Master of Science Thesis in Electrical Engineering
Department of Electrical Engineering, Linköping University, 2025

Investigating the Vulnerability of DM-RS in 5G NR to Different Interference Types

Amanda Fjellborg

LINKÖPING UNIVERSITY

Master of Science Thesis in Electrical Engineering

Investigating the Vulnerability of DM-RS in 5G NR to Different Interference Types

Amanda Fjellborg

LiTH-ISY-EX--25/5805--SE

Supervisor: **Adrian Edin**
ISY, Linköpings universitet
Kia Wiklundh
FOI – Swedish Defence Research Agency

Examiner: **Danyo Danev**
ISY, Linköpings universitet

Division of Communication Systems
Department of Electrical Engineering
Linköping University
SE-581 83 Linköping, Sweden

Abstract

With the release of 5G, society is becoming increasingly connected. The growing number of electronic devices emitting electromagnetic signals increases the risk of unintentional interference to wireless communication systems. As 5G New Radio (NR) grows beyond its commercial role to also support mission-critical services such as public safety and military communications, it places high demands on its reliability under interference. A key component in the 5G NR downlink is the Demodulation Reference Signal (DM-RS) of the Physical Broadcast Channel (PBCH), which enables accurate channel estimation and decoding. Disruption of this signal can severely degrade PBCH performance and jeopardize overall communication reliability.

This thesis investigates the robustness of 5G in the presence of different interference signals affecting the PBCH DM-RS. The study focuses on two interference types: additive white Gaussian noise (AWGN) and continuous wave (CW) signals. System performance is primarily evaluated through the bit error rate (BER) of PBCH, reflecting the overall channel performance under these conditions.

The analysis shows that CW interference generally degrades the PBCH DM-RS more than AWGN, particularly at higher E_b/N_I values. Additionally, a CW signal applied between subcarriers causes the interference to spread across multiple subcarriers, further reducing performance. Accurate estimation of key parameters via DM-RS is crucial, since errors can prevent proper PBCH operation regardless of interference conditions.

Acknowledgments

First and foremost, I would like to thank my supervisor at FOI, Kia Wiklundh, for hosting me during this thesis. Your guidance and encouragement have been invaluable throughout this process. I would also like to thank Sara Linder for participating in many interesting discussions that helped me move forward. Together, your assistance and advice have helped me stay on track and overcome challenges during the project. I also want to thank my supervisor, Adrian Edin, and my examiner, Danyo Danev, at Linköping University for their support and feedback on the report during this work.

Finally, I would like to thank my family and friends for all the support and encouragement you have given me along the way.

Linköping, September 2025
Amanda Fjellborg

Contents

Notation

Notations

Notation	Meaning
$\mathbb{N}$	Set of all natural numbers
A	Amplitude
f	Frequency
φ	Phase
$N_{\mathrm{ID}}^{\mathrm{cell}}$	Physical cell ID
v	Sequence parameter
$\bar{i}_{\mathrm{SSB}}$	Initialization parameter
i_{SSB}	SSB index
n_{hf}	Half-frame index
E	Output sequence length
n	Sample index
N_{FFT}	FFT size
m	Affected subcarrier
α	Frequency separation
E_b	Energy per bit
N_I	Interference power spectral density

Abbreviations

Abbreviation	Meaning
3GPP	Third Generation Partnership Project
5G	Fifth generation
AWGN	Additive white Gaussian noise
BER	Bit error rate
CW	Continuous wave
DL	Downlink
DM-RS	Demodulation reference signal
EMI	Electromagnetic interference
ISI	Intersymbol interference
LTE	Long Term Evolution
MMSE	Minimum mean square error
NR	New Radio
OFDM	Orthogonal frequency division multiplexing
PBCH	Physical broadcast channel
PCI	Physical cell ID
PDCCH	Physical downlink control channel
PDSCH	Physical downlink shared channel
PHY	Physical layer
PRB	Physical resource block
PSS	Primary synchronization signal
QPSK	Quadrature phase shift keying
RE	Resource element
SCS	Subcarrier spacing
SINR	Signal-to-noise-plus-interference ratio
SIR	Signal-to-interference ratio
SNR	Signal-to-noise ratio
SSB	Synchronization signal block
SSS	Secondary synchronization signal
UE	User equipment
UL	Uplink

1

Introduction

With the release of the Fifth Generation of Mobile Telephony, commonly known as 5G, an increasingly connected society is enabled. 5G has been developed to support different use cases families; Critical Communications (CC) & Ultra Reliable and Low Latency Communications (URLLC), Enhanced Mobile Broadband (eMBB) and Massive Internet of Things (mIoT). Together, these categories targets diverse markets like public safety, transport and logistics, automation and entertainment [1]. By 2027, 5G is expected to be the dominant subscription type [2].

The growing number of electronic devices emitting electromagnetic signals increase the risk of unintentional interference to wireless communication systems. As 5G becomes the dominant mobile technology, this will become a greater issue. This thesis will investigate the robustness of 5G in the presence of electromagnetic interference (EMI) affecting the Demodulation Reference Signal (DM-RS) associated with the Physical Broadcast Channel (PBCH).

1.1 Motivation

Beyond its commercial role, 5G is also expected to support mission-critical services such as public safety and military communications, making resilience to interference particularly important [3]. If 5G is to be relied upon in such critical applications, robust communication is needed. A crucial component of the 5G New Radio (NR) framework is the user-specific DM-RS, which is necessary for channel estimation and data decoding. Interference to DM-RS might compromise the reliability of 5G.

Figure 1.1 shows a scenario where there is downlink (DL) communication between a base station and user equipment (UE). The UE is in close proximity to other electrical devices that may emit at the DL frequencies used for communication, and therefore cause unintentional interference. Such passive emission

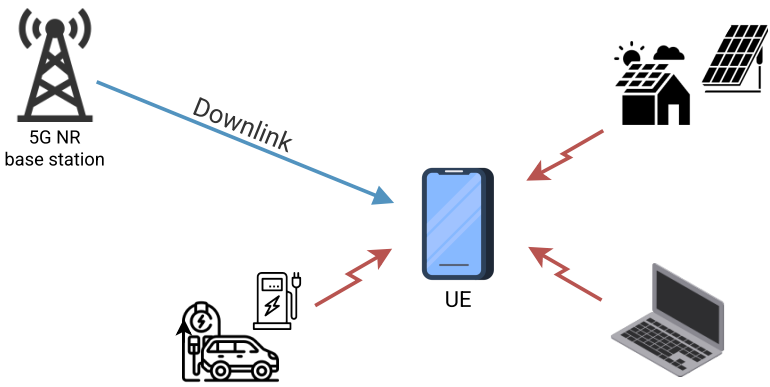


Figure 1.1: *Schematic picture of downlink communication in the presence of nearby electrical devices.*

can originate from devices like laptops, solar panels and charging stations. This has occurred in other domains, [4] mention cases where unintentional electromagnetic interference disrupted Air Traffic Control Communications, with consequences such as reduced communications range and resilience. Thus it is important to study interference effects on 5G, particularly on critical reference signals such as DM-RS.

1.2 Aim

The aim of this thesis is to investigate the vulnerability of 5G NR to unintentional interference. To achieve this, the response of PBCH and its associated DM-RS will be studied through simulations under different interference conditions. The resulting performance of PBCH in terms of bit error rate (BER) will be used to evaluate the robustness against different interference signals.

1.3 Research Questions

The thesis will focus on answering the following questions:

1. How does unintentional interference to PBCH DM-RS affect the performance of PBCH in 5G NR?

2. Which type of interference signal have the most significant impact on the robustness of PBCH DM-RS in 5G NR?

1.4 Delimitations

The problem will be investigated in a simulated environment, using a simplified 5G communications system and simulated interference signals rather than real-world data. The result will therefore be considered a conceptual demonstration on how different interference impact robustness.

Furthermore, the thesis will concentrate on DL communication as unintentional interference is most likely to affect a receiver in close proximity to emitting devices. While there are several functions and channels that may be affected by interference, the thesis will specifically examine the impact on PBCH and its associated DM-RS.

1.5 The Work in a Wider Context

The focus of this thesis is on unintentional interference which does not directly raise ethical dilemmas. The aim is to analyze unintentional interference to DM-RS, not causing disruption. Ethical issues arise in the case of intentional interference, used in for example military scenarios such as jamming. That is outside the scope of this thesis. This work is also limited to a simulated subsystem, meaning no actual networks have been affected.

The thesis does however point out the issues that unintentional interference signals can cause in society. A problem that is likely to increase as the number of electrical devices in society grows. With more possible interfering signals, there is a larger possibility that it affects everyday users who may experience issues with connectivity and performance. More critically, it could impact infrastructure and important societal functions such as emergency services, transport and healthcare.

2

Theory

This chapter presents the theoretical background of the thesis. Key elements of the 5G architecture are described as well as related work in the field.

2.1 Orthogonal Frequency Division Multiplexing

Orthogonal frequency division multiplexing (OFDM) is a digital modulation technique used in several wireless communications systems, including 5G, that employ multiple carrier transmission. That is, the available frequency band is divided into multiple subcarriers and information is transmitted on each subcarrier in parallel. This allows for greater spectral efficiency at a lower subcarrier data rate compared to single carrier systems [5].

Consider an OFDM system with N subcarriers, the modulator sums these together to form the modulated signal as

$$s(t) = \frac{1}{N} \sum_{k=0}^{N-1} X_k e^{j2\pi kt/T}, \quad 0 \leq t < T, \tag{2.1}$$

for data symbols $\{X_k\}$ and symbol duration T. In the kth subcarrier, $k = 0, 1, \ldots, N-1$, the carrier signal is

$$s_k(t) = \cos(2\pi f_k t) \tag{2.2}$$

with center frequency $f_k = k/T$. The crucial orthogonality between subcarriers is defined in Definition 2.1.

Definition 2.1 (Orthogonal Subcarriers [5]). Two adjacent subcarriers $s_k(t)$ and $s_j(t)$ with phases ϕ_k respectively ϕ_j are orthogonal over a symbol interval T if the

symbol rate is $1/T$ such that

$$\int_0^T \cos\left(2\pi f_k t + \phi_k\right) \cos\left(2\pi f_j t + \phi_j\right) dt = 0, \tag{2.3}$$

with frequency separation $f_k - f_j = n/T,\ n = 1, 2, \ldots, N-1$, independent of the phases.

The frequency separation n/T between subcarriers is commonly called *subcarrier spacing* (SCS). OFDM subcarriers have overlapping but non-interfering frequency spectra. This is illustrated in Figure 2.1, with SCS 15 kHz and carrier frequency 3.5 GHz. The center subcarrier, in yellow, has its peak at 3.5 GHz where all the other subcarriers are at its zero-crossing.

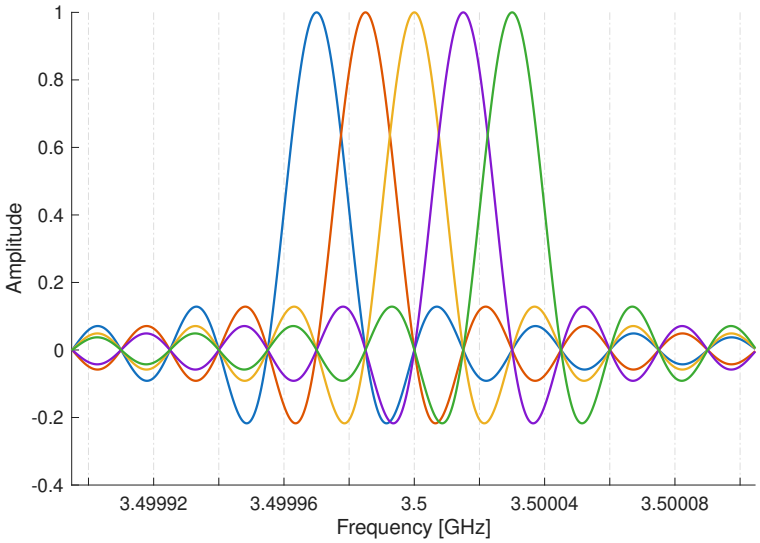


Figure 2.1: *OFDM subcarriers with overlapping frequency spectra.*

2.1.1 Intersymbol Interference & Cyclic Prefix

Single-carrier systems are susceptible to intersymbol interference (ISI) caused by multipath distortion. This occurs when multipath propagation due to e.g. reflections lead to signals arriving at the receiver via different paths with different delays. These delayed versions of the signal can overlap with subsequent symbols, causing distortion. A multi-carrier system such as OFDM has a lower data rate compared to a single-carrier system. This increases the symbol duration for each subcarrier. A longer symbol duration corresponds to a narrower bandwidth per subcarrier, which decrease the signal overlap within one symbol period. To further mitigate ISI, OFDM inserts a cyclic prefix between symbols that serves

as a guard interval against interference. For an OFDM symbol consisting of N signal samples $\{x_0, x_1, \ldots, x_{N-1}\}$, the last ν samples $\{x_{N-\nu}, x_{N-\nu+1}, \ldots, x_{N-1}\}$ are copied and appended to the beginning of the symbol, increasing the total symbol duration to $N + \nu$ samples. ISI is eliminated when cyclic prefix duration exceeds the multipath delay [5].

2.2 5G

5G was fully specified by the Third Generation Partnership Project (3GPP) in 2019 to replace the previous generation of cellular technology, 4G Long-Term Evolution (LTE). A key concept is the new radio transmission technique – 5G NR. A 5G system consists of three main parts: user equipment (UE), next-generation radio access network (NG-RAN) with NR base stations (gNodeB), and 5G core network (5GC). Communication in the NG-RAN is organized through a layered protocol stack [1, 6].

This thesis focuses on layer 1, the physical (PHY) layer, as it is the primary layer that interacts directly with the radio environment. It is specified through key components such as waveform, frame structure, modulation schemes, channel coding and reference signals for both downlink (DL) and uplink (UL) [7]. The focus will be on the DL.

2.2.1 Frame & Resource Structure

5G NR uses OFDM with cyclic prefix. One of the advancements with 5G is its flexible numerology, allowing different SCS to support diverse use cases. The available SCS are listed in Table 2.1.

Table 2.1: *5G numerology [6, 7].*

Subcarrier Spacing [kHz]	Cyclic prefix	Slots per subframe	Frequency range
15	Normal	1	FR1
30	Normal	2	FR1
60	Normal/ extended	4	FR1 and FR2
120	Normal	8	FR2
240	Normal	16	FR2
480	Normal	32	FR2
960	Normal	64	FR2

Transmission is organized into 10 ms frames, each divided into ten 1 ms subframes. A subframe is in turn divided into a number of slots that depends on the SCS, see Table 2.1. For a normal cyclic prefix each slot is 14 OFDM symbols, in the case of a extended cyclic prefix a slot instead contains 12 OFDM symbols. A higher SCS gives both a shorter slot and cyclic prefix duration [7].

A time-frequency resource grid in 5G NR spans up to 3300 subcarriers and is divided into physical resource blocks (PRBs) of 12 consecutive subcarriers in frequency domain. The smallest available unit, a resource element (RE), is defined as one subcarrier in frequency domain by one OFDM symbol in time domain. This grid forms the foundation for mapping physical channels and signals.

Figure 2.2 illustrates how the 5G NR frame changes with the SCS. The time-frequency resource grid is also depicted.

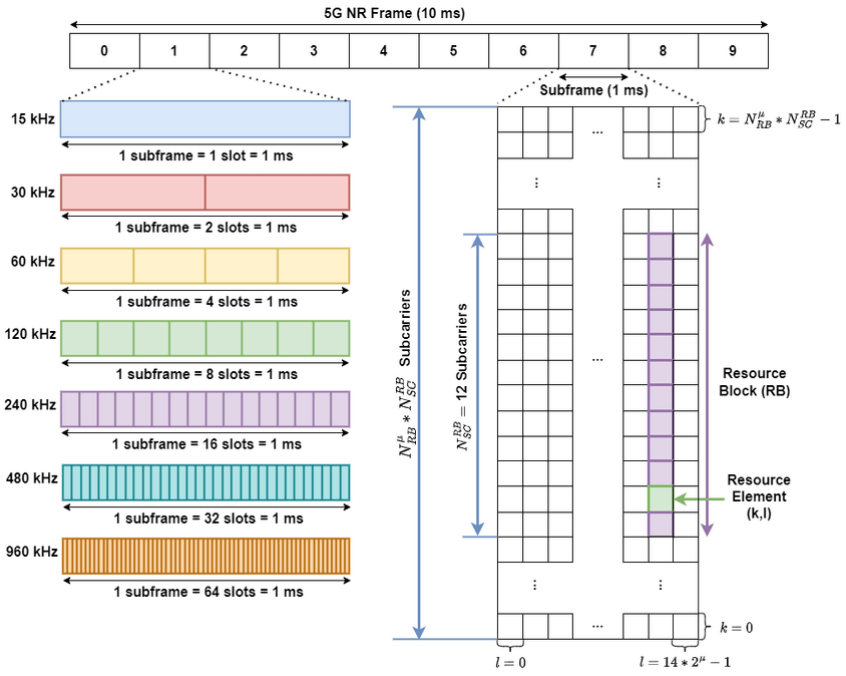


Figure 2.2: *5G NR frame structure and time-frequency resource grid [8]. In the resource grid, l and k are number of symbols and subcarriers, respectively. The numerology is given by μ. The number of subcarriers are decided by number of subcarriers per RB (N^{RB}_{sc}) and number of RBs for the given numerology (N^{μ}_{RB}).*

2.2.2 Physical Channels & Signals

In the DL, a physical channel is a set of REs carrying information, while a physical signal does not carry any data but is used by the physical layer [7]. The physical channels are [9]:

- **Physical Downlink Shared Channel (PDSCH)** which represent the bulk of the frame and is mainly used for data transmission
- **Physical Downlink Control Channel (PDCCH)** which is used for downlink control information such as scheduling decisions

- **Physical Broadcast Channel (PBCH)** that carries system information used by a UE to access the network

Channels are subject to coding for error protection and modulation that maps the channel coded binary sequence onto a waveform [10]. PBCH uses the modulation technique Quadrature Phase Shift Keying (QPSK) and polar coding [7, 11]. QPSK is visually demonstrated in Figure 2.3, showing four phases that can encode two bits per symbol.

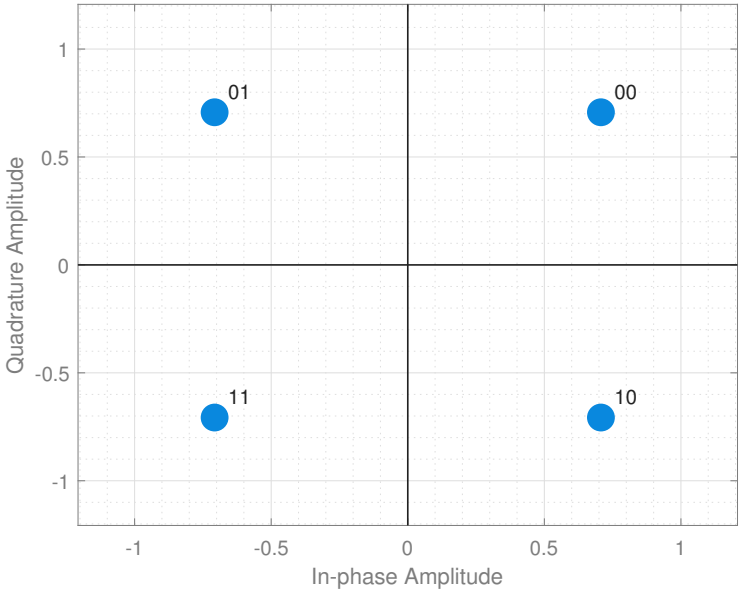


Figure 2.3: *QPSK constellation diagram with modulated symbols.*

The physical signals include the primary synchronization signal (PSS), secondary synchronization signal (SSS) and demodulation reference signals (DM-RS) for PDSCH, PDCCH and PBCH each [7]. In 5G NR, the DM-RS are both channel- and user-specific and are transmitted only when needed in the same resource blocks as the corresponding channel. Their purpose is to enable accurate channel estimation at the receiver [9].

The PBCH and its associated DM-RS together with PSS and SSS form the synchronization signal block (SSB), consisting of 4 OFDM symbols by 240 subcarriers [7]. Its time-frequency structure can be seen in Figure 2.4 and the resource mappings in Table 2.2. The SSB is the fundamental building block used by UEs to perform initial cell search, synchronization and acquire system information. The PBCH carries the minimum system information necessary for a UE to access the network, such as initial configurations for PDCCH, PDSCH and DM-RS. To accurately decode PBCH, its associated DM-RS acts as a known reference signal

that the receiver can use for channel estimation [6, 9]. The channel estimation is described in Section 2.2.3.

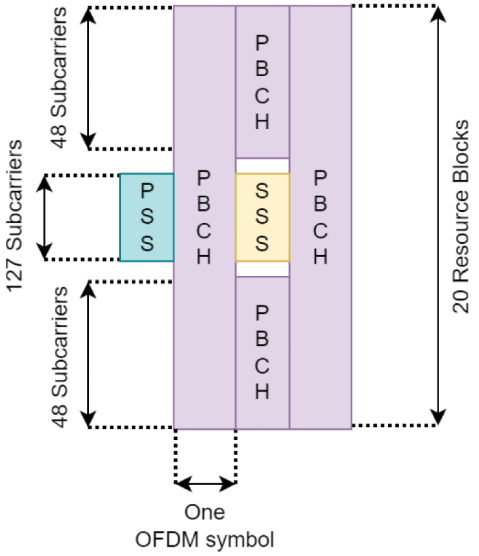


Figure 2.4: *Structure of SSB [8].*

Table 2.2: *Resource allocation within SSB, numbering relative to the start of an SSB [7, Tab. 7.4.3.1-1].*

Channel or signal	**OFDM symbol** l	**Subcarrier** k
PSS	0	$56, 57, \ldots, 182$
SSS	2	$56, 57, \ldots, 182$
No signal	0	$0, 1, \ldots, 55, 183, 184, \ldots, 236$
	2	$48, 49, \ldots, 55, 183, 184, \ldots, 191$
PBCH	1, 3	$0, 1, \ldots, 239$
	2	$0, 1, \ldots, 47, 192, 193, \ldots, 239$
DM-RS for PBCH	1, 3	$0 + v, 4 + v, 8 + v, \ldots, 236 + v$
	2	$0 + v, 4 + v, 8 + v, \ldots, 236 + v$ $192 + v, 196 + v, \ldots, 236 + v$

According to Table 2.2, the location of PBCH DM-RS depends on the parameter v which is calculated as a function of the physical cell ID (PCI) $N_{\mathrm{ID}}^{\mathrm{cell}}$ [7]:

$$v = N_{\mathrm{ID}}^{\mathrm{cell}} \mathrm{mod} 4, \tag{2.4}$$

where mod denotes the modulo operation, i.e. v is the remainder of the division of $N_{\mathrm{ID}}^{\mathrm{cell}}$ by 4. That is, the DM-RS positions move along the frequency domain for different PCI values. In practice there are 4 possible configurations: $v = 0, 1, 2, 3$. The PBCH DM-RS symbol sequence is a function of $N_{\mathrm{ID}}^{\mathrm{cell}}$ and the initialization parameter $\bar{i}_{\mathrm{SSB}}$ which is calculated as

$$\bar{i}_{\mathrm{SSB}} = i_{\mathrm{SSB}} + 4n_{\mathrm{hf}}, \tag{2.5}$$

where i_{SSB} is the two least significant bits of the SSB index and $n_{\mathrm{hf}} \in \{0, 1\}$ is the half-frame index [7].

2.2.3 Channel Estimation

Channel estimation is essential for maintaining robust and reliable communication. Since the wireless channel often distorts the signals received by the device, accurate channel estimation is needed to counteract these distortions and interpret data correctly. DM-RS act as known reference or pilot signals which can be compared with the received signal. DM-RS provide a channel estimate at its locations in the resource grid, and through interpolation techniques the channel can be estimated at other time-frequency locations. By estimating the channel matrix, the effects of noise and interference introduced by the wireless channel can be equalized and reduced [12].

Channel estimation of PBCH is done through channel estimation at PBCH DM-RS locations followed by resource grid interpolation. During initial cell search, the PCI is estimated from PSS and SSS. Subsequently, the location of PBCH DM-RS is known and the received DM-RS signal can be extracted. All possible DM-RS sequence candidates are explored based on different values of $\bar{i}_{\mathrm{SSB}}$. These are compared with the received DM-RS signal and the sequence with the maximum correlation is chosen. This results in an estimated channel response across all DM-RS subcarrier that can be interpolated to other time-frequency locations. The channel response at the REs containing PBCH symbols (known from PCI) are then estimated through interpolation, resulting in a channel matrix the same size as the resource grid. Finally, the received signal is equalized with the channel matrix to compensate for the effects of the channel [12, 13].

2.3 Interference Model

Electromagnetic interference (EMI) refers to unwanted electromagnetic disturbance transmitted from one electronic device to another. EMI can arise from man-made sources like laptops, radios, medical equipment, power cables and solar cells. It causes degraded performance of the affected system, in communications systems this could be signal degradation or system failure [14]. This section outlines common models used to represent interference in communication systems.

In real-world communication systems, interference is present from thermal vibrations, electronic components and external sources. A widely used model

for this is additive white Gaussian noise (AWGN). It is characterized by samples that are independent and identically distributed (i.i.d.) with a constant power spectral density, i.e. equal power across the whole frequency spectrum [10].

Digital electronics, such as power converters, commonly use square waves as clock signals for synchronization. It is a periodic waveform that ideally transition instantaneously between two levels. In a theoretical ideal case, square waves consist of a wide range of harmonics, mathematically expressed as the sum of infinitely many sinusoidal components at different frequencies. An ideal square wave with amplitude 1 can be represented by the infinite Fourier expansion

$$x(t) = \frac{4}{\pi}\left(\sin(\omega t) + \frac{1}{3}\sin(3\omega t) + \frac{1}{5}\sin(5\omega t) + \ldots\right), \quad \omega = 2\pi f. \tag{2.6}$$

Figure 2.5 illustrates the multiple odd-frequency sinusoidal components that make up an ideal square wave. In real-world applications, these harmonic components may leak into nearby communication systems as EMI. Instead of receiving the full harmonic spectrum of a square wave, communications systems often experience narrow-band interference where one sinusoidal component at a specific frequency enter the systems. All communication systems are susceptible to these types of disturbances, particularly in environments where digital electronics generate strong clock signals. The scenario in Figure 1.1 portray such a case with strong clock signals generated by computers, charging stations and solar panels.

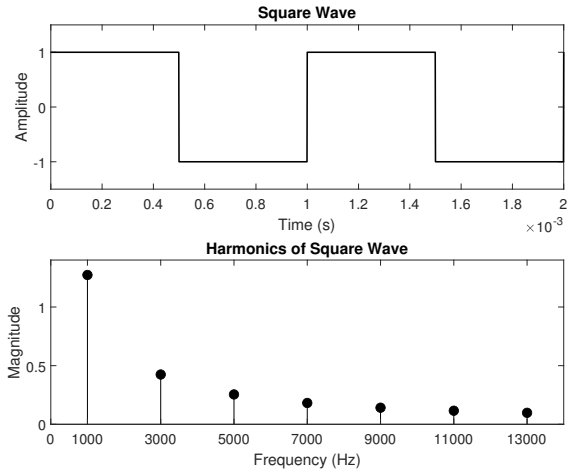


Figure 2.5: *Square wave and its ideal Fourier harmonics.*

Interference of this type can be modeled as a continuous wave (CW) signal, representing a single sinusoidal component:

$$i_{\text{cw}}(t) = A\sin(2\pi f t + \varphi) \tag{2.7}$$

with amplitude A, frequency f and phase φ.

For a complex signal, it is given by

$$\begin{aligned} i_{\text{cw}}(t) &= A\cos(2\pi f t + \varphi) + jA\sin(2\pi f t + \varphi) \\ &= Ae^{j(2\pi f t+\varphi)}. \end{aligned} \tag{2.8}$$

The average signal power P_{cw} for (2.8), with period time T can be calculated as

$$\begin{aligned} P_{\text{cw}} &= \frac{1}{T}\int_0^T \left|Ae^{j(2\pi f t+\varphi)}\right|^2 dt = \Big/ \left|e^{jx} = 1\right|,\ \forall x \in \mathbb{R} \Big/ \\ &= \frac{1}{T}\int_0^T A^2 dt = A^2. \end{aligned} \tag{2.9}$$

2.4 Performance Metrics

This section defines some performance metrics. A received signal $y(t)$ in communications system can be expressed as

$$y(t) = s(t) + n(t) + i(t),$$

where the desired signal $s(t)$ is affected by noise $n(t)$ and/or interference $i(t)$. For a signal $x(t)$ of length T, the signal power P_x is defined as

$$P_x = \frac{1}{T}\int_0^T |x(t)|^2 dt. \tag{2.10}$$

Signal-to-noise ratio (SNR) compares the power of a desired signal to the power of its noise [10].

Definition 2.2 (Signal-to-Noise Ratio). SNR is the ratio given by

$$\text{SNR} = \frac{P_s}{P_n} = \frac{\int_0^T |s(t)|^2 dt}{\int_0^T |n(t)|^2 dt} \tag{2.11}$$

for signals of length T.

Similarly, signal-to-interference ratio (SIR) quantifies the strength of interference.

Definition 2.3 (Signal-to-Interference Ratio). SIR is the ratio given by

$$\text{SIR} = \frac{P_s}{P_i} = \frac{\int_0^T |s(t)|^2 dt}{\int_0^T |i(t)|^2 dt} \tag{2.12}$$

for signals of length T.

SIR normalized per bit is denoted E_b/N_I, where E_b is the signal energy per bit and N_I the interference power spectral density.

When both noise and interference is present, signal-to-interference-plus-noise ratio (SINR) is used.

Definition 2.4 (Signal-to-Interference-plus-Noise Ratio). SINR is the ratio given by

$$\text{SINR} = \frac{P_s}{P_i + P_n} = \frac{\int_0^T |s(t)|^2 dt}{\int_0^T |i(t)|^2 dt + \int_0^T |n(t)|^2 dt} \tag{2.13}$$

for signals of length T.

The metrics are commonly expressed in decibels (dB), for SIR the formula is given by [10]

$$\text{SIR}_{\text{dB}} = 10 \log_{10}(\text{SIR}). \tag{2.14}$$

The interference power can be derived from SIR and the signal power in dB as

$$\begin{aligned} \text{SIR}_{\text{dB}} &= 10 \log_{10}\left(\frac{P}{P_i}\right) = P_{\text{dB}} - 10 \log_{10}(P_i) \\ \Leftrightarrow P_i &= 10^{0.1(P_{\text{dB}} - \text{SIR}_{\text{dB}})}. \end{aligned} \tag{2.15}$$

BER compares the transmitted data sequence with received data sequence by calculating the number of bit errors i.e. the bits that differ between the sequences.

Definition 2.5 (Bit Error Rate). For n_e bit errors and n_t total bits transmitted, BER is defined as

$$BER = \frac{n_e}{n_t}. \tag{2.16}$$

2.5 Related Work

The prior work presented in this section includes studies on vulnerabilities in 5G NR physical layer components under intentional disruption of communications, as well as studies examining how OFDM-based systems respond to different types of interference.

2.5.1 Vulnerabilities of 5G

Lichtman et al. [3] investigates how vulnerable the PHY layer control channels and signals are to jamming and spoofing by individually evaluating each component. Jamming blocks communication by injecting interference, while spoofing deceives receivers by imitating valid signals. The vulnerability assessment accounts for the percent of REs occupied, jamming power needed and the complexity required to perform an attack. Figure 2.6 ranks the attacks based on efficiency and complexity, where J/S_f is the received jammer-to-signal ratio over an entire radio frame. The paper concludes that the weakest subsystems are PBCH (to jamming) and PSS (to spoofing).

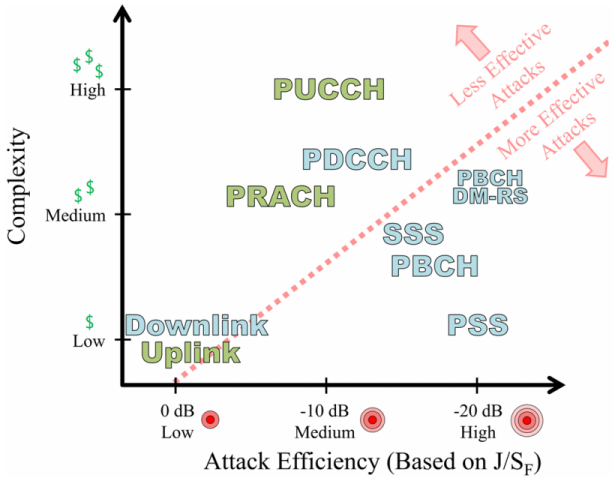


Figure 2.6: *5G PHY layer attacks [3].*

Arjoune and Faruque [15] builds on this by assessing 5G NR vulnerability to practical threat scenarios. The study states that disruption of 5G poses risks to critical infrastructure like emergency services and military communications. Notably, PBCH is said to be vulnerable to selective jamming as its symbols are placed close together. For higher-frequency carriers, this requires a jammer in close proximity.

Asemian et al. [16] instead uses a system-level simulation in a multi-user 5G network to examine barrage (noise across the entire DL bandwidth) and smart jamming attacks. Focusing on the SSB subsystem and PDSCH, the study conclude that PSS and SSS are more robust to jamming compared to both PDSCH and PBCH.

These works all build on the premise that the control and synchronization channels are critical yet vulnerable, with PBCH consistently identified as a weak point. While this thesis focuses on unintentional interference and does not examine jamming, hence it will not be explored further, the vulnerabilities pointed out by above research are still relevant. These weaknesses are interesting to investigate within the scope of this thesis.

2.5.2 Vulnerabilities of OFDM

Ankarson et al. [17] analyze how susceptible an LTE system is to different interference types. The study is conducted on downlink transmission from a base station simulator to a mobile phone, where LTE uses OFDM with a fixed SCS of 15 kHz. Common EMI scenarios are simulated with injected interference such as CW. The study concludes that interference directly targeting reference signals or the intersection between two data subcarriers affects the system more than interference centered on a data subcarrier. On the reference signal, channel estimation is disturbed.

Fors et al. [18] examine different scenarios of CW interference to a simulated OFDM system based on 5G NR. The subcarriers affected depend on the frequency separation between the CW signal and nearest subcarrier. The results indicate that the system is much more vulnerable to CW interference than to AWGN. Although the role of reference signals are not examined, it is noted that a disrupted channel estimation would degrade data transmission of the related subcarriers.

While the studies are based on different systems and methods, both use OFDM and focus on CW interference in particular. The latter study builds on the former's findings regarding interference between subcarriers. The results align to show a heightened sensitivity to narrow-band interference and point out the critical role of reference signals.

3

Method

This chapter presents the implemented 5G system and interference signals as well as evaluation methods. It also describes the performed test cases and simulations.

3.1 Implementation

This section describes the implemented 5G system used in the simulations as well as the generated interference signals. Rather than using an actual 5G system with real-world data, this work is based on a simulated system and signals. This is a drawback as signals and systems in reality does not always behave in an idealized or expected way. Therefore this thesis cannot be seen as a practical study that fully captures the complexity of a real 5G system.

3.1.1 5G System

Table 3.1 list the parameters used in all simulations, according to 5G specifications. PBCH and PBCH DM-RS are configured and generated from the parameters in 3.2, creating the symbols and RE indices. The parameter E is the length of the codeword vector according to [11]. From i_{SSB} and n_{hf}, $\bar{i}_{\text{SSB}}$ is calculated to 0 according to (2.5). From $N_{\text{ID}}^{\text{cell}}$, v is calculated to 1 according to (2.4). Throughout the simulations, $N_{\text{ID}}^{\text{cell}}$ is assumed to be known.

Table 3.1: *Simulation system parameters.*

Parameter	Value
Subcarriers	240
Subcarrier spacing	15 kHz
FFT points	256
OFDM symbol length	66.7 µs
Cyclic prefix length	4.7 µs
FEC	Polar
Modulation	QPSK

Table 3.2: *PBCH and PBCH DM-RS parameters.*

Parameter	Value
E	864
$N_{\mathrm{ID}}^{\mathrm{cell}}$	17
n_{hf}	0
i_{SSB}	0

The implemented 5G system is shown in Figure 3.1. The source generates symbols which are mapped to a resource grid, where E random bits are used to generate PBCH symbols. The transmitted, OFDM modulated signal is x_T and x_R is the signal after going through the channel and possibly being subject to interference. The received resource grid is obtained after OFDM demodulation and used to perform channel estimation

A more detailed view of the channel estimation can be seen in Figure 3.2. Based on the received resource grid, every possible value of $\bar{i}_{\mathrm{SSB}}$ is searched. The resulting DM-RS sequence with the highest SNR becomes the chosen estimate of $\bar{i}_{\mathrm{SSB}}$. This sequence is then mapped to a reference grid, which when compared to the received grid returns a channel and noise variance estimate. From this, the PBCH symbols and their channel estimates are extracted. Then, based on the noise variance estimate, the symbols are equalized with a Minimum Mean Square Error (MMSE) equalizer to remove channel distortions. Finally, the received bits are obtained through decoding the PBCH symbols.

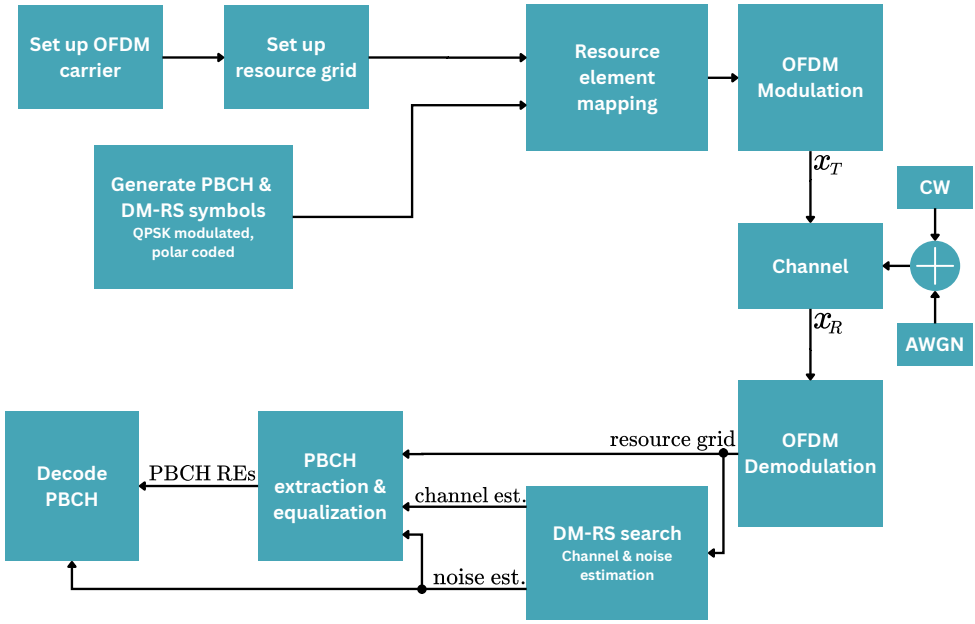


Figure 3.1: *Block diagram of the 5G simulation model.*

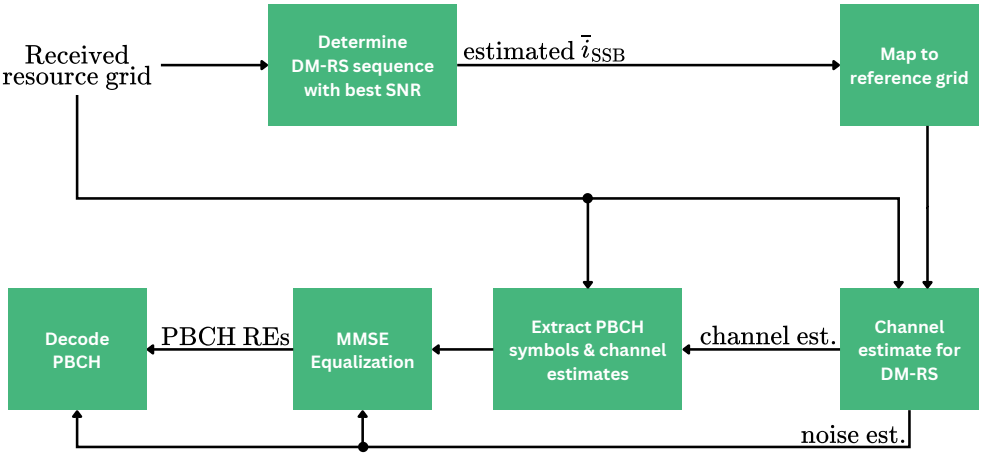


Figure 3.2: *Channel estimation block diagram.*

The thesis is delimited to PBCH and its associated DM-RS instead of considering the entire system. Figure 3.3 shows the implemented resource grid, zoomed in both time and frequency so that only the symbols and PRBs containing PBCH and PBCH DM-RS REs are used; 240 subcarriers by 3 OFDM symbols. Other channels and signals may behave differently, and therefore the conclusions cannot be generalized. It is also possible that different functions interact with and affect each other, which is not visible in this more controlled environment. The relevant parts were isolated as much as possible to understand specific effects without introducing too many variables. While this simplifies the analysis, there is a risk of oversimplifying and neglecting other factors and interactions that may have a significant impact in reality.

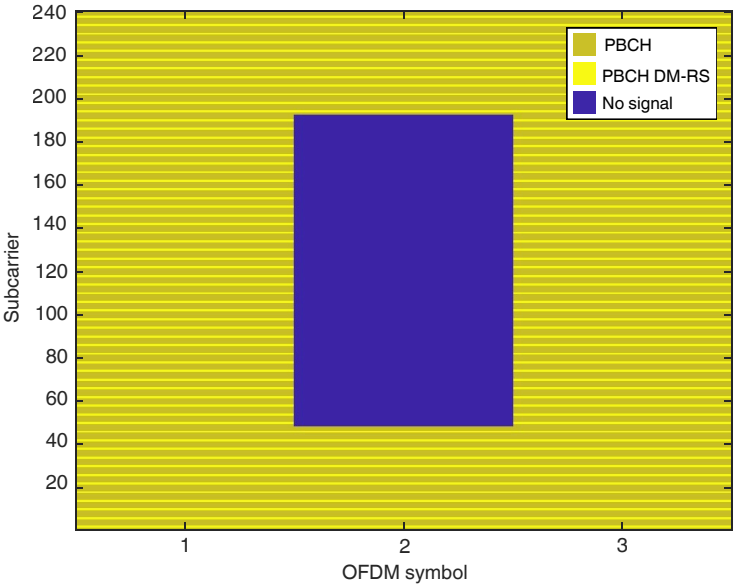


Figure 3.3: *Implemented resource grid.*

3.1.2 Interference Model

The interference model has been limited to either an AWGN or CW signal. In practice, multiple interference signals of different characteristics are likely to coexist. It is not realistic for a single CW signal to only affect a system since AWGN and internal thermal noise is always present in the environment. This means that the results cannot be generalized to the combined effect of several interference types.

The applied CW signal is constructed as

$$i_{\text{cw}}(n) = Ae^{j\left(\frac{2\pi}{N_{\text{FFT}}}(m+\alpha)n+\varphi\right)} \tag{3.1}$$

for samples $n = 1, \ldots, N_{\text{FFT}}$ where N_{FFT} is the FFT size. It has amplitude A and a randomly chosen constant phase $\varphi \in [-\pi, \pi]$. The affected subcarrier is $m \in \mathbb{N}$, shifted by frequency separation $\alpha \in [-0.5, 0.5]$.

One of the research questions focuses on the effect of different interference signals, AWGN and CW. For comparison purposes the total interference power is therefore assumed to be equal in all simulations. For a CW signal this places all power on one frequency while with AWGN the power is instead uniformly spread over the whole bandwidth.

The total interference power, P_i, for a known SIR is given by (2.15). By relating this to (2.9), the CW signal in (3.1) gets amplitude

$$A = \sqrt{P_{\text{cw}}} = \sqrt{P_i}. \tag{3.2}$$

A complex-valued AWGN signal, using circularly symmetric white Gaussian noise, has its power P_i equally split between the real and imaginary parts.

3.2 Evaluation Methods

The system will be simulated over a range of E_b/N_I values, where E_b denotes the average energy per PBCH bit and N_I the power spectral density of the added interference. Since the interference power is defined in terms of SIR, it is obtained by converting the E_b/N_I values. The conversion accounts for the modulation order (bits per symbol), code rate and the fraction of PBCH power relative to total signal power. The simulations will primarily be evaluated for the following: BER, estimated $\bar{i}_{\text{SSB}}$ and received resource grid.

BER will specifically evaluate PBCH, comparing the generated bits with the ones received after decoding. It is expressed as a ratio between 0 and 1, where a low BER (i.e. BER $\to 0$) indicate a better performance. BER is evaluated for the different interference types above, with the same total interference power for a given SIR. In most simulations, internal receiver noise is not taken into account in order to only compare the effect of different interference.

The estimated $\bar{i}_{\text{SSB}}$ is obtained in the channel estimation as seen in Figure 3.2. This will be compared to the correct $\bar{i}_{\text{SSB}} = 0$. To investigate how the estimation affects the performance and understand how much of BER comes from an incorrect estimation, this variable will be assumed to be known in some simulations.

The resource grid is received after OFDM demodulation, as seen in Figure 3.1. This can be compared to the sent resource grid in Figure 3.3, which is input to the OFDM modulation. As the channel estimation uses the received resource grid to estimate and correct for channel effects, evaluating it provides insight into how the channel has altered the signal. This can helps explain the performance of the subsequent channel estimation process and resulting BER. This will also demonstrate the difference between the broad-band AWGN and narrow-banded CW interference signals.

3.3 Test Cases & Simulations

To evaluate the affect of different interference on the system, different test cases will be investigated. The test cases are based on simulating the system with either AWGN or CW interference which are generated for a given SIR as described in Section 3.1.2. For CW, the interference can be changed by varying subcarrier m and frequency separation α. Furthermore, tests based on a known $\bar{i}_{\text{SSB}}$ will be performed. The results from the tests are presented in Chapter 4. The test cases are:

1. **AWGN Channel:** WGN is generated and added to the transmitted signal for SNR = −15 dB and 15 dB. This test will look at the received resource grids, estimation of $\bar{i}_{\text{SSB}}$ and constellation diagrams of PBCH throughout the simulation.

2. **Interference:** This test compares different cases of AWGN and CW interference and evaluates it based on BER, estimated $\bar{i}_{\text{SSB}}$ and received resource grid.

   (a) Comparing AWGN interference to different CW interference:

   - AWGN
   - CW to $m = 10$ with $\alpha = 0$
   - CW to $m = 10$ with $\alpha = 0.1$
   - CW to $m = 10$ with $\alpha = -0.25$
   - CW to $m = 10$ with $\alpha = -0.5$

   The resulting BER and estimated $\bar{i}_{\text{SSB}}$ from the interference signals above are compared. Besides comparing AWGN and CW interference, this test will demonstrate how the CW interference's frequency separation affect the result.

   (b) Comparing CW interference to different PBCH DM-RS subcarriers:

   - $m = 10$, $\alpha = 0$
   - $m = 26$, $\alpha = 0$
   - $m = 130$, $\alpha = 0$

   The BER for different PBCH DM-RS subcarriers are compared to understand if there is a large difference between the results.

   (c) Comparing CW interference to PBCH DM-RS subcarrier or PBCH subcarrier:

   - $m = 10$, $\alpha = 0$
   - $m = 11$, $\alpha = 0$

   The BER of a PBCH DM-RS subcarrier is be compared to that of a PBCH subcarrier. This test is expected to show a worse behaviour for the PBCH DM-RS subcarrier since it affects the estimation of $\bar{i}_{\text{SSB}}$ and subsequent generation of reference grid.

3. **Known $\bar{i}_{\text{SSB}}$:** The test is performed by assuming a known value of $\bar{i}_{\text{SSB}}$ in the channel estimation.

   (a) Correct $\bar{i}_{\text{SSB}}$ for:
   - AWGN
   - CW to $m = 10$ with $\alpha = 0$

   The corresponding result from the interference test will be used to compare the difference of using a known or estimated $\bar{i}_{\text{SSB}}$. The always correct $\bar{i}_{\text{SSB}}$ in this test results in a reference grid with PBCH DM-RS correctly mapped. Therefore only the interference when compared to the received resource grid affects the performance.

   (b) Incorrect $\bar{i}_{\text{SSB}}$ for:
   - AWGN
   - CW to $m = 10$ with $\alpha = 0$
   - CW to $m = 10$ with $\alpha = -0.5$
   - CW to $m = 11$ with $\alpha = 0$

   This test is made to visualize the importance of a correct estimation.

4. **SINR:** The test is performed by adding a constant AWGN noise with fixed SNR = 12 dB in addition to either AWGN or CW interference:

   - AWGN
   - CW to $m = 10$ with $\alpha = 0$
   - CW to $m = 10$ with $\alpha = -0.5$

   The corresponding result from the interference test will be used for comparison.

3.4 Source Criticism

This thesis is built upon official standards, books and research papers. It is mainly based on related work in the field such as conference papers and articles. Many of these are published by IEEE, a trusted source that applies peer review by other experts to evaluate the work before publishing. However, these studies focus on specific scenarios and do not cover all aspects.

For technical details on 5G, official 3GPP specifications that define the 5G standard used in the industry have been used as a primary and up-to-date source. Additionally, literature from established academic publishers such as McGraw Hill and Academic Press, as well as from researchers at Linköping University, are included. These are written by experts in the field.

4

Results & Discussion

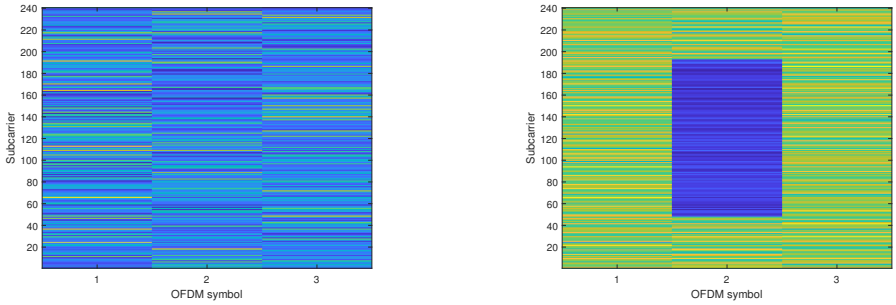
This chapter presents the results of the test cases in Section 3.3. The simulations were done in MATLAB R2024b with 5G Toolbox, Communications Toolbox and Signal Processing Toolbox. For each simulation, $N = 600$ iterations were used and averaged to get the result. In general the simulations were carried out over an E_b/N_I range from −30 dB to 40 dB with a step size of 2. In this chapter, resource grids are represented by color maps where dark blue is the lowest value (no signal) and light yellow the highest value (high signal).

4.1 AWGN Channel

Below figures present how the receiver and subsequent channel estimation is affected by adding WGN to the transmitted signal. After transmission through an AWGN channel with SNR = −15 dB or SNR = 15 dB, the received resource grid is shown in Figure 4.1. Higher SNR gives a resource grid similar to the sent resource grid in Figure 3.3.

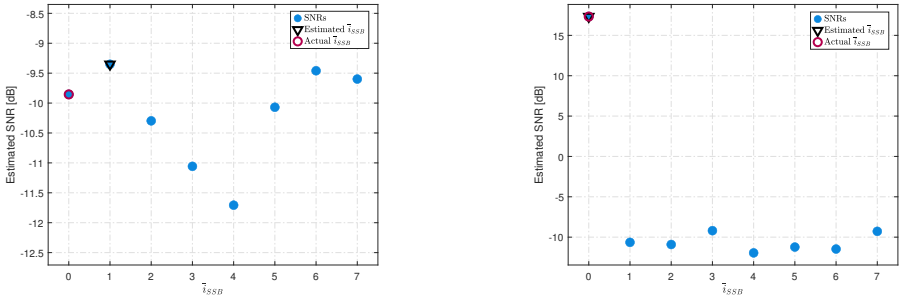
Based on the received resource grid, the estimation of $\bar{i}_{\text{SSB}}$ is seen in Figure 4.2. For every possible value of $\bar{i}_{\text{SSB}}$, the estimated SNR of the corresponding PBCH DM-RS signal is plotted. The $\bar{i}_{\text{SSB}}$ with the maximum SNR is marked as the chosen estimate along with $\bar{i}_{\text{SSB}} = 0$ as the actual value. Figure 4.2a with SNR = −15 dB shows an incorrect estimation while Figure 4.2b with SNR = 15 dB shows that the correct estimation is chosen.

In Figure 4.3a the constellation diagrams of sent, received and equalized bits for SNR = −15 dB are shown, and for SNR = 15 dB in Figure 4.3b. The lower SNR yields a larger dispersion of the received and equalized bits compared to the sent bits.



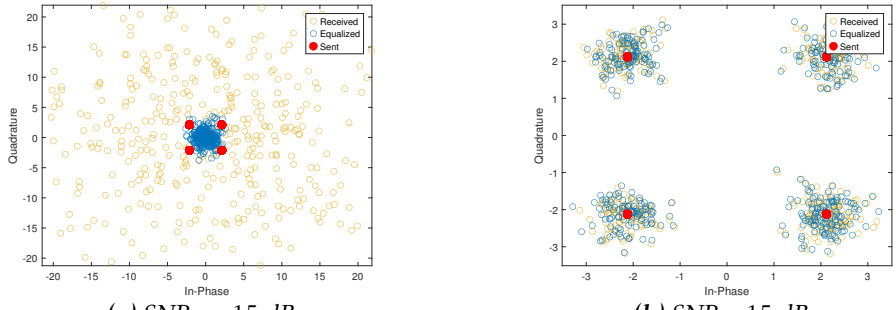
(a) SNR = −15 dB *(b) SNR = 15 dB*

Figure 4.1: *Received resource grids after going through an AWGN channel.*



(a) SNR = −15 dB *(b) SNR = 15 dB*

Figure 4.2: *Estimation of $\bar{i}_{\mathrm{SSB}}$, comparing the estimated DM-RS SNR for all possible values of $\bar{i}_{\mathrm{SSB}}$.*



(a) SNR = −15 dB *(b) SNR = 15 dB*

Figure 4.3: *PBCH constellation diagrams showing all possible symbol states throughout the simulation; sent, received and equalized.*

The results show an expected behaviour where worse conditions, i.e. lower

SNR, results in a noisy resource grid and subsequent incorrect estimation. Together the figures illustrate different steps of the channel estimation and help understand the upcoming results. This also confirms that the simulation setup behaves as intended.

4.2 Interference

This section presents the results from simulations with different interference; broad-band AWGN or a narrow-banded CW signal applied to one subcarrier.

4.2.1 BER

The Figures in this section display the BER as a function of E_b/N_I. Figure 4.4 show the BER for AWGN as well as CW on subcarrier $m = 10$ with different frequency separations. Up to $E_b/N_I = -10$ dB, all curves are at a high BER. After that, CW with $\alpha = 0$ and 0.1 drops more sharply than those with larger frequency separation. Up until $E_b/N_I = 18$ dB, AWGN has a BER very similar or higher than the CW curves. Only the green curve with $\alpha = -0.5$, i.e. directly in between two subcarriers, has a slightly higher BER at times. The BER tends towards zero fastest for AWGN, followed by CW with $\alpha = 0$. As the frequency separation becomes larger, it takes a higher E_b/N_I to reach zero.

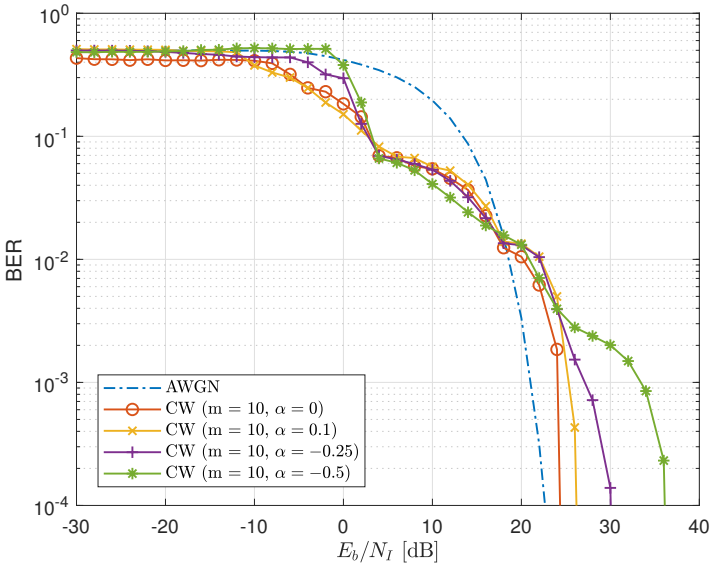


Figure 4.4: *BER as a function of E_b/N_I for AWGN interference, and CW interference to subcarrier $m = 10$ with various frequency separation α.*

In Figure 4.5 the plots for CW interference on subcarrier $m = 10$ and $m = 11$,

with $\alpha = 0$, are shown. This compares interference to a PBCH DM-RS subcarrier (blue) to that of a PBCH subcarrier (red). The black, dotted line represents $\frac{0.5}{\text{number of data carriers}}$. The BER of the PBCH data subcarrier follows that line before going towards zero. Figure 4.6 shows the BER of three different PBCH DM-RS subcarriers; $m = 10$, $m = 26$ and $m = 130$, with $\alpha = 0$. The curves follow a similar behaviour.

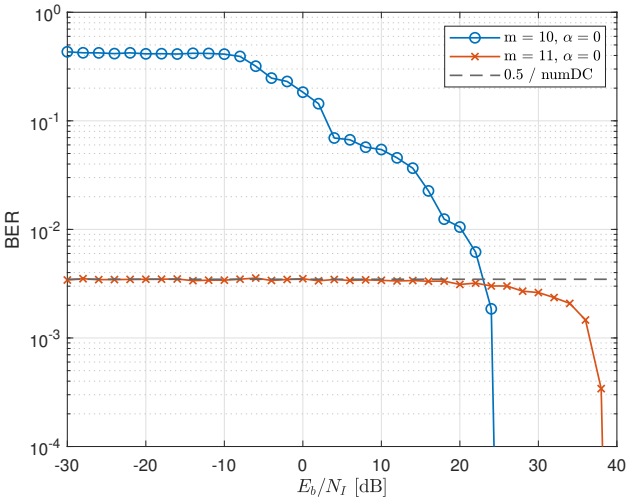


Figure 4.5: *BER for CW interference to PBCH DM-RS subcarrier $m = 10$ and PBCH subcarrier $m = 11$. The black line represents $\frac{0.5}{\text{number of data carriers}}$.*

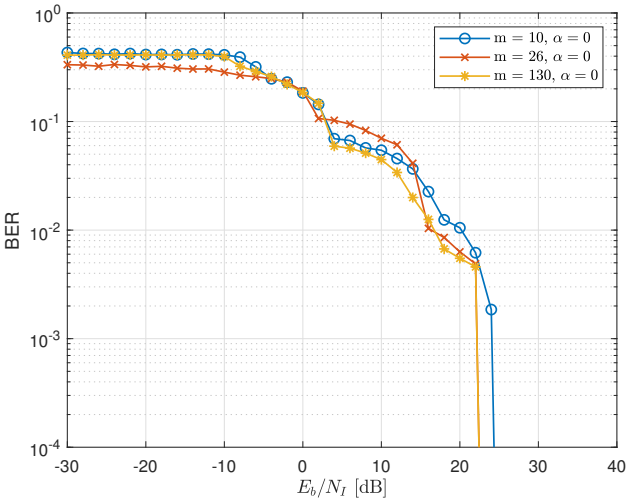


Figure 4.6: *BER for CW interference to different PBCH DM-RS subcarriers; $m = 10$, $m = 26$ and $m = 130$.*

4.2.2 Estimated $\bar{i}_{\text{SSB}}$

Figure 4.7 presents the probability that the estimated $\bar{i}_{\text{SSB}} \neq 0$ as a function of E_b/N_I for AWGN and CW to subcarrier $m = 10$ with different frequency separations α. All lines start at the maximum probability of 1, meaning an incorrect value. AWGN first reaches an probability of zero, meaning the correct value, at $E_b/N_I = 0$ dB. It is followed by CW with $\alpha = 0.1$ at $E_b/N_I = 2$ dB and the remaining at $E_b/N_I = 4$ dB.

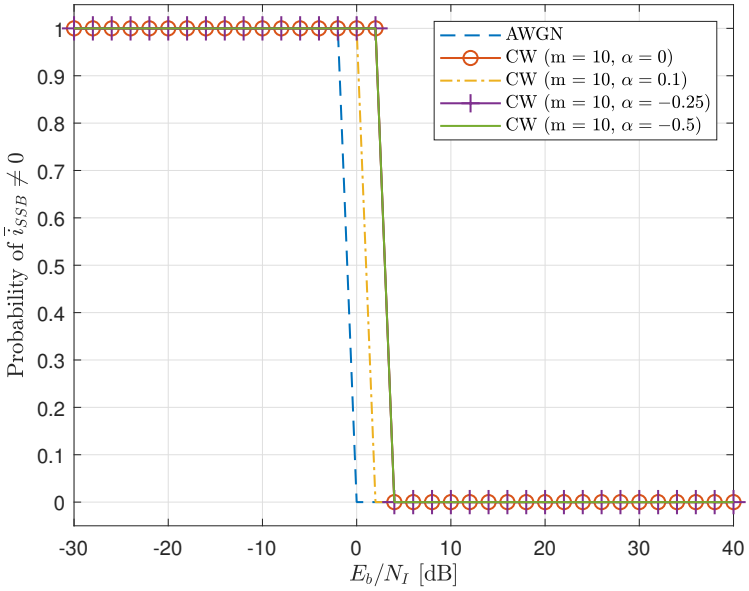


Figure 4.7: *Probability of the estimated $\bar{i}_{\text{SSB}}$ being incorrect ($\bar{i}_{\text{SSB}} \neq 0$) when E_b/N_I ranges from -30 dB to 40 dB for AWGN interference, and CW interference to subcarrier $m = 10$ with various frequency separation α. The correct value of $\bar{i}_{\text{SSB}} = 0$ is achieved when the probability is zero.*

4.2.3 Received Resource Grid

This section presents received resource grids after different interference. Figure 4.8 shows the received resource grids for AWGN when $E_b/N_I = -30$ dB and $E_b/N_I = 30$ dB. The lower E_b/N_I has not maintained any of the original structure, while the higher is similar to the sent resource grid.

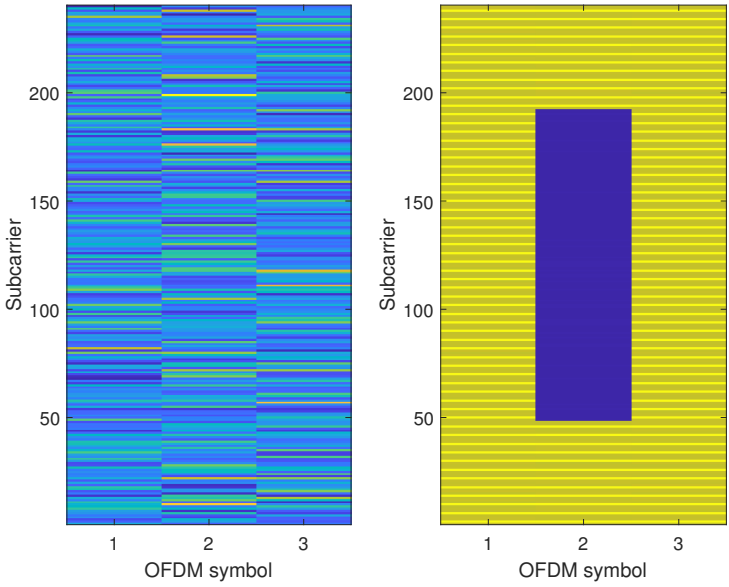
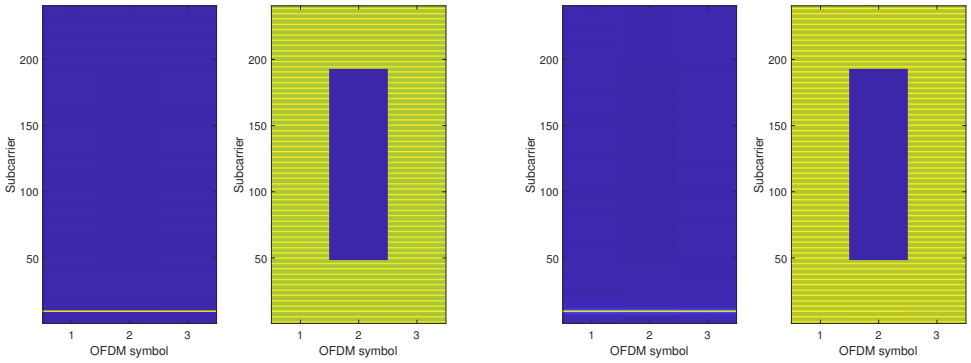
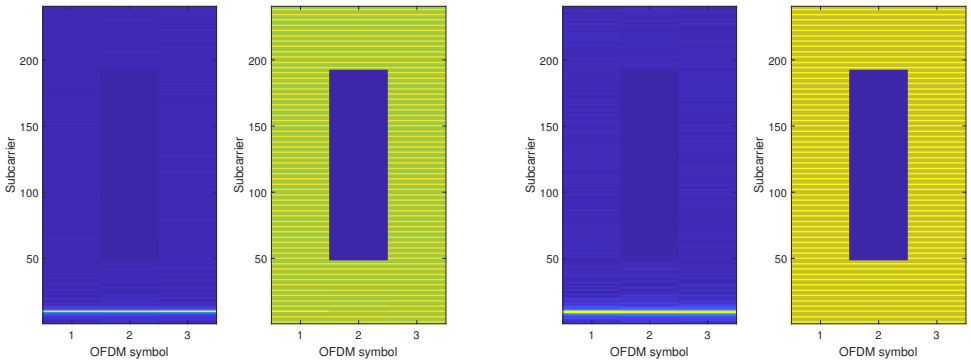


Figure 4.8: *Received resource grids after AWGN interference for $E_b/N_I = -30$ dB (left) and $E_b/N_I = 30$ dB (right).*

Figure 4.9 shows the received resource grids for CW to subcarrier $m = 10$ for different frequency separations α. When $E_b/N_I = -30$ dB, a line can be seen where the CW interference has been applied. The null space of the sent resource grid can barely be seen. The original structure is on the other hand visible when $E_b/N_I = 30$ dB.



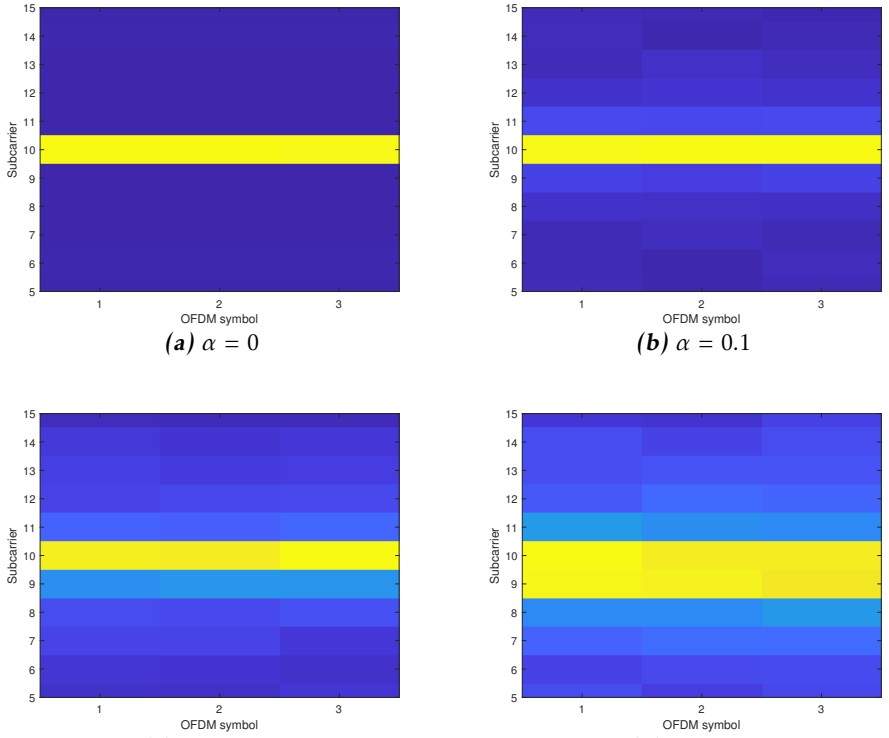
(a) $\alpha = 0$ ***(b)*** $\alpha = 0.1$



(c) $\alpha = -0.25$ ***(d)*** $\alpha = -0.5$

Figure 4.9: *Received resource grids after CW interference to subcarrier* $m = 10$ *with various frequency separation* α*, for* $E_b/N_I = -30$ *dB (left) and* $E_b/N_I = 30$ *dB (right).*

In Figure 4.10, the received resource grids when $E_b/N_I = -30$ dB have been zoomed in around the subcarrier $m = 10$ to show the interference spreading depending on the frequency separation. When $\alpha = 0$ in Figure 4.10a, the interference is only applied at the subcarrier while the surrounding subcarriers are at a low value. As the frequency separation increases, so does the interference spreading to the surrounding subcarriers. When $\alpha = -0.5$ in Figure 4.10d, the yellow area that represents the highest value has doubled in size compared to the other figures.



(a) $\alpha = 0$ ***(b)*** $\alpha = 0.1$

(c) $\alpha = -0.25$ ***(d)*** $\alpha = -0.5$

Figure 4.10: *Resource grids zoomed in around subcarrier* $m = 10$ *to show the interference spreading when CW interference with* $E_b/N_I = -30$ *dB and various frequency separation* α *is applied to the subcarrier. Dark blue indicates the lowest value in the resource grid, and yellow the highest.*

4.2.4 Discussion

By observing the BER, it can be seen that for very low E_b/N_I, the results do not differ much depending on the interference characteristics. While AWGN shows a smooth slope, CW behaves more erratically, causing different interference types to have the worst BER at different E_b/N_I values. The frequency separation starts to have a clear impact at higher values. Here it is interesting to note that the BER approaches zero at different rates depending on α: first for $\alpha = 0$, followed by $\alpha = 0.1$, then $\alpha = -0.25$, and finally, at the highest E_b/N_I values, for $\alpha = -0.5$. This ordering can be explained by the spreading of interference with larger frequency separations. For $\alpha = 0$, the interference is concentrated on a single subcarrier, maintaining the orthogonality between subcarriers as intended with OFDM. Larger α values, on the other hand, cause the interference energy to spread across multiple subcarriers and reducing orthogonality, as visible in the received resource grids. As a result, the receiver needs a higher E_b/N_I before the signal dominates enough to overcome the broader interference, delaying the im-

provement in BER. Compared to the results of [18] in Section 2.5, the difference between AWGN and CW is not as visible, nor the difference of various frequency separation across the whole E_b/N_I range. Unlike their simple OFDM model with 5G parameters, this work includes actual 5G channels and signals, making the results more representative of practical system behaviour.

The BER can be seen as the final performance measure of the last step in the system. Meanwhile, the estimated $\bar{i}_{\text{SSB}}$ and the received resource grid are gathered at earlier steps in the system, providing insight into how they contribute to the final BER. How successful a channel estimation and equalization is can broadly be attributed to a successful DM-RS sequence estimation, based on $\bar{i}_{\text{SSB}}$ estimation, and accurate estimation of the channel response over the resource grid. Errors in channel estimation lead to incorrect equalization, which may lead to a rotation of the symbol constellation. This will result in additional incorrect bit decisions due to an erroneous phase bias. Alternatively, bit errors can also occur directly from the interference effect itself, even if the channel estimation is accurate. The observed BER therefore reflects both the accuracy of the channel estimation and the direct impact of interference. Overall, the effect of whether $\bar{i}_{\text{SSB}}$ is estimated correctly or not is similar across all interference types, with it being incorrect for E_b/N_I values up to 4. Beyond that, the BER is solely caused by the interference effect itself corrupting the resource grid.

Focusing on CW interference to one subcarrier, the results show the expected worse behaviour when applied to a PBCH DM-RS subcarrier compared to a PBCH data subcarrier. The BER for a data subcarrier follows the line $\frac{0.5}{\text{number of data carriers}}$ before approaching zero. That can be attributed to PBCH using QPSK, since a single QPSK-modulated subcarrier that is disturbed contributes a maximum of 0.5 bit errors per symbol on average. In contrast, DM-RS subcarriers are used for channel estimation, meaning interference on these subcarriers can propagate errors across multiple data subcarriers via incorrect equalization, leading to higher BER.

Furthermore, while not exactly the same, BER results of different PBCH DM-RS subcarriers are largely the same. Therefore the findings can be generalized to all PBCH DM-RS subcarriers.

4.3 BER with Known $\bar{i}_{\text{SSB}}$

Figure 4.11 compares the BER of AWGN interference to CW interference on subcarrier $m = 10$ with $\alpha = 0$. For both interference types, an estimated and a known $\bar{i}_{\text{SSB}}$ has been used. The blue and yellow lines come from Figure 4.4 where a proper channel estimation has been done. The red and purple lines have instead assumed the correct value $\bar{i}_{\text{SSB}} = 0$. The Figure demonstrates exactly equal plots for AWGN. For CW on the other hand, the purple line starts at a lower BER before becoming equal to the yellow line when $E_b/N_I = 4$ dB. When an incorrect $\bar{i}_{\text{SSB}} = 1$ is used instead, it results in a constantly high BER for all cases, including CW interference to a PBCH subcarrier.

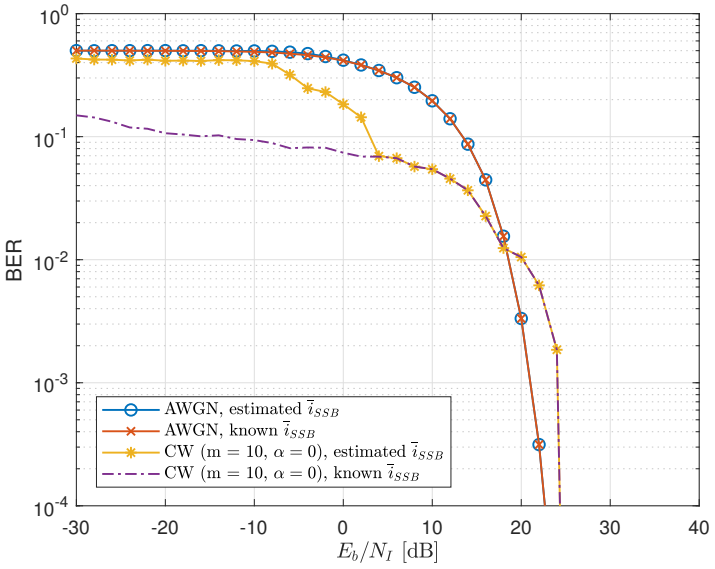


Figure 4.11: *BER when $\bar{i}_{\mathrm{SSB}}$ is either estimated or assumed to be known during the channel estimation. The blue and yellow lines estimates the value as in Figure 4.4 while the red and purple directly uses $\bar{i}_{\mathrm{SSB}} = 0$.*

Isolating the effect of $\bar{i}_{\mathrm{SSB}}$ estimation is difficult, since errors arise from a resource grid corrupted enough that an incorrect DM-RS sequence appears favourable. Meaning it is challenging to separate estimation errors from the impact of noise in the resource grid.

To get a rough understanding of how much $\bar{i}_{\mathrm{SSB}}$ estimation contributes to the BER, $\bar{i}_{\mathrm{SSB}}$ was manually set to the correct value such that only the subsequent steps of the channel estimation affects BER. This is an idealized isolation because estimation errors naturally occur at low E_b/N_I when the grid is highly corrupted. Under AWGN, this makes no difference, indicating the BER is dominated by noise. For CW interference, the BER starts lower with correct $\bar{i}_{\mathrm{SSB}}$, but converges with the original curve at $E_b/N_I = 4$ dB. Thus the estimation is shown to directly contribute additional bit errors. Notably, the results using an incorrect estimation highlight the importance of an accurate $\bar{i}_{\mathrm{SSB}}$ estimation. Unlike the previous results, this is also observed for a PBCH subcarrier.

4.4 SINR

In Figure 4.12 the BER of AWGN interference and CW interference on subcarrier $m = 10$ with $\alpha = 0$ or -0.5 is compared with and without the presence of a constant AWGN noise with SNR = 12 dB. The plots are equal at first but as E_b/N_I increases, the added noise becomes more and more visible. By introducing a constant noise, the BER expectedly reaches a floor for high E_b/N_I values instead

of approaching zero. Thus, the constant noise has introduced a floor equal to the BER totally determined by SNR = 12 dB. The relative behaviour between interference types is preserved, with CW at $\alpha = -0.5$ reaching the floor later than the others. This reflects a more realistic scenario, as noise is always present in practical systems.

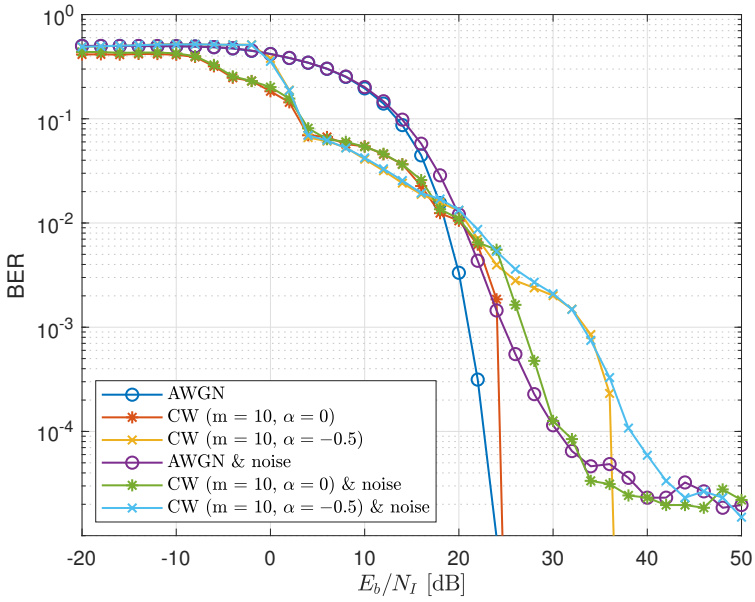


Figure 4.12: *BER for AWGN interference and CW interference to subcarrier $m = 10$ with frequency separation $\alpha = 0$ or $\alpha = -0.5$. The purple, green and light blue curves also has a constant AWGN noise with a fixed SNR = 12 dB.*

5

Conclusions

This chapter will answer the research questions presented in Section 1.3 and conclude the thesis. Some thoughts on future works based on the project are also presented.

5.1 Aim & Research Questions

This thesis aimed to investigate the impact of unintentional interference on PBCH DM-RS in 5G NR. The research focused on understanding both the performance effects on PBCH and identifying which types of interference have the most significant impact on DM-RS robustness.

How does unintentional interference to PBCH DM-RS affect the performance of PBCH in 5G NR? Overall, the results in Section 4.2 show that interference to PBCH DM-RS has a significant impact on PBCH performance. CW interference in particular illustrate that there is a significant difference in the performance when applied to PBCH DM-RS subcarriers compared to PBCH subcarriers, according to Section 4.2.1. A correct $\bar{i}_{\text{SSB}}$ estimation is also found to be critical in Section 4.3. An incorrect estimation, obtained when an incorrect DM-RS sequence appears favourable, effectively prevents the PBCH from performing correctly regardless of E_b/N_I conditions. However, it remains difficult to fully isolate and quantify the contribution of $\bar{i}_{\text{SSB}}$ estimation on DM-RS to overall PBCH performance. Notably, CW interference with larger frequency separations spreads across multiple OFDM subcarriers, as seen in Section 4.2.3, which worsens the BER at higher E_b/N_I. Finally, the BER behaviour is consistent across different PBCH DM-RS subcarriers, suggesting that these findings could be generalized to other PBCH DM-RS configurations. Nevertheless, caution should be taken when

extending these results to different numerologies or channel conditions beyond those studied here (Section 3.1.1).

Which type of interference signal have the most significant impact on the robustness of PBCH DM-RS in 5G NR? This thesis investigated two types of interference: broad-band AWGN and narrow-band CW, as described in Section 3.1.2. The results in Section 4.2 show that CW interference generally has a stronger effect on BER than AWGN, particularly at higher E_b/N_I. The impact of CW interference depends on its frequency separation, as larger separations cause interference to spread across multiple subcarriers and reduce OFDM orthogonality. In contrast, AWGN produces a smoother and less erratic BER behaviour as its energy is distributed evenly across all subcarriers. These findings highlight the importance of considering both interference type and characteristics when assessing the robustness of PBCH DM-RS in 5G NR.

5.2 Future Work

There are several potential directions for further research stemming from this thesis. Future investigations could explore additional interference types, more channels, and more realistic system conditions to better assess the robustness of 5G.

A natural extension of this thesis would be to broaden the study beyond AWGN and CW, and to include other 5G channels and signals. Since each signal has different characteristics and roles in the system, their robustness against different interference may vary. By studying additional interference types, such as chirp signals, and comparing their impact across different 5G functions, a broader understanding of 5G vulnerabilities is achieved. This would also identify the weakest parts of the system. Similarly, investigating the corresponding uplink signals would extend insights to the full 5G communication chain.

Future studies could also investigate the effect of using multiple interferers with different strengths and characteristics on the system. For example, how would multiple CW signals on different subcarriers affect the performance? Exploring different scenarios could help identify the most critical interference conditions. This would also reflect a more realistic scenario compared to a singe interference source. Finally, to better approximate real-world conditions, future work could include effects such as channel fading and path loss.

Bibliography

[1] 3GPP. 5G System Overview, 2022. URL https://www.3gpp.org/technologies/5g-system-overview. Accessed: 2025-04-04.

[2] Ericsson. Mobile Subscriptions Outlook, 2024. URL https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/mobile-subscriptions-outlook. Accessed: 2025-04-07.

[3] Marc Lichtman, Raghunandan Rao, Vuk Marojevic, Jeffrey Reed, and Roger Piqueras Jover. 5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation. In *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6, Kansas City, MO, USA, 2018. IEEE.

[4] Peter Stenumgaard and Sara Linder. Interference Impact from Solar-Panel Systems on Air Traffic Control Communications. In *2019 International Symposium on Electromagnetic Compatibility (EMC)*, pages 1044–1048, Barcelona, Spain, 2019. IEEE.

[5] John G. Proakis and Masoud Salehi. *Digital Communications*. McGraw Hill, 5th edition, 2007. ISBN 978–0–07–295716–7.

[6] 3GPP. 5G Release Description (Release 15). 3GPP TR 21.915 v15.0.0, Oct. 2019.

[7] 3GPP. 5G NR Physical Channels and Modulation (Release 18). 3GPP TS 38.211 v18.5.0, Jan. 2025.

[8] Maya Flores, Devon Poisson, Colin Stevens, Adriyel Nieves, and Alexander Wyglinski. Implementation and Evaluation of a Smart Uplink Jamming Attack in a Public 5G Network. *IEEE Access*, 11:75993–76007, 2023.

[9] Erik Dahlman, Stefan Parkvall, and Johan Sköld. *5G NR: The Next Generation Wireless Access Technology*. Academic Press, second edition, 2021. ISBN 978-0-12-822320-8.

[10] Erik G. Larsson. *Signals, Information and Communications*. LiU-Press, 2021.

[11] 3GPP. 5G NR Multiplexing and Channel Coding (Release 18). 3GPP TS 38.212 v18.5.0, Jan. 2025.

[12] Sassan Ahmadi. *5G NR: Architecture, Technology, Implementation, and Operation of 3GPP New Radio Standards*. Academic Press, 2019. ISBN 978-0-08-102267-2.

[13] Shun Yoneda, Mamoru Sawahashi, and Satoshi Nagata. Performance of NR Downlink Initial Access Using Synchronization Signal Block for mm-Wave Bands. pages 394–400, Sydney, Australia, 2023. IEEE.

[14] Phalguni Mathur and Sujith Raman. Electromagnetic Interference (EMI): Measurement and Reduction Techniques. *Journal of Electronic Materials*, 49(5):2975–2998, 2020.

[15] Youness Arjoune and Saleh Faruque. Smart Jamming Attacks in 5G New Radio: A Review. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 1010–1015, Las Vegas, NV, USA, 2020. IEEE.

[16] Ghazal Asemian, Michel Kulhandjian, Mohammadreza Amini, Burak Kantarci, Claude D'Amours, and Melike Erol-Kantarci. The Impact of Mobility, Beam Sweeping and Smart Jammers on Security Vulnerabilities of 5G Cells. *Wireless World Research and Trends Magazine*, pages 71–78, Dec. 2024.

[17] Peter Ankarson, Jan Carlsson, Björn Bergqvist, Stefan Larsson, and Markel Bertilsson. Impact of different interference types on an LTE communication link using conducted measurements. In *2015 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, pages 177–182, Dresden, Germany, 2015. IEEE.

[18] Karina Fors, Erik Axell, Sara Linder, and Peter Stenumgaard. On the Impact of CW interference on 5G NR. In *2019 International Symposium on Electromagnetic Compatibility (EMC)*, pages 1049–1054, Barcelona, Spain, 2019. IEEE.