14] proposes a few techniques, the first is based on mutual information (MI). MI for radar systems represents the amount of information about the environment that is conveyed to the receiver[15]. It is given by

$$I_R(\mathbf{H}_R; \mathbf{Y}_R|R) = M\log_2\left(\det\left(\frac{1}{\sigma_w^2}\mathbf{X}^H\mathbf{\Sigma}_{H_R}\mathbf{X} + \mathbf{I}_K\right)\right), \tag{1.11}$$

where M represents the number of antennas[1], $\mathbf{X}$ is the transmitted signal, $\mathbf{\Sigma}_{H_R}$ is the covariance matrix of the received signal, $\mathbf{I}_K$ is the identity matrix, and σ_w^2 is the noise variance.

In the same way, for communication systems, the MI represents the amount of information conveyed from the transmitter to the receiver and is given by

$$I_C(\mathbf{H}_C; \mathbf{Y}_C|C) = M\log_2\left(\det\left(\frac{1}{\sigma_w^2}\mathbf{X}^H\mathbf{\Sigma}_{H_C}\mathbf{X} + \mathbf{I}_K\right)\right), \tag{1.12}$$

A formulation based on a weighted sum of the MI is proposed. The function to optimize is given by

$$F = \frac{w_R}{F_R} I_R(\mathbf{H}_R; \mathbf{Y}_R|\mathbf{X}) + \frac{1 - w_R}{F_C} I_C(\mathbf{X}; \mathbf{Y}_C|\mathbf{H}_C), \tag{1.13}$$

where w_R is the weight of the radar system, F_R is the maximal value of the MI of the radar, and F_C is the maximal value for the one of the communication system. The optimization is then performed on F. The paper states that F is a concave function, so the optimization can be performed with a convex optimization algorithm.

[1]M is the number of antennas both at the receiver and the transmitter.

Waveform Similarity The second technique proposed by [14] is based on waveform similarity. The optimization is performed to maximize the similarity between the designed waveform and a benchmark one. In this case, the multi-user interference is minimized. The objective function is given by

$$\arg\min_{\mathbf{X}} ||\mathbf{H}_C\mathbf{X} - \mathbf{S}||_F^2 \qquad \text{s.t.} \begin{cases} ||\text{vec}(\mathbf{X}) - \text{vec}(\mathbf{X}_0)|| \leqslant \epsilon, \\ |x_{i,j}|^2 = \frac{P_T}{M_T}, \forall i, j. \end{cases} \tag{1.14}$$

In (1.14), $\mathbf{S}$ is the information symbols, $\mathbf{X}_0$ is the benchmark waveform, ϵ is the similarity threshold, P_T is the total power and M_T is the number of antennas at the transmitter side. The objective of the optimization is to minimize the difference between the transmitted signal and the benchmark signal while respecting the power constraint and minimizing the multi-user interference. The problem is non-convex, but it can be solved with a branch-and-bound algorithm[15].

1.1.4 Comparison of the Different Designs

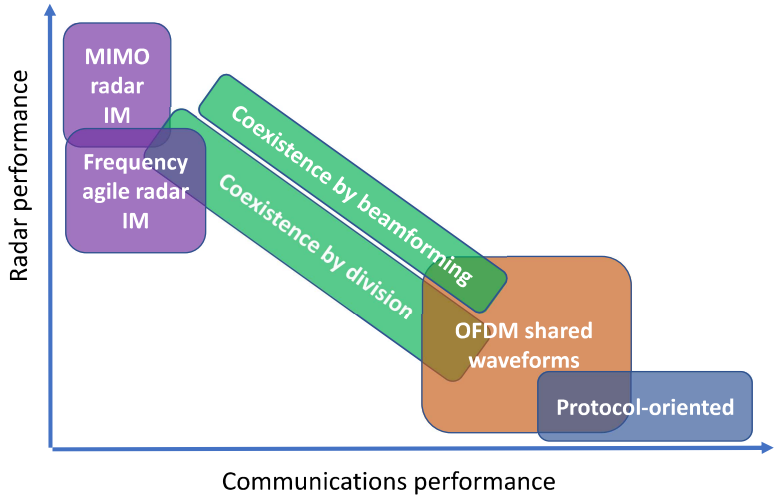


Figure 1.3: Tradeoff between the radar and the communication performances in JCAS systems[4].

[4] presents a comparison of the different designs thanks to Figure 1.3. The comparison represents the trade-off between the radar and the communication performances. It is evident that the radar-centric design has a superior radar performance than the communication-centric design. In this category stands the index modulation either with FAR or with MIMO wideband radar. Such techniques

result in a limited bit rate and thus give poor communication performances.

On the other side of the spectrum, the communication-centric design holds a better communication performance compared to the radar-centric design. In this category stands the OFDM systems, wherein a part of the subcarriers is used for sensing and the remaining for communication. The protocol-oriented JCAS system give the best performances for the communication but the worst for the radar. Indeed, in such system, the radar must use only a known portion of the signal such as the preamble, and has to use the communication protocol to perform the sensing. In such systems, the communication is the primary objective, whereas the radar is a secondary task.

The coexistence of both systems is observed between the aforementioned extremes. This coexistence can be achieved through either a division, as previously demonstrated, or through the use of beamforming techniques.

1.2 OFDM Communication and Sensing

This section is dedicated to the state of the art of the JCAS, which employs OFDM techniques to perform both communication and the sensing. This technique is used in modern communication systems such as 4G, 5G and Wi-Fi. The chapter is divided into two parts. The first part is dedicated to the OFDM communication and the second to OFDM sensing.

1.2.1 Communication

This subsection is dedicated to the use of the OFDM only for the communication part. The signal is introduced as well as the modulation and demodulation.

Time Frequency Representation

OFDM systems are based on the division of the available bandwidth into multiple subcarriers. The total number of subcarriers is N_{sc} and the spacing between them is thus given by $\Delta f = \frac{B}{N_{sc}}$, where B is the total available bandwidth. The symbols are mapped across the subcarriers of an OFDM symbol. This mapping is presented in Figure 1.4 with the time-frequency representation of the OFDM symbols. The frequency axis is divided into N_{sc} subcarriers, while the time axis is divided into N_{symb} OFDM symbols. The transition from one axis to the other is performed by the Inverse Fast Fourier Transform (IFFT) and Fast Fourier Transform (FFT) operations, which go respectively to the time and frequency domain.

A cyclic prefix is also appended between each OFDM symbol.

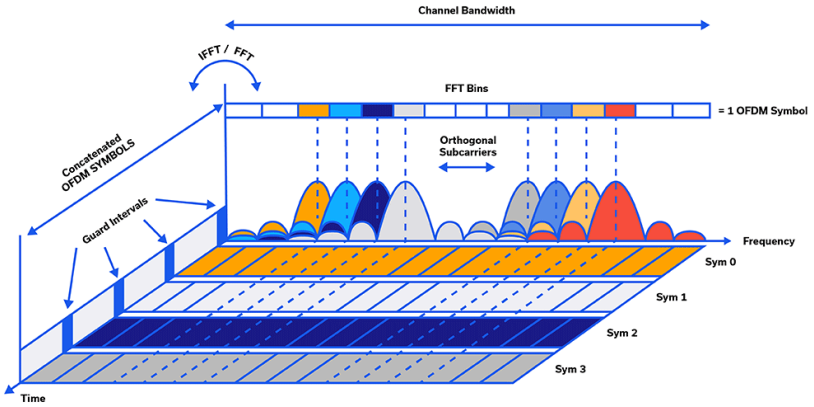


Figure 1.4: OFDM Time-Frequency representation[16].

[13] represents a flow chart of the OFDM communication system. This is presented in Figure 1.5. The flow chart is divided into two parts. The upper part is dedicated to the transmitter, while the lower part to the receiver.

Transmitter The transmitter part works as follows. The data payload, i.e. the information to be transmitted, is converted from a serial to a parallel format. The number of parallel streams is equal to the number of subcarriers N_{sc}. The data is then modulated. The modulation can be BPSK, QPSK, 16-QAM, 64-QAM, and so forth. The IFFT is applied to the data, transforming it from the frequency domain to the time domain. The parallel to serial conversion is then performed. Finally, the digital to analog conversion is carried out. A local oscillator is used to convert the signal to the desired carrier frequency.

An important aspect of OFDM systems that is not represented in this flowchart is the incorporation of the cyclic prefix[17]. The cyclic prefix is added to the signal to prevent inter-symbol interference (ISI). In fact, this prefix converts inter-symbol interference channels into ISI-free channels.[18]. The cyclic prefix is a copy of the last portion of the OFDM symbol in the time domain. It should be at least equal to the length of the channel impulse response.

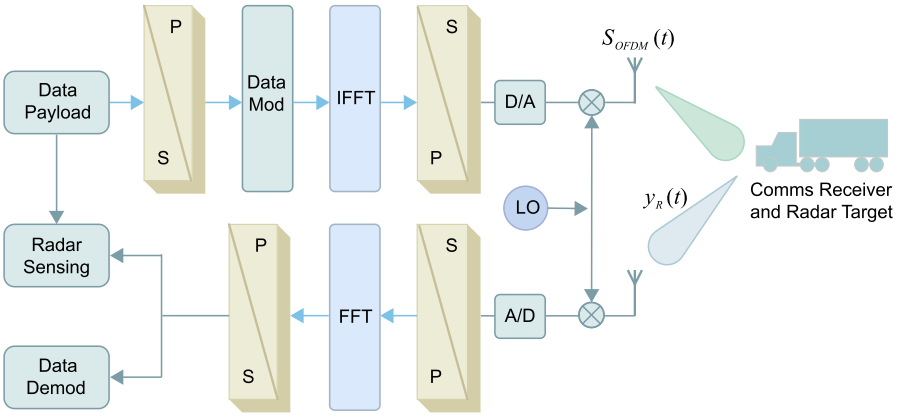


Figure 1.5: OFDM communication and sensing system flow chart[13].

[13] represents the emitted signal $s_{\mathrm{OFDM}(t)}$ as a sum of the OFDM symbols. The signal is given by

$$s_{\mathrm{OFDM}(t)} = \sum_{m=1}^{N_s} \sum_{n=1}^{N_{sc}} d_{m,n} \cdot e^{j2\pi f_n t} \mathrm{rect}\left(\frac{t-(m-1)T_{\mathrm{OFDM}}}{T_{\mathrm{OFDM}}}\right), \tag{1.15}$$

where $d_{m,n}$ represents the data on the n^th subcarrier of the m^th OFDM symbol, f_n the frequency of the n^th subcarrier, T_{OFDM} the duration of an OFDM symbol, and $\mathrm{rect}(t)$ the rectangular window function. This window function is used to limit the signal in time, but can be replaced by other functions.

Window Function Optimization Indeed, [19] proposes an algorithm for optimizing the window function with the goal of reducing the spectral side lobes that are present with a classical rectangular window. [20] suggests improved Nyquist windows that reduce the interference between the subcarriers, thereby increasing the performance of the OFDM system. Commonly used Nyquist windows are the rectangular and raised cosine ones.

Precoder To enhance the performance of the system, a precoder can be employed. It is possible to use precoders in multiple antenna systems. Such techniques are presented in [21]. The precoder allows the system to have multiplexing capabilities or to have diversity. The diversity gain will decrease the error rate for a fixed transmit power, while the multiplexing capabilities are the ability to send multiple data streams at the same time. Systems of precoder can either be used with or without channel knowledge. For instance, the Alamouti precoder[22] is a precoder that does not require the channel knowledge. Additionally, [23] cites linear precoders such as maximum ratio transmission (MRT), zero-forcing (ZF)

and minimum mean square error (MMSE). As well as non-linear precoders such as dirty paper coding[24], Tomlinson-Harashima precoding[25], and vector perturbation precoding[26]. The performances offered by non-linear precoders are superior to those of linear ones. Dirty paper coding, in particular, can achieve the capacity of the channel.

The precoder can be applied to the emitted signal as presented in (1.16) if a linear precoder is used. In this case, the precoder multiplies the signal, $\mathbf{s}(t)$, by a matrix $\mathbf{W}$ to obtain the precoded signal $\mathbf{x}(t)$.

$$\mathbf{x}(t) = \mathbf{W}\mathbf{s}(t) \tag{1.16}$$

Coding Scheme In order to enhance the performance of the communication system, a classical coding scheme can also be used on the data payload, such as error-correcting codes. As this is a separate topic in itself, it will not be discussed in this chapter.

Channel Model The channel alters the signal in a way that is defined by the channel models. [10] and [14] present such a model, which is defined at time t as follows:

$$\mathbf{H}(t) = \sum_{l=1}^{L} b_l \delta(t - \tau_l - \tau_0(t)) e^{j2\pi(f_{D,l}+f_0(t))t} \mathbf{a}(M_2, \phi_l)\mathbf{a}^{\mathbf{T}}(M_1, \theta_l). \tag{1.17}$$

In the context of OFDM systems, the channel that affects the k^{th} OFDM pulse and the n^{th} subcarrier is given by

$$\mathbf{H}_{\mathbf{n},\mathbf{k}} = \sum_{l=1}^{L} b_l e^{-2\pi n(\tau_l+\tau_0(k))f_c} e^{j2\pi k(f_{D,l}+f_0(k))T_s} \mathbf{a}(M_2, \phi_l)\mathbf{a}^{\mathbf{T}}(M_1, \theta_l). \tag{1.18}$$

The channel is multipath and composed of L paths. It is defined by the following parameters:

- b_l is the attenuation and initial phase difference of the l^{th} path.
- τ_l is the delay of the l^{th} path.
- $\tau_0(t)$ is the timing offset between the receiver and the transmitter.
- f_c is the carrier frequency offset between the receiver and the transmitter.
- $f_{D,l}$ is the Doppler shift of the l^{th} path.
- f_0 is the carrier frequency offset.
- T_s is the sampling period.

- $\mathbf{a}(M_2, \phi_l)$ is the steering vector of the receiver, M_2 is the number of antennas at the receiver and ϕ_l is the angle of arrival of the l^{th} path.
- $\mathbf{a}(M_1, \theta_l)$ is the steering vector of the transmitter, M_1 is the number of antennas at the transmitter and θ_l is the angle of departure of the l^{th} path.

The steering vector is given by

$$\mathbf{a}(M, \theta) = \begin{bmatrix} 1 \\ e^{j2\pi d/\lambda \sin(\theta)} \\ \vdots \\ e^{j2\pi(M-1)d/\lambda \sin(\theta)} \end{bmatrix}. \tag{1.19}$$

It can be observed that when the number of antennas at the transmitter and receiver is equal to one, the steering vector matrix is not present in the equation. In addition to the channel model, the signal is affected by noise. This noise is added to it at the receiver and is modeled as an Additive White Gaussian Noise (AWGN) with a variance of σ^2. The received signal is then given by

$$\mathbf{y}(t) = \mathbf{H}\mathbf{x}(t) + \mathbf{w}(t), \tag{1.20}$$

where $\mathbf{y}(t)$ is the received signal, $\mathbf{H}$ is the channel matrix, $\mathbf{x}(t)$ is the transmitted signal and $\mathbf{w}(t)$ is the noise. In the case of OFDM systems, this operation leads to the following signal for the k^{th} OFDM pulse and the n^{th} subcarrier:

$$y_{n,k} = H_{n,k}x_{n,k} + w_{n,k}, \tag{1.21}$$

Receiver The receiver part is the dual of the transmitter. As illustrated in Figure 1.5, after being downconverted to baseband, the signal is converted from analog to digital. It is then goes from serial to parallel. Prior to the DFT[2], the cyclic prefix is removed. The DFT is performed to go from the time domain to the frequency domain where the symbols are present. The demodulation is then performed.

Synchronization [13] assumes a perfect synchronization between the transmitter and the receiver. This is illustrated by the use of the same local oscillator for both the emitter and the receiver. However, it is important to note that synchronization is a critical aspect of communication systems. Synchronization can be of two nature: time and frequency synchronization. The time aspect of synchronization is used to find the start of a sequence and the correction of timing offset between the transmitter and the receiver. The frequency synchronization

[2]To reduce the complexity of the computation, the FFT is generally used.

correct the carrier frequency offset that can appear due to the Doppler effect or the oscillator drift between the two devices. In OFDM systems, the orthogonality between the subcarriers is a key aspect. However, it may be lost if the carrier frequency offset is not corrected[27].

Time synchronization can be performed with the Schmidl & Cox algorithm[28]. This algorithm is presented in Chapter 4 of this work. This algorithm uses a two-time repetition of a sequence of symbols to estimate the timing offset. Alternatively, a correlation with a known symbol can also be used to identify the start of a sequence and thus to find the timing offset. [29] proposes a comparison between the modulation constellation to identify the optimal modulation scheme and the length of the cyclic prefix that allows for a more efficient OFDM system. The cyclic prefix length allows for a time synchronization that is not perfect.

The Schmidl & Cox algorithm, as described in [28], can also be employed for frequency synchronization. [30] proposes the use of an FFT on a known preamble to estimate the frequency offset.

Equalization Figure 1.5 does not illustrate equalization. Nevertheless, this is a crucial element of multipath channels communication systems. Its objective is to rectify the channel H in the received signal. Equalization can be executed through diverse methodologies. One common approach is the zero forcing (ZF) equalization, which is expressed as follows:

$$\hat{\mathbf{x}}(t) = \mathbf{H}^{-1}\mathbf{y}(t). \tag{1.22}$$

By using (1.20), it can be demonstrated that ZF equalization is given by

$$\begin{aligned} \hat{\mathbf{x}}(t) &= \mathbf{H}^{-1}\mathbf{H}\mathbf{x}(t) + \mathbf{H}^{-1}\mathbf{w}(t) \\ &= \mathbf{x}(t) + \mathbf{H}^{-1}\mathbf{w}(t). \end{aligned} \tag{1.23}$$

One potential issue with this equalization is that it may amplify the noise if the channel is ill-conditioned. In the context of multi-user systems, ZF takes the interference between the users into account.

In order to account for the noise, a maximum likelihood (ML) equalization can be employed, and is defined as follows:

$$\hat{\mathbf{x}}(t) = \arg\min_{\mathbf{x}(t)} ||\mathbf{y}(t) - \mathbf{H}\mathbf{x}(t)||^2. \tag{1.24}$$

The ML equalization is the optimal equalization, yet it is computationally expensive and only works well if the noise is Gaussian.

An alternative form of equalization is the MMSE equalization, which is given by

$$\hat{\mathbf{x}}(t) = \mathbf{H}^H(\mathbf{H}\mathbf{H}^H + \sigma^2\mathbf{I})^{-1}\mathbf{y}(t), \tag{1.25}$$

where $\mathbf{H}^H$ is the conjugate transpose of $\mathbf{H}$ and $\mathbf{I}$ is the identity matrix. The MMSE equalization is a trade-off between the ZF and the ML ones. Those methods have been studied in [17] and [21]. All of these equalization methods are linear. They use the channel matrix, $\mathbf{H}$,which must be estimated at the receiver. The channel estimation can be performed with different methods. In [21], channel sounding is introduced. It is the emission of a known signal by the transmitter. The receiver can then estimate the channel by comparing the received signal with the known one. If both the uplink and downlink channel can be estimated. Nevertheless, in most communication systems, a preamble is added to the signal and the channel estimation is performed thanks to it. In OFDM systems, pilots can also be added either in time, frequency, or a combination of both domains. Such mapping of the pilots is presented in Figure 1.6. Those symbols are known at the receiver and can be used to estimate the channel thanks to an interpolation. The rate at which pilots are added should be sufficient to estimate the channel. If the channel is time varying, the pilots should be added more frequently in the time domain. If the channel is frequency selective, the pilots should be added more frequently in the frequency domain. [31] presents a comparison of the channel estimation with the pilots at specific pulse or at specific subcarriers.

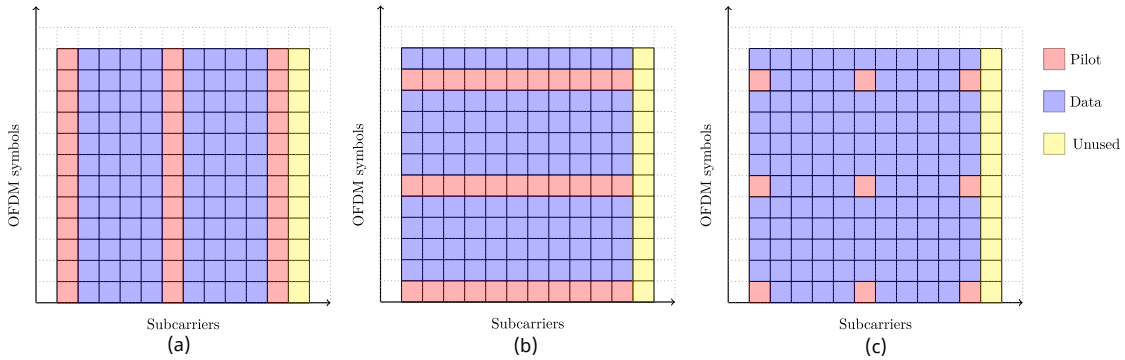


Figure 1.6: OFDM pilots arrangement : (a) pilots in specific subcarriers, (b) pilots in specific OFDM symbols, (c) pilots in both specific subcarriers and OFDM symbols.

More complex equalization techniques, such as the Decision Feedback Equalization (DFE), exist and allows for better performances. With the DFE, the equalization is performed by removing the interference between the symbols. This can be achieved by using the previous symbols to estimate the current one[32]. Turbo

equalization can also be used to perform this task. This is a non-linear equalization and is presented in [33] in an iterative way.

Performance Evaluation Following the equalization process, the data is demodulated, allowing for the evaluation of the performance of the system with different metrics. One of the most common metrics is the bit error rate (BER), which is defined as the number of bits that are received in error compared to the number of bits that are sent.

1.2.2 Sensing

OFDM modulation can also be used for sensing. [4] presents two constraints that a radar system should respect. The first one is the low side lobe level, and the second is the low peak-to-average power ratio. In OFDM, the first constraint can be achieved by replacing the rectangular window with another window function. Such windows are presented in [19] and [20]. The second one can be achieved by using a precoder or by using a weighted OFDM method. The weighted methods are presented in [34] and [35].

One of the principal advantages of the OFDM waveform is that the range and the Doppler effect are decoupled. This is presented in [4]. The range may be obtained by performing an FFT of the received signal and the Doppler effect by performing an IFFT of the received signal if simple algorithms are used. [13] presents the received signal in a SISO system, after being affected by the channel containing one target, and expresses it as

$$y_R(t) = \sum_{m=1}^{N_s} e^{j2\pi f_D t} \sum_{n=1}^{N_{sc}} \alpha_{m,n}(d_{m,n}e^{-j2\pi f_n \tau})e^{j2\pi f_n t}\text{rect}\left(\frac{t-(m-1)T_{\text{OFDM}}}{T_{\text{OFDM}}}\right) + w(t). \tag{1.26}$$

In this equation, f_D is the Doppler frequency, $\alpha_{m,n}$ is the attenuation and $d_{m,n}$ is the data on the n^{th} subcarrier of the m^{th} OFDM symbol, τ is the delay of the target, f_n is the frequency of the n^{th} subcarrier, T_{OFDM} is the duration of an OFDM symbol and $w(t)$ is the noise.
The article proposes that, following the sampling and the application of an FFT, the received signal should be rewritten as

$$y_{m,n} = \alpha_{m,n}d_{m,n}e^{-j2\pi(n-1)\Delta f \tau}e^{j2\pi f_D(m-1)T_{\text{OFDM}}} + w_{m,n}. \tag{1.27}$$

If the dependency with respect to the sent symbols is removed by dividing by the data and the noise neglected, the received signal is given by

$$y_{m,n} = \alpha_{m,n} e^{-j2\pi(n-1)\Delta f \tau} e^{j2\pi f_D (m-1) T_{\text{OFDM}}}. \tag{1.28}$$

The division by the data is possible thanks to its knowledge that the article assumes. In (1.28), the received signal is only dependent on the delay and the Doppler. Only an IFFT on the columns of the matrix is needed to obtain the Doppler estimate and an FFT on the rows of the matrix is needed to obtain the range one. This decoupling is one of the main advantages of the OFDM modulation for sensing. Nevertheless, one can notice from (1.18) that the channel is also dependent on the CFO. In the development presented by the article, the CFO is neglected. If one employs the signal with a signal with a corrected CFO for the processing, the result of the Doppler estimation will be erroneous.

In the event that the system employs multiple antennas, it is necessary to incorporate steering vectors into the received signal. One signal is obtained for each antenna and a tensor of the system is obtained. The tensor can then be used to estimate the range, the Doppler, and the angle of arrival of the received signal.

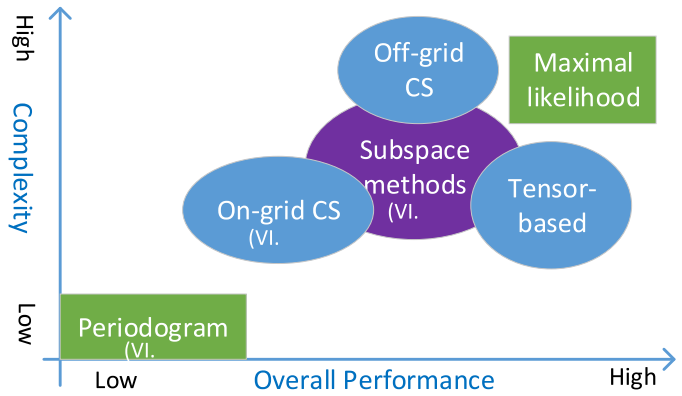


Figure 1.7: Comparison of OFDM sensing algorithms[10].

Sensing Parameters Estimation - Periodogram The estimation of the sensing parameters can be achieved through a number of different approaches. [10] shows in Figure 1.7 various methods to estimate those parameters with the qualitative performance and complexity estimates for each method. The previously presented method based on 2D-FFT is the periodogram method. [10] reminds that a windowing technique can be employed to mitigate the impact of sidelobes appearing due to the FFT. These lobes are observable in Figure 1.8 in plot (a).This method is the least complex but offers the poorest performance. It can be a first guess of the estimation and be used by the other methods as a starting point.

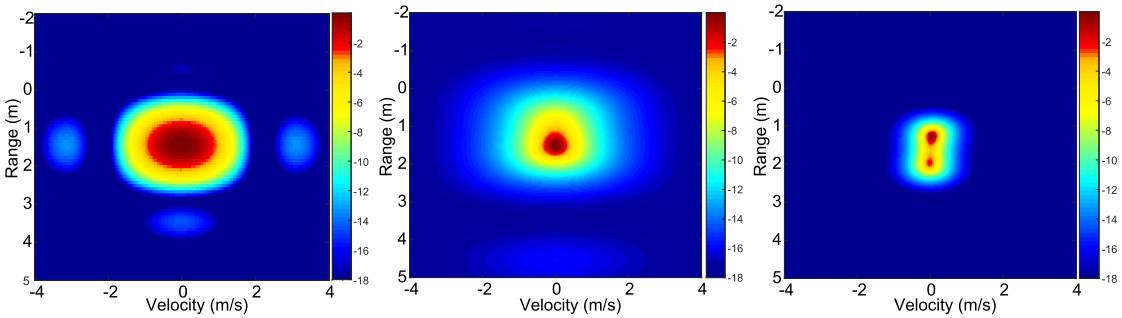


Figure 1.8: "Measured radar image for two targets using (a) 2D-DFT technique, (b) the 2D-MUSIC technique (without the communication signal) and (c) the proposed method (2D-MUSIC using the communication signal)"[36].

Sensing Parameters Estimation - Subspace Methods More complex methods than the periogoram one exist. One can note the subspace methods, which include the MUSIC (MUltiple SIgnal Classification) and the ESPRIT (Estimation of Signal Parameters via Rotational Invariant Techniques) ones. The two methods can estimate the parameters with a high resolution and can perform off-grid estimation. Both algorithms require prior knowledge of the number of targets present in the scene. They work by separating the signal space and the noise one. In order to achieve this, a significant number of samples are required.

[36] provides an overview of the direction of arrival (DOA) estimation approach based on the MUSIC algorithm. [37] proposes to use the MUSIC algorithm to estimate the range and the Doppler effect. The algorithm is based on the estimation of the covariance matrix of the received signal. It also improves the MUSIC algorithm by using the transmitted data to refine the estimation. Figure 1.8 illustrates the results of the MUSIC algorithm with and without the use of transmitted data. It demonstrates that, in comparison to the 2D-DFT technique, the MUSIC algorithm offers superior resolution and is capable of differentiating between two targets present in the scene.

Sensing Parameters Estimation - Compressive Sensing As the system is sparse (only K targets are present and must be estimated), compressive sensing can be employed to estimate the parameters of those targets. A sparse signal recovery problem is formulated. Multiple methods can be used to estimate the targets. The most common method is the Orthogonal Matching Pursuit algorithm, although other methods such as the Basis Pursuit algorithm exist, as cited

in [38].

This method can be either on-grid or off-grid. In the former case, the targets are estimated on a grid in a limited space with a limited dictionary. In contrast, the off-grid case uses a denser dictionary and can estimate the targets with a higher resolution. The off-grid case is more complex and requires more samples. Nevertheless, as the dictionary becomes denser, the correlation between the atoms[3] of the dictionary increases. This can result in a violation of the restricted isometry property, which is a prerequisite for the compressive sensing technique to work. A trade-off between the resolution and the complexity of the system should be found. [39] proposes the use of a dynamic dictionary to solve this issue. [40] proposes a background subtraction method based on recursive computation to use the compressive sensing to extract the sensing parameters. Additionally, a combination of different techniques can be employed to estimate the parameters of the targets.

Once the Delay-Doppler maps have been obtained through one of the estimation techniques presented above, the issue of clutter remains. [23] presents the clutter interference as the interference generated by unwanted scatters. For instance, in the context of automotive applications, clutter could be buildings in a city. This scenario is illustrated in Figure 1.9. The performance of the system can be significantly degraded in the absence of a clutter removal algorithm.

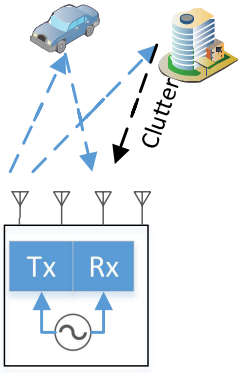


Figure 1.9: Clutter in automotive application[10].

Clutter Removal There are various methods for the removal of clutter. One such method is presented in [41], which involves the design and optimization of a waveform that will pre-suppress the clutter. However, in the context of OFDM and Wi-Fi signals, such pre-suppression is not feasible, as the waveform is im-

[3]In the context of compressive sensing, an atom is an element of the dictionary used.

posed. Two common clutter removal algorithms are the recursive moving averaging (RMA) and the Gaussian mixture model (GMM).

Clutter Removal - RMA[10] The RMA assumes that the sensing parameters remain constant over the coherence time. Another assumption is that the Doppler shift is near zero. Prior to performing the RMA, the initial timing offset should be corrected. In RMA, the averaging matrix is estimated iteratively with the following equation:

$$\bar{\mathbf{D}}(i) = \alpha\bar{\mathbf{D}}(i-1) + (1-\alpha)\hat{\mathbf{D}}(i), \tag{1.29}$$

where $\bar{\mathbf{D}}(i)$ is the outputed channel matrix at the i^{th} iteration, $\hat{\mathbf{D}}(i)$ is the estimated channel matrix at the i^{th} iteration and α is the forgetting factor. The forgetting factor is used to give more importance to the most recent estimation. The average is then removed from the channel matrix, which is then used to estimate the sensing parameters. One can see that in the event of a novel element emerging within the scene, the RMA algorithm will not eliminate it from the channel matrix. Only the static elements (clutters) will be removed. One limitation of this method is the assumption needed on the Doppler shift and a perfect synchronization. This makes the method inefficient in a real scenarios.

Clutter Removal - GMM The GMM, presented in [10] and [38], is a more complex method. The principle is to model the received signal as a summation of multiple Gaussian distributions with different densities representing the different paths of the channel. This allows for the estimation and separation of both static and dynamic paths, represented in different distributions. Indeed, the mean of the static paths is higher than the dynamic ones, and the variance of the static paths is closer to 0. The signal can be estimated by removing the static paths.

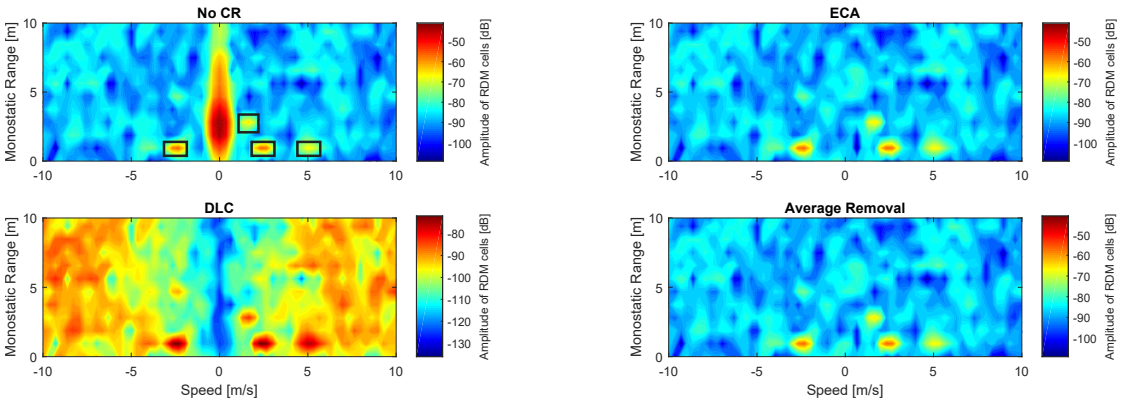


Figure 1.10: Clutter removal methods comparison[42] - "No CR" : no clutter removal, "Average removal" : removal of the Average component, "DLC" : Delay Line Canceller, "ECA" : Extended Cancellation Algorithm.

Clutter Removal - Subtraction of the Mean [42] proposes a method to remove the clutter based on the removal of the average component. It defines the average component as the zero Doppler shift frequency (zero speed of the target). In a dynamic environment, the clutter is defined as all the elements that are not moving. In the absence of a windowing operation, the paper states that the average component can be removed by cancelling the average component after the classical FFT operation of the OFDM[4] If a windowing operation is performed, the DC clutter can be spread on low frequencies bins and hide slow moving targets. In such cases, the removal of the average component will not result in the complete removal of clutters. This paper compares this method with the two others called the Delay Line Canceller (DLC) and the Extended Cancellation Algorithm (ECA). The first can be presented as a high-pass filter applied before windowing. While the second is a method based on subspace and a projection of the received signal on a subspace orthogonal to the clutter one. The paper shows that the average removal method offers performance outcomes comparable to those of the ECA. Figure 1.10 shows the obtained Range-Doppler map. The "No CR" figure represents the case where no clutter removal technique is used and the clutter can be visible on the 0 m/s speed line.

Detection Algorithm Once clutter-free range-Doppler maps have been obtained, a detection algorithm must be designed. One possible approach is to base the detection algorithm on the Neyman-Pearson criterion. The Neyman-Pearson

[4]This method is presented with the periodogram method of parameters estimation.

criterion aims to maximize the probability of detection while keeping the probability of false alarm below a certain threshold. The Neyman-Pearson criterion can be expressed as follows:

$$\frac{P_{\mathrm{d}}}{P_{\mathrm{fa}}} \geq \gamma, \tag{1.30}$$

where P_{d} is the probability of detection, P_{fa} is the probability of false alarm and γ is the threshold.

The detection algorithm used in [42] is the Constant False Alarm Rate (CFAR) algorithm. The manner in which this algorithm functions is by estimating a power level over which the target is considered a target by the receiver. On the one hand, in the event that this power level is set to be insufficient, a considerable number of false alarms would be present. However, all targets would be identified. On the other hand, if the power level is set to be excessive, targets may be overlooked. The algorithm is based on the estimation of the background noise, and the threshold level is chosen to maintain a constant probability of false alarm.

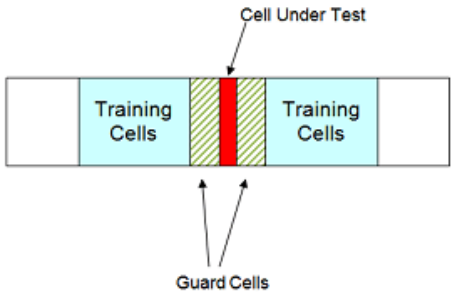


Figure 1.11: CA-CFAR detection algorithm[43].

A variant of this algorithm is called the cell-averaging CFAR (CA-CFAR). In this algorithm, the noise is estimated in a cell around the cell of interest[43]. The threshold is then chosen to keep the probability of false alarm constant. The algorithm is applied over all the cells of the Range-Doppler map to detect the targets. In a single dimension, the CA-CFAR algorithm can be presented as in Figure 1.11. The power around the cell under test is estimated in the training cells as follows:

$$P_n = \frac{1}{N_{\mathrm{train}}} \sum_{m=1}^{N_{\mathrm{train}}} x_m, \tag{1.31}$$

where N_{train} is the number of training cells, x_m is the quantity of interest in the m^{th} training cell. If x_m is chosen to be the power of the cell m in the training cells, P_n is the estimated power in the training cells. The threshold is then determined as follows:

$$\alpha = N\left(P_{fa}^{-1/N} - 1\right), \tag{1.32}$$

where N is the number of training cells, P_{fa} is the probability of false alarm chosen, and α is the threshold. The cell under examination is compared to the threshold. If the cell power is above the threshold, it is considered a target.

CHAPTER 2

Wi-Fi Standard - IEEE 802.11

The Wi-Fi standard is one of the most widely used communication standards around the globe. It is present in a multitude of residential and commercial environment. Over time, the standard has undergone enhancements to increase performance and align with the evolving needs of the community. In response to these needs, a new task group, designated as IEEE 802.11bf, was established within the IEEE 802.11 working group in 2020. The objective of this group is to develop a new amendment to the IEEE 802.11 standard that will support the operation of WLAN sensing. This novel operation would employ the PHY[1] and MAC[2] layers of the standard to estimate features of objects within an area of interest. These features may include range, velocity, angular position, and motion, among others, of humans, animals, and other entities. The area of interest can be of a relatively limited extent (e.g., a home or vehicle) or of a more expansive nature (e.g., an entire enterprise)[6].

In order to implement these sensing capabilities into the systems, the task group has to modify the existing PHY and MAC layers of the existing standard. In the current standard, a distinction is made between the two different license-exempt frequency bands that are used: the frequencies above 45 GHz and the ones between 1 GHz and 7.125 GHz. The high frequency of the first band offers an advantage in terms of sensing capabilities, as it allows for a better resolution. However, this

[1]Layer responsible for modulation of the raw bits over a physical data link[44].

[2]Layer that controls the hardware responsible for interactions with the wired or wireless transmission medium[45].

carrier frequency also presents a disadvantage in that it results in higher path loss and absorption by the environment, which could potentially reduce the reachable range. The second band must be present in all cases for backward compatibility with previous standards. Indeed, older generations of IEEE 802.11 devices only use the low carrier frequency band. The removal of this band would render the new standard incompatible with older devices, making the older devices obsolete with the communication with new Wi-Fi access points (AP). One can note that the majority of the MAC and PHY modifications will be performed on the higher frequency band.

The recently proposed amendment should facilitate the exchange of information regarding the sensing capabilities between stations. Additionally, the amendment should include a request and setup transmission, which would enable WLAN sensing measurements to be made. The final version of the revision is expected to be published in 2025[6].

This chapter presents a brief overview of the existing IEEE 802.11ax (Wi-Fi 6) standard and discusses the anticipated modifications to this standard that will facilitate its evolution into the IEEE 802.11bf standard. Finally, the scenario used in this study is presented.

2.1 IEEE 802.11ax

This section focus on the IEEE 802.11ax standard and its main features. The standard is presented in the first part of the section. The preamble and tailing of the standard are presented in the second part.

2.1.1 Presentation of the Standard

The IEEE 802.11ax is one of the most recent amendments to the IEEE 802.11 standard. It was published in 2019 and is designed to operate in the 2.4 GHz and 5 GHz bands. It is also designed to improve the performance of the existing IEEE 802.11ac (Wi-Fi 5) standard. One of the primary objectives is to enhance performance by a factor of 4 while maintaining power requirements. The emergence of the Internet of Things (IoT) has pushed for the development of the new standard, which is designed to accommodate and manage the multitude of devices connected to the same access point. The Wi-Fi 6 standard uses the 2.4 GHz and 5 GHz bands. The 60 GHz band is not included in the standard, as referenced in [7]. The primary features and enhancements of the standard are the following:

1. Downlink and uplink OFDMA
2. Downlink and uplink MU-MIMO
3. Higher order modulation (1024-QAM)
4. Advanced OFDM and coding
5. Outdoor operation
6. Reduced power consumption
7. Spatial re-use
8. Transmit beamforming
9. Single-user operation

More quantitative changes between the physical layer of the Wi-Fi 5 and Wi-Fi 6 standards can be found in the Table 2.1[7]. It can be seen that the modifications, while initially introduced to enhance communication capabilities, have the potential to be used in sensing applications. In fact, the longer cyclic prefix allows for a better long-range sensing, while the longer OFDM symbol and high bandwidth[3] allow for a better range resolution.

Parameter	**802.11ac Value**	**802.11ax Value**
Bands	5 GHz	2.4 GHz and 5 GHz
Channel width	20, 40, 80, 80+80 160 MHz	20, 40, 80, 80+80, 160 MHz
FFT sizes	64, 128, 256, 512	256, 512, 1024, 2048
Subcarrier spacing	312.5 kHz	78.125 kHz
OFDM symbols	3.2 μs	12.8 μs
OFDM symbol cyclic prefix	0.4 or 0.8 μs	0.8 or 1.6 or 3.2 μs
Highest modulation	256-QAM	1024-QAM

Table 2.1: IEEE 802.11ax parameters.

Figure 2.1 represents the 5 GHz band allocation in Wi-Fi 5. This is the same as the one used in the 6^{th} generation. Each user can have access from 1 up to 8 channels, with each channel having a bandwidth of 20 MHz. By aggregating the channels, the user can have access to a maximum of 160 MHz of bandwidth. The 2.4 GHz band allocation is not presented here, but it is similar to the 5 GHz band allocation. A band edge of 20 MHz is also present on each side of the whole band to avoid interference with other systems.

[3]The bandwidth is still the same as in the IEEE 802.11ac standard, but its high value is noticeable.

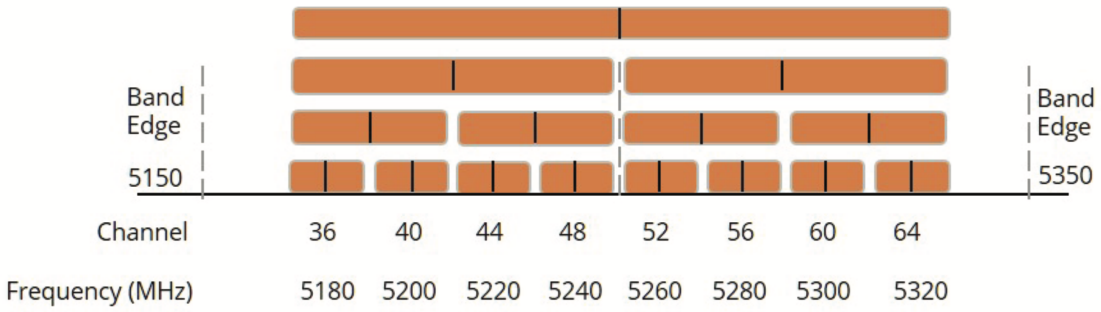


Figure 2.1: IEEE 802.11ac band allocation[7].

2.1.2 Preamble and Tailing

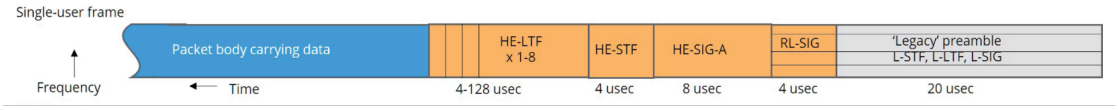


Figure 2.2: IEEE 802.11ax preamble[7].

A crucial aspect of each communication standard is the preamble of the signal. Primarily, the preamble is a known signal that is transmitted before the data. Its primary function is to synchronize the receiver and the transmitter. Additionally, it can carry essential information about the communication, such as the length of the data sequence that is sent or received, the modulation used, and so forth. Furthermore, the preamble is employed to correct the channel and perform an equalization operation, as well as to address other crucial aspects of the communication. In this standard, the addition of the preamble is performed by the physical layer of the transmitter. Figure 2.2 depicts the frame used in the IEEE 802.11ax. This frame is used in the single-user case, as it is presented in this work. A variant of this frame exists for the multi-user case, but will not be presented here. The frame is composed of three distinct sections: the legacy preamble, the high efficiency (HE) preamble, and the packet body (payload).

Legacy Preamble

The legacy preamble is employed primarily to ensure compatibility with the previous standards. It is transmitted over all the 20 MHz channels used by the user, thereby informing previous standard devices or devices utilizing such bands that a transmission is in progress on the 20 MHz channel. It is composed of a short

training field (STF), a long training field (LTF), and a signal field (SIG).

The newly established standard will not necessarily uses this legacy part. However, as previously stated, the function of the legacy part is to ensure that the receiver is aware of the ongoing transmission on the 20 MHz channel. In older systems, the roles and durations of each field are as follows[46]:

- **Short Training Field - STF -** 8 μs: This field is the succession of short training sequences. Due to its high correlation property, it is employed for packet detection. Additionally, it is used for coarse frequency offset estimation.
- **Long Training Field - LTF -** 8 μs: This field is the succession 2 long training sequences. Its function is to correct the channel, more finely estimate the CFO and the timing offset.
- **Signal Field - SIG -** 4 μs: This field contains 24 bits of information, as follows: 4 bits of rate, 12 bits of length, 1 bit of parity, 6 bits of tail bits, and a bit of reserve. It is used to indicate the different parameters of the packet.

High Efficiency Preamble

In addition to the legacy preamble, new preambles have been added as the standard has evolved. For instance, in the IEEE 802.11ac standard, a preamble called the "very high throughput" preamble has been introduced. In the IEEE 802.11ax standard, its name is "high efficiency" preamble. These new preambles are used to improve the performance of the communication. The composition of this preamble is as follows: a repetition of the legacy signal field (RL-SIG), a high efficiency signal field (HE-SIG-A), a high efficiency short training field (HE-STF), and a high efficiency long training field (HE-LTF). The preamble can be extended with the repetition of a HE-SIG-A. Indeed, as this information is of the most importance, it can be repeated twice to ensure that the receiver will receive it correctly in the event of high fading, interference, or in outdoor scenarios.

The role and duration of the different parts of the high efficiency preamble are the following [46][7][47][48]:

- **Repeated Legacy Signal Field - RL-SIG -** 4 μs: This field is used to indicate the presence of the high efficiency preamble, thereby signifying an IEEE 802.11ax transmission instead of an older IEEE 802.11 transmission.
- **High Efficiency Signal Field - HE-SIG-A -** 8 μs: This field contains information about the packet, including the bandwidth, the type of communication (Uplink/Downlink), cyclic redoundancy check, and other relevant data. This allows the receiver to identify the type of transmission and the

necessary parameters for packet demodulation.

- **High Efficiency Short Training Field - HE-STF -** 4 μs: This field is used for timing and frequency synchronization.
- **High Efficiency Long Training Field - HE-LTF -** 4 μs-128 μs: This field is used for channel estimation and synchronization. The length of the field may vary from 4 μs to 128 μs depending on the number of spatial streams.

The preamble of an IEEE 802.11ax waveform can be obtained thanks to MATLAB WLAN Toolbox. The simulated waveform is presented in Figure 2.3 with the different parts colored differently.

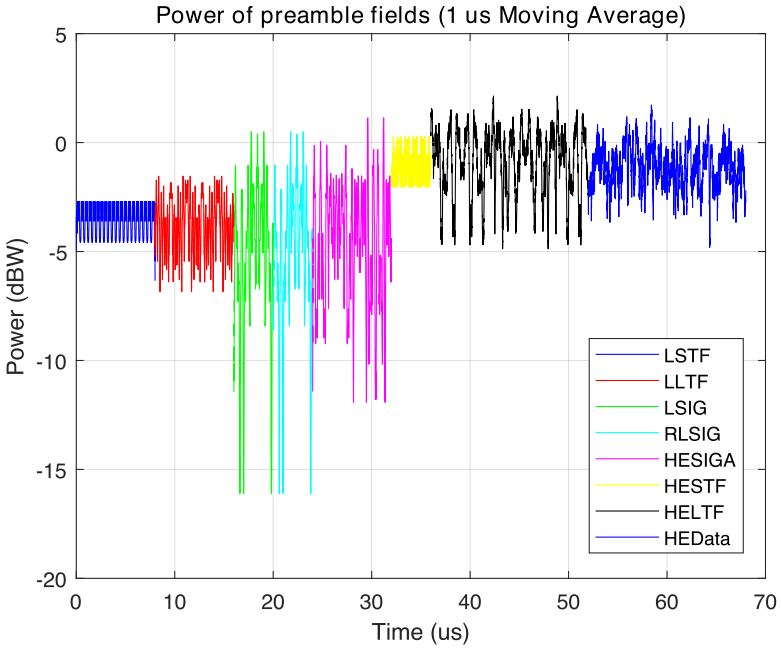


Figure 2.3: IEEE 802.11ax frame structure.

Tailing

Prior to the transmission of the actual packet, a communication between the emitter and receiver is performed to know its size. In the event that the packet is smaller than the negotiated size, a tail can be appended to the packet. The tail may be composed of three parts. The first one is the padding, which is employed to fill the negotiated space in the event that the produced frame is not sufficiently long. The second is the tail bits, which can be incorporated after this for the purpose of correcting code. This procedure is employed exclusively in cases where

binary convolutional codes are used. However, in the majority of instances, a low-density parity check is employed, as it is faster to perform, and thus the tail bit is absent. Finally, a packet extension may be incorporated. This will give the receiver additional time to process the packet. This extension is added at the demand of the receiver.

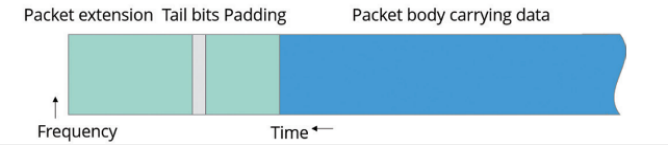


Figure 2.4: IEEE 802.11ax tailing[7].

2.2 IEEE 802.11bf

As explain in the introduction of the section, the IEEE 802.11bf standard is still in development. The IEEE 802.11ax standard will thus be used as a starting point of this work. This section will examine the principal enhancements that are anticipated to be incorporated into the IEEE 802.11bf amendment and the potential technologies that may be employed to enhance sensing capabilities.

2.2.1 PHY Layer

The new standard is set to operate in 2 different bands, the sub-7 GHz band and the 60 GHz bands.

The physical layer of the sub-7 GHz band should remain consistent with the IEEE 802.11ax standard. Consequently, the preamble and tailing presented in section 2.1.2 should be used or be similar in the new standard. As it is not optimized for sensing, the development of new algorithms is necessary to implement this feature. Moreover, as this carrier frequency is lower than the other, the performance will be limited to a coarser sensing capability.

On the other hand, the higher frequency band will be upgraded and certain portions of it should be optimized for sensing. This band should be used for more precise sensing as it has better characteristics. As the carrier frequency of the second band exceeds 6 GHz, the USRPs used in this master thesis will not be able to use such a band. Only the sub-7 GHz band will be employed.

2.2.2 Sensing Configurations

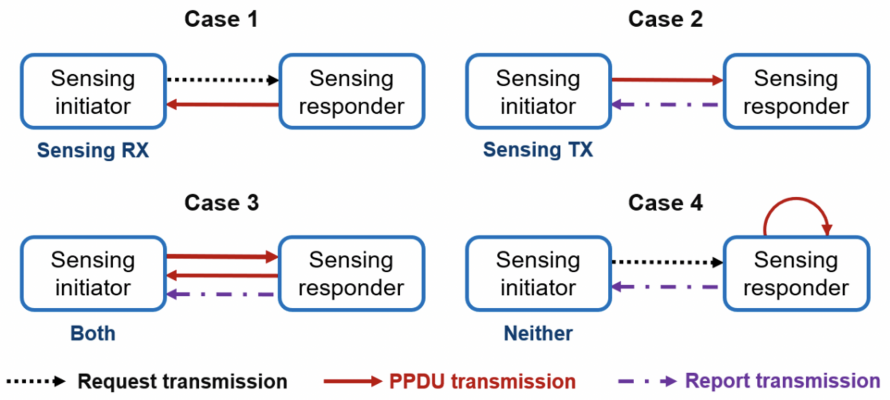


Figure 2.5: IEEE 802.11bf configurations[49].

The new amendment should propose 4 distinct configurations for the sensing procedure. Those configurations are represented in Figure 2.5. Firstly, the procedure could be initiated by either a transmitter (TX) or a receiver (RX). The entity initiating the procedure will be referred to as the "Sensing initiator," while the entity performing the sensing will be designated as the "Sensing responder." The 4 cases are as follows[49]:

- **Case 1 - RX Initiator**: RX sends a request, and is thus be called the initiator, of transmission to the TX. This request contains the sensing parameters that the initiator wants, and it tells the responder to emit a packet. The sensing responder then emits a signal called PPDU (Physical layer protocol data unit). This signal is then used by the initiator to perform the sensing.
- **Case 2 - TX Initiator**: The TX initiates the transmission of a PPDU, which is received by the responder. The responder then performs the sensing operation, which enables it to estimate the channel state information (CSI) and subsequently transmit this information back to the initiator via a report transmission.
- **Case 3 - RX and TX Initiators**: The initiator may be either RX or TX. The sensing process begins with the emission of a PPDU by the initiator. This signal enables the responder to estimate the CSI and send it back to the initiator during the report transmission. In response, the responder emits a PPDU. The initiator then has access to both the estimation of the CSI performed by the responder and its own estimation, which it can obtain from the PPDU emitted by the responder. Consequently, the initiator is able to obtain both uplink and downlink CSI estimations.

- **Case 4 - Neither**: In this case, the initiator requests that the responder perform a sensing measurement. The responder then transmits a PPDU, which it uses to estimate the CSI. The responder then transmits the CSI to the initiator within a report transmission.

2.2.3 Sensing Procedure

In the context of the different scenarios, the exchange of information between the initiator and the responder is crucial. The procedure containing this exchange can be summarized by Figure 2.6. It is divided into two different parts. The first one is for the Sub-7 GHz band and the second one is for the 60 GHz band. In both parts, the sensing procedure can be expressed in four steps.

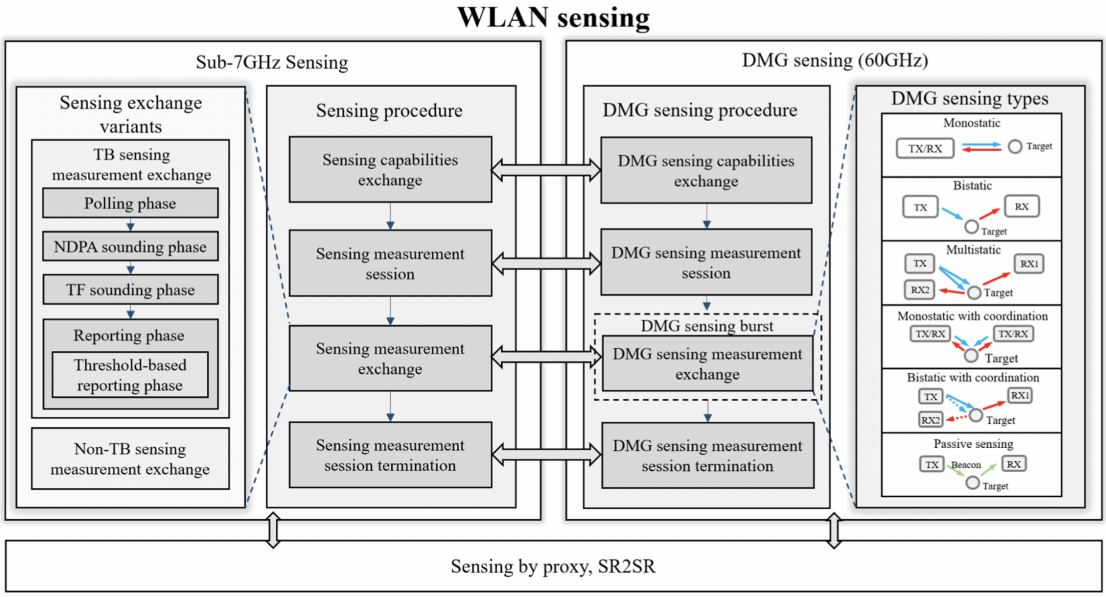


Figure 2.6: IEEE 802.11bf sensing procedure[49].

The initial stage of the process involves the initiator and the responder exchanging their respective sensing capabilities.

Following this, both devices begin a sensing measurement session. During this phase, both parties exchange and agree upon the operational attributes of the sensing. These attributes may include the type of measurement report to be fed back, the number of measurements, the time between measurements, and so forth.

The third step is the sensing measurement exchange. This part can be of multiple natures. Firstly it can be trigger-based (TB). In this case, the initiator will send a trigger frame to responders[4]. This can be seen as the pooling phase. This allows the initiator to identify the responders that will participate in the measurement exchange. The null data packet announcement (NDPA) sounding is the downlink sounding. This announcement informs the responder that the initiator will emit a null data packet (NDP). The initiator then emits a NDP, and the responder makes the CSI estimation of the downlink channel based on this packet. The trigger frame (TF) sounding is for the uplink sounding. In this case, the responder transmits a trigger frame to the initiator, whom then performs the CSI estimation for the uplink channel. The final step is the transmission of the report, which enables the initiator to access both CSI estimations.

Another variant of this procedure is a non-trigger-based (NTB) procedure. In this case, the initiator first emits a NDPA frame containing the information about the measurement. This is followed by the emission of a NDP frame for downlink sounding, after which the responder makes the CSI estimation, sends a NDP frame and a report of the estimate. The initiator can then make the CSI estimation and has access to both the CSI estimation and the report.

The main difference between the trigger-based and non-trigger-based procedure lies in the presence of the trigger frame. In a trigger-based procedure, the initiator will initially transmit a trigger frame to the responder, thereby notifying it of the measurement that will take place and establishing a pool of responders.
The number of sensing measurements that may be exchanged is determined in the second step of the process. Once the number of measurements has been reached, the sensing measurement session is terminated.

The above procedure is for the sub-7 GHz band. The 60 GHz band is alike, yet the sensing measurement exchange is different but will not be described here as it is not employed in this work.

A final potential sensing procedure is the sensing by proxy. In this case, the device requests that a responder, which is likely an access point, perform a sensing measurement. The access point then performs the sensing measurement and transmits the report to the device.

[4]Multiple responders can be present for the measurements. In Figure 2.5, only a simple scenario with 1 initiator and 1 responder are shown.

2.3 Scenario

The scenario presented in this master thesis is similar to the fourth sensing configuration depicted in Figure 2.5. The system can be divided into two distinct parts.

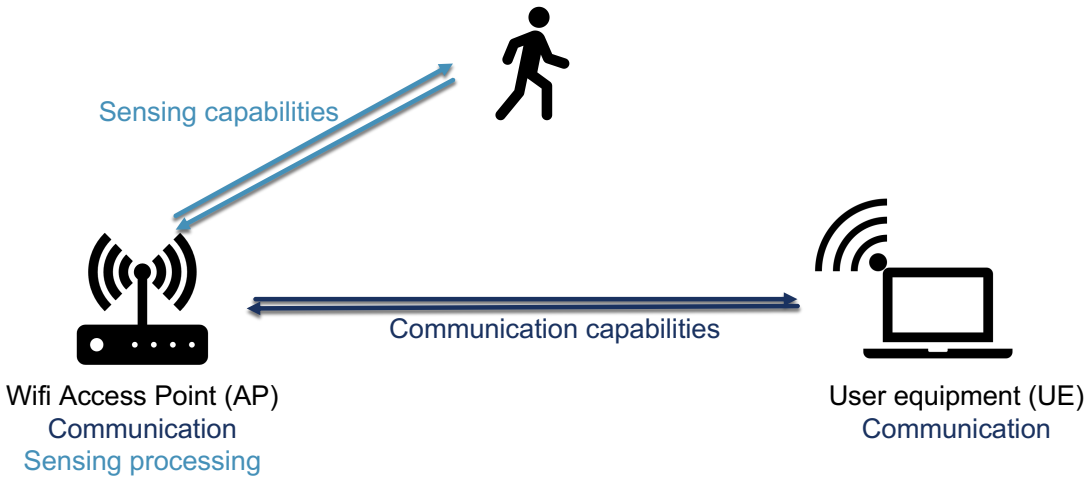


Figure 2.7: Scenario used in this work.

The first part is responsible for the communication, while the second part is responsible for the sensing. The Wi-Fi access point serves both of these applications, as it is the device acting as the transmitter in the system. For the communication part, the AP communicates with a receiver presented as the user equipment (UE) in Figure 2.7. The UE lacks access to the pre-emission signal and must rely on pilots and preamble to detect the signal, equalize it, and retrieve to the useful data.

In the context of the sensing component of the system, the receiver is the AP itself. The emitted signal will thus be sent by the AP, modified by the environment, and then received back by the AP. As the AP has access to the pre-emission signal, it can perform the sensing measurement with the entire signal rather than only a part of it. This measurement provides information about the range, speed, and angular position of the objects of interest in the area around the AP. The angular position can be estimated only if multiple antennas are present on the receiver side.

It can be reasonably assumed that the sensing process will not interfere with the communication aspect of the system. Indeed, this process uses the same signal as the communication process in order to perform the CSI estimation. However, it should be noted that this signal is not optimized for sensing purposes. An

illustrative example of the proposed scenario in a real-world context would be:

1. The UE requests information from the AP. This information may take the form of a web page, a video, or any other digital content.
2. The AP transmits the desired information to the UE in a Wi-Fi 6 frame structure. The AP also retains a local copy of the transmitted frame.
3. A distinction between the communication and sensing is made in the two subpoints that follow:
   3.1. **Communication -** The UE then receives the frame and performs the decoding process.
   3.2. **Sensing -** At the same time, the electromagnetic wave emitted by the AP is affected by the environment and a part of it is reflected back to the AP. The AP then receives the signal. Thanks to the copy of the transmitted frame, the AP can perform the CSI estimation with the whole received signal. It can then estimate the range, speed and angular position of the objects in the environment. The AP can also estimate the parameters of the UE. It is noteworthy that if the AP did not have access to the pretransmission signal, the CSI estimation would be performed only on the preamble or known sequences of the frame.
4. If needed, the AP can send the information about the environment to the UE, other devices, or store it for future use such as power optimization, etc.

Nevertheless, this scenario is based on the assumption that the UE requests information from the AP frequently and that the transmitted packets are quite long in order to have a good CSI estimation.

2.4 Summary of the Wi-Fi Standard - IEEE 802.11

In conclusion, this chapter presents the Wi-Fi standard. It discusses several generations of the standard, with a focus on the 6^{th} generation. It also presents the preamble and tailing of the standard, as well as the possible improvements that could be present in the IEEE 802.11bf standard. Additionally, it presents the different sensing configurations and the sensing procedure. Finally, the scenario that will be used in this master thesis has been presented. Throughout this work, it is this scenario that will be employed, and we will try to adhere as closely as possible to it.

CHAPTER 3

Experiment Setup

This chapter presents the experimental setup employed at UCLouvain. It begins by presenting the different components of the setup, followed by a discussion on the limitations induced by the setup. After this discussion, the improvements made to enhance the performance of the setup are presented. To illustrate the evolution of performance, a comparison between the first and second generation setup is presented, using a benchmark. The chapter then presents and explains the generated waveforms and the packet extraction processing used for both the communication and the sensing.

3.1 USRP - 2944R

The primary component of the configuration used at UCLouvain is the NI USRP 2944R[50], provided by National Instrument and depicted in Figure 3.1. This Software Defined Radio(SDR) enables the rapid prototyping of wireless systems. The large bandwidth and carrier frequency range of these SDRs, which extends respectively up to 160 MHz and from 10 MHz to 6 GHz, provides sufficient resources for sensing capabilities. Additionally, a discrete non-linear range of values is available for both the carrier frequency and the sample rate. The maximum sample rate is 200 MSamples/s. Figure 3.2 represents the block diagram of the used USRP. To interface and program them, NI provides LabVIEW, a graphical programming environment. This software has not been used because of the poor usability. An alternative method for interfacing the USRP is the open-source software GNURadio. However, due to the significant learning curve associated with this software,



Figure 3.1: USRP 2944R.

it was not selected. The optimal solution found is to use the UHD API provided by Ettus Research. This API allows for the interfacing of the USRP with the computer, which can be achieved via a C++ or a Python code. A preliminary version of this work has been coded in Python, while another one has been developed in C++ with the objective of enhancing the performance. This C++ version of the interfacing has been provided by the Université Libre de Bruxelles (ULB). This API is used to configure the USRP. (i.e., set the carrier frequency, the sample rate, etc.), send and receive the data, as well as flashing the embedded FPGA. After being generated by the computer, the samples are sent to the devices via a PCIe port with a limited rate of 1 Gb/s or via a 10 Gigabit Ethernet (10 GbE) port.

The upper portion of the circuit, as depicted in Figure 3.2, illustrates the transmitting hardware integrated within the USRP. After its generation, the IQ samples are separated and transmitted to digital upconverters (DUC) for the purpose of interpolating the signal to a rate of 200 MS/s. Subsequently, the digital signal is converted to an analog signal by a digital-to-analog converter (DAC) with 16 bits before being filtered by a low-pass filter with a cutoff frequency of 80 MHz. The obtained signal is then modulated with the desired carrier frequency. As the used carrier frequencies fall within the range of the Wi-Fi 2.4 GHz band, the signal is transmitted via the direct path (see Figure 3.2). One advantage of this direct path is that the signal is transmitted through fewer components, thereby reducing the likelihood of signal deterioration. Finally, the signal is amplified prior to being transmitted to the antenna.

The receiving part is shown at the bottom of the circuit. The receiving hardware, located within the USRP, is responsible for the reception of the signal. Initially, this signal is amplified by a low noise amplifier (LNA) and a drive amplifier. The

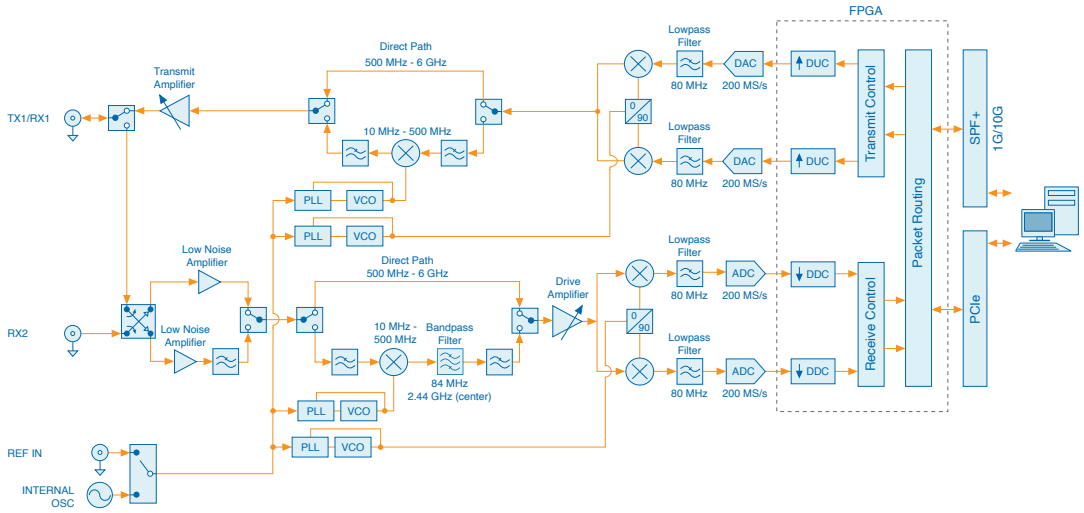


Figure 3.2: USRP 2944R - Block diagram[51].

direct path is also used at the receiver, for the same reason as the transmitter. The signal is then demixed and filtered by a low pass filter with a cut-off frequency of 80 MHz. Subsequently, the analog signal is converted to a digital format by the analog-to-digital converter (ADC) with a 14 bits resolution. A digital downconverter (DDC) is employed to reduce the signal to the desired sample rate. The resulting digital signal is then transmitted to the computer via the port (PCIe/10 GbE).

The TX1/RX1 antenna of the USRP can be used for both transmission and reception. This is achieved by the use of a duplexer, which serves to separate the transmitted and received signals. However, the use of a duplexer results in a reduction of the usable sample rate by a factor of two.

Finally, the reference frequency of the USRP can be either internal or external. In the developed setup, this is accomplished by using the OctoClock CDA-2990[52] component from Ettus Research. This component will be discussed in greater detail in the subsequent section. Additionally, a GPS antenna can be incorporated into the USRP to facilitate wireless precise synchronization.

The USRP contains two circuits, which allows for a total of four channels. Two of these channels are dedicated to reception, while the remaining two can be used for transmission, reception, or both.

3.2 OctoClock - CDA-2990



Figure 3.3: OctoClock CDA-2990[52].

For the purpose of time and frequency synchronization between the various USRPs, the OctoClock CDA-2990 from National Instrument is employed. This device offers the capability to synchronize up to eight USRP units in both time and frequency. Time synchronization is achieved through the emission of a pulse per second (PPS) signal, while frequency synchronization is accomplished through the emission of a 10 MHz signal. Both generated signals are transmitted to the USRP devices through a coaxial link. This signal is used by the USRP devices as a reference clock, replacing the internal clock. Furthermore, the OctoClock can be employed to synchronize multiple USRP units with GPS signals, provided that a GPS antenna is incorporated[52].

3.3 Switch - CPS-8910



Figure 3.4: Switch CPS-8910[53].

In order to connect multiple USRPs to a computer via a PCIe port, the CPS-8910 Switch[53] from National Instruments is employed. This device is used to

route the samples to and from the USRPs. The switch is capable of linking up to eight devices to itself via eight PCIe x4 ports of first generation. It can then be connected to the computer via a PCIe x4 port or a PCIe x8 port of second generation. The bit rate available with a PCIe x4 port is up to 1 Gb/s and is 4 Gb/s with a PCIe x8 port[54]. These bit rates may present a limitation when a high sample rate is used.

3.4 First Generation Setup

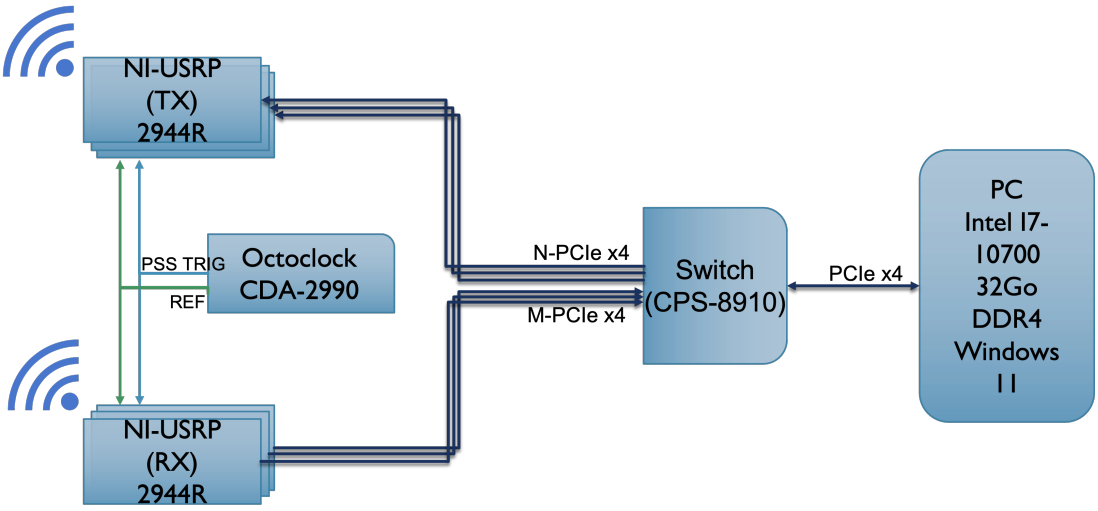


Figure 3.5: First generation setup.

The first generation setup is shown in Figure 3.5. In this configuratin, the computer is equipped with a 10^{th} generation Intel Core i7-10700 processor and 32GB of DDR4 RAM. The operating system used was Windows 11. Only a single PCIe x4 port of first generation was used for data transfer between the computer and the switch. The same link is used for both the transmission and reception of the data. Each USRP is connected to the switch through a PCIe x4 port. The different USRPs are connected to the same OctoClock to ensure precise time and frequency synchronization. In the initial configuration, the computer and the USRP communicate via the Python API. The computer generates the transmitted data, which is then sent to the USRP via the switch. The USRP receive the data and send it to the computer via the switch, where it is stored on the solid state drive (SSD) of the computer in real-time.

The limitations of this configuration result in a significant number of overflow and underflow errors at different sampling rates. These limitations can be attributed to a number of factors, including:

- **PCIe Gen 1 x4 port** - As previously stated, the maximum bit rate available in downstream is up to 1 Gb/s with this type of connection. If the sampling rate is too high or the number of channels is too important, the data cannot be sent or received effectively. This can result in overflows or underflows.
- **Windows 11** - The Windows 11 operating system incorporates a data protection system, designated as Windows Defender, which analyses the data transmitted and received by the computer. This protection system may result in the occurrence of overflows and underflows as the communication between the computer and the USRP is being slowed down.
- **Python API** - The Python API is not the most efficient way to communicate with the USRPs. Indeed there is the possibility to use the UHD API in C++, which is a compiled language and more therefore efficient.
- **SSD** - Once the data has been received, it is transmitted to the CPU and subsequently stored on the SSD. This method of data storage is not the most optimal. Instead, the data can be saved directly on the RAM and, after the acquisition of the entire signal, transmitted to the SSD. This approach avoids the bottleneck of the SSD writing speed and the utilization of the CPU to save data during the measurement.
- **Switch** - The use of the switch forces the data to traverse a unique port in order to be transmitted from and to the computer. The use of a different PCIe extension card on the computer could facilitate the establishment of multiple direct links to the computer, thus avoid the bottleneck associated with a single connection.

3.5 Second Generation Setup

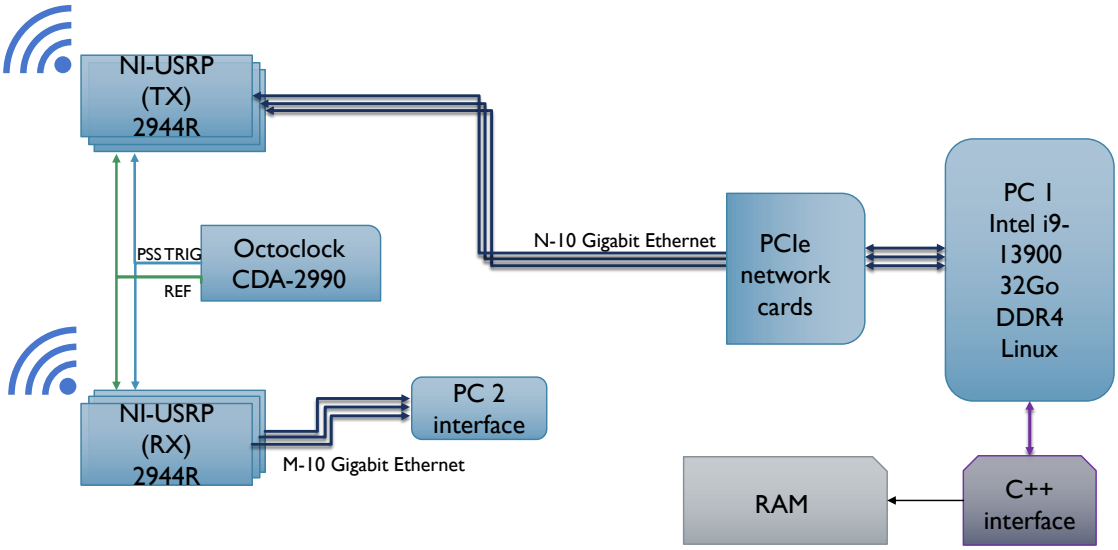


Figure 3.6: Second generation setup.

The second generation setup is presented in Figure 3.6. In order to avoid the different bottlenecks of the first generation setup, the setup is modified as follows:

- **10 GbE port** - The PCIe Gen 1 x4 port is replaced by a 10 GbE port. This port has a bit rate of 10 Gb/s, which is 10 times higher than the PCIe Gen 1 x4 port. This allows for the transmission and reception of data at a faster rate.
- **Multiple 10 GbE ports** - The communication between the USRPs and the computer is facilitated by the use of multiple 10 GbE ports. This approach avoids the potential bottleneck associated with a single connection to interface all the USRPs. Furthermore, the data can be transmitted and received directly to the computer without traversing the switch.
- **Linux** - The operating system is replaced by Linux. This operating system is more efficient than Windows 11 and does not have a non-removable protection system that can slow down the interfacing process.
- **C++ API** - The Python API is replaced by the UHD API in C++. This language is more efficient than Python.
- **RAM** - The data is stored on the RAM during the acquisition of the signal and then transmitted to the SSD after the acquisition. This approach avoids the bottleneck associated with the SSD writing speed and the utilization of the CPU to save data during the measurement.

- **RX and TX on different computers** - In contrast to the previous approach, which involved a single computer for both transmission and reception of data, a dual-computer configuration is employed. One computer is dedicated to data transmission (PC 1), while the other is responsible for data reception (PC 2). This is represented by the two interfaces for the USRP presented in Figure 3.6. This approach has the advantage of reducing the overall load on each computers. The CPU of the computers are also more powerful than the one used in the first generation setup. Indeed, the intel i7-10700 CPU is upgraded to an intel i9-13900 one for both computers.

The modifications have resulted in a reduction in the number of overflows and underflows. The performance of the setup has been enhanced, and experiments can now be performed with a higher sampling rate and a higher number of channels. These modifications have been discussed and obtained thanks to this exchange with members of the ULB team. This team is also working on the IEEE 802.11bf standard and has a similar setup which is presented and utilized in [55].

3.6 Benchmarking

To assess the performance of the system, a benchmarking exercise is conducted. A stress test is performed by running the system with different parameters and evaluating its performance. For these tests, a range of sampling rates are employed, starting from the highest (200 MS/s) and gradually decreasing until acceptable performance is achieved. For the transmitter, a number of samples are transmitted to the USRP to evaluate the quality of the uplink communication[1]. For the receiver, a number of samples are received to evaluate the quality of the downlink communication[2]. The number of samples lost due to overflow or underflow is monitored. The test was conducted over a 10 s period, with an average calculated over 5 measurements.

Figure 3.7 illustrates the improvement achieved through the second generation setup. The results demonstrate that for the second generation setup, the sampling rate can be as high as 200 MS/s without experiencing underflows, overflows, or dropped samples during a stress test. In contrast, the first generation setup is unable to handle a sampling rate higher than 20 MS/s to achieve such results[3]. The number of errors decrease as the sampling rate is reduced for the first generation setup.

[1] The uplink communication is the communication from the computer to the USRP.

[2] The downlink communication is the communication from the USRP to the computer.

[3] A value of 1 is placed on the graph for the second generation setup at 200 MS/s and for the first generation setup at 20 MS/s to indicate that no errors were observed.

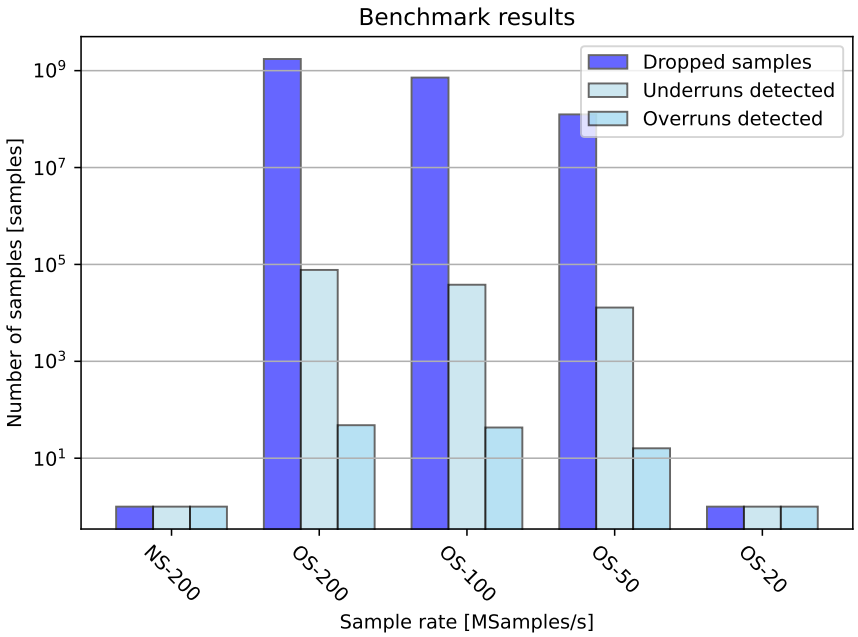


Figure 3.7: Benchmarking - First generation setup (OS) vs Second generation setup (NS).

3.7 Time Domain Representation of the Waveforms

This section presents the different waveforms emitted and received by the USRP in the experimental setup. Firstly, the waveforms are generated by the computers in Python. After this generation, the waveforms are sent to the USRP via the C++ interface. The waveforms are then transmitted by the USRP and received by the other USRP. It is those waveforms that are representation in the time domain in this section. The received waveforms are then sent back to the computer for processing.

3.7.1 Communication

The communication waveforms in the time domain are presented in this subsection. In the final setup, it is this waveform that is used to transmit data from one USRP to the other and also to perform the sensing.

Transmitted Signal

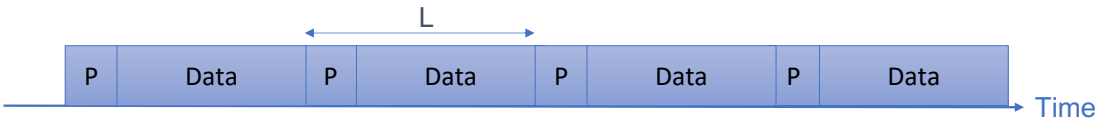


Figure 3.8: Transmitted signal in time domain. "P" represents the IEEE 802.11ax preamble and "Data" the pilots and the data part.

The transmitted signal in the time domain is presented in Figure 3.8. The signal is composed of a preamble and a data part. The preamble is the one present in the IEEE 802.11ax waveform and is introduced in Section 2.1. The data part is composed of multiple OFDM pulses. Some of those pulses are pilots used for the channel estimation and equalization. The combination of a preamble and a data part has a length of L and is transmitted continuously by the emitter.

Received Signal



Figure 3.9: Received signal in time domain. "P" represents the IEEE 802.11ax preamble and "Data" the pilots and the data part.

To assess the performance of the system, the continuously transmitted signal is measured at the receiver for a specified duration. In order to ensure that a complete packet is received, the measurement time is set to $2L$, where L is the length of the packet. The length of a packet is defined as the length of the data, which can be composed of actual data and pilots, added to the length of the preamble. Indeed, by doing so, the receiver is guaranteed to receive a complete packet. At the receiver, the beginning of the packet can be identified by using the preamble and performing a correlation as described in Section 4. The correlation is conducted on a portion of the measured sequence with the known preamble. The portion of the sequence used is of duration $L + P$, where P is the length of the preamble. On the retrieved packet, the receiver can estimate the performance of the system,

including the bit error rate (BER). Figure 3.9 presents a representation of the received signal, with the grayed-out zones being not measured.

3.7.2 Sensing

In the sensing portion of the experiment, the receiver has access to the entirety of the packet and is able to use it to accurately determine the start of the packet and precisely measure it. In the experimental section presented in Chapter 6, two methods are employed to conduct the sensing experiments.

Sensing - Method 1

The initial method is identical to the transmission and reception process presented in the communication section. The only differentiating factor between this method and the preceding one is that the entire packet is employed in a correlation to identify the start of the packet. After the extraction of the packet, the receiver can perform the Range-Doppler processing to estimate the parameters of the target.

Sensing - Method 2



Figure 3.10: Sensing - method 2: Transmitted signal in time domain."Data" represents the pilots and the data part.



Figure 3.11: Sensing - method 2: Received signal in time domain. "Data" represents the pilots and the data part.

The second method is to not use a preamble for the transmission. In this case, the signal can be represented by Figure 3.10. In this case, only the sensing is performed as no preamble is added to the transmission. Nonetheless, random data is still added to form the data part as well as pilots. A single packet of length L is used to estimate the start of a sequence of interest, and multiple

packets are recorded. By emulating a longer packet, the receiver gains access to a greater number of OFDM pulses, allowing for increased speed resolution. The measured signal without identifying the start of a sequence is depicted in Figure 3.11. The primary advantage of this system is that it consumes fewer resources for the computer at the transmitter, as the emitted packet can be smaller. This is advantageous because it reduces the likelihood of underflows, as observed in the host computer for the transmission. Indeed, the transmission of lengthy packets revealed the occurrence of underflows in an non fully optimized system[4].

3.8 Summary of the Experimental Setup

The objectives of this chapter can be summarized as follows:

- The presentation of the different components of the UCLouvain setup, including the USRP 2944R, the OctoClock CDA-2990, and the Switch CPS-8910.
- The limitations of the different components.
- The improvements made to enhance the performance of the setup.
- The assessment of the performance of the setup through benchmarking.
- The presentation of the transmitted and received waveforms for the communication and sensing.

The presented setup is capable of handling a sampling rate of 200 MS/s without experiencing underflows, overflows, or dropped samples during a stress test. The setup can be used for the purpose of conducting experiments of sensing and communication.

[4]The second method is no longer necessary in the final setup.

CHAPTER 4

Synchronization

This chapter addresses the question of synchronization in communication systems. First, different techniques for time synchronization are presented, along with the performance achieved with such algorithms. The time synchronization is a crucial aspect of communication systems, as it ensures that the start of a sequence is accurately detected. Second, the carrier frequency offset estimation problem is discussed. This problem arises due to the presence of different clocks in the transmitter and receiver, or due to environmental movement and device-related factors. The time and frequency offset estimation is presented through the use of various algorithms, and the performance of these algorithms is presented. The objective of this chapter is to identify the most effective algorithm for both time and frequency synchronization.

4.1 Time Synchronization

The objective of time synchronization is for the receiver to correctly detect the different part of the packet (preamble, data, pilots, guard intervals, and so forth). This thesis presents two techniques for time synchronization: the correlation and the Schmidl & Cox method. These techniques use a sequence in the preamble, which is respectively known or not. To assess the performance of the methods, the known sequence is the legacy long training field (L-LTF) of the IEEE 802.11ax standard. As this sequence is simpler and shorter than the HE-LTF, the error of synchronization should be higher than with this sequence, thus allowing for a more accurate assessment of the techniques. After selecting the best performing

techniques, the used sequence will be changed to the HE-LTF in the final setup.

4.1.1 Correlation

The correlation method is based on the cross-correlation between the received signal and the known sequence. The correlation is given by the following equation:

$$R[n] = \sum_{m=0}^{M-1} x[m]y^*[m+n], \tag{4.1}$$

where the received signal is x, the known sequence is y, and M is the length of the known sequence. The correlation is performed between the received signal and the known sequence. This correlation can be performed in the time or frequency domain. Indeed, a convolution in the time domain is equivalent to a multiplication in the frequency domain and efficient algorithm such as the FFT/IFFT exists to go from one domain to the other. Doing the operations in the frequency domain could thus reduce the complexity of the correlation operation. The correlation result using the property previously mentioned is given by the following equation:

$$R[n] = \text{IFFT}\{X[k]Y^*[k]\}, \tag{4.2}$$

where X is the DFT of the received signal, and Y is the DFT of the known sequence. They are used to calculate the maximum value of the correlation. The index of the maximum value of R represents the shift between the received signal and the known sequence. Consequently, the start of the sequence can be estimated as

$$n_{\text{start}} = \underset{n}{\text{argmax}}\ R[n]. \tag{4.3}$$

4.1.2 Schmidl & Cox Method

The Schmidl & Cox algorithm, as described in [28], is the second timing synchronization technique that is tested in this thesis. It is based on the use of a sequence composed of two repeating parts. If the system is not continuously performing the synchronization operation, a problem would appear for the use of such algorithm. A solution would be to use a power threshold-based algorithm to detect when the receiver should start the detection of the incoming signal. The Schmidl & Cox algorithm is based on the autocorrelation of the received signal. The autocorrelation metric $P[d]$ is employed by the algorithm and calculated as

$$P[d] = \sum_{m=0}^{L-1} r[d+m]r^*[d+m+L]. \tag{4.4}$$

In (4.4), r represents the received signal, while L denotes the length of half the sequence. The received energy is calculated as

$$R[d] = \sum_{m=0}^{L-1} |r[d+m+L]|^2. \tag{4.5}$$

In the Schmidl & Cox algorithm, the metric employed to identify the midpoint of the sequence is

$$M_{or}[d] = \frac{|P[d]|^2}{R[d]^2}. \tag{4.6}$$

The maximum value of this metric is computed, and its corresponding position is used to identify the middle of the sequence. The problem can be defined as

$$d_M = \underset{d}{\operatorname{argmax}}\ M[d]. \tag{4.7}$$

A modified version of the Schmidl & Cox algorithm is presented in [56] and the new metric is calculated as follows:

$$M[d] = \frac{|P[d]|^2}{R[d]R[d+L]}. \tag{4.8}$$

The modification forces the maximum value of the metric to be equal to 1 in any scenario. The article defines this as self-scaling and found this property to be beneficial in the case of multipath environments. Nonetheless, the problem of identifying the maximum value of the metric remains unchanged and is still given by (4.7).
In order to enhance the robustness of the algorithm in noisy environment, [57] suggested not only to identify the midpoint of the sequence by locating the maximum of the metric, but also to refine this position. This is achieved by determining the lower and upper bounds of the metric. These are defined as

$$d_L = \underset{d}{\operatorname{argmax}}\ M[d] \quad \text{s.t.} \quad M[d] \leq 0.9M[d_M] \quad \forall d < d_M, \tag{4.9}$$

$$d_U = \underset{d}{\operatorname{argmax}}\ M[d] \quad \text{s.t.} \quad M[d] \leq 0.9M[d_M] \quad \forall d > d_M. \tag{4.10}$$

In (4.9) and (4.10), a threshold of 90% of the maximum of the metric is employed to identify the bounds. However, this threshold may be modified and optimized. The index situated midway through the sequence is refined by using those bounds and can be expressed as

$$\hat{d} = \frac{d_L + d_U}{2}. \tag{4.11}$$

4.1.3 Simulation Results

The result of the algorithm with the improvement proposed in [57] is presented in Figure 4.1. In this figure, the received signal has a length of 128 samples[1]. In this simulation, the delay is fixed at 308 samples and the SNR is set to 20 dB. The maximum value n_{M} of the metric proposed by [56] is equal to 307 in this test. The lower and upper bounds are represented, respectively by n_{L} and n_{U} and are equal to 304 and 312. Finally, the refined middle n_{hat} of the sequence is equal to 308. This result is consistent with the fixed delay added to the received signal. During this test, the algorithm is capable of identifying the middle of the sequence with a precision of one sample for the modified Schmidl & Cox algorithm and with zero samples for the refined version. Figure 4.1 illustrates how the refined version could enhance the precision of the algorithm. Nevertheless, this improvement is most effective in low SNR scenarios. Indeed, in the case of high SNR, the modified version is already accurate enough, and the refined version could be less efficient and prone to errors due to the additional steps.

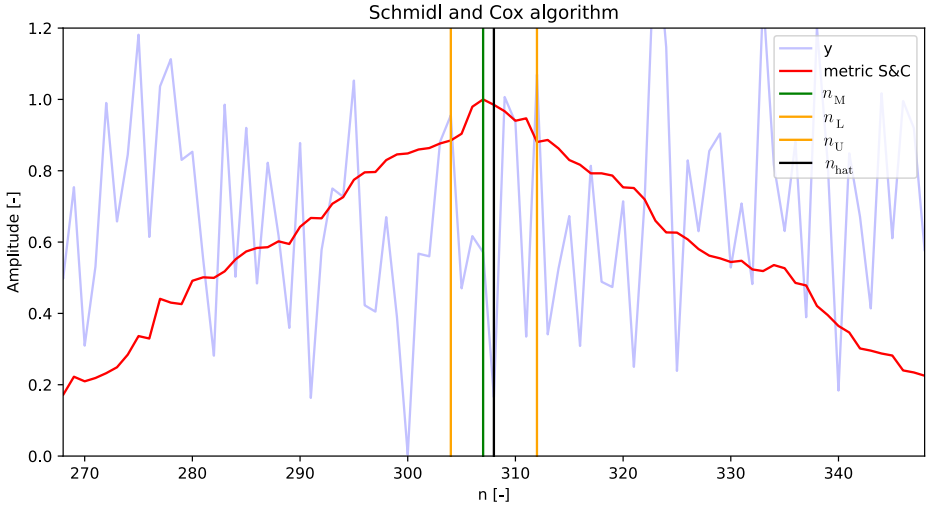


Figure 4.1: Schmidl & Cox algorithm with the improvement proposed in [57]. In blue the received signal, in red the metric proposed by [56], in green the maximum of the metric, in yellow the lower and upper bounds and in black the refined middle of the sequence.

The presented techniques have been simulated with different levels of noise. Figures 4.2 and 4.3 present a comparison between the correlation and the two pre-

[1]The sequence is composed of two parts of 64 samples.

sented versions of the Schmidl & Cox algorithm. The modified version employs (4.7) to identify the middle of the sequence, while the refined version uses (4.11). The sequence used is a sequence of 128 samples composed of 2 repeated sequences. The figure demonstrates that, regardless of the noise level, the correlation is the most reliable technique for estimating the timing offset. The modified Schmidl & Cox algorithm is most effective at high SNR, while the refined version is preferable for low SNR events. However, the difference between the two versions is not significant, as the refined version uses the estimation of the modified version.

One advantage of the Schmidl & Cox algorithm is that the sequence of interest is not required to be known. Indeed, only the length of the sequence is necessary. In this work, since the sequence is known, the correlation is the optimal technique for time synchronization, as the results are more reliable. Moreover, the correlation allows for an odd number of samples in the sequence and the use of any sequence. This is not the case for the Schmidl & Cox algorithm.

Another advantage is that the Schmidl & Cox algorithm is more robust to noise and multipath than the correlation. Indeed, the correlation is based on the cross-correlation between the received signal and the known sequence. If the signal is noisy or multipath is present, the correlation could be less efficient. The Schmidl & Cox algorithm is based on the autocorrelation of the received signal. This means that the algorithm is more robust to noise and multipath as the signal is correlated with itself.

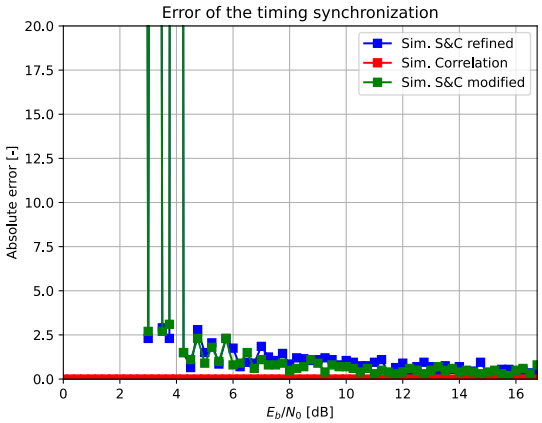


Figure 4.2: Simulation - Comparison of the correlation and the Schmidl & Cox algorithms in natural scale.

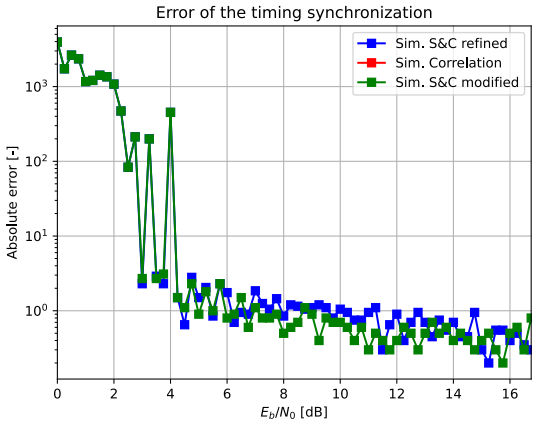


Figure 4.3: Simulation - Comparison of the correlation and the Schmidl & Cox algorithm in semi-logarithmic scale.

4.2 Frequency Synchronization

Another synchronization that must be performed is the frequency synchronization. The objective is to correct the carrier frequency offset between the transmitter or the receiver. This offset can be caused by Doppler shifts added by the environment or the motions of the transmitter and the receiver. Another source of the carrier frequency offset is the different oscillators used in those devices.

The offset can be corrected using a variety of techniques. This section presents three techniques: the Schmidl & Cox algorithm across two successive sequence, the Schmidl & Cox algorithm across multiple OFDM pulses, and an FFT-based algorithm. It is assumed that the timing offset has been corrected perfectly by one of the techniques presented in Section 4.1.2. The frequency offset in a noiseless signal can be expressed as

$$r(t) = s(t)e^{j2\pi f_{\text{CFO}}t}, \tag{4.12}$$

where $r(t)$ represents the received signal, $s(t)$ is the transmitted signal, and f_{CFO} refers to the carrier frequency offset (CFO).

4.2.1 Classical Communication Algorithm

For classical communication systems, the CFO is corrected by using a preamble at the start of a packet. This is represented in Figure 4.4 by the OFDM pulse only composed of pilots. The Schmidl & Cox algorithm presented in Section 4.1.2 can also be used to estimate the frequency offset. After having found the middle of the sequence, the frequency offset can be estimated using (4.13). This algorithm is also referred to as the Moose algorithm [58]. In this section, it is assumed that the timing offset has been perfectly corrected, which allows the middle of the sequence to be known.

$$CFO = \frac{f_s}{\pi L} \times \arg(P[d_M]). \tag{4.13}$$

In (4.13), f_s represents the sampling frequency, $P[d_M]$ is the autocorrelation metric at the midpoint of the sequence, and "arg" is the phase of the metric. In this case, the CFO is estimated across two consecutive sequences, each of which has a length of L.

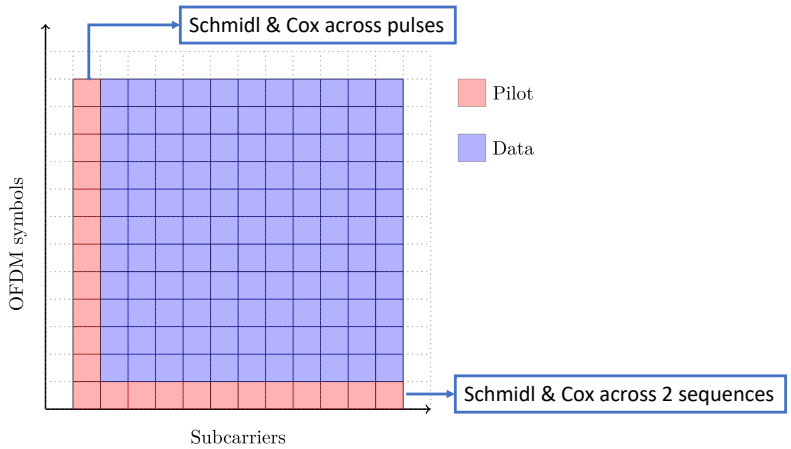


Figure 4.4: Comparison of the pilots position in the Schmidl & Cox algorithm across 2 sequences and in the Schmidl & Cox algorithm across multiple pulses.

4.2.2 JCAS Algorithm

For JCAS systems, the number of pulses transmitted is higher than for communication systems to provide sufficient Doppler resolution. This allows the CFO correction to be performed over these pulses. Two different techniques are presented: the Schmidl & Cox algorithm over multiple OFDM pulses and an FFT-based algorithm.

Schmidl & Cox Algorithm Across Different Pulses

To enhance the resolution, the Schmidl & Cox algorithm can be executed across multiple OFDM symbols. This approach extends the duration of the sequence used to estimate the CFO, thereby achieving a more accurate CFO estimation. The required modification to the system is the incorporation of a pilot symbol on a specific subcarrier. Figure 4.4 illustrates this with pilots on the first subcarrier. The pilots across the pulses are then separated in time by an interval of one OFDM symbol instead of a symbol. As the algorithm is only applicable to sequences comprising two repeating parts, the different pilots added to the subcarrier must be arranged in such a sequence. Furthermore, it is important to note that the number of pulses present in an OFDM symbol should not be less than the length of the sequence. In this technique, the CFO is estimated using

$$CFO = \frac{1}{\pi L T_{\mathrm{PRI}}} \times \arg(P[d_M]). \tag{4.14}$$

In this case, the middle of the sequence is also perfectly known. In (4.14), T_{PRI} represents the duration of an OFDM symbol, while L denotes the length of the

sequence. The metric $P[d_M]$ is calculated using the methodology presented in the previous section, but across multiple pulses. One can note that the resolution is increased compared to the Schmidl & Cox algorithm across two sequences thanks to the longer duration of the sequence used to estimate the CFO.

FFT-based Algorithm

The FFT-based method is inspired by [30]. In this article, the authors propose to use the preamble to estimate the CFO by performing a DFT. Indeed, the preamble of the received signal can be extracted, and by dividing the received preamble by the known preamble, the CFO can be isolated and estimated. To enhance the precision of the CFO estimation, the received preamble can be zero-padded prior to performing the DFT. The CFO is then estimated by selecting the maximum value of the obtained signal in the frequency domain.

This work presents an alternative approach that employs the same pilot sequences[2] as the Schmidl & Cox algorithm across multiple pulses. This approach enhances the resolution of the estimation compared to solely using the preamble, as the duration of the sequence used for CFO estimation is extended. By employing the equation referenced in (4.12), the term influencing the p^{th} OFDM symbol is

$$CFO_p = e^{j2\pi p f_{\text{CFO}} T_{\text{PRI}}}. \tag{4.15}$$

A DFT of the CFO over multiple pulses p yields the following expression:

$$\begin{aligned} |\text{DFT}\{CFO\}[k]| &= \left| \sum_{p=0}^{P-1} e^{j2\pi f_{\text{CFO}} T_{\text{PRI}} p} e^{-j2\pi \frac{k}{P} p} \right| \\ &= \left| \sum_{p=0}^{P-1} e^{j\frac{2\pi}{P}(f_{\text{CFO}} T_{\text{PRI}} P - k)p} \right| \\ &= \left| \frac{1 - e^{j\frac{2\pi}{P}(f_{\text{CFO}} T_{\text{PRI}} P - k)P}}{1 - e^{j\frac{2\pi}{P}(f_{\text{CFO}} T_{\text{PRI}} P - k)}} \right| \\ &= \left| \frac{\sin(\pi(f_{\text{CFO}} T_{\text{CPI}} - k))}{\sin(\pi(\frac{f_{\text{CFO}}}{P} T_{\text{CPI}} - k))} \right|, \end{aligned} \tag{4.16}$$

where we used the formula of a sum of a geometric series, which is given by

$$\sum_{n=0}^{N-1} a^n = \frac{1 - a^N}{1 - a}, \tag{4.17}$$

[2] Another sequence than a 2 repeating parts sequence could be used.

and the trigonometric identity by

$$\sin(x) = \frac{e^{jx} - e^{-jx}}{2j}. \tag{4.18}$$

The CFO can be estimated by selecting the value of k that maximizes the magnitude of the DFT. The resolution of the CFO is given by the expression

$$\Delta f_{\mathrm{CFO}} = \frac{1}{PT_{\mathrm{PRI}}}, \tag{4.19}$$

where the value of P is the number of pulses used to estimate the CFO. An increase in the number of pulses used to estimate the CFO results in an increase in the resolution of the CFO.

To summarize, in the FFT-based CFO estimation, the pilots present on a specific subcarrier are isolated across multiple pulses. The received pilots are divided by the known pilots and an FFT is performed. The CFO is estimated by selecting the maximum value of the FFT. A zero padding can be performed to increase the precision of the estimation. This second method offers both a better precision to estimate the CFO and a stronger robustness to noise and multipath.

4.2.3 Simulation Results

The presented techniques have been simulated with varying levels of noise. For each simulation, the timing offset is precisely corrected, and a carrier frequency offset of 3.2 kHz is added. As the carrier frequency used in the simulation is 3.2 GHz, this value is equivalent to 1 ppm[3]. In the USRP system, such high values of CFO between the internal oscillators are not present. Nevertheless, this value is employed to underscore the distinction between the techniques.

The number of resource units for each simulation is 128. The Moose algorithm employs a repeating sequence of two 64-symbol sequences, either in two successive symbols or across 128 pulses, with a single subcarrier dedicated to the pilots. The FFT-based algorithm is also performed across 128 pulses with a single dedicated subcarrier.

[3]ppm stands for Parts Per Million.

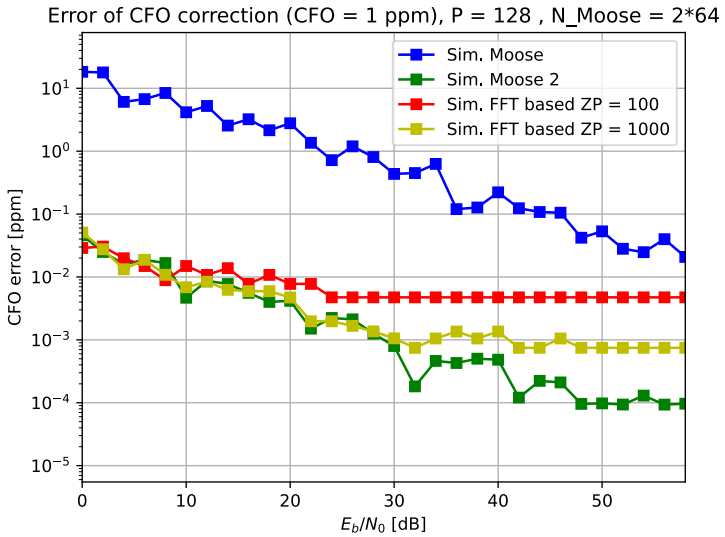


Figure 4.5: Simulation - Comparison of the different CFO estimation techniques - Moose is the classical Schmidl & Cox algorithm across 2 successive sequence, Moose 2 is the Schmidl & Cox algorithm across multiple OFDM pulses and ZP is the FFT-based algorithm with zero padding.

Figure 4.5 depicts a comparison between the presented techniques. The first observation is that the Schmidl & Cox algorithm across two consecutive sequences exhibits the poorest performance. As the duration of observation is shorter, the resolution of this method is lower than the two other methods. When performed across pulses, this method is the most precise one for all levels of noise. Nevertheless, as the precision of the FFT-based method can be increased by zero padding, this method can achieve the same performance as the second method. One significant advantage of the FFT-based method is that it does not require a repeating sequence. This allows for a more flexible system. Indeed, if the number of pulses fluctuates and is lower than the two sequences required by the Schmidl & Cox algorithm, the FFT-based method can still be employed and perform well.

4.3 Summary of the Synchronization

In conclusion, the purpose of this objective is to compare different synchronization techniques. For this purpose, the correlation and the Schmidl & Cox algorithm for timing synchronization were tested. Correlation is the most reliable technique for correcting the timing offset.

For frequency synchronization, the Schmidl & Cox algorithm was tested over two consecutive sequences and over multiple OFDM symbols, and the FFT-based algorithm was tested. The FFT-based algorithm is the most flexible method and can achieve the same performance as the Schmidl & Cox algorithm over multiple OFDM symbols, so it seems to be the best method to use for frequency synchronization.

For the experimental setup, it is the correlation with the known preamble HE-LTF that is used for the timing synchronization. For the frequency synchronization, the FFT-based algorithm is used. After having implemented those methods in the systems, The packets are well detected and the estimated CFO with the connection with an OctoClock is close to 0 Hz showing the good performance of this synchronization.

CHAPTER 5

OFDM - Joint Radar and Communication

The selected modulation for the joint radar and communication setup is OFDM. This chapter presents this modulation in the context of communication and radar used in this work. It also presents the different steps to obtain the signal and how the processing of the signal is performed to extract the information of interest. Firstly, the communication chain implemented in this work is presented, along with the choices made for the different parameters. Secondly, the radar chain is presented with the same structure. As previously stated in Section 2.3, both chains are separated and performed by different devices. The receiver of the communication chain is only aware of the preamble of the packets and the pilots present in the signal. In contrast, the radar receiver has access to the entire transmitted signal, which it can use to estimate the relevant parameters.

5.1 Communication

The used OFDM transmission chain is presented in Figure 5.1. The objective of this section is to present the distinct stages of the OFDM transmission chain, from the encoding of the binary stream to the decision of the bits based on the received signal.

The initial stage of the transmission chain is to map the binary steam of information to a constellation in the complex map. In this work, the chosen constellation is the 4-QAM constellation. The four possible coordinates in the imaginary plain are $-1+j$, $-1-j$, $1+j$ and $1-j$. Subsequently, a serial-to-parallel operation is

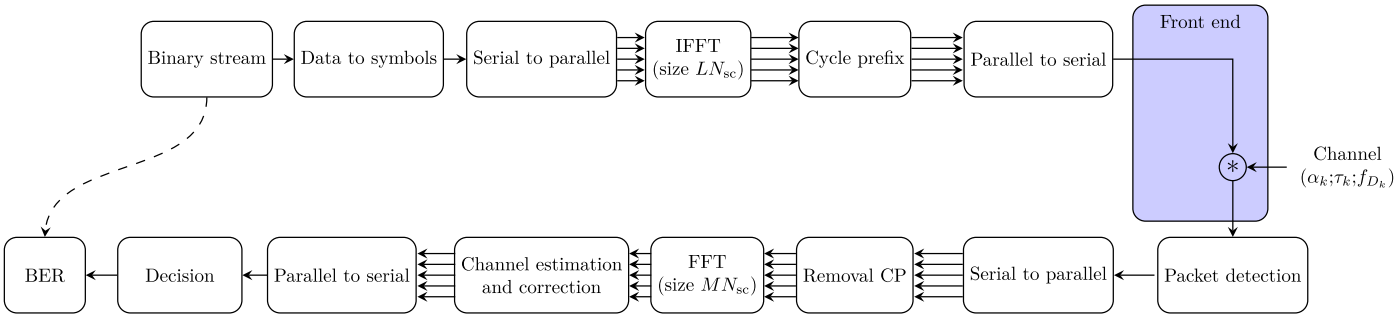


Figure 5.1: Communication - OFDM transmission chain.

performed to place the symbols on the different subcarriers. The various possibilities for the number of subcarriers (N_{sc}) in the context of Wi-Fi 6 are presented in Chapter 2. In this stage, some subcarriers may be removed and data not allocated to them.

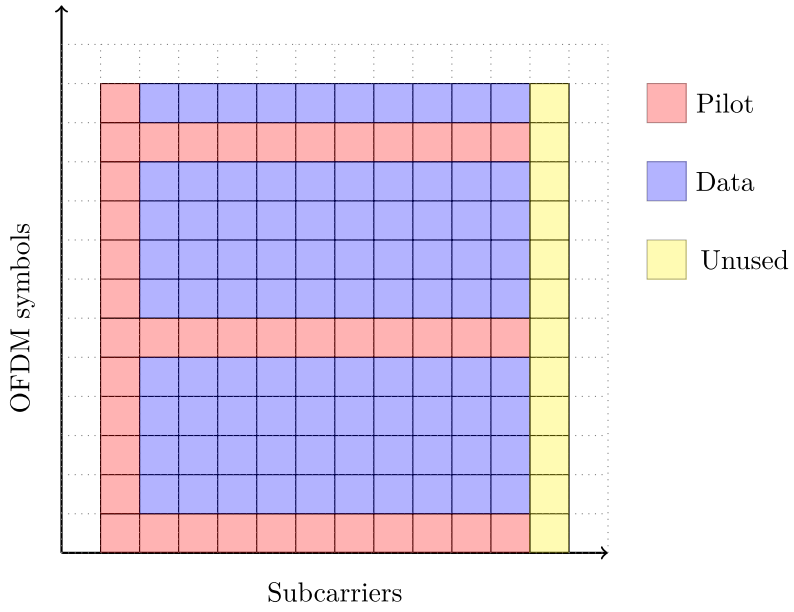


Figure 5.2: Pilot plan for the OFDM signal.

For example, the DC carrier may be removed in order to reduce noise, as well as the carriers at the edge of the bandwidth to reduce interference. Some pilots are added to some subcarriers. These can be either placed in the time domain, the frequency domain, or a combination of both. Pilots can be used to estimate the channel, correct it, or estimate the carrier frequency offset between the emitter and receiver. In this work pilots symbols are emitted on a specific subcarrier (the first

one), as well as at a repetitive interval on all the subcarriers. This is represented in Figure 5.2.

The sampling rate used by the system is 200 MS/s, with an allocated bandwidth of either 100 MHz or 80 MHz. The subcarrier spacing is defined as $\Delta_f = \frac{B}{N_{\text{sc}}}$. As the highest available bandwidths used by the USRP are constrained to 50 MHz, 100 MHz or 200MHz, the 80 MHz bandwidth is generated by employing a 100 MHz bandwidth and not using all the available subcarriers.

The next step is to transition from the frequency domain to the time domain. This is executed with an IDFT. To enhance the performance of the system, this is made with an IFFT operation. The IFFT is performed on the N_{sc} subcarriers or on a larger window of $L * N_{\text{sc}}$ size, where L is the oversampling factor and the signal is padded with $(L-1) * N_{\text{sc}}$ zeros. In this work, an oversampling factor of 2 is present to avoid aliasing.

Following these operations, the symbols are in the time domain. A cyclic prefix is added to those symbols to make the channel matrix circulant. The cyclic prefix is a copy of the last samples of the OFDM symbol which are repeated at the beginning of this symbol. The cyclic prefix will increase the robustness of the signal to ISI and multipath propagation. The duration of the cyclic prefix is selected to exceed the maximum delay spread of the channel. As presented in Chapter 2, this duration is a parameter of the transmission and in Wi-Fi 6, it is chosen to be either 0.8, 1.6 or 3.2 μs. In this work, its duration is 3.2 μs. Following the addition of the cyclic prefix, the concatenation of all OFDM symbols forms the OFDM signal, which is then transmitted over the channel.

The mathematical expression of the OFDM signal is given by

$$x(t) = \sum_{m=0}^{N_{\text{symb}}-1} \sum_{n=0}^{N_{\text{sc}}-1} S_{m,n} e^{j2\pi n \Delta f (t - mT_{\text{OFDM}} - T_{\text{CP}})} rect\left(\frac{t - mT_{\text{OFDM}}}{T_{\text{OFDM}}}\right), \tag{5.1}$$

where $S_{m,n}$ is the symbol transmitted at the m^{th} OFDM symbol and the n^{th} subcarrier. T_{OFDM} is the duration of an OFDM symbol, Δf the subcarrier spacing and T_{CP} the duration of the cyclic prefix.The OFDM signal comprises N_{sc} subcarriers and N_{symb} OFDM symbols. A rectangular window is applied around the OFDM symbol to link them together in separate time frames.

Following the emission of the signal, the environment surrounding the emitter will affect it. This channel can be modeled by multiple parameters, including the attenuation coefficient α_k, the delay τ_k and the Doppler shift f_{D_k}, where k is the

index of the path used in the environment.

$$f_{D_k} = \frac{v_k}{c} f_c \tag{5.2}$$

$$\tau_k = \frac{d_k}{c} \tag{5.3}$$

$$\alpha_k = \phi_k e^{j\gamma_k} e^{-j2\pi f_c \tau_k} \tag{5.4}$$

The expressions of the delay, Doppler shift and attenuation related to the path k are developed in (5.2) and (5.3). In these equations, c is the speed of light, v_k the velocity affecting the path k, f_c is the carrier frequency, d_k is the distance of path k, ϕ_k is the attenuation and γ_k is the phase shift due to the environment. The expression of the received signal after going through the channel is given by

$$\begin{aligned}
y(t) &= \sum_{k=0}^{K-1} \alpha_k x(t-\tau_k) e^{j2\pi f_{D_k} t} + w(t) \\
&= \sum_{k=0}^{K-1} \sum_{m=0}^{N_{symb}-1} \sum_{n=0}^{N_{\text{sc}}-1} \alpha_k S_{m,n} e^{j2\pi n\Delta f(t-mT_{\text{OFDM}}-T_{\text{CP}}-\tau_k)} e^{j2\pi f_{D_k} t} \\
&\quad rect\left(\frac{t-\tau_k-mT_{\text{OFDM}}}{T_{\text{OFDM}}}\right) + w(t) \\
&= \sum_{k=0}^{K-1} \alpha_k \sum_{m=0}^{N_{symb}-1} e^{j2\pi f_{D_k} t} \sum_{n=0}^{N_{\text{sc}}-1} S_{m,n} e^{j2\pi n\Delta f(t-mT_{\text{OFDM}}-T_{\text{CP}})} e^{-j2\pi n\Delta f \tau_k} \\
&\quad rect\left(\frac{t-\tau_k-mT_{\text{OFDM}}}{T_{\text{OFDM}}}\right) + w(t),
\end{aligned} \tag{5.5}$$

where $w(t)$ is the noise in the environment and K paths are present.

The receiver on the other side of the channel must be able to detect this signal. A coarse detection of the packet can be performed by evaluating the energy of the received signal. If this energy is above a certain threshold, the packet is detected. The signal is then sampled at a rate of $1/T_c$. After the sampling, an estimation of the main component of the delay (τ_{est}) is made, which is likely to correspond to the direct path if present. This is achieved through correlation with the HE-LTF. Additionally, at this step, a coarse estimation of the carrier frequency offset ($f_{\text{D}_{\text{est}}}$) can be performed. In this work, the recovery of a packet is performed in accordance with the methodology presented in Section 3.7, and the CFO estimation is not performed at this stage. Rather, it is performed with the FFT-Based method presented in Chapter 4. When no coarse CFO estimation is performed, the signal at this stage is given by

$$y[n] = \sum_{k=0}^{K-1} \alpha_k x(nT_c - \tau_k + \tau_{\text{est}}) e^{j2\pi f_{D_k} t} + w[n]. \tag{5.6}$$

If a coarse estimation of the CFO is performed and the estimated offset is given by $f_{\text{D}_{\text{est}}}$, the signal can be expressed as follows:

$$y[n] = \sum_{k=0}^{K-1} \alpha_k x(nT_c - \tau_k + \tau_{\text{est}}) e^{j2\pi (f_{D_k} - f_{\text{D}_{\text{est}}})t} + w[n]. \tag{5.7}$$

The remainder of this chapter will use (5.6). Once the timing offset has been corrected, the signal can be divided into multiple OFDM symbols (pulses) by transforming the serial signal into a parallel signal. The pulse notation of the signal is

$$y(p, l) = y(pT_{\text{OFDM}} + lT_c + T_{\text{CP}}), \tag{5.8}$$

where p represents the index of the pulse and l the index of the sample within the pulse. This representation facilitates a more comprehensive understanding of the signal and its processing. The received signal can be represented as follows:

$$\begin{aligned} y(p, l) = \sum_{k=0}^{K-1} \alpha_k e^{j2\pi f_{D_k} p T_{\text{OFDM}}} e^{j2\pi f_{D_k}(lT_c + T_{\text{CP}})} \sum_{n=0}^{N_{\text{sc}}-1} S_{p,n} e^{j2\pi n \Delta f (lT_c)} e^{-j2\pi n \Delta f \tau_k} \\ rect\left(\frac{lT_c + T_{\text{CP}} - \tau_k}{T_{\text{OFDM}}}\right) + w(p, l). \end{aligned} \tag{5.9}$$

If the system is well-designed, which means that T_{CP} is larger than the maximum delay spread of the channel, the received signal can be expressed as

$$\begin{aligned} y(p, l) &= \sum_{k=0}^{K-1} \alpha_k e^{j2\pi f_{D_k} T_{\text{CP}}} e^{j2\pi f_{D_k} p T_{\text{OFDM}}} \sum_{n=0}^{N_{\text{sc}}-1} S_{p,n} e^{j2\pi f_{D_k} l T_c} e^{j2\pi n \Delta f (lT_c)} e^{-j2\pi n \Delta f \tau_k} \\ &\quad + w(p, l) \\ &= \sum_{k=0}^{K-1} \tilde{\alpha}_k e^{j2\pi f_{D_k} p T_{\text{OFDM}}} \sum_{n=0}^{N_{\text{sc}}-1} S_{p,n} e^{j2\pi (n\Delta f + f_{D_k})(lT_c)} e^{-j2\pi n \Delta f \tau_k} + w(p, l) \\ &= \sum_{k=0}^{K-1} \tilde{\alpha}_k e^{j2\pi f_{D_k} p T_{\text{OFDM}}} \sum_{n=0}^{N_{\text{sc}}-1} S_{p,n} e^{j\frac{2\pi}{N_{\text{sc}}}(n + f_{D_k} T)(l)} e^{-j2\pi n \Delta f \tau_k} + w(p, l). \end{aligned} \tag{5.10}$$

The additional cyclic prefix is then removed from the signal. It is transformed from the time domain to the frequency domain by the FFT operation. Once again, the size of the FFT can be increased by a factor of M to perform an oversampling. The obtained signal is then trimmed to retain only the N_{sc} samples. The oversampling factor at the receiver is the same as at the emitter and equal to 2 in this work. In the absence of oversampling, the signal is given by

$$\begin{aligned}
\hat{S}(p,m) &= \text{FFT}(y(p,l)) \\
&= \sum_{l=0}^{N_{\text{sc}}-1} y(p,l) e^{-j2\pi \frac{ml}{N_{\text{sc}}}} \\
&= \sum_{k=0}^{K-1} \tilde{\alpha}_k e^{j2\pi f_{D_k} p T_{\text{OFDM}}} \sum_{n=0}^{N_{\text{sc}}-1} S_{p,n} e^{-j2\pi n \Delta f \tau_k} \sum_{l=0}^{N_{\text{sc}}-1} e^{-j2\pi \frac{ml}{N_{\text{sc}}}} e^{j\frac{2\pi}{N_{\text{sc}}}(n+f_{D_k}T)(lT_c)} \\
&\quad + \tilde{w}(p,m) \\
&= \sum_{k=0}^{K-1} \tilde{\alpha}_k e^{j2\pi f_{D_k} p T_{\text{OFDM}}} e^{-j2\pi m \Delta f \tau_k} \left(\sum_{l=0}^{N_{\text{sc}}-1} e^{-j\frac{2\pi}{N_{\text{sc}}}(-f_{D_k}T)l} \right) S_{p,m} \\
&\quad + \sum_{k=0}^{K-1} \tilde{\alpha}_k e^{j2\pi f_{D_k} p T_{\text{OFDM}}} \sum_{m \neq n} e^{-j2\pi n \Delta f \tau_k} S_{p,n} \left(\sum_{l=0}^{N_{\text{sc}}-1} e^{-j\frac{2\pi}{N_{\text{sc}}}(m-n-f_{D_k}T)l} \right) \\
&\quad + \tilde{w}(p,m).
\end{aligned} \tag{5.11}$$

In (5.11), the first term represents the signal of interest, the second one is the inter-carrier interference (ICI), and the last is the noise. The pilots present in the obtained signal can be used to estimate the channel and correct it. If the channel is stable in time, only one estimation over all the frequencies can be performed and kept for the whole packet. An OFDM symbol added to the preamble of the packet can be employed to perform this estimation. However, in the event that the channel undergoes rapid variation over time, pilot OFDM symbols must be transmitted at a regular interval in order to estimate the channel over time. The channel estimation is performed by the receiver and the channel matrix is obtained. In this master thesis, pilot OFDM symbols are emitted at a regular interval to perform the channel estimation. The estimation can be summarized by

$$\hat{H}(p,m) = \text{interp}\left(H_{\text{pilots}}(p,m)\right), \tag{5.12}$$

where

$$H_{\text{pilots}}(p,m) = \frac{\hat{S}(p_{\text{pilots}},m)}{S(p_{\text{pilots}},m)}, \tag{5.13}$$

where "interp" denotes the interpolation process. In (5.1), $\hat{S}(p_{\text{pilots}}, m)$ represents the received pilots, and $S(p_{\text{pilots}}, m)$ is the known send pilots. $\hat{H}(p, m)$ can directly be used to correct the signal. This signal, denoted $\tilde{S}(p, m)$, is given by

$$\tilde{S}(p, m) = \frac{\hat{S}(p, m)}{\hat{H}(p, m)}. \tag{5.14}$$

Furthermore, this stage allows for the refinement of CFO estimation and correction through the use of pilot symbols, as detailed in Chapter 4. The corrected signal can be used directly for the decision by computing the minimum distance between the received signal and the possible symbols (4-QAM). The minimization problem may be defined as follows:

$$\bar{S}(p, m) = \text{argmin}_{S_{p,m}} \left| \tilde{S}(p, m) - S_{p,m} \right|. \tag{5.15}$$

Finally, the selected symbols ($\bar{S}(p, m)$) are mapped back to the binary stream, and the BER may be computed. This allows the performance of the system to be estimated.

5.2 Radar

The majority of the components of the radar are analogous to those present in the communication chain. First, the transmission chain is identical, as it is not desired to interfere with the performance of the communication, as explained in the defined scenario in Section 2.3. The radar has access to all the information of the emitted signal to perform the detection. This information is used by the receiver to perform the detection. Figure 5.3 presents the OFDM transmission chain for the radar.

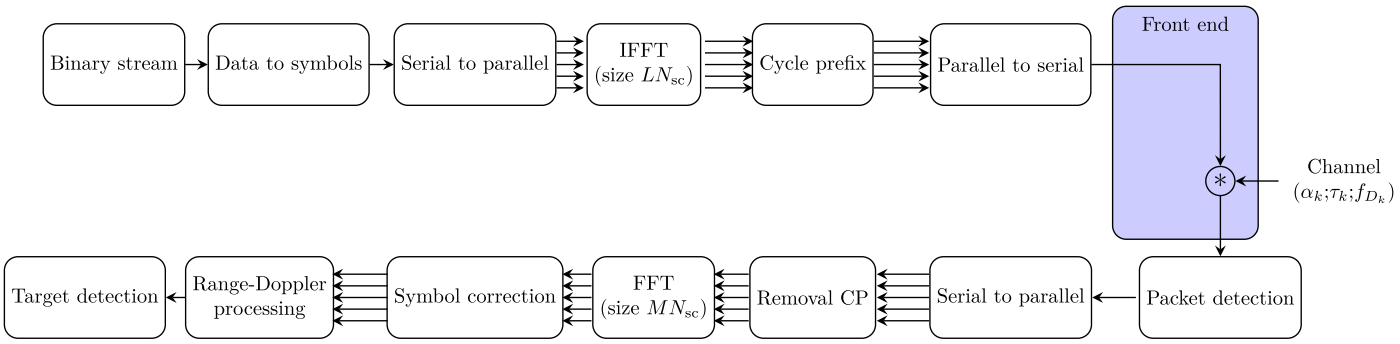


Figure 5.3: Radar - OFDM transmission chain.

At the receiver, the signal is sampled at a rate of $1/T_c$ and the timing offset is corrected. This correction corresponds to the path with the highest power, which is generally the direct path. For this correction, the entire packet can be used for the correlation instead of only the preamble in the communication case. The next step is identical to the one presented in Section 5.1. And all the processing that differs from the communication one takes place after the FFT operation previously presented.

The channel information matrix $D(m, n)$ can be obtained by dividing the received symbols $\hat{S}(m, n)$ by the known emitted symbols $S(m, n)$. This operation is presented in (5.16). In this matrix, both the delay and Doppler shift are present in two different exponential terms. For the delay, the exponential is expressed with a positive exponent term, while for the Doppler shift, the exponential is expressed with a negative exponent term. It is noteworthy that the CFO should not be corrected during the packet detection for the radar processing. Indeed, correcting it would alter the Doppler shift estimation and render it irrelevant.

$$\begin{aligned} D(m,n) &= \frac{\hat{S}(m,n)}{S(m,n)} \\ &= \sum_{k=1}^{K} \alpha_k \sum_{m=0}^{N_{symb}-1} e^{j2\pi f_{D_k} m T_{\text{OFDM}}} \sum_{n=0}^{N_{\text{sc}}-1} e^{-j2\pi n \Delta f \tau_k} \end{aligned} \tag{5.16}$$

As presented in Chapter 1, the radar signal is subject to clutters. One approach to remove the clutters is by subtracting the mean of each OFDM symbol. This method is presented in section 1.2.2 and comes from [42]. Moreover, all the element located on a relative distance[1] of 0 m are removed by subtracting the mean across the different OFDM symbols.

After this operation, an FFT is performed on the channel information matrix to estimate the Doppler shift. This operation can be zero padded to increase the precision of the estimation[2]. This FFT is performed across the different OFDM symbols. The following development expresses this operation:

[1] The relative distance of 0 m corresponds to the direct path between the transmitter and the receiver.

[2] The difference between the clutter removal method is the possible zero padding.

$$
\begin{aligned}
D_{DFT}(l,i) &= DFT\left(D(m,n)\right) \\
&= \frac{1}{\sqrt{N_{symb}}} \sum_{p=0}^{N_{symb}-1} D(m,n) e^{-j2\pi \frac{pl}{N_{symb}}} \\
&= \frac{1}{\sqrt{N_{symb}}} \sum_{p=0}^{N_{symb}-1} \sum_{k=0}^{K-1} \alpha_k \sum_{m=0}^{N_{symb}-1} e^{j2\pi f_{D_k} m T_{\mathrm{OFDM}}} \sum_{n=0}^{N_{\mathrm{sc}}-1} e^{-j2\pi n \Delta f \tau_k} e^{-j2\pi \frac{pl}{N_{symb}}} \\
&= \frac{1}{\sqrt{N_{symb}}} \sum_{k=0}^{K-1} \alpha_k \sum_{p=0}^{N_{symb}-1} \sum_{m=0}^{N_{symb}-1} e^{j2\pi f_{D_k} m T_{\mathrm{OFDM}}} e^{-j2\pi \frac{pl}{N_{symb}}} \sum_{n=0}^{N_{\mathrm{sc}}-1} e^{-j2\pi n \Delta f \tau_k}.
\end{aligned}
\tag{5.17}
$$

Equation 5.17 shows that by performing the DFT on the distinct OFDM symbols, the Doppler shift can already be estimated at this stage, while the delay is preserved. This estimation can be achieved by employing a similar methodology. Indeed, by performing an IDFT over the different subcarriers, the delay can be estimated. The following development expresses this operation:

$$
\begin{aligned}
R(y,x) &= IDFT(D_{DFT}(l,i)) \\
&= \frac{1}{\sqrt{N_{symb}}} \frac{1}{\sqrt{N_{sc}}} \sum_{t=0}^{N_{\mathrm{sc}}-1} D_{DFT}(l,i) e^{j2\pi \frac{xt}{N_{\mathrm{sc}}}} \\
&= \frac{1}{\sqrt{N_{symb}}} \frac{1}{\sqrt{N_{sc}}} \sum_{t=0}^{N_{\mathrm{sc}}-1} \sum_{k=0}^{K-1} \alpha_k \sum_{p=0}^{N_{symb}-1} \sum_{m=0}^{N_{symb}-1} e^{j2\pi f_{D_k} m T_{\mathrm{OFDM}}} e^{-j2\pi \frac{pl}{N_{symb}}} \\
&\qquad \sum_{n=0}^{N_{\mathrm{sc}}-1} e^{-j2\pi n \Delta f \tau_k} e^{j2\pi \frac{xt}{N_{\mathrm{sc}}}} \\
&= \frac{1}{\sqrt{N_{symb}}} \frac{1}{\sqrt{N_{sc}}} \sum_{k=0}^{K-1} \alpha_k \sum_{p=0}^{N_{symb}-1} \sum_{m=0}^{N_{symb}-1} e^{j2\pi f_{D_k} m T_{\mathrm{OFDM}}} e^{-j2\pi \frac{pl}{N_{symb}}} \\
&\qquad \sum_{t=0}^{N_{\mathrm{sc}}-1} \sum_{n=0}^{N_{\mathrm{sc}}-1} e^{-j2\pi n \Delta f \tau_k} e^{j2\pi \frac{xt}{N_{\mathrm{sc}}}}.
\end{aligned}
\tag{5.18}
$$

The obtained R matrix contains the information regarding the delay and Doppler shift presented in such a manner that looking at the maximum values of the matrix will give the delay and Doppler shift. These values can be obtained by using the following equations where the index m_k and n_k are the index of the maximum value of $R(m,n)$ corresponding to target k:

$$m_k = \lfloor f_{D_k} T_{\text{OFDM}} N_{symb} \rfloor \tag{5.19}$$
$$n_k = \lfloor \tau_k \Delta f N_{\text{sc}} \rfloor \tag{5.20}$$

Once the delay and Doppler shift have been obtained, the distance and speed can be calculated using the following equations:

$$\hat{\tau}_k = \frac{n_k}{\Delta f N_{\text{sc}}} \tag{5.21}$$
$$\hat{f}_{D_k} = \frac{m_k}{T_{\text{OFDM}} N_{symb}} \tag{5.22}$$
$$\hat{v}_k = \frac{\hat{f}_{D_k} c}{2 f_c} \tag{5.23}$$
$$\hat{R}_k = \frac{\hat{\tau}_k c}{2} \tag{5.24}$$

Another approach to remove those clutters would be to use the matrix D and perform a non-zero padded 2D-FFT on it and remove the values that are located at the 0 m distance and 0 m/s speed in the obtained Distance-Speed map. By doing so, the flexibility to remove zones of clutter that are not located at the 0 m distance and 0 m/s speed is added. This could be useful in a scenario where a moving vehicle performing the radar measurements want to remove the clutters, i.e. the buildings. Indeed by knowing the speed of the vehicle, the clutter can be removed by removing the values that are representing the 0 m distance and the minus speed of the vehicle. After the removal of the clutters in the frequency domain, an 2D-IFFT is performed to obtain a cleaned channel information matrix. This is presented in the first steps of Figure 5.4 and this Figure representes the radar processing, where $\tilde{R}$ is the cleaned channel information matrix.

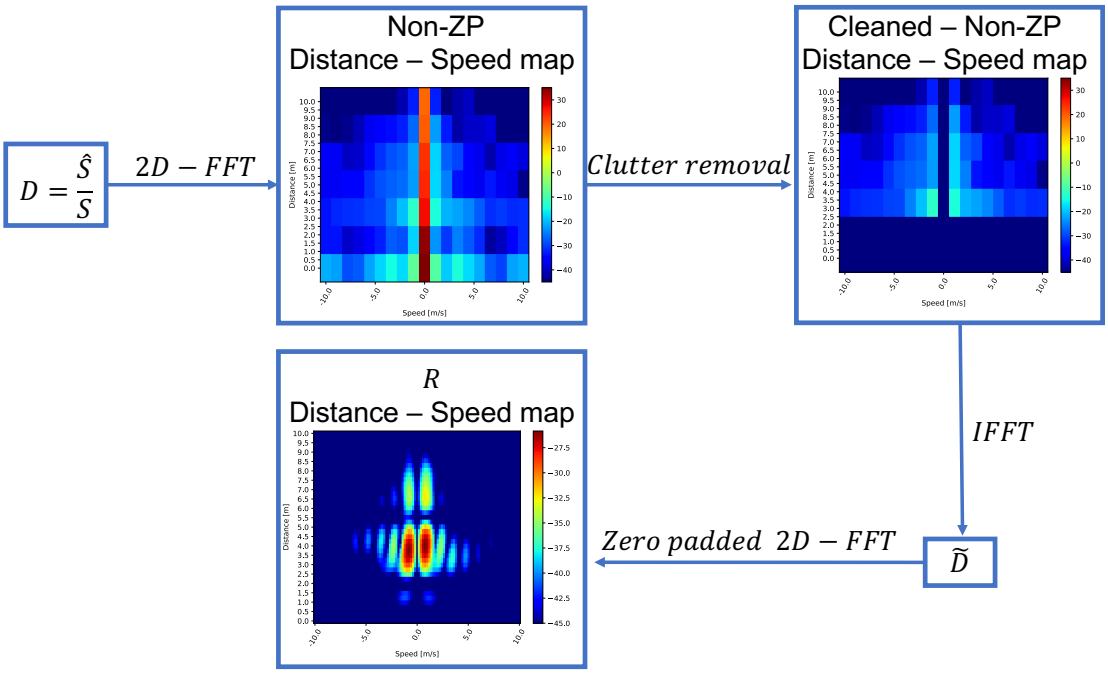


Figure 5.4: Radar - Summary of the radar processing from the CSI matrix to the estimation of the distance and speed.

It is noticeable that in the case of the radar, and with the scenario defined in Section 2.3, the delay represents the time taken for the signal to travel to the object and return to the receiver. The distance is thus the half of the delay multiplied by the speed of light. The Doppler shift is present due to the movement of the object, and only the radial velocity can be estimated.

The reachable distance and speed resolutions are defined as the ability to distinguish the parameters of two targets. The distance resolution is given by $\Delta R = \frac{c}{2B}$ and the speed resolution is given by $\Delta v = \frac{\lambda}{2PT_{\text{PRI}}}$.

5.3 Summary of the OFDM - Joint Radar and Communication

In this chapter, the structure of the OFDM communication system used in this work has been presented along with several of its recurring parameters. The different blocs of the communication chain have been introduced, as well as the different processing used. Additionally, the radar processing has also been presented and the difference between the communication and radar processing has been high-

lighted. This work employs this processing setup to perform the joint radar and communication.

CHAPTER 6

Experimental Results

In this chapter, the second generation setup presented in Section 3.5 is employed to assess the performance of the system for both communication and sensing. As described in Section 2.3, the system is tested in a scenario where the transmitter is transmitting communication frames and two receivers are present. One of the receivers is used to receive the communication frames and decode them with the help of the preamble. The second one is the AP and used to perform the sensing task. This receiver has access to the entire frame and can use it for the purpose of sensing. For each of these measurement sessions, the system is tested in accordance with this scenario.

6.1 Communication Performance

In order to assess the communication performance, the system used in this study is the one presented in the Chapter 5. The parameters used for the assessment are presented in Table 6.1. In order to estimate the SNR of the system, a measurement of the noise level, σ^2_{noise}, is performed when no signal is transmitted. The power of the signal, denoted by σ^2_{signal}, is measured when a signal is transmitted. The SNR is then calculated as follows:

$$\text{SNR} = 10 \log_{10} \left(\frac{\sigma^2_{\text{signal}}}{\sigma^2_{\text{noise}}} \right). \tag{6.1}$$

The addition of white noise to the measured signals after its reception allows for the variation of the SNR, which enables the assessment of the performance of the

system.

Parameter	Value
Frequency	3.2 GHz
Bandwidth	100 MHz
Number of subcarriers	2048
Number of transmitted bits	131072
Number of pulses	64
Rate of pilot subcarriers	1/4
Subcarriers spacing	48.828 kHz
Oversampling factor	2
Constellation	4-QAM
T_{CP}	3.2 µs
T_{OFDM}	20.48 µs

Table 6.1: Parameters used for the communication performance assessment.

To evaluate the performance of the system, the BER is used. The BER is defined as the number of bit errors divided by the total number of bits transmitted. The theoretical BER is calculated using the following formula:

$$\text{BER}_{\text{theo}} = \frac{1}{2}\text{erfc}\left(\sqrt{\frac{E_b}{N_0}}\right), \tag{6.2}$$

where E_b is the energy per bit and N_0 is the noise power spectral density.

The simulated curves are obtained by simulating the system with the channel presented in Section 5 with either 1 or 2 paths. An AWGN noise is added on top of the channel to simulate different SNRs. The BER is calculated by comparing the transmitted bits with the received bits. The results are presented in Figure 6.1. When only one path is present, the simulated BER is very close to the theoretical one, as expected. When two paths are present, the BER is higher than the theoretical one. This is due to the fact that the channel estimation is not perfect and that the multiple paths degrade the signal. The experimental BER provides the worst performance, which is likely due to the presence of multiple paths in the scene during the measurements.

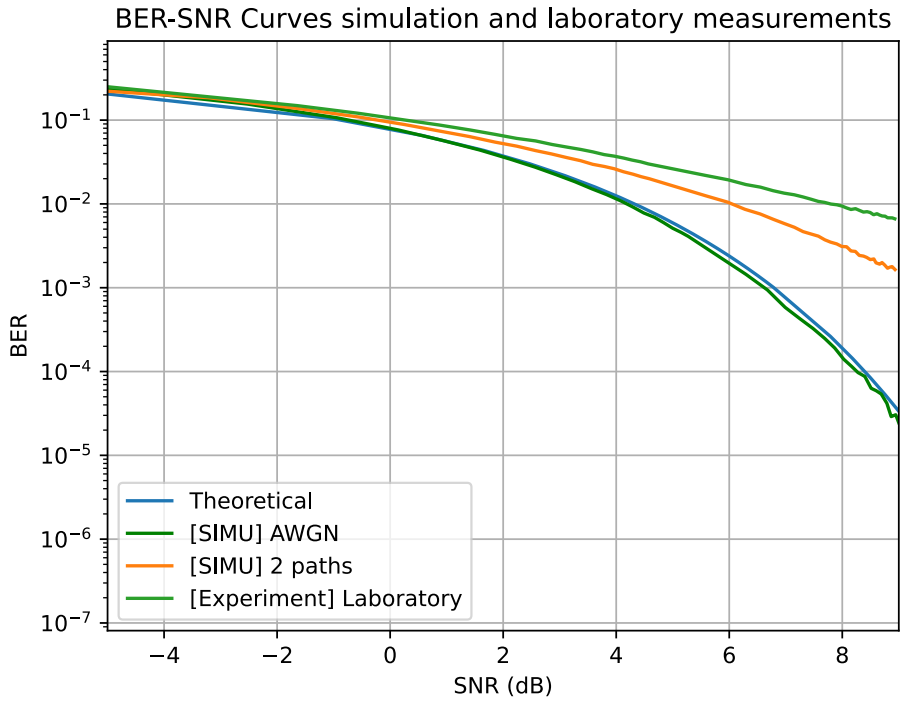


Figure 6.1: BER vs SNR for the system with 1 and 2 targets in simulation and in an experimental setup.

6.2 Sensing Performance

This section presents an evaluation of the sensing performance of the system. The system is tested in a variety of environmental conditions. The system is initially tested with a bandwidth of 100 MHz in a clutter-free environment, as well as in a laboratory setting. Secondly, the system is tested with a bandwidth of 80 MHz in a more standard-compliant setup. In this instance, the system is tested in both the laboratory and an outdoor environment. The specific parameters used for these measurements will be outlined in the respective sections.

6.2.1 Clutter-Free Environment - Anechoic Chamber

In order to assess the system in a clutter-free environment, measurements were conducted within an anechoic chamber.

Table 6.2 presents the parameters used in the experiment. The aforementioned parameters diverge from those presented in Section 2.1. In this case, the bandwidth is set to 100 MHz. The Wi-Fi standard permits the utilization of 2048 subcarriers.

Parameter	Value
Frequency	3.2 GHz
Bandwidth	100 MHz
Number of subcarriers	2048
Number of pulses	1519
Subcarriers spacing	48.828 kHz
T_{CP}	3.2 µs
T_{OFDM}	20.48 µs
Distance resolution	1.5 m
Speed resolution	1.303 m/s
Maximal detectable range	480 m
Maximal detectable speed	989.76 m/s

Table 6.2: Parameters used for the sensing experiment in an anechoic chamber.

The spacing of the subcarriers differs from that of the Wi-Fi standard, with a value of 48.828 kHz instead of 78.125 kHz. During this test, the transmitter emits a signal composed of multiple pulses, as presented in the second sensing method from Section 3.7.2, so no preamble is added to the signal and only OFDM symbols are emitted in a repeated manner. This signal is evaluated solely in terms of its sensing capabilities.

The distance resolution, which is defined as the minimal distance between two targets that can be resolved, is given by the following formula:

$$\Delta r = \frac{c}{2B}, \tag{6.3}$$

where c is the speed of light and B is the bandwidth of the signal. In this case, the range resolution is equal to 1.5 m. The speed resolution is given by the following formula:

$$\Delta v = \frac{\lambda}{2PT_{\mathrm{PRI}}}, \tag{6.4}$$

where λ is the wavelength, P is the number of pulses and T_{PRI} is the pulse repetition interval[1]. In this case, the velocity resolution is equal to 1.303 m/s.

The maximal detectable delay by the system is given by the length of the cyclic prefix, T_{CP}, which is equal to 3.2 µs. The maximal detectable range is given by

$$r_{\max} = \frac{cT_{\mathrm{CP}}}{2}, \tag{6.5}$$

[1] $T_{\mathrm{PRI}} = T_{\mathrm{OFDM}} + T_{\mathrm{CP}} = 23.68\,\mu\mathrm{s}$.

and is thus equal to 480 m.

The maximum Doppler that can be detected is given by the following formula:

$$f_{\max} = \frac{1}{2T_{\text{PRI}}}. \tag{6.6}$$

The maximal detectable speed is thus given by

$$v_{\max} = \frac{\lambda}{2T_{\text{PRI}}}, \tag{6.7}$$

and is thus equal to 989.76 m/s.

Both the maximal detectable range and velocity are high enough not to be a limitation for the measurements in the different scenarios presented in this work. To remove the clutter present in the environment, the removal algorithm presented in Section 5.2 is performed. To increase the precision of the Distance-Speed maps, a zero padding increasing the length of the FFT and IFFT processing to obtain such maps is preformed. The zero padding factor is here set to 5[2]. For the different tests with a moving target, the speed of the target is not known as this movement is created by a human operator moving during the measurement and not constant.

Experiment - Anechoic Chamber Scene

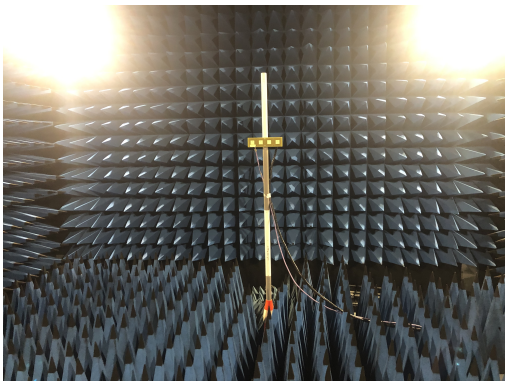


Figure 6.2: Scene in the anechoic chamber antennas.

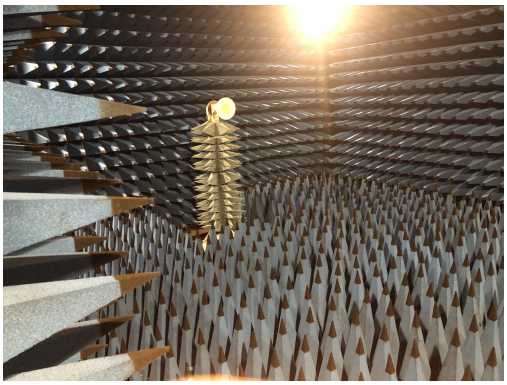


Figure 6.3: Scene in the anechoic chamber scene.

[2]If the original length is L, after the zero padding it becomes $6L$.

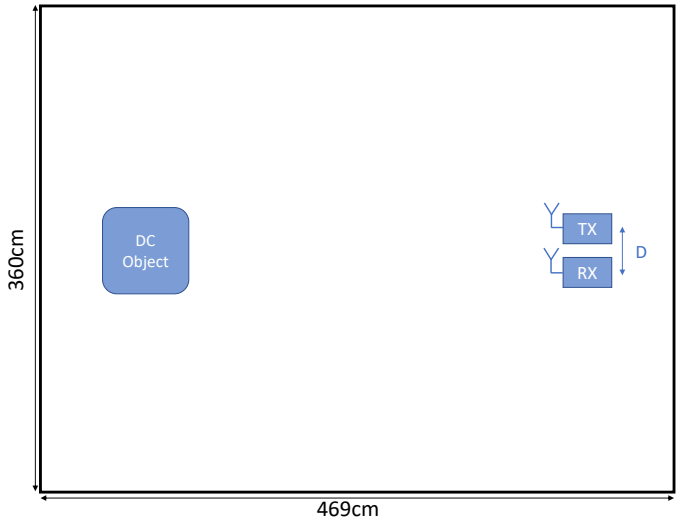


Figure 6.4: Scheme of the scene in the anechoic chamber.

The dimensions and a representation of the anechoic chamber are presented in Figure 6.4. In the scene a non-moving object covered partially with anechoic foam is present for all the measurements. This object is located at a distance of 3.8 m. A picture of this object is presented in Figure 6.3 and referred to as the "DC object". The distance between the transmitter and the receiver, D, is 21 cm and is kept constant for all the following results. Both antennas are depicted in Figure 6.2.

Experiment - Without Target

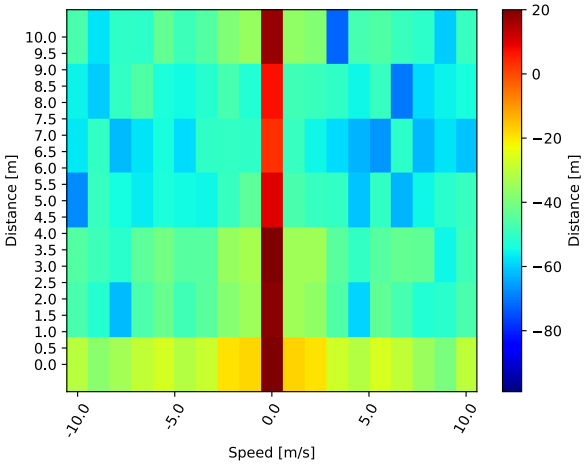


Figure 6.5: Distance-speed map in the anechoic chamber without target with clutter removal and without ZP.

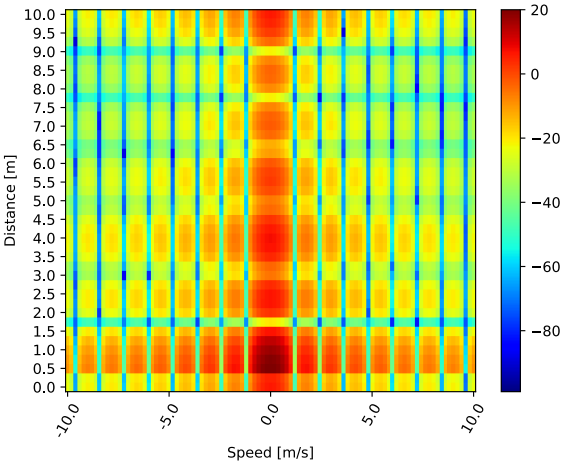


Figure 6.6: Distance-Speed map in the anechoic chamber without target with clutter removal with ZP.

The scene used in this experiment is depicted in Figure 6.4. If not removed, the clutter is present in the Distance-Speed map as shown in Figure 6.6. It can be observed that the clutter persists for all distances with a velocity equal to 0 m/s. It is probable that this phenomenon is attributable to the existence of a direct link between the transmitter and receiver, the DC object, the response of the cable linking the antennas to the USRP, as well as its internal components. The ripples observed on the map, which propagate from the clutter to other speeds, are a consequence of the zero padding performed. However, some clutters seems to be still present in at non-zero speed as the non-zero padded Distance-Speed map present in Figure 6.5 shows. As the time reference of the signal is equivalent to the direct link between the receiver and transmitter, a displacement of 21 cm is applied to the distance axis.

Once the clutter is removed, the non-moving component is eliminated, and the ripples caused by the clutter and the zero-padding operation are greatly reduced. The resulting Distance-Speed map is presented in Figure 6.7. The horizontal bar at a distance of 0.5 m and 2 m, as well as the vertical one at a speed of 0 m/s are due to the clutter removal algorithm. The amplitude of the remaining clutter after the removal is very low compared to the amplitude of the clutter before the removal. It is important to note that if a target is not moving, it cannot be distinguished from the clutter, and it will not be visible in the processed Distance-Speed map. For the different tests, the target will thus be moving.

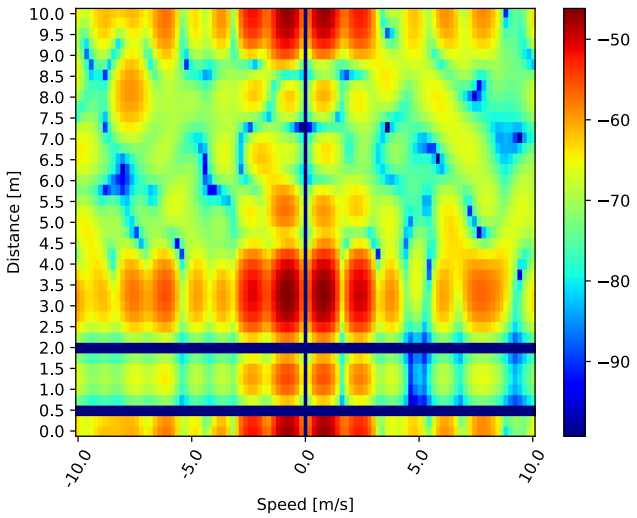


Figure 6.7: Distance-Speed map in the anechoic chamber without target with clutter removal.

Experiment - 1 Target

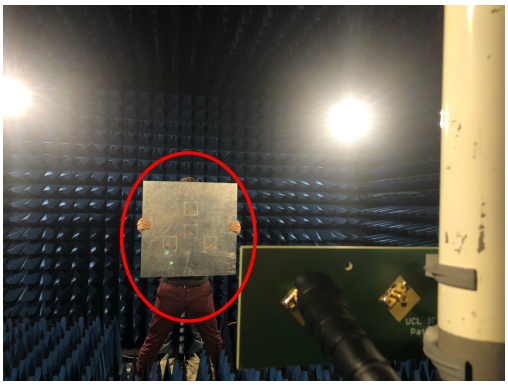


Figure 6.8: Picture - Scene in the anechoic chamber with 1 target - circled in red (view of the antenna).

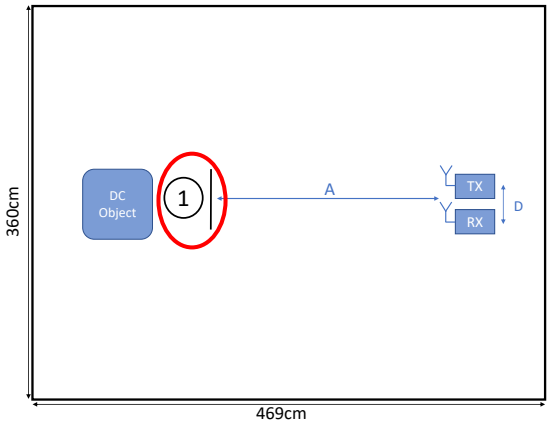


Figure 6.9: Scene in the anechoic chamber with 1 target - circled in red.

The scene with a moving target is presented in Figure 6.9. The circle labeled "1" represents the human operator, while the bar in front of him represents the metal plate. The dimensions of this plate is a square of 70 cm by 70 cm. The distance A is equal to 2.8 m. All thoses elements can be observed in Figure 6.8.

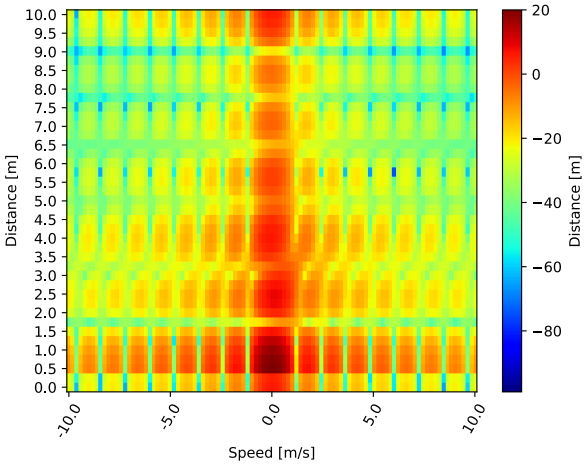


Figure 6.10: Distance-Speed map in the anechoic chamber with 1 target without clutter removal.

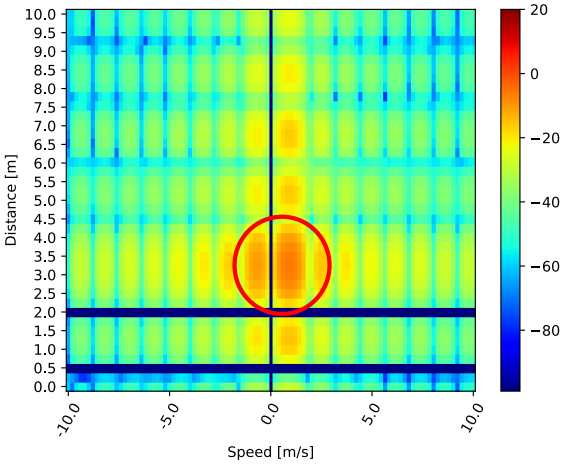


Figure 6.11: Distance-Speed map in the anechoic chamber with 1 target (circled in red) with clutter removal.

When a moving target is present in the scene, the Distance-Speed map without the removal of the clutter is presented in Figure 6.10. The outcome is comparable to the one obtained with the absence of a target and no target can be distinguished from the clutter. The Distance-Speed map that has undergone the cleaning process is presented in Figure 6.11. The target is more clearly discernible in the processed Distance-Speed map. The distance of the target is estimated to 2.75 m. The speed was not estimated, as it was not measured during the experiment. As the human operator moves the plate in a repetitive front-back motion, the speed is not constant and varies between positive and negative values as the plate moves towards or away from the receiver.

Experiment - 2 Targets

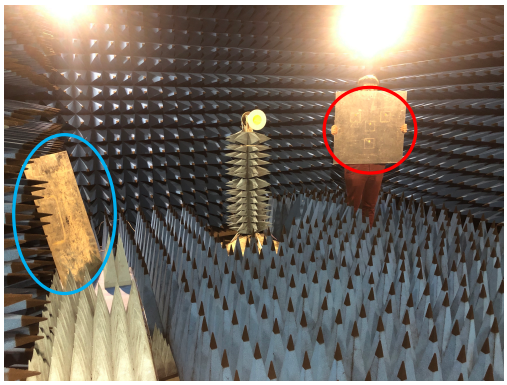


Figure 6.12: Picture - Scene in the anechoic chamber with 2 targets - the closest is circled in blue and the farthest in red.

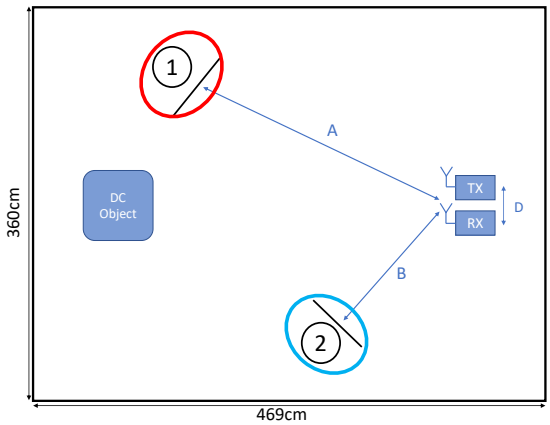


Figure 6.13: Scene in the anechoic chamber with 2 targets - the closest is circled in blue and the farthest in red, the closest is circled in blue and the farthest in red.

The scene with two moving targets is presented in Figure 6.13. The circle labeled "1" represents a human operator, and the bar in front of it represent the metal plate. This plate is a square of 70 cm by 70 cm. The distance A is equal to 3.5 m. The circle labeled "2" represents another operator, and the bar in front of it represents another metal plate. The dimensions of this plate are 50 cm by 70 cm. The distance B is equal to 1.6 m. In Figure 6.12, operator "1" is the humain in the scene, while operator "2" is the plate on the left part of the picture and during the measurement an operator comes to move it.

The result obtained without the application of the clutter removal algorithm are consistently similar and therefore not relevant for drawing any conclusions. As such, these results are not presented. Multiple measurements were performed and different results from the processed Distance-Speed maps can be drawn.

It is important to notice that in the case of targets that are close, the clutter removal algorithm needs to be adapted. Indeed, to have access to close targets during this test, only the clutters present at a distance of 0.5 m as well as all the clutters at a speed of 0 m/s are removed. Here, as the second operator is at a distance of 1.6 m, the clutter present at a distance of 2 m is not removed to be able to see this operator.

Experiment - 2 Targets - Test 1

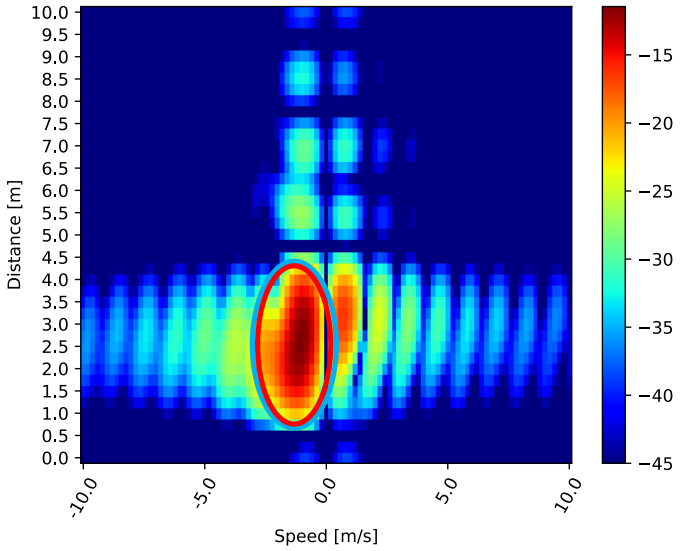


Figure 6.14: Distance-Speed map in the anechoic chamber with 2 targets (circled in both blue and red) with clutter removal.

For the first measurement, the result is presented in Figure 6.14. In this test the two targets are grouped into a single observable entity, circled in both blue and red. This is due to the fact that the two targets are moving at the same speed and are nealry at the same distance from the receiver. The resolution of the system allows for the distinction of 2 targets that are separated by more than 1.5 m. In this configuration the distance between the two targets is 1.9 m in a static position. However, this value can vary as the operators move the plate, making the distance between the plate smaller than the resolution of the system. The

estimated position of the target is 2.75 m, situated between the actual positions of the two present targets. During this measurement, Only a negative speed is observable. Two targets were thus, at this time, moving at the same speed and in the same direction.

Experiment - 2 Targets - Test 2

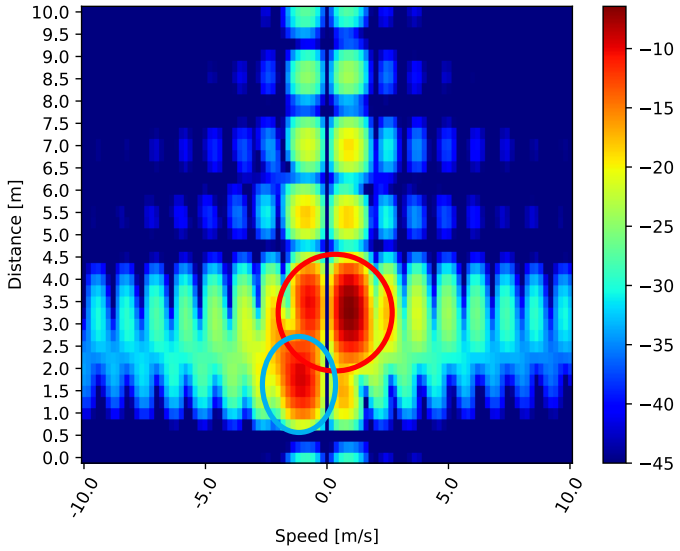


Figure 6.15: Distance-Speed map in the anechoic chamber with 2 targets (the closest is circled in blue and the furthest in red) with clutter removal.

The results of a second measurement are presented in Figure 6.15. This figure depicts the two targets, which are separated and can be distinguished. The furthest target is located at a distance of 3.25 m compared to the ground truth of 3.5 m, and the closest one is located at a distance of 1.75 m compared to the actual 1.6 m. As the two are not moving at the same speed, even if the distance between them is smaller than the resolution of the system, they can be distinguished.

Experiment - 1 Target Without Metal Plate

The scene in this test is presented in Figure 6.16. The circle 1 represents a human. The distance A is equal to 2.8 m. The operator is moving continuously in front of the receiver. Only the movement of the operator in the direction of the receiver can be observed. The scene is thus similar one in Figure 6.8 without the plate.

The Distance-Speed map is presented in Figure 6.17. The target is less discernible in the Distance-Speed map as the amplitude of the map shows. The distance of the target is estimated to be approximately 3 m.

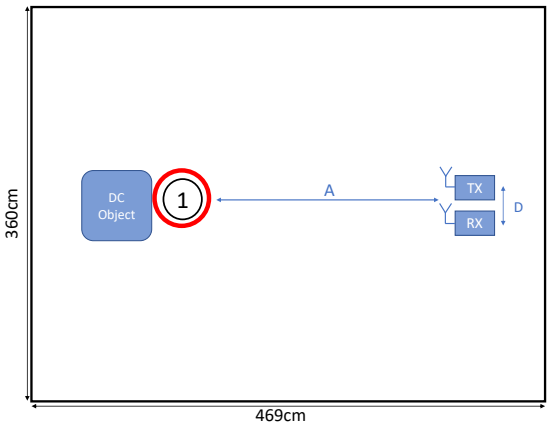


Figure 6.16: Scene in the anechoic chamber with 1 target (circled in red) without metal plate.

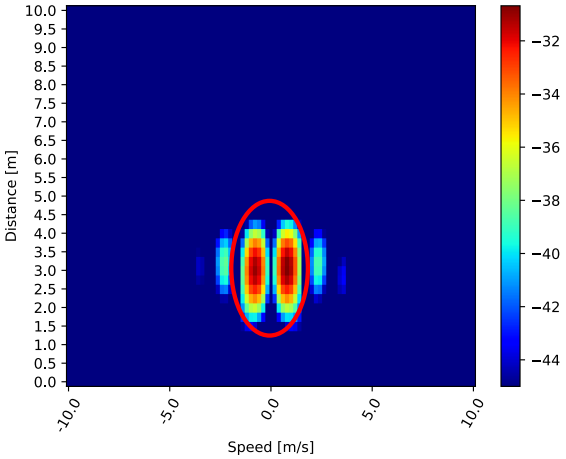


Figure 6.17: Distance-Speed map in the anechoic chamber with 1 target (circled in red) without metal plate with clutter removal.

6.2.2 Laboratory Environment

In this subsection, the results in an environment with a clutter is presented. The chosen environment is a laboratory and is first described. The results of the system are then presented in this environment.

Scene Description



Figure 6.18: Picture 1 - view of the antennas.



Figure 6.19: Picture 2 - view of the scene.



Figure 6.20: Picture 3 - view of the scene and antennas.

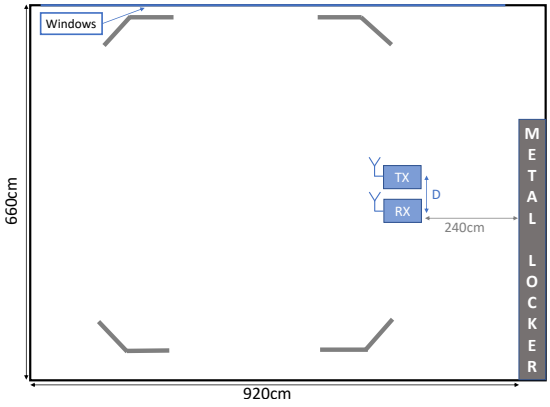


Figure 6.21: Plan of the laboratory.

In the laboratory setting, the same parameters for sensing as those presented in Table 6.2 are employed. The scene is depicted in Figure 6.21. The distance between the transmitter and the receiver, D, is 21 cm. The scene features a wall composed entirely of windows, rendering it highly reflective (see Figure 6.20). Additionally, a metal locker is situated behind the antennas (see Figure 6.18). This locker may

potentially interfere with the system. Some absorbing foams are present in the scene. They are depicted in the accompanying images and represented as gray lines on the plan. The scene is presented in three different views in Figures 6.18, 6.19, and 6.20.

Experiment - Without Target

When no target is present, the Distance-Speed map is presented in Figure 6.22. The clutters are present in the Distance-Speed map. The shape of the clutter is similar to the one obtained in the anechoic chamber and the same analysis can be made on this map. The clutter removal algorithm is applied and the processed Distance-Speed map is presented in Figure 6.23 and works as in the anechoic chamber. Nonetheless, the amplitude of the clutter and of the remaining clutter is higher than the ones of the anechoic chamber.

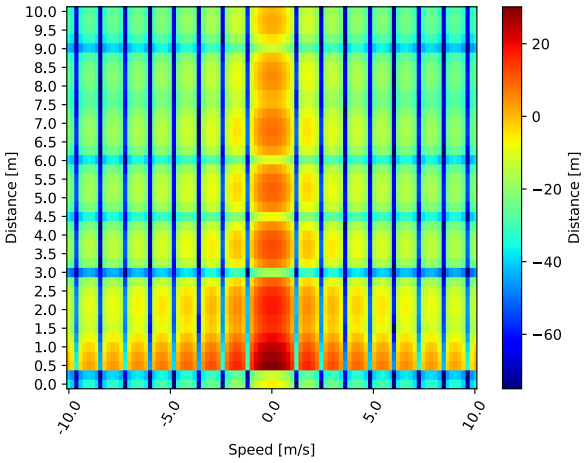


Figure 6.22: Distance-Speed map in the laboratory without target without clutter removal.

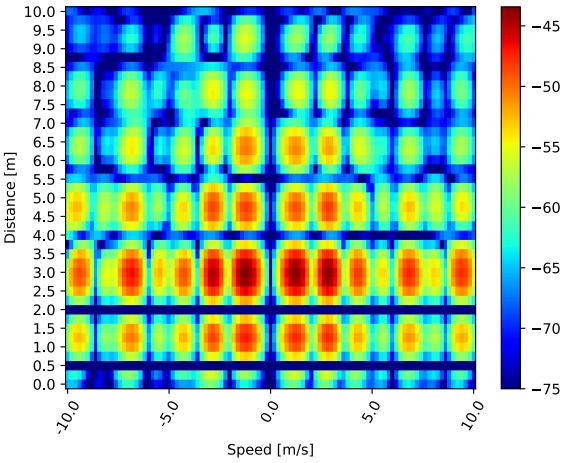


Figure 6.23: Distance-Speed map in the laboratory without target with clutter removal.

Experiment - 1 Target

The scene with a moving target is presented in Figure 6.26. The circle labeled "1" represents a human operator and the bar in front of it represent the metal plate. This plate is a square of 70 cm by 70 cm. The distance A is equal to 4.2 m.

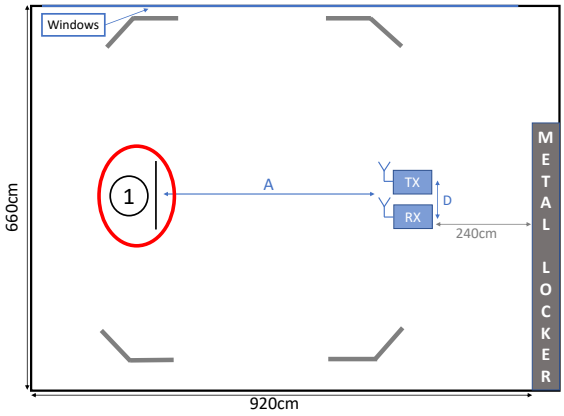


Figure 6.24: Plan of the laboratory with 1 target (cirled in red).

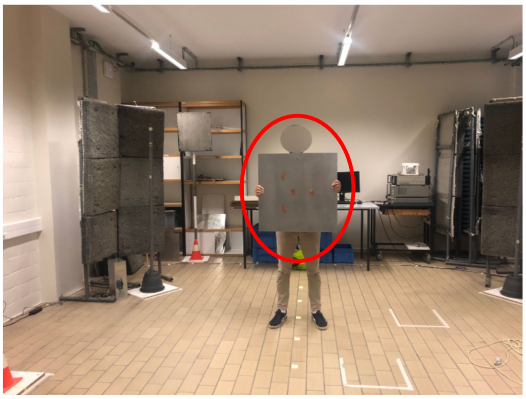


Figure 6.25: Picture - Scene with 1 target (cirled in red).

In the unprocessed map presented in Figure 6.26, the target is discernible at a distance of 3.75 m. Following the removal of the clutter (see Figure 6.27), the target is more discernible on the Distance-Speed map. The distance of the target is also estimated to be approximately 3.75 m. The speed was not estimated, as it was not measured during the experiment.

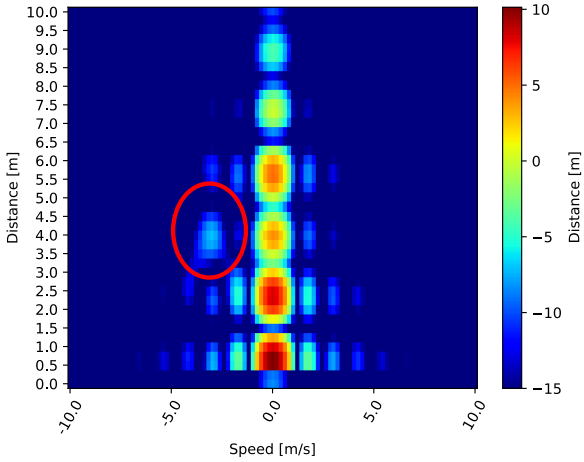


Figure 6.26: Distance-Speed map in the laboratory with 1 target (circled in red) without clutter removal.

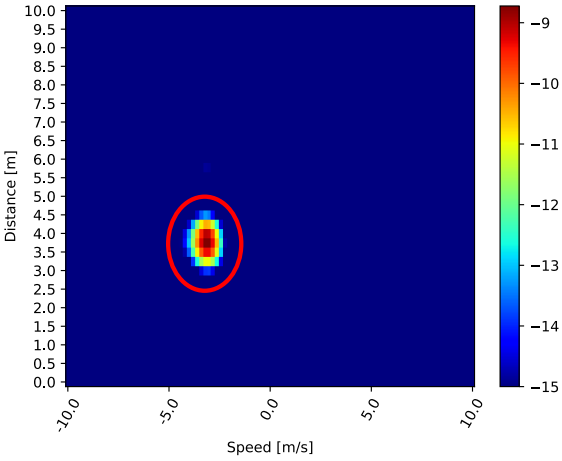


Figure 6.27: Distance-Speed map in the laboratory with 1 target (circled in red) with clutter removal.

Experiment - 2 Targets

The scene with two moving targets is presented in Figure 6.28 and a picture from the scene is present in Figure 6.29. The first operator being is holding a 70 cm by

70 cm metal plate at a distance of 3.6 m. The second one is holding a 50 cm by 70 metal plate and is located at a distance of 1.8 m. Both operators are executing a repetitive front-back movement with the plate.

The processed Distance-Speed map is presented in Figure 6.30. The two targets are clearly visible on the map. The distance of the first target is estimated to be approximately 3.5 m, while the distance of the second target is estimated to be approximately 1 m. The speed was not estimated, as it was not measured during the experiment. The ripple effect observed above the two targets is due to the zero padded FFT.

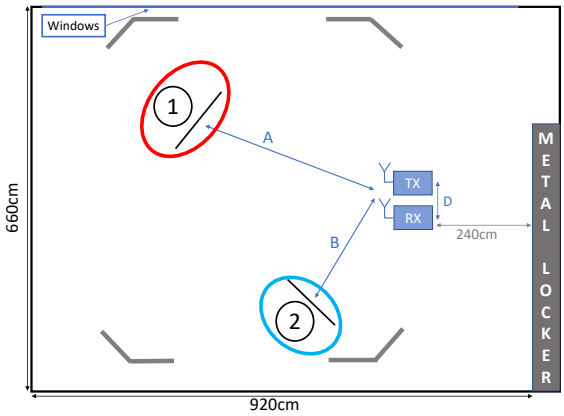


Figure 6.28: Plan with 2 targets - The closest one is circled in blue and the farthest in red.



Figure 6.29: Picture - Scene with 2 targets - The closest one is circled in blue and the farthest in red.

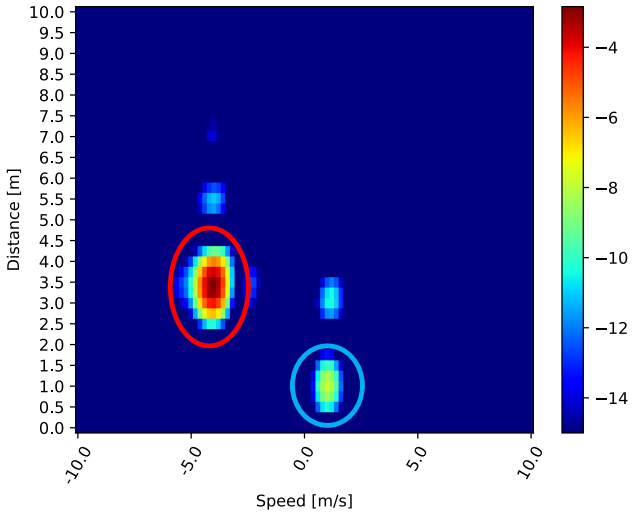


Figure 6.30: Distance-Speed map in the laboratory with 2 targets (The closest one is circled in blue and the farthest in red) with clutter removal.

Experiment - 1 Target Without Metal Plate

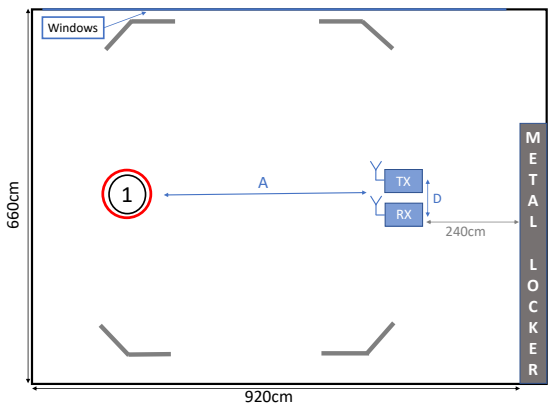


Figure 6.31: Plan of the laboratory with 1 target (circled in red) without metal plate.



Figure 6.32: Picture - Scene with 1 target (circled in red) without metal plate.

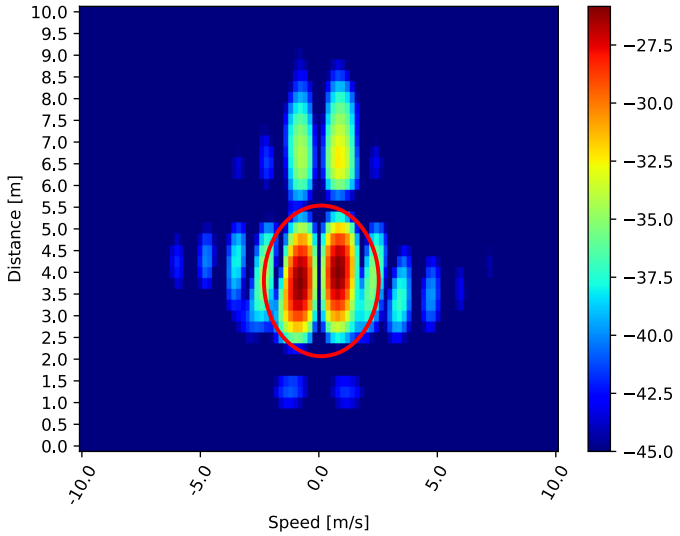


Figure 6.33: Distance-Speed map in the laboratory with 1 target (circled in red) without metal plate with clutter removal.

Without the metal plate and at a distance A of 4 m in Figure 6.31. A picture of the scene is presented in Figure 6.32.

In this scenario, the target is less visible in the Distance-Speed map, shown in Figure 6.33, as the reduced intensity shows. The distance of the target is estimated to be approximately 4 m. Due to the repeated front-back movement of the operator, the speed is not constant and varies between positive and negative values.

80 MHz Bandwidth

Going from a 100 MHz to a 80 MHz bandwidth allows the system to be more standard compliant. Measurements were performed in the laboratory environment with the same scene as the one presented in the previous subsection. The parameters for this experiment are presented in Table 6.3. For this experiment, the addition of the preamble of the Wi-Fi 6 is used and the transmitter emits a signal composed of a single packet in a repeating manner, as presented in the first sensing method from Section 3.7.2. The only difference is an increase in both resolution and the results are the similar to those obtained with a 100 MHz bandwidth. For this reason, the results are not presented here.

Parameter	Value for 80 MHz bandwidth
Frequency	3.2 GHz
Bandwidth	80 MHz
Number of subcarriers	1024
Number of pulses	1519
Subcarriers spacing	78.125 kHz
T_{CP}	3.2 µs
T_{OFDM}	12.8 µs
Distance resolution	1.875 m
Speed resolution	1.929 m/s
Maximal detectable distance	480 m
Maximal detectable speed	1464.84 m/s

Table 6.3: Parameters used for the sensing experiment - 80 MHz bandwidth.

6.2.3 Outdoor Environment

For the outdoor environment, the used parameters are the same as the one previously presented for the 80 MHz bandwidth in Table 6.3 and the Wi-Fi 6 preamble is also added.

Scene 1 - Description

The first outdoor environment is presented in Figure 6.34. The transmitter and receiver are represented by the blue pin and the spacing between them is still 21 cm. The operators are placed on the place in front of the setup. A view of the front of the antennas is shown in Figure 6.35.



Figure 6.34: Map of the outdoor environment, the blue pin represents the setup (Map data ©2021 Google).



Figure 6.35: Picture - View in front of the antennas (TX/RX).

Scene 1 - Experiment - 1 Target Without Plate and 1 With a Plate



Figure 6.36: Picture - Scene with 2 targets a few seconds after the measurement - The closest one, without metal place, is circled in blue and the farthest, with a metal plate, in red.

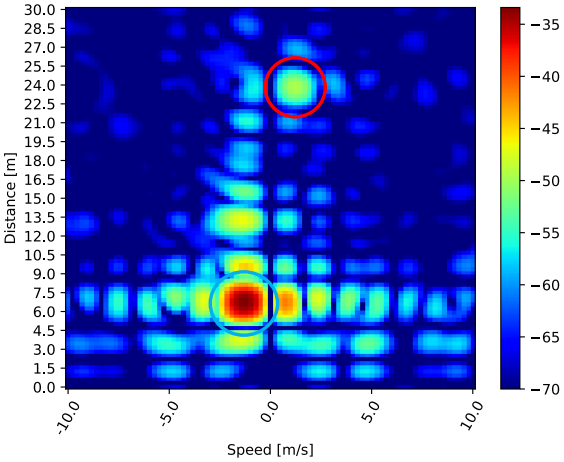


Figure 6.37: Processed Distance-Speed map in the outdoor environment with 2 targets (The closest one, without metal place, is circled in blue and the farthest, with a metal plate, in red).

In this experiment, 2 targets are present and the scene is shown in Figure 6.36. The first target, circled in green, is moving and does not have a metal plate during the displacement. The other target, circled in blue, is a moving operator holding a 70 cm by 70 cm metal plate. After the processing of the data, the obtained Distance-Speed map is presented in Figure 6.37 and the two targets are observable and circled in the same color as the scene description. The results are similar to the ones obtained in the laboratory environment and even if the distance between the farthest target is higher than the one in the laboratory, it is still observable by the system.

Scene 1 - Experiment - 2 Targets Without Plate



Figure 6.38: Picture - Scene with 2 targets - A few seconds before the measurement - The closest one is circled in blue and the farthest in red, both without metal plate.

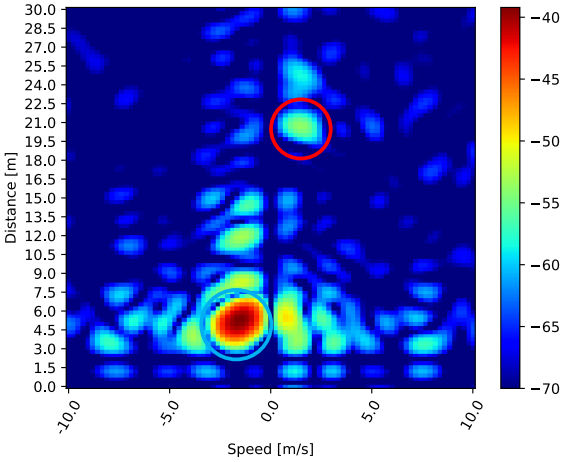


Figure 6.39: Processed Distance-Speed map in the outdoor environment with 2 targets (The closest one is circled in blue and the farthest in red, both without metal plate).

In this experiment, 2 targets are present and the scene is shown in Figure 6.38. The two targets are circled in different colors and they both move without a metal plate. After the processing of the data, the obtained Distance-Speed map is presented in Figure 6.39 and the two targets are observable and circled in the same color as the scene description. Without a metal plate, the distance of the targets can still be estimated by the system at a high distance. This highlight the possible use of the system with human targets in various environments.

Scene 2 - Description

The second outdoor scene is presented in Figure 6.40. A view of the front of the antennas is shown in Figure 6.41.



Figure 6.40: Map of the outdoor environment 2, the blue pin represents the setup (Map data ©2021 Google).



Figure 6.41: Picture - View in front of the antennas (TX/RX).

Scene 2 - Experiment - 1 Target Without Plate at Different Distances



Figure 6.42: Scene in the outdoor environment 2 with 1 target without metal plate.

For the experiment, an operator is placed at different distances going from 4 m to 24 m from the receiver. It performs a repetitive back-and-forth motion. This repetitive motion prevents a perfect ground truth of the distance of the target and thus an area of uncertainty is represented in the results. Figure 6.42 shows the scene with the operator at a distance of 24 m.

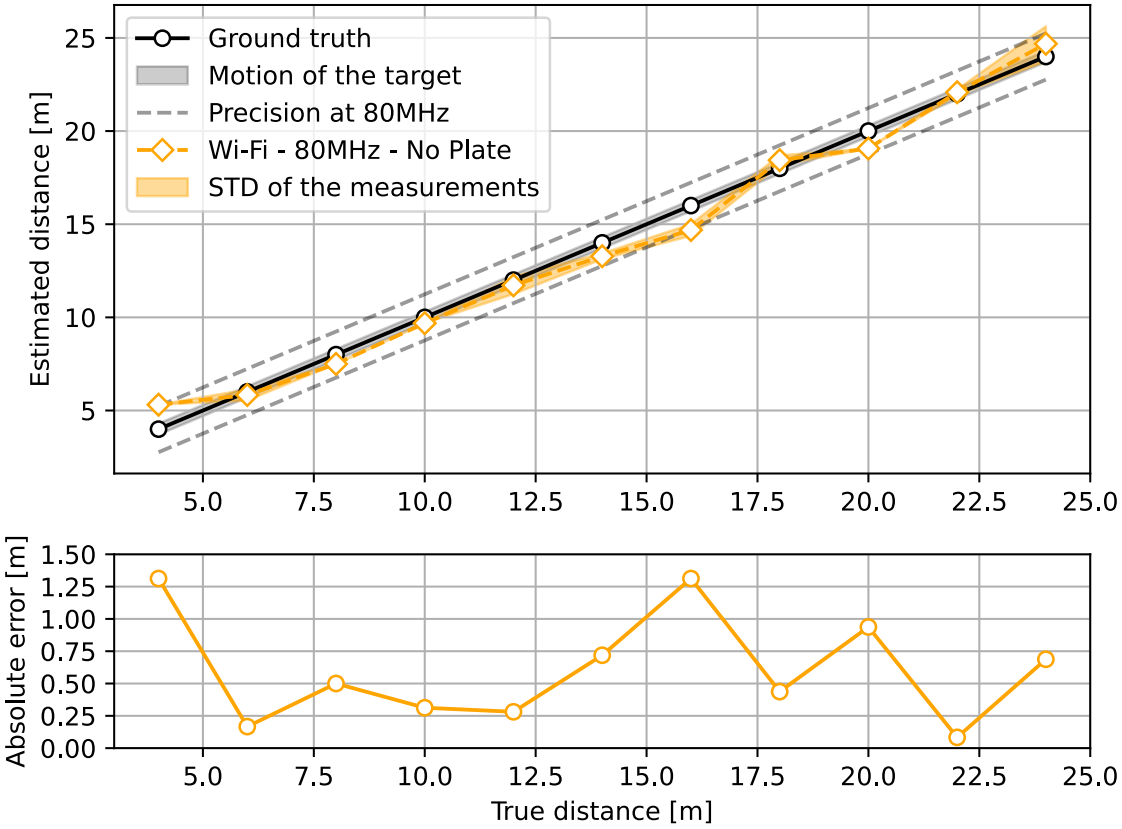


Figure 6.43: On the upper graph: Evolution of the estimated distance of the target with respect to the real distance. The real distance is represented by the black line, while the gray zone indicates the area of uncertainty of the position of the target. The gray dotted line represents the upper and lower bounds of the precision of the system around the ground truth, without zero padding at 80 MHz. The yellow line represents the mean of the estimated distance of the target, while the yellow filling represents the standard deviation of the different measurements (3). On the lower graph: the evolution of the absolute error with respect to the real distance.

Three different measurements are made for each distance and the results are shown in Figure 6.43. This figure shows the mean and standard deviation of the estimated

distance to the target. Since the resolution of the system is 1.875 m, the upper and lower bounds of the precision of the system are shown around the ground truth, allowing us to see where the target could be observed by the system. The absolute error of the estimated distance with respect to the ground truth is also shown in this figure. One can notice that the error made by the system is less than its resolution.

This experiment validates the system for the estimation the distance of moving human target, in an outdoor environment.

Scene 3 - Description

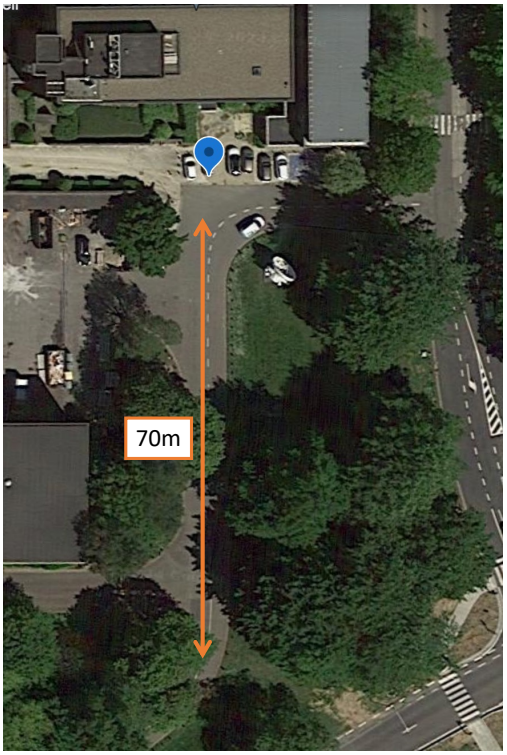


Figure 6.44: Map of the outdoor environment 3. The blue dot represents the position of the setup and the orange double arrow represents the road taken by the cars. (Map data ©2021 Google).



Figure 6.45: Picture - View in front of the antennas (TX/RX).

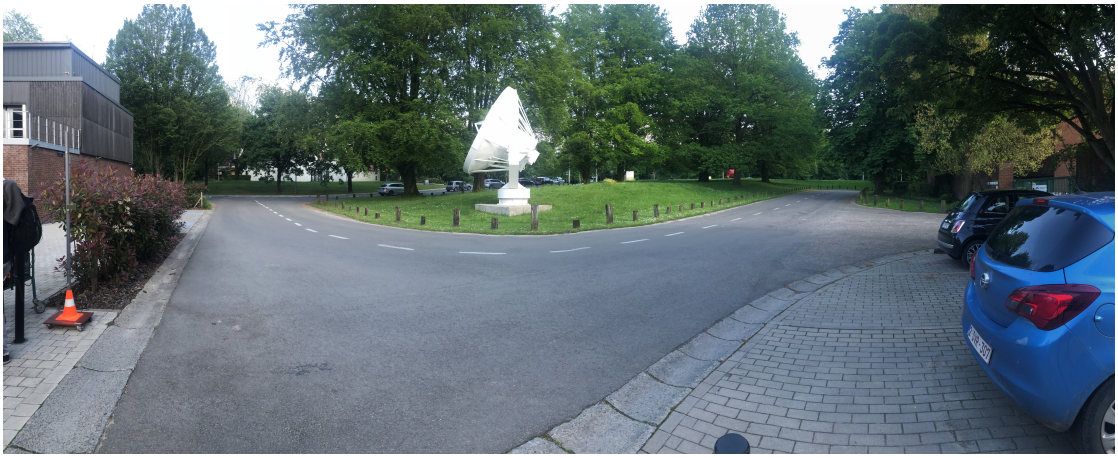


Figure 6.46: Picture - Panoramic view of the scene - on the left part is the setup and on the right part is the road used.

The map of the third outdoor environment is presented in Figure 6.44. The transmitter and receiver are represented by the blue pin and the spacing between them is still 21 cm. The scene is shown in Figure 6.45 and a panoramic view of the scene is shown in Figure 6.46. The road is used to test the system with cars as moving targets in order to observe the performance of the system with a higher speed target.

Scene 3 - Experiment - 1 Car Going Away from the Antennas



Figure 6.47: Picture - Scene with 1 car (circled in red) going away from the antennas.

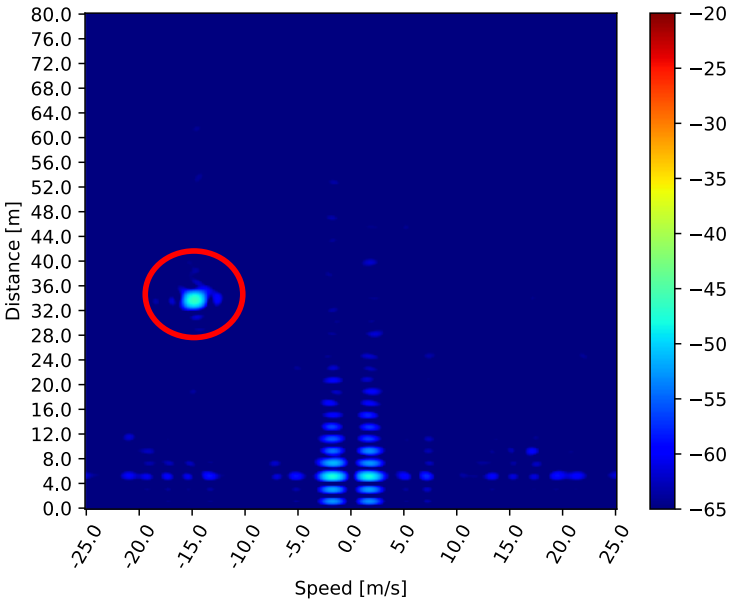


Figure 6.48: Processed Distance-Speed map in the outdoor environment with 1 car (circled in red) going away from the antennas.

One can observe that even if the car is moving away at high speed (≈65 km/h at maximal speed during the measurement on the car speedometer) from the antennas, the system is still able to detect it. The processed Distance-Speed map is presented in Figure 6.50 and the car is circled in red. The results are similar to the ones obtained in the laboratory environment and the car is observable by the system. Nevertheless, one can notice objects present at low distance. A hypothesis for those are the presence of operators behind the antennas, as well as a high reflective surface behind the antennas (an office building with some windows). To remove the clutters, the applied algorithm has removed the clutter at a distance from 0 m up to 4.25 m from the antennas, as well as all the clutters at a speed of 0 m/s.

Scene 3 - Experiment - 1 Car Going Towards the Antennas



Figure 6.49: Picture - Scene with 1 car (circled in red) going away towards antennas.

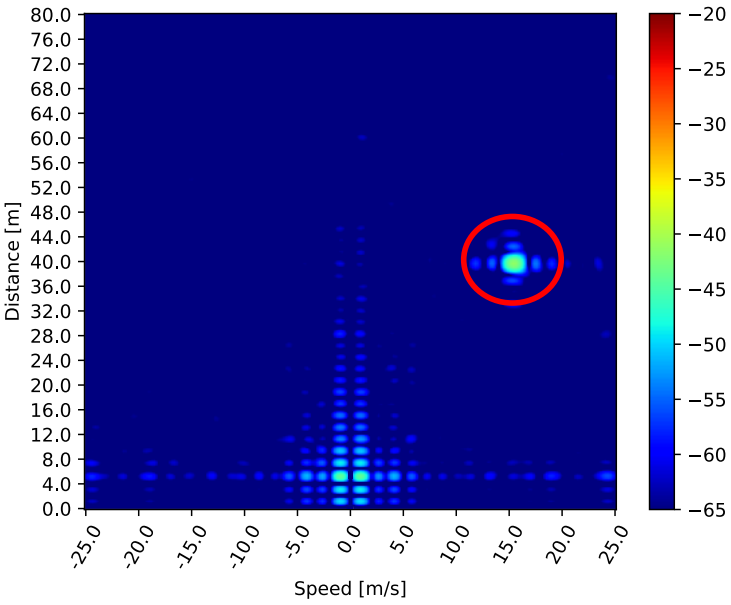


Figure 6.50: Processed Distance-Speed map in the outdoor environment with 1 car (circled in red) going towards the antennas.

When a car is moving towards the antennas, the system is also able to detect it. The processed Distance-Speed map is presented in Figure 6.50 and the car is circled in red. The results are similar to the previous experiment and the car is observable by the system. The same hypothesis as the one presented in the previous experiment can be made for the targets present at low distance.

Scene 3 - Experiment - Video of the Experiment

A video of the experiment is available at the following link: `https://www.youtube.com/watch?v=xAvA5R4mWxM`[59]. In this video, the system is tested with a car moving towards and away from the antennas. The video shows the ability of the system to detect the car in both cases. The evolution of the distance and speed of the car is also shown in the video.

This experiment with cars as moving targets validates the system for the estimation

of the distance and speed of moving targets with a higher speed in an outdoor environment. Nonetheless, this experiment should be performed with a precise ground truth to validate the system for speed estimation.

6.3 Summary of the Results

The objective of this chapter was to present the results obtained with the system in different environments. Firstly, the communication part of the system was studied and tested in a laboratory environment. Then the sensing part was tested in various scenarios, including an anechoic chamber and an outdoor environment. The sensing part functions as expected, as well as the clutter removal algorithm and the targets are visible in the processed Distance-Speed map. The outcomes observed in the laboratory environment were comparable to those observed in the anechoic chamber. Similarly, the outcomes observed in the outdoor environment were similar to those observed in the laboratory environment. Therefore, it can be concluded that the system is functioning as intended, with the targets being discernible in different environments.

Conclusion

The objective of this research was to develop an experimental JCAS setup that can perform communication and sensing tasks with an OFDM signal. In order to achieve this goal, several steps have been followed. Each of these steps has been presented in the different chapters of this report. These were the following:

- In Chapter 1, the state of the art of the JCAS systems was presented with a broad overview, with a particular focus on the OFDM JCAS systems. This allows the reader to gain an understanding of the context of the research and how such systems are used in the literature. Different points of view are presented in this chapter, from the communication to the sensing with a focus on the OFDM systems.
- In Chapter 2, the Wi-Fi standard and the new IEEE 802.11bf amendment were presented. This chapter also presents the experimental setup scenario. The IEEE 802.11bf amendment is the first amendment that focuses on the sensing capabilities of the Wi-Fi standard. This chapter is important to understand the context of the experimental setup and the new features that are available in the Wi-Fi standard.
- In Chapter 3, the experimental setup used in this work was presented, accompanied by some details on the hardware and software utilized. A characterization of performance in a stress test of the setup was also presented. This chapter is essential for understanding the setup that was used in this research and the different components that compose it. The transmitted signal is also presented, as well as how the reception of a signal is done.
- In Chapter 4, capabilities of different time and frequency synchronization methods were compared in the context of OFDM systems. This chapter

is important to understand the various methods that can be employed to synchronize the receiver with the transmitter. Synchronization is important for the correct reception of the signal and for its demodulation. The different methods are presented and compared in this chapter in order to identify the best method for the experimental setup.

- In Chapter 5, the OFDM system and its constituent blocks were presented. This chapter is important to understand the different blocks composing an OFDM system used and how they interact with each other. The different blocks are presented in this chapter.
- In the final chapter, the experimental results for the communication and sensing tasks are presented. This chapter outlines the results obtained with the experimental setup, which are then analysed and discussed.

The developed setup can be enhanced in multiple ways. Some of the improvements that can be made include the following:

- MIMO capabilities could be added to the setup. This would allow having multiple antennas at both the transmitter and the receiver. This would enhance the communication link and improve sensing with the addition of an angular resolution capabilities to the setup.
- The signal processing could be improved and conducted in real-time with the utilization of the embedded FPGA. This approach would facilitate faster signal processing at the receiver, the transmitter, or both.
- It is possible to enhance the sensing capabilities. The sensing capabilities could be enhanced by employing a distinct algorithm to process the received signal and achieve a more precise resolution of the sensing. One possible algorithm that could be employed is the MUSIC algorithm, while another is the ESPRIT algorithm. Moreover, the use of deep learning could be employed to enhance the sensing capabilities of the setup.
- It is possible to use additional aspects of the IEEE 802.11 standard. The IEEE 802.11 standard has a number of features that could be employed to enhance the communication capabilities of the system. Indeed, the algorithm used by access points could be employed to enhance the communication of the system, eliminating the necessity for the emission of pilots for the purpose of channel estimation. In the context of sensing, the utilization of only the preamble of the standard represents a viable approach for achieving non-intrusive sensing.

Bibliography

[1] OpenAI. Chatgpt. https://chat.openai.com/. [Online; accessed 2024-05-04].

[2] DeepL SE. Deepl. https://www.deepl.com. [Online; accessed 2024-05-04].

[3] GitHub. Github copilot. https://copilot.github.com/. [Online; accessed 2024-05-04].

[4] Dingyou Ma, Nir Shlezinger, Tianyao Huang, Yimin Liu, and Yonina C. Eldar. Joint Radar-Communications Strategies for Autonomous Vehicles. *IEEE Signal Processing Magazine*, 37(4):85–97, July 2020. arXiv:1909.01729 [cs, math].

[5] Aboulnasr Hassanien, Moeness G. Amin, Yimin D. Zhang, and Fauzia Ahmad. Signaling strategies for dual-function radar communications: an overview. *IEEE Aerospace and Electronic Systems Magazine*, 31(10):36–45, 2016.

[6] IEEE 802 Working Group. IEEE 802.11 Task Group BF (TGBf) - Update. https://www.ieee802.org/11/Reports/tgbf_update.htm. [Online; accessed 2024-05-04].

[7] Aruba. 802.11ax (aruba white paper). https://www.arubanetworks.com/assets/wp/WP_802.11AX.pdf. [Online; accessed 2024-02-19].

[8] Zhengxin Xia and Su Chong. Wifi-based indoor passive fall detection for medical internet of things. *Computers and Electrical Engineering*, 109:108763, 2023.

[9] Nan Bao, Jiajun Du, Chengyang Wu, Duo Hong, Junxin Chen, Robert Nowak, and Zhihan Lv. Wi-breath: A wifi-based contactless and real-time respiration monitoring scheme for remote healthcare. *IEEE Journal of Biomedical and Health Informatics*, 27(5):2276–2285, 2023.

[10] J. Andrew Zhang, Md. Lushanur Rahman, Kai Wu, Xiaojing Huang, Y. Jay Guo, Shanzhi Chen, and Jinhong Yuan. Enabling Joint Communication and Radar Sensing in Mobile Networks—A Survey. *IEEE Communications Surveys & Tutorials*, 24(1):306–345, 2022.

[11] Ningbo Long, Kaiwei Wang, Ruiqi Cheng, Kailun Yang, Hu Weijian, and Jian Bai. Assisting the visually impaired: Multitarget warning through millimeter wave radar and rgb-depth sensors. *Journal of Electronic Imaging*, 28:1, 02 2019.

[12] T. Huang, N. Shlezinger, X. Xu, D. Ma, Y. Liu, and Y. C. Eldar. Multi-carrier agile phased array radar. *arXiv preprint arXiv:1906.06289*, 2019.

[13] Fan Liu, Yuanhao Cui, Christos Masouros, Jie Xu, Tony Xiao Han, Yonina C. Eldar, and Stefano Buzzi. Integrated Sensing and Communications: Toward Dual-Functional Wireless Networks for 6G and Beyond. *IEEE Journal on Selected Areas in Communications*, 40(6):1728–1767, June 2022.

[14] J. Andrew Zhang, Fan Liu, Christos Masouros, Robert W. Heath, Zhiyong Feng, Le Zheng, and Athina Petropulu. An overview of signal processing techniques for joint communication and radar sensing. *IEEE Journal of Selected Topics in Signal Processing*, 15(6):1295–1315, 2021.

[15] M.R. Bell. Information theory and radar waveform design. *IEEE Transactions on Information Theory*, 39(5):1578–1597, 1993.

[16] Mini-Circuits. The basics of orthogonal frequency division multiplexing (ofdm). `https://blog.minicircuits.com/the-basics-of-orthogonal-frequency-division-multiplexing-ofdm`. [Online; accessed 2024-04-04].

[17] Louveaux Jérôme, Oestges Claude, Vandendorpe Luc, and Wiame Charles. Communication systems. Université catholique de Louvain - LELEC2795 - Louvain-la-Neuve, 2022–2023. [Lecture notes].

[18] Xiang-gen Xia. Precoded and vector ofdm robust to channel spectral nulls and with reduced cyclic prefix length in single transmit antenna systems. *IEEE Transactions on Communications*, 49(8):1363–1374, 2001.

[19] Lei Wang, Renhui Xu, Lei Zhang, and Laixian Peng. A novel windowing scheme to suppress spectral sidelobes for ofdma system. pages 1–6, 10 2017.

[20] Jing Di and Cuiran Li. Improved nyquist windows for reduction of ici in ofdm systems. In *2011 4th IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications*, pages 438–441, 2011.

[21] Oestges Claude and Vandendorpe Luc. Wireless communications. Université catholique de Louvain - LELEC2795 - Louvain-la-Neuve, 2023–2024. [Lecture notes].

[22] S.M. Alamouti. A simple transmit diversity technique for wireless communications. *IEEE Journal on Selected Areas in Communications*, 16(8):1451–1458, 1998.

[23] Fan Liu and Christos Masouros. A Tutorial on Joint Radar and Communication Transmission for Vehicular Networks—Part I: Background and Fundamentals. *IEEE Communications Letters*, 25(2):322–326, February 2021.

[24] M. Costa. Writing on dirty paper (corresp.). *IEEE Transactions on Information Theory*, 29(3):439–441, 1983.

[25] M. Tomlinson. New automatic equaliser employing modulo arithmetic. *Electronics Letters*, 7:138–139(1), March 1971.

[26] Johannes Maurer, Joakim Jaldén, Dominik Seethaler, and Gerald Matz. Vector perturbation precoding revisited. *IEEE Transactions on Signal Processing*, 59(1):315–328, 2011.

[27] HuiKyu Lee and Heung-Gyoon Ryu. Frequency domain estimation and time domain correction of cfo and sto offsets in ofdm system. In *13th International Conference on Advanced Communication Technology (ICACT2011)*, pages 428–431, 2011.

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

[29] Sayeed Islam, Saadmaan Rahman, Billal Hossain, and Al-Amin Ahmed. Ofdm timing offset estimation with efficient methodology and observation of different modulation schemes. In *2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation*, pages 359–363, 2013.

[30] Mohamad Basim Alabd, Benjamin Nuss, Christoph Winkler, and Thomas Zwick. Partial chirp modulation technique for chirp sequence based radar communications. In *2019 16th European Radar Conference (EuRAD)*, pages 173–176, 2019.

[31] S. Coleri, M. Ergen, A. Puri, and A. Bahai. Channel estimation techniques based on pilot arrangement in OFDM systems. *IEEE Transactions on Broadcasting*, 48(3):223–229, September 2002.

[32] Imad Barhumi. Decision feedback turbo equalization for ofdm over doubly selective channels. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 3801–3806, 2012.

[33] Michael Tüchler and Andrew C. Singer. Turbo equalization: An overview. *IEEE Transactions on Information Theory*, 57(2):920–952, 2011.

[34] Tianyao Huang and Tong Zhao. Low pmepr ofdm radar waveform design using the iterative least squares algorithm. *IEEE Signal Processing Letters*, 22(11):1975–1979, 2015.

[35] Anish Turlapaty, Yuanwei Jin, and Yang Xu. Range and velocity estimation of radar targets by weighted ofdm modulation. In *2014 IEEE Radar Conference*, pages 1358–1362, 2014.

[36] Pooja Gupta and S.P. Kar. Music and improved music algorithm to estimate direction of arrival. In *2015 International Conference on Communications and Signal Processing (ICCSP)*, pages 0757–0761, 2015.

[37] Jessica B. Sanson, Pedro M. Tome, Daniel Castanheira, Atilio Gameiro, and Paulo P. Monteiro. High-Resolution Delay-Doppler Estimation Using Received Communication Signals for OFDM Radar-Communication System. *IEEE Transactions on Vehicular Technology*, 69(11):13112–13123, November 2020.

[38] Christophe De Vleeschouwer and Laurent Jacques. Image processing and computer vision. Université catholique de Louvain - LELEC2795 - Louvain-la-Neuve, 2023–2024. [Course notes].

[39] Wei Cui, Qing Shen, Wei Liu, and Siliang Wu. Low complexity doa estimation for wideband off-grid sources based on re-focused compressive sensing with dynamic dictionary. *IEEE Journal of Selected Topics in Signal Processing*, 13(5):918–930, 2019.

[40] Md. Lushanur Rahman, J. Andrew Zhang, Xiaojing Huang, Y. Jay Guo, and Robert W. Heath. Framework for a perceptive mobile network using joint communication and radar sensing. *IEEE Transactions on Aerospace and Electronic Systems*, 56(3):1926–1941, 2020.

[41] Omar Aldayel, Vishal Monga, and Muralidhar Rangaswamy. Successive qcqp refinement for mimo radar waveform design under practical constraints. *IEEE Transactions on Signal Processing*, 64(14):3760–3774, 2016.

[42] Laurent Storrer, Hasan Can Yildirim, Claude Desset, Marc Bauduin, André Bourdoux, and François Horlin. Clutter removal for wi-fi-based passive bistatic radar. In *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pages 1–5, 2020.

[43] MathWorks. Constant False Alarm Rate (CFAR) Detection. `https://nl.mathworks.com/help/phased/ug/constant-false-alarm-rate-cfar-detection.html`, [Online; accessed: 2024-04-08].

[44] Wikipedia contributors. Physical layer — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/wiki/Physical_layer`, 2024. [Online; accessed 2024-04-28].

[45] Wikipedia contributors. Medium access control — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/wiki/Medium_access_control`, 2024. [Online; accessed 2024-04-28].

[46] MathWorks. 802.11n/ac transmission - matlab & simulink. `https://nl.mathworks.com/help/wlan/802-11n-ac-transmission.html`, 2024. [Online; accessed 2024-04-24].

[47] IEEE 802.11 Working Group. Ieee 802.11ax overview. `https://grouper.ieee.org/groups/802/11/Workshops/2019-July-Coex/Coexistence-Workshop-802-11ax-Overview.pptx`, 2024. [Online; accessed 2024-04-24].

[48] Oran Sharon and Yaron Alpert. Scheduling strategies and throughput optimization for the downlink for ieee 802.11ax and ieee 802.11ac based networks. *ArXiv*, abs/1709.04818, 2017.

[49] Rui Du, Haocheng Hua, Hailiang Xie, Xianxin Song, Zhonghao Lyu, Mengshi Hu, Narengerile, Yan Xin, Stephen McCann, Michael Montemurro, Tony Xiao Han, and Jie Xu. An Overview on IEEE 802.11bf: WLAN Sensing, October 2023. arXiv:2310.17661 [cs, eess].

[50] National Instruments. Usrp 2944r specifications. https://www.ni.com/docs/en-US/bundle/usrp-2944-specs/page/specs.html. [Online; accessed: 2024-02-19].

[51] National Instruments. Usrp 2944r features. https://www.ni.com/docs/en-US/bundle/usrp-2944-feature/page/block-diagram.html. [Online; accessed 2024-02-19].

[52] Ettus Research. Octoclock cda-2990. https://kb.ettus.com/OctoClock_CDA-2990. [Online; accessed: 2024-02-20].

[53] National Instruments. Cps-8910. https://www.ni.com/nl-be/shop/model/cps-8910.html. [Online; accessed: 2024-02-20].

[54] Wikipedia. Pci express. https://en.wikipedia.org/wiki/PCI_Express. [Online; accessed: 2024-02-20].

[55] H. C. Yildirim, J. Determe, L. Storrer, F. Rottenberg, P. D. Doncker, J. Louveaux, and F. Horlin. Super resolution passive radars based on 802.11ax wifi signals for human movement detection. *IET Radar, Sonar Amp; Navigation*, 15:323–339, 2021.

[56] Stephen G. Wilson and Rui Shang. A Modified Schmidl-Cox OFDM Timing Detector, October 2020. arXiv:2010.00762 [eess].

[57] Robert W. Heath Jr. Digital communications physical layer exploration lab using the ni usrptm platform. 2011.

[58] P.H. Moose. A technique for orthogonal frequency division multiplexing frequency offset correction. *IEEE Transactions on Communications*, 42(10):2908–2914, 1994.

[59] Jérôme L. Usrp based radcom system - 80mhz bandwidth. https://www.youtube.com/watch?v=xAvA5R4mWxM, 2024. [Online; uploaded: 2024-05-17, accessed: 2024-05-19].

UNIVERSITÉ CATHOLIQUE DE LOUVAIN
École polytechnique de Louvain
Rue Archimède, 1 bte L6.11.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/epl**