



Hamburg University of Technology  
General Engineering Science  
Bachelor Thesis

## **Coexistence of Ultra-Wideband and Wi-Fi 6E**

**How does the latest IEEE 802.11ax standard challenge UWB-based radiofrequency communication in an automotive environment?**

Bachelor of Science  
Mechatronics - 51571

**Hendrik Krack**

15.04.2022

Supervised by

Dr.-Ing. Helge Fielitz & Dr.-Ing. Tobias Pilsak

Examined by

Prof. Dr.-Ing. Hoc Khiem Trieu & Prof. Dr.-Ing. Thomas Kusserow

## **Declaration**

I hereby declare that I am the sole author of this thesis and that neither any part of this thesis nor the whole of the thesis has been submitted for a degree to any other university or institution.

I certify, to best of my knowledge, my thesis does not infringe upon that of any other person nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis review committee.

---

Date & Place

---

## Abstract

This bachelor thesis is dedicated to analyzing the immediate influence of the latest IEEE 802.11ax, more commonly known as Wi-Fi 6E, on Ultra-Wideband (UWB) communication and ranging.

With Wi-Fi 6E, the Wi-Fi Alliance has brought a great challenge to UWB systems. While the most significant advancement is an extension of the electromagnetic spectral bandwidth used within Wi-Fi, additionally, Wi-Fi 6E is also proposing frequent use of channel bandwidths up to 160 MHz with radiated output power levels of 27 dBm. This introduces a significant threat to UWB used in Passive Keyless Entry (PKE) systems, commonly utilizing IEEE 802.15.4 Channel 5 at 6.489 GHz. Known from previous experiments, WiFi6E can cause severe interference to already manufactured UWB PKE systems resulting in substantial packet-error rates or even total signal loss.

The severity of Wi-Fi 6E interference originates from various distinct signal properties. With the IEEE 802.11ax, a revolution in the protocol for Wi-Fi networks has been implemented, which enables more data throughput on single channels via the use of new features like Orthogonal Frequency Division - Multiple Access and Multi-User Multiple Input - Multiple Output. While these technological advancements provide higher data rates for Wi-Fi traffic, they also result in more airtime taken by Wi-Fi frames and greater spatial use of the environment for Wi-Fi. Consequently, this reduces airtime left for UWB transmission opportunities, unaffected by possible Wi-Fi frame collisions.

By developing a test set-up built from commercially available hardware, the question of if and how one might mitigate the effects of Wi-Fi 6E on UWB through implementing a narrowband interference cancellation filter or an optimization of software protocol is approached in this thesis.

## **Acknowledgements**

I want to thank Dr. Helge Fielitz for his ongoing support through this thesis and investigation. Dr. Tobias Pilsak for the possibility of working on such an important and exciting topic. Special thanks also go to Mahmoud Sherrah, Michel Feldfoß, Stefan Terntinek, and Maik Bode, for their many hours of discussions, suggestions, and advice. Thanks also to everyone at NXP Hamburg who has supported me through any kind of help and assistance.

# Contents

<b>1</b>	<b>Introduction</b>	<b>7</b>
1	Motivation . . . . .	8
1.1	How does the latest IEEE 802.11ax challenge UWB communication systems in an automotive environment? . . . . .	9
1.2	Assignment . . . . .	10
<b>2</b>	<b>Fundamentals</b>	<b>11</b>
1	Electromagnetic Interference . . . . .	12
1.1	Causes of EMI . . . . .	12
1.2	Quantifying Interference . . . . .	14
2	Wi-Fi 6 Extended . . . . .	15
2.1	Introduction . . . . .	15
2.2	Wi-Fi 6 (E) - IEEE 802.11ax . . . . .	16
2.2.1	Orthogonal Frequency Division Multiple Access . . . . .	16
2.2.2	Multi User - Multiple Input Multiple Output . . . . .	17
2.2.3	Channel Allocation of the Wi-Fi 6 Extension . . . . .	18
3	Ultra-Wideband . . . . .	19
3.1	Advantages of Ultra-Wideband . . . . .	21
3.2	IEEE Reference Pulse, Channels, Encoding and Frameformat . . . . .	22
3.2.1	IEEE Reference Pulse . . . . .	22
3.2.2	Pulse Modulation techniques and IEEE Channels . . . . .	23
3.2.3	UWB IEEE Frameformat . . . . .	25
3.2.3.1	Preamble . . . . .	25
3.2.3.2	Start-of-Frame Delimiter . . . . .	26
3.2.3.3	Secure Time Stamp Field . . . . .	27
3.2.3.4	Payload . . . . .	28
3.3	Modulation Techniques . . . . .	29
3.4	Channel Impulse Response . . . . .	31
3.5	UWB Receiver . . . . .	33
3.6	Distance Measurements with UWB . . . . .	35
3.6.1	Signal Propagation Time . . . . .	35
3.6.2	One-Way Ranging . . . . .	35
3.6.3	Two-Way Ranging Single Sided . . . . .	35
3.6.4	Two-Way Ranging Double Sided . . . . .	37

<b>3 UWB - Wi-Fi 6E Coexistence</b>	<b>38</b>
1 Design of Experiment . . . . .	39
1.1 Hardware . . . . .	39
1.1.1 Ultra-Wideband Device - Ranger 4 (NCJ29D5) . . . . .	39
1.1.2 Wi-Fi 6E Access Point - Netgear Raxe 500 Tri-band Router . . . . .	39
1.1.3 Wi-Fi 6E Client - Laptop Hardware Update with Intel AX210 . . . . .	41
1.2 Positioning of Hardware Components . . . . .	41
1.2.1 Antenna Beam of the Wi-Fi 6E Access Point and Client . . . . .	41
1.2.2 Placement of the UWB devices . . . . .	43
1.3 Design of Software Protocol . . . . .	45
1.4 Definition of Influencing Variables . . . . .	46
2 Measurements . . . . .	48
2.1 Results . . . . .	48
2.1.1 Correlation of Wi-Fi 6E Data Stream and UWB PER . . . . .	48
2.1.2 Effect of Wi-Fi 6E onto the UWB Channel Impulse Response . . . . .	49
2.1.3 Differentiating Failure Causes . . . . .	52
2.1.4 Influence of the Wi-Fi 6E Channel Width on the Packet-Error Rate of UWB . . . . .	54
2.2 Discussion . . . . .	58
3 Redesign of Experiment . . . . .	61
3.1 Change of Protocol . . . . .	62
3.2 Results . . . . .	63
3.3 Discussion . . . . .	64
3.4 Comparison to Results at TU Graz . . . . .	65
<b>4 Narrowband Cancellation Filter</b>	<b>67</b>
1 Introduction and Fundamentals . . . . .	68
2 Implementation . . . . .	69
3 Measurements . . . . .	70
3.1 Results . . . . .	70
3.2 Discussion . . . . .	73
<b>5 Conclusions</b>	<b>74</b>
1 Evaluation . . . . .	75
1.1 Coexistence Measurements . . . . .	75
1.2 NBIC Performance . . . . .	75
2 Outlook . . . . .	76
<b>6 Appendix</b>	<b>77</b>
1 Abbreviations . . . . .	78

“As engineers we are continually faced by great opportunities brilliantly disguised as insoluble problems.”

*Lee Iacocca, American engineer and automobile executive [12]*

# **Chapter 1**

## **Introduction**

The following prologue will introduce the challenge and complexity of electromagnetic compatibility in the landscape of modern radio frequency technologies. It will then discuss how this relates to the latest release of the IEEE 802.11ax, more commonly known as Wi-Fi 6E, and why this challenges Ultra-Wideband communication. Furthermore, it will state the assignment of the thesis and give an orientation on the content.

# 1 Motivation

The phenomenon of electromagnetic interference (EMI) has been known to mankind ever since the introduction of radio frequency-based communication systems, which dates back to 1901 by Guglielmo Marconi, who played a very substantial role in the development of radio transmission in general but especially in this thesis [17]. One can confidently say that if Marconi were among us today, he would immediately grasp the complexity of electromagnetic interference and electromagnetic compatibility (EMC) today. With increasing demand and numerous electronic devices in our daily lives, EMI is all around us. We often encounter relatively harmless but annoying interference, when for example the audio speakers make strange sounds near a mobile phone or an older TV becomes pixelated. However, EMI can have and already have had much more severe consequences. In 1967 a Navy jet, intending to land on a U.S. aircraft carrier of the coast of Vietnam, unintentionally released munitions that fell right upon a fully armed and fueled fighter plane on deck. The result was a massive explosion with 134 casualties and severe damage to the aircraft and the carrier. The incident was caused by the aircraft being illuminated with carrier-based radar resulting in EMI, which sent an unwanted signal to the weapons system. Later research revealed that cables and systems on the plane had improper shielding [16].

Obligated to avoid similar accidents, organizations like the Federal Communications Commission (FCC) in the U.S. or the European Telecommunications Standards Institute (ETSI) now hold strong regulations in which spectrum usage is free for commercial licensing and regulates emission powers especially in outdoor areas. Nevertheless, today we are still encountering numerous interference problems with new technologies. In 2003 the International Telecommunication Union (ITU) recommended a new frequency allocation in the electromagnetic spectrum for the unapproved Radio Local Area Network (RLAN) services [30]. The new Spectrum allocated a range from 5250 to 5725 MHz to be divided into 15 specific 20 MHz channels. A specific dynamic frequency algorithm was defined to ensure electromagnetic compatibility, however, effects on crucial C-band weather radar systems operating in the same frequency band were visible a little later. These systems are crucial to real-time weather precautions and contribute significantly to our safety in everyday life, especially in regions that are prone to quickly changing weather conditions. Figure 1.1 shows a picture of an Italian weather station C-Band Radar interfering with the RLAN in the 5 GHz range [2]. It should be evident by now that dealing with EMI is of paramount importance.

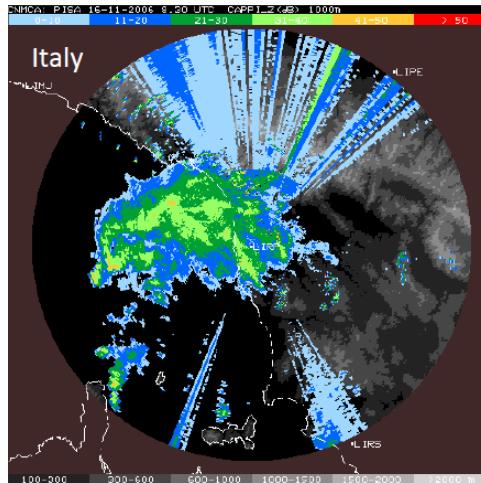


Figure 1.1: C-Band Weather Radar Interference [30]

## 1.1 How does the latest IEEE 802.11ax challenge UWB communication systems in an automotive environment?

Since its rapid rise for military use in the 60s, Ultra-Wideband (UWB) had another commercial boom at the start of the 21st century. Applications and use have been growing rapidly ever since, and compelling use cases are advancing, for example, UWB-Radar for life detection in automotive environments.

The Wi-Fi 6E threat to Ultra-Wideband communication has been a serious concern raised by the release of the latest IEEE standard 802.11ax in February 2021. This standard enlarges the spectral bandwidth used for Wi-Fi communication with an additional frequency band in the 6-7 GHz range to the traditional 2.4, and 5 GHz bands. While the United States has adopted the full scale from 5.925 to 7.125 GHz, the European Union has only certified a smaller range from 5.925 - 6.425 GHz effective since July 2021. Hardware manufacturers are pressing to release compatible devices in early 2022 in Europe. This increases the likelihood of interference problems with UWB. While the IEEE 802.15.4 allocates a spectrum from 499.2 MHz up to 9484.8 MHz, as Table 2.1 shows, the automotive industry widely utilizes Channel 5 at 6489.6 MHz, which overlaps with all commonly-used Wi-Fi 6E channels. Further intensifying this issue is the expansion of Wi-Fi channel width with frequent use of even larger 160 MHz channels in Wi-Fi 6(E) to enable higher data rates and a better multiuser experience. A total overlap can then hold up to 32% of the specified UWB Channel, which can cause substantial interference.

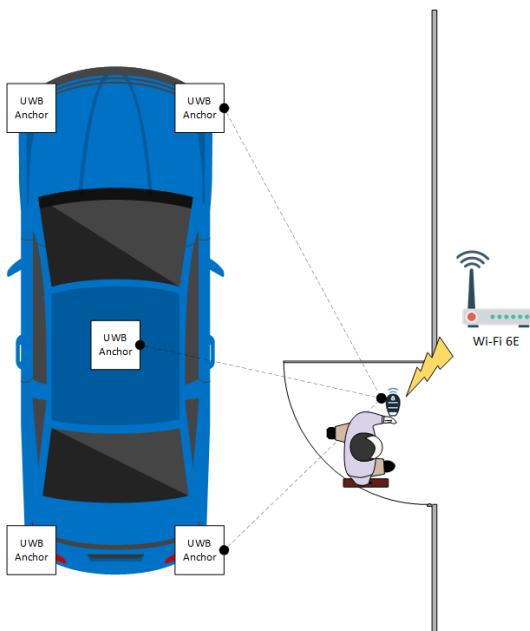


Figure 1.2: UWB PKE - Worst Case Scenario

UWB finds many applications within the industrial sector, Internet-of-Things, or smart sensors. Two popular examples for use in the automotive industry are the radar applications and the most commonly known *Passive-Keyless Entry* (PKE) system. NXP and other manufacturers have been using UWB to counteract the threat of relay attacks<sup>1</sup> that have been a great risk to traditional PKE systems. UWB could solve these problems by implementing a secure ranging method with a distance estimation of  $\Delta 10\text{cm}$  accuracy and Secure-Time-Stamp (STS) cryptography. Figure 1.2 shows a UWB PKE use case. By utilizing multiple UWB anchors at the car side, the triangulation algorithm obtains the exact position of the key fob. Now Wi-Fi 6E is threatening the functionality of UWB PKES. Previous investigations have shown that Wi-Fi 6E can cause severe data loss to UWB systems. Figure 1.2 is a theoretical worst-case user scenario in which the user parks their car in a carport in the proximity of its house. The UWB PKE system fails to calculate the distance of the key within transmission from "Unlock-" to "Lock-Zone" of the car due to interference with its Wi-Fi 6E Access Point present at the entrance, leaving the vehicle, and possibly valuable belongings unprotected. Even if highly hypothetical, this scenario raises great concern to automotive OEMs and is therefore of intriguing importance.

<sup>1</sup>Relay attack, also called Two-Thief attack, is a strategy to gain access to vehicles equipped with PKE systems by relaying the signal from the key fob, e.g., inside a house to the proximity of the car, faking a closer position of the key and therefore gaining access inside.

## 1.2 Assignment

The primary goal of this thesis, undertaken in cooperation with NXP Semiconductors Germany, was the development of a UWB - Wi-Fi 6E test set-up to reproduce, measure, and understand the interference of Wi-Fi 6E with UWB communication and ranging.

The assignment includes the exploration of different possible hardware components and configurations of such. It consequently also inherits the development of test software for measurements and data analysis. In addition, it will investigate an approach to mitigating the influence of Wi-Fi 6E by using the Narrowband Interference Cancellation (NBIC) block within NXP's latest automotive UWB integrated circuit (IC), the NCJ29D5. Furthermore, also research into alternative mitigation strategies was motivated.

In short, this thesis aims to answer to following questions:

- Does Wi-Fi 6E affect UWB communication and ranging performance? If so, how severe is the impact?
- How does the packet error/reception rate behave as a function of Wi-Fi data traffic and channel bandwidth?
- Can we improve UWB ranging in Wi-Fi 6E presence by choosing a better protocol?
- Can the NBIC block improve UWB performance as a permanent coexistence solution? If so, how good is the improvement?

To give an orientation, Chapter 2 will discuss the fundamentals and state-of-the-art science and technology dealt within this thesis, while Chapter 3 describes the detailed development of the experiment and an iterative process of improvement of the set-up, concluding with an innovation of the ranging protocol. Chapter 4 then introduces the NBIC and displays its performance and capabilities to counteract Wi-Fi 6E. In conclusion, Chapter 5 attempts to answer the questions mentioned and offers a perspective on how future work can be taken to mitigate the Wi-Fi 6E threat entirely.

## **Chapter 2**

# **Fundamentals**

As it will become apparent, the subject of interference concerning Wi-Fi 6E and UWB systems is undoubtedly complex. This chapter will introduce the basic physical phenomenon of electromagnetic interference and how it can be quantified. Furthermore, the two signaling technologies, Wi-Fi 6E and Ultra-Wideband, will be discussed appropriately for their most critical features. The main focus is on the functionality of UWB, as its recovery from Wi-Fi 6E RFI is the objective of this thesis. Therefore, the Chapter on UWB can be viewed as a reference for the discussion following in Chapters 3 and 4.

# 1 Electromagnetic Interference

*"The effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radiocommunication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy"*

Defintion by the International Communications Union (ITU) [2]

Electromagnetic Interference and particularly Radio-Frequency Interference (RFI) are among the most significant concerns in modern communication systems. Generally, one differentiates between man-made and natural EMI. As natural EMI cannot be controlled, this Chapter will focus on manufactured sources, which can be further distinguished in intentional and unintentional EMI.

Controlling man-made EMI is the primary purpose of electromagnetic compatibility. The event of EMI is called coupling and describes the mechanism by which electromagnetic emissions interfere with other susceptible electrical equipment. EMI can propagate via two routes: conducted over electrical cables and power lines or radiated over the air using the electrical wires, PCB traces, or component leads of transmitter and receiver antennas [18]. In this thesis, the effects of the latter will be further investigated.

## 1.1 Causes of EMI

A large variety of sources can generate EMI. Any occurrence of changing electric currents, whether natural or man-made, will result in a change of electromagnetic field that can potentially cause EMI. Devices like ignition systems, cellular networks of mobile phones, or natural sources like lightning or solar flares radiate electromagnetic waves that can interfere with other communication devices [7]. While RFI caused by intended transmissions from, for example, radio stations and mobile phones are categorized as Narrowband EMI. Unintentional radiation coming from sources like the ignitions system of a car or a power transmission lines results in a much larger variety of frequencies and is therefore called Broadband EMI.

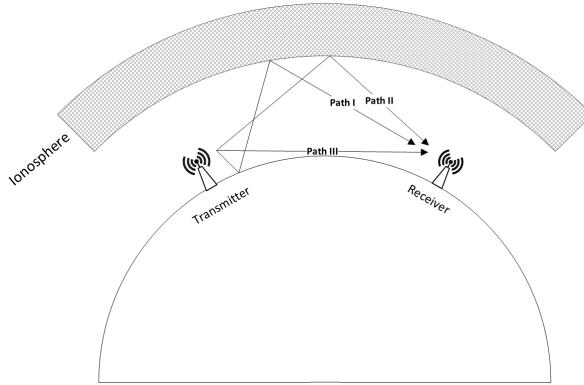


Figure 2.1: Signal Multipath Propagation [3]

The case of *Multipath Interference* gives an illustrative example of how RFI can cause severe problems to radio communication. Take a transmitter located at a longer distance from the receiver. The transmitter sends a signal to the receiver from its antenna. Figure 2.1 shows that the signal will take different paths and deflect to reach the receiver's antenna. This phenomenon is called multipath propagation. The receiver will receive the same signal

multiple times, attenuated in amplitude and shifted in phase. When meeting at the receiver, the electromagnetic waves from the different signal paths will cause constructive and destructive interference, as shown in Figure 2.2. As a result of the superposition principle of the electric and magnetic field: When waves propagate through a medium, like air, and collide, their displacement is the sum of the individual displacements. If, by assumption, the signal waves of path I and path II are arriving in phase (a) and shifted by  $180^\circ$  (b), the electrical field strength measured by the receiver could be displayed as shown below.

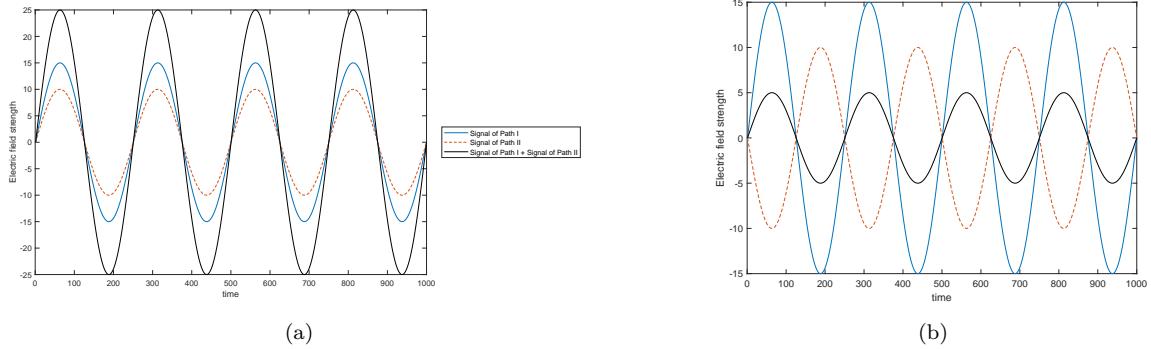


Figure 2.2: (a) Constructive and (b) Destructive Interference Case  
Signal of Path I(blue), Signal of Path II(dotted orange), Superpostion of both Signals(black)

Given, for example, a conventional energy detection receiver decoding the signal, this might lead to demodulation failures or even complete signal loss. The case demonstrates that signals that share the same frequency are particularly vulnerable to interference.

Figure 2.3 shows a simple noncoherent energy detector that demodulates a signal using a squaring device, followed by a finite integrator and a decision threshold comparator. If the evaluated values surpass a specific threshold, the data is demodulated as a digital 1, if not consequently as a digital 0.

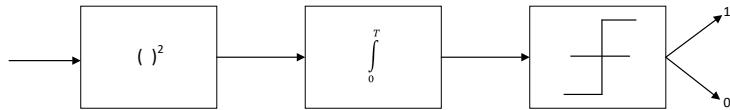


Figure 2.3: Conventional Energy Detector [17]  
Signal of Path I(blue), Signal of Path II(dotted orange), Superpostion of both Signals(back)

## 1.2 Quantifying Interference

Different quantities have been defined to measure how severely a signal is affected by interference. The most relevant ones will be introduced in the following Section:

### Packet-Error-Rate (PER)

A way to measure the impact of EMI on the desired signal is by quantifying the reliability of service and successful receptions. The Packet-Error-Rate (PER) is the number of incorrectly received data packets divided by the total number of received packets. Typically this ratio is scaled over the last 100 received frames. A packet is declared incorrect if at least one part of the frame is erroneous.

$$PER := \frac{Bit_{Error}}{100} \quad (2.1)$$

$Bit_{Error}$  : Number of generated error bits / flags out of the last 100 received frames

### Signal-to-Jammer Ratio (SJR)

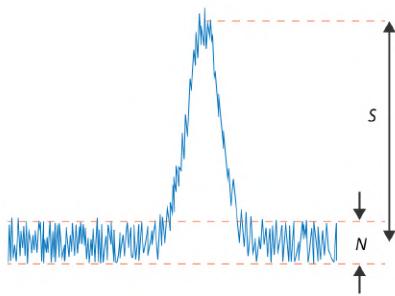
The Signal-to-Jammer Ratio (SJR) is the ratio of the desired signal power to the power of the jamming signal at a given point, like the receiver's antenna terminals. Analogously to the SNR, it is usually also expressed in dB.

$$SJR = \frac{P_{Signal}}{P_{Jammer}} = P_{Signal_{dBm}} - P_{Jammer_{dBm}} \quad (2.2)$$

$P_{Signal}$  : Signal Power in Watts  
 $P_{Jammer}$  : Jammer Power in Watts  
 $P_{Signal_{dBm}}$  : Signal Power in dBm  
 $P_{Jammer_{dBm}}$  : Jammer Power in dBm

### Signal-to-Noise Ratio (SNR)

The Signal-to-Noise Ratio (SNR) measures the proportional reception of the desired signal to the level of background noise. SNR is defined as the quotient of signal power and noise power and is therefore given in dB. A ratio greater than 0 dB indicates that the desired signal is more powerful than the noise.



$$SNR = \frac{P_{Signal}}{P_{Noise}} = P_{Signal_{dBm}} - P_{Noise_{dBm}} \quad (2.3)$$

$P_{Signal}$  : Signal Power in Watts  
 $P_{Noise}$  : Noise Power in Watts  
 $P_{Signal_{dBm}}$  : Signal Power in dBm  
 $P_{Noise_{dBm}}$  : Noise Power in dBm

Figure 2.4: SNR

## 2 Wi-Fi 6 Extended

### 2.1 Introduction

Today, the landscape of innovative technologies is evolving at an incredibly fast pace. It can be hard to keep track. The same holds for Wi-Fi, one of the most commonly used Wireless Personal Network systems globally. Taking a future smart home as an example, it is difficult to list all the appliances that will be connected to the Wi-Fi router: Phone, Laptop, smartwatch, TV, future doorbell, heating system, solar panels, or possibly even other devices such as the coffee machine.

All those connectivity devices are commonly referred to by the more popular name: Internet of Things (IoT). Figure 2.5 shows an estimation of how many devices will be part of the IoT in the years to come.

### Global IoT market forecast (in billion connected IoT devices)

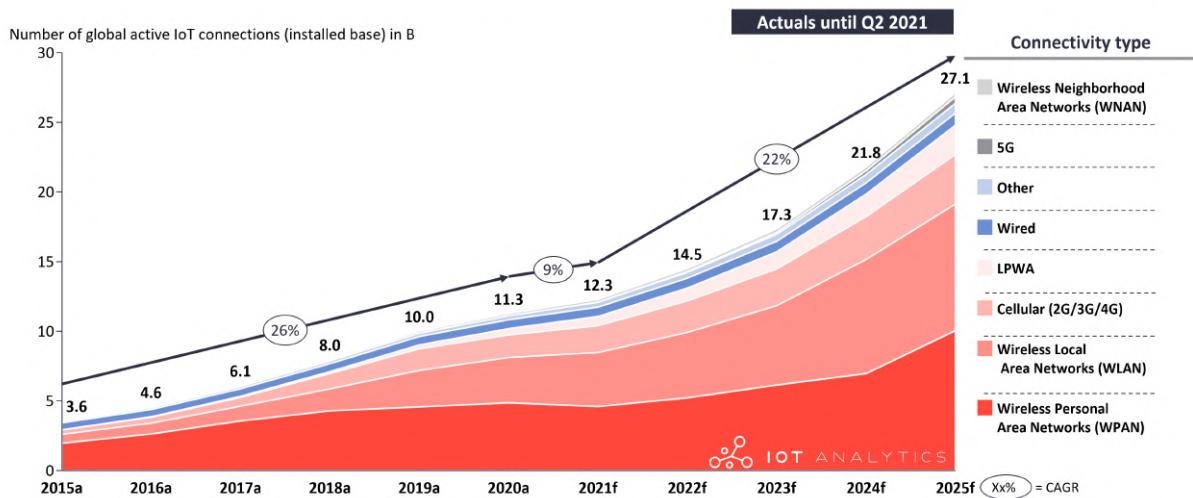


Figure 2.5: IoT Market Development [29]

Undoubtedly, a very efficient connection is needed to make all of these devices work together seamlessly, therefore also, Wi-Fi is constantly evolving. In Figure 2.6 one can observe the release and development of the famous IEEE 802.11 standard from its beginning in 1997. The first release, 802.11 - 1997, was located in the license-free ISM band with data rates up to 2 Mbit/s and Direct Sequence Spread Spectrum and Frequency Hopping Spread Spectrum modulation techniques. In 1999 a new benchmark was set when the 5 GHz spectrum was added, as an additional band to the 2.4 GHz band, with the IEEE 802.11a, allowing for higher data rates up to 54 Mbit/s and also introducing a new, significant demodulation technique: Orthogonal Frequency Division Multiplexing (OFDM) [22].

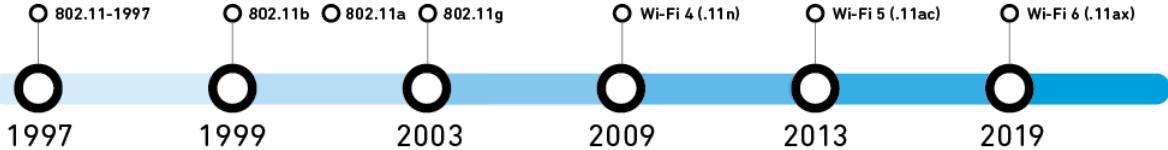
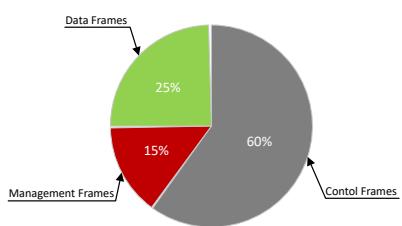


Figure 2.6: Wi-Fi Timeline [22]

In 2009, Wi-Fi 4 (IEEE 802.11n) introduced the Multiple Input - Multiple Output (MIMO) technology, increased transmit power, and started the race for larger channel bandwidths with the first 40 MHz channel next to the conventional 20 MHz. Wi-Fi 4 was followed by Wi-Fi 5, IEEE 802.11ac introducing another 80 MHz channel and a channel-bonding feature [5], till now the latest Wi-Fi 6 IEEE 802.ax in 2019 fully utilizing 160 MHz channels and implementing a significant transformation in protocols to make the Network much more efficient with data rates up to 9.6 Gbps outperforming the previous Wi-Fi 5 by 300 % [21].

## 2.2 Wi-Fi 6 (E) - IEEE 802.11ax



Heavy demand for data traffic arises from an exponentially increasing number of clients joining the Wi-Fi network. Contributing to the issue of Wi-Fi traffic jams is the apparent inefficiency of the protocol. As Figure 2.7 displays, **60 %** of all Wi-Fi frames sent are control frames. Add another 15 % of management frames and only a quarter of all Wi-Fi frames sent are actual data. This is the primary issue that Wi-Fi 6 (IEEE 802.11ax) is tackling - more throughput and more efficient use of the available bandwidth. The standard brings two significant advancements, which will be discussed below.

Figure 2.7: Dist. Wi-Fi Frame Types [5]

### 2.2.1 Orthogonal Frequency Division Multiple Access

Arguably the most essential feature of Wi-Fi 6, Orthogonal Frequency Division Multiple Access (OFDMA), is one of the key advancements within the new IEEE 802.11ax. OFDMA is coming from the previously discussed OFDM. OFDM uses low-symbol rate modulation schemes to modulate a portion of its original high data stream and spread each portion onto a subset of carrier frequencies originating from an orthogonal inner product space. This means that for any two carrier frequencies, the following will hold:

$$\langle f(\omega_1 \cdot t + \phi_1), g(\omega_2 \cdot t + \phi_2) \rangle = \int_{-\infty}^{\infty} f(\omega_1 \cdot t + \phi_1) g(\omega_2 \cdot t + \phi_2) dt = 0 \quad (2.4)$$

$f, g$  : Trigonometric functions

$\omega_1, \omega_2$  : Frequencies

$\phi_1, \phi_2$  : Respective phaseshift

OFDM has the great advantage that it is more resilient toward constructive and destructive interference from multipath propagation and narrowband jammers. Yet, it can utilize a very narrowband width more efficiently, resulting in a very dense possible frequency usage as Figure 2.8 shows.

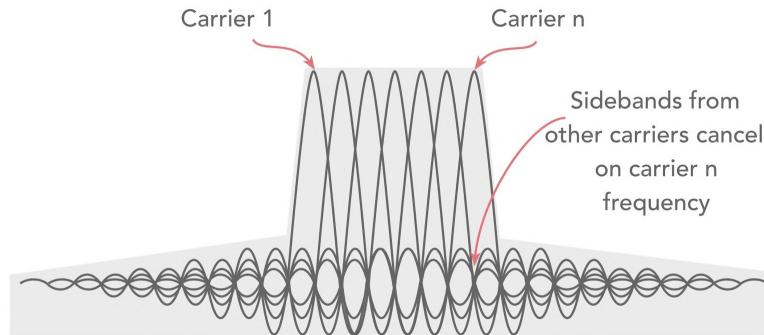
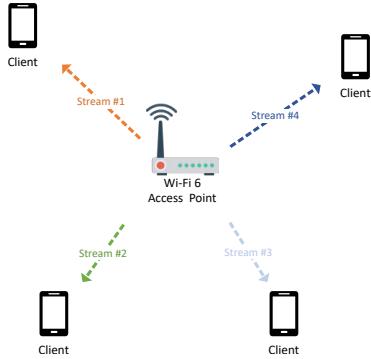


Figure 2.8: OFDM - Visualisation of In-band Carrier Allocation [20]

While OFDM offered a variety of  $n_{OFDM} = 64$  subcarriers with a width of 312.5 kHz within one 20MHz channel, OFDMA increased the number to  $n_{OFDMA} = 256$ , just as narrow as 78.125 kHz each. The subcarriers will be grouped into so-called resource units (RU's), which can be associated with one client and used for up- & download links, making the channel use much more effective than previous Wi-Fi generations. A single 160 MHz channel can now theoretically host a total of 74 clients. However, in a real-world scenario, it's more likely to hold up to four clients to maintain high data rates. In conclusion, with Wi-Fi 6, there is a lot higher flow on single channels but less congestion.

### 2.2.2 Multi User - Multiple Input Multiple Output



Multi-User Multiple-Input Multiple-Output (MU-MIMO) has already been introduced in Wi-Fi 5. However, the technology was not as refined, and there were not as many clients supporting it at the time. In comparison to OFDMA, MU-MIMO does not nest multiple clients within the subcarriers of one channel but instead uses the access points with different antennas and radios of a Wi-Fi Access Point. The objective is to transmit multiple data streams simultaneously and occupy less airtime using a single transmission opportunity. With Wi-Fi 6, MU-MIMO supports up to 8 clients simultaneously. However, one disadvantage is that MU-MIMO requires a certain spatial distribution of the clients to avoid co-channel interference. Consequently, the air space around a Wi-Fi 6 access point will be densely populated with co-current streams.

Figure 2.9: Wi-Fi - Spatial Distribution

### 2.2.3 Channel Allocation of the Wi-Fi 6 Extension

In 2021 the FCC, was the first to legalize the long-planned extension of the spectral bandwidth used for Wi-Fi, followed by the ETSI and other administrative bodies around the globe. Depending on the regional legislation, the new standard with the name Wi-Fi 6E enlarged the available channel bandwidth by up to 360%, as Figure 3.3 displays.

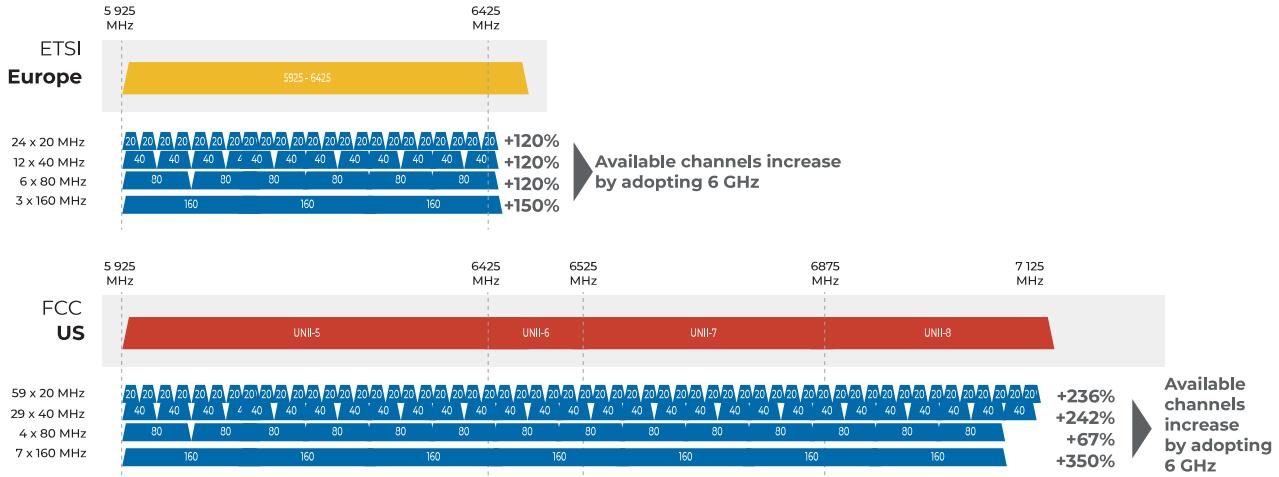


Figure 2.10: Wi-Fi 6E - Channel Map [22]

The channel allocation map also makes it very obvious to identify which 20 MHz channels merge to build 40 MHz channels and so on. Figure 3.3 in Chapter 3 shows in detail the specific channel numbers as aligned with the IEEE 802.11ax. Each channel width has a limited TX Power (effective radiated power) for indoor access points [4].

- 20 MHz : 18 dBm
- 40 MHz : 21 dBm
- 80 MHz : 24 dBm
- 160 MHz : 27 dBm

### 3 Ultra-Wideband

Ultra-Wideband is, in fact, a new name for a long-existing technology. It was firstly used by no other than Guglielmo Marconi, previously mentioned in Chapter 1, Section 1, to transmit morse code over the Atlantic ocean using his famous spark gap transmitter.[17] This is also where UWB gained its original name, "pulse radio."

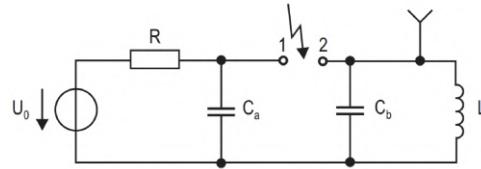


Figure 2.11: Schematic of Macconi's Spark Gap Transmitter [19]

Ultra-Wideband is one of the fast-growing wireless communication technologies of the early 21st century, originating from today's more and more crowded radio frequency (RF) spectrum. While licensing fees for the commercial use of spectral bandwidth are increasing, UWB promises a cost-effective, robust solution.[17] UWB communications differ distinctly from other technologies as here, contradicting classic narrowband signals, a very short pulse is deployed, resulting in an extensive bandwidth. Mathematically, this relates to the time scaling property of the Fourier Transformation, as Equation 2.5 displays.

$$x(at) \circ - \bullet \frac{1}{|x|} \cdot X\left(\frac{f}{a}\right) \quad (2.5)$$

As one can observe in Figure 2.12 below. Thus, given an narrow pulse of roughly two nanoseconds will result in a bandwidth of  $B = 500 MHz$ .

Figure 2.12 shows the IEEE pulse as it is standardized in the Std 802.15.4-2015[1]. The green frame shows the IEEE pulse mask setting the bandwidth requirements.

$$B = \frac{1}{T} = \frac{1}{2 \cdot 10^{-9}} = 500 MHz \quad (2.6)$$

In the traditional sense a signal is defined to be UWB when its fractional bandwidth holds[15] :  $B_f \geq 20\%$

$$B_f = \frac{B}{f_{mid}} \quad (2.7)$$

with  $f_{mid}$  being the center or carrier frequency. However, the definition was later changed to include all signals fulfilling  $B \geq 500 MHz$  to also classify signals at higher carrier frequencies as UWB.[24]

Figure 2.12: IEEE UWB Reference Pulse in Time and Frequency Domain [28]

These distinct properties motivate the use of UWB for the accurate Time-of-Arrival (TOA) measurements, which can then be used for precise distance calculations and localization (ranging). Intuitively, when comparing a narrowband signal to a UWB signal crossing a detection threshold, one can see the advantage of using a UWB pulse.

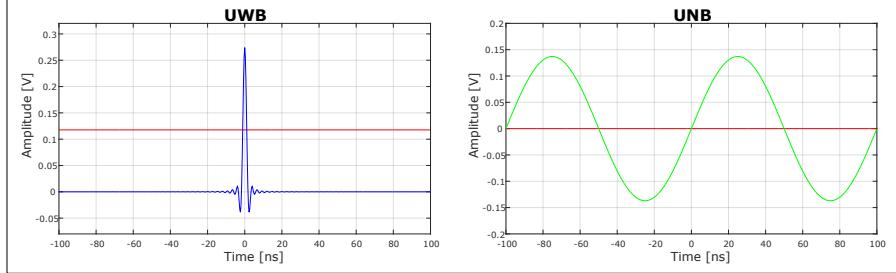


Figure 2.13: Comparison of UNB to UWB [28]

As one can observe, the point of intersection with the threshold line of the UWB line can be easily distinguished while the Ultra-Narrowband (UNB) signal crosses the threshold multiple times. It might even be possible for the system to detect an earlier or later TOA due to some Additive White Gaussian Noise (AWGN) interference. In Figure 2.14 the two signals are displayed with AWGN. Evidently, the UWB signal sustains its essential characteristics.

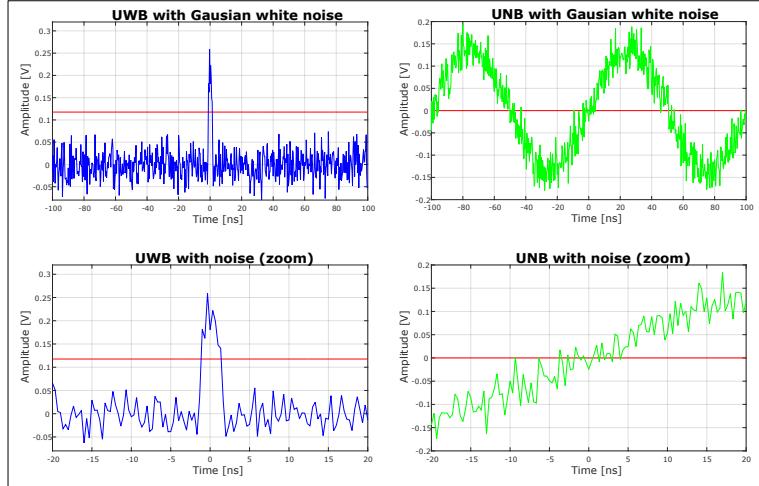


Figure 2.14: Comparison of UNB to UWB with AWGN[28]

### 3.1 Advantages of Ultra-Wideband

As previously discussed, the usage of UWB technology bears several advantages compared to traditional narrowband systems. In the following section, the most significant ones, especially concerning this thesis, shall be discussed.

#### Sharing the Frequency Spectrum with other Users

Through the European Telecommunications Standards Institute and the IEEE 802.15.4 [1] the usage of UWB is restricted to the spectrum between 3.1 GHz to 10.6 GHz with Transmit Power of  $-41,3 \frac{dBm}{MHz}$  measured over 1 ms. Additionally, the spectral bandwidth is divided into 16 channels, which are listed in 2.1, The significant advantage of this legislation is that UWB transmits below the noise level and can avoid costly spectrum licensing fees since it can generally coexist harmlessly with other technologies.

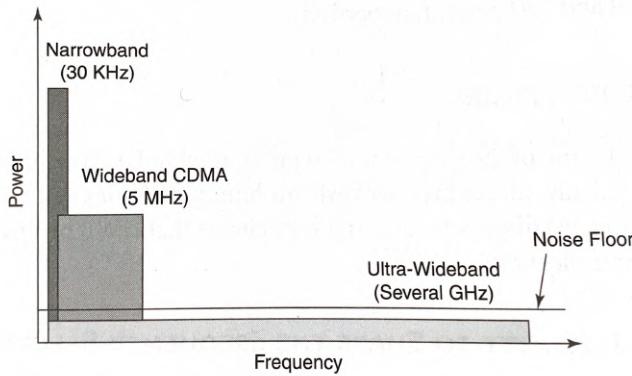


Figure 2.15: Comparison of UWB with other Narrowband and Wideband technologies [17]

In conclusion, it should be stated that although UWB devices transmit below the noise flow, different investigations have proven the impact on radio systems within a large-scale deployment of UWB devices [13].

#### Large Channel Capacity

Due to the increased bandwidth, UWB pulses offer greater channel capacity and higher data transmission rates. Following Harley-Shannon's capacity formula [17] one can identify a linear relationship between bandwidth and channel capacity.

$$C = B * \log_2(1 + SNR) \quad (2.8)$$

$C$  : Maximum Channel Capacity

$B$  : Spectral Bandwidth

$SNR$  : Signal-to-Noise Ratio

Limited by the transceive power mentioned above, the higher data rates are only available at shorter distances making UWB perfect for closer personal networks within 10 meters (e.g., ranging applications).

## High Resistance to Jamming

Having a large bandwidth available contributes a fair share to the resilience against unwanted interference from jammers. As the spectral density is distributed over such a wide variety of frequencies, interference with a narrowband jammer hypothetically will most likely not cause high degradation of service since a significant part of the spectrum is not affected. A measure of this resilience is the Processing Gain PG:

$$PG = \frac{RF\ Bandwidth}{Information\ Bandwidth} \quad (2.9)$$

The processing gain is the ratio between bandwidth of the spread signal and the required bandwidth for the data transmission. However, even a high PG does not guarantee a superior performance of UWB in the presence of a narrowband jammer as [11] has shown, and as the experimental part of this thesis will confirm.

## 3.2 IEEE Reference Pulse, Channels, Encoding and Frameformat

### 3.2.1 IEEE Reference Pulse

The IEEE Standard specifies the UWB reference pulse as follows:

$$r(t) = \frac{2}{\pi\sqrt{T_p}} \cdot \frac{\cos(\frac{3\pi t}{2T_p}) + \frac{T_p}{2t} \sin(\frac{\pi}{2T_p}t)}{1 - (2\frac{t}{T_p})^2} \quad (2.10)$$

$r(t)$  : UWB - Reference Pulse

$T_p$  : Pulse duration

$t$  : Time

The pulse duration is dependent on the chosen channel. As discussed before in regards to equation 2.5, the shorter the pulse, the more bandwidth it will allocate on the electromagnetic spectrum. The pulse shape of the IEEE reference pulse, seen in Figure 2.12, is specifically created to result in a spectral waveform that is constant over a large range of desired frequencies and has a steep decline at the borders. This design was specifically chosen to avoid peaks in the spectrum, which could disturb other narrowband signals. If the UWB pulse is deployed in such a way, UWB communication is not much more than average noise for other conventional systems allocated in the same spectral region. This relies on the UWB transceive power staying below the limit mentioned above.

Creating precisely this reference pulse is highly dependent on the hardware setup and, therefore, not always possible. As an alternative, the IEEE allows deviations as long as they fullfil certain requirements listed in [1].

### 3.2.2 Pulse Modulation techniques and IEEE Channels

In order to move the generated UWB pulse into the desired channel center frequency, it is multiplied by a carrier frequency between 499.2 MHz to 9484.8 MHz. Figure 2.16 displays a simplified diagram consisting of a pulse generator and a local oscillator.

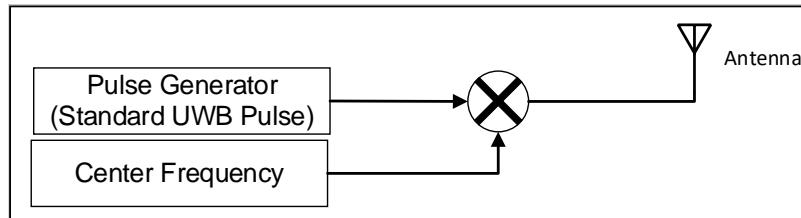


Figure 2.16: UWB Transmitter - Local Oscilator for the Carrier Frequency & Pulse Generator [25]

Figure 2.17 below shows the pulse previously displayed in Figure 2.1 multiplied with a carrier frequency of 4492.8 MHz (Channel 3 of table 2.1).

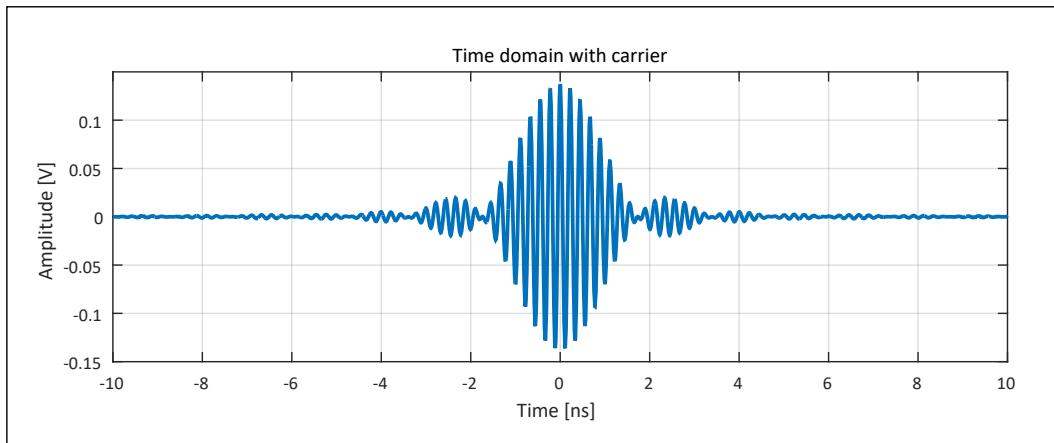


Figure 2.17: IEEE Reference Pulse multiplied with Carrier Frequency at 4492.8 MHz [25]

Table 2.1 displays the different IEEE channels with their respective bandwidth limitations and center frequencies.

Channel number	Pulse duration Tp [ns]	Center frequency [MHz]	Bandwidth [MHz]
0	2.0	499.2	499.2
1	2.0	3494.4	499.2
2	2.0	3993.6	499.2
3	2.0	4492.8	499.2
4	0.75	3993.6	1331.2
5	2.0	6489.6	499.2
6	2.0	6988.8	499.2
7	0.92	6489.6	1081.6
8	2.0	7488.0	499.2
9	2.0	7987.2	499.2
10	2.0	8486.4	499.2
11	0.75	7987.2	1331.2
12	2.0	8985.6	499.2
13	2.0	9484.8	499.2
14	2.0	9984.0	499.2
15	0.74	9484.8	1354.97

Table 2.1: IEEE Channels

In commercial UWB technologies, multiple modulations schemes are used. Systems use an On-Off Keying, Pulse-Amplitude Modulation, Pulse-Position modulation or a combination of the latter, which are later to be explained in more detail in Section 3.3. For the TOA detection a pulse modulation scheme ending the ternary alphabet  $\{ 1, 0, -1 \}$  is being used. Ternary pulses are build upon three states. The "normal" high state (+1) as depicted in Figure 2.12, a 180° phase-shifted pulse encoded as (-1) and the no-energy state encoded as (0). As it will be discussed later in Section 3.2.3, ternary pulses are only used for the Preamble and the Start-of-Frame delimiter of a UWB frame, while all other fields are decoded with a combination of Burst Position Modulation (BPM) and Binary Phase-Shift Keying (BPSK).

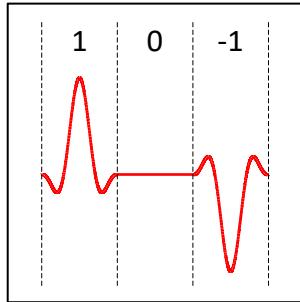


Figure 2.18: UWB Ternary Pulse [25]

### 3.2.3 UWB IEEE Frameformat

Ultra-Wideband message frames following the IEEE standard must consist of four different sections.

1. SYNC-Field holding the so-called preamble
2. Start-of-Frame Delimiter (SFD) signaling the beginning of the actual message
3. Physical Layer Architecture Header (PHR)
4. PHY Service Data Unit (PSDU)

Figure 2.19 shows the schematic composition of a standard UWB. The SYNC-Field and the SFD are encoded with the previously introduced ternary pulses. The SYNC-Field is holding the Preamble used to synchronise the receiver to encode the following PHR & PSDU sequence. The PHY header holds information about the subsequent PSDU, like the data length and rate. The PSDU then contains the actual data, which in general, for the ranging case, are the timestamps of the performed ranging interval (see Section 3.6). PHR and PSDU, differently from the SYNC Field, are encoded with a combination of BPM and BPSK. This will be discussed in detail in Section 3.3.



Figure 2.19: IEEE UWB Standard Frame [1]

**3.2.3.1 Preamble** Due to the low transmission power of UWB pulses, the reception of UWB frames becomes somewhat difficult compared to conventional narrowband systems. For a successful reception of a UWB frame, the receiver needs to synchronise itself with the transmitter. It does so by decoding the Preamble. After effective decoding, it will know if and when to expect the subsequent frames from the protocol. The question of "if" & "when" will play an essential role in observing the interference and error rates caused by Wi-Fi 6E frames in later chapters.

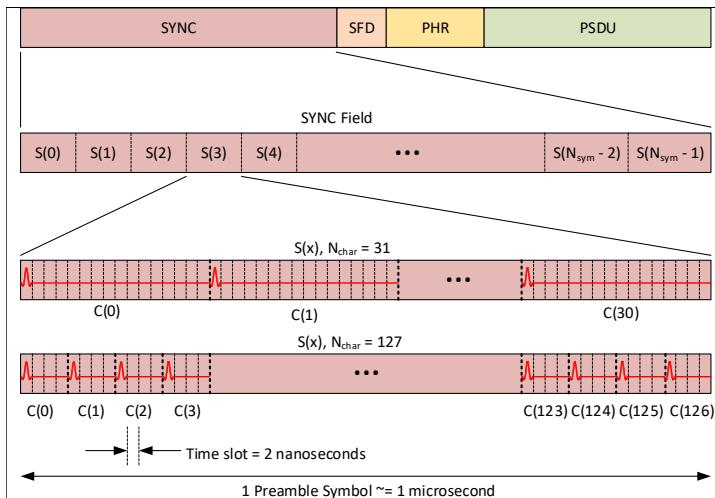


Figure 2.20: UWB Frame SYNC Field [1]

The SYNC field consists of  $N_{sync}$  repetitions of the Preamble-Symbols (S), where each Preamble-Symbol, depending on its configuration, holds 31 or 127 characters (Z) of the previously discussed ternary Code-sequence. The IEEE defines 24 different code sequences. Eight of such sequences have a length of 31 characters and the other 16 sequences a length of 127 characters, respectively. Every symbol has either value (+1), (0) or (-1), just as shown in Figure 2.21. Every character by itself is divided again into four (or 16) time slots  $\delta_L$  of which the first one indicates the value of the respective symbol and the following ones are all holding zero. Below in Figure 2.21 is an example of such a sequence of symbols. In this case, the sequences represent the IEEE code with index 12. Figure 2.20 displays the entire composition of a preamble successively.

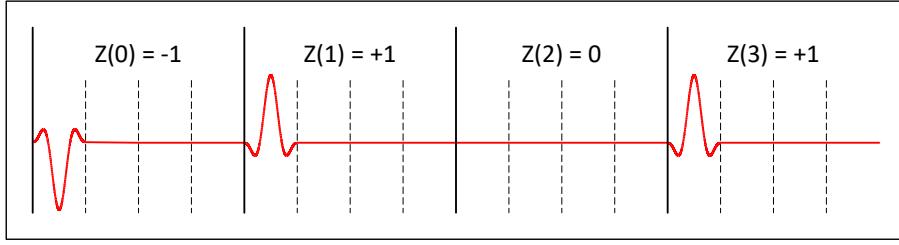


Figure 2.21: First four UWB Ternary Pulse of Symbol of Code index 12 : -+0++000000-0+0-+0-+-+00-+0++0+0+0+000-0 0-00-+00+-+000-+0-++0-0-++0-0-00-0+00+0+ 00+-00+000+-000-0-+0000-0000-0+0000+ [1]

Note that the carrier frequency has been neglected to keep the picture more comprehensible. The code sequences are defined so that they obtain a very high autocorrelation and a minimal correlation to other code sequences. This serves the purpose of making every preamble sequence unique and hard to misinterpret for another one. Every code sequence with 31-characters has  $\delta_L = 4$  allocated time slots per character while every Code sequence of 127 characters has  $\delta_L = 16$  allocated time slots. While every timeslot  $\delta_L$  has a length of 2 ns, this leads to an approximate length of 1  $\mu$ s of an entire preamble symbol.

Code index	Ternary code sequence	Channel number
1	-0000+0-0++0+-000-+-+-+00-+0-00	0, 1, 8, 12
2	0+0-0+0+000-++0-+-00+00++000	0, 1, 8, 12
3	-+0++000-+-+00++0+00-0000-0+	2, 5, 9, 13
4	0000+-00-00-+++-0+-+000+0-0++-	2, 5, 9, 13
5	-0+-00+++-+000-+0++0-0+0000-00	3, 6, 10, 14
6	++00+00-+-0++-000+0+0-0+0+0000	3, 6, 10, 14
7	+0000-+0+0+00+000+0++-0-00-+	4, 7, 11, 15
8	0+00-0-0++0000-+00-+0++-+0+00	4, 7, 11, 15

Table 2.2: IEEE 31 Characters Preamble Symbols [1]

Further, to avoid synchronization problems when maintaining a zero-state for excessively long periods, every sequence of 31 characters always holds 16 from 0 different characters and 127 character long sequences 64 respectively. Consequently, this leads to the so-called Pulse Repetition Frequency (PRF) of 16 MHz (PFR16) for 31-Character Sequences and 64MHz (PRF64) for 127 Character sequences.

This can also be observed in Table 2.2. Consequently, the autorotation will always hold the value of all non-zero symbols meaning 16 or 64, respectively.

**3.2.3.2 Start-of-Frame Delimiter** The Start-of-Frame delimiter is built exactly as the preamble from a ternary sequence. However, the code sequence differs from the previously defined IEEE sequences. This way, after synchronization, the receiver can identify the incoming start of the PHY header. This point in time will also later be used for the Time-of-Flight (TOF) calculations. Furthermore, the SFD will play an essential role in the error analysis combined with Wi-Fi 6E interference.

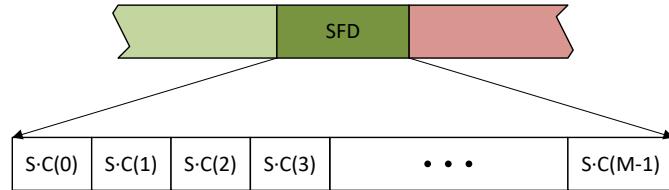


Figure 2.22: UWB SYNC Field [1]

To create a break in the preamble symbol pattern, the SFD code is spread by the preamble symbol, which is also used in the SYNC-Field. The used SFD code depends on the used data rate in the PSDU. A coded sequence example could look as depicted below.

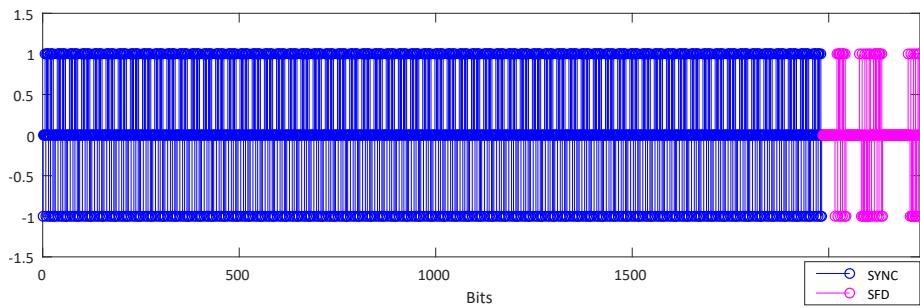


Figure 2.23: UWB Preamble & SFD

**3.2.3.3 Secure Time Stamp Field** As Table 2.2 shows, the number of used preamble symbols is limited. Therefore, it would be easy to fake a preamble using, for example, cicada attacks, which is done by the attacker sending out random preambles suggesting a shorter first path to the UWB receiver. This method has been explored before to gain access to a UWB PKE-System. The STS is inserted into the UWB frame to enable a tamper-proof distance measurement. The STS works like the SYNC, with the difference being that the STS does not repeat itself. However, it would not be possible to replace the preamble with the STS because the receiver needs to be synchronised to decode the STS.

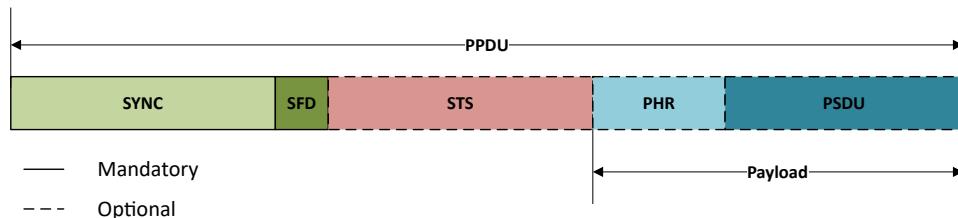


Figure 2.24: UWB UWB-Frame-StandardNoStandard

The STS uses an AES128 encryption combined with a security key, which is flashed on the transmitter and receiver for the STS generation and decoding. This way, only intended parties can receive UWB frames and validate the arrival of a secured frame to start or stop the stopwatches for Time-of-Flight calculations.

**3.2.3.4 Payload** The payload is the frame structure that holds the information to be transmitted. It consists of the PHR and the PSDU fields.

The PHR is encoded with SECDED Encoder, and the PSDU is encoded with Reed Solomon Encoder. Afterward, both are encoded with a convolutional encoder, as shown in the following Figure 2.25:

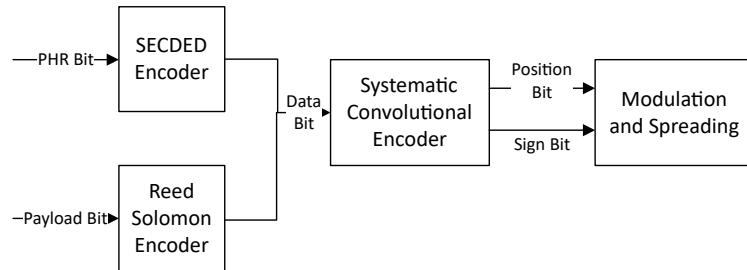


Figure 2.25: UWB Payload Modulation [25]

**Physical Layer Header field** The PHR field contains information about the frame. It holds the frame length and data rate of the PSDU and the SECDED (Single Error Correct, Double Error Detect) block of the PHR.

**Physical Layer Payload field** The PSDU field consists of the actual transmitted data. It is encoded the following way

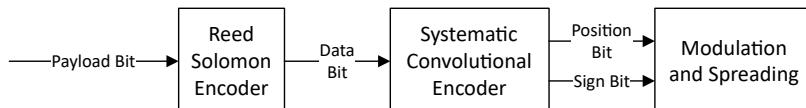


Figure 2.26: UWB PSDU Encoding [25]

Reed-Solomon (RS) codes are error-correcting codes. They are used for fixing data loss during transmission. Therefore, all Payload bits get encoded with the Reed-Solomon code. However, if the error correction fails, the receiver will give back a *Reed-Solomon decode error*.

### 3.3 Modulation Techniques

Before the used combinational technique of BPM-BPSK is discussed, a brief introduction to the fundamentals of this modulation technique shall be given.

#### On-Off Keying

Used as one of the most straightforward modulation techniques, On-Off Keying (OOK) offers a binary transmission where a pulse sent represents a 1 and the absence of a pulse a bit 0.

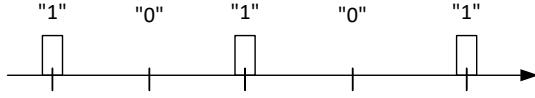


Figure 2.27: On-Off Keying Modulation [17]

$$s(t) = \sum_{m=1}^M b_m \cdot P(t - T) \quad (2.11)$$

$M$  : Maximum Number of transmitted Bits  
 $P(t)$  : UWB Pulse  
 $b_m \in \{0, 1\}$  :  $m$ 'th data bit  
 $T$  : Pulse Repetition Period

In this sense, OOK is a particular case of Pulse Amplitude modulation. This technique has some apparent advantages for its simplicity and low implementation cost. However, it is very susceptible to noise and interference and therefore not recommended for UWB systems, especially not with multiple-access requirements. Furthermore, synchronization problems are introduced when, e.g., a bitstream of all zeros is sent.

#### Pulse-Position Modulation

Pulse-Position Modulation (PPM) is based on pseudorandomly encoded positions of UWB signals. At a known reference point in time, a pulse is either encoded as 1 or, in case of no-energy detection, as a 0.

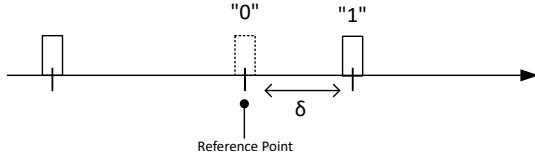


Figure 2.28: Pulse-Position Modulation [17]

$$s(t) = \sum_{m=1}^M b_m \cdot P(t - mT - b_m\delta) \quad (2.12)$$

$M$  : Maximum Number of transmitted Bits  
 $P(t)$  : UWB Pulse  
 $b_m \in \{0, 1\}$  :  $m$ 'th data bit  
 $T$  : Pulse Repetition Period  
 $\delta$  : TimeShift

Consequently, PPM is more resilient against channel noise and false detection due to the tight synchronisation pattern. However, it is very vulnerable to packet collision, e.g., through multiple-access channels. Another disadvantage comes from the previously mentioned synchronization requirement. Slight jitters and deviation in clocking accuracy, given by the Center Frequency Offset (CFO) may lead to severe decoding errors, especially when facing multipath distortion and multiple channel access.

## Biphase Modulation

Biphase modulation uses a pulse of opposite polarity, as already introduced in Section 3.2.2 for the ternary signal. However, in a Biphase Modulation, a  $180^\circ$  phase-shifted pulse corresponds to (0), not a (-1).

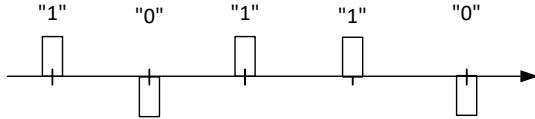


Figure 2.29: Pulse-Position Modulation [17]

$$s(t) = \sum_{m=1}^M b_m \cdot P(t - mT) \quad (2.13)$$

$M$  : Maximum Number of transmitted Bits  
 $P(t)$  : UWB Pulse  
 $b_m \in \{1, -1\}$  :  $m$ 'th data bit  
 $T$  : Pulse Repetition Period

Biphase modulation is less susceptible to interference, noise, and multipath distortion as the difference between the two binary states amplitudes is much greater than compared to PPM and OOK. Another advantage is that bipahse modulated pulses have a zero-mean in spectral power density. This means that they are less likely to cause harmful interference to other narrowband systems. Biphase modulation comes, however, at a higher integration complexity cost and energy consumption.

## Burst Position Modulation and Binary Phase-Shift Keying

In contrast to the Preamble and the SFD, the STS, PHR and PHY Payload fields are encoded using Burst Position Modulation and Binary Phase-Shift Keying (BPM-BPSK), which is a combination of the fundamental modulation techniques discussed above. Here, each symbol holds two bits. The first one is given by the pulse's position, and the second bit is within the phase. As Figure 3.2.3 the time interval is divided into two Sections  $\frac{T_{dynam}}{2} = T_{BPM}$  which are again split into *Possible Burst Position* ( $N_{hop}$ ) and the *Guard interval* which increases resilience against interference caused by others systems. Depending on the position of UWB\_pulses in the first or second interval, the bit encodes a 0 or 1. Depending on the phase, again, a respective 0 or 1.

Reliant on the configuration and desired data rate, a number of 2- 512 UWB pulses will be sent per symbol. The lower the data rate, the more time remains for one symbol, and consequently, the more UWB pulses can be sent within one symbol. An increase of pulses per symbol improves the reliability of the signal and, therefore, the resistance to jamming.

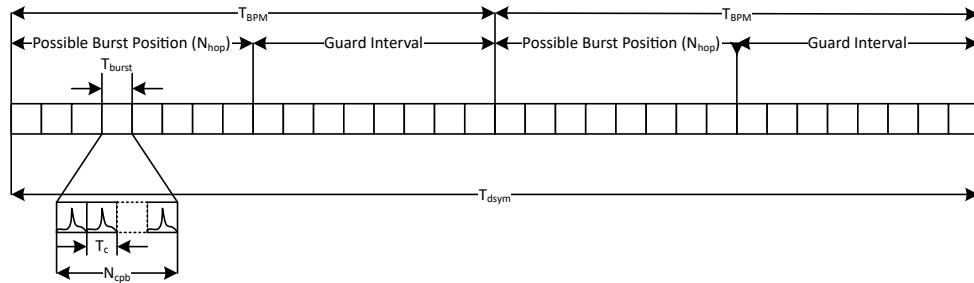


Figure 2.30: Burst Position Modulation and Binary Phase-Shift Keying [1]

### 3.4 Channel Impulse Response

Ultra-wideband pulses are electromagnetic waves that will propagate freely in space. Dependent on the choice of antenna, they will undoubtedly collide with objects, like walls, humans, or anything else in their path. Conditional on the encountering object, the electromagnetic waves will penetrate, deflect, or be absorbed, resulting in attenuation of the signal [23]. The different paths the signal may take can be differentiated into two classes: Line-Of-Sight (LOS) & Non-Line-of-Sight (NLOS). As for a Line-of-Sight scenario, the electromagnetic wave will propagate straight to the receiver from the transmitter, which is an ideal case. However, for the Non-Line-of-Sight scenario, the wave might be reflected by the wall, even multiple times, as shown in Figure 2.31.

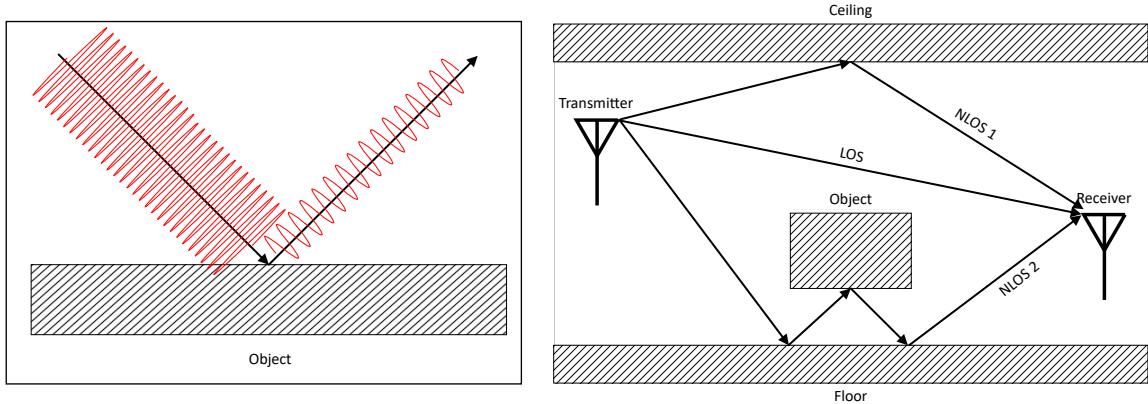


Figure 2.31: UWB Channel Impulse Response [8]

This phenomenon is called multipath propagation and results in the signal arriving at the receiver multiple times. Due to damping as a consequence of propagation through dense materials and reflections, the phase and amplitude of the wave may have been changed significantly. This may result in constructive and destructive interference that might result in a stronger or weaker signal measured at the receiver.[9]

Moreover, the signal propagating on an NLOS path will likely take longer to reach the receiver than a signal traveling on a LOS path. Therefore a graphical representation showing the time difference of arrival would be beneficial.

This is where the Channel Impulse Response (CIR) was introduced. The CIR provided a quantifiable digital representation of the multipath behaviour of a UWB frame. [28]. It is the discretisation of the received signal and its multipath reflections power measured by their time of arrival in a specified window. In Figure 2.32 one can observe different multipath behaviours and their representation with the CIR.

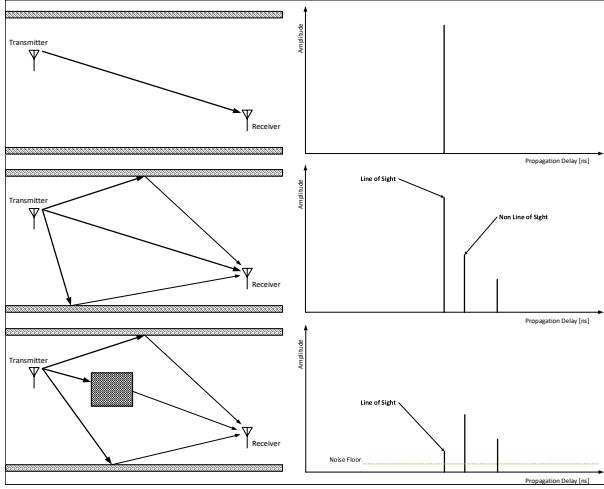


Figure 2.32: UWB CIR at different TOA, inspired by [28]

In Figure 2.32 one can quickly identify the LOS path as the strongest signal in the middle graph, while this changes dramatically when a damping material blocks the direct line of sight.

Below in Figure 2.33 is an example of a Channel Impulse measurement captured with a Ranger 4 evaluationboard, which is populated with the NCJ29D5 NXP's latest UWB IC.

The CIR estimate is plotted in blue, while the maximum power measured has a red circle. In a LOS scenario, the first path should coincide with the strongest path. If, however, the LOS is blocked by an object, the first path will be decreased in power.

In Figure 2.33 the first path is marked with a red vertical line. Additionally, the noise level and the detection threshold power are displayed. The edge index marks the point in time where the first received CIR estimate oversteps the detection threshold. The X-axis displays the time of arrival, which is scaled to the point of arrival of the first path. Consequently, one can see clearly how all weaker reflections arrive in the interval [0, 100] ns.

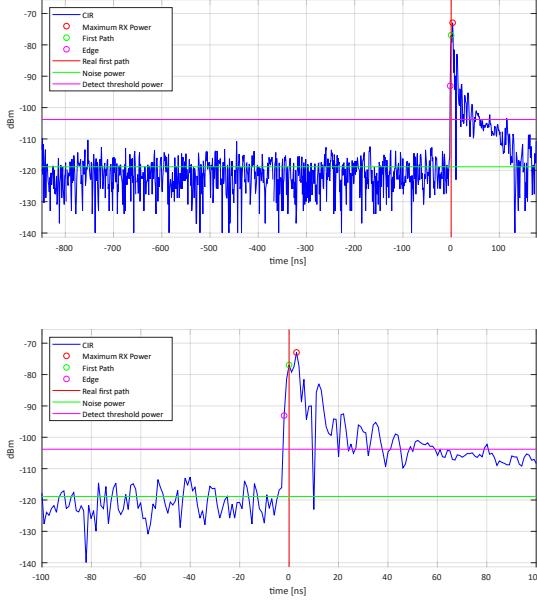


Figure 2.33: Read UWB CIR Estimate

### 3.5 UWB Receiver

A typical UWB receiver comprises four main stages:

1. LNA: Low Noise Amplifier
2. I/Q Mixer + ADC: In-phase Quadrature Mixer and Analog to Digital Converter
3. Preamble Correlator
4. CIR Accumulator: Channel Impulse Response Accumulator

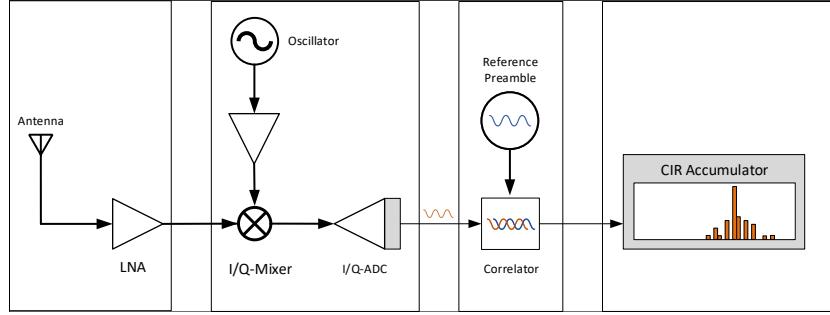


Figure 2.34: UWB Receiver

Figure 2.34 displays the four stages. Firstly the signal is received at the antenna and amplified. Then the carrier frequency is removed to obtain the original UWB pulse (down mixer). In the following, an Analog-Digital Converter (ADC) will transform the received signal into phase and amplitude (real & complex) digital values. Then the received preamble will be correlated with the chosen reference preamble (see Figure 2.35).

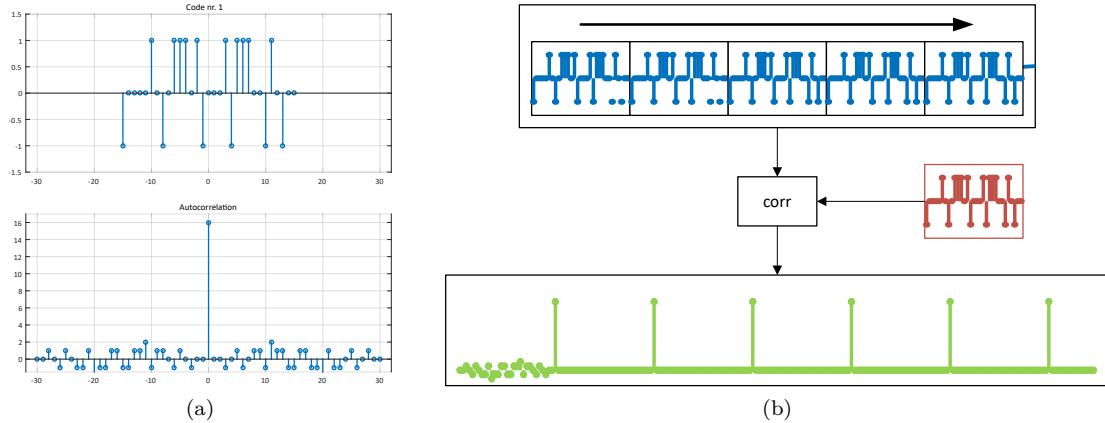


Figure 2.35: (a) Single UWB Autocorrelation (b) Multiple UWB Autocorrelations

This correlation will be displayed in the CIR Accumulator of Stage 4. If no reflection is present, each correlation should result in a single peak that can be mapped to a specific time window. If multipath propagation is present, multiple peaks will be detected as the preamble will be recognised multiple times subsequently. This is observed in

Figure 2.33. The CIR enables the receiver to detect the first path even if it is weaker than another reflection path. However, the strongest path will be used to decode the data following the preamble and the SFD. After the SFD has been detected, the correlation is deactivated, and the data will be encoded directly as described in Section 3.2.3.4

Ideally, after successfully decoding the preamble, the receiver will be completely synchronised with the transceiver. However, there will likely be a slight time drift present between the clocks running on both devices. This is called the Center-Frequency-Offset. If an offset is present, the receiver will decode the pulses in the correlator with a small drift back or forward. The receiver can recognise that shift and compensate it in CIR accordingly. This leads to the *Two-Way Ranging* approach, where this time drift on two devices can be compensated.

Finally, to detect these short UWB pulses with a bandwidth of approximately 500 MHz, the ADC has to work at least twice the frequency (1 GHz) following the Nyquist criterion. This leads to the reception process having a very high energy consumption compared to narrowband convention systems.

## 3.6 Distance Measurements with UWB

### 3.6.1 Signal Propagation Time

The latest approach to precise distance measurements using UWB pulses is through the measurement of the signal propagation time. This becomes relatively straightforward since electromagnetic waves propagate at approximately the speed of light. Hence, the distance between transmitter and receiver can be calculated if the TOF is known with Equation 2.14

$$r = c \cdot t_{flight} \quad (2.14)$$

r : Distance traveled by signal

c : Speed of Light

$t_{flight}$  : Time of Flight

A significant advantage of signal propagation measurements is the higher degree of safety against relay attacks which have been a concurrent threat to PKE-Systems based upon Received-Signal-Strength-Indicator distance measurements [25]. The challenge with the TOF method is to identify the exact time of arrival of the signal while maintaining resilience against multipath propagation and interference.

### 3.6.2 One-Way Ranging

For One-Way Ranging (OWR), also called Time-of-Arrival, the transmitter measures the time  $t_{TX}$  at which it transmits the signal, and the receiver will likewise capture the point in time where it receives the incoming signal  $t_{RX}$ . Later then, the timestamps can be exchanged with data frames depending on the application, and the distance is calculated as follows:

$$r = c \cdot (t_{RX} - t_{TX}) \quad (2.15)$$

r : Distance between transmitter and receiver

c : Speed of Light

$t_{TX}$  : Time Transmission

$t_{RX}$  : Time Reception

A significant difficulty with this approach is the requirement for a perfectly synchronized chronometer. Only a minor deviation in the center frequencies or a shift in the clock generator of any two devices will lead to an incorrect ranging result. Due to manufacturing tolerances and thermal effects, One-Way ranging by itself is not favorable for precise distance calculations.

### 3.6.3 Two-Way Ranging Single Sided

Two-Way Ranging Single Sided (TWR-SS) simply consists of two subsequent one-way rangings and is the profitable option developed from the previously explained problem of one-way ranging. The *Initiator* of the ranging round sends a so-called *Poll-Frame* which marks the start of the protocol and also triggers the stopwatch of the *Initiator* tracking  $T_{Round}$ . The *Responder* on the other side is awaiting the *Poll-Frame* and will, after successful reception, start its own stopwatch to track the time  $T_{Delay}$ , until it will send the *Response-Frame* to the *Initiator*, which terminates the ranging round.

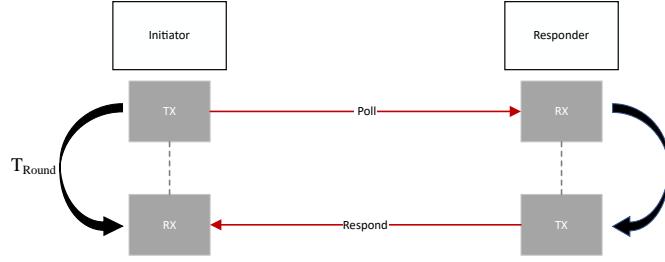


Figure 2.36: Ranging Round : Two-Way Ranging Single Sided

The calculation of the TOF hence, becomes:

$$r = c * (T_{Round} - T_{Delay}) \quad (2.16)$$

$$d = \frac{t_{flight}}{2} \cdot c \quad (2.17)$$

$d$  : Distance between Initiator and Responder

$c$  : Speed of Light

$T_{Round}$  : Time between Transmission of the first and Reception of the last Frame

$T_{Delay}$  : Time between Reception of the Poll-Frame and Transmission of the Response-Frame

$t_{flight}$  : Time of Flight

The significant advantage of TWR-SS to OWR is that a time-difference is calculated, and no absolute timestamps are needed. This eradicates the synchronisation problem of the two clock generators on each device. However, the internal clocks have to work at the exact same frequency. Deviations from the nominal center frequency will lead to an error in the distance calculation, which can be classified as  $E_{freq} = \frac{1}{2} \cdot (e_{Initiator} - e_{Ankor})$  and is measured by the CFO.

### 3.6.4 Two-Way Ranging Double Sided

Two-Way Ranging Double Sided (TWR-DS) can solve the last concern regarding the CFO on both Initiator and Responder. A third, ranging frame, called the *Final-Frame* is introduced, which compensates for the internal clock difference between the two devices automatically.

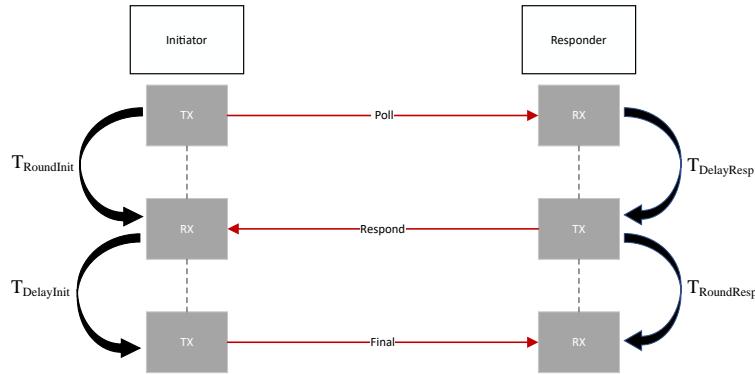


Figure 2.37: Ranging Round : Two-Way Ranging Double Sided

$$t_{flight} = \frac{T_{RoundInit} \cdot T_{RoundResp} - T_{DelayInit} \cdot T_{DelayResp}}{T_{RoundInit} + T_{RoundResp} + T_{DelayInit} + T_{DelayResp}} \quad (2.18)$$

The TOF is then given by:

$T_{RoundInit}$  : Time between Transmission of the Poll-Frame and Reception of the Response-Frame

$T_{DelayInit}$  : Time between Reception of the Poll-Frame and Transmission of the Response-Frame

$T_{DelayResp}$  : Time between Reception of the Poll-Frame and Transmission of the Response-Frame

$T_{RoundResp}$  : Time between Transmission of the Response-Frame and Reception of the Final-Frame

## **Chapter 3**

# **UWB - Wi-Fi 6E Coexistence**

As introduced in Chapter 1, Section 1.1 Wi-Fi 6E is a real threat to Ultra-Wideband communication systems operating in the same frequency spectrum. This Chapter discusses the development, measurement, and evaluation of a test set-up to reproduce this interference case reliably and find possible coexistence solutions. To simulate an automotive environment, commercially available hardware is used that is already deployed on the market.

# 1 Design of Experiment

Electromagnetic field measurements are highly susceptible to any disturbance. Therefore results can vary dramatically from measurement to measurement if precautions are not taken to hold all conceivable settings and factors at a predefined stake. It was essential to find the best possible set-up having just the right amount of components and influencing variables such that significant conclusions could be drawn from the results of the experiments.

## 1.1 Hardware

As mentioned, the set-up is intended to simulate a Wi-Fi 6E threat to UWB in an automotive environment given a possible worst-case user scenario. Thus all UWB & Wi-Fi 6E hardware components have been chosen as used in the industry.

### 1.1.1 Ultra-Wideband Device - Ranger 4 (NCJ29D5)

The NCJ29D5 is an ARM Cortex-M based UWB IC manufactured by NXP and the first of a new generation of Ultra-Wideband ICs explicitly designed to meet the connectivity and safety needs of the global automotive industry [27]. It operates in the high band between 6.0 GHz to 8.5 GHz and follows the IEEE 802.15.4 compatibility standard. As for this set-up, it simulates the UWB automotive passive-keyless-entry system.



Figure 3.1: NCJ29D5 - Ranger 4 Evaluationboard [27]

The center of interest in this investigation will be UWB IEEE Channel 5 (See Chapter 2, Section 3.2.2) with a center frequency of **6.489 GHz**

### 1.1.2 Wi-Fi 6E Access Point - Netgear Raxe 500 Tri-band Router

The Netgear RAXE 500 Wi-Fi 6E Tri-band Router is one of the latest, most advanced connectivity devices currently on the market. As the name "Tri-band" implies, it does feature the 2.4 and 5 GHz Wi-Fi Spectrum next to the desired 6 GHz range. Given  $445mW$  ( $26.5dBm$ ) Maximum Transmit Output Power in the 6 GHz band with up to 100 % duty cycles [6] it offers a very favorable option as the Wi-Fi - UWB Jammer in this set-up.

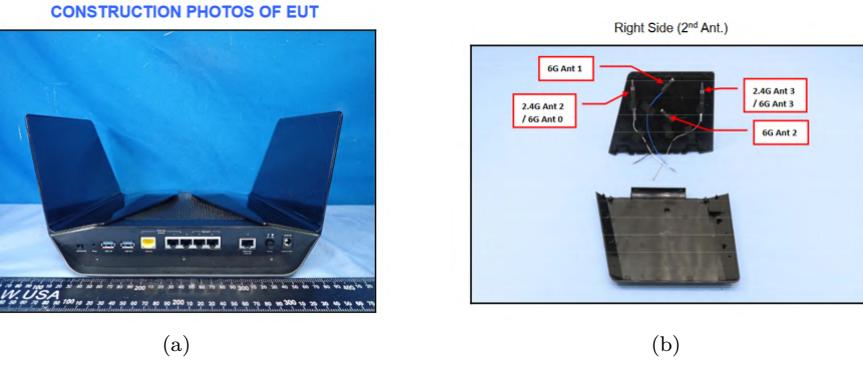


Figure 3.2: Nighthawk - Netgear Raxxe500 [6]

The Netgear Raxxe 500 features the entire channel range allocated in the IEEE 802.11ax. In the context of a UWB - Wi-Fi threat, this results in an in-band channel overlap of UWB Channel 5 with center frequency band **6.489 GHz** spanning over 500 MHz bandwidth [ 6239 MHz, 6739 MHz ] and, for example, Wi-Fi 6E Channel 109 with center frequency **6.495 GHz** starting at 20 MHz bandwidth and going up to Channel 111 with center frequency **6.505 GHz** spanning over 160 MHz bandwidth. It has been shown by [26] that the most critical in-band interference of Wi-Fi 6E and UWB is caused close to the respective center frequencies.

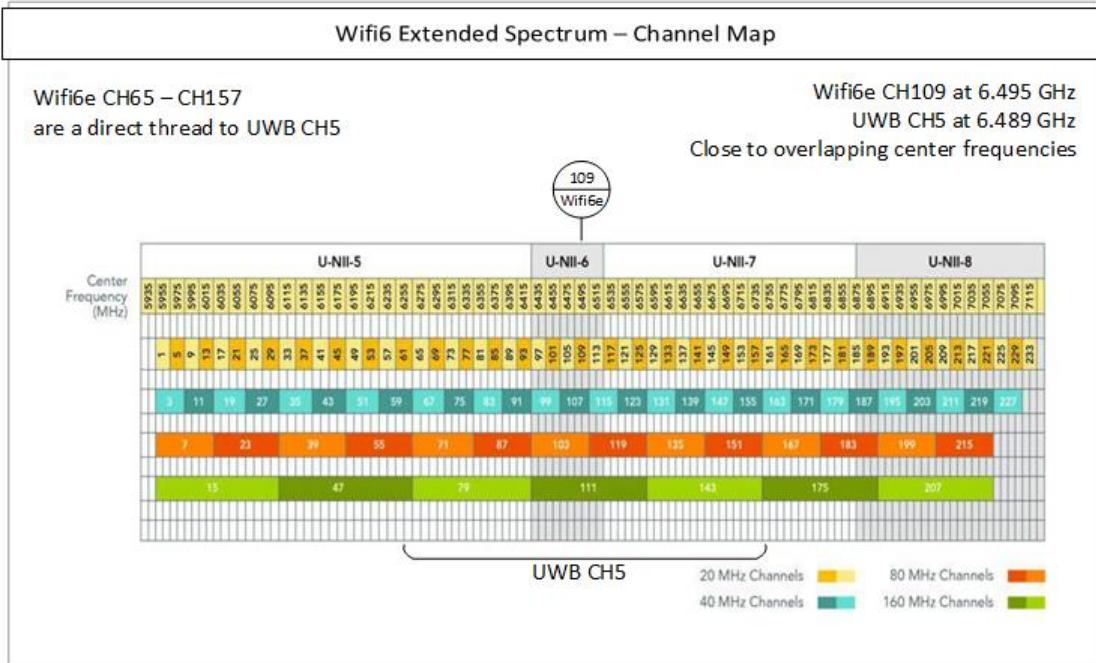


Figure 3.3: Wi-Fi 6E Channel Allocation [22]

### 1.1.3 Wi-Fi 6E Client - Laptop Hardware Update with Intel AX210

In order to access the 6 GHz bandwidth, there is currently only one network card commercially available on the market as yet. As the standard is still very new, there are very few devices on available so far that are Wi-Fi 6E compatible. The only mobile device able to use the 6 GHz spectrum as a Wireless Local Area Network (WLAN) is the SAMSUNG Galaxy S21 5G which offers little to no control over data flow and data rates on the Wi-Fi 6E network.

Hence, there is no ready-to-use hardware commercially attainable that supports this standard and can be used with the desired functionalities in this test set-up. The Intel AX210 Network Card offers a proper solution enabling a PC or Laptop to access the 6 GHz band and, therefore, a tool for more precise testing.

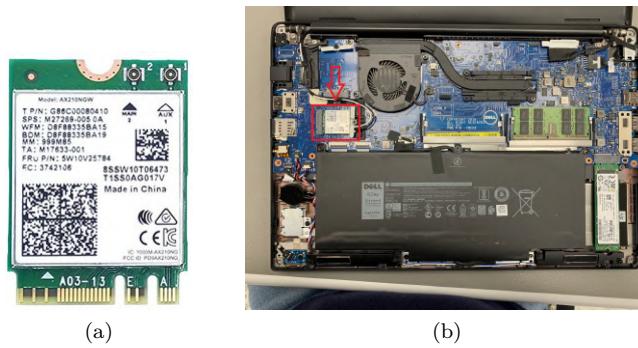


Figure 3.4: Wi-Fi 6E Network Card and Installment Process [6]

## 1.2 Positioning of Hardware Components

The rudimentary idea of the positioning has been to make the impact of Wi-Fi 6E on UWB ranging as severe as possible. A consequence of this starting point was to arrange all hardware components so that the TX power of Wi-Fi 6E is at a maximum. In conclusion, one would expect that the probability and severity of a UWB - Wi-Fi 6E packet collision should be the highest.

Following this concept, first investigations into the antenna beam of all hardware components involved have been conducted, and consequently, the information used to deduct the best spatial arrangement.

### 1.2.1 Antenna Beam of the Wi-Fi 6E Access Point and Client

A Dell Latitude 5240 laptop has been used in the test set-up, typically equipped with two PCB antennas just above the screen. As a reasonable assumption here, it is referred to the EMC study, which simulated and measured the performance of a PCB Dual Frequency inverted FL antenna inside a Notebook [23]. The resulting radiation pattern can be seen below in figure 3.10.

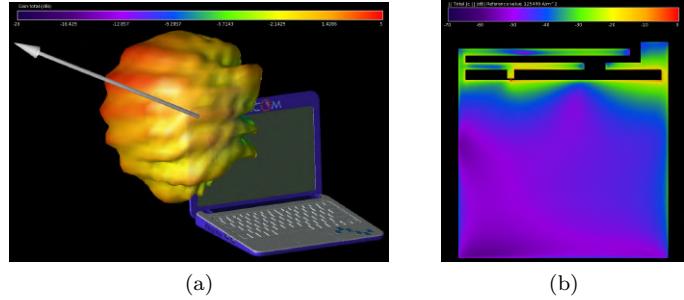


Figure 3.5: Antenna Gain (a) and Surface Current (b) at 6.42 GHz [23]

To complete the set-up, the arrangement of the laptop side-ways to the Line-of-Sight of the Wi-Fi 6E Router seemed plausible. Additionally, the angle between the laptop screen and keyboard has significant leverage and, consequently, has to be considered an influencing variable of the set-up.

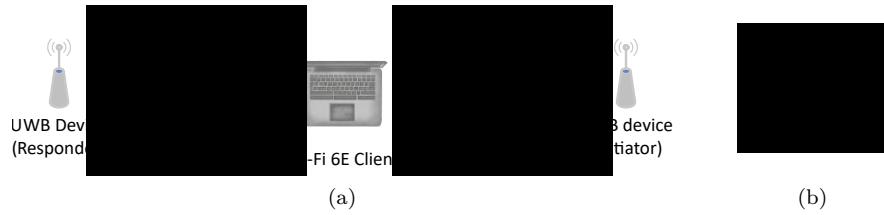


Figure 3.6: Line-Of-Sight Arrangement (a) Angle between Keyboard and Screen (b)

Following the position of the Wi-Fi 6E client, the spatial arrangement plays an important role. The Netgear Raxxe500 features a beamforming functionality that should decrease variation in TX power over spatial distribution. However, in a short test, the positioning in different angles around the Wi-Fi 6E Access point was investigated, and some differences in the Received Signal Strength Indicator (RSSI) were notable.

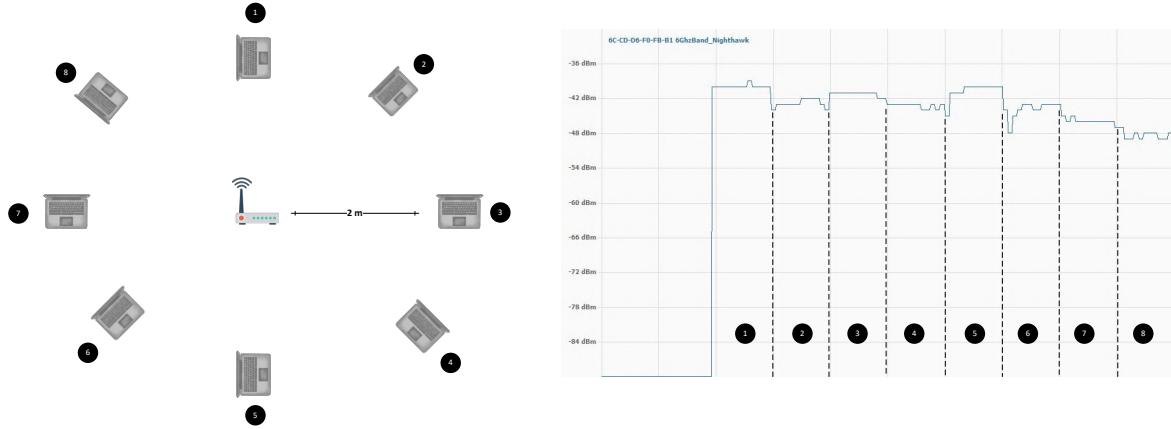


Figure 3.7: Postion of the Laptop (left) and RSSI Value from Laptop plotted in dBm (right)

In figure 3.7 a software tool, Homedale RSSI Analysis, is used to convert the RSSI value into dBm and plot it over time for a given radius and angle of the laptop to the router. As it becomes evident *Postion 1* is favorable for the set-up.

### 1.2.2 Placement of the UWB devices

As for the UWB devices, two commercially deployed antennas are compared. The radiation pattern of the board equipped with two different antennas is shown in figure 3.8 below. The TDK and Johannson antenna and their orientation performance depend on the angle of arrival of the signal.

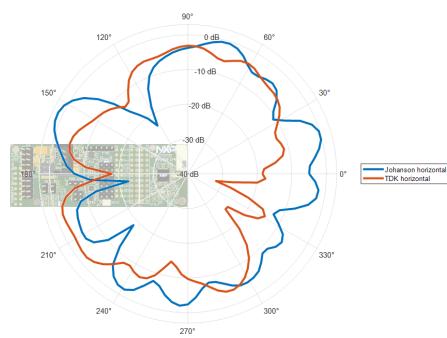


Figure 3.8: Antenna Radiation Pattern: TDK Antenna (red) , Johannson Antenna (blue)

As the Johannson antenna offers a strong radiation maximum at  $0^\circ$ , it will be used for the current set-up and an

inverted-pointing arrangement of the UWB devices to guarantee the best possible Line-of-Sight situation for the measurements.

This concludes the investigations into the final set-up with the arrangement depicted below.

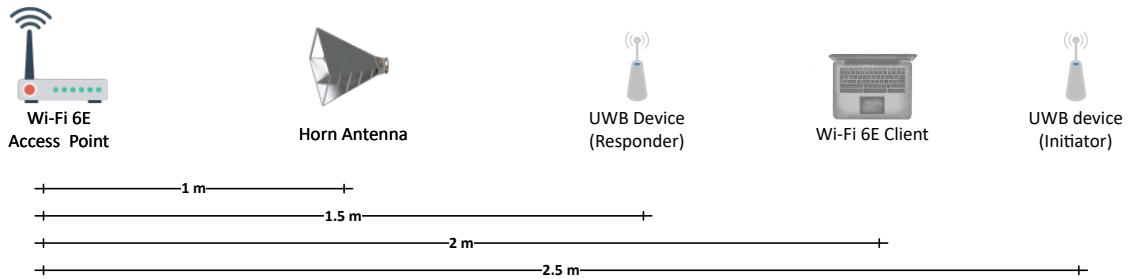


Figure 3.9: Schema of test set-up including all components

The horn antenna will be connected to a spectrum analyser, measure the Wi-Fi 6E signal power, and display it using a Fast-Fourier-Transform, in the frequency domain (see, e.g., Figure 3.16). All measurements are conducted inside an electromagnetic compatibility chamber which is fully covered in ferrite. A single side is covered with cone shaped RF absorbers that operate up to the multiple GHz range. Therefore the experiments are entirely isolated from external signals. However, reflections will occur since the set-up operates at the frequency range of around 6.5 GHz and the ferrites will reflect for frequencies above 1 GHz.

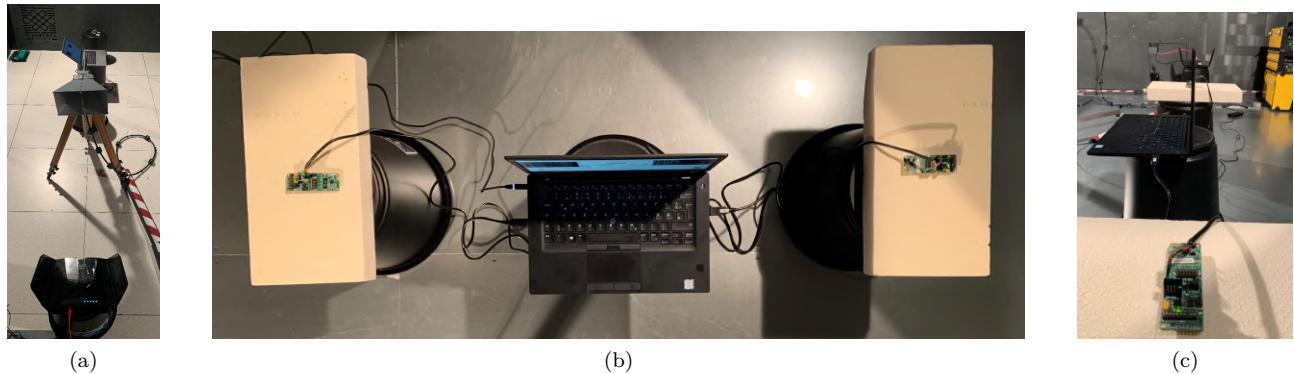


Figure 3.10: Photographs of the Test Set-up in the EMC Chamber

### 1.3 Design of Software Protocol

Following the two-way ranging concept explained in Chapter 2, Section 3.6, a software protocol for the UWB localization application has been implemented in the set-up. This protocol differs only slightly from a commercially used standard and therefore resembles a reasonable degree of compatibility to a real-life user scenario. Compared to the theoretical concept previously explained, two additional data frames have been introduced, which exchange the timestamps of Initiator and Responder after each ranging interval. As Equation 2.18 shows, these are necessary to calculate the accurate distance canceling out the center frequency offset on both devices.

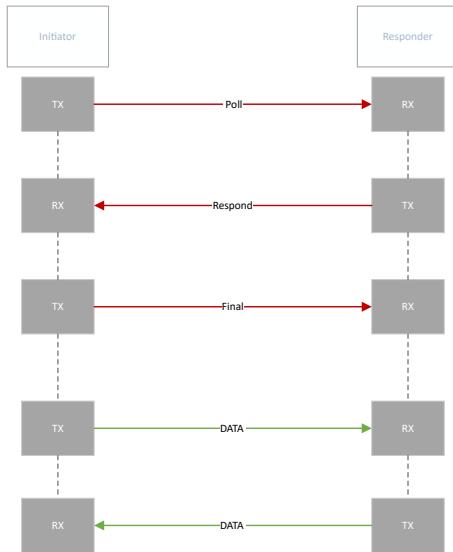


Figure 3.11: Two-Way Ranging Double Sided - Protocol: Ranging Frames (red) & Data Frames (green)

The protocol therefore consists of the *Poll-, Response-, Final- and Data-Frames*:

Like in the theoretical concept previously explained, the *Poll-Frame* begins the ranging round. While the Responder awaits the *Poll-Frame* it will go permanently into receiving mode awaiting the first frame of the protocol. After the successful reception of the preamble, it is synchronised to the Initiator. Now all subsequent frames will be sent in given time slots as both (Initiator and Responder) are aware of a commenced protocol. The objective is to restrict the interval of opening the receiver on both sides as much as possible to reduce the reception of unwanted noise and potential interference.

Referring to the Figure 2.37 of Chapter 2, Section 3.6, the protocol differs very little from the elemental idea discussed earlier. The main difference lies within in the addition of the two data frames (green) which exchange the Timestamps  $T_{RoundInit}$ ,  $T_{DelayInit}$  &  $T_{RoundResp}$ ,  $T_{DelayResp}$  respectively. This way, the accurate distance between the two devices can be calculated at the Initiator as well as the Responder.



Figure 3.12: Ranging Frame

A **Ranging Frame** (red) consists of the SYNC part, which holds the Preamble, the previously discussed SFD, and the STS. It is important to recall here that the Preamble of the SYNC field is decoded in primary pulses while all other fields are modulated with Burst Position Modulation and Binary Phase-Shift Keying.

A **Data Frame** consists of the SYNC field, an SFD, and the PHR and PSDU. It requires no secure timestamp since the stop clocks have already been stopped at that stage of the protocol, and the timestamps in the data field are encoded with the Reed-Solomon polynomials.



Figure 3.13: Data Frame

## 1.4 Definition of Influencing Variables

As a scientific approach to the design of the experiment, the theory of George Edward Pelham Box and the statistical design of experiments has been followed [10]. The starting point was the definition of the set of disturbance variables and control variables:

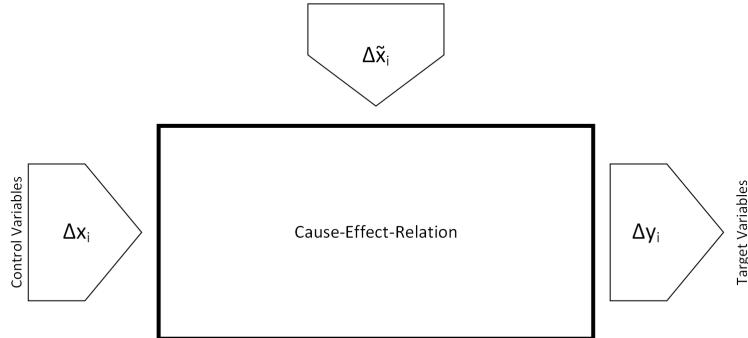


Figure 3.14: Design of Experiment

Following the theory of statistical experimental design, a set of factors  $X$  that, when changed by a  $\Delta$ , has a significant effect on the outcome of the target variables  $Y$  is called influencing variables. It is accordingly defined as the union of Control Variables  $\bar{X}$  and Disturbance Variables  $\tilde{X}$ .

$$X = \bar{X} \cup \tilde{X} \quad (3.1)$$

### Control Variables:

As a measure of influence on the Wi-Fi 6E - UWB experiment, the following set of control variables  $\bar{X}$  has been defined. It consists of distance  $d$  of the router to the client, which is proportional to the Wi-Fi 6E Signal Strength. The channel bandwidth  $B_{Channel}$  of the Wi-Fi 6E signal and the Angle  $\alpha_{screen}$  between the keyboard (Figure 3.6) are proportional to the probability of a package collision of UWB and Wi-Fi 6E frames. Finally, the center frequency  $f_{Center WiFi}$  of the Wi-Fi 6E Channel influences the severity of package collisions [4].

$$X := \{d_{distance}, B_{channel}, D_{stream}, \alpha_{screen}, f_{Center WiFi}\} \quad (3.2)$$

### Disturbance Variables:

The set of disturbance variables  $\tilde{X}$  is defined as all influencing variables that make an impact on the measurement but cannot be controlled (at least with the current set-up). As a matter of fact, this set is rather large. Therefore, only a few most important variables are listed here:

The frequency hopping pattern  $f_{hopping}$  with which the Wi-Fi 6E signal sends data over a large variety of frequencies (frequency spread) is can clearly be seen in Figure 3.16 . The network capacity of our local ethernet network  $C_{Network}$  which is time-dependent and stands in relation to the network topology, occasionally limiting the datarate  $D_{Stream}$  as we can see e.g. in figure 3.15 from 5000 to 7000 Ranging Attempts on the Download rate. The reflectivity and resulting reflections  $R$  from the ferrite on the walls in the partially anechoic chamber.

$$\tilde{X} := \{f_{hopping}, C_{ethernet}, R_{Ferrit}, \dots\} \quad (3.3)$$

*Factor levels of Control Variables:*

Varying the distance Distance  $d$  in Meter of the router to the laptop and the UWB devices.

$$d := \{0.5, 1.5, 2, 2.5, 3\} \quad (3.4)$$

Wi-Fi 6E Channel Width  $B_w$  in Mega Hertz

$$B_w := \{20, 40, 80, 160\} \quad (3.5)$$

Data stream  $D_{stream}$  in M/bits

$$D_{stream} := \{10, 50, 100, 200\} \quad (3.6)$$

Target Variables:

The Set of target variables  $Y$  is given by the **PER** previously defined in equation 2.1.

As subsets of the PER, it can be distinguished in the respective UWB error classes, which will be explained in detail in section 2.1.3

$$Y_{PER} := \{E_{PRMBL}, E_{TOA}, E_{STS}, E_{SECDED}, E_{RS}, E_{SFN}, E_{SL}\} \quad (3.7)$$

## 2 Measurements

A large variety of measurements have been conducted, investigating all possible combinations of control variables. The subsequent chapter will provide a comprehensive overview of the most significant results.

### 2.1 Results

For the coherent set-up, three major results could be identified. Each test case corresponds to a certain set of control variables mentioned above.

#### 2.1.1 Correlation of Wi-Fi 6E Data Stream and UWB PER

As a primary result in the development of the test case, one comes to understand the influence of Wi-Fi 6E on UWB when observing the change of the PER under variation of the data stream sent over Wi-Fi 6E.

When measuring, we see an interesting development of the Packet-Error-Rate in relation to a change in the data rate sent over the Wi-Fi 6E Channel. This dependency becomes obvious when plotting the PER over UWB Ranging attempts. One Ranging attempt starts with sending a UWB Poll message and, therefore, the start of the protocol. An error can be caused at any stage of the protocol sequence explained in section 1.3 and will consequently contribute to the PER calculated over the last 100 triggered Ranging Attempts. The following settings of control variables have been used for the plot below:

$$\bar{x} = [2m, 160Mhz, 100Mbit/s, 135^\circ]^T \text{ where } \bar{x} \in \bar{X} \quad (3.8)$$

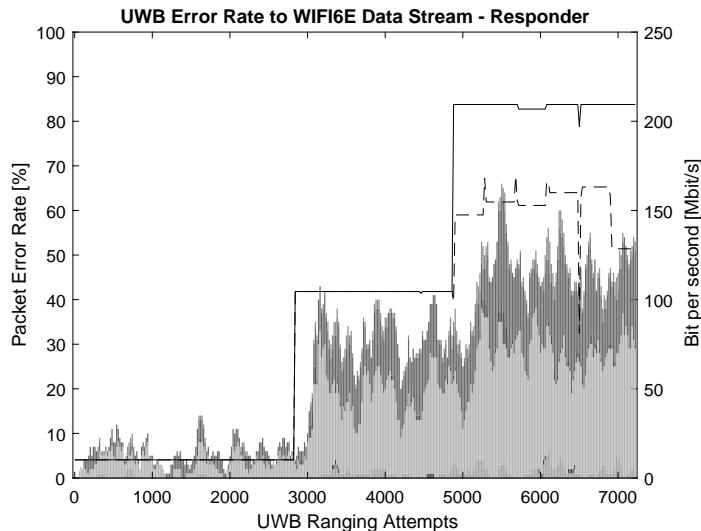


Figure 3.15: Grey Scale of UWB Error Codes accumulated at 160 MHz Wi-Fi 6E Channel Width  
Wi-Fi 6E Upload Stream (solid line), Wi-Fi 6E Download Stream (dotted line)

Higher Wi-Fi data rates are more likely to cause interference with UWB frames since the air time taken by Wi-Fi 6E frames increases with expanded data throughput. This relation becomes evident when observing the Wi-Fi 6E channel on the spectrum analyzer with the spectrogram tool:

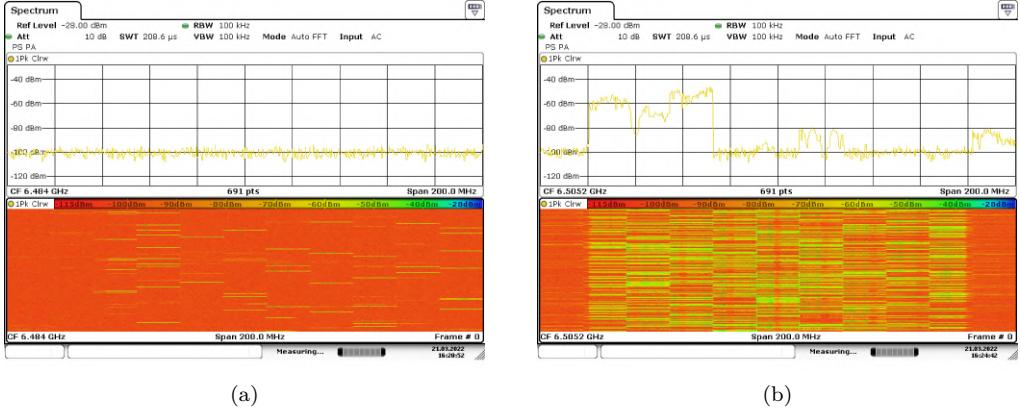


Figure 3.16: Snapshot of the Wi-Fi 6E 160 MHz Channel captured on a Spectrum Analyzer : (a) at 10 M/bits and (b) at 300 Mbit/s Download rate

The spectrogram tool adds another dimension to the spectrum analyzer plot. While one can observe the variation of frequencies encoded by a Fast-Fourier-Transform above, below a time axis is added, capturing the received signals over time. Here the increase of Wi-Fi packets and spectral power density can be seen.

### 2.1.2 Effect of Wi-Fi 6E onto the UWB Channel Impulse Response

As part of the investigations and in order to understand all possible effects of Wi-Fi 6E on UWB, the channel impulse response, as introduced in Chapter 2, Section 3.4, has been evaluated for different Wi-Fi channel widths and data rates. The most significant result can be seen in Figure 3.17 below. A measurement with  $B_{Channel} = 20MHz$  has been conducted for a changing data rate  $D_{stream} = \{10, 50, 100\}$  Mbit/s over time.

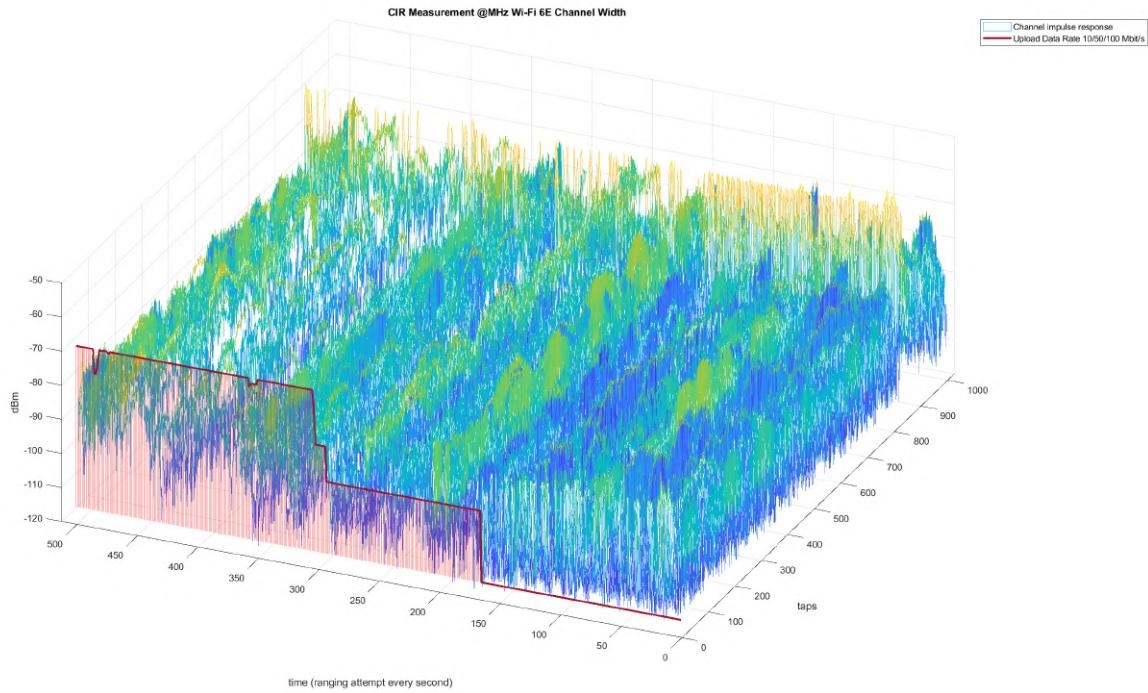


Figure 3.17: UWB Channel Impulse Response (blue color scale) at 20 MHz Wi-Fi 6E Channel Width plotted over time and taps

The Y-Axis increases with the number of *Ranging Attempts* whereas one ranging attempt has been performed every second. The X-Axis respectively allocates 1024 taps which are register fields holding a specific point in time captured of the CIR. In the two-dimensional CIR in Figure 2.33 these taps correspond to the nanosecond intervals of the CIR estimate. Around Tap 850, we always find the strongest path, which ideally correlates with the first path, meaning the highest dBm value lies here. With an increase in data rate, the plot shows more "holes," which results from failed decoding of the CIRs. Also, notable is that the noise floor seemingly increases with the increase in data rate along the Y-axis (lighter colors, towards green/yellow). However, this cannot clearly be deduced from this three-dimensional representation. Therefore, in the following, a two-dimensional graph has been used, introducing the coloring of the power.

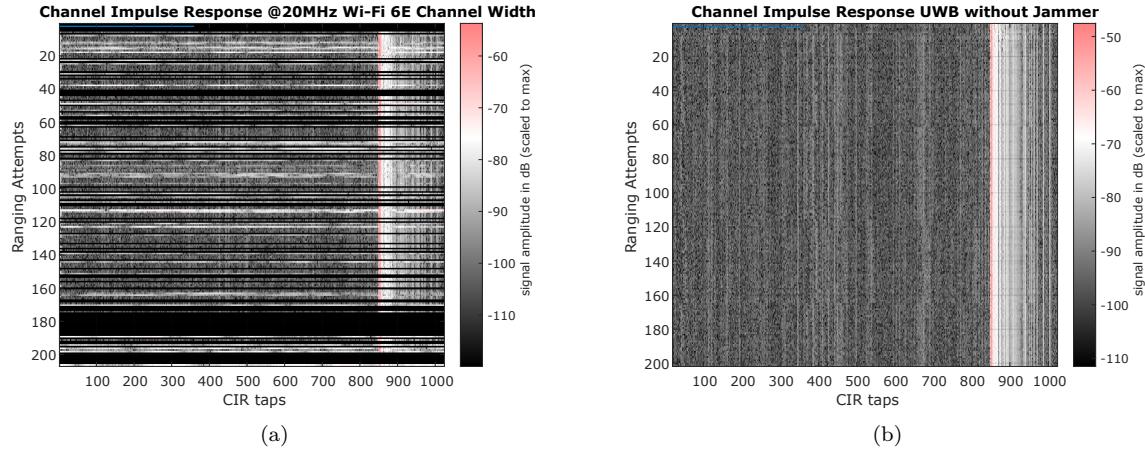


Figure 3.18: (a) CIRs - Wi-Fi 6E 20 MHz bandwidth channel from Figure 3.17 (b) CIRs measured under equivalent circumstances without Wi-Fi 6E

In the two-dimensional view, everything becomes far more straightforward. Obviously, one sees the failed attempts to decode the CIR due to Wi-Fi 6E interference. Compared to the captured CIRs on the right without any jammer present, one can observe an increase of received signal strength in dBm by a lighter color tone (more white lines). For example, the region between the 80. - 100. Ranging Attempt is a lot lighter set side by side with its counterpart. With increasing data rate, unsuccessful CIR decodings become more frequent, and also, the noise floor seems to rise as we observe the color scale to become lighter (e.g., in the region of the 200. Ranging attempt). In order to examine this assumption further, two single CIRs from the measurements have been plotted.

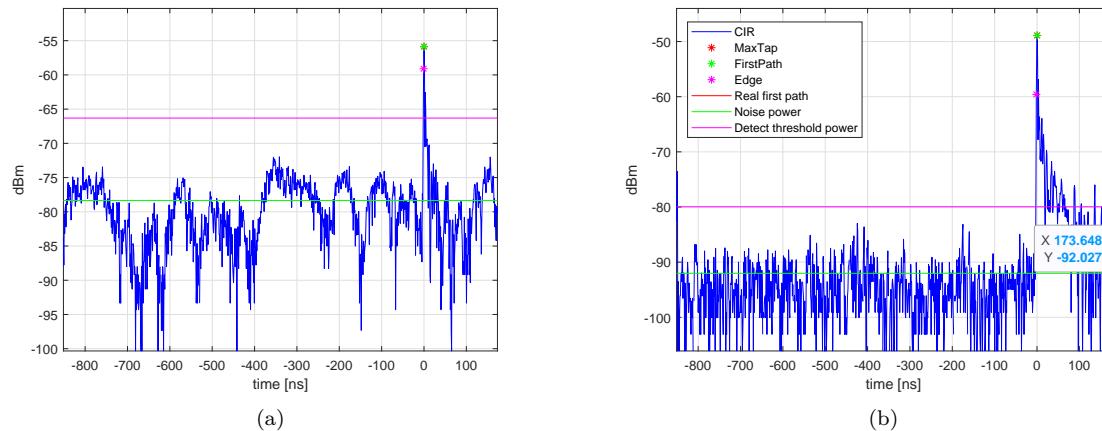


Figure 3.19: (a) Single CIR - Wi-Fi 6E 20 MHz bandwidth channel from Figure 3.17 at 100 Mbit/s Data Rate  
(b) Single CIR measured under equivalent circumstances without Wi-Fi 6E

Having these plots next to each other, the influence of Wi-Fi 6E on UWB becomes evident. Calculating the SNR, introduced in Equation 2.3, the results yield  $SNR_{Wi-Fi_{On}} = 22.464 \text{ dB}$  in presence of the Wi-Fi jammer and  $SNR_{Wi-Fi_{Off}} = 43.138 \text{ dB}$  for the measurement without Wi-Fi present. Wi-Fi 6E does therefore severely decrease the SNR. The Overall-Noise measured by the UWB receiver is about  $\Delta 14 \text{ dB}$  higher, and additionally, we can see some extreme peaks even well before the arrival of the first path. Notably, the strongest path is reduced by roughly  $\Delta 8 \text{ dB}$  compared to the case without a Wi-Fi jammer. However, some tests showed even more significant variations of up to  $\Delta 15 \text{ dB}$ .

### 2.1.3 Differentiating Failure Causes

To better understand the influence of Wi-Fi 6E on UWB frames, the different error statuses obtained from every UWB receiver during the measurements codes have been decoded. A detailed analysis should provide a transparent picture of why these errors are occurring and give insights into which parts of the UWB frames are more vulnerable to interference and which might be more robust. Again, it is essential to recall that the set-up (Figure 3.11) and protocol (Figure 3.9) allocated two different roles to the UWB devices: Initiator & Responder. The following graphs are distinguished between their respective error logs as the PER behaves very differently depending on the role of the device.

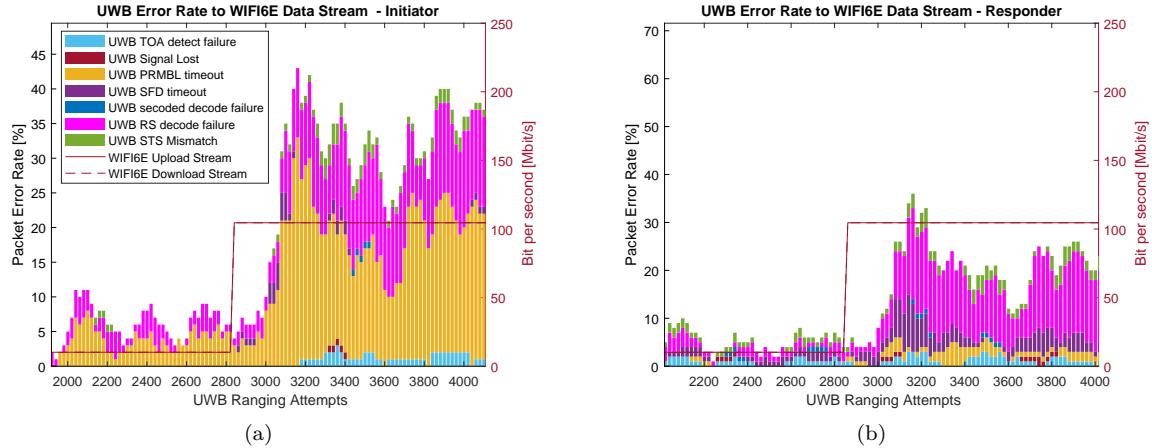


Figure 3.20: PER distinguished between different UWB Error Codes - Measurement at 160 MHz Wi-Fi 6E Channel Width with a Variation of the Data Rate

As the effect of the data rate  $D_{Stream}$  on the PER, in general, has already been observed, now a closer focus on the outcome of Wi-Fi 6E packages colliding with different parts of a UWB frame is of interest. The NCJ29D5 PHY layer provides a set of error status codes, which have already been introduced in Equation 3.7. Figure 3.20 shows a snippet of a full measurement shown in Figure 3.15 distinguishing between the different UWB PER cases.

**UWB Time-of-Arrival detect failure  $E_{TOA}$** 

This error message indicates a failure to detect a valid first path signal. This problem can have multiple causes. One possibility is that through destructive interference, as introduced in Chapter 2, Section 1.1, Figure 2.2, the received energy of the first path signal is decreased. Therefore the first path is not recognized.

**UWB Signal Lost  $E_{SL}$** 

This error code indicates that the received signal power dropped below a certain threshold during the reception of the PSDU field. This event makes decoding the data frame part impossible.

**UWB Preamble timeout  $E_{PRMBL}$** 

A *Preamble Timeout* indicates that the receiver has detected a signal but could not synchronize and correlate the ternary code with one of the IEEE codes within a given time interval. *Preamble timeouts* occur very frequently in this test set-up, as it becomes apparent later.

**UWB Start-of-Frame-Delimiter timeout  $E_{SFD}$** 

An SFD timeout is triggered when the receiver could synchronize and decode the preamble (at least partially) but fails to find or read the start-of-frame delimiter. This error could occur because either the SFD field was severely damaged due to interference. It may also be a valid assumption, the receiver could have synchronized on the preamble of a Wi-Fi frame.

**UWB Secoded decode failure  $E_{SECDED}$** 

In reference to Chapter 2, Section 3.2.3.4 the second block encodes the header of the data frame. This error message, therefore, indicates failure at one of the last frames of the ranging protocol explained in Figure 3.11. In this case, more precisely, the error code *Secded decode failure* indicates the IEEE Parity check performed on the PHR detected uncorrectable errors.

**UWB Reed-Solomon decode failure  $E_{RS}$** 

Similar to the *Secded decode failure* the *Reed-Solomon decode failure* originates from the data field of the UWB frame. In this case, not the header (PHR) of the UWB frame has been affected, but the Reed-Solomon algorithm executed on the PSDU detected uncorrectable errors.

**UWB Secure-Time-Stamp Mismatch  $E_{STS}$** 

As already discussed in Chapter 2, Section 3.2.3.3, the STS is a security measure based on AES128 encryption. An *STS-mismatch* indicates that the decoded STS does not match the calculated one.

It is important to recall that some error messages can occur at any given point in the protocol, for example, the *Preamble timeout*, while others like the *STS mismatch* or the *Reed-Solomon decode failure* are limited to data or ranging frames, respectively.

#### 2.1.4 Influence of the Wi-Fi 6E Channel Width on the Packet-Error Rate of UWB

As a consequence of the previous investigations, the effect of the Wi-Fi 6E Channel Width  $B_{Channel}$  is to be investigated. The goal of the experiment has been to hold the data rate and all other settings at a constant level and compare the PER and UWB Error Codes as a function of the Wi-Fi 6E channel bandwidth.

##### 160 MHz Channel

Factor levels for the control variables:

$$\bar{x} = [2m, 160\text{MHz}, 100\text{Mbit/s}, 90^\circ]^T \quad (3.9)$$

The 160 MHz Channel Bandwidth causes a fatal scenario for UWB ranging. With accumulated error rates as high as  $PER = 92\%$  the impact of Wi-Fi 6E on UWB is severe.

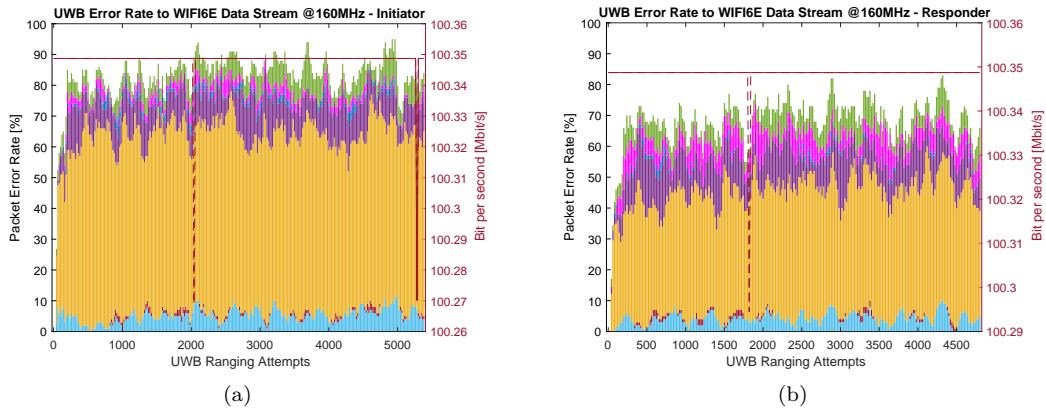


Figure 3.21: 160 MHz Channel Bandwidth - Initiator and Responder

The output is distinguished between the error log of the Initiator and the Responder. Even though the Responder has an overall slightly lower error rate, the proportions of the UWB error distribution are almost identical. The *Preamble Timeout* UWB error occurs most frequently, followed by the *SFD Timeout* and then the *STS Mismatch* and *TOA detect failure*.

For a more precise analysis and comparison to the other Wi-Fi bandwidths, the mean values of the respective error codes following Equation 3.7 are given below:

$$Y_{Init} = [5.1932, 0.5189, 57.9780, 10.1257, 1.0454, 2.1397, 5.4310]^T \quad (3.10)$$

$$Y_{Resp} = [4.1758, 0.4983, 40.5717, 10.6906, 0.4246, 5.4292, 5.8688]^T \quad (3.11)$$

These values are to be interpreted respectively with the error codes defined in Equation 3.7

$$Y_{PER} := \{E_{TOA}, E_{SL}, E_{PRMBLE}, E_{SFD}, E_{SECODED}, E_{RS}, E_{STS}\}$$

## 80 MHz Channel

The 80 MHz Wi-Fi 6E channel bandwidth causes a very similar PER distribution. Compared to the 160 MHz bandwidth the PER is slightly lower. Again, the *Preamble Timeout* is the dominant error scenario. Recalling that the 80 MHz channel has a slight decrease of  $\Delta 2 \text{ dB}$  in TX power by the IEEE 802.11ax, this seems plausible.

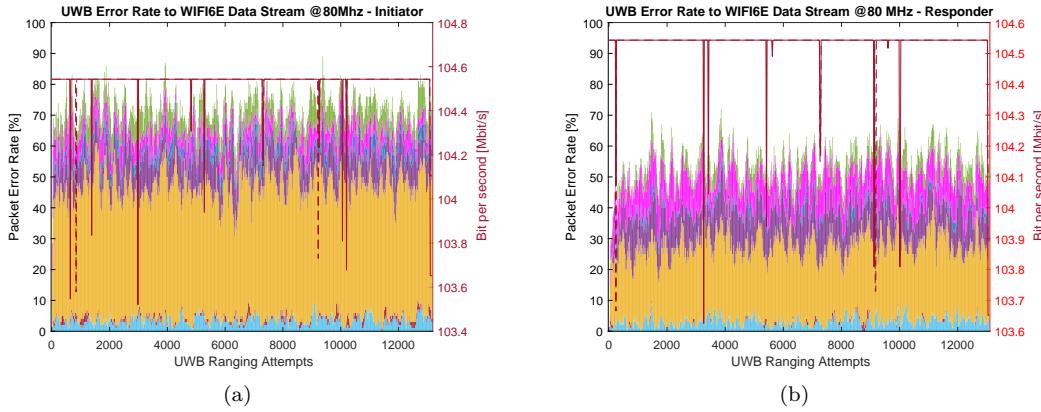


Figure 3.22: 80 MHz Channel Bandwidth - Initiator and Responder

## 40 MHz Channel

Now, with the 40 MHz Channel Bandwidth, one sees a change in the behaviour of the PER distribution. Note that the percentage of *Preamble Timeout* is decreasing while the number of *SFD timeouts* is increasing but only on the initiator side. At the same time, the responder is giving back an increasing proportion of *Reed-Solomon decode errors*.

Again, the 40 MHz channel decreases in TX power down to 21 dBm, a significant drop compared to the 160 MHz and 80 MHz channels.

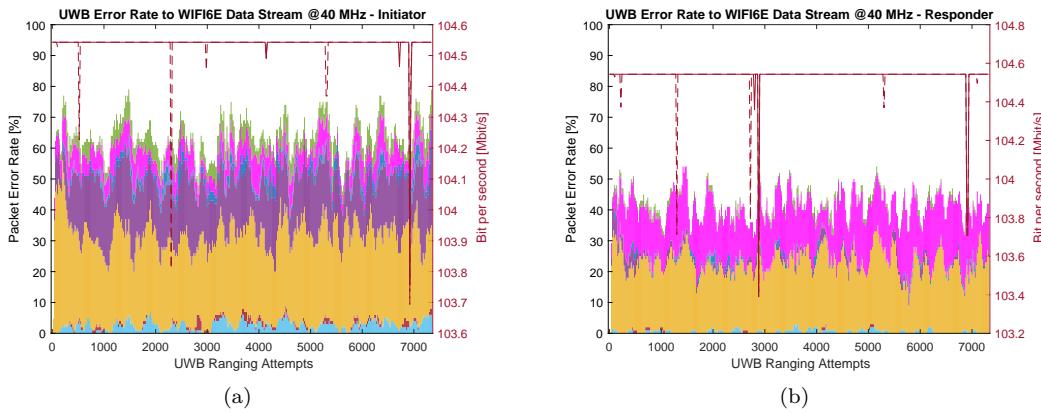


Figure 3.23: 40 MHz Channel Bandwidth - Initiator and Responder

## 20 MHz Channel

For the 20 MHz Channel, a subsequent drop to 18 dBm Wi-Fi TX Power is also perceptible in a further drop in the PER on both Initiator and Responder sides. Most notably here, the *Reed-Solomon decode error* increases even further in proportion and becomes the dominant UWB reception error scenario for the responder's side.

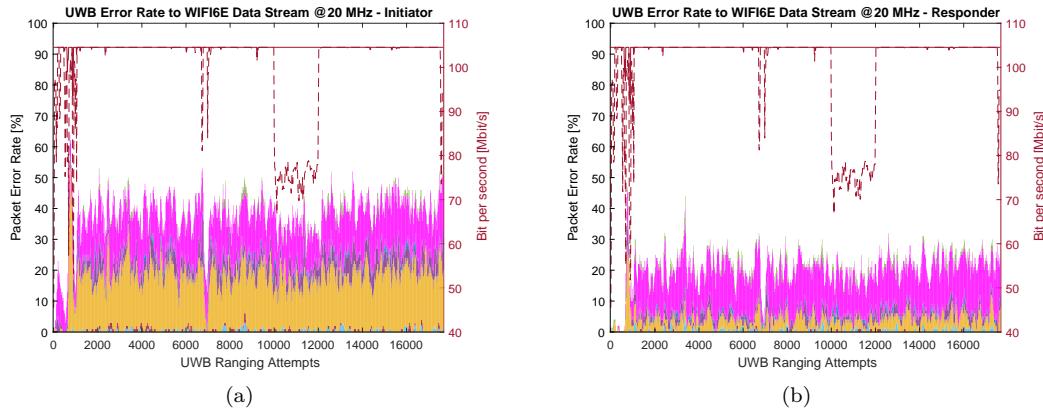


Figure 3.24: 20 MHz Channel Bandwidth - Initiator and Responder

## Comparison of the Effect of the four Wi-Fi 6E Channel Bandwidths on UWB Ranging

Below are the respective mean values of the corresponding error codes plotted and distributed over their respective channels. Five major trends are observable.

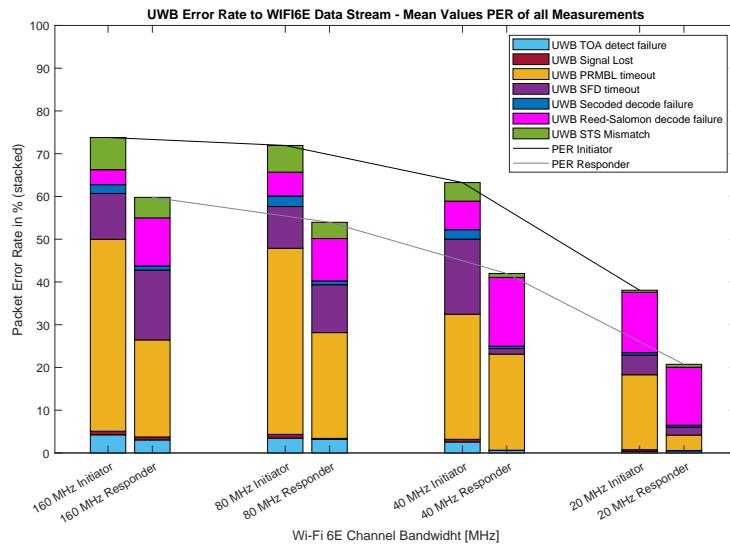


Figure 3.25: All Wi-Fi Channel Bandwidths compared - Initiator and Responder

*1. Decrease in overall PER with a decrease in channel bandwidth*

Apparently, the larger bandwidths of Wi-Fi 6E cause greater harm to UWB communication. This result actually contradicts the studies conducted at the TU Graz which will be discussed in detail later and therefore should be investigated further. However, it has some reasoning since, as mentioned, the Wi-Fi TX Power decreases respectively with the channel width by the 802.11ax standard.

*2. Start-of-Frame delimiter, Preamble, and Data field make up for the largest portion of the PER*

Evidently, the SFD-, Preamble- and Data-Field cause the most significant percentage of bit error flags after the reception.

*3. Increase in overall Reed-Solomon decode failures with a decrease in channel bandwidth*

While all other UWB reception error codes decrease with lower Wi-Fi channel bandwidth, the Reed-Solomon decode errors increase. This leads to the hypothesis, which will be continued in the hypothesis that the payload is more vulnerable to interference with Wi-Fi 6E Frames than the other fields of a UWB frame.

*4. Decrease in the percentage of Preambles Timeouts relative to the total PER*

In contradiction to Point 3. the *Preamble Timeout* occurs less frequently at lower bandwidths compared to other UWB reception errors.

*5. STS, PHR Field is relatively stable*

In these measurements, the STS and PHR Header fields are relatively stable. The UWB reception errors *STS mismatch* and *Secded decode failure* occur infrequently and decrease constantly with a decrease in bandwidth.

## 2.2 Discussion

Following the results stated in the section above, possible assumptions and explanations shall be discussed. The aim is to make some predictions, give reasoning, and develop methods to improve the experiment and the software protocol to obtain better and more significant results.

### Degradation of service with increasing data rate $D_{Stream}$

An inevitable conclusion from the measurements is the cause-effect relation between higher data rates and increased PER. These results also correlate with the investigations of the TU Graz, which concluded that higher data rates with continuous traffic are more likely to cause interference to UWB traffic since the white spaces in the Wi-Fi signal become much smaller [4]. This can also be observed, for example, in Figure 3.16.

### The influence of the Wi-Fi Channel Bandwidth $B_{Channel}$

In Chapter 2, Section 3.1 the Processing Gain Equation 2.9 was introduced. It stated that UWB signals provide higher resistance towards narrowband interferers due to their greater processing gain. Therefore it might be assumed that with an increase in Wi-Fi jammer bandwidth, the actual processing gain of UWB decreases since a significant portion of the spread bandwidth potentially interferes with the Wi-Fi 6E signal. However, in the case of Wi-Fi 6E, it is not as simple.

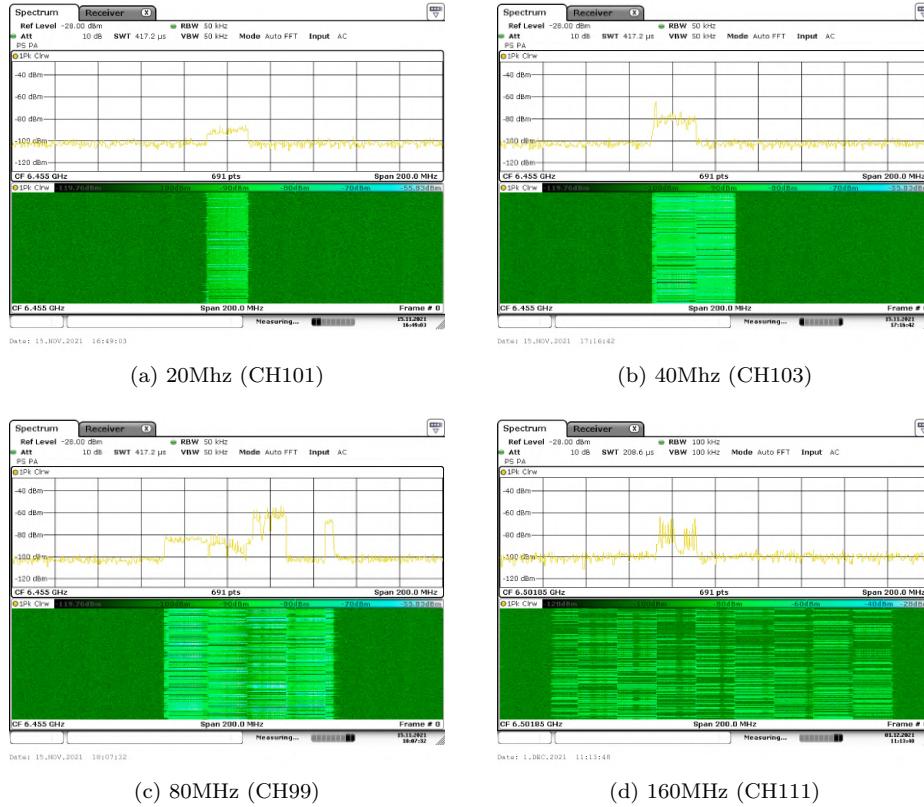


Figure 3.26: Wi-Fi 6E Channel Bandwidth

As Figure 3.26 reveals, the Wi-Fi signal changes the used subchannels with increasing bandwidth more frequently. Also, as already discussed in the previous Section 2.1.1, the increase in data rate demands more air time leading to a narrowband channel (e.g., 20 MHz) having a higher duty cycle in transmission than one with the same amount of data sent over a wideband channel (e.g., 160 MHz). While the severity of a 160 MHz Wi-Fi - UWB packet collision might be higher, the probability can be assumed to be lower than with a 20 MHz Wi-Fi packet.

*Analyzing the various UWB reception error statuses, multiple cause-effect scenarios are possible. It seems plausible to discuss the origin of every error code first.*

**1. SFD Timeout** In theory, the *SFD timeout* can be assumed to have two different cause-effect scenarios. Firstly, a Wi-Fi packet could, by chance, have collided at the exact portion of the UWB frame that holds the SFD field, given the signal was strong enough to cause severe interference. This would lead to the UWB receiver identifying the preamble but not detecting the Start-of-Frame delimiter.

Secondly, and given the high percentage of *SFD timeouts* in the PER, more likely, the UWB receiver is synchronized upon a Wi-Fi 6E packet. This means that a Wi-Fi 6E frame was mistakenly recognized as a UWB frame, making the UWB receiver unaccessible for actual UWB traffic or delaying the receiver for an actual UWB frame holding a valid SFD. The latter of theory has actually been proven by investigations at the TU Graz and will be discussed in the following sections.

**2. Preamble Timeout** As a result of the investigations into the coexistence of UWB with different Wi-Fi 6E channel widths, the *Preamble Timeout* has been decreasing in relative percentages, while for the 160 MHz Channel, *Preamble Timeouts* made for 60% of the PER of the Initiator and 34% for the Responder, respectively. At the 20 MHz Channel, the *Preamble Timeouts* only contributed 46% and 17.5% respectively. This leads to the assumption that the Preamble is more affected by the Wi-Fi 6E frames signal with a higher transmit power. The *Preamble Timeout*, just like the *SFD timeout*, can be assumed to occur on different scenarios. The most significant assumption that was taken is pictured in Figure 3.27.

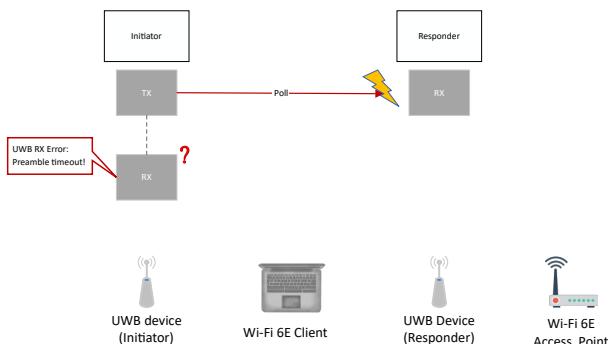


Figure 3.27: Preamble Time Out - Error Scenario

As for the theory, the *Preamble Timeout* error resembles a scenario where the Responder is awaiting the *Poll Frame* from the Initiator. The *Poll Frame* however, collides with a Wi-Fi 6E packet. Due to interference of the two signals, the Responder does not recognize the resulting signal as a UWB frame anymore. In conclusion, the Responder will not send a *Response Frame*, causing the Initiator to trigger a *Preamble Timeout* since it could not obtain a response message within a specific time interval. This scenario seems most likely since as Figure 3.27 shows the Responder is in between the two Wi-Fi 6E devices and therefore likely to be much more affected by Wi-Fi traffic. Hence, this also explains why the PER of the Initiator is always higher than the PER of the Responder. Recalling Section 1.3 the *Responder* will wait for a received *Poll Frame* in reception mode, not triggering a time out since it is not synchronized as yet, while the Initiator will expect a response within a given time interval.

The synchronisation problem exposes one of the significant disadvantages of this protocol implementation. Supporting the latest UWB - Wi-Fi 6E studies conducted by the technical university of Graz [4] have ratified the previous

assumptions that the time interval of opening the receiver for reception from UWB frames has a critical impact on ranging performance. This conclusion can be traced back to the error case of the *SFD Timeout* scenario, where the receiver synchronizes onto a Wi-Fi packet by chance. Hence, a portion of the captured *Preamble Timeouts* could also resemble the false detection of Wi-Fi frames for UWB frames (see Figure 3.32).

Generally speaking, the *Preamble Timeout* scenario can also occur at any given point in the protocol whenever a Wi-Fi packet has severely hit the Preamble. Explicitly, after the transmission of the *Response*, *Final* or any other frame. The core difference is that the Responder is simply awaiting the *Poll frame* endlessly, while after successful reception and synchronization, all other frames are estimated to arrive within a given time interval.

### 3. Reed-Solomon decode failure

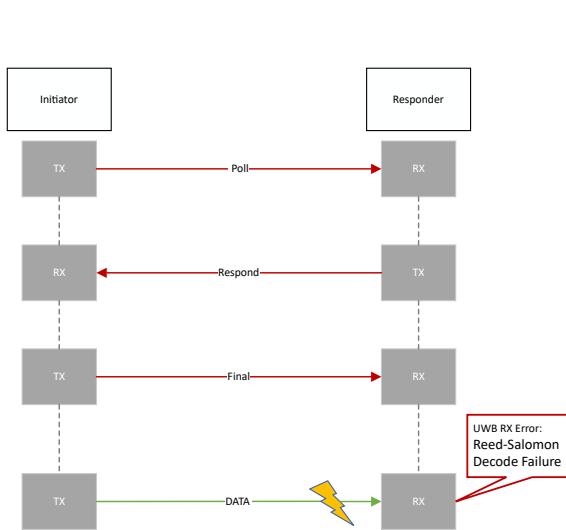


Figure 3.28: Reed-Solomon decode failure  
UWB Reception Error Scenario

Recalling Chapter 3, Section 2.1.3 this error code only occurs at the data frames when the Reed-Solomon checksum did not add up after reception of a UWB frame. So the protocol failed either after the first data frame from *Initiator* to *Responder* or the other way around. As mentioned under *Point 3.* in Section 2.1.4, it states that the *Reed-Solomon decode failures* increase with a decrease in Wi-Fi channel bandwidth. This trend could lead to an assumption that the payload of a UWB frame might be more vulnerable to Wi-Fi 6E interference than other fields. A collection of factors such as the increased length, data rate, and modulation technique could support this thesis. However, a new testing strategy would need to be implemented to verify this theory.

**4. TOA detect failure** only occurs after the reception of the Preamble. As described in Section 2.1.3 this error flag is triggered when no valid first path could be detected. Referring to Figure 3.19 it becomes evident how the Wi-Fi 6E signal perturbs the CIR of a UWB frame. A hypothesis would be that through Wi-Fi interference, the CIR is distorted to a point where the UWB receiver cannot recognize the first path anymore.

**5. STS mismatches** only makes a small portion of the PER spectrum. It is mainly and mostly affected at 160 MHz channel width. In general, however, STS errors seem to occur rather unlikely since if the Preamble and the SFD have been decoded successfully **Responder** and **Initiator** are synchronized, and therefore, the decoding of the data points has a much higher success rate. Also, compared to a data field, the STS is known to both sides, possibly leading to a better correlation outcome.

### 3 Redesign of Experiment

Concluding from the discussion 2.2, a recursion of the last Design-of-Experiment process was needed to obtain more substantial results and make a more accurate assessment of which frames are affected the most by Wi-Fi 6E collisions. Furthermore, it might be interesting to explore how to counteract the effects of Wi-Fi 6E by more or less reduced protocol choices.

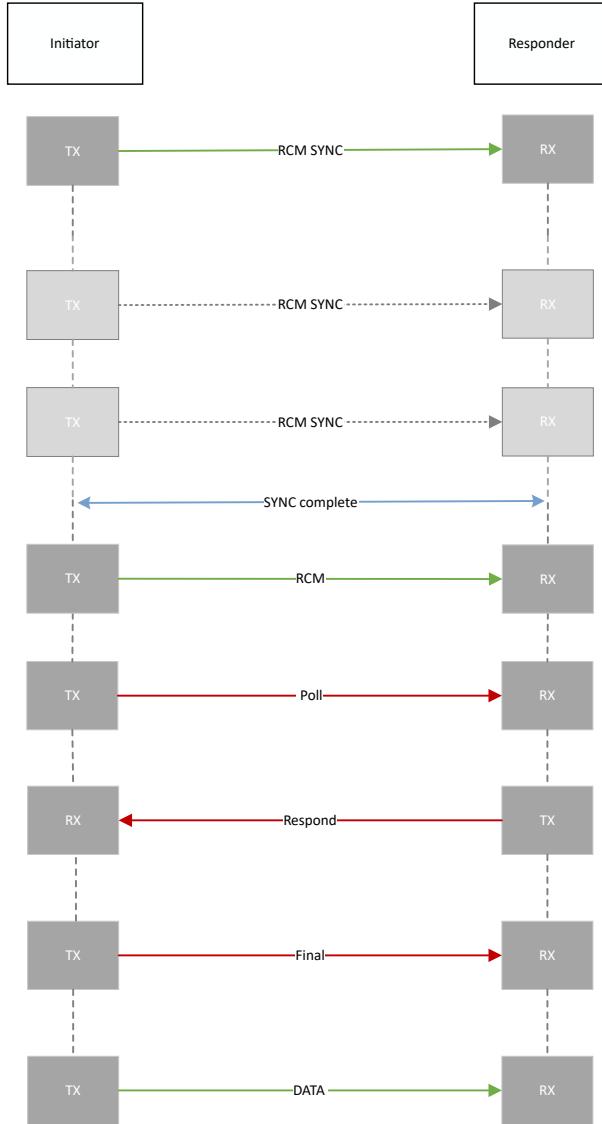
Three main factors were identified, which acted as a drawback to further conclusions:

1. **Information as to which frame (*Poll*, *Response* , *Final* or *Data<sub>Init</sub>*, *Data<sub>Resp</sub>*) has been erroneous.** Some error codes can be traced back to particular messages (like the STS mismatch - Ranging Frame or the Reed-Solomon Decode failure - Data Frame). Others (e.g., the Preamble Timeout) could occur at all protocol parts. Additionally, even after tracing back an error to a particular frame type, one could not tell at which part of the protocol the failure occurred.
2. **Time drift of clocks and missing synchronization at the very start of a measurement** While the ranging protocol is synchronized after each successful reception of the *Poll-Frame* by the Responder, still a synchronisation problem arises at the very beginning of every measurement. Two clocks, one on the Initiator and one on the Responder, are triggered and run during the measurement. This enables the mapping of the *Wi-Fi 6E Data Rate D<sub>Stream</sub>* to the *Ranging Attempts*. However, mapping of the individual frames sent by the Initiator and received by the Responder to a specific *Ranging Attempts*, later to be named *Ranging Block*, in time and vice versa was not possible since the clocks had a time drift. Furthermore, chances were that through a delay at the beginning of a measurement, a shift in the starting value  $t_{0Init} \neq t_{0Resp}$  has been introduced.
3. **The interruption of protocol after a single error** So far, the entire protocol was aborted whenever the reception of a single frame failed. This made it impossible to draw further conclusions, for example, to predict how a shortening of the protocol, e.g., Single-Sided Two-Way Ranging, could effectively countermeasure the poor performance of UWB ranging under Wi-Fi 6E presence.

### 3.1 Change of Protocol

Concluding from the points above, a redesign of the ranging protocol was needed.

At the beginning of every protocol, a new data frame has been introduced to tackle the synchronization problem.



The *Ranging-Control Frame*, which sends a block number  $Nb_{Block}$  to mark a certain *Ranging Block*. However, before the block counter starts, a *SYNC-Phase* is run between Initiator and Responder to ensure the clocks are synchronised.

After completion of the *SYNC-Phase* the actual ranging protocol begins. Each frame is sent after a time interval of 5ms regardless of whether or not the previous frame was received correctly. Consequently, by logging all received frames with their respective block number, it will be possible to assess the number of cases that could still be used for distance calculations using a simpler ranging protocol.

After the successive three ranging frames, only one data frame is sent from Initiator to the Responder. This design was chosen because it resembles the automotive case, whereas the keyfob acts as an Initiator and only transmits its timestamps to the car side.

Each *Ranging Frame* has a total length of  $139.9\mu s$  containing as before the Preamble holding 65 symbols, the SFD holding 8 symbols, and STS field with 4096 bit. Meanwhile, the D data frames vary in length. The *RCM Frame* holds 46 byte of data, and the *Final Data Frame* a payload worth 121 byte with a length of  $149.7\mu s$  and  $238\mu s$  respectively.

Figure 3.29: Two Way Ranging Double Sided - Synchronous Protocol

## Measurements

$$X = [2m, 160MHz, 100Mbit/s, 135^\circ]^T \quad (3.12)$$

The new measurement was conducted using the  $B_{Channel} = 160MHz$  Wi-Fi Channel Bandwidth,  $D_{Stream} = 100Mbit/s$ .

### 3.2 Results

1500 Ranging Attempts were evaluated after the successful *SYNC\_Phase*. Each Ranging Attempt was mapped to a certain Block Number. Through the evaluation process, the UWB reception error codes were sorted to the frame type in which they occurred.

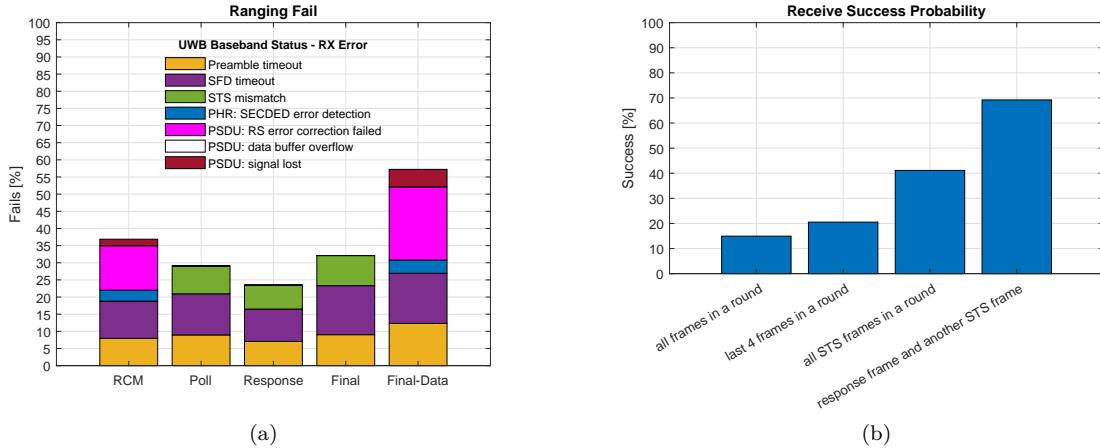


Figure 3.30: Two Way Ranging Double Sided - Synchronous Protocol

With a  $PER_{FinalData} = 57.22\%$  and  $PER_{RCM} = 38.86\%$  the data frames are most affected by Wi-Fi 6E. The *Reed-Solomon decode failure* is holding the majority of the PER in both data frames. The *SFD Timeout* as well as the *Preamble Timeout* occur with a relatively constant percentage of  $9.5 - 14.5\% = PER_{SFC}$  and  $75 - 12.3\% = PER_{PREAMBLE}$  respectively, while the *STS Mismatch* is very stable at  $7 - 8.8\% = PER_{STS}$ . As intended by the new protocol design, via the mapping of the block numbers, it is possible to obtain a statistical analysis of the reception probability of certain frame combinations:

#### 1. ALL FRAMES ARE RECEIVED CORRECTLY IN THE PRESENCE OF WI-FI 6E

In this event, every single frame has to be received in an entire ranging block. Therefore an AND connector is needed.

$$P_{AllFrames} = Q_{RxRCM} \& Q_{RxPoll} \& Q_{PxResp} \& Q_{RxFinal} \& Q_{RxData} \quad (3.13)$$

$Q_{Rx} := \{0, 1\}$  The State of reception of a specific frame of the protocol from a coherent ranging block

As Figure 3.30 reveals the probability for a successful Double Sided Two-Way Ranging yields  $P_{AllFrames} = 14.9\%$

## 2. LAST 4 FRAMES IN ONE ROUND ARE RECEIVED CORRECTLY

$$P_{Last4} = Q_{RxPoll} \& Q_{PxResp} \& Q_{RxFinal} \& Q_{RxData} \quad (3.14)$$

The probability of receiving the last four frames, which is equivalent to a double sided Two-Way ranging without synchronization through the *RCM frame*, yields  $P_{Last4} = 20.5\%$

## 3. ALL STS FRAMES

$$Q_{AllFrames} = P_{RxPoll} \& P_{PxResp} \& P_{RxFinal} \quad (3.15)$$

Receiving all *STS Frames* means all ranging frames have passed. The probability for this event under the given conditions lies at  $P_{AllSTS} = 41.13\%$

## 4. THE RESPONSE FRAME AND ANOTHER RANGING FRAME

$$Q_{AllFrames} = (P_{RxPoll} | P_{RxFinal}) \& P_{PxResp} \quad (3.16)$$

The *Response Frames* and one other *STS Frame* are necessary to calculate a distance for a Single-Sided Two-Way Ranging. However, the center frequency offset (CFO) will have to be accounted for in this case. Since we are sending three ranging frames, an OR-connector is needed. The probability for receiving the *Response Frame* and either *Response Frame* or *Response Frame* yields  $P_{AllSTS} = 69.21\%$

### 3.3 Discussion

*Susceptibility of certain UWB frames and frame fields to Wi-Fi Jamming*

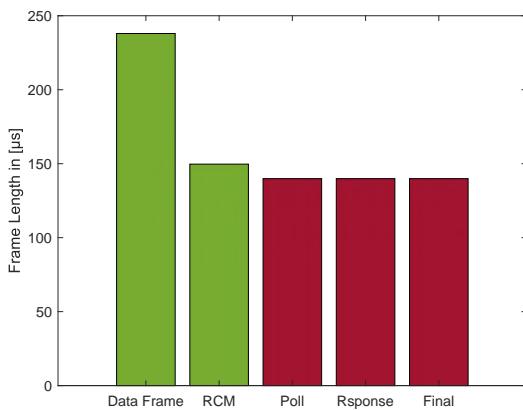


Figure 3.31: Two Way Ranging Double Sided Synchronous Protocol

As for the susceptibility of UWB frames to interference through Wi-Fi packets, the latest investigations have proven a particular vulnerability of the data frames. To be specific, the payload field. This may undoubtedly originate in the frame length. Reflecting that the *Data Frame* takes almost double the time to transmit than a *Ranging Frame*, it seems plausible that collisions with Wi-Fi packets become more likely. However, the *RCM Frame* is not extensively longer than the *Ranging Frames* but the  $PER_{RCM}$  shows a deviation of  $\Delta 10.6\%$  above from the mean PER (28.16 %) of the three ranging frames.

Results from the studies undertaken at the TU Graz have shown a similar susceptibility of the data frame, they related in proportion to the data rate and the associated symbols (UWB pulses combinations) per bit.

An additional contributing factor could be the modulation technique. It has been stated before that binary-phase and burst-shift modulation are more susceptible to interference.

Nevertheless, these assumptions need further testing with different data rates and possibly modulation techniques to be verified for the present case.

*Probability of frame reception and further use:*

As it has already become apparent from figure 3.30 (b), even with a tight synchronization pattern, the probability of a successful Double-Sided Two-Way Ranging becomes relatively small under heady Wi-Fi 6E traffic conditions. Therefore, it would make sense to consider other ranging possibilities or extend the protocol with a so-called "Take-What-We-Get" approach. Integrating an On-Demand Single-Sided Two-Way Ranging functionality or using this Procedure only for tracking while TWR-DS has successfully calculated the first distance should be promising, given a success rate of almost 70% for the latter case.

### 3.4 Comparison to Results at TU Graz

The institute for Technical Informatics of the Technical University of Graz has published a study titled "Understanding and Mitigating the Impact of Wi-Fi 6E Interference on Ultra-Wideband Communications and Ranging" [4]. The study involved the development of a test set-up using similar hardware equipment, a significant variation of testing and measurements. Even though the set-up differed to some extent, the results showed remarkable similarities. A few measurements are worth mentioning here to better understand the outcome from the previous discussion.

#### Impact of Overlapping Wi-Fi and UWB Traffic

Using a mixed-signal oscilloscope, they captured UWB - Wi-Fi 6E packet collisions and investigated the corresponding frames for successful reception on the UWB receiver side. Figure 3.32 shows the results below.

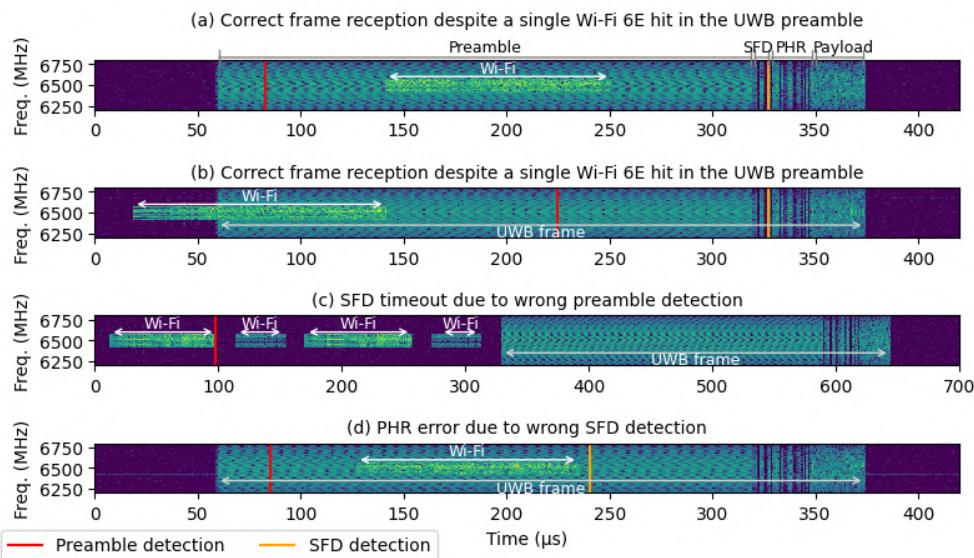


Figure 3.32: Oscilloscope traces of captures UWB - Wi-Fi 6E collisions [4]

Three major conclusions were made from the measurements contributing to the previous discussion.

*1. The Preamble, out of all fields, is most likely to recover from a Wi-Fi hit*

Compared to all other parts of a UWB frame, the Preamble was most likely to recover from a Wi-Fi 6E packet hit.

*2. SFD timeouts are likely to be caused by mistaken recognition of Wi-Fi packets for UWB Preambles*

Indeed, as previously assumed, the SFD Timouts are, at least partially, caused by false detection of Wi-Fi frames for UWB Preambles.

*3. The payload is particularly vulnerable depending on the data rate and length*

Correlating to the results discussed in Section 3.3, the TU Graz recognized a substantial proportionality of the PER and the amount and rate of data being sent in each UWB frame.

#### Wi-Fi 6E impact as a function of different PHY settings

Another compelling measurement of the TU Graz has been investigating UWB performance coexisting with Wi-Fi 6E using different UWB PHY settings. The Figure 3.33 reveals the results of an extensive combination of the Preamble-Symbol-Repetition rate (PSR), introduced in Chapter 1, Section 3.2.3.1, the data rate, and payload length.

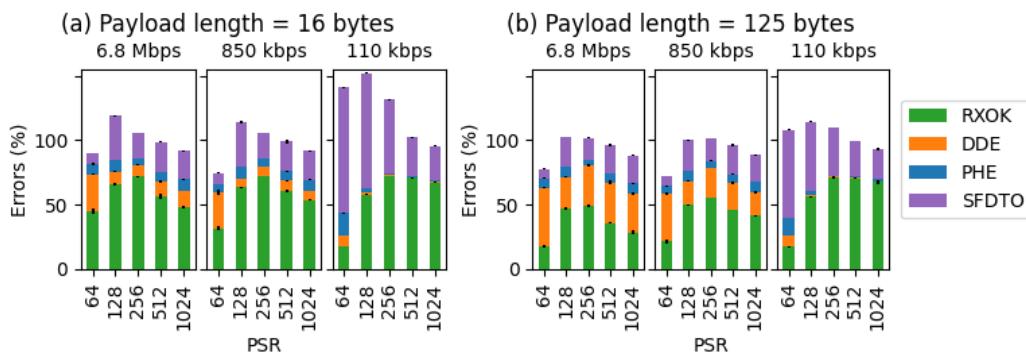


Figure 3.33: Influence of UWB PHY Settings Variation on PER

RXOK - SUCCESSFULL RECEPTION ; DDE - DATA DECODING ERRORS ; PHE - PHR (DATA HEADER) ERROR ; SFDTO - SFD TIMEOUT

While it has been stated by [11] that an increase of PSR increases the robustness of UWB communications, under the presence of Wi-Fi 6E traffic, this seemingly does not hold anymore. The institute of Technical Informatics found that the length of the preamble, proportional to the PSR, increases reliability but also the probability of potential Wi-Fi 6E hits. Figure 3.33 (b) shows that a lower data rate of 110 kbps increases robustness even with a longer payload. This correlates with a higher PRF used at lower data rates proportional to the pulses transmitted per symbol, which increasing reliability.

## **Chapter 4**

# **Narrowband Cancellation Filter**

This chapter discusses the implementation, testing, and results of a Narrowband Interference Cancellation block to counteract the effects of Wi-Fi 6E on UWB. The NBIC block is a complex unit used to identify narrowband interferers in a received ultra-wideband signal and cancel them by applying a digital Filter. The block contains a Jammer Detection and Frequency Estimation Unit that detects the presence of a jamming signal and estimates its center frequency.

# 1 Introduction and Fundamentals

Initially intended for narrowband interferers in lower spectral regions, this block is already built into the NCJ29D5 signal processing unit. Nevertheless, it has proven to work very effectively against Wi-Fi jammers. The fundamental building blocks consist of a *Signal mixer*, *Band-Stop Filter*, *Frequency Estimation*, *Jammer Detection Unit*, and *the State Machine*.

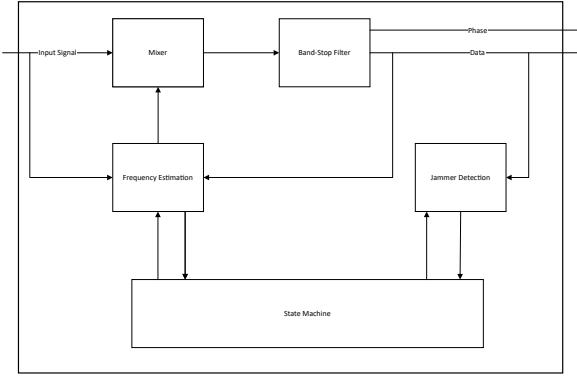


Figure 4.1: Schmematic Build up

Initially the *Frequency Estimation Unit* is applied to correlate deviations of the input data. The incoming signal is demodulated and differentiated by a delay-demodulator. The pulse from a pure Ultra-Wideband signal will naturally dissolve into a wide spread of frequencies, meaning the variation of occurring frequencies will become relatively large.

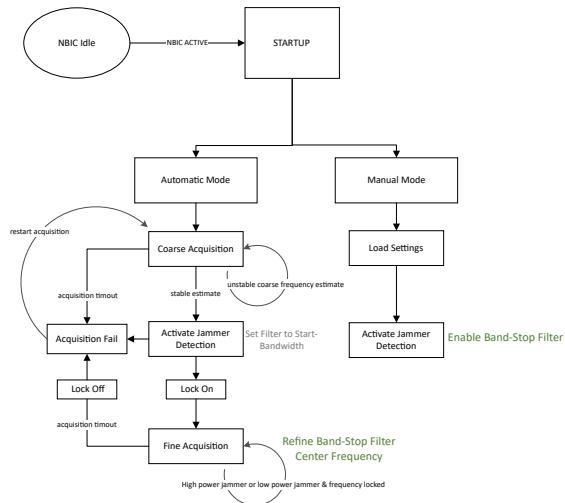


Figure 4.2: NBIC - Statemachine

If a narrowband jammer is present, the variation of demodulated frequencies will become relatively small within a specific range. This will trigger the *Jammer Detection unit*, which will compare the spectral energy density of the signal for a refined bandwidth in the region of the frequency estimate. A jammer is present if the signal's energy is higher than an expected threshold. The band-stop filter, designed after Kaiser's filter-sharpening method [14], will then be activated, and the *State Machine* will proceed to the *Fine Acquisition State*. The NBIC block will proceed in "locked-on" mode. If, however, the jammer detection unit does not detect the presence of a jammer, the machine will jump back to restart the *Coarse Acquisition State*. This concludes the *Automatic Mode*.

Additionally, a *Manual-Mode* is also available where the *Jammer Detection unit* is always locked on, meaning the bands-stop filter is always enabled and set to the previously defined bandwidth. This mode allows precise filtering when the jammer frequency is known and demonstrates the performance of the digital band-stop filter.

## 2 Implementation

The Narrowband Interference Cancellation Block has four different input parameters used for configuration. Previously introduced, the *Frequency Estimation unit* can be set to start approximations of the jammer frequency at a certain *Starting Point - Frequency*  $f_0$ . A good starting point increases the performance of the NBIC. Therefore, if the jammer frequency is approximately known, the NBIC results can significantly improve.

Another parameter is the *Filter Type*  $T_{Filter}$ . The NBIC features two different digital filters: a *linear* and a *phase filter*. However, only the *Linear Filter* will be discussed here since the phase filter only offers a minimal bandwidth and is therefore not applicable in this use case.

$$T_{Filter} \begin{cases} linear, \\ phase \end{cases} \quad (4.1)$$

$$f_0 \in [6000MHz, 7000MHz] \quad (4.2)$$

The *linear Filter* offers a *Filter Bandwidth*  $B_{Filter}$  configuration of four stop-bands, which have to be configured previously. In addition, as touched on in Figure 4.2, the NBIC offers different *NBIC operation modes*  $M_{NBIC}$ .

$$B_{Filter} := \{27MHz, 54MHz, 108MHz\} \quad (4.3)$$

$$M_{NBIC} \begin{cases} Manual \\ Automatic \end{cases} \quad (4.4)$$

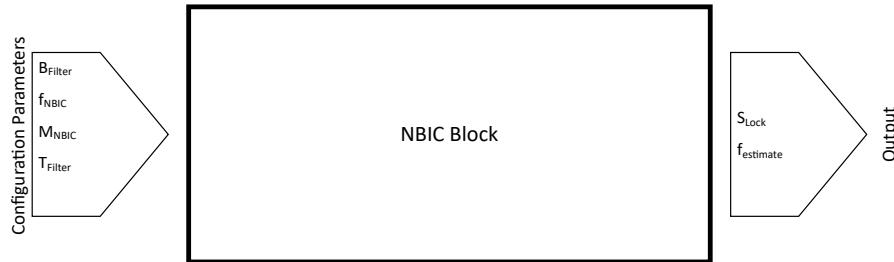


Figure 4.3: NBIC Block - Input & Output Parameters

The NBIC block returns the *Frequency Estimate*  $f_{estimate}$  and the *NBIC Lock State*  $S_{Lock}$  to the user.

$$S_{Lock} := \begin{cases} 0, & NBIC \text{ unlocked} \\ 1, & NBIC \text{ locked} \end{cases} \quad (4.5)$$

$$f_{estimate} \in [5500 MHz, 7500 MHz] \quad (4.6)$$

### 3 Measurements

A new measurement series has been conducted to investigate the performance of the Narrowband Interference Cancelation block as a countermeasure for better UWB performance in the presence of Wi-Fi 6E. All possible combinations of different NBIC settings given the parameters above have been investigated in this series. In order to avoid redundancy, only the most relevant results will be discussed here.

#### 3.1 Results

The most significant results to demonstrate the performance of the NBIC Block are the measurements on the Wi-Fi 20 MHz and 160 MHz channels.

##### 20 MHz Wi-Fi Channel Bandwidth NBIC Automatic Mode

The measurement has been executed with the following NBIC settings:

$$B_{Filter} = 27 \text{ MHz} \quad f_0 = 6600 \text{ MHz} \quad T_{Filter} = \text{Linear} \quad M_{NBIC} = \text{Automatic} \quad (4.7)$$

The aim was to investigate the performance and behaviour of the NBIC under the influence of different Wi-Fi 6E data rates. Figure 4.4 (a) displays the behaviour of the PER during the measurement, while (b) shows the two return values  $S_{Lock}$  and  $f_{estimate}$  of the NBIC over time.

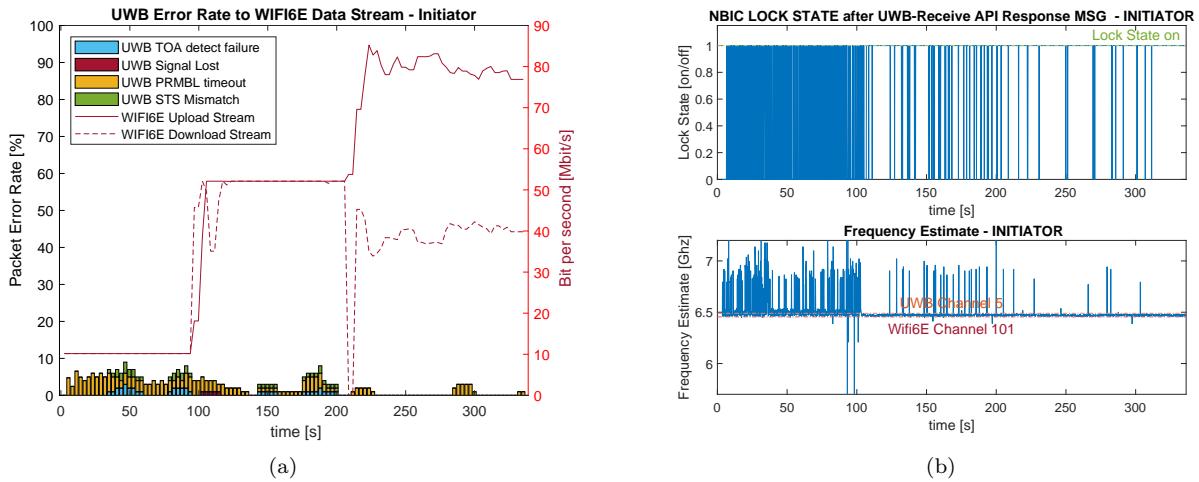


Figure 4.4: NBIC Automatic Mode - 20 MHz Wi-Fi Channel

A very interesting trend becomes visible as the Wi-Fi data rate is gradually increased. Contradicting the previous results from measurements without the NBIC Block active, the PER actually decreases with an increase of Wi-Fi 6E signal strength. Also, as is clearly seen in Figure (b) the lock state becomes more stable, meaning "lock-on"  $S_{Lock} = 1$  is held for longer periods, and the frequency estimate gets closer to the jammer center frequency  $f_{estimate} \approx 6495 \text{ MHZ}$ . Generally, the NBIC Block performs exceptionally well in mitigating the effects of Wi-Fi 6E

on UWB ranging. As the PER graph reveals, UWB communication is working seemingly without greater disruption at very high Wi-Fi data rates.

### 160 MHz Wi-Fi Channel Bandwidth - NBIC Automatic Mode

The measurement has been executed with the following NBIC settings:

$$B_{Filter} = 108 \text{ MHz} \quad f_0 = 6500 \text{ MHz} \quad T_{Filter} = \text{Linear} \quad M_{NBIC} = \text{Automatic} \quad (4.8)$$

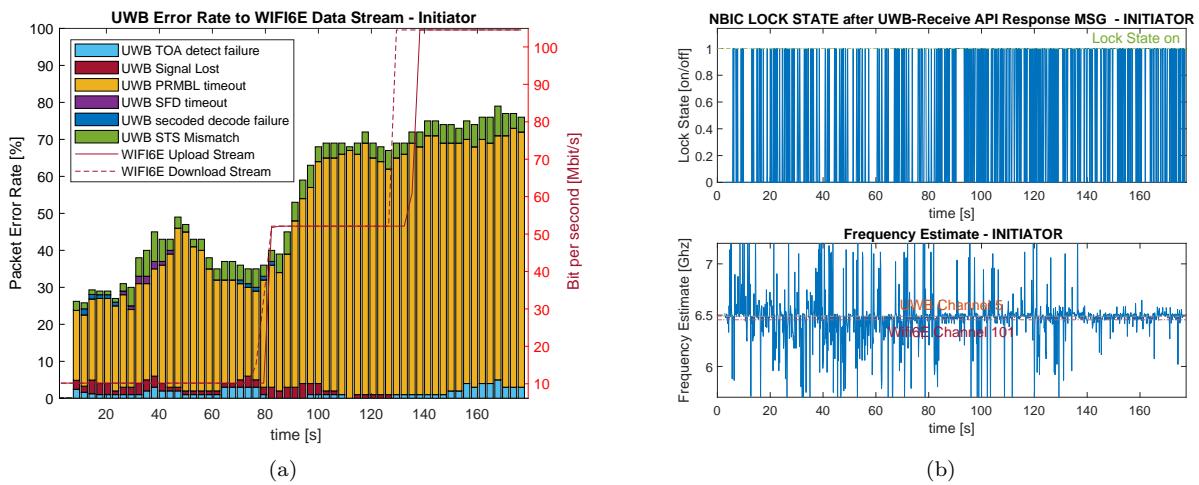


Figure 4.5: NBIC Automatic Mode - 160 MHz Wi-Fi Channel

As evidenced by Figure 4.5 above, the NBIC Block automatic mode cannot counteract the severe effects of a Wi-Fi 160 MHz Channel against UWB. While we see a similar PER distribution as in previous measurements, the resulting NBIC output does not promise any improvement either. We can see the frequency estimate getting better with an increase in signal strength, but the lock state reveals that the NBIC block does not seem to catch onto the Wi-Fi jammer.

### 160 MHz Wi-Fi Channel Bandwidth - NBIC Manual Mode

The measurement has been executed with the following NBIC settings:

$$B_{Filter} = 108 \text{ MHz} \quad f_0 = 6495 \text{ MHz} \quad T_{Filter} = \text{Linear} \quad M_{NBIC} = \text{Manual} \quad (4.9)$$

After the *Automatic Mode* failed to improve the UWB - Wi-Fi coexistence condition for the 160 MHz Channel, next, the *Manual Mode* was tested. The *Starting Point - Frequency*  $f_0$  has been set at proximity to the Wi-Fi jammer center frequency, and the widest linear filter bandwidth was applied.

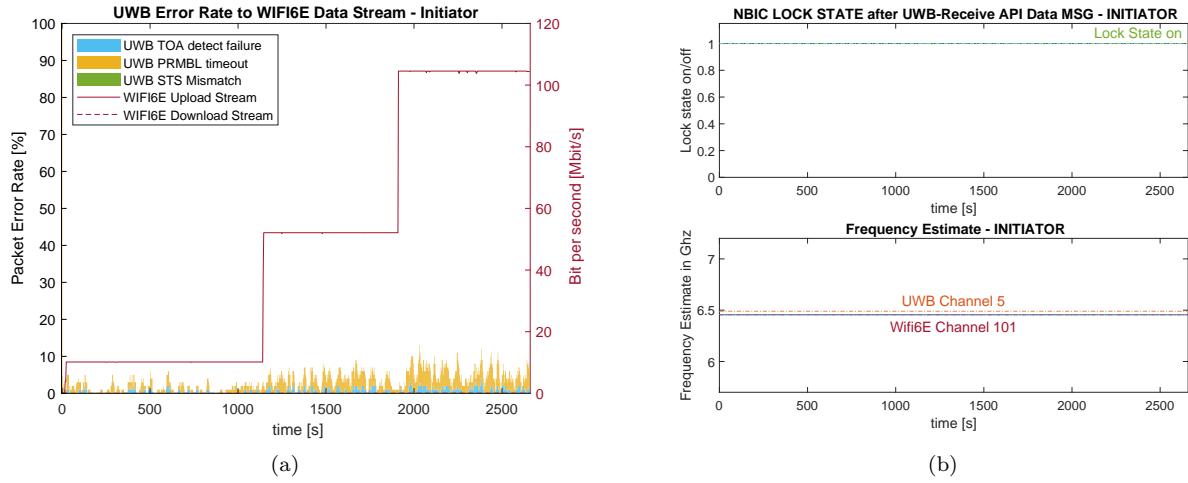


Figure 4.6: NBIC Manual Mode - 160 MHz Wi-Fi Channel

Through the measurement it becomes evident that the digital filter of the NBIC Block performs remarkably well when manually set at its optimal position. Even with an increasing data rate, the PER stays very low.

### 3.2 Discussion

On first impression the results, the NBIC technology, even though initially not intended for use against Wi-Fi 6E, seems very promising. At least for the 20 MHz Wi-Fi channels, the NBIC proposes an effective countermeasure. As for the 160 MHz bandwidth channel, a theory of why we see such poor performance in the *Automatic Mode* can be deducted from a closer look at the spectral trace of the two channels compared in the Figure 4.7 below.

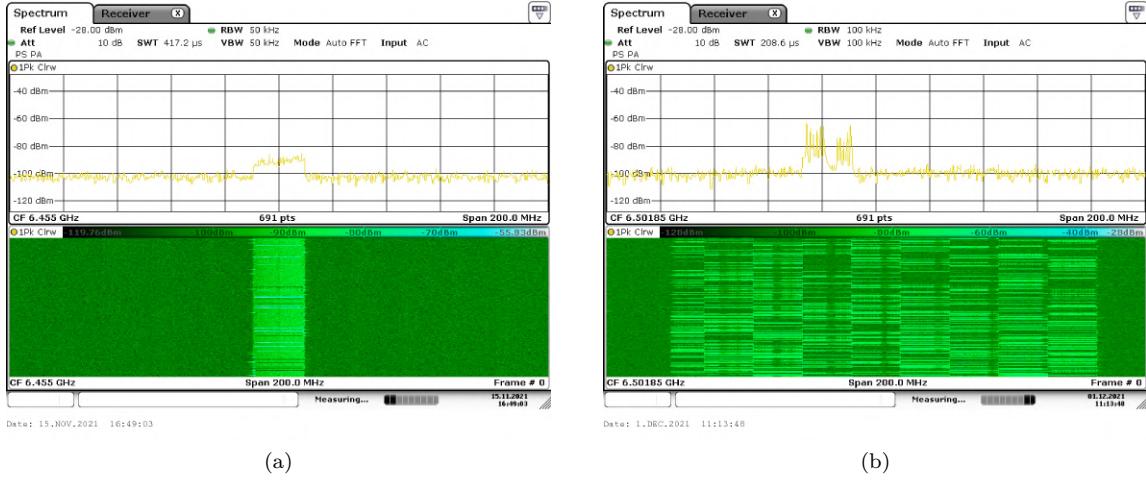


Figure 4.7: Comparison 20 MHz to 160 MHz Wi-Fi Channel

On the left side (a), a captured snapshot of the Wi-Fi 20 MHz Channel is shown at a very consistent data rate of 100 Mbits. The snapshot was taken from the spectrum analyzer during the first measurement (Figure 4.4). The signal has a high duty cycle, and just by observation, the frequency variation within the jammer signal can be assumed to be relatively low. In conclusion, this would mark an ideal case for the NBIC *Frequency Estimation Unit*, which consequently should result in a reasonably stable estimate, as we can see in Figure 4.4. Given a high spectral energy density within the specified band region, the jammer detection unit locks on to the jammer and applies the band-stop filter, which reduces the PER by about 40 % and 20 % for Initiator and Responder, respectively.

As already discussed in Chapter 3, Section 2.2 the 160 MHz channel is compositely assembled out of eight 20 MHz channels that follow a specific frequency-hopping pattern for data transmission.

Recalling that the NBIC Block during the *Coarse Acquisition State* tries to identify a bandwidth with a low-frequency variation using the delay-demodulator, a hypothesis could be that due to a high variation of occurring frequencies within the jamming signal in the 160 MHz case, the *State Machine* rarely proceeds into the *Jammer detection* and *Fine Acquisition State*. Consequently, the lock state is jittering between 0 and 1, leading to the band-stop filter not being applied most of the time. Concluding the theory, as Figure 4.6 proves, a simple application of the filter, even at a coarse estimate, would mitigate the interference due to Wi-Fi 6E, but the state machine is not proceeding to a successful jammer detection state when the band-stop filter is applied.

## **Chapter 5**

# **Conclusions**

This last chapter briefly evaluates the experimental design, measurements, results, and outcomes. Referring to Chapter 1, Section 1.2, this chapter will attempt to answer the central inquiries.

Further, an outlook on the proceedings of the investigations of the coexistence of Wi-Fi 6E and UWB is discussed. In short, two potential strategies are offered to follow up on the outcome of this thesis to mitigate the effects of Wi-Fi 6E on UWB and enable secure ranging under all circumstances.

# 1 Evaluation

Overall the investigations into the coexistence of UWB and Wi-Fi 6E can be described as a success at this stage. Referring to the expectations identified in Chapter 1, Section 1.2, it can be stated that the outcome of this thesis has exceeded the expectations. The reproduction of the interference case of WI-Fi 6E and UWB reliability has been achieved. Also, a test set-up has been developed that can work consistently. This has been broadly explored.

## 1.1 Coexistence Measurements

Does Wi-Fi 6E affect UWB communication and ranging performance? If so, how severe is the impact?

It is evident from the investigations undertaken that Wi-Fi 6E has a extremely severe impact on UWB signals. Observing the  $PER_{max} \approx 90\%$  and  $PER_{mean} \approx 75\%$  for the 160 MHz channel, one may conclude that the high Wi-Fi transmit power paired with wide channel bandwidth raises serious concerns for future automotive PKE and other UWB systems.

How does the packet error/reception rate behave as a function of Wi-Fi data traffic and channel bandwidth?

As Chapter 3, Section 2.1.1, shows, we obtain a strong correlation between Wi-Fi data rate and UWB PER. An increase in Wi-Fi data rate is proportional to an increase in the UWB PER. The channel bandwidth holds a similar relationship, yet the difference is only slightly notable for the 80 MHz to 160 Mhz channel.

Can we improve UWB ranging in Wi-Fi 6E presence by choosing a better protocol?

Chapter 3, Section 3.3, suggests that a tight synchronisation pattern can improve ranging performance due to reduced chance for invalid reception of Wi-Fi traffic for UWB frames and false detection of preamble symbols. Furthermore, Figure 3.30 reveals the possibility of utilizing a somehow simpler ranging protocol like TWR SS. Going from the "Take-What-We-Have" approach, a state machine could evaluate the current status bound to the PER and choose a less accurate but still valid protocol using the information that has been retrieved successfully to obtain a better estimate for a distance.

## 1.2 NBIC Performance

Can the NBIC block improve UWB performance as a permanent coexistence solution? If so, how good is the improvement?

The Narrowband Cancellation Block has proven an auspicious starting point for an effective countermeasure against Wi-Fi 6E. Chapter 4 shows that the NBIC block can mitigate the effects of Wi-Fi 6E for the smaller bandwidth channel at 20 MHz with a compelling performance of  $PER_{max} \approx 20 - 40\%$  to 0 - 5 % PER in automatic mode. For smaller Wi-Fi bandwidths, it can therefore be concluded that the NBIC block as it is, would provide a suitable solution.

For the more extensive bandwidth at 80 MHz and 160 MHz, the NBIC block achieved no improvement at all. Nevertheless, Chapter 4, Section 3.1, proves that the band-stop filter can decrease the PER by approximately 75%, if configured manually. This suggests that through a further improvement of the state machine and NBIC block, the automatic mode might be capable of filtering 160 MHz entirely, thus providing a compatible solution for the challenge of UWB and Wi-6E coexistence.

## 2 Outlook

The mitigation of Interference of Wi-Fi 6E and UWB will be an ongoing concern in the future. As Figure 2.5 has already highlighted, the demand for Wi-Fi bandwidth and usage is only going to increase in years to come, and so is the data traffic sent over the channels. The coexistence of UWB with Wi-Fi 6E and possible other Wi-Fi standards will be crucial as UWB is used these days in many other applications apart from the automotive industry. Any further development of this current test set-up will offer a beneficial contribution to continual investigation.

For further investigation, this thesis suggests two methods:

- *Correlating the level of PER to specific ranging protocol*

According to the reliability of service and reception, protocols using greater or lesser ranging frames should be implemented. As the statistics in Figure 3.30 show, still a reasonable amount of TWR-DS frames pass through, which may be used to the accurate distance, while TWR-SS ranging rounds can be taken for position tracking. A classification of ranging results may then be implemented.

- *Investigating further into the accuracy of the frequency estimation and jammer detection unit and the process or the state machine*

Seemingly the NBIC filter has high potential. The data in Chapter 4, Section 3.1 suggests that this feature can be improved.

## **Chapter 6**

## **Appendix**

## 1 Abbreviations

ADC	Analog-Digital Converter
AWGN	Additive White Gaussian Noise
ADC	Analog-Digital Converter
AWGN	Additive White Gaussian Noise
BPM	Burst Position Modulation
BPM-BPSK	Burst Position Modulation and Binary Phase-Shift Keying
BPSK	Binary Phase-Shift Keying
CFO	Center Frequency Offset
CIR	Channel Impulse Response
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
IC	Integrated Circuit
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ITU	International Telecommunication Union
LOS	Line-Of-Sight
MIMO	Multiple Input - Multiple Output
MU-MIMO	Multi-User Multiple-Input Multiple-Output
NBIC	Narrowband Interference Cancelation
NLOS	Non-Line-of-Sight
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OOK	On Off Keying
OOK	On-Off Keying
OWR	One-Way Ranging
PCB	Printed Circuit Board
PG	Processing Gain
PHR	Physical Layer Architecture Header
PHY	Physical Layer
PKE	Passive-Keyless Entry
PPM	Pulse-Position Modulation
PRF	Pulse Repetition Frequency

PSDU	PHY Service Data Unit
RF	Radio Frequency
RLAN	Radio Local Area Network
RS	Reed-Solomon
RSSI	Received Signal Strength Indicator
SECDED	Single Error Correct, Double Error Detect
SFD	Start of Frame
STS	Secure Time Stamp
TOA	Time of Arrival
TOF	Time of Flight
TWR-DS	Two-Way Ranging Double Sided
TWR-SS	Two-Way Ranging Single Sided
UNB	Ultra-Narrowband
UWB	Ultra-Wideband

# List of Figures

1.1	C-Band Weather Radar Interference [30]	8
1.2	UWB PKE - Worst Case Scenario	9
2.1	Signal Multipath Propagation [3]	12
2.2	(a) Constructive and (b) Destructive Interference Case Signal of Path I(blue), Signal of Path II(dotted orange), Superposition of both Signals(black)	13
2.3	Conventional Energy Detector [17] Signal of Path I(blue), Signal of Path II(dotted orange), Superposition of both Signals(back)	13
2.4	SNR	14
2.5	IoT Market Development [29]	15
2.6	Wi-Fi Timeline [22]	16
2.7	Dist. Wi-Fi Frame Types [5]	16
2.8	OFDM - Visualisation of In-band Carrier Allocation [20]	17
2.9	Wi-Fi - Spatial Distribution	17
2.10	Wi-Fi 6E - Channel Map [22]	18
2.11	Schematic of Macconi's Spark Gap Transmitter [19]	19
2.12	IEEE UWB Reference Pulse in Time and Frequency Domain [28]	19
2.13	Comparison of UNB to UWB [28]	20
2.14	Comparison of UNB to UWB with AWGN[28]	20
2.15	Comparison of UWB with other Narrowband and Wideband technologies [17]	21
2.16	UWB Transmitter - Local Oscilator for the Carrier Frequency & Pulse Generator [25]	23
2.17	IEEE Reference Pulse multiplied with Carrier Frequency at 4492.8 MHz [25]	23
2.18	UWB Ternary Pulse [25]	24
2.19	IEEE UWB Standard Frame [1]	25
2.20	UWB Frame SYNC Field [1]	25
2.21	First four UWB Ternary Pulse of Symbol of Code index 12 : -+0++000000-0+0-+0---++00- +0++0+0+000-0 0-00-+00+-++000-+-0-++0-0+++0-00-0++00+0+ 00++-00+000+-000-0- +0000-0000-0+00000+ [1]	26
2.22	UWB SYNC Field [1]	27
2.23	UWB Preamble & SFD	27
2.24	UWB UWB-Frame-StandardNoStandard	27
2.25	UWB Payload Modulation [25]	28
2.26	UWB PSDU Ecoding [25]	28
2.27	On-Off Keying Modulation [17]	29
2.28	Pulse-Position Modulation [17]	29

2.29	Pulse-Position Modulation [17] . . . . .	30
2.30	Burst Position Modulation and Binary Phase-Shift Keying [1] . . . . .	30
2.31	UWB Channel Impulse Response [8] . . . . .	31
2.32	UWB CIR at different TOA, inspired by [28] . . . . .	32
2.33	Read UWB CIR Estimate . . . . .	32
2.34	UWB Receiver . . . . .	33
2.35	(a) Single UWB Autocorrelation (b) Multiple UWB Autocorrelations . . . . .	33
2.36	Ranging Round : Two-Way Ranging Single Sided . . . . .	36
2.37	Ranging Round : Two-Way Ranging Double Sided . . . . .	37
3.1	NCJ29D5 - Ranger 4 Evaluationboard [27] . . . . .	39
3.2	Nighthawk - Netgear Rax500 [6] . . . . .	40
3.3	Wi-Fi 6E Channel Allocation [22] . . . . .	40
3.4	Wi-Fi 6E Network Card and Installment Process [6] . . . . .	41
3.5	Antenna Gain (a) and Surface Current (b) at 6.42 GHz [23] . . . . .	42
3.6	Line-Of-Sight Arrangement (a) Angle between Keyboard and Screen (b) . . . . .	42
3.7	Postion of the Laptop (left) and RSSI Value from Laptop plotted in dBm (right) . . . . .	43
3.8	Antenna Radiation Pattern: TDK Antenna (red) , Johannson Antenna (blue) . . . . .	43
3.9	Schema of test set-up including all components . . . . .	44
3.10	Photographs of the Test Set-up in the EMC Chamber . . . . .	44
3.11	Two-Way Ranging Double Sided - Protocol: Ranging Frames (red) & Data Frames (green) . . . . .	45
3.12	Ranging Frame . . . . .	45
3.13	Data Frame . . . . .	45
3.14	Design of Experiment . . . . .	46
3.15	<b>Grey Scale of UWB Error Codes accumulated at 160 MHz Wi-Fi 6E Channel Width</b> Wi-Fi 6E Upload Stream (solid line) , Wi-Fi 6E Download Stream (dotted line) . . . . .	48
3.16	Snapshot of the Wi-Fi 6E 160 MHz Channel captured on a Spectrum Analyzer : (a) at 10 M/bits and (b) at 300 Mbit/s Download rate . . . . .	49
3.17	UWB Channel Impulse Response (blue color scale) at 20 MHz Wi-Fi 6E Channel Width plotted over time and taps . . . . .	50
3.18	(a) CIRs - Wi-fi 6E 20 MHz bandwidth channel from Figure 3.17 (b) CIRs measured under equivalent circumstances without Wi-Fi 6E . . . . .	51
3.19	(a) Single CIR - Wi-fi 6E 20 MHz bandwidth channel from Figure 3.17 at 100 Mbit/s Data Rate (b) Single CIR measured under equivalent circumstances without Wi-Fi 6E . . . . .	51
3.20	PER distinguished between different UWB Error Codes - Measurement at 160 MHz Wi-Fi 6E Channel Width with a Variation of the Data Rate . . . . .	52
3.21	160 MHz Channel Bandwidth - Initiator and Responder . . . . .	54
3.22	80 MHz Channel Bandwidth - Initiator and Responder . . . . .	55
3.23	40 MHz Channel Bandwidth - Initiator and Responder . . . . .	55
3.24	20 MHz Channel Bandwidth - Initiator and Responder . . . . .	56
3.25	All Wi-Fi Channel Bandwidths compared - Initiator and Responder . . . . .	56
3.26	Wi-Fi 6E Channel Bandwidth . . . . .	58
3.27	Preamble Time Out - Error Scenario . . . . .	59
3.28	Reed-Solomon decode failure UWB Reception Error Scenario . . . . .	60
3.29	Two Way Ranging Double Sided - Synchronous Protocol . . . . .	62
3.30	Two Way Ranging Double Sided - Synchronous Protocol . . . . .	63

3.31 Two Way Raning Double Sided Synchronous Protocol . . . . .	64
3.32 Oscilloscope traces of captures UWB - Wi-Fi 6E collisions [4] . . . . .	65
3.33 Influence of UWB PHY Settings Variation on PER RXOK - SUCCESSFULL RECEPTION ; DDE - DATA DECODING ERRORS ; PHE - PHR (DATA HEADER) ERROR ; SFDTO - SFD TIMEOUT . . . . .	66
4.1 Schmematic Build up . . . . .	68
4.2 NBIC - Statemachine . . . . .	68
4.3 NBIC Block - Input & Output Parameters . . . . .	69
4.4 NBIC Automatic Mode - 20 MHz Wi-Fi Channel . . . . .	70
4.5 NBIC Automatic Mode - 160 MHz Wi-Fi Channel . . . . .	71
4.6 NBIC Manual Mode - 160 MHz Wi-Fi Channel . . . . .	72
4.7 Camparison 20 MHz to 160 MHz Wi-Fi Channel . . . . .	73

# List of Tables

2.1 IEEE Channels . . . . .	24
2.2 IEEE 31 Characters Preamble Symbols [1] . . . . .	26

# Bibliography

- [1] Ieee standard for low-rate wireless networks. *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*, pages 1–709, 2016.
- [2] Itu radio regulations. *International Telecommunication Union*, Section VII.(Definition 1.166, Interference), 2016.
- [3] Heinrich Arbrüster and Gerhard Grünberger. *Elektromagnetische Wellen im Hochfrequenzbereich*. Hültig und Pflaum Verlag., 1978.
- [4] Hannah Brunner, Michael Stocker, Maximilian Schuh, Markus Schuß, Carlo Alberto Boano, and Kay Römer. Understanding and Mitigating the Impact of Wi-Fi 6E Interference on Ultra-Wideband Communications and Ranging. In *Proceedings of the 21<sup>st</sup> International Conference on Information Processing in Sensor Networks (IPSN)*. IEEE, May 2022.
- [5] David Coleman. *Wi-Fi 6 Extreme Networks Special Edition*. John Wiley and Sons Inc., 2020.
- [6] Federal Communications Commission. Nighthawk AXE11000 Tri-Band WiFi 6E Router. <https://fccid.io/PY320300508>, 2020. [Online; accessed 14-March-2022].
- [7] Normaln Ellis. *Elcteical Interference Handbook*. Newnes, 1998.
- [8] Michel Feldvoß. Durchführung einer machbarkeitsstudie zu einem intelligenten fahrzeugzugangssystem unter verwendung von uwb und ble, 2019.
- [9] Helge Fielitz. *Zuverlässige drahtlose Übertragung in maritimen Umgebungen unter Berücksichtigung komplexer metallischer Strukturen*. PhD thesis, Technische Universität Hamburg, 1st ed. Göttingen: Cuvillier Verlag, 2016.
- [10] William G. Hunter George E. P. Box, J. Stuart Hunter. *Statistics for Experimenters: Design, Innovation, and Discovery, Second Edition*. 2 edition, 2005.
- [11] Bernhard Großwindhager, Carlo Alberto Boano, Michael Rath, and Kay Römer. Enabling runtime adaptation of physical layer settings for dependable uwb communications. In *2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, pages 01–11, 2018.
- [12] Lee A Iacocca and William Novak. *Iacocca : an autobiography*. Bantam Books, Toronto , New York, 1984.
- [13] Recommendation ITU-R. Impact of devices using ultra-wideband technology on systems operating within radiocommunication services. *International Telecommunication Union*, 14:1–88, 05 2006.

- [14] J. F. Kaiser and R. W. Hamming. *Sharpening the Response of Symmetric Nonrecursive Filter by Multiple Use of Same Filter*. Bell Laboratories Education, Murray Hill, New Jersey 07974, 1977.
- [15] Dan Kreiser. *Optimierung und Erweiterung des IEEE 802.15.4a UWB-Standards für den Einsatz in Automatisierungssystemen*. PhD thesis, 05 2016.
- [16] GR.R. Leach and Editor MB Alexander. Electronic systems failures and anomalies attributed to electromagnetic interference. *NASA Reference Publication 1374*, 1995.
- [17] Faranak Nekogar. *Ultra-Wideband Communications*. Person Education Inc., 2006.
- [18] William R. Nelson. *Interference Handbook*. Radio Publications INC., 1990.
- [19] Homayoun Nikookar and Ramjee Prasad. Introduction to ultra wideband for wireless communications. 2008.
- [20] Electronic Notes. What is OFDM: Orthogonal Frequency Division Multiplexing. <https://www.electronics-notes.com/articles/radio/multicarrier-modulation/ofdm-orthogonal-frequency-division-multiplexing-what-is-tutorial-basics.php#.YMr-aHIp8.twitter>. [Online; accessed 13-April-2022].
- [21] Purple. History of WiFi. <https://purple.ai/blogs/history-wifi/?msclkid=26d99565b95111ec875d9473bb6d83ee>, 2014. [Online; accessed 11-April-2022].
- [22] Qorvo. Back to the Future: Wi-Fi Predictions from 15 Years Ago. <https://www.qorvo.com/design-hub/technical-articles/back-to-the-future-wi-fi-predictions-from-15-years-ago>, 2019. [Online; accessed 12-March-2022].
- [23] REMCOM. WiFi Antenna in Notebook. <https://www.remcom.com/examples/wifi-antenna-in-netbook.html>, 2022. [Online; accessed 14-March-2022].
- [24] Gernot Schmid Mobile Communicatios Satety. Exposition durch Ultra-Widband Technologien. <https://iot-analytics.com/number-connected-iot-devices/>, 2008. [Online; accessed 12-April-2022].
- [25] Mirko Schimkat. Schutz typischer passiver, schlüsselloser zugangssysteme für pkws mit sicherer ultra-breitband-distanzbegrenzung, 2018.
- [26] Maximilian Peter Schuh, Hannah Brunner, Michael Stocker, Markus Schüß, Carlo Alberto Boano, and Kay Uwe Römer. First steps in benchmarking the performance of heterogeneous ultra-wideband platforms. In *Proceedings of the 5th International Workshop on Benchmarking Cyber-Physical Systems and Internet of Things (CPS-IoTBench)*, May 2022. 5th International Workshop on Benchmarking Cyber-Physical Systems and Internet of Things : CPS-IoTBench 2022, CPS-IoTBench 2022 ; Conference date: 03-05-2022.
- [27] NXP Semiconductors. NCJ29D5: Trimension™ Evaluation Board for Automotive Ultra-Wideband. <https://www.nxp.com/products/wireless/secure-ultra-wideband-uwb/ncj29d5-trimension-evaluation-board-for-automotive-ultra-wideband:LID2435-R4>, 2022. [Online; accessed 14-March-2022].
- [28] Mahmoud Sherrah. Security implementation and validation for pke systems with rsd defense based on ranger4 uwb chip, 2019.

- [29] Satyajit Sinha. State of IoT 2021: Number of connected IoT devices growing 912.3 billion globally, cellular IoT now surpassing 2 billion. <https://iot-analytics.com/number-connected-iot-devices/>, 2021. [Online; accessed 12-March-2022].
- [30] Philippe Tristant. C-band meteorological radars - threats related to rlan 5 ghz. In *EUMETNET*, 2017.