Tampere University

Sarada Adhikari

PHYSICAL LAYER JAMMING DETECTION FOR 5G NR UPLINK

Faculty of Information Technology and Communication Sciences
M. Sc. Thesis
November 2022

ABSTRACT

Sarada Adhikari: Physical Layer Jamming Detection for 5G NR Uplink
M.Sc. Thesis
Tampere University
Master's Degree Programme in Communication System and Networks
November 2022

The shared and open scenario of wireless communication makes it more vulnerable towards jamming attacks than the wired communication techniques. It is important to have an idea to what extent the communication system is vulnerable to jamming. The proper knowledge about the types of existing jammer and the prevailing jammer detection techniques is also equally essential to develop a module for detecting the jammer that is attacking the communication system.

With this in regard, the prime motive of this thesis is to study about the vulnerabilities of 5G NR physical layer channels and signals to jamming, to review several jammers along with jammer detection methodologies, to design a constant and frequency sweeping jammer, and to develop a jammer detection algorithm by utilizing MATLAB. To develop a jammer detection module, the power of each empty or unoccupied physical resource blocks (PRBs) in each symbol was calculated per slot and each individual power was averaged per occurrence of empty PRBs per slot and per short and long-term averaging window and then the measured average power was compared with the initialized threshold values to detect the jammer. A reference jammer detection block was created to test whether the detected jammer is a correct detection or only a false alarm.

Keywords: 5G NR physical layer vulnerabilities, Jammers, Jammer detection algorithm, empty PRBs, correct detection, false alarm rate.

PREFACE

This thesis ‘Physical Layer Jamming Detection for 5G NR Uplink’ was carried out to fulfil the partial requirements of Master of Science (M.Sc.) degree in Communication Systems and Networks under Information Technology.

First, I would like to express my sincere gratitude to Nokia Solutions and Networks, Tampere for providing me with the platform from where I could work and complete my thesis. Meanwhile I am also very thankful to my supervisors Toni Aleksi Levanen from Nokia and Taneli Riihonen from Tampere Universities for their continuous support and guidance at all the phases of my thesis without whom this work would not have been possible.

I would love to give a huge bunch of thanks to my mother Maya Adhikari, Father Netra Prasad Adhikari, and my husband Milan Kharel for always believing in me and motivating me to tackle and overcome hindrances at every phases. Also, I am thankful to my brothers, sisters and friends for their never-ending love and support.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

4G	Fourth Generation
5G	Fifth Generation
3GPP	3rd Generation Partnership Project
ACK	Acknowledgement
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPR	Bad Packet Ratio
BS	Base Station
BW	Bandwidth
BWP	Bandwidth Part
CD	Correct Detection
CP	Cyclic Prefix
CPE	Common Phase Error
CRC	Cyclic Redundancy Check
CSI	Channel State Information
dB	Decibels
DC	Data Communication
DCI	Downlink Control Information
DD	Detection Delay
DFT	Discrete Fourier Transform
DFT-s-	Discrete Fourier Transform-spread-
DL	Downlink
DL-SCH	Downlink Shared Channel
DMRS	Demodulation Reference Signal
DP	Detection Probability
ECA	Energy Consumption Amount
eMBB	Enhanced Mobile Broadband
eNB	Evolved Node B
FAR	False Alarm Rate
FEC	Forward Error Correction
FHSS	Frequency Hopping Spread Spectrum
FPGA	Field Programmable Gate Array

FR	Frequency Range
GHz	Gigahertz
gNB	Next-generation Node B
HARQ	Hybrid Automatic Repeat Request
HD	High Definition
IEEE	Institute of Electrical and Electronics Engineers
INR	Interference to Thermal Noise Ratio
IP	Internet Protocol
kHz	Kilohertz
LDPC	Low Density Parity Check
LTE	Long Term Evolution
MAC	Media Access Control
MD	Miss Detection
MHz	Megahertz
MIMO	Multiple Input Multiple Output
MITM	Man-In-The-Middle
mMTC	Masstive Machine Type Communication
NACK	Negative Acknowledgement
NR	New Radio
OFDM	Orthogonal Frequency Division Multiplexing
PBCH	Physical Broadcast Channel
PDCCH	Physical Downlink Control Channel
PDCP	Packet Data Convergence Protocol
PDPT	Packet Drop Per Terminal
PDR	Packet Delivery Ratio
PDSCH	Physical Downlin Shared Channel
PHY	Physical Layer
PRACH	Physical Random Access Channel
PRB	Physical Resource Block
PSR	Packet Sent Ratio
PSS	Primary Synchronization Signal
PTRS	Phase Tracking Reference Signal
PUCCH	Physical Uplink Control Channel
PUSCH	Physical Uplink Shared Channel

QAM	Quadrature Amplitiude Modulation
QPSK	Quadrature Phase Shift Keying
RACH	Random Access Channel
RB	Resource Block
RE	Resource Element
RF	Radio Frequency
RLC	Radio Link Control Layer
RNTI	Radio Network Temporary Identifier
RRC	Radio Resource Control
RSS	Received Signal Strength
SCS	Sub-Carrier Spacing
SDAP	Service Data Adaptation Protocol Layer
SINR	Signal-to-Interference and Noise Ratio
SIR	Signal to Interference Ratio
SNR	Signal to Noise Ratio
SR	Scheduling Request
SRS	Sounding Reference Signal
SSS	Secondary Synchronization Signal
TDD	Time Division Duplexing
TS	Technical Specification
UCI	Uplink Control Information
UE	User Equipment
UL	Uplink
UL-SCH	Uplink Shared Channel
UMTS	Universal Mobile Telecommunications System
URLLC	Ultra-Reliable Low Latency Communications
WLAN	Wireless Local Area Network

1 INTRODUCTION

1.1 Background and Motivation

Of the many wireless mobile technologies from 2nd Generation to 4th Generation that evolved in the last 40 years, the 5th Generation wireless communication system initiated by 3GPP Release 15 [1] in 2018 has been the burning topic for many users and researchers not only due to its ability to deal with the increasing demand of traffic volume but also due to its availability, reliability and efficiency for a broad application areas [2]. 5G NR can operate either in standalone mode where it works without depending to other radio access technology or in non-standalone mode, where it uses 4G system for initial access procedure and mobility [3]. To overcome the challenges that comes with the large number of connected devices and huge traffic volume, 5G NR gives access to more spectrum and wider bandwidths [2].

5G has been designed with 3 main use cases: eMBB (Enhanced Mobile Broad Band), mMTC (Massive Machine Type Communication), and URLLC (Ultra Reliable Low Latency Communication) which support varied applications areas like: Self-driving cars, Advanced IoT, industrial automatization, Ultra High Definition (UHD) videos streaming, Smart city etc. [4]. Due to wider applications, it is more sensitive to malicious jamming attacks which could be a possible threat to critical infrastructure or personal safety [5]**.** For example, jammer could harm the main power plant in industries causing unwanted result at the output. The jammer could also mislead heath assistants about the patient's body condition in a remote health monitoring system**.** So, knowledge of the types of existing jammers, and their detection mechanism are the key steps towards robust communication system [6]**.** Under regular and smart categories jammers are mainly classified into 4 main groups: Constant Jammers, Reactive Jammers, Random Jammers, and Deceptive Jammers. In contrary to regular jammers, smart jammers can quickly learn in depth about the transmitted signal and update their attacks to cause more damage. On the other hand, several jammer detection methods have been proposed which are categorized under metric threshold-based approach and machine learning approach. While metric threshold-based method monitors any access energy of a physical channel, and compares the threshold with some metrices like PDR, SNR, BER etc., the machine learning based approach uses classifiers like support vector machine and neural networks with advanced features to detect jamming [7].

1.2 Objectives and Thesis Scope

The prime objective behind this thesis is to study the detection of jamming or interference in the physical layer of 5G NR uplink, design a constant and frequency sweeping jammer, propose three different algorithms with the concept of relative and absolute thresholding to detect those jammers in PUSCH channel, understand the benefits and limitations of this approach, and evaluate the quality of the proposed algorithms in terms of correct detection probability and false alarm probability.

Initially, the thesis provides introduction to physical layer of 5G, types of existing and known jammers and available jammer detection techniques, which is then followed by 5G physical layer parameter measurement where power in resource elements in UL (that are not assigned to any UEs) or abnormally high amount of power in UL region altogether are measured along with the power of each PRBs. Finally, a simple MATLAB model is developed from 5G NR toolbox to model the jammers and its detection algorithm.

The jammer detection in this thesis is focussed on the physical layer due to its low latency, easy access to empty PRBs, reliable detection of the dominant interference in those PRBs, and simple computation for interference detection as information are easily compressed into the heat maps which are then used for detection.

1.3 Research Outcomes

The implementation of two detection algorithms: absolute and relative thresholding in three methods of heat map calculation: slot, short-term window, and long-term window, led to six different detection techniques: slot based relative and absolute thresholding, short-term window based relative and absolute thresholding and long-term window based relative and absolute thresholding. These techniques were individually utilized to detect the interfered PRBs due to a constant or frequency sweeping jammer in an OFDM symbol.

Among all the chosen techniques, the long-term window based relative thresholding was the best method to detect the interfered PRBs due to constant jammer as it provided targeted 99% correct detection point at INR value 3 dB which is the lowest INR value when compared with other techniques. Whereas, in case of frequency sweeping jammer, slot based relative thresholding was the best method among all techniques as reached the targeted 99% correct detection point at INR value: 32 dB which is the lowest INR value when compared with the INR value at which other detection technique provided 99% correct detection.

Also, the false alarm rates in case of constant jammer were less and better when compared with the false alarm rates of frequency sweeping jammer. So, it is concluded that the constant jammer is easily detected and does not even give greater false alarm values. While frequency sweeping jammer takes more time to be detected. Additionally, relative thresholding was the best detection algorithm in comparison to absolute thresholding.

1.4 Thesis Organization

The overall thesis is structured into 5 chapters. Chapter 2 outlines the 5G Physical layer and presents vulnerabilities of this layer. Similarly, the types of existing jammer types and their detection mechanism is highlighted in Chapter 3. Chapter 4 emphasizes physical layer jamming detection highlighting the thresholding and averaging window concepts. MATLAB model setup, simulation, results, and related discussions are performed in Chapter 5. Whereas Chapter 6 draws the conclusion from the overall work and proposes future research lines.

2 5G NR AND ITS PHYSICAL LAYER VULNERABILITIES

This chapter encompasses background information about 5G NR highlighting the main features of its physical layer along with its functions. It gives a short introduction about the key new components of physical layer: waveform, numerology, bandwidth parts, frame structure and presents their respective functionalities explaining in brief about the CP-OFDM waveform structure. The later part then explains several uplink and downlink channels associated with the physical layer and focuses on how different uplink channels, downlink channels and reference signals of physical layer are vulnerable to potential jamming.

According to 3GPP terminology [8], 5G NR uses two frequency ranges FR1 (Sub 6 GHz), which is utilized in this thesis, and FR2 (mmWave ranging 24.25 – 52.6 GHz). Along with advanced modulation and coding techniques, it supports high data rates of up to 10 Gbps [9]. The 5G technology is designed based on OFDM (Orthogonal Frequency-Division Multiplexing): a modulation scheme which modulates a digital signal among several channels to minimize inter-symbol interference. In OFDM, the subcarriers overlap in frequency orthogonally and do not interfere with each other [10].

In 3G UMTS, the network node is logically termed as Node B (NB) and in 4G LTE, the network node is defined as evolved Node B (eNB). Similarly, the network node for 5G is termed as next generation Node B (gNB). The device is then termed as UE [11]. The gNB to UE connection is known as downlink which uses PBCH, PDSCH, and PDCCH channels whereas the connection from UE to gNB uses PRACH, PUSCH and PUCCH channels and is known as uplink [12]. However, the work in this thesis focuses on the uplink.

The radio protocol architecture is divided into user-plane and control-plane as described in Figure 2.1. A control plane performs connection setup, maintains security, and supports mobility whereas the user-plane delivers user data, and its protocol stack consists of Physical layer (PHY), Medium Access Control Layer (MAC), Radio Link Control layer (RLC), and Packet Data convergence protocol layer (PDCP). Whereas the user-plane protocol stack is divided further into PHY, MAC, RLC, PDCP, and Service Data Adaptation protocol layer (SDAP). Where, a PHY layer deals with coding/decoding, multiantenna processing, signals mapping to physical time-frequency resources, and modulation and demodulation. The MAC layer handles the error correction via Hybrid Automatic Repeat Request (HARQ) technique and UL and DL scheduling. RLC layer does error correction via ARQ techniques. PDCP layer mainly handles IP header compression to minimize the number of bits to be sent over an interface and decompression, detection of duplicate data

and their removal via reordering and duplicate detection, ciphering to protect system from eavesdropping and deciphering. And SDAP layer maps the IP packets into radio bearers as required by Quality of Service (QoS) [11].

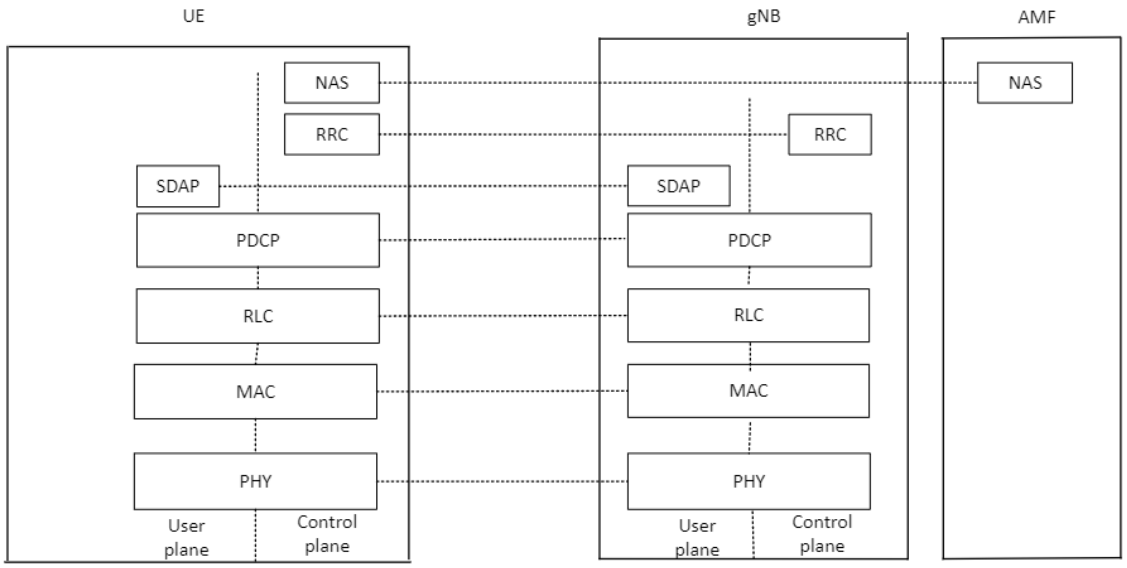

Figure 2.1: User plane and control plane protocol stack of 5G NR [13]

Physical layer is the 1st layer among all the layers of 5G NR. TS 38.200 [14] series describes about the specifications of physical layer. The physical layer interfaces the MAC (Medium Access Control) sub-layer of 2nd layer which then interfaces RRC (Radio Resource Control) layer of 3rd layer. It provides transport channels to MAC sublayer. Data transport services to higher layers is also supported by physical layer. As prioritized in TS 38.201 [15], to support data transport service, physical layer performs several functions like: it detects error on the transport channel and indicates about the error to higher layers, provides HARQ soft combining, provides Forward Error Correction (FEC) encoding or decoding of transport channel, supports rate matching of coded transport channel to physical channels, maps the coded transport channel into physical channels, modulates and demodulates the physical channel, performs power weighing of physical channels, supports Multiple Input Multiple Output (MIMO) antenna processing, time and frequency synchronization, RF processing, measures the radio characteristics and indicates it to higher layers [16].

2.1 5G NR Key New Components of Physical Layer

5G NR system can meet most of the advanced technological requirements as compared to other communication technologies due to the new components and ideas that have been added to it to enhance its technical power. The system supports dynamic Time Division Duplexing (TDD) to improve the scalability. Front loaded DMRS (pipelined implementation) along with the availability to use mini slots have provided the users with low latency communication. The key components that changed the face of 5G are briefly discussed below.

5G NR uses Cyclic Prefix OFDM (CP-OFDM) multicarrier waveform for both UL and DL up to 52.6 GHz. The same waveform for both UL and DL directions makes the overall design simple in communication technology. It also supports an option for DFT-s-OFDM single carrier waveform in UL in case of coverage-limited aspects. Practically, gNB (5G BS) can choose UL waveform to be either CP-OFDM or DFT-s-OFDM where UE should be capable of supporting both [11]. The use of CP-OFDM in both UL and DL supports some advantages as: it simplifies the transmitter and receiver design, gives aligned control and RS design, supports efficient estimation of interferences and their cancellation. The main disadvantage of OFDM signal is high Peak to Average Power Ratio (PAPR). Although, CP-DFT-s-OFDM has lower PAPR, but it is not a good support for MIMO [16].

As shown in Figure 2.2, in a CP-OFDM system, Inverse FFT (IFFT) based modulation of data streams is performed. In an IFFT modulated data streams, a CP is added in the beginning of the signal as a guard interval to avoid intersymbol interference. CP is a copy of the last samples in a time-domain symbol [17]. In this system, the data symbols are obtained by mapping the transmitted bit stream to some constellation points. With the utilization of N-point Inverse Fast Fourier Transform (IFFT), time-domain CP-OFDM symbols are obtained [18] which is given by the expression.

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

Where, S(k) is the data symbol at subcarrier k, N represents total number of subcarriers, T is the OFDM symbol time, $k \in \{0,1, \ldots . N-1\}$ is the subcarrier index, and T_g is the length of guard interval and s(t) is the time domain representation of the OFDM symbols. CP is chosen in such a way that it is greater than the delay spread of the channel. The CP added signal is at the receiver after convolving with the channel [18] [19]. At the receiver,

the CP is removed, followed by the Fast Fourier Transform of the signal to receive a frequency domain representation of the OFDM signal as expressed as:

$$S(k) = \frac{1}{N}\sum_{t=0}^{N-1} s(t)e^{\frac{-j2\pi kt}{T}} \qquad 2.2$$

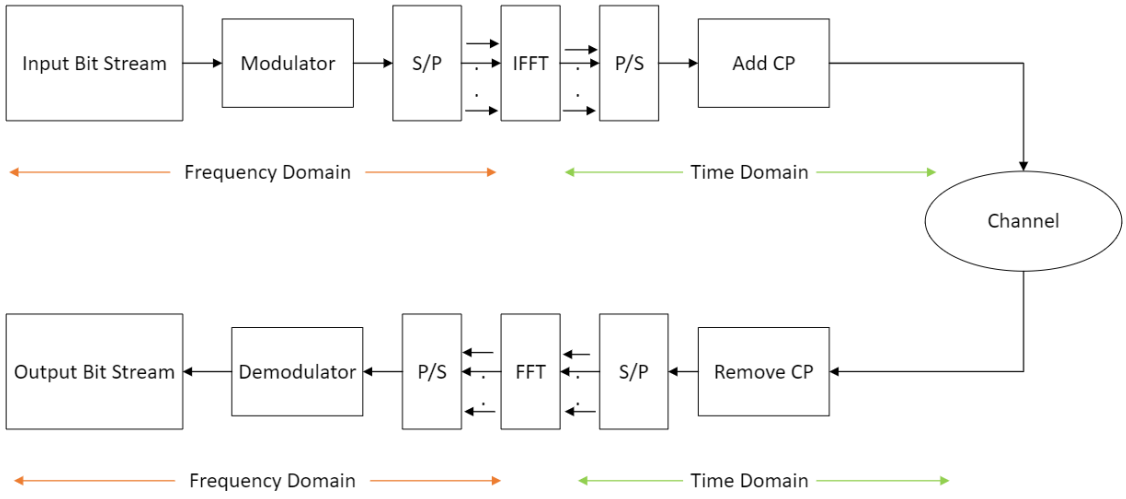

Figure 2.2: CP-OFDM Transceiver block diagram [18]

The OFDM subcarriers in time and frequency domain is shown by Figure 2.3. OFDM has a sinc-shaped spectrum for each available subcarriers because of the rectangular pulse shaping. Figure 2.3 shows the overlapping between the subcarriers in frequency domain, which are separated at the receiver due to orthogonality of OFDM signal and do not interfere with each other. With subcarrier spacing of $\Delta f = \frac{1}{T}$, any two subcarriers are pairwise mutually uncorrelated. The significant reason for the success of OFDM is that it is robust against narrowband interference and frequency selective fading, it is a best suit for the MIMO transmission scenario, there is a simple equalization process when signal combines with CP and it is effectively implemented with the use of IFFT/FFT algorithms.

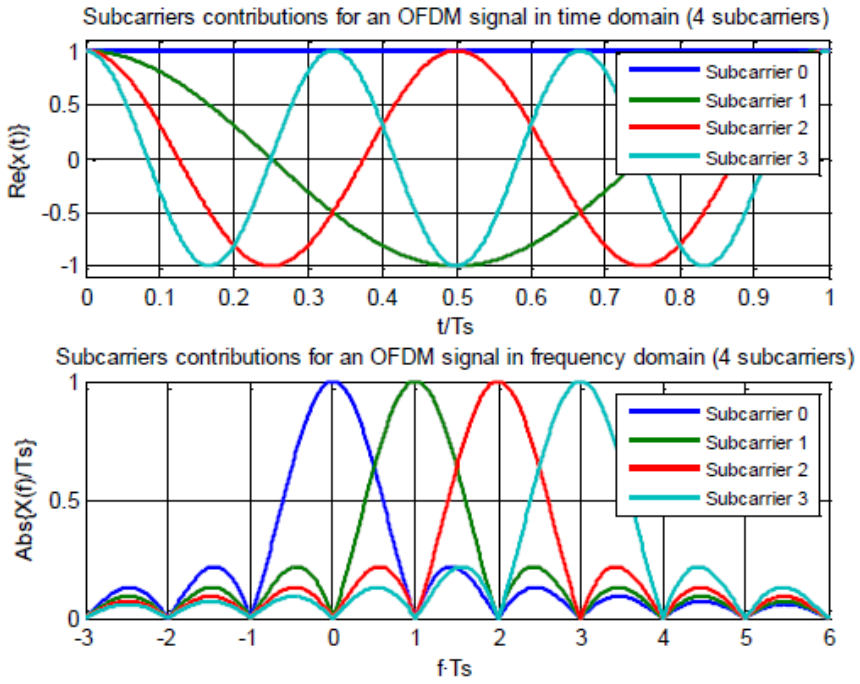

Figure 2.3: OFDM subcarriers in time and frequency domain [20]

Numerology includes Subcarrier spacing (SCS), OFDM symbol duration, cyclic prefix (CP), and Slot duration. The slot duration and cyclic prefix depend upon OFDM symbol duration while OFDM symbol duration is inverse of SCS.

While LTE uses 20 MHz carrier bandwidth along with a fixed CP duration (T_{CP} = 4.96 µs) and a fixed subcarrier spacing (Δf = 15 kHz), contrarily, 5G NR introduces the concept of scalable numerology to provide support for wide range of frequencies and deployment models. Subcarrier spacing is the parameter that sets the change in overall numerology which is scaled by the factor: 2^{μ}, where µ is an integer that ranges from 0 to 4. 2^{μ} is used in 5G NR to ensure that slots and symbols of several numerologies are aligned in the time domain to enable TDD networks efficiently [21] . Table below shows the summary of numerology where a 15 kHz SCS, uses a normal CP of 4.7 μs and has a symbol duration of 66.7 μs. Similarly, all the SCS utilize a normal CP except a 60 kHz which uses both normal and extended CP. From the definition of OFDM, $T = \frac{1}{\Delta f}$. So, when the SCS of the carrier increases, the CP and symbol duration go on decreasing.

Table 2.1: 5G NR numerology structure [21]

μ	$\Delta f = 15 \times 2^{\mu}$ kHz	Cyclic Prefix (T_g) (μs)	Symbol Duration (T) (μs)
0	15	4.7	66.7
1	30	2.4	33.3
2	60	Normal 1.2 Extended 4.2	16.6
3	120	0.6	8.33
4	240	0.3	4.17

LTE is basically designed in such a way that it assumes that the maximum carrier bandwidth is 20 MHz which eliminated several complexities during DC subcarrier handling while causing minimum impact on the cost of device. It was assumed that all the devices received full carrier bandwidth. But this concept is not used in NR. To support the devices which are unable to receive full carrier bandwidth and for the receiver-side bandwidth adaptation, NR introduces the concept of Bandwidth Parts (BWPs) [22].

A BWPs consists of SCS and CP and a set of resource blocks. A particular device can be configured to have up to four DL BWPs as well as up to four UL BWPs for each cell that is serving to the UE. At a given time, in each cell, one of the configured DL BWPs is termed as an active and one of the configured UL BWPs, is termed as an active one. The centre frequency for active UL BWPs and active DL BWPs can be assumed same in case of unpaired spectra, which refers to TDD. The gNB uses same downlink control signalling that it uses for scheduling to activate or inactivate the BWPs. Outside the active BWPs, a device does not receive downlink data transmissions. For example, it does not receive the PDSCH and PDCCH transmissions. A device is only capable of receiving one numerology at a particular time as multiple BWPs cannot be active at the same time. Whereas in the uplink, PUSCH and PUCCH is transmitted by a device only in the active BWPs [22].

In time domain, length of a subframe is always 1ms. However, it has different number of OFDM symbols and slots depending upon the SCS. There are integer number of slots, and each slot has 14 OFDM symbols. These symbols in a slot can be either UL or DL. Each slot carries control signals or control channels at the start or at the end of the slot. This model makes a gNB capable to allocate resources for URLLC immediately after the urgent data comes. Also, NR facilitates the mini-slot configuration to support the transmission of small packets. There are two, four or seven OFDM symbols in a mini slot. These mini slots can also carry the control channels or control signals [23]. Figure 2.2 demonstrates the frame structure of 5G NR. The 15 kHz subcarrier spacing has one slots having 1ms slot duration, 30 kHz SCS has 2 slots with 500 μs duration. With the increase in SCS, the number of slots increases, and slot duration go on decreasing.

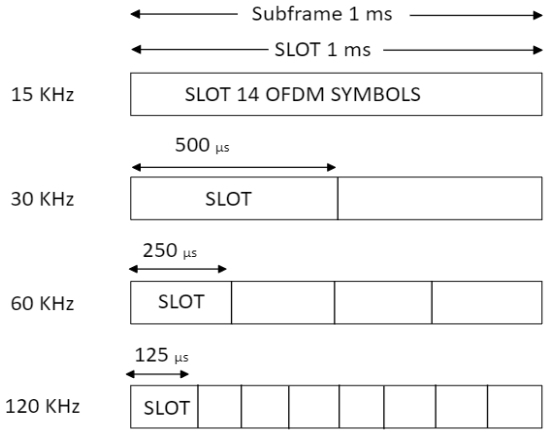

Figure 2.4: Frame structure

The time or frequency grid of subcarriers and symbols are created by the modulated multicarrier waveform. The subcarriers are placed together as Physical Resource Blocks (PRBs) to give frequency domain structure and in the time domain the symbols are placed together to from slots, sub-frames, and radio frames. PRB always contains 12 subcarriers. The bandwidth of a PRB increases when subcarrier spacing increases but symbol duration is shortened [24]. Figure 2.3 is an example of a resource block where x-axis is the function of time containing the OFDM symbols according to the number of slots and y-axis is the function of frequency containing 12 subcarriers in each PRB.

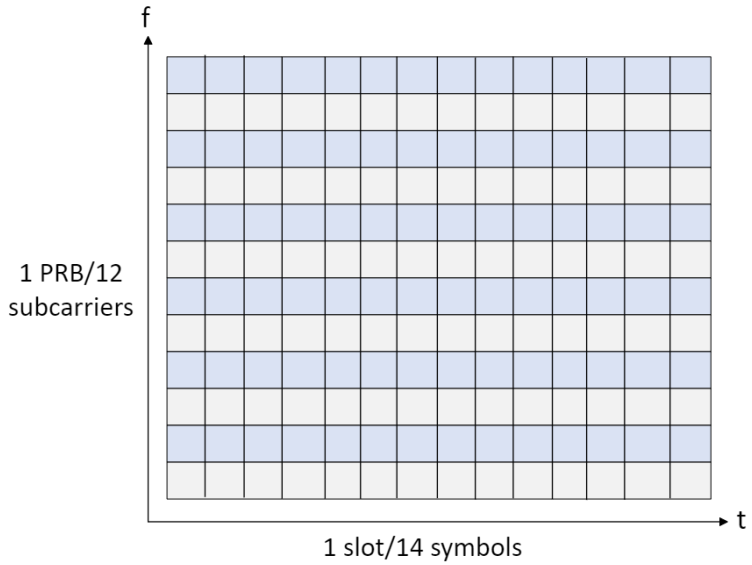

Figure 2.5: PRB / Slot grid [24]

2.2 Physical Layer Vulnerabilities

5G physical layer includes various types of signalling reference signals and synchronization pilots that are exchanged on both the uplink and downlink. The vulnerability of each channel or signal to be attacked by jammer is dependent on the series of factors such as: the sparsity of signals or channels in the uplink or downlink frame that is the percentage of resource elements occupied by the channel or signal, the jamming power required to eventually distort the signal or channel and the level of complexity of the jammer which is based on the need of synchronization to the cell and the need to decode some system parameters [25].

Jammer attacks protocol level, physical layer channels, and signals of 5G. In a physical layer attack, when jammer targets a synchronization signal, it shifts symbol timing peak and prevents UE from receiving primary synchronization signal (PSS). Also, the secondary synchronization signal (SSS) uses a gold sequence within the same set which makes it to have low cross-correlation allowing a UE to differentiate between base stations on same carrier at low SINR making itself prone to jamming [26]. The jammer synchronizes to the system in time and identifies the subcarrier spacing hence jamming the PSS and SSS. The vulnerabilities of channels, signals and resources of physical layer can be reduced significantly by mapping these physical layer resources on the time and frequency grid by utilizing a scheme in which a jammer will not know such mapped structure as it uses the higher layer parameters [27]. This section highlights the structure and resources in the physical uplink and downlink channels, and signals and outlines how they are vulnerable to potential jamming. Although the work in this thesis focuses mainly on the

PUSCH channel, other channels are described for general understanding of the vulnerabilities in those channels.

From the gNB point-of-view, the uplink channels carry the information to upper layer that originates in the lower layer. The physical layer consists of altogether three channels for Uplink which are PUCCH, PUSCH under Uplink Shared Channel (ULSCH) and PRACH under Random Access Channel (RACH) as shown in Figure 2.6. ULSCH supports the use of beamforming, HARQ, dynamic and static resource allocation, and so on, and RACH has limited control information. These channels are also vulnerable towards jamming or interference attack in the system. Their vulnerability to jamming is described in the following sections.

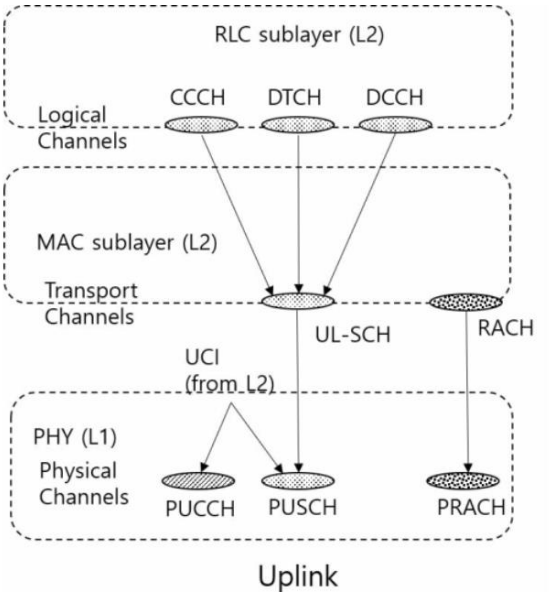

Figure 2.6: Uplink Channels Mapping [28]

PUCCH is mainly entitled to provide the Uplink Control Information (UCI). UE sends an UCI on PUCCH to carry information such as: acknowledgement of the HARQ and the channel state information (CSI) for the transport block of DL-SCH and uplink scheduling request for UL-SCH [28]. There are five formats under which UCI is transmitted on PUCCH. Format 0, a short duration PUCCH, which may be either HARQ-ACK bits or Scheduling Request (SR) bit or both, spanning over 1-2 symbols within a slot and carrying 1-2 Uplink Control Information (UCI) bits. Format 2, a short PUCCH carries more than 2 HARQ-ACK feedback bits and a CSI report. Formats 1, 3 and 4 are long duration PUCCH formats spanning over 4-14 OFDM symbols [29].

These five formats along a set of available parameters by higher layer inform the UE about the subcarrier and symbol that is used to transmit each PUCCH message. Also, its intra-slot hopping mechanism and facility that the PUCCH can be multiplexed into the

PUSCH transmission makes PUCCH a complicated system which cannot be easily jammed. However, if the jammer knows about the intra-slot hopping, it will then jam PUCCH [25].

5G NR PUSCH carries user application data and multiplexed control information. It supports only a single codeword at each time that will be mapped up to four layers. It may contain the UCI such as ACK/NACK, scheduling request and channel-state report to the BS. PUSCH performs CRC addition with payload to detect in case of any errors, then LDPC base graph selection, segmentation of code block, rate matching, code block interlinking, codeword addition, data and control multiplexing, scrambling is done followed by modulation. After scrambling, when one pair of scramble bit is transmitted, PUSCH selects the QPSK modulation techniques but when more than one pair of scrambled bits are transmitted then PUSCH selects 16 QAM, 64 QAM and 256 QAM respectively for modulation. Then, the modulated signals are simultaneously mapped into resource blocks (RB) [30].

PUSCH is jammed by using a white noise in this channel. This white noise is very easy to implement and in return it causes the Denial of Service (DoS) in the entire cell. However, a system either uses a dedicated PUCCH channel or UCI is multiplexed to PUSCH, so even though one is jammed, the other can easily carry UCI to higher layers [26].

The access procedure provided by 5G NR to a regular UEs is like that of the LTE. It enables the random-access preamble from UE to gNB which is a base station for 5G NR on a dedicated RACH. When the base station receives the preamble, it estimates a temporary parameter and assigns radio resources to continue to communicate with UE. The preambles generated by Zadoff chu sequence are used to identify the UE [31].

Although it has large number of possible locations and is too complex to determine the real time positions, the jammer may succeed in determining these locations and jams PRACH. If it fails to determine those locations, then in return it floods the channel with invalid preamble and 5G NR would not have any idea what to be done in this situation [5].

From the gNB point-of-view, the downlink channels carry the information to lower layer that originates in the upper layer. The physical layer consists of altogether three channels for downlink which are PDCCH, PDSCH and PBCH as shown in figure 2.7. This section describes how these channels are vulnerable to jamming.

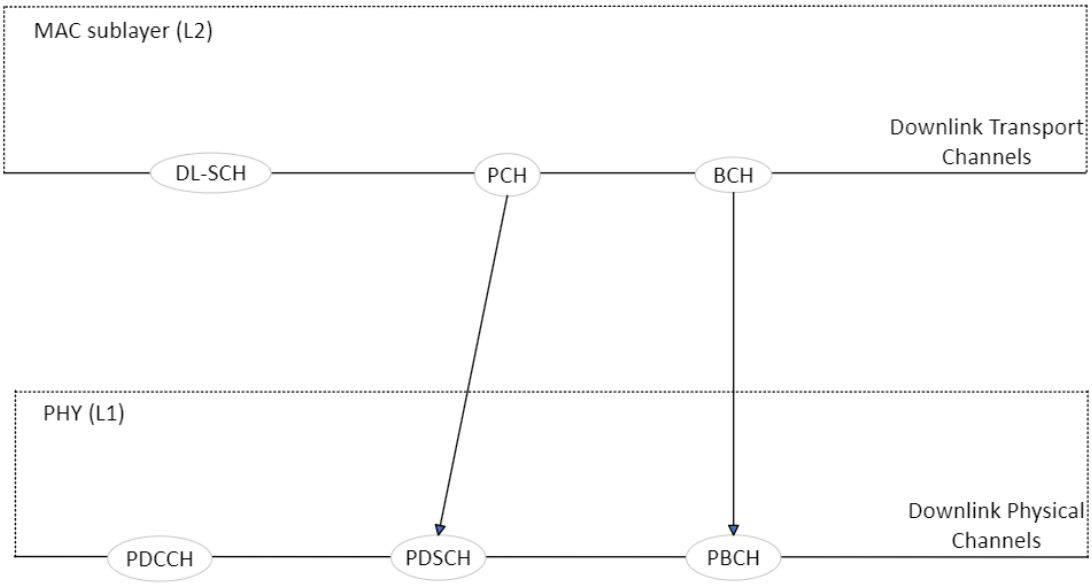

Figure 2.7: Downlink Channels Mapping

PDCCH carries Downlink Control Information (DCI). These DCI data are added with CRC and then performed a RNTI scrambling which is then followed by channel coding, rate matching, scrambling, QPSK modulation and resource mapping. NR CORESET which is a set of physical resource located in a particular region in frequency domain, and a set of parameters carry PDCCH [32].

Jamming the PDCCH means that the jammer must over crowd each area in which PDCCH lies if the jammer is unknown about the CORESET frequency domain. However, the jammer interprets and decodes the information about CORESET frequency allocation via which it jams the sub-carrier via a very small duty cycle according to the CORESET-time-duration value [5]. By assumption of CORESET-frequency domain knowledge, the jammer jams each subcarrier to particularly locate the PDCCH and distort it eventually in both frequency and time grid [27].

PDSCH transmits DL user data, UE-specific higher layer information, paging and system information. In a DL transport block transmission, transport block CRC is appended to give error detection and then selection of LDPC base graphs (NR supports two base graphs: one for small transport block and the other one for the larger transport blocks). Then rate matching done to the coded blocks followed by concatenation of code block, scrambling, and modulation to generate complex-valued modulation symbols [33].

Since it carries both the configuration as well as the downlink user data, it permits the jammer to target more than one UEs to jam. Hence it requires DCI decoding and precise synchronization to locate UE’s resources [26].

The SS/PBCH block transmitted in PBCH is used for beam and cell measurements, initial cell search, new beam identification, and radio link monitoring process. PBCH is assigned with 4 OFDM symbols and 240 subcarriers. SSS is transmitted through the unused subcarriers in between frequency allocation in a PBCH symbol [34]. If the carrier is below 3 GHz, base station PBCH are given 2 slots and for above 3 GHz, it is assigned with 4 slots. With the increase in SCS, slot duration decreases. As a result, jamming duty cycle also decreases [25].

The jammer jams PBCH so that the UEs are deprived of accessing the vital information from the 5G NR system distorting the channel in a time-selective format [27]. Still, the selective jammer can target to jam the PBCH with a low duty cycle since the symbols are close to each other in any scenario. The PBCH has so vulnerable design that even the use of higher frequency in it does not permit for signal propagation at a longer distance and hence making a jammer to get close to mobile station to launch its attack. The source of this jammer can be identified and stopped by using a localization-based detection mechanism. But in case of a movable jammer, the jammer detection technique should monitor its movement to detect its position [5].

2.3 Reference Signals and Their Vulnerabilities

An OFDM uses reference signals to estimate the multipath communication channel as well as to detect the traffic channel or control channel reliably. Reference signals allows the estimation of the channel frequency response. Several reference signals transmitted in the uplink and downlink support the channel tracking [35].

DMRS, PTRS, CSI-RS, SRS are the reference signal used by 5G. In uplink, two types of waveforms are supported which are: CP-OFDM and DFT-s-OFDM. The front loaded DMRS are situated at first OFDM symbol that are assigned for PUSCH. During transmission, PTRS is aligned with one DMRS port. It is restricted towards scheduled BW and duration that are utilized for PUSCH. SRS signal is used for UL channel sounding. It is also UE-specific like DMRS. Multiple number of SRS symbols support extended coverage and enhanced sounding capacity [36].

UE-specific DMRS for PDCCH is used to estimate the downlink channel to demodulate the PDCCH coherently. UE-specific DM-RS for PDSCH is used to estimate the downlink channel to demodulate PDSCH coherently. UE-specific PT-RS is used with DM-RS for PDSCH to correct Common Phase Error (CPE) between PDSCH symbols that does not contain DM-RS. UE-specific CSI-RS is used to estimate CSI to measure and report CSI which helps gNB in case of resource allocation, MIMO rank selection, beamforming, and modulation coding scheme [35].

Jammers usually select to jam those reference signals which are important to operate the link between the transmitter and receiver and require less amount of energy to be jammed which means the presence of least number of resource elements (REs) per frame. This criterion is matched with DM-RS for PBCH because it is in the same place in each frame while it only needs the information about the cell ID and the location of PBCH which can be known if the jammer has time synchronized with the frame. DM-RS for PBCH occupies one-fourth of the REs that are allocated to PBCH by jamming 60 subcarriers without requiring synchronization to cell [25]. The jammer causes faulty channel conditions for DMRS. It diverges the channel conditions which in return limits the physical channel throughput [26].

3 ATTACKS ON WIRELESS NETWORK AND THEIR DETECTION TECHNIQUES

Although the wireless network technologies are gaining a wide popularity in terms of their deployment, usage and efficiency, these technologies are more easily attacked than any wired system. The broadcast feature and open communication of wireless technology makes it available to both the authorized and illegal users in contrary to wired system in which the devices are physically connected via wires making it unavailable to illegal users. Wireless networks are prone to jamming attack, eavesdropping attack, DoS attack, MITM attack, spoofing attack, message falsification attack [37], node capture attack, etc.

In a communication system, network node is a point where it receives, sends, creates, or stores the information. One node communicates with another by transmitting data via a link which could be cable, fiber, or a wireless communication [38]. So, there are more chances that jammer captures the node to inject its effect on the communication system. Some of those attacks in wireless networks are briefly described below:

The unintentional failure of nodes or some suspicious actions produce Denial of Service DoS attack in a wireless network. The DoS attack captures the resources before it is being sent to the receiving node and sends the unnecessary packets preventing the receiver to get the original one. DoS attack could happen in any layer of 5G system. The physical layer DoS attack is termed as jamming [39] which is briefly summoned in Section 3.4.

Eavesdropping is the method of hearing a private conversation illegally. Eavesdropping attack in wireless network is the process in which the essential information is collected from a network by snooping on transmitted data. Although it does not impact the data rate of the desired link, the attacker steals the very private information like User ID and password [40]. Due to its passive nature, it is hard to detect this attack. To overcome its effect, encryption of the signals is done over a radio link. However, the encryption algorithm must be strong enough [41].

Man In the Middle (MITM) attack is an active attack where the attacker secretly controls the communication channel between two authorized users [42]. The message between the users could be intercepted, replaced, or modified. Being the most common threat in wireless networks, in a false base station based MITM attack, an attacker forces the authorized users to make a connection to a false BS which is solved by the mutual authentication between a BS and UE [43].

3.1 Jamming attack

All wireless networks contain interference due to the nature of wireless communications. This is something that the network operators may control and something we need to handle in the receiver. The work in this thesis focuses on non-intentional interferences, targeting to degrade the quality of wireless service in specific geographic area.

Jamming is the disturbance caused in the already existing wireless communication system by decreasing signal to interference and noise ratio (SINR) at the receiver part by transmitting interfering wireless signals in the system. Jamming differs from interference in the sense that jamming is intentional whereas interference is unintentional [44]. Like any other wireless technology, 5G is also vulnerable to potential jamming attacks. Jammers introduce an unwanted DoS by sending radio signals that gets mixed up in the channel causing decrease in SINR of the legal users and interrupts the actual communication link. Jammers target both the physical layer and cross-layer of the wireless system [7]. While there exists any problem, there is always some rays of hope for the solution. A list of possible types of jammers that could harm the 5G system in various ways are defined in Figure 3.1 and eventually the jammer detection mechanism is described in section 3.3.

Under Elementary and Advanced categories, jammers are further divided into Proactive, Reactive, Function-specific, and Smart-Hybrid groups which are again sub-grouped into constant jammer, random jammer, deceptive jammer, Data/Ack jammer etc. which is pictured in the Figure 3.1 and further described in the following sections.

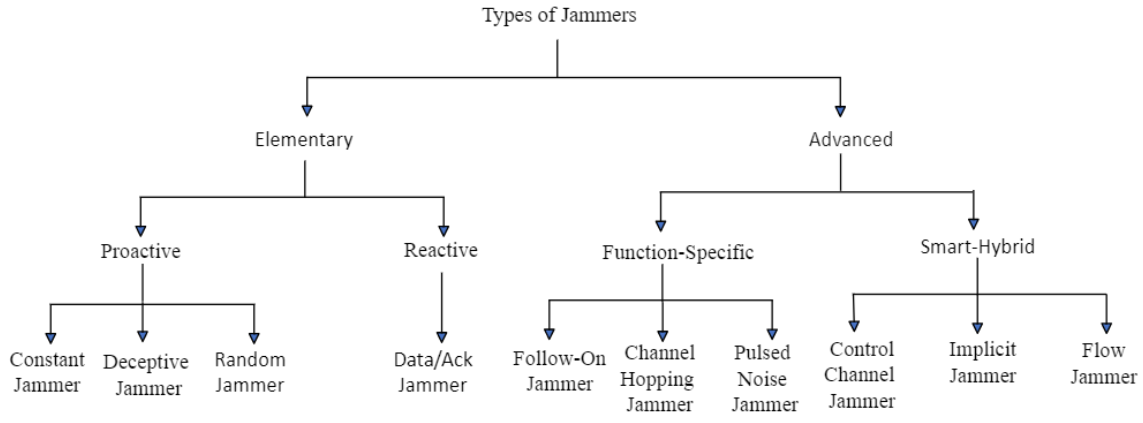

Figure 3.1: Types of Jammers [45]

3.1.1 Proactive Jammer

Proactive jammer sends the jamming signal regardless of any communication of data in the system. It sends the random bits and packets into the channel where it is operating, making all other nodes in non-operating mode. It stays on the same channel unless its energy is completed and does not switch channels [44]. Under proactive jammer, there are three types of jammers namely constant jammer, deceptive jammer, and random jammer.

A constant jammer continuously sends radio signals in a wireless medium. These continuous signals consist of random bits eventually interfering any node that has been transmitting signals to corrupt the output at the receiver by lower packet delivery ratio (PDR) where PDR is the ratio of number of successfully sent packets by the transmitter to the total number of packets received. This jammer puts a legal transmitter in illusion by making it feel the channel busy and preventing it from getting access to the channel which is termed as lower packet sent ratio (PSR) [46]. PSR is the ratio of successfully sent packets by a transmitter as compared to the packets that were intended or assumed to be sent out [47].

A deceptive jammer continuously sends normal packets instead of random packets which makes other nodes believe that the actual or valid transmission is going on so the nodes will always be in receiving mode until jammer itself gets turned off [48]. In other words, the jammer deceives the nodes.

A random jammer, also termed as a memoryless jammer attacks the wireless system by sending the signals only for a random period whereas turns the sleep mode on for itself at other times. This type of jammer is more difficult to detect in comparison to constant jammer [49].

3.1.2 Reactive Jammer

Reactive jammer is also known as an intelligent jammer which takes the active or inactive position with respect to the situation of channel. If it detects any transmission going on in a channel, then it becomes active and sends illegitimate packets. And when channel is inactive, it also stays inactive and keeps sensing the channel [50]. This jammer is also known to be an energy efficient jammer since it only operates when it senses any transmission in the channel. Since the jammer must quickly shift from the listening mode or sensing mode to the transmitting mode, it requires very sharp timing constraints [49]. The sensing of a channel causes a small delay. For example, to sense a channel, the jammer should detect the energy (which is most popular technique to sense the channel) and upon

implementation in a FPGA system for fast speed, jammer takes about 1ms for energy detection to detect the presence of target signal. Additionally, after detecting the target signal, it needs to switch its quiet mode to transmitting mode which further takes time. This type of jammer is not only cost effective in comparison to constant jammer, but also difficult to track and remove due to its irregular behaviour [51]. Data/Ack jammer falls under reactive jammer.

Data/Ack jammer interferes the system by corrupting data of acknowledgement packet transmission. When a transmission of data starts, the jammer starts to react. It either corrupts the data packet or waits until the packets reach to the receiver side and harms the ACK packets. The interference in the data or ACK packet will result in the re-transmission. When the data packets were not received correctly at the receiver, there should be a re-transmission and further when the ACK packet is not received by the receiver, something wrong is sensed for example, buffer overflow hence, re-transmission occurs [44].

3.1.3 Function-specific jammers

This jammer is implemented via a pre-determined function. These jammers can be proactive or reactive which works on single channel to save energy and then consecutively jam multiple channels. Although the jammer is jamming a single channel initially, it can change the channel as per the specific functionality [44]. Follow-on jammers, pulsed noise jammers, and channel-hopping jammers are categorized under function specific jammer.

Follow on jammers disorganize several channels randomly and at high speed for a short period of time. It is effective against FHSS modulation which uses slow hopping rate [45] due to the jammer's high frequency hopping rate. Even if the transmitter detects the jamming and changes its channel, this jammer will again scan for the entire band and search for the new frequency to distort again. This jammer preserves its power as it only attacks to a single channel before it hops to the next one [52].

Pulsed-noise jammer jams multiple channels with several different bandwidths over multiple periods. It conserves its energy by turning on and off multiple times [45] like a random jammer as per the schedule by which it is programmed for. It can jam multiple channels rather than jamming a single channel [52].

Channel-hopping jammer hops between several channels to distort or interfere data transmission simultaneously [45]. These jammers have direct access to channels. It also has the capability to jam multiple channels like pulsed-noise jammer. At the time of its discovery or initial phase, it is invisible to its neighbours and remains in a quiet mode [52].

3.1.4 Smart-hybrid jammers

These jammers are smart due to their effective jamming behaviour as well as power efficient feature. Their significant motive is to magnify own jamming effect in any network that they jam. On the other hand, they conserve their own energy and can act as both proactive and reactive jammer [44]. Three types of jammers come under smart-hybrid jammers namely, implicit jammer, control-channel jammer, and flow jammer.

In an Implicit jamming, soon after jammer completes deactivating the intended target, it passes to another node of the network to distort it by causing DoS attack [45]. It not only distorts the communication mechanism of intended node or channel but also causes the starvation to other clients in the neighbour that uses same access point as the attacked client [53].

In a multi-channel communication network, control channel jammer jams the control channel specifically, blocking the exchange of information between the transmitter and receiver. It targets and alters the control channel which causes severe damage to all channels on same network [45]. These types of jammers come into action even before the communication system is in operation. In 5G communication system, the control channel that is most vulnerable to malicious jamming is CORESET [27].

A flow jammer blocks the flow of network traffic via multiple jammers by taking information about the network layer [45]. This jammer involves several other jammers in the networks to interfere packets to minimize the data flow. These jammers can also be proactive and reactive both and are energy efficient. They can jam single channel as well as multiple channels. In a centralized control model, the jammer acts respectively after the minimum power to jam the network has been computed. Similarly, in a non-centralized model, every jammer exchange information with their neighbors to enhance the efficiency [54].

3.2 Jammer Detection Mechanism

Jammer detection mechanism is the initial step towards introducing a secure wireless communication system. However, it is relatively challenging because of the unusual behavioural model of jammers and difficulty to locate a jamming scenario from a legitimate activity. Other conditions like congestion in the network due to excess traffic loads affecting the packet sent ratio and packet delivery ratio, and the communication interruption due to some error at the receiver section might cause confusion about the presence of the jammer. So, the system must be capable to determine the presence of jammer by evaluating certain conditions [55].

The utilization MIMO technology in the system might make the vulnerabilities in the uplink transmission more resilient. A massive MIMO configuration in the base station can receive multiple streams of data from multiple users and can separate them with respect to the direction of their arrival [27]. Meanwhile, jammers can be detected either via metric threshold-based mechanism or via machine learning techniques. Detection mechanisms range from packet-level network measurements like PDR, bad packet ratio (BPR) to energy consumption amount (ECA) and channel utilization. Some also use received signal strength (RSS) and signal collision ratio-based detection strategy for jamming detection [56]. These detection strategies are briefed below. Most of the detection mechanisms explained here works above physical layer.

Packet Delivery Ratio with Received Signal Strength (PDR with RSS) PDR alone, cannot determine the jamming since the reason for PDR packets drop could also be bad connection, node defect and collisions. These states are false alarms. PDR along with RSS can improve the detection of jamming [57]. In case of low PDR and high signal strength, it can be assumed that the jammer is present. The threshold PDR and signal strength could be assumed beforehand. If obtained PDR is above threshold PDR and signal strength is lower than threshold signal strength, the channel is assumed not to be interfered [58].

Bad Packet Ratio (BPR) is the ratio of number of damaged packets in the receiver to the total number of packets received at that certain time. The bad packets are determined via cyclic redundancy check. These received damaged packets are discarded and good packets are approved for transmission. This mechanism is efficient due to its easy calculation. Also, this method can be utilized in the channels where acknowledgements are not required. Bit Error Rate (BER) can be determined via calculating the ratio of number of corrupted bits to the total bits received during a transmission by a node. This mechanism helps in the detection of reactive jammers [59].

Energy Consumption Amount (ECA) is the amount of energy that is consumed by a node at a given time. It is computed by multiplying the squared value of voltage drop in the battery of the node with time duration and dividing the result with average resistance of the node. Jammers force the node to remain in the BACKOFF state although they should have been in IDLE mode which causes the nodes to consume more energy than regularly consumed energy. This metric-based detection mechanism is usually referred in case of Wireless Sensor Network areas [57] [59] [60].

Signal-to-Noise Ratio (SNR) is measured as the ratio of received signal power to the received noise power at a particular node. It is one of the effective jammer detection mechanisms at physical layer since there is no jamming experience at the physical layer without the drop in SNR value [60]. Fuzzy Interference System computes the jamming

index via SNR and packet dropped per terminal (PDPT) values. Here, a base station processes the detection algorithm to get the information about the number of packets received by the node, packets dropped by the node, and signal strength. Then the PDPT and SNR is calculated to analyze the presence of jammer [44].

Ant system mechanism detects jamming at physical layer. It proposes the method to test whether the system has experienced an interference or not. For this, an agent is created that travels through the nodes iteratively and with the information given by this agent, the system then gathers a set of data about several routes that reach to the destination. These collected information are stored in the list and used for redirection. The jamming is identified to be either true or false based on metrics like PDR, BER, SNR, energy, packet loss, expanse etc. After checking the available metrics, a decision model is developed that clarifies if jamming exists or not [54] [48].

Jammed-area mapping protocol (JAM) is a jammer detection as well as jamming mitigation techniques that prepares the jammed region in wireless networks and directs the packet around the jammed area. It is particularly applicable for wireless sensor networks. A jammer is detected if the node's utility drops below some threshold value. For example, if the number of unsuccessful attempts to capture a node exceeds 10, then the presence of jammer is assumed. Similarly, the system gives jammed or unjammed message that is transferred to the neighbouring node to make them known about the situation. After the reception of jammed message, the node formulates the countermeasure to overcome jamming [44].

4 PHYSICAL LAYER JAMMING DETECTION

A general description on the jammer detection algorithms is needed before designing the system model. Many of the notations and definitions mentioned in this chapter will be applied in the later chapter for algorithm development. Theoretical and mathematical analysis and characterization of power calculation of empty PRBs to be utilized in relative and absolute thresholding is presented in this chapter. Short-term averaging window and long-term averaging window methods are also briefed. These averaging window methods are later combined with thresholding technique to detect the interfered PRB. This chapter also includes the introduction about basic probabilities of jammer detection like correct detection, false alarm rates, miss detection and detection delay. However, this thesis presents the detection result only in terms of correct detection and false alarm rates.

In this thesis, the physical layer jamming is detected based on the presence of energy in the resource elements in the UL region that are not assigned to any UEs. The power of each empty or unoccupied physical resource blocks (PRBs) in each symbol is calculated per slot and each individual power is averaged per occurrence of empty PRBs by utilizing an averaging window concept. Empty PRBs are those PRBs that are not allocated to any physical channel in the system. Here, slot based relative and absolute thresholding, short-term window based relative and absolute thresholding and long-term window based relative and absolute thresholding techniques are utilized to detect the interfered PRBs. The power calculation method is taken in reference to the power calculation of any complex symbols which is explained in Section 4.1. The metrices like SNR, SIR, SINR and INR that are used in the jammer detection and in the calculation of jammer probabilities are also described in this section.

SNR is the ratio of signal power to thermal noise power. It is expressed in decibels (dB). If the ratio is greater than 0 or 1 dB, it signifies that there is more signal power than the noise power. Mathematically,

$$SNR = 10\log(\frac{P_s}{P_n}) \tag{4.1}$$

Where P_s is the signal power and P_n is the thermal noise power.

SIR is the signal power to interference power ratio. Here, the interference power is the received power from the co-channel interference. For example, crosstalk. SIR is also expressed in dB. Mathematically,

$$SIR = 10\log(\frac{P_s}{P_I}) \quad 4.2$$

Where P_s is the signal power and P_I is the interference power.

SINR is the ratio of signal to interference and noise power ratio which measures the wanted signals strength with respect to the unwanted interference and noise signal strength. Mathematically,

$$SINR = 10\log(\frac{P_s}{P_n + P_I}) \quad 4.3$$

The Interference to Thermal Noise Ratio (INR) is defined as INR (dB) = SNR (dB) - SIR (dB). So, basically higher INR means interference is greater than the thermal noise, it is easier to detect the interference and results are far better with higher INR. And then INR is more intuitive, because it gives better picture about the detection conditions than the SINR. In this thesis, the results related the probabilities of jammer detection like correct detection probability and false alarm rates are demonstrated in terms of INR.

4.1 Jammer Detection via Relative and Absolute Threshold

After converting the received signal y(t) into the frequency domain Y(k) (the process of obtaining the received signal Y(k) is briefly described in Section 5), the subcarriers outside the bandwidth parts are removed and then the PRBs are re-ordered and indexed from 0 to $N_{PRB} - 1$ (Number of PRBs remaining in the bandwidth part).

To calculate the power of empty PRBs in an OFDM, let the set of all PRB indices is defined as S_{PRB} equals $\{0,1, \ldots . N_{\text{PRB}} - 1\}$ where N_{PRB} is the total number of PRBs in an OFDM symbol. The size of the set of all PRB is $|S_{PRB}|$ equals N_{PRB} . Set of empty PRB indices is defined as $S_{empty} \epsilon S_{PRB}$. So, the empty PRB wise power computation is given by:

$$P(n,s) = \sum_{k=12n}^{k+11} [real(Y(k))^2 + imag(Y(k))^2], n \epsilon S_{empty} \quad 4.4$$

Where, $P(n,s)$ is power of an empty PRB, n refers to the PRB index, s refers to the OFDM symbol index, Y(k) frequency domain representation of the received sample on subcarrier k, k is the subcarrier indices running through the given PRBs.

When number of slots would be less or equal to the measuring period (measured in slots when there is no jammer), maximum threshold (max_{Th}) and minimum threshold (min_{Th}) are updated with respect to maximum PRB wise power ($\max(P(n,s))$) and minimum PRB wise power ($\min(P(n,s))$) obtained from the measuring period. So, max_{Th} equals ($\max(P(n,s))$) and min_{Th} equals ($\min(P(n,s))$). Then the difference between this maximum threshold and minimum threshold is stored as delta threshold. Mathematically,

$$\Delta_{Th} = max_{Th} - min_{Th} \qquad 4.5$$

Where, Δ_{Th} is the delta threshold, max_{Th} equals maximum threshold, and min_{Th} equals minimum threshold.

In this thesis, the calculated power is accordingly compared with the threshold power value to detect whether the system has undergone jamming attack or not. Threshold is the value above which a higher power would mean that there is a jamming attack. It is very informative when determining if there exist a jamming or not [61]. Threshold is further divided into two sub-groups: Absolute and relative threshold.

Absolute threshold is related to absolute power like thermal noise power in receiver. In this thesis, we simply focus on measurements within slot duration. For the calculation, we assume that there is no interference at a given period, this period is then used to measure the power in empty PRBs. After extracting the power of each empty PRBs, the minimum and maximum power values over a measuring period is taken as a reference. The maximum value of the measured PRB wise power is used for absolute threshold-based detection technique.

Relative threshold is the relative difference in frequency domain within the slot. In relative thresholding, the power of all empty PRBs is compared with the sum of delta threshold and minimum power per PRB per OFDM symbol. If the power of an empty PRBs is found to be greater than or equal to the sum of delta threshold and minimum power of empty PRBs, that PRB is an interfered PRB as shown in figure 4.1. Here, the minimum power is a minimum power of empty PRBs of slot, the minimum power of a short-term window as average power matrix or the minimum power of a long-term window as average power matrix during measurement based on slot, short-term window, and long-term window respectively. And total power of empty PRB is the total power of empty PRB per OFDM symbol in case of slot, average power matrix in a short-term window ($PE_{WST}(n,s)$) and average power matrix in a long-term window $PE_{WLT}(n,s)$ during measurement based on slot, short-term window, and long-term window respectively.

Whereas in absolute thresholding, *power_matrix_slot* (a matrix containing the power of empty PRBs in a slot) is created which is always reset for the next slot. For a slot based absolute thresholding, if a single element in the *power_matrix_slot* is greater than or equal to the maximum threshold, then the PRBs in that slot is an interfered PRB as illustrated in figure 4.1. Whereas in a short-term window based absolute thresholding, if the short-term window's single element in the average power matrix is greater than or equal to the maximum threshold, then the PRB of the short-term window is interfered. Similarly, in a long-term window based absolute thresholding, if the long-term window's single element in the average power matrix is greater than or equal to the maximum threshold, then the PRB of the long-term window is interfered.

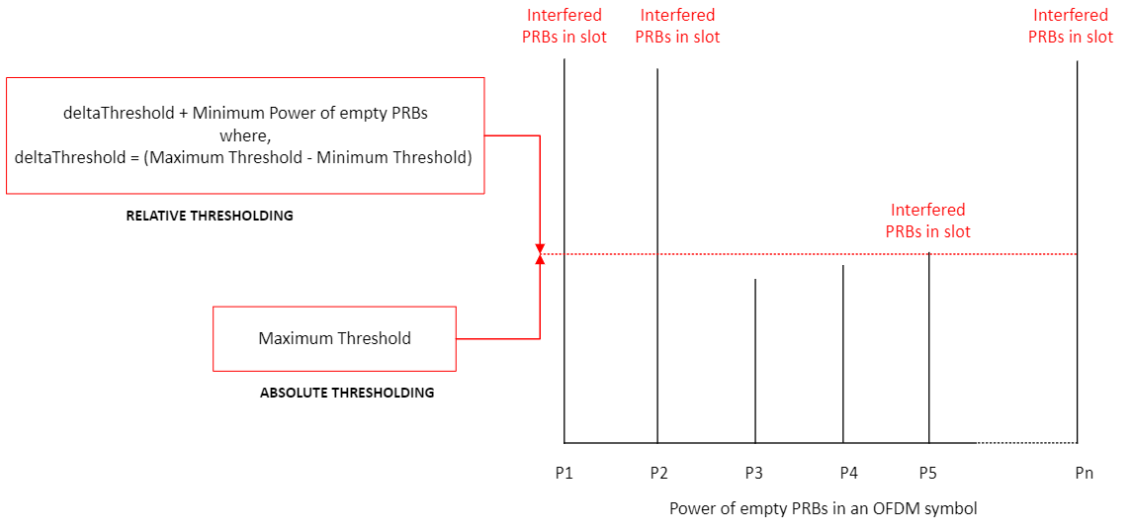

Figure 4.1: Relative and Absolute Thresholding

4.2 Averaging Window

Averaging window concept is the element wise division of accumulated power of empty PRBs of each OFDM symbol in all available slots within the averaging window with their frequency of occurrence respectively. Once the power of each empty PRB is calculated, it is averaged per averaging window with the count on how many times that empty PRB position is being repeated over each averaging window. This process is pictorially expressed below where s1…s14 are the fourteen OFDM symbols in a slot, PE equals $P(n, s)$ is the power of each empty PRBs in the symbol, and N is the total number of PRBs per carrier. This accumulation of power matrix and the count of the frequency of occurrence of empty PRBs continues until the last slot. Averaging window is classified further into two subgroups following the slot-specific calculation which is described in sub-section 4.2.1 and 4.2.2.

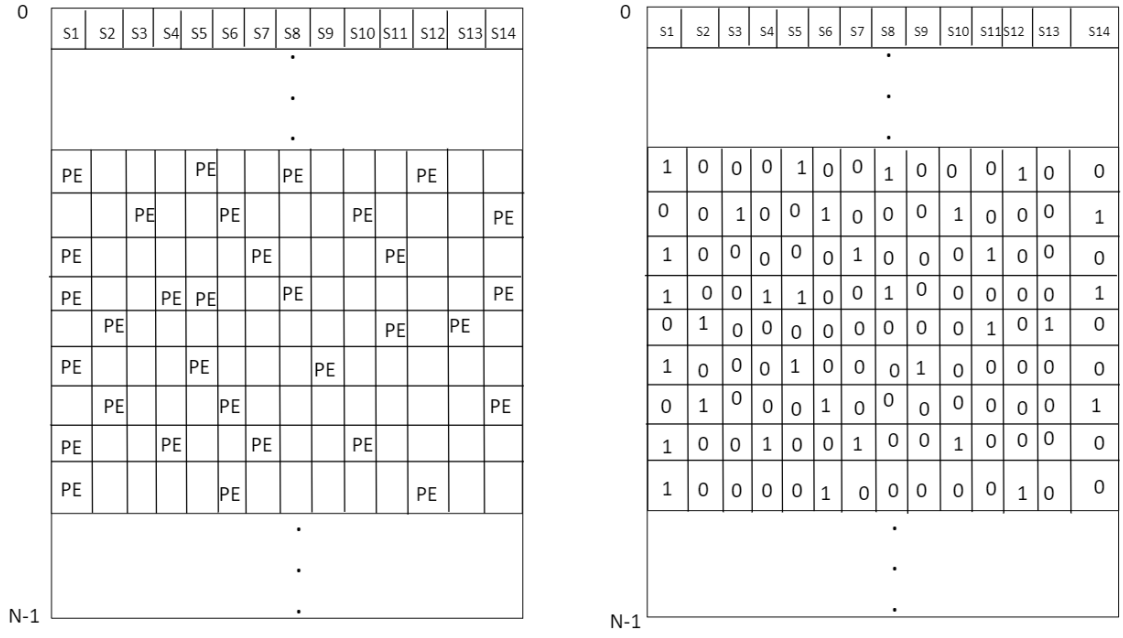

Figure 4.2: Accumulated power matrix and frequency of occurrence of empty PRBs in each symbol of 1st slot.

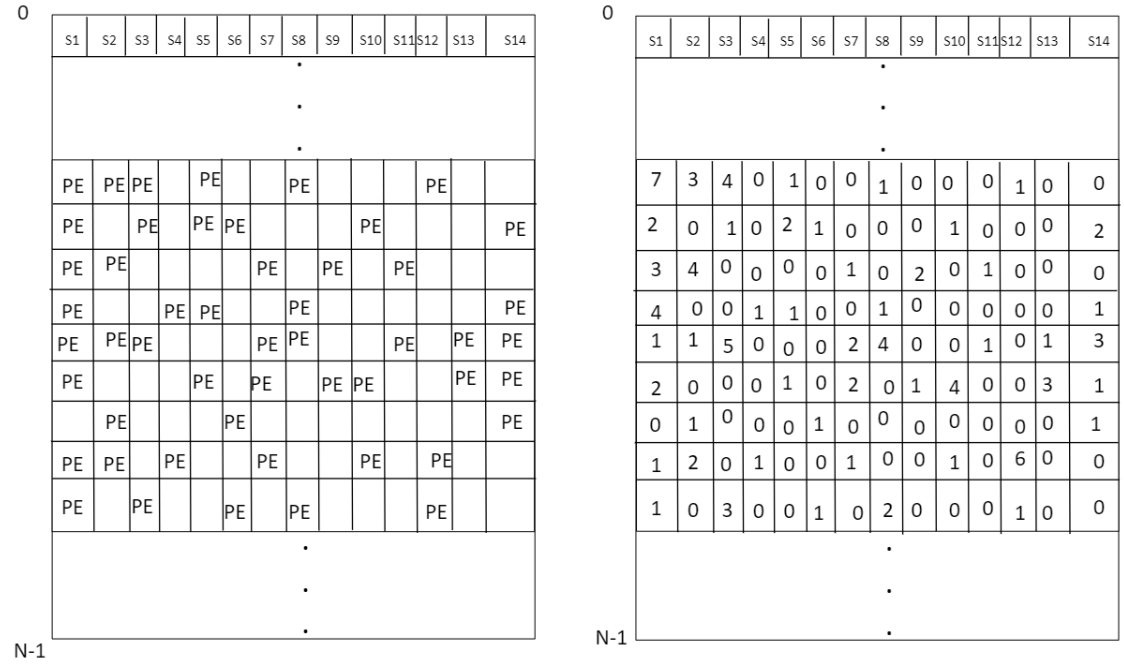

Figure 4.3: Accumulated power matrix and frequency of occurrence of empty PRBs in each symbol of 7th slot.

4.2.1 Short-term averaging window: In a short-term window, a given number of radio frames is defined, a radio frame lasts 10ms. For instance, from 1 to 100 radio frames and average window is taken during that period. It allows the faster detection of interferers and adopts faster to the changes in the operation environment.

In this thesis, the duration of short-term window in slots is initialized with some value and denoted by short_time. If the number of slots is equal to the short_time, then the short-term window is supposed to be completed. After this the short-term window is calculated as average power matrix by dividing the accumulated power matrix in a short-term window with the occurrence of empty PRBs in that short-term window. Accumulated power matrix and occurrence of empty PRBs of short-term window are emptied after the completion of that short-term window. Mathematically,

$$WST = PE_{WST}(n,s)/N_{WST\_emptyPRBs}(n,s) \qquad 4.6$$

Where, WST equals short-term window as average power matrix, $PE_{WST}(n,s)$ is the accumulated power matrix of empty PRBs in a short-term window (adding multiple $P(n,s)$ obtained in a short-term window), and $N_{WST\_emptyPRBs}(n,s)$ is the occurrence of empty PRBs in a short-term window.

4.2.2 Long-term averaging window: Two different methods to calculate a long-term window were utilized in this thesis and tested. After each produced similar result, the long_time utilization approach was adapted for easiness since it is like the approach for calculating short-term window.

In a long-term averaging window, after the completion of each short-term window, the previous long-term window is combined with the current one by using a forgetting factor. It allows to create better time average information of the nominal interference level in the environment. In the beginning when first short-term window is obtained, forgetting factor is not applied to it but after that for instance for second, third and so on, we combine it with forgetting factor. It is represented in formula below.

$$WLT(t) = \Big(\big(WLT(t-1)\big) * f\Big) + \big((1-f) * WST(t)\big) \qquad 4.7$$

Where, $WLT(t)$ is the long-term window as average power matrix at time t, $\big(WLT(t-1)\big)$ is the previous long-term window, f is the forgetting factor and $WST(t)$ equals new short-term window at time t.

Initially, $WLT(t) = WST(t)$.

Another way to calculate the long-term window is like that of the short-term window. The duration of long-term window in slots is initialized with some value and denoted by long_time. If the number of slots is equal to the long_time, then the long-term window is supposed to be completed. After this the long-term window is calculated as average power matrix by dividing the accumulated power matrix in a long-term window with the occurrence of empty PRBs in that long-term window. Accumulated power matrix and occurrence of empty PRBs of long-term window are emptied after the completion of that long-term window. Mathematically,

$$WLT(t) = PE_{WLT}(n,s)/N_{WLT\_emptyPRBs}(n,s) \qquad 4.8$$

Where, $PE_{WLT}(n,s)$ is the accumulated power matrix of empty PRBs in a long-term window (formed by adding multiple $P(n,s)$ obtained in a long-term window), $N_{WLT\_emptyPRBs}(n,s)$ equals occurrence of empty PRBs in a long-term window.

Averaging windows impact the detection probability and detection delay in such a way that with the increase in averaging window, detection probability and detection delay (described briefly in later part) might increase or decrease depending upon which jammer is present. The increased detection delay prevents the system from detecting the jammer soon. And until it gets detected, it would have caused a larger damage which could possibly increase the system complexity.

4.3 Basic Probabilities for Jammer Detection

Physical layer security issues are rather critical matter because this layer has a vital role in establishing communication between via physical medium, so, it requires more attention towards maintaining the desired security level [62]. Based on local detection, simple threshold algorithm and cumulative sum (cusum) change point detection algorithms are applied by some references. Where, cusum is a sequential change point detection technique in which an interferer is detected based on instantaneous change of a particular metric. These both types are based on measuring SNR: average SNR, maximum SNR, minimum SNR, maximum-minus-minimum SNR over a small-time window and comparing it with the large time window. Whereas cusum detects the abrupt change of a measured metric (SNR) before the jammer attack and after the attack. It is applicable only when the average metric value is assumed negative before attack and becomes positive after the attack. The performance of these algorithms is determined with respect to false alarm rate (FAR), detection probability (DP) also known as correct detection, average

detection delay (DD), faulty detection and robustness to several detection threshold values calculated over a slot, short-term window, and long-term window based on relative and absolute thresholding [61].

If an interferer is active within the slot or short-term window or long-term window, then it is termed as an attack. One jammer attack is defined as one random realization when the interferer is in on mode. Alternatively, if somewhere in the slot there was interferer, and in some PRBs and in some OFDM symbol if we get the indication of interference then it is correct detection.

Detection probability is the ratio of only the detected attacks over received total number of attacks in a communication system [61]. It is the probability of detecting the interferer when it is present over an input heat map (described in later part). A heat map can be based on slot wise power measurement, short-term window wise power measurement and long-term window wise power measurement. In this thesis, probability of detecting a jammer is quite directly dependent on the fraction of empty PRBs where, the fraction of empty PRBs is defined as the number of empty PRBs divided by the total number of PRBs. In this thesis, we focus on 50% of empty PRBs. The more the empty PRBs, the better the detection is assumed since more measurements is obtained with a greater number of empty PRBs. Also, increase in SNR, increases the detection probability.

In a heat map, in case of presence of jammer, it would be one attack. It is possible for the interferer to be in only some part of averaging window or in the whole part. Overall, the simulated averaging window gives the idea about how many attacks have been detected. The output of the jammer detection block at every slot is analyzed. In this thesis, 99% target is defined to be the maximum detection probability value that could be achieved by utilizing relative and absolute thresholding method in slot, short-term window, and long-term window.

A false alarm occurs when there is not any jammer attack but the alarm tiggers denoting the attack. It is the ratio of total false alarm numbers over the total duration of experiments [61]. We have a false alarm when interference is detected in the PRB in an OFDM symbol, but it’s not present there. In this thesis, the maximum allowed false alarm is set to be 1%.

Misdetection (MD) is the probability of not detecting the interferer even though it was present in the system. Technically, there was an interferer in some PRB in some OFDM symbol, but we could not detect it. Detection Delay (DD) is the average time between the jammer attack initiation and its detection is known to be detection delay time [61]. For example, in a 30 kHz SCS, if we average the empty PRBs over 10 slots then the detection

delay is 5ms and similarly for 1000 slots, the delay is 5s. With the increase in number of slots, the detection delay increases.

4.4 Noise and Interference Heat Map

A heat map is a technique to represent the data which demonstrates magnitude of certain phenomena in two dimensions in the form of colors [63]. Here, it is a plot which shows how power variates over frequency and time within a slot time duration for a given average matrix. From the heat map, the high-power variation suggests that there is an interference in that region. It also gives a visual representation of those PRBs that are interfered. The power levels represent the noise and interference, and the size of the matrix is defined by the dimension of the slots. Figure 5.2 and 5.3 gives the idea about the heatmap.

Each UE represents one PUSCH channel in the system. Interferers are being modelled as one region of PRBs filled up with random M-QAM symbols. M level is generic representation for 4 QAM, 16 QAM, 64 QAM, etc. symbols.

From the detection technique as mentioned in this chapter, not all the jammers could be detected. Since this technique is completely focused on PUSCH and based on presence of empty PRBs, the calculation of average energy of empty PRBs per slot basis enables the detection of the constant jammer, channel hopping jammer, follow-on jammer, and pulsed noise jammer.

5 SIMULATIONS AND RESULTS

This chapter explains the overall simulation process performed by utilizing the slot and averaging window concept with relative and absolute thresholding methods which was explained in Chapter 4. As per the desired objective, the detection of jamming or interference in the physical layer of 5G NR uplink is studied and presented in a simulated system where MATLAB is utilized as a simulation environment. This chapter also includes a set of parameters that are utilized during simulator development.

5.1 Simulation System Model

The overall system model to detect the presence of any jamming or interference entity in the system is shown in Figure 5.1 and described in the later section. The main components in the system include NR UL transmitter, jamming signal generator, which get added up with the noise in AWGN signal generator. Then the power of the empty PRBs from the received signal is computed followed by averaging matrix formation, the power is then compared with the threshold power at a jammer detection block to identify the interfered PRBs, and a reference jammer detection block confirms whether the detected interfered PRB is a correct detection or only a false alarm.

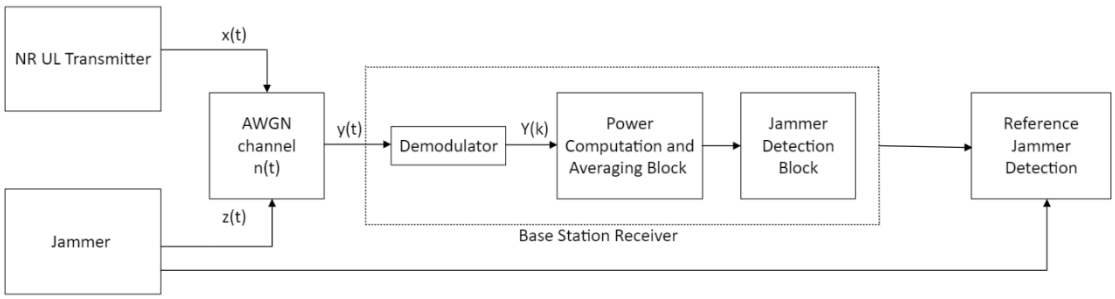

Figure 5.1: System block diagram

5.1.1 NR UL Transmitter

From the 5G NR toolbox, the example file NRUplinkWaveformGenerator [64] was used in this system after some modification. This file presents the idea on how to parameterize and generate a 5G NR UL waveform. PUSCH with its associated DMRS and PTRS signals were generated from it. Multiple bandwidth parts could be parameterized and generated over which PUSCH could be created. With 50 MHz channel bandwidth, 15 kHz and 30 kHz subcarrier spacing for the two carriers respectively, and after defining the position of bandwidth parts with normal CP, an OFDM symbol was created. For configuring the waveform, following parameters were considered in the NRUplinkWaveformGenerator file.

Table 5.1: Parameters required for waveform generation

Parameters	**Values**
Channel bandwidth	50 MHz
NcellID	0
Frequency range	FR1

Table 5.2: Parameters for generating carrier1 and carrier 2

Parameters	**Carrier 1**	**Carrier 2**
Subcarrier spacing	15 MHz	30 kHz
NRB	270	133
RB start	0	1

Table 5.3: Parameters set for generating two bandwidth parts

Parameters	**BWP 1**	**BWP 2**
Subcarrier spacing	15 MHz	30 kHz
Cyclic prefix	Normal	Normal
Size	129	64
Position	0	69

After assigning the values to the respective parameters, PUSCH is configured to provide random scheduling. The fraction of empty PRBs is modelled. The occupied PRBs are allocated to PUSCH channel whereas the empty ones are not allocated to any channels. The OFDM symbol is generated from this block after the selection of respective parameters. Suppose, N subcarriers are used, t is the OFDM symbol time, the desired OFDM signal is generated in time domain after each subcarrier is QAM modulated using M = 4 alternative symbols and IFFT is performed on the frequency-domain samples. In an OFDM signal, a guard interval of length T_g is inserted before the OFDM signal to remove

the intersymbol interference. During the guard interval, the desired CP is transmitted as explained in Section 2.1. The time domain representation of OFDM signal is:

$$x(t) = \sum_{k=0}^{N-1} X(k) e^{\frac{j2\pi kt}{T}}, \qquad -T_g \leq t < T \tag{5.1}$$

Where, $x(t)$ is the desired OFDM signal, T is the OFDM symbol time.

5.1.2 Jammer

Along with the waveform generation, the jammer is also introduced in the system. This section is all about modelling the constant and frequency sweeping interferers. In the first radio frame, the system would not have a jammer so that it would measure the metrics with the effect of channel and possible leakage from allocated PRBs. Here, Measuring Period is the period when it is assumed that there is no jammer. So, for first frame, jammer waveform is not created. A Jammer Waveform is the waveform obtained after modulating a jammer carrier where a jammer carrier is the 15 kHz SCS carrier that contains the jammer. After this, the parameter for jamming is defined which is shown in Table 5.4.

Table 5.4: Jammer Parameters

Jammer Parameters	**Values**
Jammer gain	-SIR (dB)
Jammer bandwidth	5 MHz
Jammer modulation	16 QAM
Jammer modulation order	4

Then, the number of PRBs occupied by the jammer is calculated and the random sequence of bit introduced by the jammer is extracted which is then modulated as per the QAM order of modulation to model the jammer. These created symbols are reshaped into a matrix form as symbol_matrix for PRB allocation.

In case of **Constant Jammer**, a default offset (it is the lower level from where the jammer starts making its consequence) of a jammer is calculated. Here, Similarly, the subcarrier spacing (SCS) carrier is created and then the symbol_matrix is allocated into this SCS carrier to enable the jammer to jam the system. The figure 5.2 shows the heat map for the constant jammer. The dark red spots in figure 5.2 and 5.3 is a jammer carrier containing

270 symbols. Jammer window contains all PRBs per OFDM symbol occupied by jammer within the detection window where, a detection window can be a slot, short-term window, or a long-term window. Basically, a jammer carrier has a jammer window.

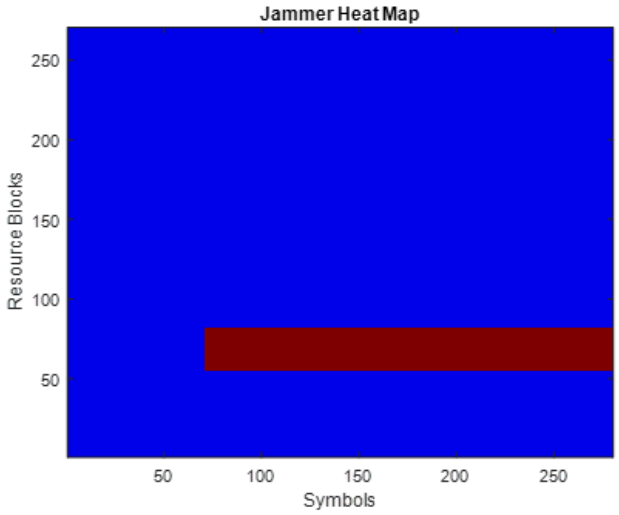

Figure 5.2: Constant Jammer heatmap

While in case of **Frequency Sweeping jammer**, the jammer sweeps through all the used frequencies starting from the bottom as shown in figure 5.4. Here it is configured in such a way that at every slot it changes from one frequency block to another. Initially, the counter for PRB is set to 1 and the SCS carrier is created for symbol allocation. Then the jammer is configured to use every slot where a loop is created for frequency sweeping algorithm to cover all the slots after the 1st frame, followed by creation of a set of subcarriers that changes every iteration according to sweeping. Then the symbol_matrix is allocated into the SCS carrier. If the sweeping gets to the end of the bandwidth, the process gets restarted.

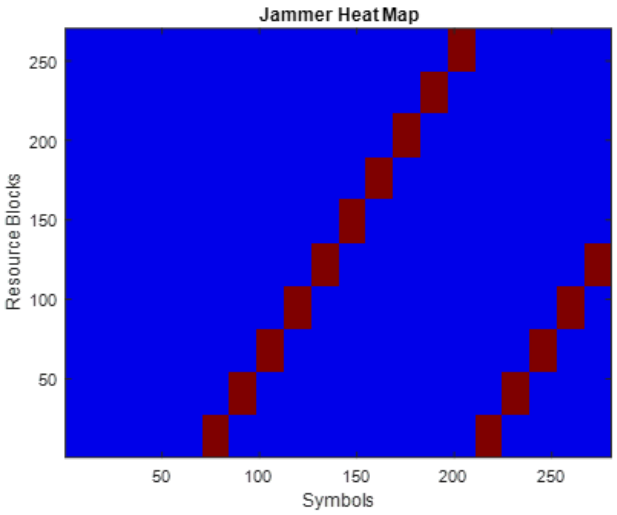

Figure 5.3: Frequency Sweeping Jammer heatmap

Since both jammers are in frequency domain, so, these jammers are modulated into the time domain to create a Jammer Waveform. The jammer and the desired UE signals are generated the same way as the generation of OFDM signal. The jammer signal is expressed as:

$$z(t) = \sum_{k=0}^{N-1} Z(k) e^{\frac{j2\pi k t_j}{T_j}}, \qquad -T_g \leq t_j < T_j \tag{5.2}$$

Where, $z(t)$ is the jammer signal, T_j is the jammer signal time

After extracting and modifying the MATLAB example file from MathWorks toolbox to and creating jammer signal, an OFDM waveform and a jammer waveform was generated for the system. These waveforms were then fed to the AWGN channel to get the signal to be transmitted to the receiver.

At an appropriate SNR level, a white gaussian noise is to be generated to add it with the input signal. If the input signal y(t) is real, then the noise is expressed as:

$$n(t) \sim N_{re}(t) \tag{5.3}$$

If the input signal y(t) is complex, then the noise is expressed as:

$$n(t) \sim [N_{re}(t) + N_{im}(t)] \quad 5.4$$

Where, $N_{re}(t)$ and $N_{im}(t)$ represent the random real and imaginary numbers from the standard normal distribution of input signal x(t) and z(t) at time t. Finally, the received OFDM signal and jammer signal with noise looks like:

$$y(t) \; = \; x(t) + \; z(t) + n(t) \quad 5.5$$

Where, $y(t)$ is the input signal with noise, $x(t)$ is the desired OFDM signal, $z(t)$ is the jammer signal and $n(t)$ is the gaussian noise from AWGN channel.

Then the cyclic prefix is removed from the desired OFDM and jamming signal and entire grid of each SCS carrier is further demodulated such that a time domain OFDM signal is converted into the frequency domain signal which is expressed as:

$$Y(k) = \frac{1}{N}\sum_{t=0}^{N-1} y(t)e^{\frac{-j2\pi kt}{T}} \quad 5.6$$

Then the power of each empty resource elements is calculated. This power is converted into resource block format where the mean from every 12 subcarriers is taken and is placed in resource block column. Similarly, the power of only the empty PRBs is computed along with the minimum power and maximum power for the current symbol. The power calculation is followed by short-term and long-term averaging which is explained in Chapter 4.

5.1.3 Jammer Detection Block

Here, slot based relative and absolute thresholding, short-term window based relative and absolute thresholding and long-term window based relative and absolute thresholding techniques are utilized to detect the interfered PRBs indices. Then the basic probabilities of jammer detection like correct detection, false alarm rate, miss detection and correct rejection are calculated after comparing the interfered indices with the reference jammer detection block in Subsection 5.1.4. This thesis is limited to the calculation of correct detection probability and false alarm rate.

The relative and absolute thresholding-based detection algorithm described in Section 4.1 is used here to return the interfered PRBs in slot, short-term window, and long-term window respectively. Hence if the power of empty PRB is greater than or equal to threshold, then the respective PRB in interfered otherwise it is not interfered.

Initially, the measuring period is converted from milliseconds to number of slots. At this period, in a loop of multiple OFDM symbols, the power of current OFDM symbol in an empty PRB $P(n,s)$ (explained in Section 4.1) is calculated and allocated to *power_matrix_slot*. Then if the number of slots is less than measuring period slots, the maximum and minimum threshold is updated. Whenever the slot is completed, *power_matrix_slot* is reset and process for next OFDM symbol continues otherwise, there is a direct process for next OFDM symbol.

For the detection based on slot relative and absolute thresholding, when the number of slots is greater than the measuring period, on the completion of a slot, if $P(n,s)$ is greater than or equal to $(\Delta_{Th} + \min(P(n,s))$, the indices of the interfered PRB are obtained from the relative thresholding. and if $P(n,s)$ is greater than or equal to max_{Th},, the indices of interfered PRBs are obtained from absolute thresholding as shown in Figure 4.1. Let $I_{slot,rel}$ and $I_{slot,abs}$ represent interfered PRBs from slot relative and absolute thresholding. Then, the power per slot is accumulated, the occurrences of empty PRBs per slot is counted to be used for short and long-term window.

For the detection by short-term window based relative and absolute thresholding, if the short-term window is completed, the short-term window as average power matrix: WST is calculated per number of slots. If WST is greater than or equal to $(\Delta_{Th} + \min(P(n,s))$, indices of interfered PRBs are obtained from relative thresholding and if WST is greater than or equal to max_{Th}, indices of interfered PRBs are received from absolute thresholding. In case of incomplete short-term windows, there is processing for next OFDM symbol. Let $I_{short,rel}$ and $I_{short,abs}$ represent indices of interfered PRBs from a short-term window relative and absolute thresholding.

For the detection by long-term window based relative and absolute thresholding, if the long-term window is completed, the long-term window as average power matrix: $WLT(t)$ is calculated per number of slots. If $WLT(t)$ is greater than or equal to $(\Delta_{Th} + \min(P(n,s))$, indices of interfered PRBs are obtained from relative thresholding and if $WLT(t)$ is greater than or equal to max_{Th}, indices of interfered PRBs are received from absolute thresholding. In case of incomplete long-term window, next OFDM symbol is processed. Let $I_{long,rel}$ and $I_{long,abs}$ represent indices of interfered PRBs from a long-term window relative and absolute thresholding. The basic concept of different techniques is represented by a flowchart below.

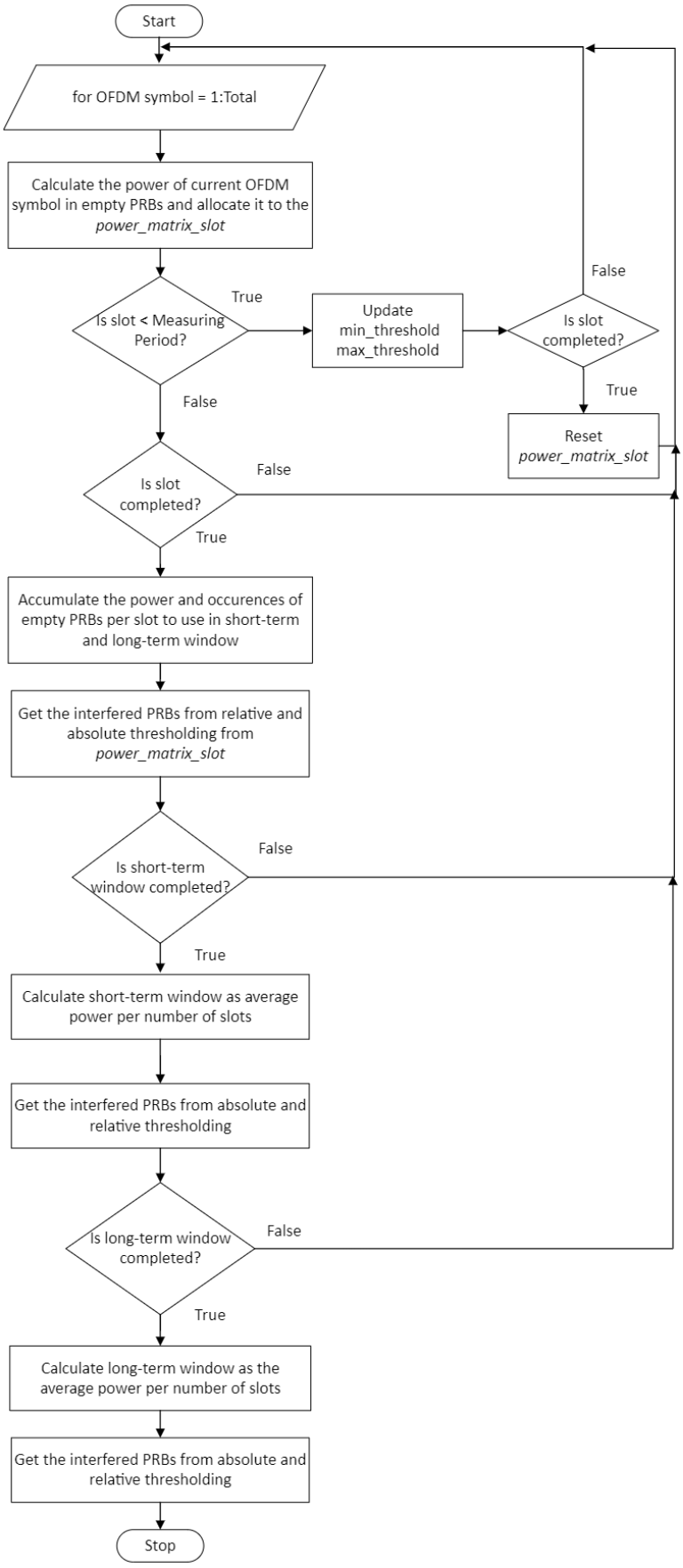

Figure 5.4: Flowchart for the Jammer Detection Method

5.1.4 Reference Jammer Detection

Whenever any PRB used by a jammer overlaps with any PRB of the desired signal PRB grid, that PRB is interfered. Even if the jammer is using 15 kHz SCS, then it is possible that it partially overlaps a 30 kHz signal. In case of any overlapping, the overlapped PRB is an interfered PRB. From this block, a reference information is obtained about which PRB in which OFDM symbols are interfered. Meanwhile Detection Algorithm is called here to get interfered PRBs from the transmitted signal of the jammer which is then compared with the jammer window which provides ideal reference for the computation of different probabilities. Jammer window is a window that contains all PRBs per OFDM symbol occupied by jammer within the slot, short-term, and long-term window respectively.

In a reference detection block, primarily, the total number of PRBs are extracted from the SCS resource grid along with the initialization of counters for basic probabilities of jammer detection like correct detection and false alarm rate with respect to slot, short-term window and long-term window basis. Here, one OFDM symbol is processed at a time per slot basis, the current OFDM symbol is obtained from the demodulated SCS resource grid and the index of the empty resource elements is extracted from the current OFDM symbol. And the measuring period for thresholding is converted from milliseconds to the number of slots respectively.

For jammer detection based on slot relative and absolute thresholding, for each slot, the jammer window is obtained from a jammer carrier (jammer carrier is a 15 kHz SCS carrier containing the jammer). Here, jammer window is a jammer slot window that contains all PRBs per OFDM symbol occupied by jammer within the slot. Let J_{slot} represent jammer slot window.

If $I_{slot,rel} = J_{slot}$ and $I_{slot,abs} = J_{slot}$, correct detection probability is calculated otherwise false alarm rate is updated.

For the jammer detection based on short-term windowing relative and absolute thresholding method, if the short-term window is completed, jammer short-term window is calculated by accumulating all the jammer slot windows present in a jammer slot window and dividing it by the occurrences of jammer slot window present in a short-term window. Let J_{short} represent jammer short-term window.

If $I_{short,rel} = J_{short}$ and $I_{short,abs} = J_{short}$, correct detection probability is updated otherwise there is update on the false alarm. This is followed by resetting matrices for window averaging.

For jammer detection based on long-term windowing relative and absolute thresholding, if the long-term window is completed, jammer long-term window is calculated by accumulating all the jammer slot windows present in a long-term window and dividing it by the occurrences of jammer slot window present in that long-term window. Let J_{long} represent jammer long-term window.

If $I_{long,rel} = J_{long}$ and $I_{long,abs} = J_{long}$, the correct detection probability is calculated otherwise there is a false alarm rate. Then the matrices are reset for window averaging. Finally, results are calculated in a table in MATLAB and plots for correct detection and false alarm rate are generated.

5.2 Simulation Findings for a Constant Jammer

After developing a jammer detection and reference jammer detection module, to meet the simulation requirements, a set of simulation parameters are initialized in the system which are tabulated in table 5.5 respectively,

Table 5.5: Main Simulation parameters

Parameters	**Values**
Number of radio frames	Upto 100
Measuring time	0.5 ms
SNR of interferers	10:1:15 (dB)
SIR of interferers	-20:2:20 (dB)
INR	SNR-SIR (dB)
Fraction of empty PRBs	50%
Number of transmitter antenna	1
Number of receiver antenna	1
Forgetting factor	0.1
Duration of short-term window in slot	10
Duration of long-term window in slot	100

The presence of a jammer in an empty PRB is identified via two detection methods: relative and absolute thresholding-based detection method which are then applied to three different heat maps: slot-based, short-term averaging window, and long-term averaging window-based power measurements. In total, slot based relative and absolute thresholding, short-term window based relative and absolute thresholding, and long-term window based relative and absolute thresholding concepts are utilized to detect the interfered PRBs. Section 5.1 explained about the simulation techniques used in a detecting an interfered PRB in an OFDM symbol. Similarly, this section presents the findings from the simulation that were carried out via MATLAB. Correct detection and false alarm rate for each method were calculated and represented in a plot.

As a result of comparing the interfered PRBs obtained as an output of Detection Algorithm with the output of Reference Jammer Detection in a Slot, figures 5.5 is obtained which gives information about whether the detected PRB was a correct detection, or it was only a false alarm. Both, relative thresholding, and absolute thresholding for the slot-based jammer detection technique gave false alarms of around 0.01% which is below the maximum allowed value 1%, although the correct detection is seen to be increasing with the increment in INR values. The measurements from absolute thresholding show that the correct detection starts ramping up to target 99% at lower INR values as compared to the relative thresholding. Correct detection is somehow interpolated as it exceeds 99%.

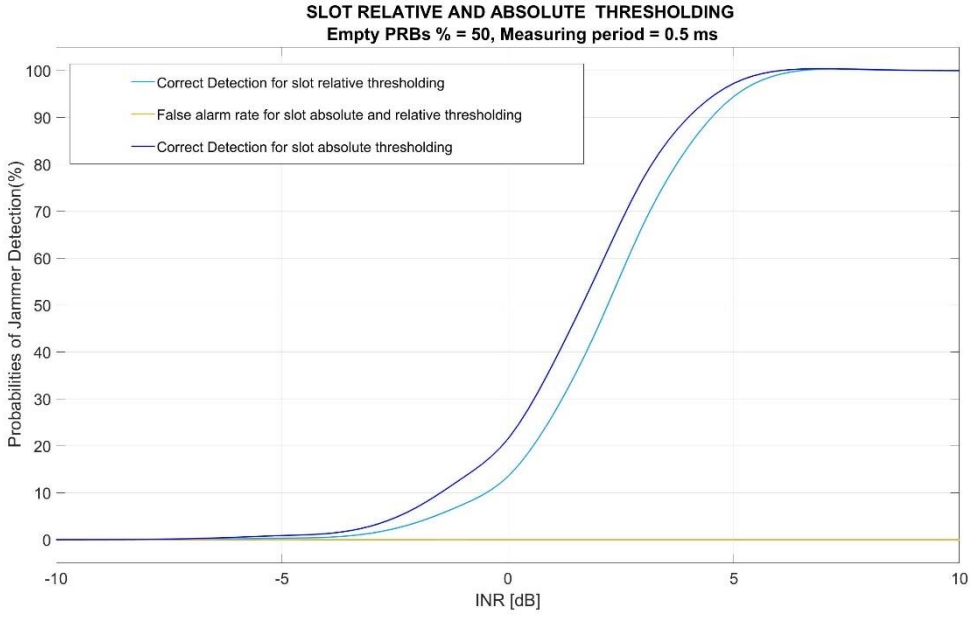

Figure 5.5: Correct detections and false alarm rates for slot relative and absolute thresholding

Figure 5.6 shows the plot including correct detections and false alarm rates from relative and absolute thresholding respective in a short-term window. These plots are the result from the comparison between the output of Detection Algorithm and Reference Jammer Detection. The short-term window relative thresholding-based detection method reaches the desired correct detection of 99% at around 4 dB INR value whereas the short-term window absolute thresholding-based detection method reaches the desired 99% correct detection probability at around 4.2 dB INR value.

With false alarm less than 1% at all the INR points, the correct detection ramps from 0 to target 99% faster at lower INR value in case of relative thresholding when compared with the absolute thresholding. Relative thresholding denotes the success of correct detection since it is improved earlier and receives 99% point sooner.

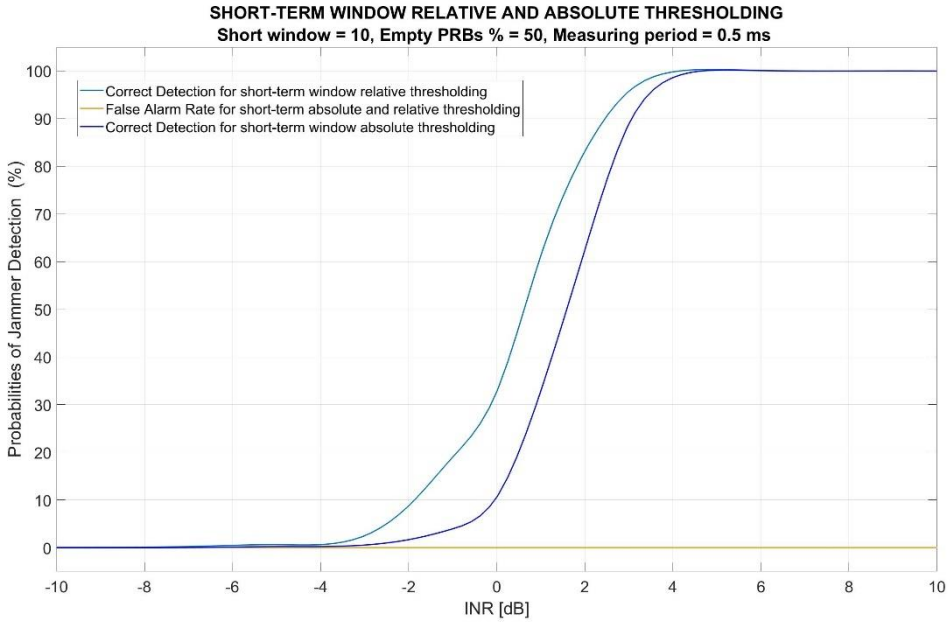

Figure 5.6: Correct detections and false alarm rates for short-term window relative and absolute thresholding

The plot including correct detection and false alarm rate for detection based on long-term window relative and absolute thresholding are shown in figure 5.7 respectively which is obtained after comparing the results of Detection Algorithm and Jammer Reference Detection in a long-term window. The long-term window relative thresholding-based detection method reaches the desired correct detection of 99% at around 2.1 dB INR value whereas the short-term window absolute thresholding-based detection method reaches the desired 99% correct detection probability at around 2.3 dB INR value.

Correct detection in long-term window shows similar response with correct detection in a short-term window. With almost negligible false alarm rates at all INR values, correct detection goes on increasing with the increase in INR values. The correct detection is seen ramping from 0 to 99% quickly (at low INR values) in case of relative thresholding than that at the absolute thresholding.

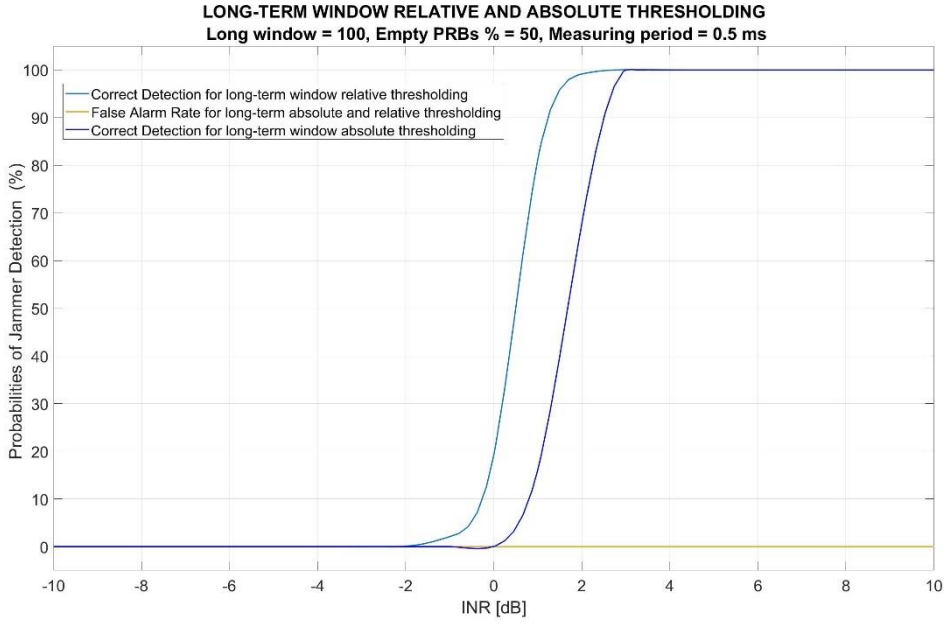

Figure 5.7: Correct detections and false alarm rates for long-term window relative and absolute thresholding

The figure 5.8 is the combination of correct detection and false alarm values in case of detection via slot relative and absolute thresholding, short-term window relative and absolute thresholding, and long-term window relative and absolute thresholding. The long-term window relative thresholding has a better performance as compared to other techniques since the correct detection in this method starts to meet 99% criteria quickly than the other techniques. Whereas correct detection in slot relative thresholding is the slowest to reach 99%. And false alarm rate is below 1% in all the cases. Hence, the long-term window relative thresholding is the best method among the chosen methods in this thesis. Table 5.6 shows the INR values at which each detection method reached the targeted correct detection point with almost negligible false alarm rates.

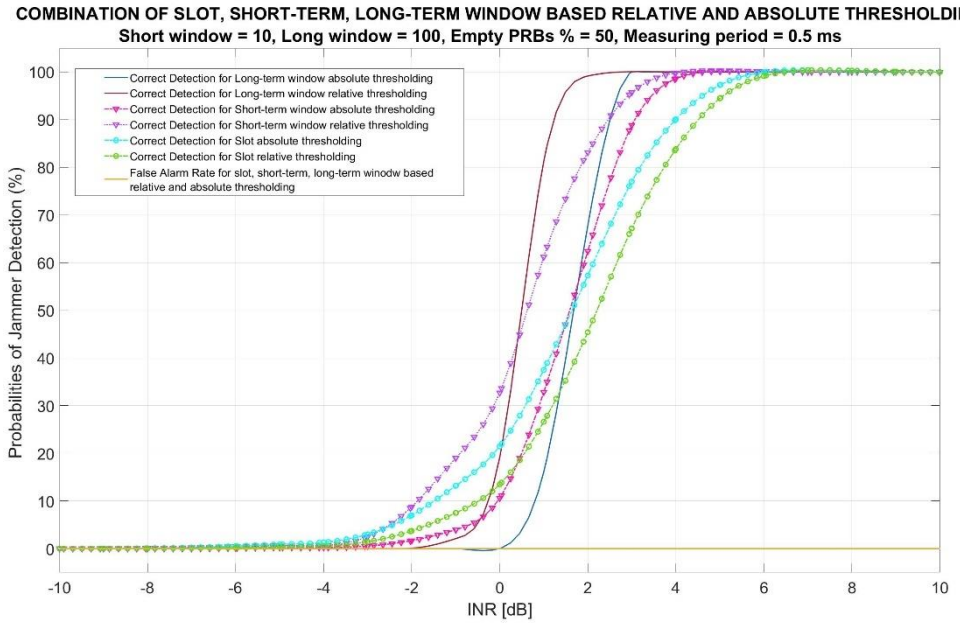

Figure 5.8: Combination of correct detection and false alarm rates for slot, short-term, long-term window based relative and absolute thresholding

Table 5.6: INR values where each detection Methods reached 99% correct detection

Detection Methods (Constant Jammer)	**INR values for correct detection (dB)**
Slot Relative Thresholding	5.2
Slot Absolute Thresholding	5.1
Short-term window Relative Thresholding	4.5
Short-term window Absolute Thresholding	5
Long-term window Relative Thresholding	2.5
Long-term window Absolute Thresholding	3

5.3 Simulation Findings for a Frequency Sweeping Jammer

This section includes the correct detection and false alarm rates in a slot, short-term, and long-term window based relative and absolute thresholding in case of frequency sweeping jammer by utilizing simulation parameters as mentioned in Table 5.5. The correct detections and false alarms from this jammer implementation are explained in figures 5.9 and 5.10. The figure 5.9 is the combination of correct detections in slot, short-term and long-term window based relative and absolute thresholding. The slot relative thresholding has a better performance since the correct detection in this technique meets the 99% criteria at lower INR values as compared to other techniques. Table 5.7 shows the INR values at which each detection method reached the targeted correct detection point.

As compared to constant jammer, frequency sweeping jammer is detected at much higher INR values, it is because of the reason that a frequency sweeping jammer keeps changing every time and power averaging technique makes it hard to detect. This jammer does not concentrate on the same PRBs for a long time rather it keeps changing from one PRB to another and average power is also decreased per PRBs in case of short and long-term window. So, frequency sweeping jammer is not detected easily.

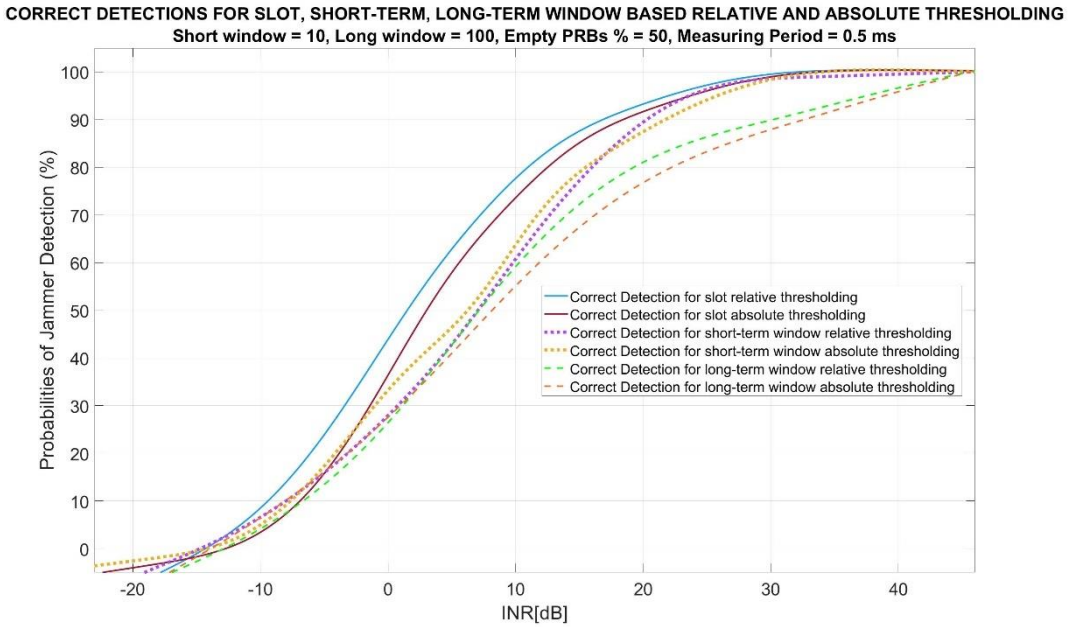

Figure 5.9: Correct Detections for slot, short-term, and long-term window based relative and absolute thresholding

Table 5.7: INR values where each detection Methods reached 99% correct detection

Detection Methods (Frequency Sweeping Jammer)	**INR values for correct detection (dB)**
Slot Relative Thresholding	31
Slot Absolute Thresholding	32
Short-term window Relative Thresholding	42
Short-term window Absolute Thresholding	33
Long-term window Relative Thresholding	44
Long-term window Absolute Thresholding	45

Figure 5.10 shows false alarm rates for slot, short-term and long-term based relative and absolute thresholding. The false alarm rate for slot relative thresholding is seen to achieve about 0.2% which is a very small and acceptable since it is below the maximum allowed false alarm rate of 1%. But other techniques seem to have either a modest increment or decrement in the false alarm rates. The false alarm rates for short-term window based relative thresholding and long-term window based relative and absolute thresholding are quite good since both methods give a decreasing false alarm rate and around 0.1% is the maximum value. Although the slot absolute thresholding has a maximum value above 0.2% among all methods, it is still below the maximum allowed false alarm rate and is acceptable. Short-term window absolute thresholding has also slight increase in the false alarm rate, but it is below 1%.

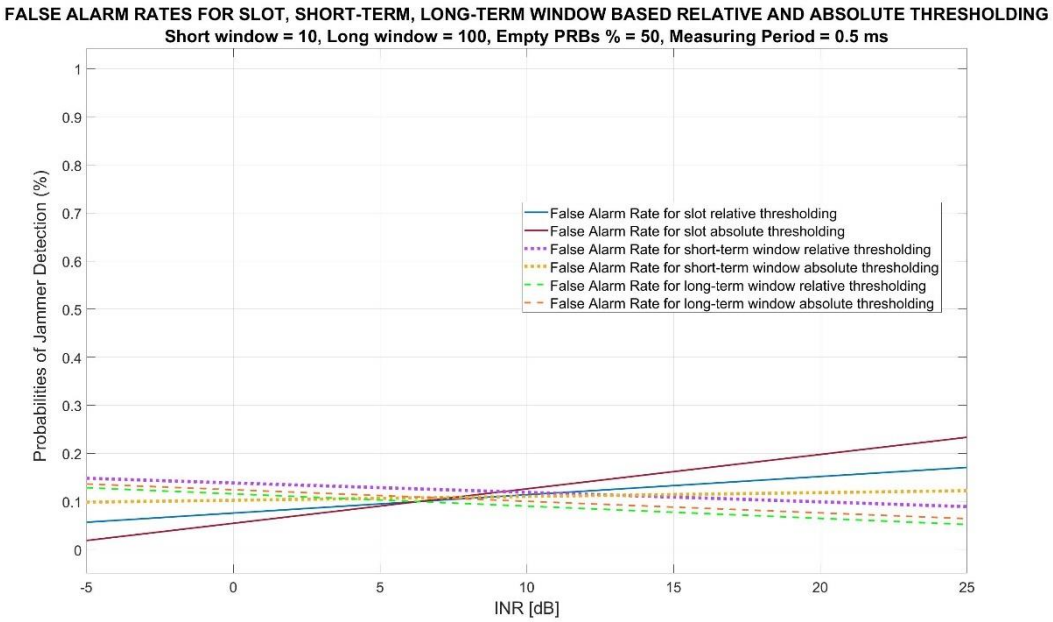

Figure 5.10: False Alarm Rates for slot, short-term and long-term window based relative and absolute thresholding

6 SUMMARY AND CONCLUSIONS

6.1 Conclusion

This thesis has investigated jammer detection mechanism as a solution against jamming in the physical layer of 5G NR system. After a short description about the 5G NR physical layer, the thesis explained how different physical channels and signals are vulnerable towards jamming. Although the thesis is limited to PUSCH channel, other channels and signals were studied to enhance understanding and to point out future research topics. It was also important to know the prevailing jammers and how those jammers could be detected. So, the main target was to study different types of existing jammer and various jammer detection strategies. After detailed research on jammer and jammer detection mechanism, constant jammer and frequency sweeping jammer were designed. To detect these jammers, two different detection algorithms were developed in MATLAB by utilizing the concept of relative and absolute thresholding. Jammer detection performance was further analyzed over three different power measurement heat maps: slot wise, short-term window, and long-term window.

Different detection algorithms and power measurement averaging options were evaluated by correct detection and false alarm probability. The detection delay related to different power measurement averaging windows was also shortly discussed. A reference jammer detection module was also developed to verify if the detected interference is a correct detection or only a false alarm. Then the results of slot based relative and absolute thresholding, short-term window based relative and absolute thresholding and long-term window based relative and absolute thresholding from detection algorithm were compared with the reference jammer detection to clarify on the correct detection and false alarm probabilities.

With respect to the developed algorithms, results were created for slot based relative and absolute thresholding, short-term window based relative and absolute thresholding and long-term window based relative and absolute thresholding for constant jammer as well as for the frequency sweeping jammer. From the results, it was analyzed that with 0.01% false alarm rates at all detection methods, long-term window based relative thresholding technique was successful to achieve 99% correct detection with lower INR in comparison to other techniques, making it the best method of jammer detection among all proposed techniques in case of constant jammer. However, in case of frequency sweeping jammer, with negligible false alarm rates at all detection methods, slot based relative thresholding technique was proved to be the best one with faster approach to meet 99% correct detection at lower INR in comparison to other detection strategies.

In case of both constant and frequency sweeping jammer, relative thresholding was proved to be the best detection algorithms as compared to absolute thresholding since in both the cases long-term window and slot-based heat maps were successful to achieve 99% target detection probability only with relative thresholding. Although false alarm rate values in case of frequency sweeping jammer was quite high (with maximum around 0.3%) as compared to that of constant jammer (with maximum around 0.01), both relative and absolute thresholding-based detection algorithm in combination with three different heatmaps gave false alarm rates less than 1% (a target value for false alarm rate) in both jammer types which is a pretty good outcome.

The long-term window based relative thresholding in case of constant jammer reached the targeted 99% correct detection point at INR value 3 dB, whereas the slot based relative thresholding in case of frequency sweeping jammer reached the targeted 99% correct detection point at INR value around 32 dB which is more in comparison to correct detection INR point in a constant jammer. This difference in the detection of constant and frequency sweeping jammer is due to the reason that a frequency sweeping jammer changes ever time from one PRB to another without concentrating on same PRB throughout its time as in a constant jammer which causes the decrease in average power per PRB. This decrease in the average power makes the jammer hard to be detected. And false alarm values in case of constant jammer were less and better as compared to that of frequency sweeping jammer for all detection algorithms. So, it can also be concluded that the constant jammer is easily detected and does not even give greater false alarm values. While frequency sweeping jammer is detected at larger INR value.

In this thesis, correct detection probability, and false alarm rate for two different jammers were calculated on the basis of three different detection methods: slot relative and absolute thresholding, short-term window relative and absolute thresholding, and long-term window relative and absolute thresholding. These calculated correct detection probability and false alarm rate were compared among six detection methods. The detection method that resulted the target detection probability at lowest INR value was considered to be best among all methods. So, based on these results, it is clear that relative thresholding is the best detection algorithm.

6.2 Future Research Lines

During this thesis preparation, some interesting lines of research were recognized that require more in-depth study. This thesis only includes two types of jammers whereas in the future, multiple different jammer types could be implemented, and their individual effect could be studied and evaluated with different fractions of empty PRBs. Along with implementing new jammer types, the optimal combination of slot, short-term window and

long-term window based relative and absolute thresholding techniques could be studied. The jammer detection techniques could be adapted from metric-based detection technique to machine learning based detection technique. Then, its performance could be compared with the metric-based threshold detection techniques which is used in this thesis.

Further research could also be carried out regarding jammer localization. This could be done by estimation of general covariance matrix of the interferer or estimation of the angle of arrival of the interferer. It could also be studied whether a jammer that fills the PRACH channel with random sequences or preambles could be detected or not. Most of these preambles have same delay or similar properties which should not happen at least in the wide area networks.

This thesis could also be extended to the addition of channels models other than AWGN. Frequency selective channel model could be introduced in the existing system with the addition of multiple receiver antennas in the base station receiver to analyze how correct detection and false alarm probabilities behave during this situation. Also, for further enhancement of the system performance, urban micro and urban micro-environments could be mapped to the newly introduced channel model.

7 REFERENCES

[1] "3GPP-Release-15-Specific-Aspect," [Online]. Available: https://www.3gpp.org/release-15. [Accessed 29 May 2022].

[2] T. B. Iliev, G. Y. Mihaylov, I. S. Stoyanov and E. P. Ivanova, "LTE and 5G NR – Coexistence and Collaboration," in *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*, Opatija, Croatia, 2020.

[3] S. Parkvall, Y. Blankenship, R. Blasco, E. Dahlman, G. Fodor, S. Grant, E. Stare and M. Stattin, "5G NR Release 16: Start of the 5G Evolution," *IEEE Communications Standards Magazine,* vol. 4, no. 4, pp. 56-63, 2020.

[4] L. Wan, Z. Guo and X. Chen, "Enabling Efficient 5G NR and 4G LTE Coexistence," *IEEE Wireless Communications,* vol. 26, no. 1, pp. 6 - 8, February, 2019.

[5] Y. Arjoune and S. Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2020.

[6] H. Akhlaghpasand, E. Björnson and S. M. Razavizadeh, "Jamming Suppression in Massive MIMO Systems," *IEEE Transactions on Circuits and Systems II: Express Briefs ,* vol. 67, no. 1, pp. 182-186, January, 2020.

[7] Y. Arjoune, F. Salahdine, M. S. Islam, E. Ghribi and N. Kaabouch, "A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication," in *2020 International Conference on Information Networking (ICOIN)*, Barcelona, Spain, January, 2020.

[8] "3GPP-Release-17-Specific-Aspects," 3GPP A GLOBAL INITIATIVE, [Online]. Available: https://www.3gpp.org/release-17. [Accessed 18 May 2022].

[9] M. Barberis, *Understanding and Modeling the 5G NR Physical Layer,* MATLAB EXPO 2019, 2019.

[10] "What is 5G," [Online]. Available: https://www.qualcomm.com/5g/what-is-5g. [Accessed 22 April 2022].

[11] A. Zaidi, F. Athley, J. Medbo, U. Gustavsson, G. Durisi and X. Chen, "Waveform," in *5G Physical Layer: Principles, Models and Technology Components*, ELSEVIER, 2018, p. 24.

[12] "5G-NR-Physical-Layer," [Online]. Available: https://www.rfwireless-world.com/Articles/5G-NR-Physical-Layer.html. [Accessed 22 April 2022].

[13] E. Dahlman, S. Parkvall and J. Sköld, in *5G NR The Next Generation Wireless Access Technology* , San Diego, Elsevier Science & Technology, 2020, p. 86.

[14] "5G-NR,TS-38.200-Document-Series," [Online]. Available: https://www.3gpp.org/DynaReport/38-series.htm. [Accessed 18 May 2022].

[15] "TS-38.201-Related-Aspects," [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3211. [Accessed 18 May 2022].

[16] ”5G NR PHY Layer,” DEVOPEDIA, [Online]. Available: https://devopedia.org/5g-nr-phy. [Haettu 12 10 2022].

[17] K. Jang, D. Kim, C. An ja H. G. Ryu, ”Window Processing of SSB CP-OFDM System for the OOB Spectrum Reduction,” tekijä: *International Conference on Electronics, Information, and Communication (ICEIC)*, Auckland, New Zealand, 2019.

[18] A. F. Demir, "Performance Enhancement Techniques for Next-Generation Multi-Service Communication and Medical Cyber-Physical Systems," ResearchGate, Florida, 2020.

[19] A. Lipovac, V. Lipovac and B. Modlic, "PHY, MAC, and RLC Layer Based Estimation of Optimal Cyclic Prefix Length," *Sensors,* p. 22, 2021.

[20] M. H. Habaebi, A. A. H. Budalal, A. M. A. Awad, I. M. Ali, A. S. Youssouf and S. A. Hameed, "A critique study on phase optimized generalized discrete fourier transform based partial transmit sequence for PAPR in OFDM systems," *ARPN Journal of Engineering and Applied Sciences,* vol. 10, no. 21, pp. 10077-10087, 2015.

[21] J. Flores de Valgas, J. F. Monserrat , . H. Arslan and M. Condoluci, "Flexible Numerology in 5G NR: Interference Quantification and Proper Selection Depending on the Scenario," *Hindawi,* vol. 2021, pp. 1-9, 10 March 2021.

[22] E. Dahlman, S. Parkvall and J. Sköld, in *5G NR The Next Generation Wireless Access Technology*, San Diego, Elsevier Science & Technology, 2020, pp. 125-126.

[23] S.-Y. Lien, S.-L. Shieh, Y. Huang, B. Su, Y.-L. Hsu and H.-Y. Wei, "5G New Radio: Waveform, Frame Structure, Multiple Access, and Initial Access," *IEEE Communications Magazine,* vol. 55, no. 6, pp. 64-71, 2017.

[24] M. Enescu, 5G New Radio: A Beam-based Air Interface, Newark: Wiley, 2020.

[25] M. Lichtman, R. Rao, V. Marojevic, J. Reed and R. P. Jover, "5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, Kansas City, MO, USA, May, 2018.

[26] F. Girke, F. Kurtz, N. Dorsch and C. Wietfeld, "Towards Resilient 5G: Lessons Learned from Experimental Evaluations of LTE Uplink Jamming," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, Shanghai, China, 11 July, 2019.

[27] P. Skokowski, J. M. Kelner, K. Malon, K. Maslanka, A. Birutis, M. A. Vazquez, S. Saha , W. Low, A. Czapiewska, J. Magiera, P. Rajchowski and S. Ambroziak, "Jamming and jamming mitigation for selected 5G military scenarios," in *International Conference on Military Communications and Information Systems*, 2022.

[28] Y.-H. Kim, H. Ju, C. B. Jeong and M.-S. Lee, "Performance comparison of DTX detection schemes for 5G NR PUCCH," in *International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, South Korea, 2020.

[29] L. Kundu, G. Xiong and J. Cho, "Physical Uplink Control Channel Design for 5G New Radio," in *2018 IEEE 5G World Forum (5GWF)*, Silicon Valley, CA, USA , July 2018 .

[30] Y. Kabalci and M. Ali, "Throughput Analysis over 5G NR Physical Uplink Shared Channels," in *Global Power, Energy and Communication Conference (GPECOM)*, Izmir, Turkey, 2020.

[31] "5G-NR-PRACH," [Online]. Available: https://www.rfwireless-world.com/5G/5G-NR-PRACH.html. [Accessed 28 May 2022].

[32] L. Tianyi and Z. Huijie , "Research on PDCCH Channel in 5G NR System," in *International Conference on Networking and Network Applications (NaNA)*, Lijiang City, China, 2021.

[33] X. Lin, J. Li, R. Baldemair, T. Cheng, S. Parkvall, D. Larsson, H. Koorapaty, M. Frenne, S. Falahati, A. Grövlen and K. Werner, "5G New Radio: Unveiling the Essentials of the Next Generation Wireless Access Technology," Research Gate, June 2018.

[34] M. Enescu, Y. Yuk, F. Vook, K. Ranta-aho, J. Kaikkonen, S. Hakola, E. Farag, S. Grant and A. Manolakos, "PHY Layer," in *5G New Radio: A Beam-based Air Interface*, Chichester, UK, Wiley, 2020, pp. 95-260.

[35] S. Ahmadi, "New Radio Access Physical Layer Aspects (Part 2)," in *5g Nr: Architecture, Technology, Implementation, and Operation of 3GPP New Radio Standards*, San Diego, Elsevier Science & Technology, 2019.

[36] "5G-NR,Reference-Signal-Structure," [Online]. Available: https://www.rfwireless-world.com/5G/5G-NR-Reference-Signals-DMRS-vs-PTRS-vs-CSI-RS-vs-SRS.html. [Accessed 1 June 2022].

[37] Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE ,* vol. 104, no. 9, pp. 1727 - 1765, September, 2016.

[38] "Node-Definition," [Online]. Available: https://www.techtarget.com/searchnetworking/definition/node. [Accessed 2 June 2022].

[39] A.-S. K. Pathan, H.-W. Lee and C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges," in *2006 8th International Conference Advanced Communication Technology*, Phoenix Park, February, 2006.

[40] K. Venkatraman, J. V. Daniel and G. Murugaboopathi, "Various Attacks in Wireless Sensor Network: Survey," *International Journal of Soft Computing and Engineering (IJSCE),* vol. 3, no. 1, pp. 208-211, March 2013.

[41] "Security for 5G Mobile Wireless Networks," *IEEE Access,* vol. 6, no. 2169-3536, pp. 4850 - 4874, 04 December 2017.

[42] M. A. Hasnat, M. Mamun-Or-Rashid, S. T. A. Rumee and M. A. Razzaque, "Security Study of 5G Heterogeneous Network: Current Solutions, Limitations & Future Direction," in *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, Cox'sBazar, Bangladesh, 2019.

[43] D. Fang, Y. Qian and R. Q. Hu, "Security for 5G Mobile Wireless Networks," *Security for 5G Mobile Wireless Networks,* vol. 6, no. 2169-3536, pp. 4850 - 4874, 04 December 2017 .

[44] K. Grover, A. Lim and Q. Yang, "Jamming and anti–jamming techniques in wireless networks: a survey," *International Journal of Ad Hoc and Ubiquitous Computing,* vol. 17, no. 4, pp. 197-215, 2021.

[45] I. Bennageh, H. Mahmoudi and M. Labbadi, "Impact of the Electromagnetic Environment on UAV's Datalink," in *International Conference on Innovative Research on Renewable Energy Technologies*, Malda, West Bengal, India, 2021.

[46] K. Pelechrinis, M. Iliofotou and S. V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," *IEEE COMMUNICATIONS SURVEYS & TUTORIAL,* vol. 13, no. 2, pp. 245-257, 2011.

[47] M. Zuba, Z. Shi, Z. Peng and J.-H. Cui, "Launching denial-of-service jamming attacks in underwater sensor networks," in *WUWNet '11: Sixth ACM International Workshop on Underwater Networks*, Washington, Seattle, 2011.

[48] K. Sharma and S. Bhatt, "Jamming Attack – A Survey," *International Journal of Recent Research Aspects,* vol. 5, no. 1, pp. 74-80, March, 2018.

[49] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials,* pp. 1-39, 14 March, 2022.

[50] M. Hachimi, G. Kaddoum, G. Gagnon and P. Illy, "Multi-stage Jamming Attacks Detection using Deep Learning Combined with Kernelized Support Vector Machine in 5G Cloud Radio Access Networks," in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, Montreal, QC, Canada , 25 December, 2020.

[51] S. Fang, Y. Liu and P. Ning, "Wireless Communications under Broadband Reactive Jamming Attacks," *IEEE Transactions on Dependable and Secure Computing,* vol. 13, no. 3, pp. 394 - 408, May-June 1 2016.

[52] A. Jain, M. K. Bhushanwar and M. V. Malviya, "A Survey on Jamming Attacks and Its Types in Wireless Networks," *International Journal of Technology Research and Management,* vol. 4, no. 6, pp. 1-8, June 2017.

[53] I. Broustis, K. Pelecrinis, D. Syrivelis, S. V. Krishnamurthy and L. Tassiulas, "FIJI: Fighting Implicit Jamming in 802.11 WLANs," in *International Conference on Security and Privacy in Communication Systems*, 2009.

[54] D. Pajkovski, N. Rendevski, Z. Kotevski and T. Dimovski, "Classification of Jamming Attacks and Detection and Prevention Techniques in Local Wireless Networks," in *International Conference on Applied Internet and Information Technologies*, 2018.

[55] W. Xu, W. Trappe, Y. Zhang and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *MobiHoc '05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computingMay*, May, 2005.

[56] M. Cheng, Y. Ling and W. B. Wu, "Time Series Analysis for Jamming Attack Detection in Wireless Networks," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Singapore, December, 2017.

[57] A. Bengag, O. Moussaoui and M. Moussaoui, "A new IDS for detecting jamming attacks in WBAN," in *2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS)*, Marrakech, Morocco, 28-30 Oct. 2019.

[58] B. Yu and L.-Y. Zhang, "An improved detection method for different types of jamming attacks in wireless networks," in *The 2014 2nd International Conference on Systems and Informatics (ICSAI 2014)*, Shanghai, China, 15-17 Nov. 2014.

[59] O. Osanaiye, A. S. Alfa and G. P. Hancke, "A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks," *Sensors,* vol. 18, no. 6, pp. 1-15, 2018.

[60] S. Mishra, R. Singh and S. R. Mohan, "Information Warfare-Worthy Jamming Attack Detection Mechanism for Wireless Sensor Networks Using a Fuzzy Inference System," *Sensors,* vol. 10, no. 4, pp. 3444-3479, 2010.

[61] A. G. Fragkiadakis, V. A. Siris and A. P. Traganitis, "Effective and robust detection of jamming attacks," in *2010 Future Network & Mobile Summit*, Florence, Italy, 16-18 June 2010.

[62] F. Salahdine and N. Kaabouch, "Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey," *Physical Communication,* vol. 39, April, 2020.

[63] "Heat-Map-Definition," [Online]. Available: https://www.techtarget.com/searchbusinessanalytics/definition/heat-map. [Accessed 28 May 2022].

[64] "UL-Carrier-Aggregation," MathWorks, [Online]. Available: https://ch.mathworks.com/help/5g/ug/uplink-carrier-waveform-generation.html. [Accessed 5 June 2022].